Araştırma *Kaymakçı&Karabayır/Kırklareli University Journal of Engineering and Science 9-1 (2023) 130-154*
DOI: 10.34186/klujes.1250928 *Geliş Tarihi:14.02.2023* *Kabul Tarihi:01.03.2023*

ASANSÖRLER İÇİN HATADA GÜVENLİ BİR ELEKTRONİK KART TASARIMI

Özgür Turay KAYMAKÇI[1*], Furkan KARBAYIR[2]

[1*]*Çanakkale Onsekiz Mart Üniversitesi, Mühendislik Fakültesi, Elektrik-Elektronik Mühendisliği Bölümü, Çanakkale, Türkiye*
[2]*Arkel Elektrik Elektronik A.Ş., İstanbul, Türkiye*

Öz

Dijitalleşme ve endüstri 4.0'ın etkisi ile gündelik hayatımızda kullandığımız birçok sistemde artık daha fazla elektronik ve programlanabilir elektronik bileşen bulunmaktadır. Bu artan karmaşıklık beraberinde birçok güvenlik riskini de açığa çıkartmıştır. İlgili sistemleri güvenli kılmak adına uluslararası camia birçok standart ve regülasyon ortaya koymuştur. Bu noktada IEC 61508 standardı güvenlikle ilgili sistemin hayata geçirebilmek için donanımsal ve yazılımsal açıdan gerekli özellikleri tanılamaktadır. Zaman içinde IEC 61508 temel alınarak birçok sektörel standart türetilmiştir. Lakin hem akademik camia hem de sektör temsilcileri EN 81-20 ve IEC 61508 kapsamında asansör sistemleri için ne şekilde elektronik sistemler geliştireceklerini tam olarak bilmemektedirler. Bu çalışma ile bu boşluğun kapatılması hedeflenmiş, ilgili tasarımı yapar iken nelere dikkat edilmesi gerektiği ve ilgili hesaplamaların hangi standartlara göre ne şekilde yapılması gerektiği ve çıkan sonuçların anlamı irdelenmiştir. Bu kapsamda asansör kapılarının pozisyonları hatada güvenli bir şekilde takip eden hatada güvenli bir elektronik kart geliştirilmiştir. Ayrıca yapılan hesaplamalar sonucunda tasarlanan kartın PFH_{SYS}=3.64 10^{-8} 1/h, SFF=0.876 ve HFT=1 değerlerine sahip olduğu gözlemlenmiş, buna göre sistemin IEC 61508 standardındaki SIL 3 güvenlik seviyesine sahip olduğu gösterilmiştir.

Anahtar Kelimeler: Fonksiyonel Güvenlik, Asansör, FMEA, Güvenilirlik

A FAIL SAFE ELECTRONIC CARD DESIGN FOR LIFTS

Abstract

With the impact of digitalization and Industry 4.0, many systems used in our daily lives include more electronic and programmable electronic components. This increased complexity has also revealed many safety risks. The international community has put forward many standards and regulations to make these systems safer. At this point, the IEC 61508 standard identifies the hardware and software requirements for a safety-related system to be implemented. Over time, many sectoral standards have been derived from IEC 61508.

Sorumlu Yazar: Özgür Turgay KAYMAKÇI, okaymakci@comu.edu.tr

DOI: 10.34186/klujes.1250928 *Geliş Tarihi:14.02.2023* *Kabul Tarihi:01.03.2023*

However, both academic community and sector representatives do not know exactly how to design electronic systems for lifts within the scope of EN 81-20 and IEC 61508. With this study, it was aimed to close this gap. What should be considered while making the relevant design, how the relevant calculations should be made according to which standards, and the meaning of the results were examined. In this context, a fail-safe electronic card has been designed that follows the positions of the lift doors safely in case of failure. In addition, it was observed that the designed card had PFH_{SYS}=3.64 10^{-8} 1/h, SFF=0.876 and HFT=1 values as a result of the calculations. It has also shown that the system has the SIL 3 safety level according to IEC 61508 standard.

Keywords: Functional Safety, Lifts, FMEA, Reliability

1. GİRİŞ

Modern asansörlerin tarihi, hammaddelerin dağ eteklerinden taşınma ihtiyacıyla başlar. Bu kapsamda ilk elektrikle çalışan asansör, Werner von Siemens tarafından 1878 yılında üretilmiştir. Malzeme mühendisliğindeki gelişim ve endüstri devrimi ise 1929 yılında Clarence Conrad Crispen'in ilk konut asansörünü üretmesini önünü açmıştır. Zaman içinde yolcu ve yük taşımacılığını bugünkü seviyesine taşımıştır.

Günümüzde asansör sistemleri hem mekanik hem de elektriksel pek çok güvenlik fonksiyonunu bünyesinde barındırmaktadır. Bu güvenlik fonksiyonları genellikle röleler ile birbirine bağlanmakta öyle ki rölelerin seri olarak bağlanmış normalde kapalı kontakları üzerinden bir güvenlik devresi oluşturmaktadır. En nihayetinde bu devre asansör motorunu süren ana kontaktörün bobinine seri olarak bağlanmakta ya da ilgili motoru süren sürücünün acil durdurma girişine bağlanmaktadır. Bu noktada güvenlik kontaklarından herhangi birisinin açması halinde ana kontaktörünün enerjisi kesilmekte ve asansör durmaktadır.

Klasik asansör sistemlerinde güvenlik devresinde bulunan alt ve üst limit anahtarlar, zorunlu yavaşlama anahtarları, kapı bölgesi manyetik anahtarları, vb. birçok eleman ya mekanik ya da elektromekanik cihazlardır. Diğer taraftan bu tip cihazlar gerek bakım ihtiyaçları gerekse montaj, bağlantı ve kablolama zorlukları nedeni ile günümüzde programlanabilir elektronik cihazlar ile hayata geçirilmeye başlanmıştır. Lakin bu elektronik sistemler diğer sistemlerden farklı olarak yüksek güvenilirlik ve hatada güvenli çalışma koşullarını sağlamak zorundadır.

DOI: 10.34186/klujes.1250928 *Geliş Tarihi:14.02.2023* *Kabul Tarihi:01.03.2023*

Bu noktada elektrik, elektronik ve programlanabilir elektronik cihazlarda fonksiyonel güvenliğin sağlanması için IEC 61508 standardı tanımlanmıştır [1]. Ayrıca konu ile alakalı EN 81-50 gibi sektörel standartlar da tanımlanmıştır. EN 81-50 standardı, asansör sistemlerinde güvenlik bütünlük seviyesine uygun programlanabilir elektronik cihazların tasarımı ile alakalı normatif kurallardan tanımlamaktadır [2].

EN 81-50 sektörel bir standart olması neticesinde asansör sistemlerinde olması gereken minimum güvenlik fonksiyonlarının neler olduğu ve bu güvenlik fonksiyonlarının sağlaması gereken en düşük güvenlik bütünlük seviyesi hakkında tavsiyeler vermektedir. Standarda göre ilgili güvenlik fonksiyonunun bertaraf ettiği riskin büyüklüğüne göre tasarlanması hedeflenen elektrik, elektronik ya da programlanabilir elektronik sistemin genellikle SIL 3 seviyesinde bir güvenlik bütünlük seviyesine sahip olması gerektiğini tavsiye etmekle beraber bazı güvenlik fonksiyonlarının SIL 2 olarak da tasarlanmasına izin vermektedir.

Endüstriyel sistemlerdeki dijitalleşmenin bir sonucu olarak sistemlerde açığa çıkan karmaşıklık fonksiyonel güvenliğe olan ilgiyi arttırmaktadır. Sistemlerde yazılım ve donanımsal olarak artan karmaşıklık birçok riski de beraberinde getirmekte; bu artan riskleri yönetmek ve kabul edilebilir seviyede tutmak için uygun risk yönetim süreçlerini ve sonuçta fonksiyonel güvenliğe uygun sistemlerin tasarlanmasını zorunlu kılmaktadır.

Bu kapsamda özellikle son yıllarda bir çok araştırma yapılmıştır. Flesch ve ekibi, sayısal sinyal işleme alanında bir vaka çalışmasını değerlendirerek FPGA uygulamalarında hata toleransına uygulanan bir güvenlik metodolojisi geliştirmişlerdir [3]. Meany ise değişken hız sürücüleriyle ilgili temel güvenlik standartlarını incelemiş ve motor enerjisinin güvenli şekilde sıfırlanmasının nasıl yapılabileceğini araştırmıştır [4]. Kim ve ekibi ise elektrikli gemiler için güç yönetim sistemleri için fonksiyonel güvenlik standartlarının uygulanabilirliğini ele almış ve EN 61508 standardına göre bir risk grafiği ve saat başına başarısızlık ihtimali değerlendirmesi sunmuşlardır [5]. Diğer taraftan Gradwell ise acil kapatma sistemlerinin emniyet bütünlük seviyesini belirlemek için fonksiyonel güvenlik tekniklerini kullanmış ve güvenli tasarım yaklaşımlarının proses endüstrileri tarafından nasıl uygulandığı üzerinde bir çalışma yapmıştır [6].

