TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

AKTİF TIBBİ CİHAZLARDA FONKSİYONEL GÜVENLİK GEREKLİLİKLERİNİN İNCELENMESİ

YÜKSEK LİSANS TEZİ

Ümit SEVİM

Biyomedikal Mühendisliği Anabilim Dalı

Tez Danışmanı: Prof. Dr. Osman EROĞUL

ARALIK - 2019

Fen Bilimleri Enstitüsü Onayı

……..
Prof. Dr. Osman EROĞUL
Müdür

Bu tezin Yüksek Lisans derecesinin tüm gereksininlerini sağladığını onaylarım.

……
Prof. Dr. Osman EROĞUL
Anabilimdalı Başkanı

TOBB ETÜ, Fen Bilimleri Enstitüsü'nün 161711032 numaralı Yüksek Lisans Öğrencisi **Ümit SEVİM**'in ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı **"AKTİF TIBBİ CİHAZLARDA FONKSİYONEL GÜVENLİK GEREKLİLİKLERİNİN İNCELENMESİ"** başlıklı tezi **17/12/2019** tarihinde aşağıda imzaları olan jüri tarafından kabul edilmiştir.

Tez Danışmanı : **Prof. Dr. Osman EROĞUL** .....
TOBB Ekonomi ve Teknoloji Üniversitesi

Jüri Üyeleri : **Doc. Dr. Fatih BÜYÜKSERİN (Başkan)** ….....
TOBB Ekonomi ve Teknoloji Üniversitesi

Dr. Öğr. Üyesi Mehmet Feyzi AKŞAHİN.....
Başkent Üniversitesi

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, alıntı yapılan kaynaklara eksiksiz atıf yapıldığını, referansların tam olarak belirtildiğini ve ayrıca bu tezin TOBB ETÜ Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırlandığını bildiririm.

Ümit Sevim

ÖZET

Yüksek Lisans

AKTİF TIBBİ CİHAZLARDA FONKSİYONEL GÜVENLİK GEREKLİLİKLERİNİN İNCELENMESİ

Ümit Sevim

TOBB Ekonomi ve Teknoloji Üniversitesi
Fen Bilimleri Enstitüsü
Biyomedikal Mühendisliği Anabilim Dalı

Danışman: Prof. Dr. Osman Eroğul

Tarih: Aralık 2019

Aktif tıbbi cihazlarda tehlike riski taşıyan fonksiyonlar, programlanabilir elektrikli tıbbi sistemler kullanılarak önleniyor ise bu kontrol sistemlerinde oluşacak hataların kabul edilemez riske yol açmaması gerekmektedir. IEC 60601-1 ve özel cihaz standartları programlanabilir elektrikli tıbbi sistemlerinin(PEMS) geliştirilmesi ve hayata geçirilmesi için gereklilikleri tanımlamış, cihazın risk taşıyan fonksiyonlarının koruyucu sistemler tarafından otomatik olarak yerine getirilmesini talep etmektedir. Ayrıca, Tıbbi Cihaz Yönetmeliği de tıbbi cihazlardaki programlanabilen elektronik sistemlerin süreklilik, güvenilirlik ve performans şartları sağlanacak şekilde tasarlanmasını şart koşmaktadır. Öncelikle Tıbbi Cihaz Yönetmeliği ve standartlarında güvenilirlik şartlarının nasıl açıklandığı bu tez kapsamında incelenmiştir. Tıbbi cihaz standartlarında programlanabilir kontrol sistemleri için istenilen güvenilirlik sağlama kriterlerinin, fonksiyonel güvenlik standartları ile eşleştiği tespit edilmiştir. Ancak tıbbi cihaz standartlarında kontrol sisteminin güvenlik bütünlük seviyesinin (SIL) ne olması gerektiği ve tasarımında kullanılacak tekniklerin açıklamadığı tespit edilmiştir. Bu doğrultuda otomotiv sanayi, proses güvenliği ve nükleer enerji santralleri de dahil olmak üzere emniyet kritik uygulamaların tamamında kullanılan fonksiyonel güvenlik

standartlarının aktif tıbbi cihaz ürün geliştirme süreçlerinde de kullanılması ile tıbbi cihazların güvenilirliğinin sağlanacaktır. Kontrol sistemlerini oluşturan donanımların fonksiyonel güvenliği için sistematik hatalar ve rastgele donanım arızaları incelenerek, güvenilirlik hesaplamasının nasıl yapılacağı açıklanmıştır. 1oo1, 1oo2, 2oo2, 1oo2D ve 2oo3 mimari yapıları için IEC 61508 standardına göre güvenilirlik blok diyagramı metodu kullanılarak elde edildi. Daha sonra, rastgele donanım arızaları için bileşenlerin hata modları ve hata oranları kullanılarak SIL hesaplamasında kullanılacak hata oranlarının Hata Türü ve Etkileri Analizi (FMEA) ile nasıl elde edileceği açıklanmıştır. Donanım mimari yapıları için her bir alt sistemin hata olasılığının hesaplanması için MATLAB'da bir program geliştirilmiş ve örnek hata olasılıkları hesaplanmıştır. Daha sonra elde edilen değerler kullanılarak örnek bir kontrol sisteminin güvenilirlik seviyesinin nasıl artırılabileceği gösterilmiştir.

Anahtar Kelimeler: Fonksiyonel güvenlik, Aktif tıbbi cihaz, Programlanabilir elektrikli tıbbi sistem, Güvenlik bütünlük seviyesi, IEC 61508, IEC 60601.

ABSTRACT

Master of Science

INVESTIGATION OF FUNCTIONAL SAFETY REQUIREMENTS IN ACTIVE MEDICAL DEVICES

Ümit Sevim

TOBB University of Economics and Technology
Institute of Natural and Applied Sciences
Biomedical Engineering Science Programme

Supervisor: Prof. Dr. Osman Eroğul

Date: December 2019

If functions with risk of danger in active medical devices are prevented by using programmable electrical medical systems, faults in these control systems must not lead to an unacceptable risk. IEC 60601-1 and particular device standards define the requirements for the development and implementation of programmable electrical medical systems, requiring that the safety functions of the device shall be carried out automatically by the protective systems. In addition, 2017/745 numbered Medical Device Regulation requires that the programmable electronic systems in medical devices shall be designed to ensure continuity, reliability and performance. This thesis examines how the reliability requirements of Medical Device Regulations and standards are explained. It has been determined that the reliability criteria required for programmable control systems in medical device standards match the functional safety standards. However, it has been determined that the safety integrity level (SIL) of the control system and the techniques to be used in the design of the medical device standards do not explained. In this respect, the reliability of active medical devices will be ensured by using functional safety standards used in all safety critical applications

including automotive industry, process safety and nuclear power plants. For functional safety of the hardware, the systematic errors and random hardware failures are examined and the method of reliability calculation is explained. For the architectural structures 1oo1, 1oo2, 2oo2, 1oo2D and 2oo3, the failure probabilities obtained using the reliability block diagram method according to IEC 61508. Then, it is explained how to obtain the failure rates to be used in SIL calculation by using failure modes and failure rates of components for random hardware failures according to Failure Mode and Effects Analysis(FMEA). A program was developed in MATLAB to calculate the failure probability of each subsystem according to hardware architecture and failure probabilities was calculated. Then, using the calculated failure probabilities, it was shown how to increase the reliability level of a sample control system.

Keywords: Functional safety, Active medical device, Programmable electrical medical system, Safety integrity level, EN IEC 61508, EN IEC 60601.

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren danışman hocam Prof. Dr. Osman EROĞUL'a, kıymetli tecrübelerinden faydalandığım TOBB Ekonomi ve Teknoloji Üniversitesi Biyomedikal Mühendisliği Bölümü öğretim üyelerine ve destekleriyle her zaman yanımda olan aileme ve arkadaşlarıma çok teşekkür ederim. Ayrıca bana sağladığı burs ve destekler için TOBB Ekonomi ve Teknoloji Üniversitesi'ne şükranlarımı sunarım.

İÇİNDEKİLER

Sayfa

ŞEKİL LİSTESİ

Sayfa

ÇİZELGE LİSTESİ

Sayfa

KISALTMALAR

AB	:	Avrupa Birliği
ALARP		Makul Ölçüde Uygulanabildiği Kadar (As Low As Reasonably Practicable)
AFAP		Mümkün Olduğunca (As Far As Possible)
CCF		Ortak Nedenli Hatalar (Common Cause Failure)
CDF		Kümülatif Dağılım Fonksiyonu (Cumulative Distribution Function)
DC		Teşhis Kapsamı (Diagnostic Coverage)
E/E/PE	:	Elektrikli/Elektronik/Programlanabilir Elektronik (Electrical / Electronic / Programmable Electronic)
EN	:	Avrupa Standardı (European Norm)
EUC	:	Kontrol Altındaki Ekipman (Equipment Under Control)
FMEA		Hata Türü ve Etkileri Analizi (Failure Mode and Effect Analysis)
HFT		Donanım Hata Oranı (Hardware Fault Rate)
IEC	:	Uluslararası Elektroteknik Komisyonu (International Electrotechnical Commission)
ISO		Uluslararası Standardizasyon Teşkilatı (International Organization for Standardization)
iid	:	Türdeş ve Bağımsız Dağılımlı (Independent and Identically Distributed)
MD	:	2006/42/AT Makine Emniyeti Yönetmliği (2006/42/EC Machinery Directive)
MDD	:	93/42/AT Tıbbi Cihaz Yönetmeliği (93/42/EEC Medical Device Directive)
MDR	:	Tıbbi Cihaz Tüzüğü (2017/745 Medical Device Regulation)
MTTF		Ortalama Hataya Düşme Süresi (Mean Time to Failure)
MTTR		Ortalama Onarım Süresi (MEan Time to Repair)
PDF		Olasılık Yoğunluk Fonksiyonu (Probability Density Function)
PEMS		Programlanabilir Elektrikli Tıbbi Sistem (Programmable Electrical Medical System)
PFD_{avg}		Talep Anındaki Tehlikeli Hata Olasılığının Ortalama Değeri (The Average Probability of Dangerous Failure on Demand)
PFH		Saatte Hataya Düşme Olasılığı (The average frequency of a dangerous failure)
RBD		Güvenilirlik Blok Diyagramı (Reliablity Block Diagram)
SFF		Güvenli Hata Oranı (Safe Failure Fraction)
SIL	:	Güvenlik Bütünlük Seviyesi (Safety Integrity Level)
TSE	:	Türk Standardları Enstitüsü

SEMBOL LİSTESİ

Bu çalışmada kullanılmış olan simgeler açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	Açıklama
β	Ortak nedenli hatalardan kaynaklanan tespit edilemeyen hatalar oranı
β_D	Ortak nedenli hatalardan kaynaklanan tespit edilen hatalar oranı
$\lambda = \lambda_b$	Hata oranı
λ_D	Tehlikeli hata oranı
λ_{DD}	Tespit edilen tehlikeli hata oranı
λ_{DU}	Tespit edilemeyen tehlikeli hata oranı
λ_S	Güvenli hata oranı
λ_{SD}	Tespit edilen güvenli hata oranı
λ_{SU}	Tespit edilemeyen güvenli hata oranı
π_T	Sıcaklık faktörü
π_R	Güç oranı faktörü
π_S	Gerilim stres faktörü
π_Q	Kalite faktörü
π_E	Çevresel faktör
T_1	Doğrulama test aralığı
t_{CE}	Kanalın ortalama bozuk olma süresi
t_{CE}'	Kanalın ortalama bozuk olma süresi(1oo2D mimari için)

1. GİRİŞ

Tıbbi cihazlar, günümüz sağlık alanında hastalık tanı ve tedavi süreçlerinde hekimlerin en büyük yardımcıları olarak görev yapmaktadırlar. Bu doğrultuda, gelişen teknoloji cihaz tasarım ve üretim süreçlerine yansımakta ve insanlığın hizmetine sunulmaktadır. Elektrik, elektronik ve yazılım alanındaki teknolojiler de yaygın olarak tıp alanında kullanılmaktadır. Aktif tıbbi cihaz olarak adlandırılan bu cihazlar; yer çekiminin ya da insan vücudunun doğal olarak oluşturduğu enerji haricinde herhangi bir elektrik enerjisi veya güç kaynağıyla ve bu enerjinin dönüşümüyle çalışan cihazlar olarak tanımlanmaktadır [1].

Aktif tıbbi cihazlar tasarım ve üretim süreçlerinde risk yönetim süreçleri zorunlu olarak uygulanmakta ve tüm riskler ya ortan kaldırılarak ya da ekonomik çıkar gözetmeksizin olabildiğince azaltılmaktadır(AFAP). Tıbbi cihazların çoğunda meydana gelebilecek hatalar hayat kaybı veya ciddi yaralanma ile sonuçlanabileceği için bu sistemler *emniyet kritik*(safety-critical) sistem olarak değerlendirilmektedir. Emniyet kritik sistemler; meydana gelecek hataların hayat kaybına, ciddi maddi hasara veya çevre hasarına yol açabildiği sistemler olarak tanımlanmaktadır [2].

Günümüzde emniyet kritik (safety-critical) sistemlerde güvenlik fonksiyonlarını yerine getiren elektrikli ve/veya elektronik ve/veya programlanabilir elektronik kontrol sistemleri kullanılmakta ve bu sistemler *fonksiyonel güvenlik* gerekliliklerine göre tasarlanıp üretilmektedir. Aktif tıbbi cihazlar da gerekli performans ve temel güvenlik gereklerinin yerine getirilmesi için programlanabilir kontrol sistemlerinden yararlanmaktadır. Örnek bir programlanabilir kontrol sistemi Şekil 1.1'de verilmiştir.

Aktif tıbbi cihazlar için ilgili cihaz özelinde kabul edilemez riske yol açan tehlikeler eğer programlanabilir elektronik kontrol sistemi kullanılarak önleniyorsa veya kullanılan kontrol sisteminde olabilecek hatanın kabul edilemez risk oluşturduğu durumda, elektronik programlanabilir kontrol sisteminin sürekliliğini, güvenilirliğini ve performansını sağlayacak şekilde tasarlanması şartı bulunmaktadır [4].

Şekil 1.1: Örnek Programlanabilir Kontrol Sistemi yapısı [3].

Programlanabilir elektronik kontrol sistemlerinin sürekliliği, güvenilirliği ve performansı, günümüzde emniyet kritik sistemlerde fonksiyonel güvenlik metodolojisinin uygulanması ile yerine getirilmektedir. Bu doğrultuda fonksiyonel güvenlik uygulamaları için "EN IEC 61508 Güvenlikle ilgili elektrikli veya elektronik veya programlanabilir elektronik sistemlerde fonksiyonel güvenlik" standardı oluşturulmuştur. Bu standardın ilgili alanlarda uygulanmasına yönelik; proses güvenliği için IEC 61511, nükleer santraller ile ilgili IEC 61513, otomotiv ile ilgili ISO 26262, demiryollarıyla ilgili EN 50129 ve makinalarla ilgili IEC 62061 standartları yayınlanmış ve fonksiyonel güvenlik açısından uygulanmaktadır. Aktif tıbbi cihazlar ile ilgili özel bir fonksiyonel güvenlik standardı yayınlanmamış olup, bu kapsamdaki gerekliliklerin sağlanması için EN IEC 60601-1 standardının 14. Maddesinde ilgili şartlar yer almaktadır.

Fonksiyonel güvenlik standartları mimari yapının oluşturulması ve hayata geçirilmesi ile ilgili süreçleri tanımlamakta ve oluşturulan kontrol sisteminin güvenilirliğini gösteren *güvenlik bütünlük seviyesi (safety integrity level, SIL)* kavramını kullanmaktadır. Programlanabilir elektronik kontrol sitemleri ile ilgili tıbbi cihaz standartlarında ise fonksiyonel güvenlik standartlarındaki tasarım kriterlerinin uygulanmasına atıf yapılmakla birlikte sistemin güvenilirliğinin ne olması gerektiği ve nasıl hesaplanması gerektiği ile ilgili bilgi yer almamaktadır. Bu doğrultuda bu sistemlerin geliştirilmesinde fonksiyonel güvenlik standartlarının referans alınması fayda sağlayacaktır.

Aktif tıbbi cihazlardaki programlanabilir elektronik kontrol sistemlerinin sürekliliğini, güvenilirliğini ve performansının nasıl sağlanabileceğini incelemeden önce bu zorunlulukların yerine getirilmesinin yasal dayanağına bakmak faydalı olacaktır.

1.1. Tıbbi Cihazların Performans ve Temel Güvenliği ile İlgili Mevzuatlar

Tıbbi cihazlar, günümüz sağlık alanında hastalık tanı ve tedavi süreçlerinde hekimlerin en büyük yardımcılarıdır. Tıbbi cihazlar amaçlanan görevlerini yerine getirirken güvenlik ve performans şartlarını sahip olup sürdürmesi gerekmektedir. Bu doğrultuda, tıbbi cihazların tasarım ve geliştirme süreçlerinde temel güvenlik ve gerekli performans şartları dikkate alınarak güvenliğin sağlanması bir zorunluluktur. Bu kapsamda güvenli cihazların üretilmesi ve piyasaya sürülmesi ülkelerin yasal otoriteleri tarafından yasa ve yönetmeliklerle güvence altına alınmıştır [5].

Ülkemiz, AB Gümrük Birliğinin üyesi olduğu için tıbbi cihazlar ile ilgili mevzuatımız Avrupa Birliği mevzuatı ile aynıdır. Tıbbi cihazların tasarım, üretim, sınıflandırma, piyasaya arz ve denetlenmesi 93/42/AT sayılı Tıbbi Cihaz Yönetmeliği(MDD) ile düzenlenmektedir. Ayrıca bu yönetmelikte bir güncelleme olmuş ve 5 Mayıs 2017 tarihinde Avrupa Birliği Resmi Gazetesinde ilgili yönetmeliğin yerine geçecek 2017/745 sayılı Tıbbi Cihaz Tüzüğü(MDR) yayımlanmıştır. Yeni yayımlanan tüzüğe geçiş ile ilgili olarak 26 Mayıs 2020 tarihine kadar üç yıllık bir geçiş süresi bulunmaktadır [4].

Hem yönetmelik hem de yerine geçecek tüzüğün Ek1 bölümlerinde tıbbi cihazların sağlaması gereken gerekli performans ve temel güvenlik gereklilikleri yer almaktadır. MDR ile MDD Ek1 temel gereklerinin kapsam ve konuları birbirine paralel olarak yayımlanmıştır [6].

Ayrıca, MDD/MDR temel gerekleri ile birlikte, bir tıbbi cihazın 2006/42/AT Makine Emniyeti Yönetmeliği(MD) kapsamına da girmesi halinde bu yönetmeliğin MDD/MDR tarafından kapsanmayan temel gereklerine de uygun olarak tasarlanıp üretilmesi gerekmektedir [4]. Bu şartın ilgili cihaza uygulanması için cihazın Makine Emniyeti Yönetmeliğindeki *"makine; doğrudan insan veya hayvan gücü uygulaması dışındaki bir tahrik sistemi ile donatılmış veya donatılması amaçlanmış, ilişkili parçaları veya kısımlarının en az biri hareketli olan ve belli bir uygulama amacıyla bir araya getirilmiş olan parçalar topluluğu ile bunlardan; sadece kullanım sahasına veya bir enerji ve hareket kaynağına bağlantı için gerekli olan aksamları bulunmayan veya monte edilmeye hazır ve sadece bir ulaştırma vasıtasına monte edildiğinde veya*

bir bina ya da yapıya kurulduğunda çalışma yeteneğine sahip veya aynı sonucu elde etmek için bir bütün halinde çalışacak şekilde düzenlenen ve kumanda edilen veya yük kaldırma amaçlı ve güç kaynağı doğrudan uygulanan insan gücü olan birbiriyle bağlantılı en azından biri hareketli bağlantılı parçalar ve aksamdan oluşan parçalar topluluğudur. [7] *"* tanımına girmesi gerekir.

Aktif tıbbi cihazlarda yer alan programlanabilir elektronik kontrol sistemleri ile ilgili şartlar MDD Ek1 madde 12.1 ve MDR madde 17.1 bölümlerinde birbiriyle aynı olarak "*Programlanabilen elektronik sistemler içeren tıbbi cihazlar, öngörülen kullanıma uygun olarak bu sistemlerin sürekliliğini, güvenilirliğini ve performansını sağlayacak şekilde tasarlanmalıdır. Tıbbi cihaz, sistemde herhangi bir tek hata durumunda, muhtemel tehlikeleri asgariye indirecek veya ortadan kaldıracak uygun araçlarla donatılmalıdır* [1]." hükmü yer almaktadır.

Programlanabilir elektronik kontrol sistemlerinin öneminin vurgulayan bir diğer hususta yeni mevzuat metnine bu konuda yapılan eklemedir. MDR metnine, bu cihazların uygunluk değerlendirmesini gerçekleştirecek belgelendirme kuruluş personellerinin sahip olması gereken yetkinlik alanları arasına "fonksiyonel güvenlik" kavramı da eklenmiş bulunmaktadır [4].

Makine Emniyeti Yönetmeliğinde de kontrol sistemlerinin güvenliği ve güvenilirliği ile ilgili şartlar Ek1 madde 1.2.1 bölümünde açıklanmaktadır. Makine Emniyeti Yönetmeliği açısından ilgili temel güvenlik gereğin sağlanması için "IEC 62061 Makina güvenliği- Güvenliğe ilişkin elektrik, elektronik ve programlanabilir elektronik kontrol sistemlerinin fonksiyonel güvenliği" standardı uygulanmaktadır.

