UÇAK TASARIM SÜRECİNDE EMNİYET ANALİZLERİ

2024
YÜKSEK LİSANS TEZİ
MAKİNE MÜHENDİSLİĞİ

Sergen OĞUZ

Tez Danışmanı
Doç. Dr. Harun ÇUĞ

UÇAK TASARIM SÜRECİNDE EMNİYET ANALİZLERİ

Sergen OĞUZ

Tez Danışmanı
Doç. Dr. Harun ÇUĞ

T.C.
Karabük Üniversitesi
Lisansüstü Eğitim Enstitüsü
Makine Mühendisliği Anabilim Dalında
Yüksek Lisans Tezi
Olarak Hazırlanmıştır

KARABÜK
Ocak 2024

Sergen OĞUZ tarafından hazırlanan "UÇAK TASARIM SÜRECİNDE EMNİYET ANALİZLERİ" başlıklı bu tezin Yüksek Lisans Tezi olarak uygun olduğunu onaylarım.

Doç. Dr. Harun ÇUĞ .....
Tez Danışmanı, Makine Mühendisliği Anabilim Dalı

Bu çalışma, jürimiz tarafından Oy Birliği ile Makine Mühendisliği Anabilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir. 31/01/2024

Ünvanı, Adı SOYADI (Kurumu) İmzası

Başkan : Doç. Dr. Harun ÇUĞ (KBÜ) .....

Üye : Prof. Dr. Mehmet Akif ERDEN (KBÜ) .....

Üye : Doç. Dr. Bülent ÖZKAN (GÜ) .....

KBÜ Lisansüstü Eğitim Enstitüsü Yönetim Kurulu, bu tez ile, Yüksek Lisans derecesini onamıştır.

Doç. Dr. Zeynep ÖZCAN .....
Lisansüstü Eğitim Enstitüsü Müdürü

"Bu tezdeki tüm bilgilerin akademik kurallara ve etik ilkelere uygun olarak elde edildiğini ve sunulduğunu; ayrıca bu kuralların ve ilkelerin gerektirdiği şekilde, bu çalışmadan kaynaklanmayan bütün atıfları yaptığımı beyan ederim."

Sergen OĞUZ

ÖZET

Yüksek Lisans Tezi

UÇAK TASARIM SÜRECİNDE EMNİYET ANALİZLERİ

Sergen OĞUZ

Karabük Üniversitesi
Lisansüstü Eğitim Enstitüsü
Makine Mühendisliği Anabilim Dalı

Tez Danışmanı:
Doç. Dr. Harun ÇUĞ
Ocak 2024, 104 sayfa

Havacılık endüstrisi, insanlığın en büyük başarılarından biridir. İnsanların hava yoluyla seyahat etmesini, ticaret yapmasını ve kültürler arası iletişim kurmasını sağlayan bu endüstri, teknolojik, ekonomik ve sosyal açıdan büyük bir öneme sahiptir. Ancak, havacılık endüstrisinin bu başarısının arkasında büyük bir emek, bilgi ve sorumluluk yatmaktadır. Havacılık endüstrisinde en temel sorumluluk emniyettir. Bu çalışmada, havacılık endüstrisinin en önemli ürünlerinden olan uçakların tasarım aşamasında model tabanlı emniyet analizi süreçlerine odaklanılmıştır. Model tabanlı yaklaşımların, tasarımın karmaşıklığını yönetme ve emniyeti azami düzeye çıkarma konusundaki kritik önemine vurgu yapılır. Çalışma, kapsamlı bir literatür taraması ile başlayıp model tabanlı emniyet çalışmalarının teorik temellerini ortaya koymakta ve seçilen durum çalışmaları aracılığıyla bu yöntemlerin geliştirme süreçlerine uygulanabilirliği ile etkinliği incelenmektedir. Belirtilen çalışmalar, uçak tasarım süreçlerinde emniyet analizlerinin nasıl optimize edilebileceğine dair önemli bilgiler sunarak, havacılık emniyeti alanındaki mevcut bilgi birikimine önemli katkılarda

bulunmayı hedeflemektedir. Ayrıca, tasarım aşamasında yapılan model tabanlı emniyet analizlerinin potansiyel risklerin azaltılmasındaki rolü ve bu analizlerin sektördeki emniyet kültürünün gelişimine olan etkileri üzerinde durulmaktadır. Bu çalışmanın havacılık emniyeti alanında önemli bir katkı sağlama potansiyeline sahip olduğu ve uçak tasarımı ve mühendisliği alanındaki gelecek çalışmalara yön verebileceği değerlendirilmektedir.

Anahtar Sözcükler : Havacılık, Uçak, Tasarım, Emniyet, Model Tabanlı Emniyet Analizi

Bilim Kodu : 91410

ABSTRACT

Master Thesis

SAFETY ANALYSIS IN THE AIRCRAFT DESIGN PROCESS

Sergen OĞUZ

Karabük University
Institute of Graduate Programs
Department of Mechanical Engineering

Thesis Advisor:
Assoc. Prof. Dr. Harun ÇUĞ
January 2024, 104 pages

The aviation industry represents one of humanity's greatest achievements. It facilitates air travel, commerce, and intercultural communication, holding significant technological, economic, and social value. Yet, the industry's success is underpinned by immense labor, knowledge, and responsibility, with safety as its cornerstone. This study focuses on model-based safety analysis processes during the design phase of aircraft, one of the industry's most critical products. Emphasizing the pivotal role of model-based approaches in managing design complexity and maximizing safety, the research begins with an extensive literature review, laying the theoretical foundations of model-based safety efforts. Through selected case studies, the applicability and effectiveness of these methods in development processes are examined. The findings offer valuable insights into optimizing safety analyses in aircraft design processes, contributing significantly to the existing knowledge in aviation safety. Moreover, the study explores the role of model-based safety analyses in mitigating potential risks during the design phase and their impact on the evolution of safety culture within the

industry. This research is deemed to have the potential to make a significant contribution to the field of aviation safety and to guide future work in aircraft design and engineering.