Ayrıca şunu ifade etmek gerekir ki son yıllarda yapılmış fonksiyonel güvenlik ve elektronik sistem tasarımı araştırmaları genellikle otomotiv endüstrisi merkezlidir. Sinha ve arkadaşları arızada

DOI: 10.34186/klujes.1250928 *Geliş Tarihi:14.02.2023* *Kabul Tarihi:01.03.2023*

çalışma yeteneklerine sahip telli fren sistemi için bir sistem mimarisi önermişlerdir öyle ki önerilen sistem mimarisine ait güvenlik ve güvenilirlik analizi, karayolu taşıtlarında elektrik/elektronik sistemlerin fonksiyonel güvenliği için ortaya atılmış ISO 26262 standardına göre yapılmıştır [7]. Bir başka çalışmada da Kilian ve arkadaşları ise otomotiv endüstrisinde güç sistemlerinin fonksiyonel güvenliğini incelemişler, ISO 26262'nin pratik uygulaması için yorumlar ve öneriler ortaya koymuşlardır. Bu kapsamda güvenlik gereksinimlerinin ASIL tahsisi ve ASIL ayrıştırma konumu, başarısızlık oranlarının türetilmesi ve farklı bileşenler arasındaki girişimin önlenmesi konusunda analiz ve tavsiyelere değinmişlerdir [8]. Yine bir diğer otomotiv endüstrisi ile ilgili çalışmada Pancik ve arkadaşları elektronik park freni ile ilgili kontrol yazılımıyla ilgili tehlike analizi ve risk değerlendirmesini incelemiş, sistemin fonksiyonel mimarisine kapsayan yazılım öğelerinin sağlaması gereken ASIL risk seviyelerini belirlemiştir [9].

Konunun artan önemine istinaden birçok derleme çalışması da yapılmıştır. Yakın zaman önce Wang ve arkadaşları güç elektroniği bileşenleri ve donanım sistemleri üzerine yapılan araştırmaların güvenilirlik yönlerine ilişkin bir güncelleme çalışması yapmışlar; başarısızlık mekanizmaları, test yöntemleri, birikmiş hasar modellemesi ve görev profiline dayalı güvenilirlik tahmini konusundaki en son gelişmeleri sunmuşlardır [10]. Bir başka derleme çalışmasında ise özellikle küçük şebekelerde güç elektroniği güvenilirliğinin ve bunun sistem tasarımı üzerindeki etkisinin doğru bir şekilde araştırılmasını sağlamak için mevcut güvenilirlik yöntemleri incelenmiş, güç elektroniği ve güç sistemi güvenilirliği arasında köprü kuran son yayınlarla birlikte aşınma modelleme kavramlarının temel özellikleri ayrıntılı olarak tartışılmıştır [11].

Diğer taraftan asansör kontrol sistemine fonksiyonel güvenlik perspektifinden bakan çok fazla akademik çalışma ne yazık ki bulunmamaktadır. Uluslararası sektör temsilcileri genellikle sektörel olarak sağlaması gereken minimum koşulların tanımlandığı tasarım aşamasında yol göstermekten çok uzak, sadece hedefleri belirten EN 81-20 ya da EN 81-50 gibi standartlar yayınlamaktadırlar. Bu kapsamda yapılan tüm aktiviteler genellikle patent ile koruma altına alınmaktadır. Nadir yapılmış çalışmalardan bir tanesinde Soury ve arkadaşları PESSRAL merkezli olarak güvenlik zincirini incelemiş ve güvenlik zinciri içinde gerçek zamanlı iletişim sağlayan deterministik bir işlemci çekirdek mimarisi önermişlerdir [12]. Bu çalışmanın Soury ve arkadaşlarının yaptığı çalışmadan en büyük farklı ilgili çalışmada Soury ve arkadaşları sadece bir mimari önerir iken ilgili

DOI: 10.34186/klujes.1250928 *Geliş Tarihi:14.02.2023* *Kabul Tarihi:01.03.2023*

mimarinin ne şekilde geliştirilmesi gerektiği noktasında bir yol gösterme ya da hesaplama yapmamışlardır. Bu çalışmada ise gerekli hesaplama ve teknikler ile ilgili güvenlik bütünlük seviyesine ne şekilde ulaşılabileceği net bir şekilde gösterilmiştir.

Bu noktada bu çalışma ile hem literatüre katkı sağlamak hem de sektör temsilcilerine yol gösterebilmek adına güvenlik zincirine kolaylıkla dâhil edilebilecek bir elektronik kart tasarımı yapılmış, gerekli hesaplamalar yapılarak istenilen güvenlik bütünlük seviyesinin sağlandığının gösterilmesi hedeflenmiştir.

Bu kapsamda konu olan elektronik kart asansör kuyusuna güvenli erişim sağlanması maksadı ile kapıların açılmasının kontrolünü yapmayı hedeflemektedir. Bu kapsamda tasarlanan sistem asansör kat kapılarını gerçek zamanlı ve izlemekte ve herhangi bir şekilde kapının açılması durumunda kuyuya giriş algılayarak çıkış üretir. Bu çalışmaya konu olan elektronik kartın var olan asansör sistemleri ile uyumlu çalışabilmesi için hali hazırda işletilen güvenlik zincirine bağlanabilecek şekilde tasarlanmıştır. Kart bünyesinde hayata geçirilen tüm spesifikasyonlar özellikle EN 81-50 ve EN 81-20 referans alınarak oluşturulmuş ve minimum SIL 2 güvenlik bütünlük seviyesinde bir sistem geliştirilmesi hedeflenmiştir [13].

Bu çalışma 4 ana başlık altında toplanmıştır. Giriş kısmında konunun önemi, literatüre özeti ve makalenin yazılmasındaki ana motivasyon paylaşılmıştır. Materyal ve metot bölümünde genel olarak fonksiyonel güvenlik ve endüstrideki uygulama süreçlerinden bahsedilmiştir. Ayrıca bu bölümde bir sistemin güvenilirlik analizini yapabilmek için gerekli parametre ve yöntemlerden bahsedilmiştir. Sonraki bölümde tasarlanan elektronik kart tanıtılmış ve ilgili güvenilirlik hesaplamaları yapılmıştır. Son bölümde ise elde edilen sonuçlar paylaşılmış, kazanımlardan bahsedilmiştir.

2. MATERYAL VE METOT

Risk, bir olayın istenmeyen biçimde sonuçlanması olasılığıdır. Bir riskin ortaya çıkabilmesi için bir tehlikenin açığa çıkması ve bu kapsamda insanın direkt ya da dolaylı olarak ilgili tehlikeye maruz kalması gerekir. Bu noktada IEC, güvenliği mülkiyete veya çevreye verilen zararın bir sonucu olarak doğrudan veya dolaylı olarak insanların fiziksel yaralanma veya sağlığına zarar verme gibi kabul edilemez risklerden kurtulması olarak tanımlar. O zaman risk analizinde asıl

DOI: 10.34186/klujes.1250928 *Geliş Tarihi:14.02.2023* *Kabul Tarihi:01.03.2023*

amaç, sistemde oluşabilecek tehlikeli durumları sistematik bir şekilde tespit etmek ve bu riskleri kabul edilebilir seviyeye çekmektir [14]. Bu kapsamda risk yönetim süreçleri ile ilgili olarak ortaya koyulan aktiviteler 5 adımda toplanmıştır. Bu aktiviteler sırası ile

- Risklerin tanımlanması
- Risklerin analiz edilmesi
- Risklerin sınıflandırılması
- Riskleri engelleyici aktivitelerin belirlenmesi
- Riski takip edilmesi, izlenmesi

Risklerin doğru şekilde belirlenmesi ve kaynaklarının analiz edilmesi çok kritik bir süreçtir. Bu kapsamda asansör sistemleri ile ilgili sektörel standartlar belli oranda yol göstericidir. EN 81-50 Ek B ve ISO 22201-2 standartlarında konu detaylı bir şekilde incelenmiş ve asansör sektöründe sağlanması gereken fonksiyonel güvenlik isterlerinin neler olduğu genel olarak ifade edilmiştir. Diğer taraftan bilindik bir sistem olan asansör sisteminin bünyesinde bulunan bu riskler IEC 61508'e göre tasarlanmış uygun güvenlikle ilgili sistem üzerinden hayata geçirilmesi ve sektörel standartlarda tavsiye edilen güvenlik bütünlük seviyesinde olması gerekmektedir [15].