Programlanabilir kontrol sistemleri ile ilgili MDR madde 17 hükümleri, Makine Emniyeti Yönetmeliği madde 1.2.1 bölümündeki gereklilikleri kapsadığı için programlanabilir kontrol sistemleri için MDR madde 17'nin dikkate alınması mevzuat açısından yeterli olacaktır [8].

Aktif tıbbi cihazların MDR Ek1 genel sağlık ve performans gerekliliklerine uygunluğun varsayımı, ilgili mevzuat kapsamında yayımlanmış harmonize standartlara uygunluğun sağlanması ile yerine getirilebilmektedir. Aktif tıbbi

cihazların temel güvenlik ve gerekli performans şartları için IEC 60601 serisi ve IEC 80601 serisi standartlar yürürlüktedir.

Programlanabilir elektronik kontrol sistemleri ile ilgili olarak "IEC 60601-1 Elektrikli Tıbbi Donanım – Bölüm 1:Temel Güvenlik ve Gerekli Performans İçin Genel Kurallar" standardının 14. maddesinde *Programlanabilir Elektrikli Tıbbi Sistemler(PEMS)* ile ilgili şartlar tanımlanmaktadır.

1.2. Tıbbi Cihaz Standartları ve Programlanabilir Kontrol Sistemleri

Elektrikli tıbbi cihaz standartları, gerekli performans ve temel güvenliğin sağlanması için tüm cihazların risk yönetim süreçlerinden geçmesini şart koşmaktadır. Tüm tıbbi cihazların tasarım ve üretim aşamalarında risk yönetim sürecinin uygulanması hem ilgili mevzuatta hem de IEC 60601 serisi standartlarda zorunlu olarak istenmektedir. IEC 60601 standardı PEMS için uygulanacak risk yönetim sürecinde programlanabilir elektrikli kontrol sistemlerinin temel güvenlik ve gerekli performansın sağlamasında görev alması veya bu sistemde olabilecek hatanın kabul edilemez bir riske yol açması durumunda standardın madde 14 gerekliliklerinin uygulanmasını şart koşmaktadır [9].

IEC 60601 standardı PEMS'in geliştirilmesi ve hayata geçirilmesi sürecinin takip edilmesi ve bu sürecin bir kaydının oluşturulmasını istemektedir. Bu sürecin Risk Yönetim süreci ile birlikte yönetilmesi ve ISO 14971 standardında talep edilen Risk Yönetim Dosyasının bir bölümü olarak oluşturulması gerekmektedir.

Bu geliştirme ve hayata geçirme ile ilgili döngünün dokümante edilmesi talep edilmekte ve bu kapsamda geliştirme süreci için Şekil 1.2'de gösterilen V-model önerilmektedir.

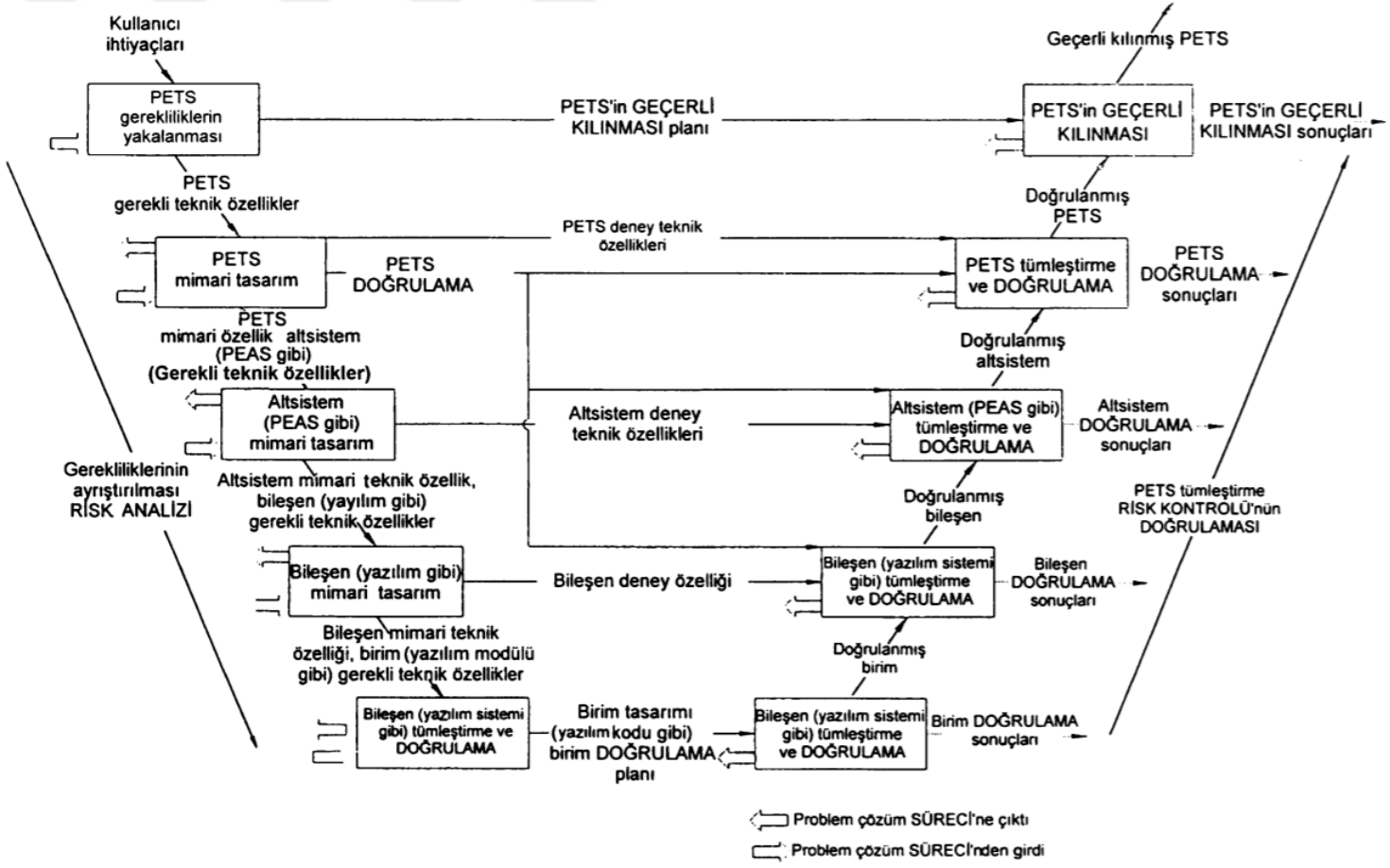
IEC 60601-1 standardına göre PEMS geliştirme sürecinde uygulanması gereken adımlar şunlardır.

1. Risk yönetim sürecinde bilinen ve öngörülebilir tehlikelerin belirlenmesi.
2. PEMS'in teknik özelliklerinin belirlenmesi.
3. Mimari yapının oluşturulması.
4. Tasarım ve geliştirmenin gerçekleştirilmesi.

5. PEMS'in doğrulanması.
6. PEMS'in geçerli kılınması.
7. PEMS modifikasyonlarının gerçekleştirilmesi.

PEMS'in hayata geçirilmesi için standartta öncelikle PEMS ile ilgili gerekliliklerinin risk değerlendirmede ele alınması ve gerekli teknik özelliklerin belirlenmesi istenmektedir. Daha sonra bu teknik özelliğe uygun olarak mimari yapının oluşturulması gerekmektedir. Mimari yapı oluşturulurken uygun olduğu yerde kullanılması istenen tasarım şartları aşağıda sıralanmıştır [9].

- Üstün özelliklere sahip bileşen kullanımı (Components With High-Integrity Characteristics).
- Hata emniyetli (fail-safe) fonksiyon.
- Yedekli sistem mimarisi.
- Farklı mimari yapı kullanımı.
- Mevcut çıkış gücünün sınırlandırılması veya hareket veren sistemlerin hareketini sınırlandırmak için araçların devreye sokulması sonucu oluşan muhtemel zararlı etkiler üzerindeki sınırlama gibi koruyucu tasarım öğeleri.
- İşlevselliğin bölünmesi (kritik ve kritik olmayan bölümlerin birbirinden ayrılması).
- Risk kontrol önlemlerinin alt sistemlere ve bileşenlere tahsis edilmesi.
- Bileşenlerin hata modları ve etkileri.
- Ortak nedenlere bağlı hatalar (common-cause failure).
- Sistematik hatalar.
- Doğrulama test aralığı ve hata teşhis kapsamı.
- Bakım kolaylığı.
- Makul öngörülebilir hatalı kullanımdan kaynaklanan koruma.
- Varsa ağ/veri kanallarının özelliği.



Şekil 1.2: V model [9].

Yazılım geliştirme süreci için ise “IEC 62304 - Tıbbi cihaz yazılımı - Yazılım yaşam çevrimi süreçleri” standardının şartlarının uygulanması istenmektedir. Tıbbi cihaz yazılımları geliştirilme süreçlerinde risk yönetimi ve yazılım risk seviyelerini içermektedir. Ancak, yazılım geliştirme teknikleri ve metodlarını içermemektedir ve bu konuda IEC 61508 fonksiyonel güvenlik standardının kullanılması önerilmektedir [10].

Donanım ve yazılım olarak PEMS’in tasarlanıp hayata geçirilmesine baktığımızda PEMS’in yerine getirdiği fonksiyonun kritikliğine göre hangi güvenilirlik seviyesinde olması gerektiği üreticinin risk değerlendirme sürecine bırakılmıştır. Ayrıca, IEC 60601-1 standardı, oluşturulan mimari yapının sağlayacağı güvenilirliğin nasıl değerlendirileceği ile ilgili şartları içermemektedir.

Programlanabilir elektronik kontrol sistemlerinin güvenilirlikleri ve performansları fonksiyonel güvenlik kavramı ile ele alınmaktadır. Bu doğrultuda oluşturulmuş fonksiyonel güvenlik standartları tasarım ve mimari yapının oluşturulması dahil kontrol sistemlerinin tüm yaşam döngüsünü kapsayacak şekilde oluşturulmuştur. Bu standartlardaki yaklaşımların aktif tıbbi cihazlara uygulanması programlanabilir elektronik kontrol sistemlerinin daha güvenilir bir şekilde tasarlanmasını ve mimari yapının oluşturulmasını sağlayacaktır.

IEC 60601’ standardının PEMS tasarımı için istediği yedekli sistem mimarisi, ortak nedenli hatalar, bileşenlerin hata modları ve hata oranları, sistematik hatalar , doğrulama testleri ve hata teşhis kapsamı gibi hususlar fonksiyonel güvenliğin temel unsurları olup, bu tez kapsamında incelenecektir.

1.3. Tıbbi Cihazlarda Yer Alan Güvenilirlik Şartları

Aktif tıbbi cihazlar geliştirilirken güvenlik ve temel performans ile ilgili yayımlanmış ilgili ürün standartlarının dikkate alınması ve bu standartlarda verilen gereklerin cihaz tasarımlarında yerine getirilmesi gerekmektedir. Bu doğrultuda aktif tıbbi cihazlar ile ilgili IEC 60601 ve ISO 80601serisi standartlar bulunmaktadır.

İlgili ürün standartları incelendiğinde cihazlarda ne gibi koruyucu sistemlerin bulunması gerektiği görülecektir. Örneğin; IEC 60601-2-16 hemodiyaliz cihaz

standardında Çizelge 1.1'de yer alan fonksiyonları yerine getiren ve bir alarm sistemini harekete geçiren otomatik koruyucu sistem kullanılması istenmektedir [11].

Çizelge 1.1: Hemodiyaliz cihazı standardında istenen koruyucu sistemler.

Koruyucu Sistem İstenen Fonksiyon	**IEC 60601-2-16 Madde Numarası** (Elektrikli tıbbî cihazlar - Bölüm 2-16: Hemodiyaliz, hemodiyafiltrasyon ve hemofiltrasyon cihazlarının temel güvenliği ve gerekli performansı için belirli özellikler)
Diyaliz sıvı bileşimi	201.12.4.4.101
Diyaliz sıvısı ve değişim sıcaklığı	201.12.4.4.102
Net sıvı çıkarımı	201.12.4.4.103
Çevreye ekstrakorporeal kan kaybı	201.12.4.4.104.1
Diyaliz sıvısına kan sızıntısı	201.12.4.4.104.2
Pıhtılaşmaya bağlı ekstrakorporeal kan kaybı	201.12.4.4.104.3
Hava infüzyon	201.12.4.4.105

Hemodiyaliz cihazı standardına istenen koruyucu sistemde oluşabilecek bir hatanın günde en az bir kez operatör tarafından kontrol edilmesi istenmektedir. Koruyucu sistemin kontrolü için aşağıda verilen metodlardan birisinin uygulanması gerekmektedir.

- Koruyucu sistemin, operatör tarafından başlatılan ve kontrol edilen periyodik fonksiyonel kontrolleri.
- Koruyucu sistemin, operatör tarafından başlatılan ve cihaz tarafından kontrol edilen periyodik fonksiyonel kontrolleri.
- Koruyucu sistemin yedekli mimarisi ve cihazın kendi kendini kontrol etmesi.
- Koruyucu sistemin kontrol işlevi, koruyucu sistem ile aynı anda başarısız olamayacak şekilde tasarlandı ise hemodiyaliz cihazı tarafından başlatılan ve hemodiyaliz cihazı tarafından kontrol edilen periyodik fonksiyonel kontrol.

Benzer şekilde diğer elektrikli tıbbi cihaz standartları da kritik parametrelerin kontrolü için kontrol sistemi kullanılmasını istemektedir. Örneğin; EN 60601-2-19 Elektrikli tıbbi donanım - Bölüm 2-19: Bebek kuvözlerinin temel güvenliği ve gerekli performansı için belirli özellikler standardı; aşırı sıcaklık, hava sirkülasyon hatası, termostat hatası, cilt sıcaklık sensörlerinin çıkması, fan dönme hatası, kuvözden hava çıkışının engellenmesi ve kuvöze hava girişinin engellenmesi durumlarını kontrol edecek koruyucu sistemler kullanılmasını şart koşmaktadır [12].

Yukarıda verilen örneklerde görüleceği gibi, standartlar hasta için tehlike olabilecek konuların kontrolü için kontrol sistemi kullanılmasını istemektedir. Bu kontrol sistemlerinde olabilecek bir arıza durumunda hastanın zarar görmemesi için kontrol sistemlerinin güvenilirliğinin tasarım aşamasında dikkate alınması elzemdir. İlgili kontrol sistemleri tasarlanırken, tasarlanan sitemin güvenilirliğinin objektif kriterlere göre değerlendirilmesi ve sistem güvenilirliğinin artırılması için fonksiyonel güvenlik standartlarının uygulanması cihaz güvenliğini artıracak ve dolayısıyla hasta ve operatör güvenliğini sağlayacaktır.

2. FONKSİYONEL GÜVENLİK

2.1. Fonksiyonel Güvenlik Nedir?

Fonksiyonel güvenlik, genel güvenliğin bir parçası olarak bir sistem veya donanımın girdilerine göre doğru olarak çalışmasını ifade etmektedir. Fonksiyonel güvenlik, tanımlanan tüm güvenlik fonksiyonlarının yürütülmesi ve bu fonksiyonlardan istenen performans seviyesinin karşılanması ile sağlanmaktadır [13].

Fonksiyonel güvenlik, güvenlikle ilişkili(safety-related) sistemlerdeki güvenliğin bir parçası olarak kullanılmaktadır. Emniyet kritik sistemler, bir veya daha fazla güvenlik fonksiyonunu yerine getirmek için donanım, yazılım ve insan faktörü dahil her şeyi kapsamaktadır. Bu güvenlik fonksiyonunda meydana gelecek hataların insan ve/veya çevre güvenliğine karşı ciddi bir risk artışına sebebiyet verdiği durumlar emniyet kritik sistemlerin kapsamında değerlendirilmektedir [Url-1].

Güvenlikle ilişkili sistem, belirli bir güvenlik işlevini (yangın algılama bastırma sistemi veya hemodiyaliz cihazının hava infüzyon algılama sistemi gibi) gerçekleştirmek için bağımsız donanım olabileceği gibi, başka tesislere veya ekipmanlara (bir makine takımındaki motor hızı kontrolü gibi) entegre edilebilir.

Fonksiyonel güvenlik aktif sistemler ile ilgili bir kavramdır. Örnek olarak, yanıcı bir sıvı içeren bir tanktaki sıvı seviyesinin tehlikeli bir noktaya ulaştığının seviye anahtarı ile tesit edilerek valfin kapanmasının sağlanması verilebilir. Bu sayede daha fazla sıvının içeri girmesini önlenerek tanktaki yanıcı sıvının dışarı taşması engellemiş olur [Url-1].

Pasif sistemler ile güvenliğin sağlanması fonksiyonel güvenlik değildir. Yangına dayanıklı bir kapının kullanılması pasif bir güvenlik sistemidir, ancak fonksiyonel güvenlik uygulaması değildir.

Fonksiyonel güvenlik ile ilgili ana standart IEC 61508 serisi standartlardır. Bu standardın çeşitli sektörlere uyarlanmış özel uygulama standartları da bulunmaktadır. Fonksiyonel güvenlik, havacılıktan makine güvenliğine ve nükleer santrallere kadar çeşitli sektörlerde aktif olarak kullanılmaktadır. Bu kapsamda sektör bazında uygulanan fonksiyonel güvenlik standartları Çizelge 2.1'de verilmiştir.

Çizelge 2.1: Fonksiyonel güvenlik standartları.

Elektrikli ve Elektronik Sistemler	IEC 61508
Otomotiv Endüstrisi	ISO 26262
Demir Yolu	IEC 62425, EN 62269
Proses (Petrol/Gaz)	IEC 61511
Nükleer Santraller	IEC 61513
Havacılık	DO 178B, DO 254
Makine	EN 62061, ISO 13849
Elektrikli Güç Cihazları	EN 61800-5-2

Fonksiyonel güvenlik değerlendirmesi, güvenlikle ilgili elektrikli, elektronik ve/veya programlanabilir elektronik(E/E/PE) sistemler ile yeterli fonksiyonel güvenliğin sağlanmasını sorgular. Fonksiyonel güvenlik değerlendirmesi; yetkin, bağımsız ve tarafsız uzmanlar tarafından, tüm yaşam döngüsü için yürütülen faaliyetlerin çıktıları dikkate alınarak fonksiyonel güvenlik standart şartlarına uygunluğun sağlandığının doğrulanmasıdır.

E/E/PE içeren güvenlikle ilgili sistemlerin güvenlik fonksiyonlarında meydana gelecek hatalardan kaynaklanacak tehlikeler fonksiyonel güvenlik kavramı kapsamındadır. Uygulama ve sektörden bağımsız olarak E/E/PE içeren güvenlikle ilgili sistemlerin tümüne uygulanabilmektedir.

Fonksiyonel güvenliğin uygulanacağı E/E/PE içeren güvenlikle ilgili sistemlere örnek olarak aşağıda hususlar verilebilir.

- Acil kapatma sistemleri.
- Yangın ve gaz sistemleri.
- Türbün kontrolleri.
- Makinalar için koruyucu kilitleme ve acil durdurma sistemleri.
- Tıbbi cihazlar.
- Dinamik konumlandırma sistemleri (bir limana yakın geminin hareketinin kontrolü).
- Tren yolu sinyalizasyon sistemleri.
- Hızı bir koruma aracı olarak sınırlamak için kullanılan değişken hızlı motor sürücüleri.
- Ağa bağlı bir proses tesisinin uzaktan izlenmesi, çalıştırılması veya programlanması.
- Hatalı sonuçların güvenliği etkilediği bilgi tabanlı bir karar destek sistemi.

Fonksiyonel güvenlik, kontrol sistemlerinin yerine getirdiği güvenlik fonksiyonları üstünden değerlendirilmektedir. Güvenlik fonksiyonlarının gerçekleştirilmesi için elektro-mekanik röleler (elektrikli), programlanamaz katıhal elektronik cihazlar(elektronik) ve programlanabilir elektronik cihazlar kullanılabilmektedir. Programlanabilir elektronik sistemler genellikle programlanabilir kontrolcüler, programlanabilir mantık kontrolcüleri (PLC), mikroişlemciler, uygulamaya özel entegre devre (ASIC) veya diğer benzeri programlanabilir cihazları kapsamaktadır.

Fonksiyonel güvenliğin temel standardı olan IEC 61508 bölüm 1,2,3 ve 4 IEC temel güvenlik yayını olarak belirlendiği için güvenlikle ilişkili E/E/PE içeren ürün ve sektörler için hazırlanacak tüm standartlarda IEC 61508'in referans alınması gerekmektedir. Ancak, IEC 60601-1 kapsamındaki standartlar için bu zorunluluk uygulanmamaktadır [Url-1]. Elektrikli tıbbi cihaz standartlarında PEMS sistemler için gereklilikler yer almaktadır. Ancak, güvenlikle ilişkili kullanılacak kontrol sistemlerinin hangi güvenlik seviyesinde olacağı ve nasıl tasarlanacağı ile ilgili şartlar IEC 60601-1 standardında üreticinin sorumluluğuna bırakılmıştır. Bu doğrultuda tıbbi cihaz standartlarının PEMS için istediği güvenilirliğin sağlanması için IEC 61508 ve

diğer uygulamaya yönelik sektör standartlarının tıbbi cihaz ürün geliştirme süreçlerinde referans alınmasının önünde de bir engel yoktur. Ayrıca, fonksiyonel güvenlik kavramının uygulanmasıyla aktif tıbbi cihazların gerekli performans ve temel güvenliğinin artırılmasına katkı sağlanacaktır.