Key Word **:** Aviation, Aircraft, Design, Safety, Model Based Safety Analysis.
Science Code : 91410

TEŞEKKÜR

Bu tez çalışmasının tamamlanması, yalnızca kişisel bir çaba değil, aynı zamanda birçok değerli bireyin desteği, bilgisi ve teşviki ile mümkün olmuştur.

Bu vesileyle, beni bilgi ve deneyimleriyle destekleyen öncelikle, tez danışmanım Sayın Doç. Dr. Harun ÇUĞ'a, akademik rehberliği ve tez sürecim boyunca bana gösterdiği destek için derin minnettarlığımı ifade etmek isterim. Bilgeliği ve rehberliği, bu akademik yolculuğumun her aşamasında bana ışık tutmuştur. Kendisinin rehberliği, sadece bu tez sürecinde değil, aynı zamanda gelecekteki akademik ve profesyonel yolculuğumda da benim için bir pusula olacaktır.

Beni akademik ve kişisel gelişimimde cesaretlendirerek her zaman destekleyici bir el uzatan Sayın Doç. Dr. Bülent ÖZKAN'a kalpten teşekkürlerimi sunmak isterim. Benzersiz perspektifleri, derin bilgisi ve değerli önerileri, bu çalışmanın çok daha zengin, kapsamlı ve aydınlatıcı olmasını sağlamıştır. Onunla çalışmak, sadece bir öğrenme deneyimi değil, aynı zamanda bu yolculuğu daha anlamlı ve keyifli kılan bir fırsat olmuştur.

Tez çalışmam sırasında yanımda olan ve değerli katkılarıyla bu süreci daha anlamlı kılan Ertuğrul YÜCEBAŞ ve İlhan ŞAHİN'e de özel bir teşekkür sunmak isterim. İlhan ve Ertuğrul'un dostlukları ve profesyonellikleri, onları sadece değerli iş ortakları yapmakla kalmamış, aynı zamanda pratik bilgileri ve analitik yaklaşımları ile bu akademik eserin şekillenmesinde kilit rol oynamalarını sağlamıştır.

Bu tez yolculuğum boyunca sabırla yanımda duran ve sonsuz sevgiyle beni destekleyen aileme en derin minnettarlığımı ifade etmek isterim. Ailemin sağladığı huzurlu sığınak ve koşulsuz destek, bu akademik başarının temel taşlarından biri olmuştur.

İÇİNDEKİLER

Sayfa

ŞEKİLLER DİZİNİ

Sayfa

Sayfa

ÇİZELGELER DİZİNİ

Sayfa

SİMGELER VE KISALTMALAR DİZİNİ

SİMGELER

α : Koşullu Fonksiyon Kaybı Olasılığı

β : Hata Modu Oranı

λ_p : Parça Hata Oranı (Hata / Milyon Saat)

t : Çalışma Süresi veya Çalışma Döngüsü Sayısı

KISALTMALAR

AB : Avrupa Birliği
ABD : Amerika Birleşik Devletleri
ASAC : Aviation Safety Advisory Committee (Havacılık Emniyeti Danışma Komitesi)
ASAP : Aviation Safety Action Program (Havacılık Emniyeti Eylem Programı)
ASIAS : Aviation Safety Information Analysis and Sharing (Havacılık Emniyeti Bilgi Analizi ve Paylaşımı)
ASRS : Aviation Safety Reporting System (Havacılık Emniyeti Raporlama Sistemi)
CA : Criticality Analysis (Kritiklik Analizi)
CAST : Commercial Aviation Safety Team (Havacılık Emniyeti Eylem Takımı)
CCA : Common Cause Analysis (Ortak Sebep Analizi)
CMA : Common Mode Analysis (Ortak Mod Analizi)
DAL : Development Assurance Level (Geliştirme Güvence Seviyesi)
DD : Dependency Diagram (Bağımlılık Diyagramı)
EASA : European Aviation Safety Agency (Avrupa Havacılık Emniyeti Ajansı)
EASP : European Aviation Safety Programme (Avrupa Havacılık Emniyeti Programı)
ECAC : European Civil Aviation Conference (Avrupa Sivil Havacılık Konferansı)
FAA : Federal Aviation Agency (Federal Havacılık İdaresi)
FC : Failure Condition (Hata Durumu)
FDAL : Functional Development Assurance Level (Fonksiyonel Geliştirme Güvence Seviyesi)
F-FMEA : Functional Failure Modes and Effects Analysis (Fonksiyonel Hata Modu ve Etki Analizi)
FHA : Functional Hazard Analysis (Fonksiyonel Tehlike Analizi)
FMEA : Failure Modes and Effects Analysis (Hata Modları ve Etkileri Analizi)
FMECA : Failure Mode, Effects, and Criticality Analysis (Hata Modu, Etkileri ve Kritiklik Analizi)