Bu noktada IEC 61508 güvenlikle ilgili bir sistemi " Kontrol altındaki ekipmanın güvenli bir duruma ulaşmak için gerekli güvenlikle ilgili işlevleri hayata geçirmesi tasarlanmış sistem" olarak ifade etmektedir [1]. Bu tanıma göre, tasarım aşamasında belirtilen koşullar ihlal edildiğinde güvenlikle ilgili sistem prosesi güvenli duruma taşımaktadır. Güvenlikle ilgili sistemler diğer gömülü sistemlerden farklı olarak özel olarak tasarlanmış algılayıcılar, kontrolörler ve eyleyicilerin oluşmaktadır öyle ki sistem risk analiz neticesinde öngörülen güvenlik fonksiyonlarını hayata geçiren algılayıcı, kontrolör ve eyleyicilerin bir kombinasyonudur. Tüm bu ekipmanların ortak kullanım amacı riskleri kabul edilebilir seviyeye indirgemektir. İlgili sektörlerde belirli bir kaliteyi korumak için bağımsız kuruluşlar bazı standartlar geliştirmiştir. IEC 61508, elektrikli, elektronik ve programlanabilir elektronik cihazlar için işlevsel güvenliği tanımlayan uluslararası ve önde gelen standarttır. Güvenlikle ilgili sistemlerin sahip oldukları güvenlik bütünlük seviyesinin hesaplanabilmesi için sistemi oluşturan bileşenler ile ilgili olarak bazı parametreler tanımlanmıştır. Güvenlikle ilgili sistemler, tanımlanan bu parametreler üzerinden sınıflandırılmış ve karşılaştırılmıştır.

DOI: 10.34186/klujes.1250928 *Geliş Tarihi:14.02.2023* *Kabul Tarihi:01.03.2023*

2.1. Arıza Oranı

Sistemin arızalanma sıklığıdır ve λ ile gösterilir. Sistemin, tanımlanan işlevleri yerine getirebileceği anlamına gelen güvenilirlik fonksiyonunun R(t) sistemin başarısız olma olasılığını gösteren, hata yoğunluğu fonksiyonuna f(t) oranıdır. Denklem 1'de verildiği gibi ifade edilir. Elektronik sistem bileşenleri için genellikle milyar çalışma saati başına arızalanan birim sayısı (FIT) ile ifade edilir. Arıza oranı, Denklem 2 ve Denklem 3'de ifade edildiği gibi sırasıyla güvenli arıza ve tehlikeli arıza olmak üzere iki farklı arızanın toplamıdır ve güvenli arıza oranı ise güvenlik oranı (S) ile arıza oranının çarpımıdır [16].

$$\lambda(t) = \frac{f(t)}{R(t)} \tag{1}$$

$$\lambda = \lambda_S + \lambda_D \tag{2}$$

$$\lambda_S = S\ x\ \lambda \tag{3}$$

Denklem 4'te belirtildiği gibi, tehlikeli bir arıza, tehlikeli tespit edilmiş arıza (DD) ve tehlikeli tespit edilmemiş arıza (DU) olmak üzere iki bölümden oluşur. Güvenlikle ilgili çalışmalarda, sistemin kullanım süresi içerisinde arıza oranının sabit olduğu kabul edilmektedir.

$$\lambda_D = \lambda_{DD} + \lambda_{DU} \tag{4}$$

Elektronik bileşen üreticileri yaptıkları bir dizi testler ile ilgili bileşene ait arıza oranını Denklem 5'de ifade edilen formül üzerinden belirtmektedirler [17].

$$\lambda = \frac{X^2(a,v)}{2\ D\ H\ A_f} \tag{5}$$

Burada X^2 ki-kare dağılımına karşı gelir iken D toplam teste tabi tutulan eleman sayısı, H değeri her bir eleman için test edilen süreyi ve son olarak A_f termal ivmelenme faktörü ise Denklem 6'da verilen Arrhenius denklemi ile tanımlanır.

$$A_f = \mathrm{e}^{\frac{E_a}{k}\left(\frac{1}{T_{use}} - \frac{1}{T_{test}}\right)} \tag{6}$$

Bu denklemde Ea değeri komponente ilişkin aktivasyon enerjisini (eV), T_{use} Kelvin cinsinden kullanma sıcaklığını, T_{test} değeri Kelvin cinsinden test sıcaklığını ifade eder iken k değeri Boltzmann sabitini tanımlamaktadır.

DOI: 10.34186/klujes.1250928 *Geliş Tarihi:14.02.2023* *Kabul Tarihi:01.03.2023*

2.2. Güvenli Arıza Oranı (SFF)

Denklem 5'te de verildiği gibi IEC 61508'e göre güvenli arıza ile tehlikeli tespit edilmiş arızanın tüm arızaya oranıdır. IEC 61508-6 Ek C'de Denklem 7'de gösterildiği gibi ifade edilir [1].

$$\mathrm{SFF} = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU}} \tag{7}$$

2.3. Ortalama Arıza Süresi (MTTF)

Bu süre endüstri tarafından kullanılan yaygın parametrelerden biridir ve bir sistemin veya herhangi bir ürünün ilk arıza meydana gelmesine kadar operasyonda kaldığı sürenin istatistiksel ortalamasıdır. Literatürde genellikle MTTF kısaltması ile sembolize edilir. Bir bileşenin MTTF değeri ne kadar yüksekse, o bileşenin birim zamanda arızalanma olasılığı o kadar düşüktür.

$$\mathrm{MTTF} = \int_0^T \mathrm{R(t)dt}$$

Tek bir bileşen için arıza oranı ve MTTF arasındaki ilişki $\mathrm{MTTF} = \frac{1}{\lambda}$ olarak ifade edilir [16].

2.4. Teşhis Kapsamı (DC)

İlgili sistemlerde ne ölçüde tehlikeli arızaların meydana gelebileceğinin bir ölçümüdür. DC ile sembolize edilir. IEC 61508-4 bölüm 3.8.6'ya göre Denklem 8'de verildiği gibi tanımlanır [1].

$$\mathrm{DC} = \frac{\sum \lambda_{DD}}{\sum \lambda_{DD} + \sum \lambda_{DU}} \tag{8}$$

Diğer taraftan $MTTF_{D,1}, MTTF_{D,2}, \dots, MTTF_{D,N}$ N farklı bileşen için ortalama tehlikeli arıza süresi olmak üzere teşhis kapsamı Denklem 9 ile hesaplanır.

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D,1}} + \frac{DC_2}{MTTF_{D,2}} + \cdots + \frac{DC_n}{MTTF_{D,N}}}{\frac{1}{MTTF_{D,1}} + \frac{1}{MTTF_{D,2}} + \cdots + \frac{1}{MTTF_{D,N}}} \tag{9}$$

2.5. Ortak Nedenli Arızalar

Bu tür arızalar, tek bir olay veya nedenin sonucu olarak birden çok alt sistemin arızalanmasına neden olan arıza türüdür. Literatürde ortak nedenli hataları tanımlamak için birden fazla yöntem tanımlanmış olmasına rağmen Fleming tarafından önerilen β faktör yöntemi halen yaygın olarak

DOI: 10.34186/klujes.1250928 *Geliş Tarihi:14.02.2023* *Kabul Tarihi:01.03.2023*

kullanılmaktadır [16], [18]. Bu yöntem β ve β_D değerlerini belirlemek için kantitatif bir yöntem önerir. Burada β ve β_D, sırasıyla tespit edilmemiş arızalar için genel ortak nedenli başarısızlık faktörünü ve tespit edilen arızalar için genel ortak nedenli arıza faktörünü tanımlar.

2.6. Donanım Hata Toleransı (HFT)

Donanım hata toleransı, alt sistemin veya bileşenin amaçlanan işlevini yerine getirmeye devam edebileceği maksimum hata sayısıdır. HFT, Denklem 10'a göre hesaplanır. Donanım hata toleransının N sayıda olması, N+1 sayıdaki hatanın emniyet fonksiyonunun emniyet kaybına sebep olacağı anlamına gelmektedir [16].

$$HFT_{sys} = \min_i HFT_i \tag{10}$$

2.7. Tip A ve Tip B Ekipman

IEC 61508 elektronik ekipmanları iki grup altında sınıflandırmıştır. İlgili ekipman için arıza modları iyi tanımlanmış ve elemanın hata koşulları altındaki davranışı tamamen tespit edilebilir durumda ise bu tip ekipmanları Tip-A olarak sınıflandırmıştır. Diğer taraftan ekipmana ait bileşenlerden en az bir tanesinin arıza modu iyi tanımlanmamış veya elemanın hata koşulları altındaki davranışı tam olarak belirlenemez durumdaysa bu tip olan ekipmanı Tip-B olarak kabul etmiştir [1].

2.8. Emniyet Bütünlük Seviyesi (SIL)

IEC 61508 tasarlanması hedeflenen sistemin güvenlik seviyesi Güvenlik Bütünlük Seviyesi kısaca SIL ile ifade edilen bir metrik üzerinden tanımlamıştır. Bu metriğe göre SIL 1 en düşük güvenlik seviyesi iken SIL 4 en yüksek güvenlik seviyesine karşılık gelir. Sistemin düşük talep modunda ya da yüksek talep modunda çalışmasına bağlı olarak sistemin sahip olduğu güvenlik bütünlük seviyesi Talep Esnasında Ortalama Arıza Olasılığı (PFD_{avg}) değeri ya da saat başına tehlikeli arıza olasılık değeri (PFH) üzerinden karar verilir. IEC 61508-1'e göre güvenlik bütünlük seviyelerinin olasılık aralıkları Tablo 1'de verilmiştir [16].