Tıbbi cihazlar için E/E/PE sistemler PEMS olarak adlandırılmakta ve IEC 60601-1 standardı kapsamında ele alınmaktadır. Tıbbi cihazlar için fonksiyonel güvenliği ele alırken IEC 61508 serisi standartların uygulanması bu tez kapsamında incelenecektir.

2.2. IEC 61508 ve IEC 62061 fonksiyonel güvenlik standartları

Programlanabilir elektronik kontrol sistemlerinin fonksiyonel güvenliği, güvenlik fonksiyonlarının yerine getirilmesi üzerinden ele alınmaktadır. *Güvenlik fonksiyonu*; E/E/PE tarafından yerine getirilerek ekipman veya sistemin tehlikeli bir olay anında (örneğin gaz sızıntısı) güvenli durumda kalmasını veya güvenli duruma geçmesini sağlayan fonksiyon olarak tanımlanmaktadır [13].

Güvenlik fonksiyonunun tatmin edici olarak tanımlanmış tüm durumlar ve belirlenmiş zaman aralığında yerine getirme olasılığı ise *güvenlik bütünlüğü* olarak tanımlanmaktadır.

Fonksiyonel güvenlik, güvenlik fonksiyonlarının belirlenmesini iki aşamalı olarak ele almaktadır.

- Güvenlik fonksiyonu gerekliliği (fonksiyon ne yapacak) ve
- Güvenlik bütünlük seviyesi (*Safety Integrity Level - SIL*) (güvenlik fonksiyonunun tatmin edici şekilde yerine gelme olasılığının belirlenmesi).

Güvenlik bütünlük seviyesi; kontrol sistemlerinin hata ihtimalini ifade eden değer aralıklardır. SIL 1 en düşük güvenilirliği göstermekte yani en yüksek hata olasılığına sahip aralığı ifade etmektedir. SIL 4 seviyesi ise en yüksek güven aralığını yani en düşük hata olasılığa sahip seviyeyi temsil etmektedir. Güvenlik bütünlük seviyelerindeki güvenilirlik aralığı, kontrol sisteminin ilgili fonksiyonu yerine getirme sıklığına göre düşük ve yüksek/sürekli çalışma moduna göre farklılık göstermektedir.

Fonksiyonel güvenlik standartları, uygulamalara yönelik güvenlik fonksiyonunu gerekliliği ve güvenlik bütünlük gerekliliğinin ne olacağını koşul olarak belirtmemektedir. Ancak bazı ürün standartları oluşturulurken çeşitli güvenlik fonksiyonları için standart hazırlama teknik komiteleri tarafından risk değerlendirme gerçekleştirilerek SIL değerleri belirtilmektedir. Bu kapsamda, bazı özel makine (C tipi) standartlarında, o makineyle ilgili güvenlik fonksiyonlarının güvenlik bütünlük seviyesinin asgari değeri Çizelge 2.2'de gösterildiği şekilde standartlarda yer almaktadır.

Çizelge 2.2: EN 81-40 Eğimli Kaldırma Platformları için gerekli SIL değerleri.

Anahtar veya Güvenlik Devresi	**İlgili Maddeler**	**SIL**
Askı halatında veya zincirdeki gevşekliği tespit eden güvenlik cihazı	5.4.1.5	1
Taşıyıcı durdurma cihazı	5.5.14.1	1
Hassas kenarlar veya yüzeylerle çalışan cihazlar	5.6.2.4, 5.6.3.4, 5.6.4.7	1
Nihai sınırlama cihazı	5.5.15	1
Güvenlik dişlisi cihazı	5.3	1
Bariyer kolu konumlandırma cihazı	5.6.4.6	1
Civata/somun tahrik arıza cihazı	5.3.8	1
Rampa güvenlik cihazı	5.6.4.6.1	1
Koltuk dönmesi veya hareketi	5.6.2.3	1
Koltuk seviyeleme veya hareketi	5.6.2.6	2
Tahrik kontrolü	5.5.2, 5.5.3	1

2.3. Fonksiyonel Güvenlikte Çalışma Modları

IEC 61508 ve diğer fonksiyonel güvenlik standartları, güvenlik fonksiyonları için iki çalışma modu tanımlamaktadır. Çalışma modu; güvenlikle ilişkili sistemin çalışması için gelecek taleplerin frekansını ifade etmektedir. Bunlar, düşük talepli çalışma modu ve yüksek/sürekli talepli çalışma modu olarak ikiye ayrılmaktadır.

Bu iki modu anlamak için öncelikle talepli çalışma modu ile sürekli çalışma modunu anlamak gerekir.

Talepli modda çalışan bir güvenlik fonksiyonu, kontrol altındaki ekipmanı (EUC) tanımlanan duruma geçirmek için talep geldiği durumlarda çalışır. Güvenlik fonksiyonunu yerine getiren E/E/PE güvenlikle ilgili sistemin, güvenlik fonksiyonuna yönelik bir talep bulunana kadar EUC üzerinde hiçbir etkisi yoktur. Örnek olarak; kimyasal fabrikalardaki EUC'lerin hatalarını tespit eden koruma sistemleri ve araçlardaki ABS fren sistemi verilebilir.

Sürekli çalışma modunda çalışan güvenlik fonksiyonu, EUC'yi güvenli durumunda tutmak için sürekli görev yapmaktadır. Bu durumda E/E/PE güvenlikle ilgili sistem EUC'yi sürekli sürekli kontrol eder ve E/E/PE güvenlikle ilgili sistemde meydana gelecek tehlikeli bir hata olması durumunda eğer başka güvenlikle ilgili sistem veya risk azaltma önlemi müdahale etmezse tehlikeli bir olay meydana gelir. Örnek olarak bir makinadaki hız kontrolü ve manuel uçuş kumandalarını elektronik bir arayüz ile değiştiren gelişmiş uçuş kumanda sistemi verilebilir [Url-1].

Buna göre yüksek veya sürekli çalışma modunda güvenlik fonksiyonun fonksiyonel güvenliğin sürdürülmesi için sürekli etkin olmasını ifade etmektedir [13].

Düşük talepli mod, güvenlikle ilgili sistemdeki çalışma talebi yılda 1 kereden fazla olmadığı durumları kapsar. Yüksek veya sürekli talepli mod ise güvenlikle ilgili sistemdeki çalışma talebi yılda 1 kereden fazla olduğu durumları kapsar. Sürekli talepli mod, çok yüksek talepli mod olarak değerlendirilmektedir [13].

Düşük ve yüksek çalışma modları için güvenlik fonksiyonlarının güvenlik bütünlük seviyelerinin hata olasılıkları farklı olarak tanımlanmaktadır.

Düşük talepli çalışma modu, talep anındaki tehlikeli hata olasılığının ortalama değeri (PFDavg), yüksek talepli çalışma modu ise saatteki tehlikeli sonuçlanan arızaya geçme olasılığı (PFH) ile ifade edilmektedir ve Çizelge 2.3'de gösterilmiştir.

Çalışma modu, güvenlik bütünlük seviyesinin nasıl tespiet edileceğini belirlemektedir. Öncelikle tehlike oranı kavramı düşük talepli mod ve yüksek talepli mod arasındaki farkın anlaşılması için gereklidir. *Tehlike oranı*, diğer koruyucu önlemler olmadıkça, tehlikeli olayların gerçekleşme ihtimalidir. Temel amaç, güvenlikle ilgili bir sistemin

tasarlanmasıdır. Böylece ortaya çıkan tehlike oranı, o uygulama bağlamında tolere edilebilir riski karşılamak için yeterince düşük olmalıdır.

Çizelge 2.3: Güvenlik Bütünlük Seviyeleri (SIL).

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

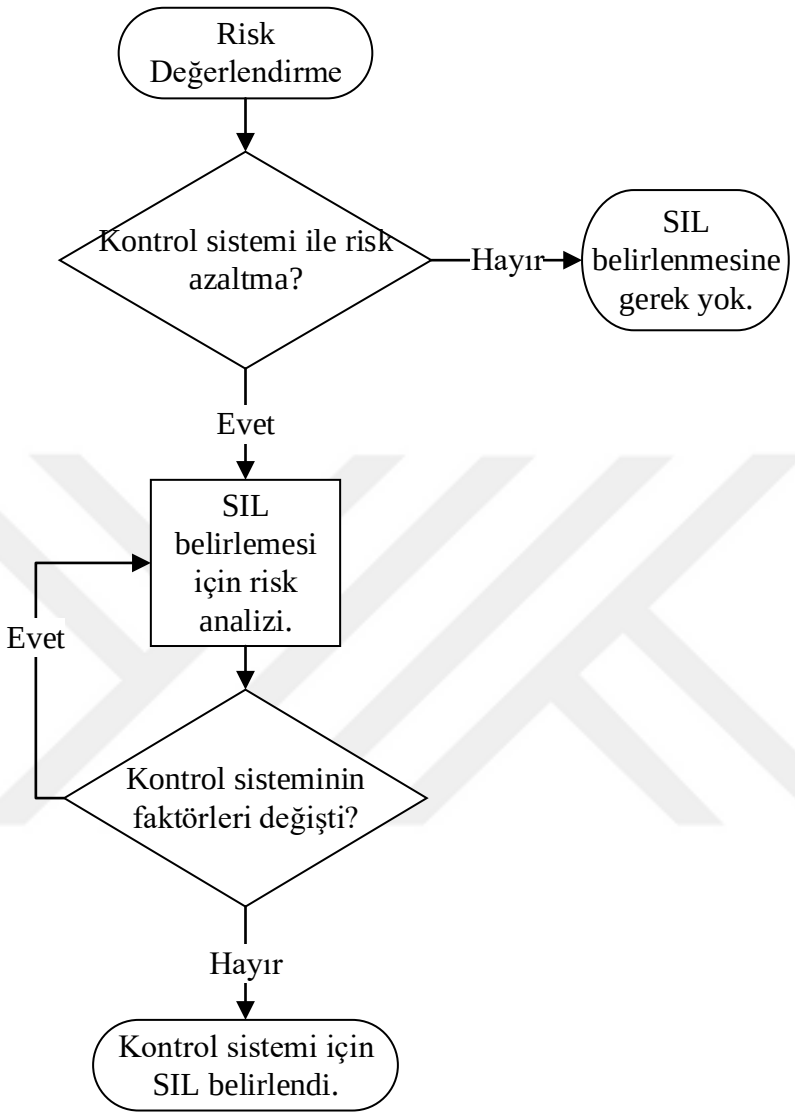
IEC 62061 standardı makinelerde yer alan güvenlikle ilişkili kontrol sistemleri için düşük talepli çalışma modunun uygun olmadığı için sadece yüksek talepli çalışma modu üzerinden kontrol sistemlerinin değerlendirmesini dikkate almıştır. Tıbbi cihazlar özelinde benzer bir yaklaşımın yapılması çoğu uygulama için uygun olacağından tez kapsamında yüksek talepli çalışma modu dikkate alınmıştır.

2.4. Fonksiyonel Güvenliğin Sağlanması için Risk Değerlendirme

Programlanabilir elektronik kontrol sistemlerinde fonksiyonel güvenliğin sağlanması için ürün tasarım ve geliştirme aşamasında yapılacak risk analizi ile programlanabilir elektronik kontrol sistemleri ile sağlanacak güvenlik fonksiyonlarının belirlenmesi gerekmektedir. Güvenlik fonksiyonunun belirlenmesi için uygulanacak risk değerlendirme akışı Şekil 2.1'de yer almaktadır.

Cihaz ile ilgili riskler bir programlanabilir kontrol sistemi kullanılarak gerçekleştirilmeyecek ise bir güvenlik bütünlük seviyesi değerlendirmesine gerek bulunmamaktadır. Eğer cihaz ile ilgili bir veya daha fazla riskin programlanabilir kontrol sistemi kullanılarak azaltılması söz konusu ise ilgili güvenlik fonksiyonu için SIL değerinin ne olması gerektiği risk analizi ile gerçekleştirilir.

SIL değeri belirlenirken kantitatif ve kalitatif risk değerlendirme metodolojileri, IEC 61508 ve diğer standartlar tarafından önerilmektedir.



Şekil 2.1: SIL belirleme süreci akış diyagramı.

Kantitatik ve kalitatif yöntemlerin kullanımı eldeki veriye, risk değerlendirmesini gerçekleştirecek olan kişilerin bilgi birikimine, konu hakkındaki deneyimine ve yöntemleri kullanma becerisine bağlıdır. Risklerin etkin bir şekilde yönetilebilmesi için kantitatif ve kalitatif yöntemlerin uygun bir şekilde harmanlanması gerekir.

Fonksiyonel güvenlik tehlike ve risk analizi sonucunda ortaya çıkacak güvenlik fonksiyonlarının belirlenmesi güvenlik için en önemli ve ilk adımdır. Güvenlik

fonksiyonlarının güvenlik bütünlükleri kadar bu fonksiyonların doğru ve etkili bir şekilde belirlenmesi de önem arz etmektedir.

EN 14971 Tıbbi cihazlar risk değerlendirme standardı da dahil olmak üzere tüm risk değerlendirme standartları öncelikle riski kaynağında yok etmeyi hedeflemektedir [3]. Riskin kaynağında yok edilmesi, doğal güvenlik ilkelerinin uygulanması veya iyi mühendislik uygulamaları ile olabilir.

Risk değerlendirmede kalitatif ve kantitatif metodlar uygulanmaktadır. Hem IEC 61508 standardı hem de EN 14971 her iki metodun risk değerlendirme aşamasında uygulanmasına izin vermektedir [14]. Risk analizi genellikle geniş bir uzmanlık alanı gerektirmektedir. Bir takım çalışması ile ortak bir sonuca ulaşılarak gerçekleştirilir.

Risk değerlendirme için farklı metodolojiler uygulanabileceği gibi IEC 61508-5 standardı bu kapsamda uygulanacak metotlar için kılavuzluk etmektedir.

Belirli bir tehlikeli olay için kabul edilebilecek riskin belirlenmesinin amacı, tehlikeli olayın frekansı (veya olasılığı) ve bunun özel sonuçları ışığında uygun önlemlerin belirlenmesidir. Güvenlikle ilgili sistemler, tehlikeli olayın sıklığını (veya olasılığını) ve / veya tehlikeli olayın sonuçlarını azaltmak için tasarlanmaktadır [14].

Kabul edilebilir risk birçok faktöre (örneğin, yaralanma şiddetine, tehlikeye maruz kalan kişi sayısına, kişi veya kişilerin maruz kaldığı sıklığa ve maruz kalma süresine) bağlı bir kavramdır. Belirli bir uygulama için kabul edilebilir bir risk belirlemede, birtakım girdiler dikkate alınır. Bunlar:

- İlgili güvenlik otoritelerinin kılavuzları;
- uygulamada yer alan farklı taraflarla yapılan görüşmeler ve uzlaşmalar;
- endüstri standartları ve yönergeleri;
- uluslararası görüş ve anlaşmalar; Ulusal ve uluslararası standartların rolü, belirli uygulamalar için kabul edilebilir risk kriterlerine ulaşmada giderek daha önemli hale gelmektedir;
- danışma organlarından en iyi bağımsız endüstriyel, uzman ve bilimsel tavsiyeler;

- yasal gereklilikler, hem genel hem de belirli uygulamalarla doğrudan ilgili olanlar.

Tıbbi cihazlarda risk yönetimi EN 14971 standardına göre gerçekleştirilmektedir. IEC 61508 fonksiyonel güvenlik standartları risk değerlendirmede "makul ölçüde uygulanabildiği kadar-ALARP" (*as low as reasonably practicable*) kavramı ile ekonomik değerlendirme unsurlarının da risk yönetimine katılmasını istemektedir. Ancak, Tıbbi Cihaz Yönetmeliğinin EK I temek gerekliliklerine ve EN 14971 standardına göre risk değerlendirmede "mümkün olduğunca -AFAP" (*as far as possible*) kavramı uygunlanması ve ekonomik unsurların dikkate alınmaması istenmektedir. Bu hükümden dolayı fonksiyonel güvenlik açısından gerçekleştirilecek risk değerlendirmede mümkün olan en iyi güvenlik bütünlük seviyesinin(SIL) ilgili cihaz tasarımında uygulanması MDR şartlarına uygunluk için gerekecektir.

Tıbbi cihaz yönetmeliğinin AFAP yaklaşımına göre, E/E/PE güvenlikle ilgili sistemlerin hata olasılığının en düşük olması için SIL 4 olarak dikkate alınması beklenir. Ancak, SIL 4 gereklerine erişmek için çok ciddi bir tasarım analizi ve eforu gerektirdiği için SIL 4 güvenlik fonksiyonlarından kaçınılması ve ek risk azaltma uygulanarak SIL hedeflerinin azaltılması gerektiği önerilmektedir [2]. SIL 4'ün uygulandığı senaryolar, yüksek olasılıklı bir riskin ölümcül bir sonuca tek bir seviye kontrol önlemi ile ulaşıldığını göstermektedir ki, bu tip senaryoların uygulamada kabul edilebilirliği çok düşüktür. Bir riski bertaraf etmek için birden fazla kontrol önleminin uygulanması önerilmekledir.

Bu doğrultuda uygulanabilirliği göz önüne alındığında, güvenlik fonksiyonlarının SIL 3 seviye olarak tasarlanması AFAP prensibinin sağlanması için uygun durmaktadır.

Ayrıca E/E/PE güvenlikle ilgili sistemler tasarlanırken risk analizi her aşamada gözden geçirilmeli ve tehlikeye yol açabilecek E/E/PE ile ilgili durumlar da dikkate alınmalıdır.

Kontrol sistemlerinin güvenilirliği için fonksiyonel güvenlik gereklerinin belirlenmesinden sonra güvenlik fonksiyonlarını yerine getirecek donanım ve yazılım mimarisinin gerekli SIL seviyesi uygun tasarlanması gerekmektedir. Kontrol

sistemlerinin güvenilirliği için öncelikle güvenilirlik teorisinin anlaşılması ve IEC 61508'e göre donanım mimarilerinin nasıl oluşturulması ve değerlendirilmesi bu tezin 3. ve 4. Bölümünde incelenmiştir.

2.5. Yazılımların Fonksiyonel Güvenliği

Donanım güvenilirlik mühendisliği, II. Dünya Savaşı sırasında balistik füzelerin başarı oranını değerlendirmek için ortaya çıkmıştır. 1950'lerde ise savunma ve havacılık alanlarında kullanılan mekanik, elektrikli ve elektronik bileşenlerin yaşam süresi hesaplamalarında gelişmiş metodlar uygulanmıştır. 1960'lı yıllara gelindiğinde, güvenilirlik mühendisliği kendisini askeri ürünlerde olduğu kadar ticari ürünlerde de son kullanıcı ürün geliştirmelerinin ayrılmaz bir parçası olarak ortaya koydu [15].

Yazılım güvenilirliği ise 1970'lerin ortasında yazılım geliştirme araçlarının stabil olması ile başlamıştır. Gündelik hayatın bir parçası olan sistemler yazılıma bağımlı hale geldikçe, yazılım güvenilirliği konusundaki algılar da değişti. Otomobil gibi araçların yazılımla kontrolünün arttırılması, bu araçlarla ilgili sorumluluk sorunlarının yanı sıra, "gizli" yazılım hatalarının azaltılmasının öneminin artmasına neden oldu [16].

Genel olarak, yazılımın güvenilirlik ölçüsü, verilen bir girdi için, belirli bir ortamda çalışan yazılımın, hatasız bir şekilde çalıştığını açıklamak için kullanılır. Bu nedenle; yazılımın güvenilirliği, yazılımın belirtilen koşullar altında belirli bir süre içinde sistem arızasına neden olmama olasılığı olarak tanımlanır [16].

Yazılım güvenilirliği her alanda olduğu gibi tıbbi cihazların güvenilirliğinde de vazgeçilmez bir yere sahiptir. Bu kapsamda tıbbi cihaz yazılım çevrim süreçleri için IEC 62304 standardı oluşturulmuş ve bu standart kapsamında cihazların kritikliğine göre yazılım geliştirme süreç gerekleri işletilmektedir.

IEC 62304 standardı yazılımın fonksiyonel güvenliği ile ilgili gerekleri doğrudan tanımlamamakla birlikte IEC 61508 fonksiyonel güvenlik standartlarının yazılım geliştirme süreçlerinde kullanılması ile ilgili yönlendirme yapmaktadır. IEC 62304 ile IEC 61508 standartlarının yazılım geliştirme süreçlerinde nasıl kullanılmaları gerektiği hususu üç başlık altında incelenebilir [10].

1- Risk yönetimi ve yaşam çevrimi süreçleri.
2- Güvenlik Bütünlük Seviyelerinin tanımlanması.
3- Yazılım geliştirme için tekniklerin, araçların ve yöntemlerin önerilmesi ve farklı görevlerin gerçekleştirilmesinden sorumlu personelin bağımsızlık düzeyleri.

Fonksiyonel güvenlik kapsamında yer alan bu üç hususun IEC 62304 ile ilişkisi incelendiğinde:

Konu 1'de yer alan risk yönetim süreçlerine uyum IEC 62304 tarafından "ISO 14971 Tıbbi cihazlara risk yönetiminin uygulanması" standardına referans verilerek sağlanmaktadır. Ancak ISO 14971 standardına göre yazılım ile ilgili riskler değerlendirilirken yazılım güvenilirliğinin değerlendirilmesi risk değerlendirmeyi yapacak takımın yetkinlik seviyesine bağlı olacaktır. Bu doğrultuda risk değerlendirme takımı oluşturulurken istenecek yetkinlik kriterlerinde bu hususlara dikkat edilmelidir [10].

Konu 2'de yer alan Güvenlik Bütünlük Seviyesi tanımlamaları için; IEC 62304 daha basit bir yaklaşım uygulamaktadır. IEC 61508 yazılımları güvenilirlik hedefine göre güvenilirliği 4 SIL seviyesine ayırırken, tehlikenin ciddiyeti ve olasılığını dikkate almaktadır [10].