FRHS : Factor of Failure Severity (Hata Şiddeti Faktörü)
FRPOC : Factor of Probability of Occurrence (Meydana Gelme Olasılığı Faktörü)
FTA : Fault Tree Analysis (Hata Ağacı Analizi)
ICAO : International Civil Aviation Organization (Uluslararası Sivil Havacılık Örgütü)
IDAL : Item Development Assurance Level (Öğe Geliştirme Güvence Seviyesi)
IFF : Identification Friend or Foe (Dost-Düşman Tanıma)
IPT : Integrated Product Team (Entegre Ürün Takımı)
JAA : Joint Aviation Authorities (Ortak Havacılık Alanı)
MA : Markova Analysis (Markov Analizi)
MBSE : Model Based Safety Engineering (Model Tabanlı Emniyet Mühendisliği)
NASS : National Aviation Safety Strategy (Havacılık Emniyeti ve Ulusal Stratejisi)
Pf : Hata Olasılığı
PRA : Particular Risk Analysis (Özel Risk Analizi)
PSSA : Preliminary System Safety Assessment (Ön Sistem Emniyet Değerlendirmesi)
Ps : Güvenilirlik
RAC : Risk Assessment Code (Risk Değerlendirme Kodu)
RHS : Failure Severity (Hata Şiddeti)
RPOC : Probability of Occurrence (Meydana Gelme Olasılığı)
SFHA : System Functional Hazard Analysis (Sistem Seviyesi Fonksiyonel Tehlike Analizi)
SSA : System Safety Assessment (Sistem Emniyet Değerlendirmesi)
UFHA : Uçak Seviyesi Fonksiyonel Tehlike Analizi
ZSA : Zonal Safety Analysis (Bölgesel Emniyet Analizi)

BÖLÜM 1

GİRİŞ

Emniyet, havacılık endüstrisinde, hava araçlarının tasarımı ve işletimi sırasında oluşabilecek beklenmedik olayların ve kazaların önlenmesini hedefleyen bir kavramdır. Bu kavram, sadece reaktif bir yaklaşımdan ziyade, proaktif bir emniyet kültürünü ve sürekli iyileştirme anlayışını temsil etmektedir. Emniyetin önemi, havacılık sektörünün doğasında yatar; zira bu alanda meydana gelebilecek herhangi bir aksaklık veya kaza, genellikle ciddi sonuçlara ve hatta can kayıplarına yol açabilir.

Hava araçlarının tasarımı ve üretimi, karmaşık mühendislik disiplinlerinin bir araya gelmesiyle şekillenmektedir. Bu süreçlerde asli öneme sahip olan bir faktör, şüphesiz ki emniyettir. Emniyet, sadece tasarımın estetik ve işlevsel (fonksiyonel) yönlerini değil, aynı zamanda hava aracının emniyetli kullanımını da doğrudan etkilemektedir. Hava taşıtlarının insan hayatını taşıyan araçlar olması, emniyetin bu alanda temel bir öncelik haline gelmesinin başlıca sebebidir. Model tabanlı emniyet analizleri, uçak tasarımının her aşamasında riskleri tanımlamak, analiz etmek ve azaltmak için kullanılır. Bu analizler, karmaşık sistemlerin emniyet performansını değerlendirmek ve potansiyel emniyet sorunlarını önceden tespit etmek için hayati öneme sahiptir. Bu durum, hava araçlarının tasarım ve üretim süreçlerinde emniyetin sadece bir gereklilik değil, aynı zamanda bir zorunluluk olduğunu göstermektedir.

Bu çalışmada, uçakların tasarım sürecinde model tabanlı emniyet çalışmaları sürecinin öncelikle temel kavramları üzerinde durulmuştur. Sonrasında başlıca standartlara göre teorik bilgileri işlenmiştir. Daha sonra ise Ansys Medini programı kullanılarak teorik bilgiler pratiğe dönüştürülmüştür

Binghao Hu ve diğerleri taşıyıcı uçak denetim sistemlerinin emniyetini değerlendirmek için dört aşamalı bir süreç önermektedir [1]. Bu süreç, Sun Qin'in aydınlatma sistemleri [2] ve Bo Yu'nun elektrikli eyletim sistemleri üzerine çalışmalarıyla paralellik göstermektedir [3]. Her üç çalışma da sistem emniyet değerlendirmelerinin ayrıntılı ve çok aşamalı yapısını vurgulamaktadır. Syed Haider'in uçak iniş takımı sistemlerinin sertifikasyonu [4] ve Yimin Jiang'ın fren sistemleri [5] üzerine çalışmaları, MBSE (İng. model based safety engineering, model tabanlı emniyet mühendisliği) metodolojisinin etkinliğini vurgulamaktadır. Bu metodoloji, Nve Xiao'nun hava taşıtlarının sistem ve ekipmanı üzerine çalışması [6] ve P. Biswas'ın modern uçak emniyet standartları üzerine analizi [7] ile paralellik göstermektedir. R.E. Caldwell ve D.B. Merdgen'in zonal analizi [8], sistem emniyeti değerlendirmesinin son adımını vurgulamaktadır. Bu, Qunfeng Ye'nin sivil hava araçlarının güvenilirlik ve emniyet üzerine çalışması [9] ve Hao Rong'un STPA (İng. System-Theoretic Process Analysis) temelli emniyet tasarımı [10] ile ilişkilidir, her ikisi de sistem emniyet değerlendirmesinde yenilikçi yaklaşımlar sunmaktadır. Nve Xiao'nun sivil hava taşıtları ve demiryolu sinyal sistemleri arasındaki emniyet değerlendirme süreçlerini karşılaştıran çalışması [11], Salihler'in karar verme aracı olarak sistem emniyet analizi [12] ve Gradel'in kavramsal uçak sistemleri tasarımında MBSA kullanımı [13] ile karşılaştırıldığında, emniyet değerlendirmelerindeki çeşitliliği ve karmaşıklığı göstermektedir. Walter Tye ve Ted Lloyd'un hava aracı sistemlerinin emniyet değerlendirmesi üzerine tarihsel çalışması [14], Yoo, Seung-woo'nun arıza verilerinin olasılıksal analizi [15] ve Koo, Min-Sung'un ölümcül kaza risk seviyeleri analizi [16] ile birlikte değerlendirildiğinde, emniyet değerlendirmesi yaklaşımlarının zaman içinde nasıl evrildiği gösterilmektedir. Kang, Min Seong'un KC-100 sivil hava aracının sistem emniyet değerlendirmesi [17] ve Lee, Kyung-Chol'un uçak ve parçalarının sertifikasyonundaki sistem emniyet değerlendirmesinin önemi üzerine çalışması [18], emniyet değerlendirmesinin uygulama örneklerini ve yöntemlerini sunmaktadır. Bu çalışmalar, Lee, Kang-Yi'nin uçak motorlarının emniyet değerlendirmesi [19] ile birlikte, farklı uçak sistemleri için emniyet değerlendirme süreçlerinin kapsamlılığını ve önemini vurgulamaktadır. Temel Caner Ustaömer'in havacılık kazalarının sebeplerinin insan ve örgütsel faktörlere kayması üzerine çalışması [20], Ayşe Küçük Yılmaz'ın havacılıkta risk yönetiminin önemi üzerine araştırması [21] ile birlikte değerlendirildiğinde, havacılık sektöründe emniyet