DOI: 10.34186/klujes.1250928 *Geliş Tarihi:14.02.2023* *Kabul Tarihi:01.03.2023*

Tablo 1. IEC 61508'e göre Güvenlik Bütünlük Seviyeleri

SIL	Düşük Talep Modu	Yüksek Talep Modu
4	$10^{-5} \leq PFD_{avg} < 10^{-4}$	$10^{-9} \leq PFH < 10^{-8}$
3	$10^{-4} \leq PFD_{avg} < 10^{-3}$	$10^{-8} \leq PFH < 10^{-7}$
2	$10^{-3} \leq PFD_{avg} < 10^{-2}$	$10^{-7} \leq PFH < 10^{-6}$
1	$10^{-2} \leq PFD_{avg} < 10^{-1}$	$10^{-6} \leq PFH < 10^{-5}$

Ayrıca bir sistemin SFF ve donanım hata tolerans değeri olan HFT'ye dayalı ulaşabileceği izin verilen maksimum güvenlik bütünlük seviyesi, IEC 61508-2'e göre

Tablo 2'de verilmiştir.

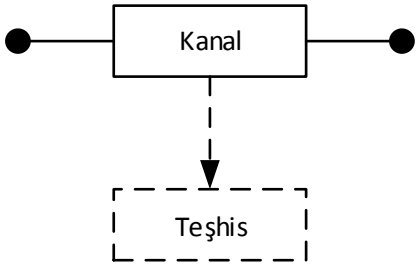
Tablo 2. Sistemin Ulaşabileceği Maksimum SIL Değeri

SFF	Donanım Hata Toleransı (HFT)		
	0	1	2
<60%	SIL1	SIL2	SIL3
60%<…<90%	SIL2	SIL3	SIL4
90%<…<99%	SIL3	SIL4	SIL4
>99%	SIL3	SIL4	SIL4

2.9. 1oo1 Güvenlikle İlgili Sistem Mimarisi

Bu mimaride sistem tasarımda tek bir bileşen bulunmaktadır. Bu tasarımda tarafından hiçbir hata toleransı sağlanmaz ve arıza modu korumasına sahip değildir. Elektronik devreler güvenli bir şekilde veya tehlikeli bir şekilde arızalanabilir. Bu sisteme ait güvenilirlik blok diyagramı Şekil 1'deki gibidir [1]

DOI: 10.34186/klujes.1250928 *Geliş Tarihi:14.02.2023* *Kabul Tarihi:01.03.2023*



Şekil 1. 1oo1 Fiziksel Sistem Mimarisi

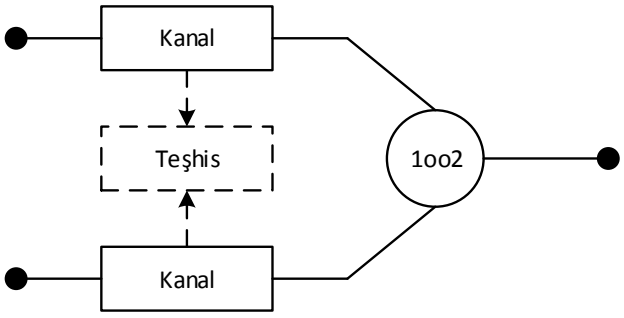
$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \quad (11)$$

$$PFD_{avg} = \lambda_D \, t_{CE} \quad (12)$$

$$PFH = \lambda_{DU} \quad (13)$$

2.10. 1oo2 Güvenlikle İlgili Sistem Mimarisi

Bu mimaride güvenlik fonksiyonu paralel bağlı iki kanal kullanarak hayata geçirilir. Bu nedenle, talep esnasında ilgili güvenlik fonksiyonunun arızalanması için her iki kanalda da öncesinde tehlikeli bir arıza olması gerekir. Bu mimaride herhangi bir teşhis testinin yalnızca hataları bildireceği ve herhangi bir çıkış durumunu veya çıkış oylamasını değiştirmeyeceği varsayılır. Bu sisteme ait sistem mimari şeması Şekil 2'deki gibidir. PFD_{avg} ve PFH değerleri Denklem 15 ve Denklem 16'ya göre hesaplanır [19].



Şekil 2. 1oo2 Fiziksel Sistem Mimarisi

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \quad (14)$$

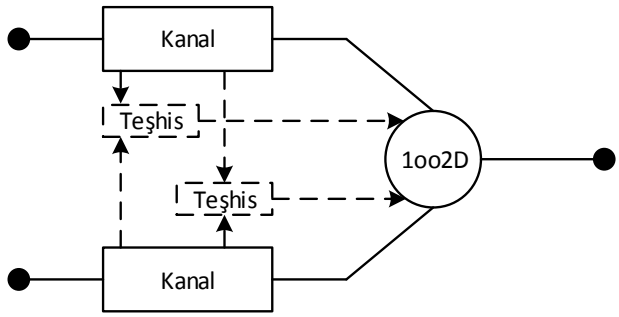
$$PFD_{avg} = 2[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]^2 \, t_{CE} \, t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU}\left(\frac{T_1}{2} + MRT\right) \quad (15)$$

DOI: 10.34186/klujes.1250928 *Geliş Tarihi:14.02.2023* *Kabul Tarihi:01.03.2023*

$$\text{PFH} = 2[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}](1-\beta)\lambda_{DU}t_{CE} + \beta\lambda_{DU} \quad (16)$$

2.11. 1oo2D Güvenlikle İlgili Sistem Mimarisi

Bu mimari, paralel olarak bağlanmış iki kanal içerir. Normal çalışma süresinde, güvenlik fonksiyonunun hayata geçirilebilmesi için her iki kanalında talepte bulunması gerekir. Ayrıca, herhangi bir kanaldaki teşhis testleri bir arıza tespit ederse, oylama devre dışı kalır ve diğer kanal tarafından verilen karar çıkışta üretir. Eğer her iki kanaldaki teşhis testleri arızalı bulunursa veya herhangi bir kanala atanamayan bir farklılık varsa sistem güvenli duruma gider. 1oo2D güvenlikle ilgili sisteme ilişkin prensip fiziksel sistem mimarisi Şekil 3'de verilmiştir. Bu mimari sisteme ilişkin olarak talep esnasında ortalama arıza olasılığı Denklem 20'ye göre hesap edilir [19].



Şekil 3. 1oo2D Fiziksel Sistem Mimarisi

$$\lambda_{SD} = \lambda_S\, DC \quad (17)$$

$$t'_{CE} = \frac{\lambda_{DU}\left(\frac{T_1}{2}+MRT\right)+(\lambda_{DD}+\lambda_{SD})MTTR}{\lambda_{DU}+(\lambda_{DD}+\lambda_{SD})} \quad (18)$$

$$t'_{GE} = \frac{T_1}{3} + MRT \quad (19)$$

$$PFD_{avg} = 2(1-\beta)\lambda_{DU}[(1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} + \lambda_{SD}]t'_{CE}t'_{GE} + 2(1-K)\lambda_{DD}t'_{CE} + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right) \quad (20)$$

2.12. Hata Modları ve Etki Analizi (FMEA)

Elektronik bileşenlerin birçok arıza modu bulunmaktadır ve bu modların analizi tasarımcıların bileşen arızalarını ve olası riskleri tanımasına yardımcı olmaktadır. Bu noktada güvenilirlik ihtiyaçlarını karşılayabilmek ve tasarımı iyileştirmek için gerekli alanların belirlenmesi gerekir. Hata modları ve etki analizi her bir elemanın hata modlarını ve sistemdeki olası risk kapsamındaki

DOI: 10.34186/klujes.1250928 *Geliş Tarihi:14.02.2023* *Kabul Tarihi:01.03.2023*

etkilerini tanımlar. Bu analiz neticesinde tanımlanmış risklere karşı önlemler tanımlanır. Donanım FMEA analizi, her bir elektronik elemanın hata modlarını kapsar. Elektronik bileşenler için donanım FMEA, EN IEC 60812 standardına göre standardize edilmiştir ve bileşenlerin temel hata modları tanımlanmıştır [20]. Örneğin, direnç veya kondansatör gibi pasif bir eleman için açık devre, kısa devre, değerin yükselmesi veya düşmesi olmak üzere 4 farklı hata modu bulunabilir. Aynı şekilde, transistor gibi bir yarıiletken içinde açık devre, kısa devre, fonksiyonun değişimi gibi hata modları da mevcuttur. Tablo 3'de bazı elektronik bileşenlerin hata modları verilmiştir.