IEC 62304 standardı yazılım hata ihtimalinde bağımsız, hatadan kaynaklanacak tehlikenin sonucuna göre yazılımları 3 kategoride değerlendirmektedir. Buna göre de farklı yazılım güvenilirlik sınıfına göre farklı süreçlerin işletilmesini talep etmektedir [10].

Konu 3'de yer alan yazılım geliştirme teknikleri, araçları ve yöntemleri IEC 62304 standardı tarafından kapsanmamaktadır. Bu doğrultuda IEC 62304 standardı, yazılım geliştiricilerin IEC 61508 fonksiyonel güvenlik standartlarını yazılım metodları, teknikleri ve araçları için kullanılmasını önermektedir. Yazılım geliştirme süreçlerindeki personelin bağımsızlığı ile ilgili olarak IEC 62304 standardı bir şart içermemekte, bu konu ISO 14971 kapsamında ele alınmaktadır [10].

Bu doğrultuda yazılım güvenilirliğini artırmak ve doğrulamak için tıbbi cihaz yazılım geliştiricileri IEC 62304 standardı yanında IEC 61508 fonksiyonel güvenlik standartlarından da yararlanmalıdır. Bu tez kapsamında yazılım güvenilirliği nasıl sağlanacağı incelenmemiş olup sadece donanım güvenilirliği incelenmiştir.

3. GÜVENİLİRLİK TEORİSİ

Fonksiyonel güvenlikte sistemin güvenilirliği belirlenirken sistemi oluşturan bileşenlerin sunabileceği güvenilirlik seviyesi de önem arz etmektedir. Fonksiyonel güvenlik hesaplamalarında bileşenlerin hata oranları ve sunabileceği güvenilirliğin irdelenmesi gerekmektedir.

Sistem güvenliğinin analizi için güvenirlik teorisi ve olasılık hesaplamaları çoğu risk değerlendirme yöntemi uygulamaları için büyük önem taşır.

Güvenirliğin genel tanımı, belirli bir zaman aralığında tanımlanmış durumlarda bir bileşenin istenen fonksiyonu yerine getirme ihtimalidir. Güvenilirlik analizi, basit anlamda bir sistemin parçalarının ve birimlerinin arıza oranlarının analizidir. Bu doğrultuda hata modellemelerinin incelenmesi gerekir.

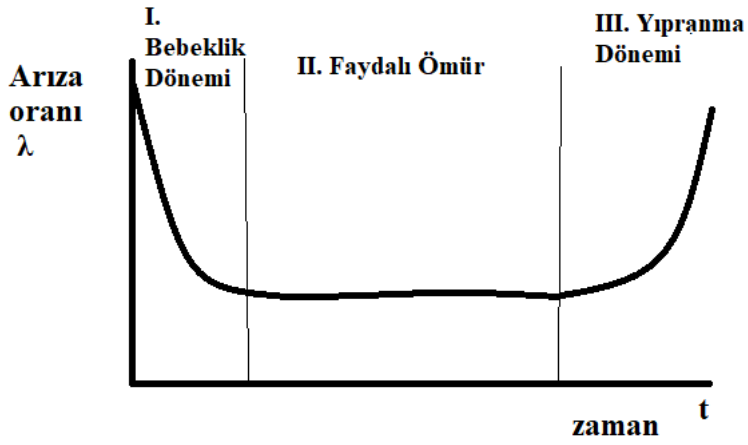
3.1. Hata Modelleme

Güvenilirlik analizinde elektronik bileşenlerin zamana bağlı hata oranı Şekil 3.1'de verildiği gibi küvet eğrisi le modellenmektedir [17].

Birinci dönem, bebeklik dönemi olarak ifade edilmektedir ve yüksek hata oranı göstermektedir. Zayıf tasarım, standart dışı bileşen kullanımı veya üretimde yetersiz kontrol araçlarının kullanılmamasından kaynaklanmaktadır. Bu hatalar kalite kontrol faaliyetleri ile tespit edilemez ise erken hataların ortaya çıkması muhtemeldir. Bu hatalar kullanıcı tarafından, bileşenin amaçlanan kullanım koşullarında test edilmesi ile ortaya çıkarılabilir.

İkinci bölge, yararlı kullanım dönemi olarak nitelendirilmekte ve bileşenler bu dönemde sabit bir hata oranına sahiptir. Bu dönemdeki hatalar rastgele donanım arızası olarak nitelendirilmektedir. Bu hatalar önleyici bakım veya kullanımdan önce yapılacak testler ile önlenememektedir. Ancak bu dönemde olacak hatalar, bileşen

veya ekipman tasarımının analiz edilmesi ile istatistiksel olarak hesaplanmaktadır. Hata oranının çok yüksek çıkması durumunda tasarım değişiklikleri ile bu oran düşürülebilir.



Şekil 3.1: Elektronik bileşenlerin hata eğrisini gösteren küvet eğrisi.

Sabit hata oranının görüldüğü dönem, güvenilirlik mühendisliği tasarım metotlarının temelini oluşturmaktadır. Hata oranının sabit olmasından dolayı; üstel dağılım, zamana göre hata oranının modellemesinde kullanılmaktadır [17].

Üstel dağılım yaklaşımının basitliği hata oranı hesaplamalarında tercih edilmesini sağlamıştır. Ayrıca, kompleks ekipman ve sistemlerin modellemesinde de uygulanabilmektedir [17].

Son dönem, yıpranma dönemi olarak değerlendirilmekte ve hata oranı yaşlanma ve yıpranmaya bağlı olarak zamanla artan davranış göstermektedir. Yıpranma dönemindeki hataları önlemenin çözümü, hata oluşmadan önce bileşeni değiştirme veya tamirdir.

Küvet eğrisinde yer alan üç dönemi modellemek için farklı istatistiki dağılımlar kullanılabilir. Örneğin, bebeklik dönemi gama veya Weibull dağılımları ile, faydalı ömür dönemi üstel dağılım ile ve yıpranma dönemi gama veya normal dağılım ile modellenebilir [17].

3.2. Güvenilirlik Teorisi ve Basit Yapıların Güvenilirlik Modelleri

Elektriksel bileşenlerin bozulma olasılıklarının üstel dağılım gösterdiği varsayılmıştır [17]. Buna göre bu bozulmayı modelleyen üstel dağılım fonksiyonu Eşitlik (3.1)'de verilmiştir. Üstel dağılımın kümülatif yoğunluk fonksiyonu (CDF) ise Eşitlik (3.2)'de verilmiştir.

$$f_X(t) = \lambda e^{-\lambda t} \quad t \geq 0, \lambda > 0 \tag{3.1}$$

$$F_X(t) = 1 - e^{-\lambda t} \tag{3.2}$$

Bir bileşenin bozulma olasılığını veren üstel dağılım olasılık yoğunluk fonksiyonunda yer alan λ arıza oranı (*failure rate*), t=0 anında faaliyete geçen bir sistemin [0,t] aralığında bozulmadan çalışma olasılığını ifade etmektedir.

Seri ve paralel olarak bağlanmış bileşenlerden oluşan bir sistemin ömrünü belirlerken sistemi oluşturan elemanların bozulma zamanları dikkate alınmaktadır. Bu tarz problemlerin çözümünde sıra istatistiği kullanılmaktadır.

$X_1, X_2, \ldots X_n$ bir popülasyondan seçilen olasılık dağılımları aynı ve birbirinden bağımsız (iid – türdeş ve bağımsız dağılımlı) rastgele örnekler için $Y_1 < Y_2 < \ldots < Y_n$ örneklerin sıra istatistiği olarak adlandırılmaktadır. Örneğin, birden fazla bileşenden oluşan bir sistemde her bir bileşenin bozulma süreleri 9,2,3,8,4,6 ise $Y_1=2$ olarak elde edilmektedir. En son bozulan bileşen için $Y_n=9$ olmaktadır. En büyük ve en küçük sıralı istatistik değerleri Eşitlik (3.3 – 3.4) ile gösterildiği şekildedir.

$$Y_1 = \min(X_1, X_2, \ldots, X_n) \tag{3.3}$$

$$Y_n = \max(X_1, X_2, \ldots, X_n) \tag{3.4}$$

$$Y_1 < Y_2 < \cdots < Y_n$$

Şekil 3.2: Seri bağlı sistem mimarisinin genel gösterimi.

Seri sistemlerde sistemin bozulması, sistemde bozulacak ilk eleman ile gerçekleşmektedir. Bu yüzden sistemin ömrünü sistemin en zayıf elemanı belirlemektedir.

Sistemin güvenilirliği, sistemin en zayıf halkasının ömrünün belirlenen süreden fazla olması ile hesaplanır. Bu durum matematiksel olarak Eşitlik (3.5) ile gösterilmektedir.

$$P(Y_1 > t) = P(Y_1 > t, Y_2 > t\ , \dots , Y_n > t) \tag{3.5}$$

Olasılık yoğunluk fonksiyonları iid olduğu için, sistemin güvenilirliğini gösteren R(t) değeri Eşitlik (3.9) ile gösterilmektedir.

$$P(X_1 > t, X_2 > t\ , \dots , X_n > t) = P(X_1 > t)P(X_2 > t) \dots P(X_n > t)$$

$$R_1(t) = P(X_1 > t) = 1 - F_{X_1}(t)$$

$$= 1 - (1 - e^{-\lambda_1 t})$$

$$R_1(t) = e^{-\lambda_1 t} \tag{3.6}$$

Burada R(t) güvenilirlik olarak adlandırılır ve bileşenin en az t süre güvenli çalışma ihtimalinin olasılığını göstermektedir. Eşitlik (3.7) de güvenilirlik fonksiyonu $t \geq 0$ için gösterilmiştir.

$$R(t) = P(X_1 > t) = 1 - F_{X_1}(t) \tag{3.7}$$

Sistemin toplamda en az t süre çalışma ihtimali Eşitlik (3.8)'in hesaplanması ile bulunur.

$$P(X_1 > t, X_2 > t\ , \dots , X_n > t) = R_1(t)\ R_2(t) \dots R_n(t) \tag{3.8}$$

$$= e^{-\lambda_1 t} e^{-\lambda_2 t} \dots e^{-\lambda_n t}$$

$$R(t) = e^{-(\lambda_1+\lambda_2+\cdots+\lambda_n)t}$$

$$\lambda = \lambda_1 + \lambda_2 + \cdots + \lambda_n$$

$$R(t) = e^{-\lambda t}$$

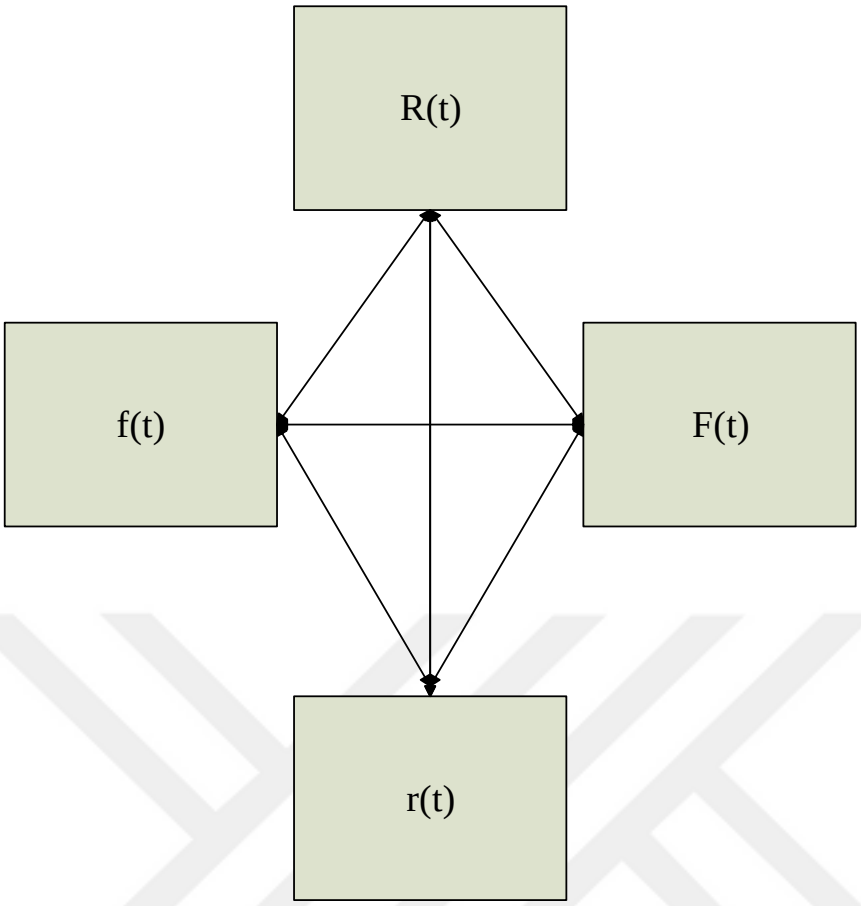
Güvenilirlik hesaplarındaki bir diğer önemli parametre de Ortalama Hataya Düşme Süresidir (Mean Time to Failure - MTTF) ve sistemin ortalama ömrünü ifade eder. MTTF, sistemin beklenen değeri ile hesaplanır. Beklenen değer iki farklı denklemle hesaplanmaktadır. Bu denklemlerinden birinde, sistemin beklenen değeri yani ortalama hayata düşme süresi sistemin güvenilirliği $R(t)$ kullanılarak hesaplanır. Bu durum Eşitlik (3.9)'da detaylandırılmıştır. Bununla birlikte bir sistemin olasılık yoğunluk fonksiyonu (f(t)-PDF) bilinirse bu sistemin kümülatif dağılım fonksiyonu (F(t)-CDF), güvenilirlik fonksiyonu (R(t)), ortalama hayata düşme süresi (MTTF), başarısızlık hızı (r(t)) hesaplanabilir. Bu durum Şekil 3.3'de gösterilmektedir. Beklenen değer X rastgele değişkeni için $x \geq 0$ için göre Eşitlik (3.9) ile verilmiştir.

$$E(X) = MTTF = \int_0^\infty x f(x) dx = \int_0^\infty \big(1 - F(x)\big) dx = \int_0^\infty R(x) dx \qquad (3.9)$$

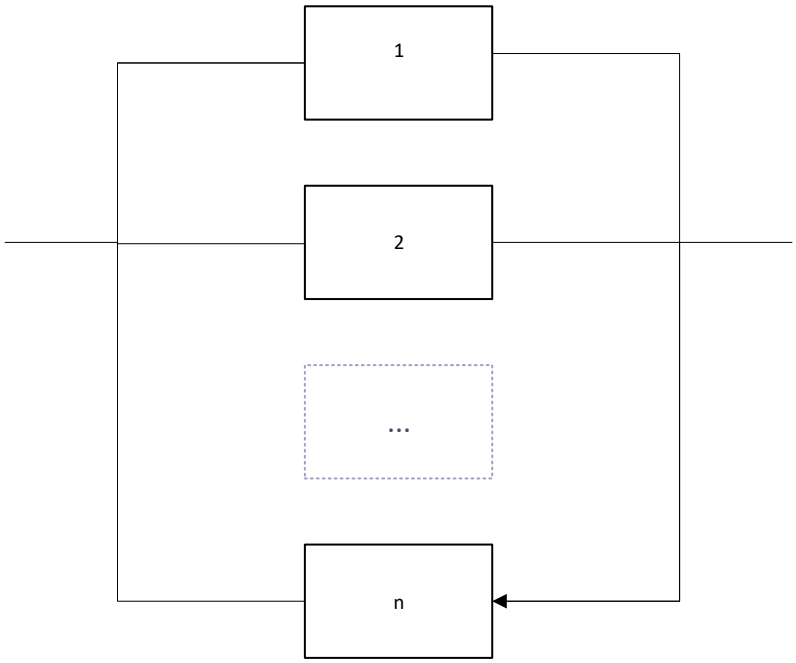
$$MTTF = \int_0^\infty e^{-\lambda x} dx$$

$$MTTF = \frac{1}{\lambda}$$

MTTF değeri seri sistemler için $\frac{1}{\lambda}$ olarak elde edilmektedir.



Şekil 3.3: Olasılık yoğunluk fonksiyonu ile CDF, R(t) ve r(t) ilişkisi.



Şekil 3.4: Paralel bağlı(yedekli) yedekli sistem genel mimarisi.

Sistem paralel olarak tasarlandığında yani yedekli olarak tasarlandığında sistemin bozulması için paralel kollardaki tüm bileşenlerin bozulması gerekmektedir. Paralel bağlı sistemlerde sistemin güvenilirliğini en geç hataya düşecek eleman belirlemektedir.

$$P(Y_n \leq t) = P(Y_1 \leq t, Y_2 \leq t\ , \dots , Y_n \leq t)$$

$$P(Y_n \leq t) = P(Y_1 \leq t)P(Y_2 \leq t) \dots P(Y_n \leq t)$$

Burada:

$$P(Y_i \leq t) + P(Y_i > t) = 1$$

$$P(Y_i \leq t) = 1 - P(Y_i > t)$$

$$P(Y_i \leq t) = F_{X_i}(t) = 1 - e^{-\lambda_i t}$$

Bu durumda paralel sistemin güvenilirliği Eşitlik (3.10) ile gösterilmektedir.

$$P(Y_n \leq t) = F_{X_1}(t)F_{X_2}(t) \dots F_{X_n}(t)$$

$$P(Y_n \leq t) = \left(1 - e^{-\lambda_1 t}\right)\left(1 - e^{-\lambda_2 t}\right) \dots (1 - e^{-\lambda_n t})$$

$$R(t) = \left(1 - e^{-\lambda_1 t}\right)\left(1 - e^{-\lambda_2 t}\right) \dots \left(1 - e^{-\lambda_n t}\right) \tag{3.10}$$

Sistemin MTTF değerini hesaplamak için örneğin ikili bir paralel sistemi değerlendirildiğinde, sonuç Eşitlik (3.11)'de gösterilmektedir.

$$MTTF = \int_0^\infty xf(x)dx$$

$$MTTF = \int_0^\infty \big(1 - F(x)\big)dx = \int_0^\infty (1 - \left(1 - e^{-\lambda_1 x}\right)\left(1 - e^{-\lambda_2 x}\right))dx$$

$$MTTF = \int_0^{\infty} e^{-\lambda_1 x} + e^{-\lambda_2 x} - e^{-(\lambda_1+\lambda_1)x} dx = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1 + \lambda_2} \quad (3.11)$$

Paralel mimari kullanmak veya yedekleme, yüksek sistem güvenilirliği sağlama yöntemlerinden birisidir ve bireysel bileşen güvenilirliğinden daha yüksek güvenilirlik sağlamaktadır. Ancak uygulamada, bu sistemler paralel ve seri tasarımların birlikte kullanılması ile sağlanmaktadır.

3.3. KooN Çok Kanallı Konfigürasyon

Paralel ve seri sistem mimarilerini yanında güvenilirlik tasarımlarında KooN çok kanallı mimari sıklıkla kullanılmaktadır. Bir sistemin başarılı bir şekilde çalışması için "N" adet bileşenden "K" tanesinin çalışmasının gerektiği tasarımlara KooN konfigürasyonu denilmektedir. Bu tip tasarımlar donanım mimari tasarımlarında güvenilirliği yükseltmek için kullanılmaktadır [17].

KooN mimarisini anlamak için tüm birimlerin birbiriyle eş, aynı anda çalıştığı ve hatalarının istatistiki olarak bağımsız olduğunu kabul edelim.

R: bir ünitenin belirli bir zaman için güvenilirliğidir.

Q: bir ünitenin belirli bir zaman için güvensizliğidir.

ve R+Q=1'dir.

n ünite için:

$(R + Q)^n = 1$

$$(R + Q)^n = R^n + nR^{n-1}Q + \frac{n(n-1)}{2!}R^{n-2}Q^2 + \cdots + Q^n = 1$$

Binom açılımı ile elde edilen bu değerleri 3 ünite için gerçekleştirirsek;

$$(R + Q)^3 = R^3 + 3R^2Q + 3RQ^2 + Q^3$$

R^3: üç ü$nitenin\ de\ çalışma\ g$ü$venilirliği$

$3R^2Q$: iki ü$nitenin\ çalışma\ g$ü$venilirliği$

$3RQ^2$: bir ü$nitenin\ çalışma\ g$ü$venilirliği$

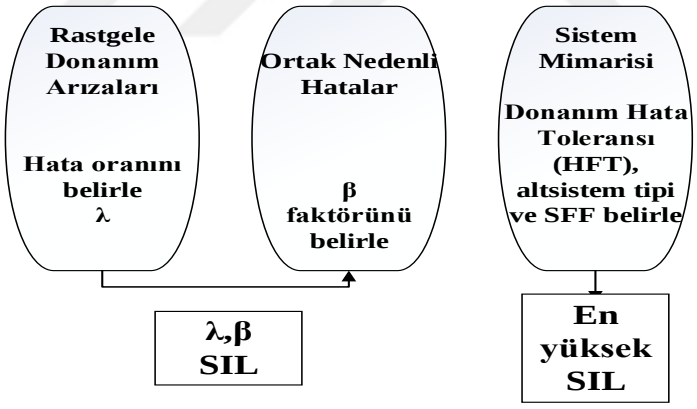
Q^3: $hepsinin\ çalışmama\ g$ü$vensizliği$

en az k ünitenin çalışma güvenilirliği Eşitlik (3.12) ile gösterilmiştir.

$$R(k) = \sum_{i=k}^{n} \binom{n}{j} R^i Q^{n-k} \tag{3.12}$$

4. DONANIMLARIN FONKSİYONEL GÜVENLİĞİNİN SAĞLANMASI

IEC 61508 standardı güvenlikle ilişkili kontrol sistemlerinin güvenilirliği için tüm yaşam döngüsü boyunca yürütülmesi gereken faaliyetleri açıklamaktadır. Bu standart elektrikli, elektronik ve programlanabilir elektronik için güvenlik fonksiyonlarını ve sistemin güvenilirlik seviyesini gösteren SIL gereklerini içermektedir. Dört SIL seviyesi, sistem ile ilişkili risklere göre tanımlanmaktadır ve SIL 4 en yüksek güvenilirlik seviyesini ifade etmektedir. Donanım mimarisinde gerekli SIL seviyesinin elde edilebilmesi için gerekli işlemler Şekil 4.1'de verilmiştir. Gerekli fonksiyonel güvenliği sağlamak için IEC 61508'e göre izlenecek yollar alt başlıklar halinde verilecektir.