kültürünün ve etkili risk yönetiminin önemini göstermektedir. Muhammed Seyda Akdağ'ın Türkiye'deki hava aracı sertifikasyon süreçleri üzerine Hürkuş eğitim uçağı örneği [22] ile birlikte ele alındığında, ulusal ve uluslararası sertifikasyon süreçlerindeki zorlukları ve gereksinimlerini ortaya koymaktadır.

BÖLÜM 2

UÇAK TASARIM AŞAMASINDA GERÇEKLEŞTİRİLEN EMNİYET ÇALIŞMALARI

2.1. EMNİYET ÇALIŞMALARININ HAVACILIK SEKTÖRÜNDEKİ TARİHSEL ARKA PLANI

Havacılık sektöründeki emniyet çalışmalarının tarihsel arka planı, havacılığın ilk yıllarından günümüze kadar uzanan bir süreci kapsamaktadır. Bu süreçte, havacılık endüstrisi, teknolojik, operasyonel ve çevresel faktörlerin etkisi altında sürekli değişim ve gelişim göstermiştir. Bahsedilen değişim ve gelişim, emniyet standartlarının ve yöntemlerinin de sürekli evrim geçirmesini gerektirmiştir. Havacılık endüstrisindeki emniyet çalışmalarının tarihsel arka planını, aşağıdaki dönemlere ayırarak incelenebilir.

Havacılığın İlk Yılları: Havacılığın ilk yılları, 1903'te Wright Kardeşler'in ilk uçuşunu gerçekleştirmesinden, 1914'te I. Dünya Savaşı'nın başlamasına kadar olan dönemi kapsamaktadır. Bu dönemde, havacılık, henüz yeni bir olgu olduğu için, emniyet çalışmaları çok sınırlı ve yetersizdir. Uçaklar, basit ve ilkel tasarımlara sahiptir ve uçuş emniyeti, büyük ölçüde pilotların beceri ve şansına bağlıdır. Bu dönemde, uçak kazaları ve can kayıpları sıkça yaşanmaktadır. Örneğin, 1908'de, Amerika Birleşik Devletleri (ABD) Ordusu'ndan Thomas Selfridge, Orville Wright ile birlikte uçarken, uçağın pervanesinin kırılması sonucu hayatını kaybeden ilk uçak kazası kurbanı olmuştur. Bu dönemde, havacılık endüstrisinde, emniyet standartları veya yönetmelikleri henüz yoktur ve emniyet çalışmaları, daha çok deneme-yanılma yöntemiyle yapılmaktadır [39].

I. Dünya Savaşı ve Sonrası: I. Dünya Savaşı, havacılık endüstrisinde bir dönüm noktası olmuştur. Bu savaşta, uçaklar, askeri amaçlar için yaygın bir şekilde kullanılmıştır. Bu

durum, uçak tasarımı ve üretiminde büyük bir gelişme ve rekabet ortamı yaratmıştır. Uçaklar, daha hızlı, daha güçlü ve daha karmaşık hale gelmiştir. Bu dönemde, emniyet çalışmaları, daha çok uçak performansı ve dayanıklılığı üzerine odaklanmıştır. Uçakların, savaş koşullarına uyum sağlayabilmesi ve düşman ateşinden korunabilmesi için, çeşitli tasarım ve malzeme iyileştirmeleri yapılmıştır. Bu dönemde, havacılık endüstrisinde, emniyet standartları veya yönetmelikleri hala yetersizdir ve emniyet çalışmaları, daha çok mühendislik ve teknik açıdan yürütülmektedir.

Sivil Havacılığın Gelişimi: Sivil havacılığın gelişimi, 1919 yılında ilk uluslararası uçuşun gerçekleştirilmesinden 1939'da II. Dünya Savaşı'nın başlamasına kadar olan dönemi kapsamaktadır. Bu dönemde, havacılık, sadece askeri bir araç olmaktan çıkıp, ticari ve ulaşım amaçlı bir sektör haline gelmiştir. Uçaklar, daha büyük, daha konforlu ve daha güvenli hale gelmiştir. Bu dönemde, emniyet çalışmaları, daha çok sivil havacılığın gereksinimleri ve beklentileri doğrultusunda şekillenmiştir. Uçakların, yolcu ve yük taşıyabilmesi ve uzun mesafeli uçuşlar yapabilmesi için, çeşitli tasarım ve operasyonel iyileştirmeler yapılmıştır. Bu dönemde, havacılık endüstrisinde, emniyet standartları ve yönetmelikleri, ulusal ve uluslararası düzeyde geliştirilmeye başlanmıştır. Örneğin, 1919'da, Paris'te, Uluslararası Sivil Havacılık Konvansiyonu imzalanmıştır. Bu konvansiyon, sivil havacılığın temel ilkelerini ve kurallarını belirlemiştir [40].