Tablo 3. EN IEC 60812:2018 standardına göre bazı bileşenlerin hata modları

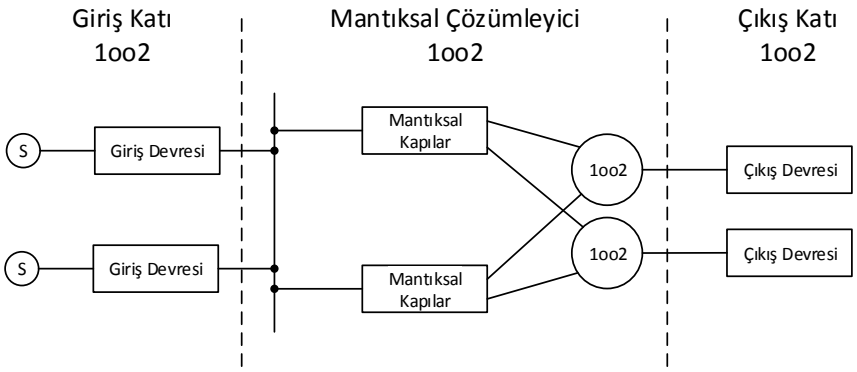
Bileşen	**Hata Modları**				
	Açık Devre	Kısa Devre	Değer Yükselmesi	Değer Düşmesi	Fonksiyon Değişimi
Direnç	✓	✓	✓	✓	
Kondansatör	✓	✓	✓	✓	
İndüktans	✓	✓		✓	
Diyot	✓	✓			✓
Tristör	✓	✓			✓
Tümleşik Devre	✓	✓	✓	✓	✓
Sigorta		✓			
Röle	✓	✓			
PCB	✓	✓			

3. ELEKTRONİK KART TASARIMI VE GÜVENİLİRLİK DEĞERLERİNİN HESAPLANMASI

EN 81-20 standardı, asansör sistemleri özelinde sağlanması gereken güvenlik fonksiyonları ve bu fonksiyonları hataya geçirecek sistemlerin sağlaması gereken minimum güvenlik bütünlük seviye değerlerini belirtmektedir. "Kuyu boşluğu erişimine olanak veren herhangi bir kapının açılmasının kontrolü" güvenlik fonksiyonu için sistemin ez az SIL 2 seviyesinde olması gerektiğini ortaya koymaktadır. Bu çalışmaya konu olan elektronik kartın bu güvenlik fonksiyonunu hayata geçirmesi hedeflendiğinden tüm tasarım ve analiz süreçleri en nihayetinde sistemin minimum SIL 2 sağlamasını hedefleyecek yönde yapılmıştır. Sistem tasarımı noktasında güvenilirlik değerinin

DOI: 10.34186/klujes.1250928 *Geliş Tarihi:14.02.2023* *Kabul Tarihi:01.03.2023*

artırılması ve teşhis kapsam oranının yükseltilmesi amacıyla 1oo2 güvenlik mimarisinin seçilmesinin uygun olduğu kanaatine varılmıştır. Bu kapsamda tasarlanan elektronik karta ilişkin sistem blok mimarisi Şekil 4'de verilmiştir.

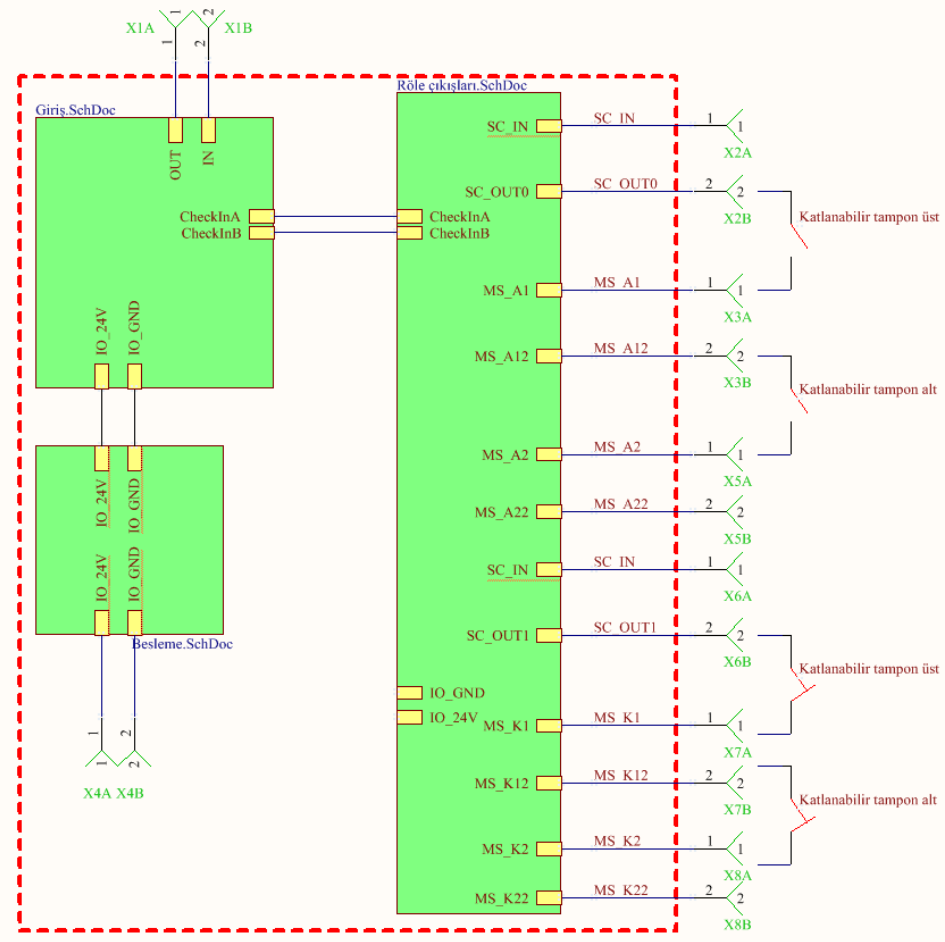


Şekil 4. Sistem blok mimarisi

Şekil 4'ten de gözlemlendiği gibi sistem 3 alt sistemden oluşmaktadır. Bunlar sırası ile giriş katı, mantıksal çözümleyici ve çıkış katıdır. Giriş katı gelen algılayıcı verilerini düzenleyerek mantıksal çözümleyiciye aktarmakta ve en nihayetinde alınan karar çıkış devreleri üzerinden asansör güvenlik zincirine hatada emniyetli röleler üzerinden iletilmektedir.

Asansör güvenlik zinciri normalde kapalı kontaklar üzerinden bağlı birçok röleden oluşan seri bir devredir. Bu devredeki herhangi bir röle açar ise devrenin enerjisi kesilmekte ve güvenlik çevrimi devre dışı kalmaktadır. Bu kapsamda tasarlanan elektronik karta ilişkin donanım temel şeması Şekil 5'de verilmiştir.

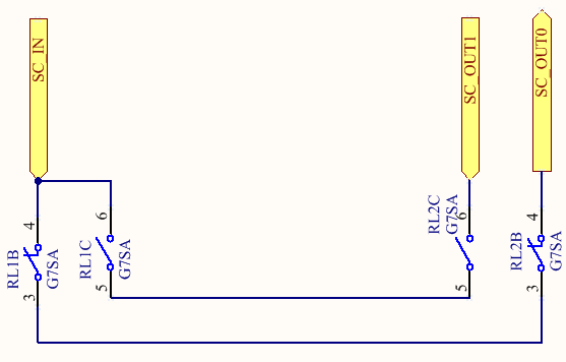
DOI: 10.34186/klujes.1250928 *Geliş Tarihi:14.02.2023* *Kabul Tarihi:01.03.2023*



Şekil 5. Donanım Şeması

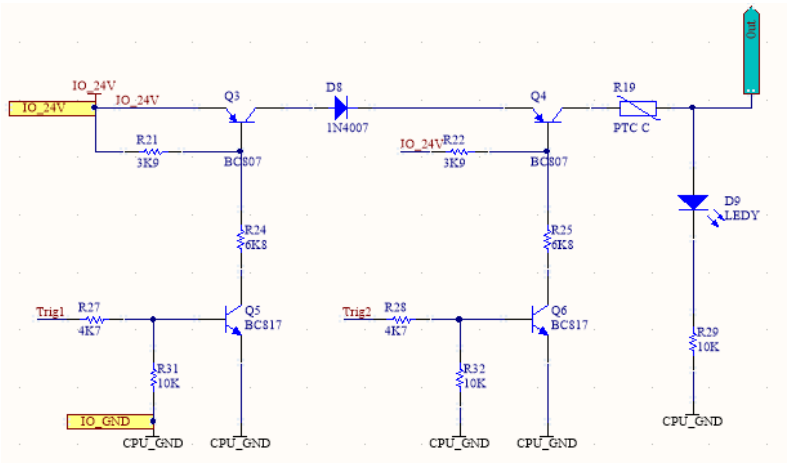
Emniyet devresi anahtarlama hattı şematik gösterimi ayrıca Şekil 6'da verilmiştir. Bu şematik, asansörün bakım durumunda ya da normal çalışma durumunda ilgili hat üzerinden hareket ettirilebilme durumunu gösterir. Eğer kuyu boşluğuna erişim sağlayan bir kapı açılmışsa (asansör bakım durumunda ise), emniyet röleleri düşecek ve emniyet devresi SC_Out0 hattından tamamlanacaktır. Ancak, eğer kuyu boşluğuna erişim sağlayan bir kapı açılmamışsa (asansör normal çalışma durumunda ise), emniyet röleleri çekecek ve emniyet devresi SC_Out1 hattından tamamlanacaktır. Aksi takdirde, asansör normal çalışma moduna geçemez.