Şekil 4.1: SIL seviyesinin hesaplanmasında kullanılan faktörler.

Kontrol sistemlerinin fonksiyonel güvenliği için sistemde oluşabilecek hatalar; sistematik hatalar ve rastgele donanım arızaları olmak üzere iki gruba ayrılmaktadır.

4.1. Sistematik Hatalar

Fonksiyonel güvenlik sağlanırken Sadece bir tasarımın ya da üretim sürecinin değişikliği, çalışma prosedürleri, dokümantasyon veya diğer ilgili faktörler ile ortadan kaldırılabilen belli bir neden için rastgele olmayan hatalara sistematik hata denilmektedir [18]. Sistematik hatalar sistemi hata durumuna geçirir ve değişiklik gerektiren düzeltici bakım ile hata nedeni ortadan kaldırılabilir.

Bu hatalar tasarım ve üretim sürecinde tespit edilerek ortadan kaldırılmalıdır. Sistematik hataların önlenmesi için uygulanabilecek yöntemler aşağıda sıralanmıştır [19].

- Proje Yönetimi.
- Dokümantasyon tutulması.
- Güvenlikle ilişkili sistemler ile diğer sistemlerin birbirinden ayrılması.
- Donanım çeşitliliği.
- Güvenlik gerekliliklerinin belirlenmesi sürecinde kontrol listeleri kullanımı.
- Tasarım ve geliştirme için kılavuz ve standartlardan yararlanma.
- Denenmiş bileşen seçimi.
- Modüler tasarım.
- Bilgisayar destekli tasarım araçları kullanımı ve simülasyon yapma.
- Tasarım gözden geçirmeleri.
- İşletme ve bakım prosedürleri geliştirme.
- Kullanıcı dostu tasarım ilkeleri.
- Doğrulama ve geçerli kılma süreçlerini işletme.
- Hata modları ve etkileri analizi (FMEA) veya hata ağacı analizi gibi teknikleri kullanma.
- Fonksiyonel testler.

4.2. Ortak Nedenli Hatalar

Donanım hataları; rastgele donanım arızaları ve sistematik hatalardan kaynaklanmaktadır. Sistem mimarisi oluşturulurken sistematik hatalardan kaynaklanan hata olasılığı da etkili olmaktadır. Çok kanallı sistemler için sistematik hatalardan birisi de ortak nedenli hatalar olarak ortaya çıkmaktadır. Ortak nedenli hatalar tek kanallı mimaride bulunmamaktadır.

Ortak nedenli hataların etkisinin güvenilirlik hesaplamalarında nasıl dikkate alınacağı ile ilgili IEC 61508-6 standardı bir metodoloji tanımlamakta ve hata oranı β faktörünün hesaplanması ile elde edilmektedir [20].

Ortak nedenli hatalar, belirli sebeplerden dolayı ortaya çıkabilmekte ve paralel kanalları etkilemektedir. Bu hatalar, tasarım veya spesifikayon hatası gibi sistematik bir hata olacağı gibi, örneğin aşırı sıcaklığın soğutma fan ömrünü kısaltması gibi dış bir etkinin rastgele donanım arızasını erken ortaya çıkarması da olabilir. Ortak nedenli hatalar, çok kanallı mimaride birden fazla kanalı etkilemeye yatkındır ve toplam hata oranı hesaplamalarında baskın faktör olarak yer almaktadır.

Ortak nedenli hatalar; tek bir nedenden kaynaklanmasına rağmen, etkisini tüm kanallarda hemen gösteremeyebilir. Örneğin, çok kanallı sistemde bir soğutma fan arızasında tüm kanallar bozularak ortak nedenli hataya sebep olabilir. Yine de tüm kanallar birbirinden farklı ısınma oranlarına sahiptir ve bu yüzden hatalar farklı kanallarda farklı zamanlarda meydana gelir.

Ortak nedenli hata oranını azaltmak için dikkate alınacak üç yol vardır.

1- Sistemin toplan rastgele donanım ve sistematik arızalarını azaltmak. Şekil 4.2'deki dairelerin alanlarının küçülmesine sebep olur.
2- Paralel kanalların bağımsızlığını artırmak. Bu Şekil 4.2'deki kesişim kümesini azaltacaktır.
3- Eş zamanlı ortaya çıkmayan ortak nedenli hataları, tanı testleri kullanarak önceden tespit et.

Şekil 4.2: Ortak nedenli hataların bireysel kanalların hataları ile ilişkisi.

Ortak nedenli hata oranı β faktörünün hesaplanması ile bulunmaktadır. Bu değerin hesaplanmasında kullanılacak metodoloji sadece donanım mimarileri ile sınırlıdır. Yazılımdan kaynaklanan ortak nedenli hataların azaltılması için IEC 61508-3 standardında metodlar uygulanmalıdır.

Sensör, mantık sistemi ve final elemanları; farklı çevresel koşullarda ve farklı kabiliyette tanı testlerine sahip olduğundan her bir alt sistemin ayrı ayrı ortak nedenli hataları analiz edilmelidir. IEC 61508-6 standardında verilen metodoloji bir mühendislik değerlendirmesini içermektedir ve yapılan değerlendirme sonucunda β değeri hesaplanmaktadır.

IEC 61508-6 standardında yer alan kontrol listesinde ortak nedenli hataların azaltılması için 8 kontrol metodu yer almakta ve metodlar için 37 önlem geliştirilmiştir. Kontrol listesinin tamamı IEC 61508-6'da görülebilir. Standartta yer alan kontrol metodları aşağıda verilmiştir.

- Ayırma/ayrışma
- Çeşitlilik/ yedeklilik
- Karmaşıklık/tasarım/uygulama/olgunluk/tecrübe
- Değerlendirme/ veri analizi ve geri beslemesi
- Prosedürler ve kullanıcı arayüzü
- Yetkinlik/eğitim/güvenlik kültürü
- Çevresel kontrol
- Çevresel test

Standartta yer alan bu kontrol listesine göre 37 sorunun mühendislik değerlendirmesine göre ele alınması gerekmektedir.

Ortak nedenli hata değerini veren β değerinin hesaplanmasında X ve Y parametreleri kullanılmaktadır. X, tanı testinin β faktörün etkinliğini artırması anlamına gelmekteyken, Y tanı testinin hiçbir etkisi olmaması durumunu ifade etmektedir. Kontrol listesinde yer alan her bir soru için cevap evet ise X ve Y değeri için ilgili değerler elde edilmektedir. LS; mantık alt sistemini, SF ise sensör / final eleman alt sistemini ifade etmektedir. Ayırma/ayrışma ile ilgili sorular Çizelge 4.1'de verilmiştir.

Çizelge 4.1: CCF için Ayırma/Ayrışma soruları.

Soru	**Mantık Alt sistemi**		**Sensör ve Final Eleman Alt Sistemi**	
	X_{LS}	**Y_{LS}**	**X_{SF}**	**Y_{SF}**
Ayırma/ayrışma				
Kanalların tüm sinyal kabloları her konumda ayrı ayrı yönlendiriliyor mu?	1,5	1,5	1,0	2,0
Mantık alt sistemi kanalları ayrı baskı devre kartlarında mı?	3,0	1,0		
Mantık alt sistemi kanalları ayrı dolaplarda mı?	2,5	0,5		
Sensörler / final elemanlar özel kontrol elektroniğine sahipse, her bir kanalın elektroniği ayrı baskılı devre kartlarında mı?	-	-	2,5	1,5
Sensörler / final elemanlar özel kontrol elektroniğine sahipse, her kanalın elektroniği iç mekanlarda ve ayrı dolaplarda mı?	-	-	2,5	0,5

Tüm sorular cevaplanarak X_{LS}, Y_{LS}, X_{SF}, Y_{LS} değerleri sırasıyla belirlenerek bu değerlerden toplam skor Eşitlik (4.1- 4.2) ile hesaplanır. Eşitlik (4.2)'nin

hesaplanmasında kullanılan Z değeri sırasıyla mantık alt sistemi ve sensör/final eleman alt sistemi için Çizelge 4.2 ve Çizelge 4.3'den elde edilir. Z faktörü, teşhis test kapsamı ve teşhis test aralığı ile tespit edilen teşhis test anlamına gelir.

$$S = \sum X_i + \sum Y_i \tag{4.1}$$

Skor "S" değeri ile β değeri elde edilir ve teşhis testin dikkate alındığı CCF değeri β_D değerini bulmak için de S_D değeri hesaplanır.

$$S_D = \sum X_i(Z+1) + \sum Y_i \tag{4.2}$$

Çizelge 4.2: Programlanabilir elektronikler için Z değeri [20].

Teşhiş Kapsamı(DC)	**Teşhis test aralığı**		
	<1 dakika	1 dakika ile 5 dakika arası	>5 dakika
≥ %99	2,0	1,0	0
≥ %90	1,5	0,5	0
≥ %60	1	0	0

Çizelge 4.3: Sensörler ve final elemanlar için Z'nin değeri [20].

Teşhis Kapsamı(DC)	**Teşhis test aralığı**			
	<2 saat	2 saat 2 gün arası	2 gün 1 hafta arası	>1 hafta
≥ %99	2,0	1,5	1	0
≥ %90	1,5	1,0	0,5	0
≥ %60	1	0,5	0	0

S ve S_D değerlerine göre elde edilecek β ve β_D değerleri 1oo2 mimari için Çizelge 4.4 kullanılarak elde edilir.

Çizelge 4.4: β ve βD 'in hesaplanması [20].

Skor (S veya S_D)	**β ve β_D değerleri**	
	Mantık Alt Sistemi	**Sensör veya Final Eleman**
120 ve üstü	%0,5	%1
70-120	%1	%2
45-70	%2	%5
45 altı	%5	%10

Farklı sayıda yedekli yapıya sahip mimariler için β farklı değerlere sahiptir. Yedekli mimarideki mimariler için değereler Çizelge 4.5 kullanılarak elde edilebilir.

Çizelge 4.5: 1oo2'den büyük yedeklilik seviyesine sahip sistemler için β 'nın hesaplanması [20].

KooN		**N**			
		2	**3**	**4**	**5**
K	1	β	0,5 β	0,3 β	0,2 β
	2	-	1,5 β	0,6 β	0,4 β
	3	-	-	1,75 β	0,8 β
	4	-	-	-	2 β

4.3. Rastgele Donanım Arızaları

Rastgele donanım arızaları, donanımdaki bir veya birden fazla bozulma mekanizması sonucu rastgele meydana gelmektedir. Belirlenemeyen bir zamanda oluşmasına rağmen, tahmin edilebilir oranlara sahiptir. Rastgele arızalar, cihazın hata bulma özelliği ile veya harici hata tespit araçları veya doğrulama testleri ile tespit edilebilmektedir. Bu arızalardan kaçınmak için genellikle yedekli, hata toleranslı alt sistemler kullanılmaktadır.

Hata oranlarının belirlenmesinde güvenilirlik blok diyagramları(RBD), Markov modelleri, FMEA ve hata ağacı analizi gibi teknikler kullanılmaktadır. Bunlardan RBD ve Markov modelleri en çok tercih edilen yöntemlerdir [19].

IEC 61508 standardı örnek mimariler için güvenilirlik blok diyagramı hesaplamalarını içermektedir. Bu tez kapsamında da güvenilirlik blok diyagramı tekniği dikkate alınmıştır.

4.4. Mimari Kısıtlar ve Fonksiyonel Güvenlik Değişkenleri

Bir güvenlik fonksiyonunu yerine getiren sistemin sahip olabileceği en yüksek SIL seviyesi donanım mimarisi ile kısıtlıdır. IEC 61508 standardının 2. bölümü donanım mimarileri için bir alt sistemin elde edebileceği SIL seviyelerini tanımlamıştır. Mimari kısıtlar Çizelge 4.6 ve Çizelge 4.7'de gösterilmiştir.

Çizelge 4.6: Donanım güvenlik bütünlüğü: Tip A alt sistemler için mimari kısıtlar [21].

Güvenli Hata Oranı (SFF)	**Donanım Hata Toleransı**		
	0	**1**	**2**
<%60	SIL 1	SIL 2	SIL 3
%60-<%90	SIL 2	SIL 3	SIL 4
%90-<%99	SIL 3	SIL 4	SIL 4
≥%99	SIL3	SIL 4	SIL 4

Çizelge 4.7: Donanım güvenlik bütünlüğü: Tip B alt sistemler için mimari kısıtlar [21].

Güvenli Hata Oranı (SFF)	**Donanım Hata Toleransı**		
	0	**1**	**2**
<%60	İzin verilmez.	SIL 1	SIL 2
%60-<%90	SIL 1	SIL 2	SIL 3
%90-<%99	SIL 2	SIL 3	SIL 4
≥%99	SIL 3	SIL 4	SIL 4

Alt sistemler Tip A ve Tip B olarak iki farklı kategoride değerlendirilmekte ve karmaşıklığına ve hata modlarının belirlenebilmesine göre sınıflandırılmaktadır.

Tip A alt sistem; bu alt sistemi oluşturan tüm bileşenlerin hata modlarının tanımlanabildiği, hata modlarında alt sistem davranışının tam olarak belirlenebildiği ve geçmiş kullanımlarına göre davranışlarını doğrulayacak güvenilir hata verilerine sahip olan sistemler olarak tanımlanmaktadır.

Tip B alt sistem; kendisini oluşturan bileşenlerden en az birinin hata modu tam olarak tanımlanamıyorsa, hata modalarında alt sistem davranışları tam olarak belirlenemiyor veya geçmiş kullanımlarına göre güvenilir hata verilerine sahip olunamayan sistemleri kapsamaktadır.

4.4.1. Donanım hata toleransı (HFT)

Donanım hata toleransı, bir sistemin gerekli güvenlik fonksiyonunu yerine getirmesi için donanımdaki bir veya birden fazla hatanın tolere edilebilirliğinin bir ölçütüdür. Donanım hata toleransının N olduğu bir sistem, N+1 hatanın sistemi güvenlik fonksiyonunu yerine getirmeyeceğini ifade etmektedir. Eğer sistem KooN konfigürasyonuna sahip ise, HFT basit olarak N-K değeri ile hesaplanabilmektedir. HFT değeri 0 olan bir alt sistem oluşabilecek ilk hatada güvenlik fonksiyonunu yerine getiremeyecek duruma gelecek demektedir.

4.4.2. Güvenli hata oranı (SFF)

Güvenli Hata Oranı(SFF), dahili hata tanıma özelliklerinin etkinliğini gösteren bir ifadedir. SFF, Teşhis Kapsamı (DC) ile benzerdir ancak, sistemin güvenli hataya düşme yatkınlığını da dikkate almaktadır. SFF yüzdesel olarak ifade edilmekte ve aşağıdaki Eşitlik (4.3) ile hesaplanmaktadır.

$$SFF = \frac{\sum \lambda_{SD} + \sum \lambda_{SU} + \sum \lambda_{DD}}{\sum \lambda_{SD} + \sum \lambda_{SU} + \sum \lambda_{DD} + \sum \lambda_{DU}} = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_D} = 1 - \frac{\sum \lambda_{DU}}{\sum \lambda} \qquad (4.3\ [3])$$

λ_D: $Tehlikeli\ hata\ oranı$

λ_{DD}: $Tespit\ edilen\ tehlikeli\ hata\ oranı$

λ_{DU}: $Tespit\ edileeyen\ tehlikeli\ hata\ oranı$

λ_S: $Güvenli\ hata\ oranı$

λ_{SD}: $Tespit\ edilen\ güvenli\ hata\ oranı$

λ_{SU}: $Tespit\ edilemeyen\ güvenli\ hata\ oran$

SFF; tespit edilen veya edilemeyen güvenli hatalar ile tespit edilen tehlikeli hataların tüm hatalara oranını ifade etmektedir.

4.4.3. Teşhis kapsamı (DC)

Teşhis kapsamı; tüm tehlikeli hatalardan yüzde kaçının teşhis edilebildiğini gösteren bir ifadedir. Eşitlik (4.4)'de verilen DC değeri yüzdesel olarak değer almaktadır ve her bir bileşen için ayrı ayrı değerlendirilmektedir.

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_D} = \frac{\sum \lambda_{DD}}{\sum \lambda_{DD} + \sum \lambda_{DU}} \qquad (4.4\ [3])$$

DC değeri IEC 61508 standardına Çizelge 4.8'de gösterildiği gibi göre dört kategori ile sınıflandırılmıştır.

Çizelge 4.8: Teşhis değeri kategorileri [20].

DC	**İsimlendirme**
<%60	Yok
%60- <%90	Düşük
%90-<%99	Orta
>%99	Yüksek

DC ve SFF değerinin hesaplanması için alt sistemi oluşturan her bir bileşenin hata modları dikkate alınarak Hata Türü ve Etkileri Analizi (FMEA) yapılması ile tespit edilmektedir. Detaylı hesaplama yöntemi tezin ilerleyen bölümlerinde açıklanmaktadır.

4.4.4. Doğrulama testi

Güvenlikle ilişkili sistemin istenilen güvenlik fonksiyonu yerine getirip getirmediğini doğrulamak için belirli periyotlar ile yapılan testtir. Bu test, tanı sistemi ile tespit edilemeyen tehlikeli hataların tespitini sağlamaktadır. Eğer gerekli olursa tamir süreci işletilerek sistem tekrar yeni pozisyona getirilmektedir.

4.5. Donanım Mimari Yapıları

Fonksiyonel güvenlik kapsamında oluşturulan mimari yapıların hata oranları güvenilirlik blok diyagramları, markov metodu ve hata ağacı analizi gibi güvenilirlik belirleme metodları kullanılarak analiz edilmektedir. IEC 61508 standardı bu tekniklerden güvenilirlik blok diyagramı tekniğini ele alarak tasarımlarda en çok kullanılan 1oo1, 1oo2, 2oo2, 1oo2D ve 2oo3 mimari yapıları için saatte hataya düşme olasılığı (PFH) değerlerini hesaplayarak ortaya koymuştur.

Güvenilirlik blok diyagram metodu uygulanırken sistemi alt sistemlere bölerek her bir sistemin güvenilirlik seviyesinin hesaplanması gerekmektedir. Alt sistemlerden oluşan örnek sistem mimarisi Şekil 4.3'de verilmiştir.

Şekil 4.3: Kontrol sistemi oluşturan alt sistemler.

Sistemin toplam hatası PFH_{sys} ile ifade edilmektedir ve Eşitlik (4.5) ile hesaplanmaktadır.

$$PFH_{SYS} = PFH_S + PFH_L + PFH_{FE} \qquad (4.5\ [20])$$

burada;

$PFH_{SYS}: Sistemin\ saatteki\ ortalama\ hatası$

$PFH_S: Sensör\ alt\ sisteminin\ saatteki\ ortalama\ hatası$

$PFH_L: Mantık\ alt\ sisteminin\ saatteki\ ortalama\ hatası$

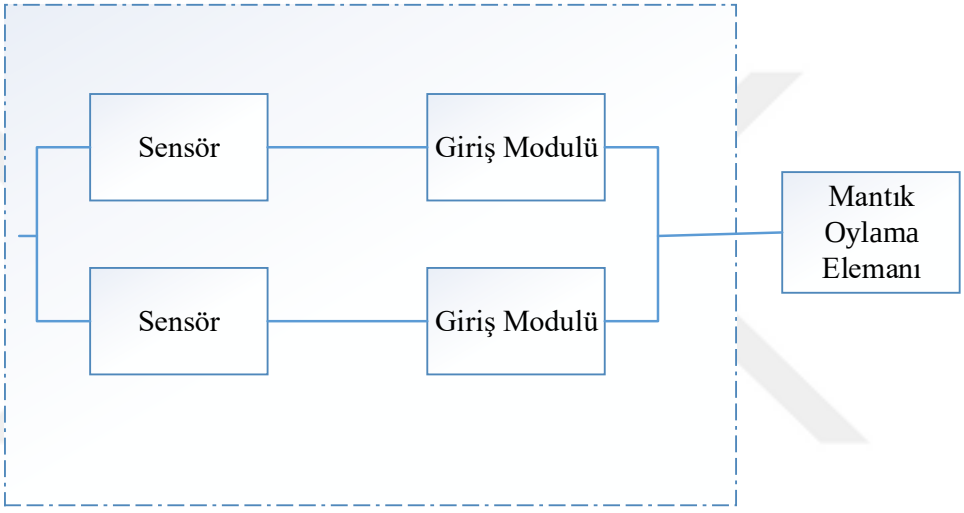
$PFH_S: Son\ Eleman\ alt\ sisteminin\ saatteki\ ortalama\ hatası$

IEC 61508 standardında RBD metoduna göre ilerleyen bölümde verilecek örnek mimari yapılar için yapılan hesaplamalar aşağıda yer alan varsayımlara göre gerçekleştirilmiştir.