1926-1939 Dönemi: Bu dönem, havacılık endüstrisinde, emniyet standartları ve yönetmeliklerinin ulusal ve uluslararası düzeyde geliştirilmeye başlandığı bir dönemdir. Bu dönemde, ABD'de, Hava Ticareti Yasası çıkarılmıştır. Bu yasa, ABD'deki sivil havacılığın düzenlenmesi ve denetlenmesi için bir çerçeve sunmuştur. Ayrıca, 1929'da, Paris'te, Uluslararası Sivil Havacılık Konvansiyonu imzalanmıştır. Bu konvansiyon, sivil havacılığın temel ilkelerini ve kurallarını belirlemiştir. Bu dönemde, havacılık endüstrisinde, emniyet çalışmaları, daha çok uçak tasarımı ve üretimi üzerine odaklanmıştır. Uçaklar, daha büyük, daha konforlu ve daha emniyetli hale gelmiştir. Bu dönemde, havacılık endüstrisinde, emniyet çalışmaları, daha çok mühendislik ve teknik açıdan yürütülmektedir [40].

1939-1945 Dönemi: Bu dönem, II. Dünya Savaşı'nın yaşandığı bir dönemdir. Bu dönemde, havacılık endüstrisi, askeri amaçlar için büyük bir önem kazanmıştır. Bu

dönemde, havacılık endüstrisinde, emniyet çalışmaları, daha çok uçak performansı ve dayanıklılığı üzerine odaklanmıştır. Uçaklar, daha hızlı, daha güçlü ve daha karmaşık hale gelmiştir. Bu dönemde, havacılık endüstrisinde, emniyet çalışmaları, daha çok savaş koşullarına uyum sağlayabilmesi ve düşman ateşinden korunabilmesi için, çeşitli tasarım ve malzeme iyileştirmeleri yapılmıştır. Bu dönemde, havacılık endüstrisinde, emniyet çalışmaları, daha çok askerî açıdan yürütülmektedir [41].

1945-1969 Dönemi: Bu dönem, II. Dünya Savaşı'nın sona ermesi ve jet çağının başlaması ile karakterize edilen bir dönemdir. Bu dönemde, havacılık endüstrisi, sivil ve ticari amaçlar için büyük bir gelişme göstermiştir. Bu dönemde, havacılık endüstrisinde, emniyet çalışmaları, daha çok uçak teknolojisi ve operasyonu üzerine odaklanmıştır. Uçaklar, jet motorları, basınçlı kabinler, radarlar, oto pilotlar ve diğer elektronik sistemler ile donatılmıştır. Bu dönemde, havacılık endüstrisinde, emniyet çalışmaları, daha çok teknolojik ve operasyonel açıdan yürütülmektedir [42].

1969-2024 Dönemi: Bu dönem, havacılık endüstrisinde, emniyet çalışmalarının daha kapsamlı ve sistematik bir şekilde yapılmasına yönelik önemli adımların atıldığı bir dönemdir. Bu dönemde, havacılık endüstrisinde, emniyet çalışmaları, daha çok insan faktörleri ve risk yönetimi üzerine odaklanmıştır. Bu dönemde, havacılık endüstrisinde, emniyet çalışmaları, daha çok bilimsel ve analitik açıdan yürütülmektedir. Bu dönemden günümüze, havacılık endüstrisinde, emniyet çalışmalarının önemli başlıca gelişmeleri aşağıda yer almaktadır [43-45]:

- 1970: Uluslararası Sivil Havacılık Örgütü (ICAO), havacılık emniyeti ile ilgili uluslararası standartları ve tavsiyeleri içeren Ek13'ü yayınlamıştır. Bu ek, havacılık kazalarının ve olaylarının soruşturulması, raporlanması ve önlenmesi için bir rehber sunmaktadır.
- 1974: ABD'de, Federal Havacılık İdaresi (İng. Federal Aviation Agency, FAA), havacılık emniyeti için birincil sorumlu kurum olarak kurulmuştur. FAA, havacılık endüstrisini düzenlemek, denetlemek ve geliştirmek için çeşitli programlar ve politikalar geliştirmiştir.
- 1978: ABD'de, Havacılık Emniyeti Raporlama Sistemi (ASRS) oluşturulmuştur. ASRS, havacılık endüstrisindeki çalışanların, gönüllü

ve gizli bir şekilde, havacılık emniyetini etkileyebilecek herhangi bir olay veya durumu raporlamalarını sağlayan bir sistemdir. ASRS, havacılık emniyeti ile ilgili veri toplamak, analiz etmek ve yaymak için kullanılmaktadır.

- 1981: ABD'de, Havacılık Emniyeti Eylem Programı (ASAP) başlatılmıştır. ASAP, havacılık endüstrisindeki çeşitli kurum ve kuruluşların, havacılık emniyeti ile ilgili ortak sorunları tanımlamak, analiz etmek ve çözmek için iş birliği yapmalarını sağlayan bir programdır. ASAP, havacılık emniyeti ile ilgili araştırma, eğitim ve farkındalık faaliyetlerini desteklemektedir.
- 1987: Avrupa'da, Ortak Havacılık Alanı (JAA) kurulmuştur. JAA, Avrupa ülkelerinin, havacılık emniyeti ile ilgili ortak standartlar ve yönetmelikler geliştirmek ve uygulamak için bir araya geldikleri bir kuruluştur. JAA, havacılık endüstrisindeki emniyet, çevre ve ekonomik performansı iyileştirmeyi amaçlamaktadır.
- 1990: ABD'de, Havacılık Emniyeti Danışma Komitesi (ASAC) kurulmuştur. ASAC, havacılık endüstrisindeki çeşitli paydaşların, havacılık emniyeti ile ilgili konularda FAA'ye tavsiyelerde bulunmalarını sağlayan bir komitedir. ASAC, havacılık emniyeti ile ilgili politika, yönetmelik ve programların geliştirilmesine katkıda bulunmaktadır.
- 1994: Avrupa'da, Avrupa Sivil Havacılık Konferansı (ECAC) tarafından, Avrupa Havacılık Emniyeti Programı (EASP) başlatılmıştır. EASP, Avrupa'daki havacılık emniyeti seviyesini yükseltmek ve uyumlu hale getirmek için bir programdır. EASP, havacılık emniyeti ile ilgili veri toplama, analiz, paylaşım, eğitim ve iş birliği faaliyetlerini kapsamaktadır.
- 1996: ABD'de, Beyaz Saray Komisyonu tarafından, Havacılık Emniyeti ve Ulusal Stratejisi (NASS) yayınlanmıştır. NASS, ABD'deki havacılık emniyeti ve güvenliğinin iyileştirilmesi için bir yol haritası sunmaktadır. NASS, havacılık emniyeti ve güvenliği ile ilgili hedefler, eylemler, sorumluluklar ve performans ölçütleri belirlemektedir.