DOI: 10.34186/klujes.1250928 *Geliş Tarihi:14.02.2023* *Kabul Tarihi:01.03.2023*



Şekil 6. Anahtarlama hattı şematik devre

Tasarlanan elektronik karttaki kuyu boşluğuna erişim sağlayacak kapı kontaklarından dolaştırılacak olan 24 V sinyalinin anahtarlama devresi Şekil 7'de verilmiştir. Asansör sistemindeki kapıların kapalı olduğunun doğruluğunu belirlemek için, iki kanal üzerinden bir sinyal gönderilmiştir. Bu, transistorlar arasındaki seri bağlantıların arızalanması durumunda sistemi güvenli hale getirmek için tasarlanmıştır. Bunun nedeni de 1oo2 yapısının kullanılmasıdır. Ayrıca 24 V dönen sinyal, tekrar iki kanal üzerinden okunmaktadır. Çift kanal üzerinden okuma bloğu, okuma devrelerinden birinin arızalanması durumunda, bu arızanın tespit edilmesi ve sistemin güvenli bir durumda tutulmasını sağlamaktadır.

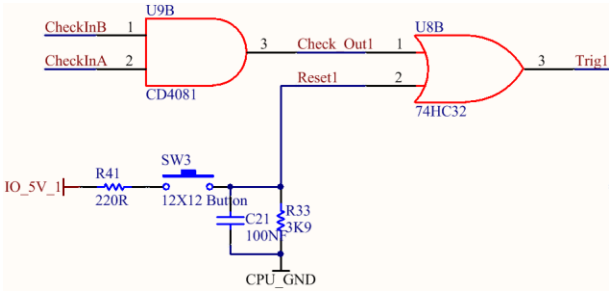


Şekil 7. Giriş bloğu sürme devresi

Şekil 8'de giriş bloğundaki elemanların arıza teşhis devresi verilmiştir. Buna göre kuyu boşluğuna erişim sağlayan kapıların kapalı olduğunun kontrolü için 24V sinyalini gönderen sistem, dönüş sinyalinin iki kanal üzerinden doğru olarak "1" olarak okunmasına dayanır. Eğer okuma

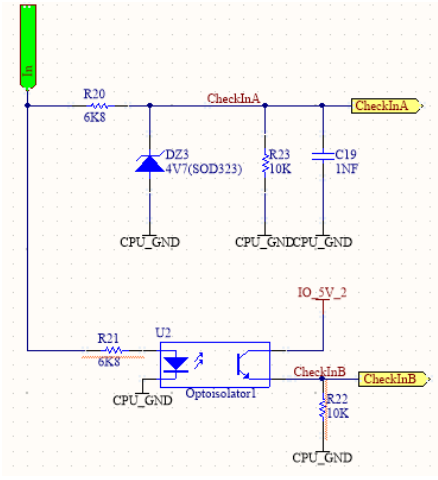
DOI: 10.34186/klujes.1250928 *Geliş Tarihi:14.02.2023* *Kabul Tarihi:01.03.2023*

devrelerinden birinde sinyal pozisyonu farklıysa, 24V sinyalini ileten transistorlar duracak ve sistem emniyetli durumda kalacaktır.



Şekil 8. Teşhis devresi

Hata! Başvuru kaynağı bulunamadı.'de de görüldüğü üzere ara yüz devresi çift kanallı olarak t asarlanmıştır. Ayrıca, ortak nedenli hata olasılığını azaltmak için, farklı tasarımlar kullanılmıştır. Bu amaçla, bir tasarım zener diyot ile ve diğeri optokuplör ile yapılmıştır. Bu tip tasarımlar, mantıksal çözücü bloğunda ya da giriş ve çıkış bloğunda tasarlanırsa, β faktörü oylamaları tablosunda ekstra puan olarak kabul edilmesi neticesinde bloğa ait ortak nedenli hata ihtimali azalmaktadır.



Şekil 9. Algılayıcı arayüz devresi

Giriş katındaki bileşenler, Tip-B türüne aittir. Bu durumda daha önce de ifade etmiş olduğumuz gibi sistem mimarisi olarak 1oo2 güvenlik mimarisi tercih edilmiştir. Şekil 4'de ilgili mimari verilmiştir. Buna göre giriş katına ilişkin HFT değeri 1'dir.

DOI: 10.34186/klujes.1250928 *Geliş Tarihi:14.02.2023* *Kabul Tarihi:01.03.2023*

Giriş katı alt sistem bloğu için eleman bazında detaylı donanım FMEA analizi Tablo 4'de verilmiştir. Tüm bileşenlere ait güvenilirlik değerleri IEC 62380 standardı referans alınarak türetilmiştir [21]. Bu tabloda λ ile ilgili elemanın FIT cinsinden arıza oranı verilmiştir.

Tablo 4. Giriş Katına ait Donanım FMEA

Eleman	**ID**	**λ**	**DC**	**S**	**λ_S**	**λ_D**	**λ_{DD}**	**λ_{DU}**
Direnç 6K8 Ω, %5, 0.125W	R20	10	0,9	0,5	5	5	4,5	0,5
Direnç 10K Ω %5, 0.125W	R23	10	0,9	0,5	5	5	4,5	0,5
Kondansatör seramik 1Nf	C19	3,5	0,9	0,5	1,75	1,75	1,58	0,18
Zener diyot BZX84B4V7	DZ3	0,79	0,9	0,75	0,593	0,197	0,178	0,02
Direnç 4K7 Ω, %5, 0.125W	R27	10	0,9	0,75	7,5	2,5	2,25	0,25
Direnç 10K Ω, %5, 0.125W	R31	10	0,9	0,75	7,5	2,5	2,25	0,25
Transistor BJT BC817 NPN	Q5	7	0,9	0,5	3,5	3,5	3,15	0,35
Direnç 6K8Ω, %5, 0.125W	R24	10	0,9	0,75	7,5	2,5	2,25	0,25
Direnç 3K9 Ω, %5, 0.125W	R21	10	0,9	0,75	7,5	2,5	2,25	0,25
Transistor BJT BCP53 PNP	Q3	7	0,9	0,5	3,5	3,5	3,15	0,35
Direnç 6K8 Ω, %5, 0.125W	R26	10	0,9	0,5	5	5	4,5	0,5
Direnç 10K Ω, %5, 0.125W	R30	10	0,9	0,5	5	5	4,5	0,5
Kondansatör seramik 1nF	C20	3,5	0,9	0,5	1,75	1,75	1,57	0,18
Zener diyot BZX84B4V7	DZ4	0,79	0,9	0,75	0,59	0,19	0,17	0,02
Direnç 4K7Ω %5, 0.125W	R28	10	0,9	0,75	7,5	2,5	2,25	0,25
Direnç 10K Ω %5, 0.125W	R32	10	0,9	0,75	7,5	2,5	2,25	0,25
Transistor BJT BC817 NPN	Q6	7	0,9	0,5	3,5	3,5	3,15	0,35
Direnç 6K8 Ω, %5, 0.125W	R25	10	0,9	0,75	7,5	2,5	2,25	0,25
Direnç 3K9 Ω %5, 0.125W	R22	10	0,9	0,75	7,5	2,5	2,25	0,25
Transistor BJT BCP53 PNP	Q4	7	0,9	0,5	3,5	3,5	3,15	0,35
Direnç PTC C	R19	22,9	0,9	1	22,94	0	0	0
Diyot 1N4007	D8	6,68	0,9	1	6,68	0	0	0
Buton	SW3	20	0,9	0,5	10	10	9	1
Kondansatör seramik 100nF	C21	3,5	0,9	0,5	1,75	1,75	1,58	0,18
Direnç 3K9 Ω, %5, 0.125W	R33	10	0,9	0,5	5	5	4,5	0,5
Buton	SW4	20	0,9	0,5	10	10	9	1
Kondansatör seramik 100nF	C22	3,5	0,9	0,5	1,75	1,75	1,58	0,18
Direnç 3K9 Ω, %5, 0.125W	R34	10	0,9	0,5	5	5	4,50	0,50

DOI: 10.34186/klujes.1250928 *Geliş Tarihi:14.02.2023* *Kabul Tarihi:01.03.2023*

İkinci alt sistem olan mantıksal çözümleyici blok da Tip-B türündedir, çünkü bu alt sistemde de hata koşulları altındaki davranışı tam olarak tanımlanmayan elemanlar bulunmaktadır. Bu nedenle, bu alt sistem de 1oo2 güvenlik mimarisi kullanılarak tasarlanmıştır. Mantıksal çözümleyici bloğa ait donanım FMEA Tablo 5'de sunulmuştur.