- Sonuçta ortaya çıkan saatteki ortalama hata değeri 10^{-5}'den azdır.
- Bileşen hata ve tamir oranları bileşen ömrü boyunca sabittir.
- Hesaplamalarda kullanılan donanım hata oranları tek bir kanal içindir.
- Oylamalı grupta (KooN mimari) yer alan paralel kollar aynı hata ve DC değerine sahiptir.
- Alt sistemdeki bir kanalın toplam hata oranı o kanaldaki hata oranlarının toplamıdır ve bu oranların birbirine eşit olduğu varsayılmıştır.
- Her bir güvenlik fonksiyonu için mükemmel doğrulama testi ve onarımı olduğu varsayılmıştır. Tespit edilemeyen hataların tümü doğrulama testinde bulunmaktadır.

- Doğrulama test periyodu, tanı test aralığından en az on kat büyüktür.
- Her bir alt sistemin tek bir doğrulama test aralığı ve MTTR değeri vardır.
- Çoklu tamir ekipleri bilinen tüm hata tiplerinde çalışmak için hazırdır.
- Talep oranı, tanı test aralığından en az on kat büyüktür.
- Güç kaynağı arızaları, sistemin kapanıp güvenli moda geçeceği varsayımı ile hariç tutulmuştur.

Oylamalı bir mimaride, mantık oylama devresi mantık alt sisteminde olacak şekilde değerlendirilmektedir ve sensör alt sistemi için örnek gösterim Şekil 4.4'de verilmiştir.



Şekil 4.4: Sensör alt sistemi ve mantık oylama elemanı gösterimi.

Mimari yapılar IEC 61508 kapsamında 1oo1, 1oo2, 2oo2, 1oo2D ve 2oo3 konfigürasyonları için oluşturulmuş ve bu yapıların güvenilirlik blok diyagram gösterimleri ile PFH değeri verilmiştir. Hata oranları hesaplanırken kullanılan terimler Çizelge 4.9'da açıklanmaktadır.

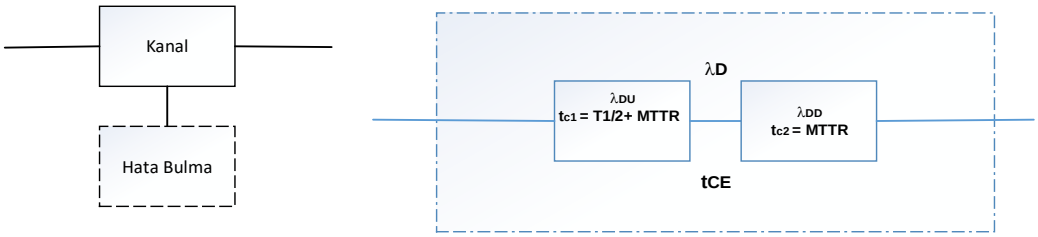
Çizelge 4.9: Örnek mimari yapıların PFH değerlerinin hesaplanmasında kullanılan terimler ve değerleri.

Kısaltma	**Terim (Birim)**	**Parametre aralığı**
T_1	Doğrulama test aralığı (h)	Bir ay(730 h) Üç ay(2190 h) 6 Ay(4380 h) Bir yıl(8760 h)
MTTR	Ortalama tamir süresi (h)	8 h
DC	Teşhis kapsamı(%)	%0 %60 %90 %99
β	Tespit edilmeyen ortak nedenli hata oranı (%)	%2 %10 %20
β_D	Tespit edilen ortak nedenli hata oranı (%)	%1 %5 %10

4.5.1.1oo1 mimari

Bu mimari tek kanallı bir yapıdan oluşmaktadır ve oluşabilecek herhangi bir tehlikeli hata güvenlik fonksiyonun hataya düşmesine sebep vermektedir. Tek kanallı bu

mimari yapının blok diyagramı ve güvenilirlik blok diyagramı Şekil 4.5'de verilmiştir. 1oo1 mimarinin PFH değeri Eşitlik (4.6)'de gösterilmektedir.



Şekil 4.5: (a)1oo1 fiziksel blok diyagramı (b) 1oo1 güvenilirlik blok diyagramı [20].

$$\lambda_D = \lambda_{DU} + \lambda_{DD} = \frac{\lambda}{2}$$

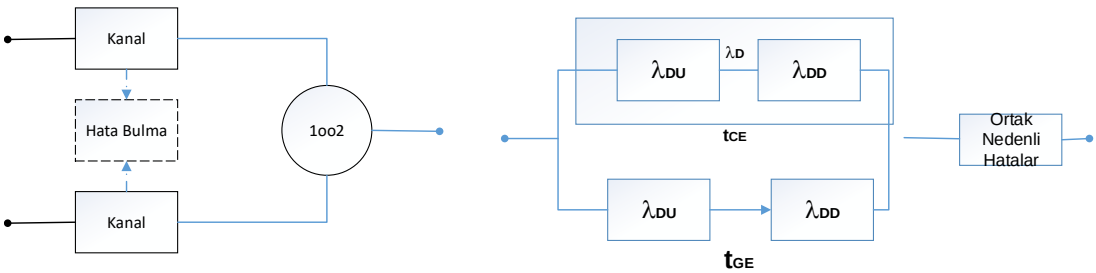
$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$\lambda_{DU} = \frac{\lambda}{2}(1 - DC); \lambda_{DD} = \frac{\lambda}{2} DC$$

$$PFH_G = \lambda_{DU} \quad (4.6\ [20])$$

4.5.2. 1oo2 mimari

Bu mimari birbirine paralel olarak bağlanmış iki kanaldan oluşmaktadır ve bu iki kanalda tek başına güvenlik fonksiyonunu yerine getirmektedir. Bu yüzden bir talep anında güvenlik fonksiyonunun başarısız olması için her iki kanalda da tehlikeli hatanın oluşması gerekmektedir. Hata bulma testinin sadece bulunan hataları bildirme fonksiyonu olduğu ve çıkış durumlarını veya oylamayı etkilemediği varsayılmaktadır.



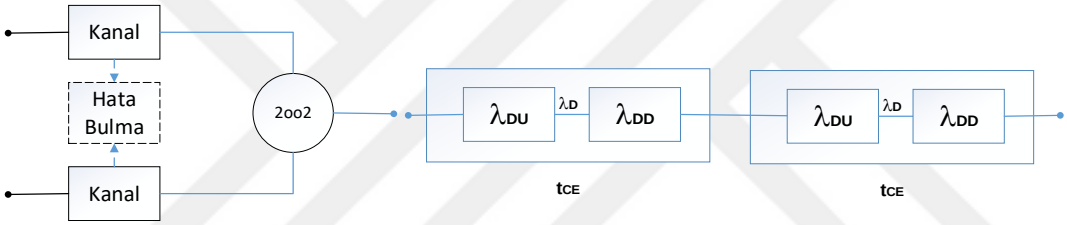
Şekil 4.6: (a) 1oo2 fiziksel blok diyagramı. (b) 1oo2 güvenilirlik blok diyagramı [20].

1oo2 mimarinin blok diyagramları Şekil 4.6'de gösterilmektedir. "tce" değeri bu mimari için de 1oo1 mimari ile aynıdır. Saatteki ortalama hata oranı Eşitlik (4.7) ile elde edilmektedir.

$$PFH_G = 2[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]^2 t_{CE} + \beta_D\lambda_{DD} + \beta\lambda_{DU} \qquad (4.7\ [20])$$

4.5.3. 2oo2 mimari

Bu mimari birbirine paralel olarak bağlanmış iki kanallı bir yapıdır ve her iki kanalında güvenlik fonksiyonunu yerine getirmesi gerekmektedir. Hata bulma testinin sadece bulunan hataları bildirme fonksiyonu olduğu ve çıkış durumlarını veya oylamayı etkilemediği varsayılmaktadır. 2oo2 mimarisinin blok diyagram gösterimleri Şekil 4.7'da verilmiştir.



Şekil 4.7: (a) 2oo2 fiziksel blok diyagramı.(b) 2oo2 güvenilirlik blok diyagramı [20].

Tespit edilen her hata için her iki kanalında güvenli duruma geçtiği varsayılırsa 2oo2 mimarinin saatteki ortalama hata değeri Eşitlik (4.8) ile elde edilir.

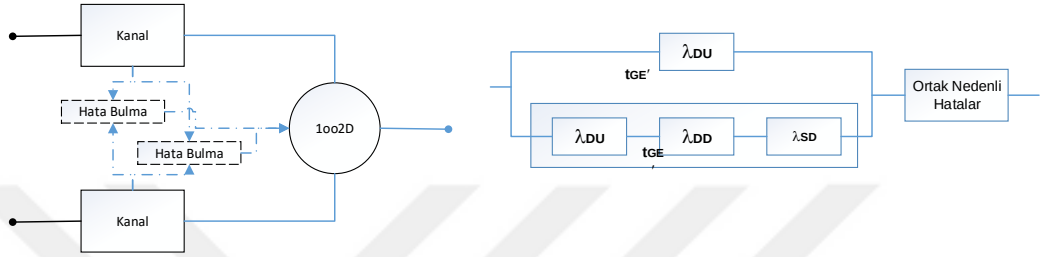
$$PFH_G = 2\lambda_{DU} \qquad (4.8\ [20])$$

4.5.4. 1oo2D mimari

Bu kanal birbirine paralel olarak bağlanmış iki kanaldan oluşmaktadır. Normal çalışma sırasında her iki kanal da güvenlik fonksiyonunu yerine getirmektedir. Ek olarak, eğer her iki kanalda bulunan hata bulma fonksiyonu bir hata tespit ederse, çıkış oylaması genel çıkış durumunun diğer kanal tarafından verilen durumu takip etmesi için

uyarlanır. Hata bulma her iki kanalda da arıza bulursa veya herhangi bir kanala atanamayan bir tutarsızlık varsa, o zaman çıkış güvenli duruma geçirilir. Kanallar arasındaki bir uyuşmazlığı tespit etmek için, her iki kanal da diğer kanaldan bağımsız bir yolla diğer kanalın durumunu belirleyebilir. 1oo2D mimarisinin blok diyagram gösterimleri

Şekil 4.8'de verilmiştir.



Şekil 4.8: (a)1oo2D fiziksel blok diyagramı. (b) 1oo2D güvenilirlik blok diyagramı [20].

1oo2D mimari yapının saatteki ortalama hata oranı Eşitlik (4.9) ile gösterilmiştir.

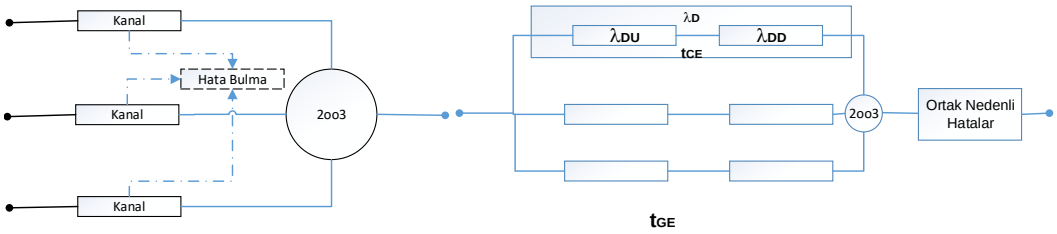
$$\lambda_{SD} = \frac{\lambda}{2} DC$$

$$t_{CE'} = \frac{\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) + (\lambda_{DD} + \lambda_{SD})MTTR}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}}$$

$$PFH_G = 2(1-\beta)\lambda_{DU}[(1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} + \lambda_{SD}]t_{CE'} + \beta_D\lambda_{DD} + \beta\lambda_{DU} \quad (4.9\ [20])$$

4.5.5. 2oo3 mimari

Bu mimari birbirine paralel üç kanal ve çıkış sinyali için çoğunluk oylama sisteminden oluşmaktadır. Eğer bir kanal diğer iki kanaldan farklı bir sonuç veriyorsa, çıkış durumu bu mimari yapıda etkilenmemektedir. Hata bulma testinin sadece bulunan hataları bildirme fonksiyonu olduğu ve çıkış durumlarını veya oylamayı etkilemediği varsayılmaktadır.



Şekil 4.9: (a) 2oo3 fiziksel blok diyagramı.(b) 2oo3 güvenilirlik blok diyagramı [20].

2oo3 mimari yapısında tce değeri 1oo1 mimari ile aynıdır. Saatteki ortalama hata durumu Eşitlik (4.10) ile elde edilmektedir.

$$PFH_G = 6[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]^2 t_{CE} + \beta_D\lambda_{DD} + \beta\lambda_{DU} \qquad (4.10\ [20])$$

4.6. Donanım Mimarilerinde Güvenilirlik Hesaplaması

Güvenilirlik analizinin bir sistemin tüm yaşam döngüsü boyunca ekipmanın bağımlılığını artırmak için yapılması gerekir. Başarılı bir güvenilirlik tahmini, ekipmanın yapısını dikkate alarak oluşturulmuş bir model ile olabilir. Bu model oluşturulurken, ekipman ile ilgili bilgiler (örneğin; parça listesi, devre diyagramı) ve probleme uygun seçilen güvenilirlik modelleri(örneğin; güvenilirlik blok diyagramı, hata ağacı analizi, durum uzay metodu) kullanılır.

Donanım mimarilerinde güvenilirlik analizi yapılırken Hata Türü ve Etkileri Analizi (FMEA) risk değerlendirme motodu IEC 61508 tarafından önerilmekte ve uygulanmaktadır.

Hata Türü ve Etkileri Analizi(FMEA), askeri sistemlerdeki hataların analizi için güvenilirlik mühendisleri tarafından geliştirilmiştir. FMEA, yeni bir ürünün tasarım aşamasında oluşabilecek muhtemel hataların tanımlanmasında kullanılan bir risk değerlendirme metodolojisidir. Donanımların fonksiyonel güvenilirlik analizinde; her bir bileşen veya bileşen grubunun her bir hata türünün etkisi analiz edilmekte ve bu analiz sonucunda istenilen güvenlik bütünlük seviyesi belirlenebilmektedir.

Her bir alt sistem için FMEA'nın gerçekleştirilebilmesi için gerekli olan bilgiler ve adımlar aşağıda sıralanmıştır.

- Güvenlik fonksiyonunu etkileyebilecek tüm bağlantılarda dahil olmak üzere, alt sistemin detaylı blok diyagramı.
- Her bir bileşen veya bileşen grubu ve birbiriyle bağlantıları da dahil olmak üzere donanım devre çizimi.
- Her bir bileşenin veya bileşen grubunun hata modları ve oranları ve bunların güvenli ve tehlikeli hatalara karşılık gelen toplam hata olasılığı.
- Hata modlarının güvenli ve tehlikeli hata olarak kategorize edilmesi.
- Bileşenlerin hata oranları ve FMEA sonucuna göre, güvenli hata (λ_S) ve tehlikeli hata(λ_D) olasılıklarının belirlenmesi.
- Her bir bileşen için tanı testi ile tespit edilebilecek, tespit edilen tehlikeli hata oranı belirlenmesi.
- Bir alt sistem için toplam tehlikeli hata oranı ($\Sigma\lambda_D$), toplam tespit edilen tehlikeli hata oranı ($\Sigma\lambda_{DD}$) ve toplam güvenli hata oranının ($\Sigma\lambda_S$) belirlenmesi.
- Alt sistemin teşhis kapsamı hesaplanır. ($DC= \Sigma\lambda_{DD}/\Sigma\lambda_D$)
- Alt sistemin güvenli hata oranı belirlenir. ($SFF= \Sigma\lambda_S + \Sigma\lambda_{DD})/(\Sigma\lambda_S + \Sigma\lambda_D$).)

DC ve SFF değerleri hesaplanırken güvenlik fonksiyonunun çalışmasında görev alan, alt sistemi oluşturan elektrik, elektronik, elektromekanik ve mekanik tüm bileşenler dikkate alınmalıdır.

FMEA analizini gerçekleştirmek için sistemin devre diyagramı, çalışması ve kullanılan bileşenler belirlendikten sonra ihtiyaç duyulan en önemli iki husus hata oranlarının ve hata modlarının belirlenmesidir. Bu iki kavramın belirlenmesi aşağıdaki bölümlerde detaylı olarak incelenmektedir.

4.6.1. Hata oranı belirleme

Konsept ve ilk tasarım aşamalarında; hata oranı hesaplamaları, donanım mimarisinin doğru oluşturulması ve hedeflenen güvenilirlik hedefinin tutturulması için gereklidir. Bundan dolayı, güvenilirlik hesaplamaları ekipman tasarım aşamasından başlayacak şekilde olabilecek en erken dönemde uygulanmalıdır [22].

Bir elektronik bileşenin hata modları birçok faktöre bağlıdır. Bunlar; çalışma fazı, kırılma kriteri, stres süresi, çalışma modu, ortam sıcaklığı, sıcaklık döngü oranı, nem, elektriksel stres, döngüsel anahtarlama süresi, mekanik stres, hava basıncı ve özel gerilmeler olarak sıralanabilir. Bu doğrultuda, bileşenin çalışma şartları bilinmeden hata oranı değerinin doğru olarak belirlenmesi mümkün değildir. Bundan dolayı, ilgili tüm faktörler hata oranı hesaplanırken verilmelidir.

Hata oranlarının tahmini değerleri, ömür testleri veya saha verilerinden elde edilebilir. Bu tahmini değerlerin sadece test ortam şartları veya kullanıldığı saha şartları için olduğunun unutulmaması gerekir. Bu tahmini değerler, bileşenlerin sabit hata oranına sahip olduğu dönem için üstel dağılım, bebeklik döneminde Weibull ve yıpranma dönemi için gama veya normal dağılım ile hesaplanır [17].

Hata oranının boyutu, birim zamanda olan hata sayısıdır. Burada birim zaman ifadesi bileşen tipine göre; döngü, çalışma sayısı gibi ifadeler ile değiştirilebilir. Genel olarak bileşen hata oranları 10^6 saatteki hata sayısı veya 10^9 saatteki hata sayısı ile ifade edilmektedir.

4.6.2. Hata oranı veri kaynakları ve seçim metodu

Güvenilirlik hesaplamaları yapılırken, ilgili ekipman ve bileşen için ilk olarak uygulanabilir güvenilir saha verilerinin kullanılması önerilmektedir**.** Bunun haricinde veriler aşağıda verilen sıralamaya uygun olarak seçilmelidir [22].

- Kullanıcı verisi.
- Üretici verisi.
- El kitabı (veri tabanı) verisi.

Eğer tahmin için kullanıcı verisi mevcut ise bu verilerin kullanılması gerekmektedir. Eğer kullanıcı verisi yok ise, üreticinin verileri incelenmeli ve uygun olarak değerlendirildiği taktirde kullanılmalıdır. Eğer üreticinin sağladığı böyle bir veri tabanı mevcut değil ise, el kitabı verileri değerlendirilerek uygun olanlar kullanılmalıdır.

Eğer hiçbir veri kaynağına ulaşılamazsa, daha fazla verinin elde edilmesine bir risk değerlendirme sonucunda karar verilmelidir. Örneğin bu veriler, oluşturulacak bir güvenilirlik test programı sonucunda elde edilebilir.

Tüm bu aşamalarda yapılan seçimin teknik olarak doğruluğu gerekçeleri ile gösterilmelidir.

Kullanıcı verileri; kurum içi test, kullanıcı saha tecrübesi, çıkarılan dersler veya uzman değerlendirmesi olabilir. Tüm bu durumlarda; toplanan verilerin uygun olarak toplanıp, detaylı gözden geçirmelerin ve analizlerin yapıldığından emin olmak gerekir. İkinci olarak, üretici tarafından ilgili ürünlere yapılan testler sonucunda oluşturulmuş verilerin kullanılması durumunda; yine bu verilerin uygun olarak toplanıp, detaylı gözden geçirmelerinin ve analizlerinin yapıldığından emin olmak gerekir. Bu doğrultuda hem kullanıcının hem de üreticinin elde ettiği verilerin oluşturulmasında IEC 60300-3-2 ve IEC 60300-3-5 standartları rehber olarak kullanılır.

Kullanıcı ve üretici verilerinin sınırlı sayıda olmasından dolayı genellikle güvenilirlik analizlerinde el kitabı verilerinden yararlanılmaktadır. Bu doğrultuda bileşenlerin hata oranlarının yer aldığı çeşitli güvenilirlik el kitapları mevcuttur. Bu veriler, askeri ve haberleşme gibi özel uygulamalardan elde edilerek oluşturulmuştur. Bazı durumlarda bu verilerin nereden elde edildiği belli olmadan, sadece saha verilerinden elde edildiği durumlar olmaktadır. Bundan dolayı, hata oranı tahminleri saha gözlemlerine göre farklılıklar göstermekte ve yanlış sonuçlara yönlendirebilmektedir. Bundan dolayı veri tabanı seçiminin uygulamaya yönelik yapılması gerekir. Bu doğrultuda kullanılabilecek güvenilirlik el kitapları (veri tabanları) aşağıda sıralanmıştır [22].