- 1997: ABD'de, FAA tarafından, Havacılık Emniyeti Eylem Takımı (CAST) oluşturulmuştur. CAST, havacılık endüstrisindeki çeşitli paydaşların, havacılık kazalarını ve can kayıplarını azaltmak için birlikte çalışmalarını sağlayan bir takımdır. CAST, havacılık kazalarının nedenlerini analiz etmek, riskleri değerlendirmek ve bu riskleri azaltmak için çözümler geliştirmek ve uygulamak için veri odaklı bir yaklaşım benimsemektedir.
- 2002: Avrupa'da, Avrupa Birliği (AB) tarafından, Avrupa Havacılık Emniyeti Ajansı (EASA) kurulmuştur. EASA, AB üyesi ülkelerin havacılık emniyeti ile ilgili standartlarını ve uygulamalarını uyumlu hale getirmek ve denetlemek için bir kurumdur. EASA, havacılık emniyeti ile ilgili sertifikasyon, düzenleme, denetim ve araştırma faaliyetlerini yürütmektedir.
- 2005: ABD'de, FAA tarafından, Havacılık Emniyeti Bilgi Analizi ve Paylaşımı (ASIAS) sistemi oluşturulmuştur. ASIAS, havacılık emniyeti çeşitli kaynaklardan gelen havacılık emniyeti ile ilgili verileri toplamak, analiz etmek ve paylaşmak için bir sistemdir. ASIAS, havacılık emniyeti ile ilgili eğilimleri, kalıpları ve riskleri belirlemek ve bu riskleri azaltmak için stratejiler geliştirmek için kullanılmaktadır.
- 2006: Uluslararası Sivil Havacılık Örgütü (ICAO), havacılık emniyeti ile ilgili uluslararası standartları ve tavsiyeleri içeren Ek19'u yayınlamıştır. Bu ek, havacılık emniyeti yönetimi ile ilgili bir rehber sunmaktadır. Havacılık emniyeti yönetimi, havacılık emniyeti sürekli olarak izlemek, değerlendirmek ve iyileştirmek için bir yönetim sistemi olarak tanımlanmaktadır.
- 2009: ABD'de, FAA tarafından, Havacılık Emniyeti Eylem Programı (ASAP) genişletilmiştir. ASAP, havacılık endüstrisindeki çalışanların, gönüllü ve gizli bir şekilde, havacılık emniyetini etkileyebilecek herhangi bir olay veya durumu raporlamalarını sağlayan bir sistemdir. ASAP, havacılık emniyeti ile ilgili veri toplamak, analiz etmek ve yaymak için kullanılmaktadır. ASAP, daha önce sadece pilotlar için geçerli iken, bu yıldan itibaren, uçuş görevlileri, bakım teknisyenleri,

hava trafik kontrolörleri ve diğer havacılık çalışanları için de geçerli hale getirilmiştir.

- 2010: Avrupa'da, EASA tarafından, Avrupa Havacılık Emniyeti Programı (EASP) yayınlanmıştır. EASP, Avrupa'daki havacılık emniyeti seviyesini yükseltmek ve uyumlu hale getirmek için bir programdır. EASP, havacılık emniyeti ile ilgili politika, strateji, hedef, eylem ve gösterge belirlemektedir.
- 2013: ABD'de, FAA tarafından, Havacılık Emniyeti Eylem Takımı (CAST) genişletilmiştir. CAST, havacılık endüstrisindeki çeşitli paydaşların, havacılık kazalarını ve can kayıplarını azaltmak için birlikte çalışmalarını sağlayan bir takımdır. CAST, havacılık kazalarının nedenlerini analiz etmek, riskleri değerlendirmek ve bu riskleri azaltmak için çözümler geliştirmek ve uygulamak için veri odaklı bir yaklaşım benimsemektedir. CAST, daha önce sadece ticari havacılık için geçerli iken, bu yıldan itibaren, genel havacılık için de geçerli hale getirilmiştir.
- 2017: Uluslararası Sivil Havacılık Örgütü (ICAO), havacılık emniyeti ile ilgili uluslararası standartları ve tavsiyeleri içeren Ek19'u güncellemiştir. Bu ek, havacılık emniyeti yönetimi ile ilgili bir rehber sunmaktadır. Havacılık emniyeti yönetimi, havacılık emniyetini sürekli olarak izlemek, değerlendirmek ve iyileştirmek için bir yönetim sistemi olarak tanımlanmaktadır. Bu ek, havacılık emniyeti yönetimi ile ilgili yeni gereklilikler ve tavsiyeler içermektedir. Örneğin, bu ek, havacılık emniyeti yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve iyileştirilmesi için bir çerçeve sunmaktadır.
- 2018: Avrupa'da, EASA tarafından, Avrupa Havacılık Emniyeti Programı (EASP) güncellenmiştir. EASP, Avrupa'daki havacılık emniyeti seviyesini yükseltmek ve uyumlu hale getirmek için bir programdır. EASP, havacılık emniyeti ile ilgili politika, strateji, hedef, eylem ve gösterge belirlemektedir. Örneğin, bu program, havacılık emniyeti ile ilgili veri toplama, analiz, paylaşım, eğitim ve iş birliği faaliyetlerini desteklemektedir.
- 2019: ABD'de, FAA tarafından, Havacılık Emniyeti Eylem Takımı (CAST) genişletilmiştir. CAST, havacılık endüstrisindeki çeşitli