Tablo 5. Mantıksal Çözümleyici için Donanım FMEA

Eleman	**ID**	**λ**	**DC**	**S**	**λ_S**	**λ_D**	**λ_{DD}**	**λ_{DU}**
CD4081	U9	100	0,6	0,5	50	50	30	20
74HC32	U8	100	0,6	0,5	50	50	30	20
74HC08	U5	100	0,6	0,5	50	50	30	20
CD4030	U6	100	0,6	0,5	50	50	30	20
TC4001	U7	100	0,6	0,5	50	50	30	20

Tasarlanan elektronik kartın çıkış bloğu da Tip-B dir ve 1oo2 mimaride tasarlanmıştır. Benzer şekilde bu alt sistemin de HFT değeri Denklem 10'a göre 1'dir. Bu alt sisteme ait detaylı donanım FMEA analizi Tablo 6'da verilmiştir.

Tablo 4, Tablo 5 ve Tablo 6'da analog kart üzerinde bulunan tüm elemanlar ve bu elemanlara ait güvenilirlik parametreleri verilmiştir. Hesaplamalar bu güvenilirlik parametreleri ve Şekil 4'de verilen 1oo2 güvenlik mimarisine göre yapılmıştır. Ayrıca ortak nedenli hata oranı oranını tespit edebilmek için IEC61508-6 Annex D'de verilen tablo referans alınmıştır. Buna göre giriş katı, mantıksal çözümleyici ve çıkış katlarına ait ortak nedenli hata oranları elde edilmiş ve Tablo 7'de verilmiştir.

DOI: 10.34186/klujes.1250928 *Geliş Tarihi:14.02.2023* *Kabul Tarihi:01.03.2023*

Tablo 6. Çıkış Katı için Donanım FMEA

Eleman	**ID**	**λ**	**DC**	**S**	**λ_S**	**λ_D**	**λ_{DD}**	**λ_{DU}**
Güvenlik rölesi SFS3	RL1	190	0,9	0,5	95	95	85,5	9,5
Diyot 1N4007	D4	6,68	0,6	0,5	3,34	3,34	2,004	1,336
MELF direnci 100R Ω 1W	R4	10	0,6	0,5	5	5	3	2
Direnç 6K8 Ω, %5, 0.125W	R6	10	0,6	0,75	7,5	2,5	1,5	1
Direnç 4K7 Ω, %5, 0.125W	R5	10	0,6	0,75	7,5	2,5	1,5	1
Transistor BJT BC817 NPN	Q1	7	0,6	0,5	3,5	3,5	2,1	1,4
Güvenlik rölesi SFS3	RL2	190	0,9	0,5	95	95	85,5	9,5
Diyot 1N4007	D6	6,68	0,6	0,5	3,34	3,34	2,01	1,34
MELF direnci 100R Ω 1W	R12	10	0,6	0,5	5	5	3	2
Direnç 6K8 Ω, %5, 0.125W	R14	10	0,6	0,75	7,5	2,5	1,5	1
Direnç 4K7 Ω , %5, 0.125W	R13	10	0,6	0,75	7,5	2,5	1,5	1
Transistor BJT BC817 NPN	Q2	7	0,6	0,5	3,5	3,5	2,1	1,4
Direnç 3K9 Ω, %5, 0.125W	R7	10	0,6	0,5	5	5	3	2
Kondansatör seramik 100nF	C13	3,5	0,6	0,5	1,75	1,75	1,05	0,7
Direnç 3K9 Ω , %5, 0.125W	R10	10	0,6	0,5	5	5	3	2
Kondansatör seramik 100nF	C15	3,5	0,6	0,5	1,75	1,75	1,05	0,7
Direnç 3K9 Ω , %5, 0.125W	R15	10	0,6	0,5	5	5	3	2
Kondansatör seramik 100nF	C16	3,5	0,6	0,5	1,75	1,75	1,05	0,7
Direnç 3K9 Ω , %5, 0.125W	R16	10	0,6	0,5	5	5	3	2
Kondansatör seramik 100nF	C17	3,5	0,6	0,5	1,75	1,75	1,05	0,7
Buton	SW1	20	0,6	0,5	10	10	6	4
Direnç 3K9 Ω , %5, 0.125W	R9	10	0,6	0,5	5	5	3	2
Kondansatör seramik 100nF	C14	3,5	0,6	0,5	1,75	1,75	1,05	0,7
Buton	SW2	20	0,6	0,5	10	10	6	4
Direnç 3K9 Ω, %5, 0.125W	R18	10	0,6	0,5	5	5	3	2
Kondansatör seramik 100nF	C18	3,5	0,6	0,5	1,75	1,75	1,05	0,7

DOI: 10.34186/klujes.1250928 *Geliş Tarihi:14.02.2023* *Kabul Tarihi:01.03.2023*

Tablo 7. Ortak Nedenli Hata Oranları

	β	**β_D**
Giriş Devresi	%10	%10
Mantıksal Çözümleyici	%5	%5
Çıkış Devresi	%10	%10

Tablo 4, Tablo 5 ve Tablo 6'da verilen bileşenlere ait güvenilirlik parametrelerine göre alt sistemler MIL-HDBK – 217'e göre parça sayım metoduna üzerinden hesap edildiğinde her bir alt sisteme ilişkin hesaplanan güvenilirlik parametreleri Tablo 8'de verilmiştir. Bu tabloda arıza oranları FIT cinsindendir.

Tablo 8. Alt sistem güvenilirlik parametreleri

Alt Sistem	**λ**	**DC**	**S**	**λ_S**	**λ_D**	**λ_{DD}**	**λ_{DU}**
Giriş devresi	253,20	0.9	0.625	161.805	91,395	82,255	9,139
Mantıksal çözümleyici	500,00	0.639	0.5	250	250	150,00	100
Çıkış devresi	588	0.8005	0.5169	304.18	284.18	227.508	56.672

Tablo 8'de elde edilen güvenilirlik parametreleri üzerinden bir alt sistem için Denklem 16'ya ve Denklem 9'a göre hesaplanan PFH ve SFF değerleri ise Tablo 9'da verilmiştir.

Tablo 9. Alt sistemlere güvenilirlik değerleri

Alt Sistem	**PFH**	**SFF**	**HFT**
Giriş devresi (S)	$3.65\ 10^{-9}$	0.964	1
Mantıksal çözümleyici (L)	$1.002\ 10^{-8}$	0.8	1
Çıkış devresi (FE)	$2.28\ 10^{-8}$	0.904	1

Sisteme ilişkin saat başına tehlikeli arıza olasılık değeri ise tüm 3 alt sistemin PFH değerlerinin toplamı ile elde edilir. Buna göre

$$PFH_{SYS} = PFH_S + PFH_L + PFH_{FE} = 3.65\ 10^{-9} + 1.002\ 10^{-8} + 2.28\ 10^{-8}$$

$$PFH_{SYS} = 3.64x10^{-8}\ \ 1/h$$

DOI: 10.34186/klujes.1250928 *Geliş Tarihi:14.02.2023* *Kabul Tarihi:01.03.2023*

olarak elde edilir. Ayrıca sisteme ait SFF değeri de Denklem 9'a göre hesap edildiğinde 0.876 olduğu görülür ve sistemin tüm alt bileşenleri 1oo2 mimariye sahip olduğu için sistemin donanım hata tolerans değeri HFT=1'dir.

Tablo 1'e göre PFH değeri $10^{-9} \leq PFH < 10^{-8}$ aralığında olması neticesinde sistemin SIL 4 güvenlik bütünlük seviyesinde olduğu izlenimi açığa çıkmaktadır. Lakin HFT=1 ve SFF=0.876 olduğu için system

Tablo 2'ye göre tasarlanan elektronik kart maksimum SIL 3 seviyesinde olabilmektedir. Bu şartlar altında yukarıda tasarımı verilen kart için güvenlik bütünlük seviyesi IEC 61508'e göre SIL 3 olduğu söylenebilir.