- AT&T Güvenilirlik El Kitabı (AT&T Reliability manual)
- Nükleer enerji santrallerindeki PSA için bileşen hata oranı tahmini, 1982-1997 (Prediction of component failure rates for PSA on nuclear power plants 1982-1997)
- FIDES
- Proses ekipman güvenilirlik veri kılavuzu ve data tabloları (Guidelines for process equipment reliability data –With data tables)

- HDR5: Britanya Telekom güvenilirlik el kitabı (HRD5: British Telecom Handbook of reliability data)
- IEEE 493-2007
- IRPH 2003: Italtel güvenilirlik tahmin el kitabı (IRPH 2003: Italtel Reliability prediction Handbook)
- MIL-HDBK-217F Elektronik ekipmanların güvenilirlik tahmini (MIL-HDBK-217F Reliability prediction of electronic equipment)
- NPRD 2016
- NSWC-11 Mekanik ekipman güvenilirlik tahmin prsedürleri el kitabı (NSWC-11 Handbook of reliability prediction procedures for mechanical equipment.)
- OREDA: Açık deniz ve kıyı güvenlik verisi (OREDA: Offshore and onshore reliability data)
- UTE C80-810
- Güvenlik enstrümanlı ekipmanların güvenilirlik verisi için PDS veri el kitabı (Reliability data for safety instrumented equipment PDS data handbook, 2006 Edition)
- Hata modu/mekanizması dağılımları FMD-2016 (Failure Mode/Mechanism Distributions FMD-2016)
- Güvenlik Ekipmanı Güvenilirlik El Kitabı – 4. Baskı (Safety Equipment Reliability Handbook - 4th Edition)
- Siemens SN 29500
- TELCORDIA SR-332

İlgili el kitapları arasında, tıbbi uygulamalardan elde edilerek oluşturulmuş bir güvenilirlik veri tabanı halihazırda mevcut değildir.

Güvenilirlik el kitabı kaynaklarından yararlanırken izlenecek yok aşağıda verilmiştir.

- Yapılan uygulamaya uygun veri tabanının seçimi.
- Referans şartların belirlenmesi.
- Bu şartlara göre hata oranlarının belirlenmesi.

Örneğin genel amaçlı bir transistor için belirlenen referans şartlar için veri tabanı kullanılarak yapılacak bir hata oranı hesaplaması Eşitlik (4.11)'de verilen çalışma

koşulları altındaki bileşen hata oranı denklemine göre aşağıdaki adımlar uygulanarak hesaplanır [22].

1. El kitabı seçimi, örneğin MIL-HDBK-217F, 1995
2. Referans şartları belirle:
   Referans eklem sıcaklığı: θ ref = 55°C ,
   Voltaj oranı: Uref / Urat = 0,5 (Anma geriliminin yarısı)
3. Referans şartlar için el kitabından hata oranını belirle.
   (MIL-HDBK-217F:1995, Madde 6.6)

$$\lambda_p = \lambda_b \, x \, \pi_T \, x \, \pi_R \, x \, \pi_S \, x \, \pi_Q \, x \, \pi_E \qquad (4.11\ [23]\ )$$

$\lambda_b = 0{,}18\, x10^{-6}h^{-1}$ $(Baz\ hata\ oranı)$

$\pi_T = 1{,}9$, θ ref $=$ 55°C için (Sıcaklık faktörü)

$\pi_R = 0{,}43,\ \ g$üç $< 0{,}1\ W\ için$ (Güç oranı faktörü)

$\pi_S =$ $0{,}21, Vs \equiv U$ref$/\ U$rat $=$ $0{,}5$ için (Gerilim stres faktörü)

$\pi_Q = 1$ (Kalite faktörü)

$\pi_E = 1$ (Çevresel faktör)

$\lambda_p = 0{,}18\, x10^{-6}h^{-1} x\ 1{,}9\ x\ 0{,}43\ x\ 0{,}21\ x\ 1 x\ 1 \cong 30{,}9 x10^{-9}h^{-1}$

Direnç için örnek hata oranı;

1. El kitabı seçimi, örneğin MIL-HDBK-217F, 1995
2. Referans şartları belirle:
   RC tipi MIL-R-11 standardına uygun direnç:
   Referans eklem sıcaklığı: θ ref = 50°C ,
   Voltaj oranı: Uref / Urat = 0,2 (Anma geriliminin %20 si)
   Gücü 1 W
3. Referans şartlar için el kitabından hata oranını belirle

(MIL-HDBK-217F:1995, Madde 9.1)

$$\lambda_p = \lambda_b \, x\pi_T \, x\pi_R \, x \, \pi_S \, x \, \pi_Q \, x \, \pi_E$$

$\lambda_b = 0{,}0017 \, x10^{-6}h^{-1}$ $(Baz\ hata\ oranı)$

$\pi_T = 1{,}8$, θ ref $=$ 50°C için (Sıcaklık faktörü)

$\pi_R = 1$, $1\ W\ için$ (Güç oranı faktörü)

$\pi_S = 0{,}81, Vs \equiv Uref/\ Urat = 0{,}2$ için (Gerilim stres faktörü)

$\pi_Q = 10$ (Kalite faktörü), $\pi_E = 1$ (Çevresel faktör)

$\lambda_p = 0{,}0017 \, x10^{-6}h^{-1}x \, 1{,}8 \, x \, 1 \, x \, 0{,}81 \, x \, 10 \, x \, 1 \cong 24{,}8x10^{-9}h^{-1}$

4.6.3. Hata modlarının belirlenmesi

Her bir bileşen için hata oranları ilgili veri tabanı üstünden belirlendikten sonra FMEA için her bir bileşenin muhtemel hata modlarının belirlenmesi gerekmektedir. Elde edilen hata oranı sonrası ilgili bileşenin hata modları ve ilgili hataya düşme oranları kullanılarak FMEA gerçekleştirilir. Bu analiz sonunda donanımın, DC ve SFF değerleri hesaplanır. Bileşen hata modları için kullanılabilecek kaynaklar aşağıda verilmiştir.

- IEC 61709 Elektronik bileşenler-Güvenirlik -Arıza dereceleri için referans şartları ve değiştirme için gerginlik modelleri
- MIL-HDBK-338B MILITARY HANDBOOK, ELECTRONIC RELIABILITY DESIGN HANDBOOK

Örneğin, direnç, transistör ve diyotların tipine göre hata modları IEC 61709 standardına göre Çizelge 4.10'de gösterilmiştir.

Devreyi oluşturan baskı devre kartı dahil tüm bileşenlerin hata modları IEC 61709 standardı veya diğer veri kaynaklarından elde edilerek FMEA'da hata modları olarak ele alınmalıdır.

Çizelge 4.10: Direnç, diyod ve transistörlerin IEC 61709'a göre hata oranları.

Direnç Tipi	**Açık Devre (OC) Hata Oranı %**	**Kısa devre (SC) Hata Oranı %**	**Değer Değişimi(Drift) Hata Oranı %**
Karbon film direnç	100	-	-
Metal film direnç	40	-	60
Yüksek kayıplı film direnç	100	0	-
Tel sargılı direnç (wire-wound)	100	-	-
Değişken direnç(tel sargısız sermet potansiyometre)	80	-	20
Direnç ağları(yüzey montajlı dirençler ve direnç dizileri)	40	-	60
Transistör Silikon	85	15	-
GaAs	95	5	-
Diyot Silikon	80	20	-
GaAs	95	5	-

4.6.4. Örnek FMEA uygulaması

FMEA için gereklilikler anlatıldığı gibi elde edildikten sonra sistemi oluşturan her bir bileşen veya bileşen grubunun hata modları değerlendirilerek etkileri analiz edilmelidir. Bu doğrultuda güvenilirlik hesaplaması için Çizelge 4.11'de direnç ve tiransistör için verilen örnek gibi donanımı oluşturan tüm bileşenlerin hata oranları analiz edilerek dokümante edilmelidir.

Her bir bileşen için λ_{SD}, $\lambda_{SU,}$ λ_{DD} ve λ_{DU} değerleri hata modları ve hata oranları ile hesaplandıktan sonra DC ve SFF değerleri hesaplanır. Bu elde edilen değerler ile 4.5 bölümünde verilen PFH hesaplama formüllerine göre hata oranları alt sistemin hata oranı tespit edilir. Daha sonra sistemi oluşturan tüm alt sistemlerin PFH değerleri toplanarak kontrol sisteminin hata oranı bulunup istenilen SIL değerini karşılayıp karşılamadığı analiz edilir.

Çizelge 4.11: Örnek FMEA çizelgesi.

Bileşen Adı:	**Sayısı:**	**Tipi:**	**Hata modu**	**Hata oranı %**	**Hatanın sonucu**	**Hata güvenlik fonksiyonu için tehlikeli mi? (Evet/Hayır)**	**Hata tespit edilebilir mi? (Evet/Hayır)**	**DC değeri**	**Hata oranı λ**	**λ_{SD}**	**λ_{SU}**	**λ_{DD}**	**λ_{DU}**
R1	1	Karbon Fim Direnç	Açık Devre	100	Etkisi yok	Hayır	Hayır	1	24,8 x10^{-9}	0	24,8 x10^{-9}	0	0
			Kısa Devre	0	-	-	-	0	0	0	0	0	0
			Değer Değişimi	0	-	-	-	0	0	0	0	0	0
T1	1	BC217 (Silikon)	Açık Devre	85	Çıkış sinyali kesiliyor	Evet	Evet	1	26,3 x10^{-9}	26,3 x10^{-9}	0	0	0
			Kısa Devre	15	Çıkış sinyali yükseliyor	Evet	Evet	1	4,6 x10^{-9}	0	0	4,6 x10^{-9}	0
			Değer Değişimi	0				-	0	0	0	0	0
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .
TOPLAM:									55,7 x10^{-9}	26,3 x10^{-9}	24,8 x10^{-9}	4,6 x10^{-9}	0

5. FONKSİYONEL GÜVENLİK HESAPLAMA PROGRAMI

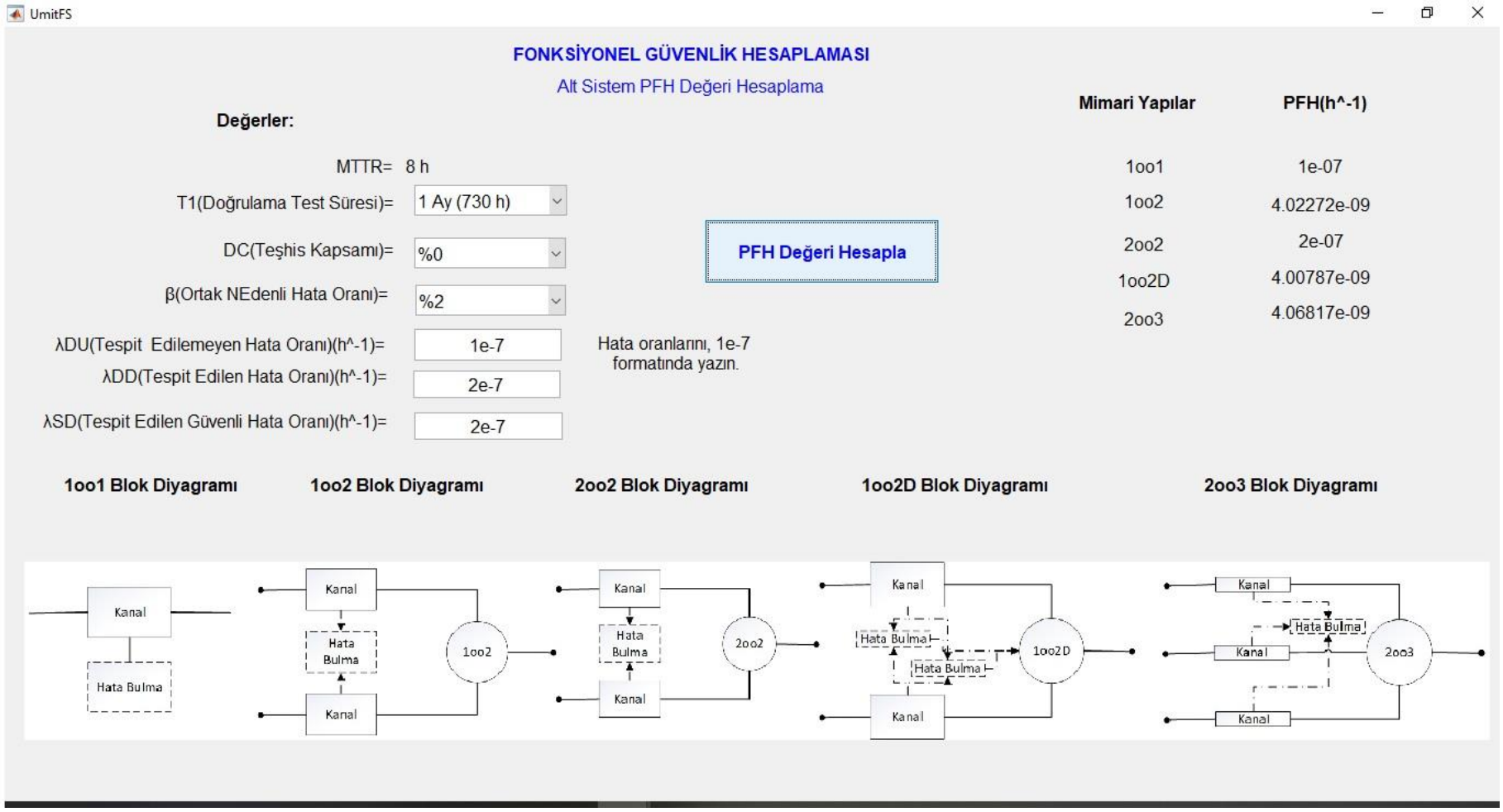
5.1. Fonksiyonel Güvenlik Hesaplamaları için PFH Hesaplama Programı

Bu tezin 4. Bölümünde donanım mimarilerinin fonksiyonel güvenliğinin nasıl sağlanacağı açıklanarak, farklı donanım mimari yapı örnekleri ve bu mimarilerin saatteki hataya düşme olasılıklarının (PFH) nasıl hesaplanacağı açıklanmıştır. Tez kapsamında; hata oranı (λ), β, DC ve T_1 değerlerinin sistem hata oranlarını nasıl etkilediğinin anlaşılması için bu tezin 4.5 bölümünde detayları açıklanan 1oo1, 1oo2, 2oo2,1oo2D ve 2oo3 mimari yapılarının PFH değeri hesaplaması için MATLAB kullanılarak bir program geliştirilmiştir.

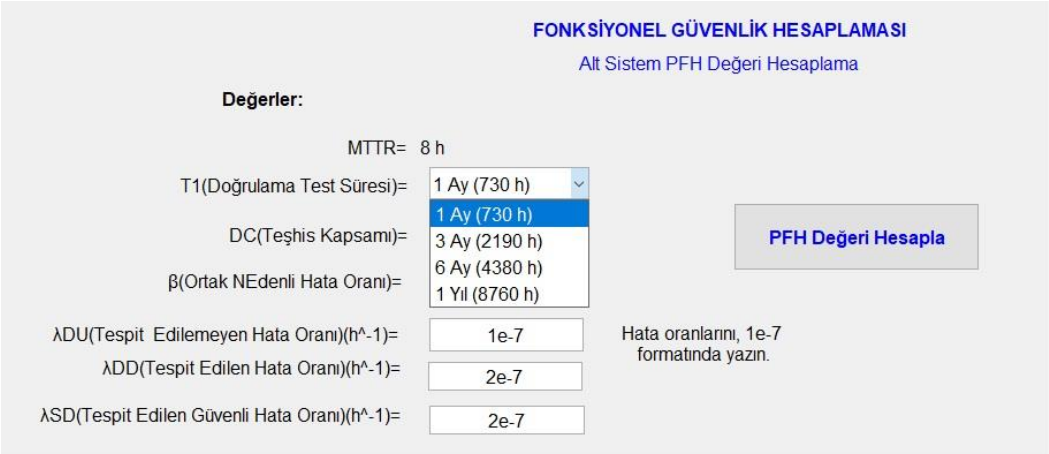
Geliştirilen bu program ile PFH değerlerini etkileyen T_1, β, DC ve bu tezin 4.6 bölümünde hesaplama yöntemi açıklanan λ değerleri, kullanıcı tarafından girilerek her bir mimari yapı için PFH değerleri hesaplanmaktadır.

İlgili parametreler kullanıcı tarafından girildikten sonra "PFH Değeri Hesapla" tuşu ile beş farklı mimari yapı için sonuçlar elde edilmekte ve program arayüzünde gösterilmektedir. Alt sistemler için PFH hesaplama programının arayüzü Şekil 5.1'de görülmektedir.

PFH değerlerinin hesaplanması için ilgili programda Şekil 5.2'de de görüldüğü üzere β, DC ve T_1 değerleri seçilebilmektedir. Doğrulama test süresi T_1 için IEC 61508 kapsamında sürekli çalışma modlu sistemler için verilen 730,2190,4380 ve 8760 saat seçenekleri bulunmaktadır. Teşhis kapsamı %0, %60, %90 ve %99 olarak seçilebilirken, ortak nedenli hata oranı β, %2, %10 ve %20 olarak programda yer almaktadır.



Şekil 5.1: Alt sistem PFH değeri hesaplama program arayüzü.



Şekil 5.2: Programın, PFH değerini etkileyen değişkenlerin giriş bölümü.

Hata oranı değerleri olan λ_{DU}, λ_{DD} ve λ_{SD} değerlerinin kullanıcı tarafından programa girilmesi gerekmektedir. Seçilen parametreler ve hata oranı değerlerinden sonra program

Şekil 5.3'de görüldüğü programın sağ tarafında ilgili mimari yapılar için PFH değerlerini hesaplayarak göstermektedir.

Mimari Yapılar	PFH(h^-1)
1oo1	1e-07
1oo2	4.02272e-09
2oo2	2e-07
1oo2D	4.00787e-09
2oo3	4.06817e-09

Şekil 5.3: Beş farklı mimari yapı için hesaplanan PFH değerleri.

5.2. PFH Hesaplama Programı ile Yapılan Örnek Hesaplama

Geliştirilen PFH hesaplama programı kullanılarak λ, β ve DC değerlerine göre PFH değerleri hesaplanmıştır. Bu hesaplamada, alt sistemin hata oranını sabit kabul ederek

(λ_1 ve λ_2), bir aylık doğrulama test aralığı için β ve DC değerlerine göre hesaplanan PFH değerleri Çizelge 5.1'de gösterilmiştir.

Çizelge 5.1: İki farklı hata değeri bir aylık doğrulama test aralığı için PFH değerleri.

Mimari	**DC**	**λ_1 =1e-9**			**λ_2 =5e-7**		
		β =%2 β_D =%1	**β =%10 β_D =%5**	**β =%20 β_D =%10**	**β =%2 β_D =%1**	**β =%10 β_D =%5**	**β =%20 β_D =%10**
1oo1	%0	5e-10	5e-10	5e-10	2,5e-7	2,5e-7	2,5e-7
	%60	2e-10	2e-10	2e-10	1e-7	1e-7	1e-7
	%90	5e-11	5e-11	5e-11	2,5e-8	2,5e-8	2,5e-8
	%99	5e-12	5e-12	5e-12	2,5e-9	2,5e-9	2,5e-9
1oo2	%0	1e-11	5e-11	1e-10	5,04e-9	2,50e-8	5e-8
	%60	2e-12	3,5e-11	7e-11	3,52e-9	1,75e-8	3,5e-8
	%90	5,5e-12	2,75e-11	5,5e-11	2,76e-9	1,38e-8	2,75e-8
	%99	5,1e-12	2,53e-11	5,1e-11	2,53e-9	1,26e-8	2,53e-8
2oo2	%0	1e-9	1e-9	1e-9	5e-7	5e-7	5e-7
	%60	4e-10	4e-10	4e-10	2e-7	2e-7	2e-7
	%90	1e-10	1e-10	1e-10	5e-8	5e-8	5e-8
	%99	1e-11	1e-11	1e-11	5e-9	5e-9	5e-9
1oo2D	%0	1e-11	5e-11	1e-10	5,04e-9	2,5e-8	5e-8
	%60	7e-12	3,5e-11	7e-11	3,51e-9	1,75e-8	3,5e-8
	%90	5,5e-12	2,75e-11	5,5e-11	2,75e-9	1,38e-8	2,75e-8
	%99	5,1e-12	2,53e-11	5,1e-11	2,53e-9	1,26e-8	2,53e-8
2oo3	%0	1e-11	5e-11	1e-10	5,1e-9	2,51e-8	5e-8
	%60	7e-12	3,5e-11	7e-11	3,56e-9	1,76e-8	3,5e-8
	%90	5,5e-12	2,75e-11	5,5e-11	2,77e-9	1,38e-8	2,75e-8
	%99	5,1e-12	2,53e-11	5,1e-11	2,53e-9	1,26e-8	2,53e-8

Yapılan hesaplama sonuçlarına göre çok kanallı mimari yapılara geçildikçe PFH değerinin azaldığı görülmektedir. Alt sistemlerdeki hataların teşhis edilme oranını gösteren DC değerinin PFH değerini düşürdüğü Çizelge 5.1'de görülmektedir.

Ayrıca, ortak nedenli hataları gösteren β faktörünün 1oo1 ve 2oo2 gibi tek kanallı yapıdaki sistemlerde bir etkisinin olmadığı, β değerinin artması ile çok kanallı mimarilerde hata oranının arttığı görülmektedir.

5.3. Bir Kontrol Sisteminin Güvenilirlik Bütünlük Seviyesinin Artırılması

Alt sistemler için hesaplanan PFH değerleri sonrasında, kontrol sistemini oluşturan sensör, mantık ve final eleman alt sistemlerinin mimari yapısının sistemin SIL değerine etkisi incelenmiştir. Bu doğrultuda, tek kanallı mimari yapıya sahip bir sistemin 5.2 bölümünde verilen PFH çizelgesine göre toplam saatteki hata olasılığı hesaplanmıştır. Sistemin ilk durumu ve daha sonra sistemde yapılan iyileştirme sonuçları Çizelge 5.2'de gösterilmiştir.

Çizelge 5.2: Sistemde yapılan iyileştirmenin SIL değerine etkisi.