paydaşların, havacılık kazalarını ve can kayıplarını azaltmak için birlikte çalışmalarını sağlayan bir takımdır. CAST, havacılık kazalarının nedenlerini analiz etmek, riskleri değerlendirmek ve bu riskleri azaltmak için çözümler geliştirmek ve uygulamak için veri odaklı bir yaklaşım benimsemektedir. CAST, daha önce sadece ticari ve genel havacılık için geçerli iken, bu yıldan itibaren, insansız hava araçları için de geçerli hale getirilmiştir.

2.2. HAVACILIK EMNİYETİ ÜZERİNE TARİHSEL BAKIŞ: SİVİL VE ASKERİ UÇAK KAZALARI

2.2.1. Sivil Havacılık Kazaları

Tenerife Havaalanı Felaketi (1977): Kaza Detayları: İki Boeing 747 uçağı Los Rodeos Havaalanı'nda sis nedeniyle görüş mesafesinin düşük olmasının ve yanlış anlaşılan komutların sonucunda pistte çarpışmıştır.

Sonuçlar ve Etkiler: Bu kaza, uluslararası havacılıkta iletişim standartlarının ve hava trafik denetim prosedürlerinin önemli ölçüde gözden geçirilmesine ve geliştirilmesine yol açmıştır. Ayrıca, havaalanı tasarımı ve acil durum protokollerinin de yeniden değerlendirilmesini tetiklemiştir [46].

Japan Airlines Uçuş 123 (1985): Kaza Detayları: Boeing 747'nin Tokyo'dan Osaka'ya seyahati sırasında, arka basınç bölmesinin patlaması sonucu oluşan yapısal hasar nedeniyle dağlık bir alana düşmüştür.

Sonuçlar ve Etkiler: Bu trajedi, uçak bakım prosedürlerinin ve yapısal bütünlüğün denetim mekanizmalarının gözden geçirilmesine sebep olmuştur. Ayrıca, uçak tamiratı sırasında yapılan hataların önemini ve bu hataların uzun vadeli etkilerini ortaya koymuştur.

Challenger Uzay Mekiği Faciası (1986): Kaza Detayları: Challenger uzay mekiğinin kalkıştan kısa bir süre sonra, düşük sıcaklık koşulları nedeniyle başarısız olan O-ring contaları sebebiyle patlamıştır.

Sonuçlar ve Etkiler: Bu kaza, NASA (İng. National Aeronautics and Space Administration) 'nın emniyet kültürü ve prosedürleri üzerinde derin bir etki yaratarak uzay mekiği programının tasarım, test ve işletme süreçlerinde önemli değişikliklere yol açmıştır.

Charkhi Dadri Çarpışması (1996): Kaza Detayları: Suudi Arabistan Havayolları ve Kazakistan Havayolları'na ait iki uçağın Hindistan'da havada çarpışmıştır.

Sonuçlar ve Etkiler: Bu kaza, uluslararası pilotlar için İngilizce dil becerilerinin standardizasyonunu ve hava trafik denetim prosedürlerinin iyileştirilmesini gündeme getirmiştir.

Air France Uçuş 447 (2009): Kaza Detayları: Airbus A330 tipi uçak, Atlantik Okyanusu üzerindeki uçuşu sırasında, hız ölçerlerinin donması ve ardından pilot hataları nedeniyle düşmüştür.
Sonuçlar ve Etkiler: Bu olay, pilot eğitiminin önemini ve özellikle uçuş sırasında otomatik sistemlerle etkileşim konusunda daha fazla vurgu yapılmasının gerekliliğini vurgulamıştır.

Malaysia Airlines Uçuş 370 (2014): Kaza Detayları: Boeing 777 tipi uçak Kuala Lumpur'dan Pekin'e giderken kaybolmuştur.

Sonuçlar ve Etkiler: Bu gizemli olay, uluslararası uçak izleme sistemlerinin ve acil durum yanıt protokollerinin geliştirilmesine büyük bir ivme kazandırmıştır.

2.2.2 Askeri Uçak Kazaları

1982 Falkland Savaşı Harrier Kazaları: Kaza Detayları: Kötü hava koşulları ve zorlu savaş şartları altında birden fazla Harrier jetinin kaybedilmiştir.

Sonuçlar ve Etkiler: Bu olaylar, çatışma bölgelerindeki uçuş güvenliği prosedürlerinin ve pilot eğitimlerinin önemini gösterdi.

1994 Black Hawk Vurulması (Irak): Kaza Detayları: İki ABD Black Hawk helikopteri, yanlışlıkla ABD jetleri tarafından vurulmuştur.

Sonuçlar ve Etkiler: Bu trajedi, dost-düşman tanıma (IFF) sistemlerinin geliştirilmesi ve askeri operasyonlarda iletişim protokollerinin yeniden gözden geçirilmesine yol açmıştır.

2000 Concorde Uçak Kazası (Paris, Fransa): Kaza Detayları: Air France şirketine ait Concorde uçağı, Paris'ten New York'a hareket etmeye hazırlanırken kalkıştan kısa bir süre sonra düşmüştür. Kazanın nedeni, kalkış sırasında pistte bulunan metal bir parçanın uçağın bir lastiğini patlatması ve bu parçanın yakıt tankına zarar vermesi olarak belirlenmiştir. Bu olay, yakıt tankından sızan yakıtın alev almasına ve uçağın denetiminin kaybedilmesine sebep olmuştur [47].