3. SONUÇLAR

Dijitalleşmenin bir sonucu olarak gündelik hayatta kullandığımız birçok sistem tasarım noktasında giderek karmaşıklaşmaktadır. Asansör sistemleri de bu perspektiften son yıllarda çok büyük bir değişim geçirmiştir öyle ki birçok elektromekanik sistem yerini elektronik ya da programlanabilir elektronik sisteme bırakmıştır. Bu değişim beraberinde birçok riski de açığa çıkartmaktadır. Bu noktada geliştirilen bu sistemlerin IEC 61508 fonksiyonel güvenlik standardı merkezli olarak tasarlanması ve uygun güvenlik bütünlük seviyelerini sağlaması beklenmektedir. Bu çalışmada da bu değişime öncelik etmek adına "Kuyu boşluğu erişimine olanak veren herhangi bir kapının açılmasının kontrolü" güvenlik fonksiyonunu hayata geçiren yüksek güvenilirliğe sahip hatada güvenli bir elektronik kart geliştirilmiştir. Geliştirilen bu kartın SIL 3 güvenlik bütünlük seviyesine sahip olduğu ispat edilmiştir. İlgili tasarım EN 81-50 ve EN 81-20 referans alınarak hayata geçirilmiş, standartlardaki kısıtlara göz önünde bulundurulmuştur. Sektörel ihtiyaçları düşünerek sistemin asansör sistemlerine rahatlıkla entegre edilebilmesi için var olan güvenlik zincirine bağlanabilecek bir mimaride tasarım yapılmıştır. Kartın tasarımında kullanılan tüm elemanlara ait arıza oranları IEC 62380 referans alınarak sektörel çalışma koşullarına göre türetilmiştir. Geliştirilen bu güvenli elektronik kart ile asansör kontrol panosundaki bir kısım elektromekanik eleman azalmış ve kablo bağlantı yığınlarında azalma gözlemlenmiştir. Bu da bakım onarım noktasında zaman ve maliyet avantajı yaratacaktır.

Bu tasarlanan kart ile asansör kuyusuna güvenli erişim sağlanması maksadı ile kapıların açılmasının kontrolünün yapılması hedeflemektedir öyle ki asansör kat kapıları gerçek zamanlı

DOI: 10.34186/klujes.1250928 *Geliş Tarihi:14.02.2023* *Kabul Tarihi:01.03.2023*

olarak izlenmekte ve herhangi bir şekilde kapının açılması durumunda kuyuya giriş algılayarak 1oo2 güvenlik mimarisi üzerinden çıkış üretilmektedir. Bu elde edilen çıkış güvenlik zinciri üzerindeki iletimi kesmesi neticesinde asansör duruşa geçmektedir. 1oo2 güvenlik mimarisi üzerinden tasarıma gidilmesinin bir sonucu olarak sistemin herhangi bir katında bir arıza olması halinde sistem çalışmaya devam etmekte ve görevini ifa etmektedir. Tasarlanan sistemin güvenli arıza oranı değeri 0.876'dır. Bu da elektronik kart üzerinde oluşabilecek arızaların %87.6'sında sistemin güvenli duruma geçeceği manasına gelmektedir. EN 81-50 "Kuyu boşluğu erişimine olanak veren herhangi bir kapının açılmasının kontrolü" güvenlik fonksiyonunu için SIL 2 seviyesinde bir tasarımın yeterli olduğunu ifade etmektedir. Bu çalışmada ise SIL 3 seviyesinde daha güvenli bir çözüm ortaya koyulmuştur. Son olarak günümüzde yaşanan endüstri devriminin asansör sistemlerinde de birçok değişimi tetiklemesi bu çalışmaya konu olan yüksek güvenilirliğe sahip hatada güvenli elektronik kartların ilerleyen günlerde daha fazla gündeme geleceğini bizlere göstermektedir.

Semboller

SIL	Güvenlik Bütünlük Seviyesi
λ	Arıza Oranı
R(t)	Güvenilirlik Fonksiyonu
f(t)	Hata Yoğunluğu Fonksiyonu
FIT	Milyar Çalışma Saati Başına Arızalanan Birim Sayısı
S	Güvenlik Oranı
λ_S	Güvenli Arıza
λ_D	Tehlikeli Arıza
λ_{DD}	Tehlikeli Tespit Edilmiş Arıza
λ_{DU}	Tehlikeli Tespit Edilmemiş Arıza
SFF	Güvenli Arıza Oranı
MTTF	Ortalama Arıza Süresi
DC	Teşhis Kapsamı
β	Tespit Edilmemiş Arızalar İçin Genel Ortak Nedenli Başarısızlık Faktörü
β_D	Tespit Edilen Arızalar İçin Genel Ortak Nedenli Arıza Faktörü
HFT	Donanım Hata Toleransı
PFD_{avg}	Talep Esnasında Ortalama Arıza Olasılığı
PFH	Saat Başına Tehlikeli Arıza Olasılık Değeri
1oo1	Birde Bir
1oo2	İkide Bir

DOI: 10.34186/klujes.1250928 *Geliş Tarihi:14.02.2023* *Kabul Tarihi:01.03.2023*

1oo2D	Teşhis ile İkide Bir
FMEA	Hata Modları ve Etkisi Analizi
MTTR	Ortalama Tamir Zamanı

KAYNAKLAR

[1] CENELEC/IEC (2010). EN 61508-Functional safety of electrical/electronic/programmable electronic safety-related systems.

[2] CENELEC/IEC (2020). EN 81-50-Safety rules for the construction and installation of lifts. Examinations and tests Design rules, calculations, examinations and tests of lift components.

[3] Flesch B. F., Brand B., Figueiredo R. M. de, Prade L. R., and Silva M. Rosa Da (2016). Proposal of a functional safety methodology applied to fault tolerance in FPGA applications, in LATS 2016-17th IEEE Latin-American Test Symposium. doi: 10.1109/LATW.2016.7483331.

[4] Meany T. (2016). Functional safety for integrated circuits used in variable speed drives, PCIM Europe 2016, International Exhibition and Conference for Power Electronics, Intelligent Motion, Renewable Energy and Energy Management.

[5] Kim S. D., Kim T. O., and Kang G. H. (2016). A study on the application of functional safety for PMS of electric propulsion ships, in 2016 IEEE Transportation Electrification Conference and Expo, Asia-Pacific, ITEC Asia-Pacific 2016. doi: 10.1109/ITEC-AP.2016.7512958.

[6] Gradwell B. (2017). Arc Flash\Blast, Safe by Design a Safety Integrity Level approach (SIL), IEEE IAS Electrical Safety Workshop. doi: 10.1109/ESW.2017.7914852.

[7] Sinha P. (2011). Architectural design and reliability analysis of a fail-operational brake-by-wire system from ISO 26262 perspectives, Reliab Eng Syst Saf, vol. 96, no. 10. doi: 10.1016/j.ress.2011.03.013.

[8] Kilian P. et al. (2021). Principle Guidelines for Safe Power Supply Systems Development, IEEE Access, vol. 9. doi: 10.1109/ACCESS.2021.3100711.

[9] Pancik J., Drgona P., and Paskala M. (2020). Functional Safety for Developing of Mechatronic Systems - Electric Parking Brake Case Study, Communications - Scientific Letters of the University of Žilina, vol. 22, no. 4. doi: 10.26552/com.C.2020.4.134-143.

[10] Wang H. and Blaabjerg F. (2021). Power Electronics Reliability: State of the Art and Outlook, IEEE J Emerg Sel Top Power Electron, vol. 9, no. 6. doi: 10.1109/JESTPE.2020.3037161.

[11] Sandelic M., Peyghami S., Sangwongwanich A., and Blaabjerg F. (2022). Reliability aspects in microgrid design and planning: Status and power electronics-induced challenges, Renewable and Sustainable Energy Reviews, vol. 159. doi: 10.1016/j.rser.2022.112127.

DOI: 10.34186/klujes.1250928 *Geliş Tarihi:14.02.2023* *Kabul Tarihi:01.03.2023*

[12] Soury A., Genon-Catalot D., and Thiriet J. M. (2015). New lift safety architecture to meet PESSRAL requirements, 2nd World Symposium on Web Applications and Networking, WSWAN 2015. doi: 10.1109/WSWAN.2015.7210314.

[13] CENELEC/IEC (2020). EN 81-20-Safety rules for the construction and installation of lifts. Lifts for the transport of persons and goods Passenger and goods passenger lifts, 2020.

[14] IEC/ISO (2019). IEC 31010 - Risk management - Risk assessment techniques.

[15] CENELEC/IEC (2020). EN 81-50-Safety rules for the construction and installation of lifts. Examinations and tests Design rules, calculations, examinations and tests of lift components.

[16] Rausand M. (2014). Reliability of Safety-Critical Systems: Theory and Applications, vol. 9781118112724. doi: 10.1002/9781118776353.

[17] Pham H. (2009). Reliability and Risk Issues in Large Scale Safety-critical Digital Control Systems. doi: 10.1007/978-1-84800-384-2.

[18] Rausand M. and Haugen S. (2020). Risk assessment: Theory, methods, and applications. doi: 10.1002/9781119377351.

[19] Rausand M. (2014). Reliability of Safety-Critical Systems: Theory and Applications, vol. 978111811272. doi: 10.1002/9781118776353.

[20] CENELEC/ISO (2018). IEC 60812-Failure modes and effects analysis (FMEA and FMECA).

[21] CENELEC/IEC (2005). IEC 62380-Reliability data handbook Universal model for reliability prediction of electronics components, PCBs and equipment.