Sistem	**Sensör Alt Sistemi**	**Mantık Alt Sistemi**	**Final Eleman Alt Sistemi**	**Toplam PFH**	**Sistemin SIL Değeri**
İlk Durum	1oo1 β =%2 DC =%60 **λ =5e-7** PFH_S=1e-7	1oo1 β =%10 DC =%0 **λ =5e-7** PFH_L=2,5e-7	1oo1 β =%10 DC =%60 **λ =5e-7** PFH_F=1e-7	PFH_{SYS}=4,5e-7	SIL 2
İyileştirme (Çok kanallı mimariye geçiş.)	2oo3 β =%2 DC =%60 λ =5e-7 PFH_S=3,56e-9	1oo2 β =%10 DC =%0 **λ =5e-7** PFH_L=2,50e-8	1oo2 β =%10 DC =%60 λ =5e-7 PFH_F=1,75e-8	PFH_{SYS}=4,61e-8	SIL 3

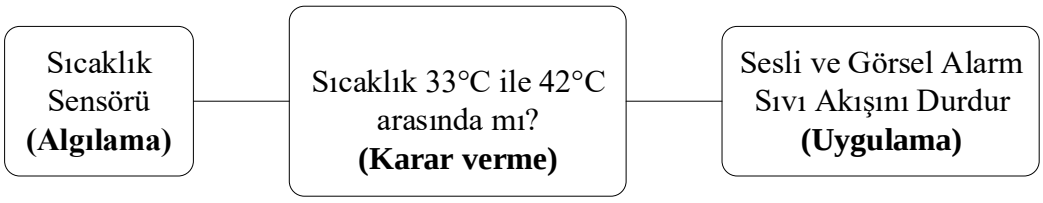
Tek kanallı mimari yapılara sahip alt sistemlerin ilk durumda toplam PFH_{SYS} değeri SIL 2'ye karşılık gelmektedir. Sistemin güvenilirlik seviyesini artırmak için tüm alt sistemlerin β, Dc ve λ değerleri değiştirilmeden sadece çok kanallı mimari yapıya dönüştürülmüştür. Yapılan bu iyileştirme sonucu, PFH_{SYS} değeri düşmüş ve sistem güvenilirlik seviyesi SIL 2'den SIL 3'e çıkmıştır.

Bu doğrultuda, emniyet kritik bir kontrol sisteminde yedekli sensör, işlem birimi ve aktüatörler kullanılarak sistemin güvenilirlik seviyesinin nasıl iyileştirileceği görülmüştür.

5.4. Hemodiyaliz Cihazı için Örnek SIL Hesaplama

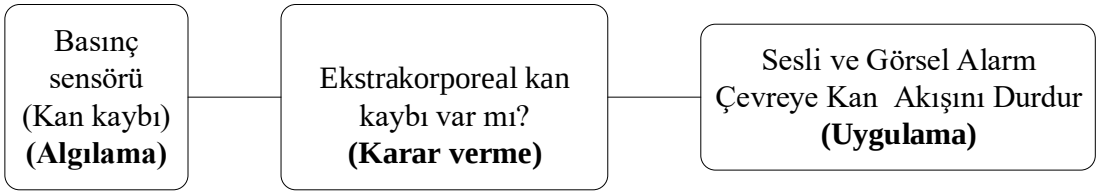
Bu tezin 1.2 bölümünde anlatıldığı üzere, tıbbi cihaz standartları koruyucu sistemlerin cihaz tasarımlarında kullanılmasını istemektedir. Bu doğrultuda IEC 60601-2-16 hemodiyaliz cihaz standardı bu tezin 1.2 bölümünde detayları verilen fonksiyonların kontrolü için koruyucu sistemlerin kullanılmasını istemektedir. Bu doğrultuda, aşağıda örnek olarak diyaliz sıvısı ve değişim sıcaklığının izlenmesi ile çevreye ekstrakorporeal kan kaybı tehlikesi için oluşturulacak koruyucu sistemlerin fonksiyonel güvenliği incelenmiştir.

IEC 60601-2-16 hemodiyaliz cihaz standardı, diyaliz sıvısı ve değişim sıcaklığını 33°C ile 42°C arasında olduğunu takip edecek diğer sıcaklık izleme sistemlerinden bağımsız bir koruyucu sistemin kullanılmasını istemektedir. Sıcaklık seviyesinin bu sınırlar dışına çıkması durumunda hemodiyaliz cihazının sesli ve görsel uyarı sistemini çalıştırması ve sıvı akışını durdurması gerekmektedir. Sıcaklık izleme kontrol sisteminin blok diyagramı Şekil 5.4'de verilmiştir.



Şekil 5.4 Diyaliz sıvısı ve değişim sıcaklığı izleme sistemi blok diyagramı.

Yine aynı şekilde, ekstrakorporeal devrede olabilecek bir yırtılma sonucunda kan kaybının oluşmasını izleyecek bir koruyucu sistemin kullanılması gerekmektedir. Bu koruyucu sistemin kan kaybını algılaması durumunda sesli ve görsel uyarı sistemini çalıştırarak çevreye olan kan akışını durdurması gerekmektedir. Kay kaybı izleme kontrol sisteminin blok diyagramı Şekil 5.5'de verilmiştir.



Şekil 5.5 Çevreye ekstrakorporeal kan kaybını önleyen koruyucu sistem

Sıcaklık ve kan kaybı izlemesi için oluşturulacak kontrol sistemlerinin tasarımında Şekil 5.4 ve Şekil 5.5'de verilen her bir alt sistem, bu tezin önceki bölümlerinde anlatılan fonksiyonel güvenlik gereklerine göre tasarlanıp kullanılabilir. Bunun yanında piyasada özellikle endüstriyel uygulamalar için geliştirilmiş SIL sertifikalı sensör, mantık ünitesi ve final elemanlar da bulunmaktadır. Bu belgeli alt sistemler kullanılarak da kontrol sistemlerin güvenlik bütünlük seviyesi belirlenebilir.

Bu doğrultuda karar verme ünitesi olarak fonksiyonel güvenlik uygulamaları için geliştirilmiş mikro denetleyiciler bulunmaktadır. Bu mikro denetleyicinin fonksiyonel güvenlik uygunluğunun her bir güvenlikle ilişkili ürün veya proje için doğrulanması gerekmektedir. Bu amaçla üreticilerin mikro denetleyicilerin hata modları ve hata oranlarının analizi için araçları bulunmaktadır. Fonksiyonel güvenlik uygulamalarında kullanılabilecek bazı mikro denetleyici modelleri Çizelge 5.3'de verilmiştir.

Çizelge 5.3 Fonksiyonel güvenlik uygulamaları için geliştirilmiş bazı mikro denetleyiciler.

Üretici	**Model**	**SIL seviyesi**
Texas Instruments	Hercules RM46L850	SIL 3'e kadar
STMicroelectronics	STM32	SIL 2/3
Microchip	PIC24/dsPIC	Otomotiv Uygulamaları için (Automotive Safety Integrity Level D, ASIL D)

Hemodiyaliz standardının istediği sıcaklık ve kan kaybının kontrolü için sıcaklık ve basınç sensörü kullanılması gerekmektedir. Sıcaklık ve basınç sensörü olarak tıbbi uygulamalar için geliştirilmiş SIL belgeli bir ürün piyasada bulunmamaktadır. Ancak, endüstriyel uygulamalar için geliştirilmiş ve hata oranları ile SIL seviyesi üretici tarafından sağlanan sensörler bulunmaktadır. Bu doğrultuda endüstriyel uygulamalar

için geliştirilmiş bazı alt sistemlerin fonksiyonel güvenlik parametreleri Çizelge 5.4'de verilmiştir. Endüstriyel uygulamalar için geliştirilmiş basınç sensörlerinin çalışma aralığı, insan kan basınç değeri olan 120/80 mmHg (0,16/0,11 bar) seviyesinin çok üstünde değerlere sahiptir. Bu sensörlerin tıbbi uygulamalara yönelik versiyonlarının geliştirmesi tıbbi cihaz güvenilirliği için gerekmektedir.

Çizelge 5.4 SIL belgeli alt sistem örnekleri.

Alt sistem	Üretici	Fonksiyonel Güvenlik Parametreleri
Sıcaklık sensörü alt sistemi	Siemens TH420 Sıcaklık Vericisi (PT10..10000 sıcaklık sensörü ile kullanılır.) (-200 ... +850 °C)	SIL 3 PFH= $4,8x10^{-8}$ SFF=%94 DC=%94 HFT=1 $\lambda_{SU}=0$ $\lambda_{DD}=443x10^{-9}$ $\lambda_{DU}=27x10^{-9}$
Basınç sensörü alt sistemi	Danfoss DST P92S (0-40 bar)	SIL2 PFH= $8,4x10^{-7}$ SFF=%95 HFT=0

IEC 60601-2-16 hemodiyaliz cihaz standardı tarafından istenilen sıcaklık ve kan kaybı izleme sistemlerinde Çizelge 5.4'de verilen alt sistem parametreleri tıbbi uygulamalar için geliştirilmemesine rağmen referans değer olarak güvenlik bütünlüğü seviyesi hesaplamasında dikkate alınmıştır. Bununla birlikte sesli ve görsel alarm ve sıvı/kan akışını durdurma sistemi için bir referans alt sistem bulunamadığı için Çizelge 5.5'de verilen değerler referans olarak alınmıştır.

Alt sistemlerin PFH değerleri üstünden SIL karşılıkları belirlenebilmektedir. Her bir alt sistemin SIL değeri belirlendikten sonra kontrol sisteminin SIL seviyesi belirlenir. Kontrol sistemin SIL seviyesi, sistemi oluşturan alt sistemlerin en küçük SIL seviyesine eşit veya daha düşük olabilmektedir. Mantık alt sisteminde kullanılacak mikro denetleyicinin SIL seviyesi sistem tasarımından sonra analiz edilerek bulunması gerektiğinden dolayı, ilgili mikro denetleyicinin sağlayabileceği en yüksek SIL seviyesi SIL 3(1x10-8) dikkate alınmıştır. Sıcaklık ve kan kaybı kontrol sistemleri için hesaplanan güvenlik bütünlük seviye Çizelge 5.5'de gösterilmiştir.

Çizelge 5.5 Hemodiyaliz cihazı için örnek kontrol sistem güvenlik bütünlük seviyesi.

Sistem	**Sensör Alt Sistemi**	**Mantık Alt Sistemi**	**Final Eleman Alt Sistemi**	**Toplam PFH**	**Sistemin SIL Değeri**
Diyaliz sıvısı ve değişim sıcaklığı koruyucu sistemi	β =%20 DC =%0 PFH_S=4,8e-8 SIL 3	TI Hercules RM46L850 Mikro denetleyicisi 1e-8 SIL 3	1oo2 β =%10 DC =%60 λ =5e-7 PFH_F=1,75e-8 SIL 3	En düşük SIL:3 PFH_{SYS}=7,8e-8	SIL 3
Çevreye ekstrakorporeal kan kaybını önleyen koruyucu sistem	1oo1 β =%20 DC =%0 PFH_S=8,4e-7 SIL 2	TI Hercules RM46L850 Mikro denetleyicisi 1e-8 SIL 3	1oo2 β =%10 DC =%60 λ =5e-7 PFH_F=1,75e-8 SIL 3	En düşük SIL:2 PFH_{SYS}=8,7e-7	SIL 2

Diyaliz sıvı ve değişim sıcaklığı için SIL3 sertifikalı sıcaklık sensörü ve Texas Instruments'ın RM46L850 mikro denetleyicisi kullanılarak oluşturulacak kontrol sistemi ile kontrol sisteminin saatteki hata oranı $7,8x10^{-8}$ olarak elde edilmiştir. Oluşturulan bu sistem ile güvenlik bütünlük seviyesi SIL 3 olarak elde edilmiştir.

Çevreye ekstrakorporeal kan kaybını önleyen kontrol sistemi için oluşturulan kontrol sisteminde basınç sensörü kullanılmıştır. Kullanılan basınç sensörü SIL2 güvenlik bütünlük seviyesine sahip olduğu için sistemin sahip olabileceği en yüksek SIL seviyesi 2 ile sınırlanmıştır. Daha yüksek güvenlik bütünlük seviyesine sahip basınç sensörü kullanılarak veya 1oo2 veya 1oo3 mimari yapıda çok kanallı basınç sensörleri kullanılarak sistemin güvenlik bütünlük seviyesi artırılabilir.

6. SONUÇ VE ÖNERİLER

Aktif tıbbi cihazlarda kullanılan programlanabilir elektrikli tıbbi sistemlerin IEC 60601 elektrikli tıbbi cihaz standartları ve Tıbbi Cihaz Yönetmeliği kapsamında süreklilik, güvenilirlik ve performans şartları dikkate alınarak tasarlanması gerekmektedir. Bu tez çalışmasında, aktif tıbbi cihazlarda tehlike riski taşıyan fonksiyonların programlanabilir kontrol sistemi kullanılarak önlendiği durumlarda, yönetmelik şartının sağlanması için bu sistemlerin güvenilir olarak nasıl tasarlanması gerektiği incelenmiştir. Bu doğrultuda elektrikli tıbbi cihaz standartları incelenerek, güvenilirlik şartlarına göre tasarlanması gereken otomatik koruyucu sistemler için örnekler verilmiştir.

Öncelikle Tıbbi Cihaz Yönetmeliği ve standartlarında güvenilirlik şartlarının nasıl açıklandığı bu tez kapsamında incelenmiştir. Tıbbi cihaz standartlarında programlanabilir kontrol sistemleri için istenilen güvenilirlik sağlama kriterlerinin, fonksiyonel güvenlik standartları ile eşleştiği tespit edilmiştir. Ancak tıbbi cihaz standartlarında kontrol sisteminin güvenlik bütünlük seviyesinin (SIL) ne olması gerektiği ve tasarımında kullanılacak tekniklerin açıklamadığı tespit edilmiştir. Bu doğrultuda otomotiv sanayi, proses güvenliği ve nükleer enerji santralleri de dahil olmak üzere emniyet kritik uygulamaların tamamında kullanılan fonksiyonel güvenlik standartlarının tıbbi cihaz ürün geliştirme süreçlerinde de kullanılması ile tıbbi cihazların güvenilirliğinin sağlanacağı açıklanmıştır.

Fonksiyonel güvenliğin temel standardı olan IEC 61508 temel alınarak, fonksiyonel güvenlik için süreçler bu tez kapsamında açıklanmıştır. Kontrol sistemlerinin güvenilirliği hem yazılım hem de donanım mimarileri için incelenmesi gereken bir husustur. Bu tez kapsamında yazılım güvenilirliğine değinilmekle birlikte donanım güvenilirliğine odaklanılmıştır. Donanımların güvenilirliğinin anlaşılması için güvenilirlik teorisi açıklanarak, donanım mimari yapılarının için IEC 61508 standardı

kapsamında güvenilirlik hesaplama adımları incelenmiştir. Güvenilirlik artırma yöntemlerinden çok kanallı mimari yapı için ortak nedenli hataların nasıl azaltılacağı açıklanıp, çok kanallı mimarilerin hata oranını gösteren β faktörü incelenmiştir.

Donanımların fonksiyonel güvenliği için sistematik hatalar ve rastgele donanım arızaları incelenerek, güvenilirlik hesaplamasının nasıl yapılacağı açıklanmıştır. 1oo1, 1oo2, 2oo2, 1oo2D ve 2oo3 mimari yapıları için IEC 61508 standardına göre güvenilirlik blok diyagramı metodu kullanılarak elde edilen hata oranları gösterilmiştir. Daha sonra, rastgele donanım arızaları için bileşenlerin hata modları ve hata oranları kullanılarak SIL hesaplamasında kullanılacak hata oranlarının FMEA ile nasıl elde edileceği açıklanmıştır.

Fonksiyonel güvenlik için her bir alt sistemin PFH değerlerini hesaplayan bir program MATLAB kullanılarak geliştirilmiştir. Bu program, 1oo1, 1oo2, 2oo2, 1oo2D ve 2oo3 mimari yapıları için β, DC, T_1 ve hata oranlarına göre PFH değerini otomatik hesaplamaktadır. Bu program kullanılarak bu mimariler için değişen parametrelere göre PFH değerleri bulunmuştur. Daha sonra elde edilen bu değerler kullanılarak örnek bir kontrol sisteminin güvenilirlik seviyesinin nasıl artırılabileceği gösterilmiştir.

Bu tez çalışması ile tıbbi cihazlarda kullanılan programlanabilir kontrol sistemlerinin güvenilirliği için fonksiyonel güvenlik şartlarının nasıl kullanılabileceği gösterilmiştir. Gelecekte yapılacak çalışmalarda aktif tıbbi cihazlardaki yazılımların güvenilirliğinin de nasıl sağlanması gerektiği araştırılmalıdır. Ayrıca, bileşenlerin hata oranları için kullanılan el kitapları genellikle askeri ve haberleşme sektörleri için mevcuttur. Tıbbi cihazların güvenilirliği için bileşen hata oranlarını gösteren bir veri tabanının tıbbi uygulamalar özelinde oluşturulması güvenilirlik analizlerinin daha doğru yapılmasını sağlayacaktır.

KAYNAKLAR

[1] **Tıbbi Cihaz Yönetmeliği.** (2011). Ankara: Resmi Gazete (Sayı: 27957).

[2] **Knight, J. C.** (2002). Safety critical systems: challenges and directions. *ICSE 2002,* s. pp. 547-550, Orlando, FL, USA.

[3] **IEC 61508-1.** (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements*. Genevre: International Electrotechnical Commission.

[4] **2017/745 Medical Device Regulation.** (2017). Brüksel: Avrupa Birliği Resmi Gazetesi.

[5] **TBMM.** (2001). Ürünlere İlişkin Teknik Mevzuatın Hazırlanması ve Uygulanmasına Dair Kanun. Ankara: Resmi Gazete (Sayı: 24459).

[6] **Laurel Macomber, A. S.** (2018). *General Safety and Performance Requirements (Annex I) in the New Medical Device Regulation.* Milton Keynes: BSI Standards Ltd.

[7] **Makine Emniyeti Yönetmeliği 2006/42/AT.** (2009). Ankara: T.C. Resmi Gazete (Sayı: 27158).

[8] **Guidance on the applicability of EHSR of the Machinery Directive.** (2008). Brüksel: COCIR.

[9] **IEC 60601-1.** (2012). *Medical electrical equipment - Part 1: General requirements for basic safety and essential performance*. Genevre: International Electrotechnical Commission.

[10] **IEC 62304.** (2015). *Medical device software - Software life cycle processes*. Genevre: International Electrotechnical Commission.

[11] **IEC 60601-2-16.** (2018). *Medical electrical equipment - Part 2-16: Particular requirements for basic safety and essential performance of haemodialysis, haemodiafiltration and haemofiltration equipment*. Genevre: International Electrotechnical Commission.

[12] **IEC 60601-2-19.** (2016). *Medical electrical equipment - Part 2-19: Particular requirements for the basic safety and essential performance of infant incubators*. Genevre: International Electrotechnical Commission.

[13] **IEC 61508-4.** (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations*. Genevre: International Electrotechnical Commission.

[14] **IEC 61508-5.** (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 5: Examples of methods for the determination of safety integrity levels*. Genevre: International Electrotechnical Commission.

[15] **Coppola, A.** (1984, Nisan). Reliability Engineering of Electronic Equipment - A Historical. *IEEE Transactions on Reliability,*, s. pp. 29-35.

[16] **Rook, P. E.** (1990). *Software Reliability Handbook.* Netherlands: Springer .

[17] **Mil-HDBK-338.** (1998). *MIL-HDBK-338B MILITARY HANDBOOK ELECTRONIC RELIABILITY DESIGN HANDBOOK*. The USA Department of Defence.

[18] **IEC 61508-7.** (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures*. Genevre: International Electrotechnical Commission.

[19] **IEC 61508-6.** (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*. Genevre: International Electrotechnical Commission.

[20] **IEC 61508-2.** (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*. Genevre: International Electrotechnical Commission.

[21] **IEC 61709.** (2017). *Electric components - Reliability - Reference conditions for failure rates and stress models for conversion*. Genevre: International Electrotechnical Commission.

[22] **MIL-HDBK-217F.** (1991). *Reliability Prediction of electronic Equipment*. the USA Departmant of Defence.

[23] **Özkılıç, Ö.** (2014). *Risk Değerlendirme.* Ankara: TİSK.

[24] **David J. Smith, K. G.** (2011). *Safety Critical Systems Handbook.* Elsevier Ltd.

Url-1 < *https://www.iec.ch/functionalsafety/faq-ed2/* >, alındığı tarih: 05.15.2019

ÖZGEÇMİŞ

Ad-Soyad	:	Ümit SEVİM
Uyruğu	:	T.C.
Doğum Tarihi ve Yeri	:	27.11.1990 Ankara/TÜRKİYE
E-posta	:	umitsevim@hotmail.com

ÖĞRENİM DURUMU:

- **Lisans :** 2013, Ankara Üniversitesi, Mühendislik Fakültesi, Elektrik-Elektronik Mühendisliği

MESLEKİ DENEYİM VE ÖDÜLLER:

Yıl	**Yer**	**Görev**
2015-Halen	Türk Standardları Enstitüsü	TSE Uzmanı

YABANCI DİL:

İngilizce	2019 IELTS Academic: 6.5/9

TEZDEN TÜRETİLEN YAYINLAR, SUNUMLAR VE PATENTLER:

Sevim Ü, Eroğul O, (2019) "Aktif Tıbbi Cihazlarda Fonksiyonel Güvenlik Gerekliliklerinin İncelenmesi" 10. Uluslararası Avrupa Fen- Matematik-Mühendislik ve Sağlık Bilimleri Kongresi, İzmir