Sonuçlar ve Etkiler: Kazanın ardından yapılan detaylı incelemeler, Concorde uçağının tasarımındaki zayıf noktaları ve risk faktörlerini ortaya çıkarmıştır. Özellikle, yakıt tanklarının yetersiz korunması ve lastiklerin parçalanmaya karşı dirençli olmaması gibi sorunlar dikkat çekmiştir. Bu trajik kaza, havaalanı pist güvenliği ve uçak yakıt tankı koruması gibi alanlarda emniyet standartlarının yeniden değerlendirilmesine yol açmış ve havacılık endüstrisinde emniyet bilincinin artırılmasına önemli ölçüde katkıda bulunmuştur.

2002 Hainan Adası EP-3 Olayı (Çin): Kaza Detayları: ABD Donanmasına ait bir EP-3 keşif uçağı, Çin hava kuvvetleri tarafından engellenmiş ve acil iniş yapmaya zorlanmıştır.

Sonuçlar ve Etkiler: Bu olay, uluslararası hava sahasında askeri etkileşimlerle ilgili protokollerin ve prosedürlerin gözden geçirilmesini teşvik etmiştir.

2008 B-2 Spirit Kazası (Guam): Kaza Detayları: B-2 Spirit bombardıman uçağının sensör hataları ve bakım protokollerinin yetersizliği nedeniyle düşmüştür.

Sonuçlar ve Etkiler: Bu kaza, askeri uçaklar için daha kapsamlı bakım ve denetim prosedürlerinin geliştirilmesine katkı sağlamıştır.

2018 F-35B Kazası (ABD): Kaza Detayları: F-35B'nin eğitim sırasında düşmesi, malzeme yorgunluğu ve tasarım hatalarını ortaya çıkarmıştır.

Sonuçlar ve Etkiler: Bu kaza, beşinci nesil avcı uçaklarının tasarım ve bakım süreçlerinde önemli değişikliklere yol açmıştır.

2.3. TEMEL KAVRAMLAR

2.3.1. Emniyet ve Güvenlik

"Emniyet" ve "Güvenlik" kavramları, özellikle uçak tasarımı gibi hassas ve teknik alanlarda sıklıkla birbirinin yerine kullanılsa da aslında farklı anlamlara sahiptir. Bu iki terimi karşılaştırmalı olarak açıklamak, uçak tasarım aşamalarında model tabanlı emniyet analizi süreçlerini anlamak için önemlidir.

2.3.1.1. Emniyet

Emniyet (İng. safety), havacılık endüstrisinde, hava araçlarının tasarımı ve işletimi sırasında oluşabilecek beklenmedik olayların ve kazaların önlenmesini hedefleyen bir kavramdır. Bu kavram, sadece reaktif bir yaklaşımdan ziyade, proaktif bir güvenlik kültürünü ve sürekli iyileştirme anlayışını temsil etmektedir. Emniyetin önemi, havacılık sektörünün doğasında yatar; zira bu alanda meydana gelebilecek herhangi bir aksaklık veya kaza, genellikle ciddi sonuçlara ve hatta can kayıplarına yol açabilir. Emniyet, bir sistemin, beklenmeyen veya istenmeyen durumlar sırasında insanlara, çevreye veya sisteme zarar verme olasılığının minimize edilmesidir. 2006 yılında Uluslararası Sivil Havacılık Örgütü ICAO, emniyetin modern bir tanımını yapmıştır. Bu tanıma göre emniyet; “kişiye veya mülke zarar verme ihtimalinin kabul edilebilir

seviyede veya altında tutulduğu ve sürekli olarak tehlike tanımlama ve emniyet risk yönetiminin işletildiği durumdur" [48].

Havacılıkta emniyet, uçuş sırasında ve yerdeki operasyonlar sırasında sırasında riskleri azaltmayı hedefler. SAE ARP 4761 ve MIL-STD 882'ye göre emniyet tanımları aşağıda yer almaktadır.

- SAE ARP 4761' e göre emniyet: Emniyet, kişilere veya mülkiyete zarar verme riskinin, tehlike tanımlama ve risk yönetimi sürekli bir süreç aracılığıyla kabul edilebilir bir seviyeye indirilmesi ve bu seviyede tutulması durumu veya koşulu olarak tanımlanmaktadır [25].
- MIL-STD-882E'ye göre emniyet: Ekipman veya mülkün zarar görmesi, çevreye zarar verilmesi gibi koşullara yol açabilecek ölüm, yaralanma, meslek hastalığı gibi durumların olmaması durumu [27].
- Odak Noktası: Emniyet, genellikle teknik arızalar, tasarım hataları, işletme hataları veya doğal nedenler gibi kazara veya rastgele olaylara odaklanır.
- Uygulama Alanları: Emniyet, uçak tasarımı, bakım prosedürleri, operasyonel prosedürler ve pilot eğitimi gibi alanlarda risk analizi ve yönetimi ile ilgilidir.
- Örnekler: Emniyet tedbirleri arasında arıza toleranslı sistem tasarımı, acil durum prosedürleri, emniyet kritik sistemlerin test edilmesi ve bakım standartlarının belirlenmesi yer alır.

2.3.1.2. Güvenlik

Güvenlik (İng. security), havacılık endüstrisinde, hava yolcu ve yük taşımacılığının güvenli bir şekilde gerçekleştirilmesini sağlamak amacıyla uygulanan prosedürler ve tedbirler bütünüdür. Bu kavram, sadece meydana gelen güvenlik ihlallerine tepki göstermekten öte, potansiyel tehditleri önceden belirleyerek önlemeye yönelik proaktif bir yaklaşımı ifade eder. Güvenliğin hayati önemi, havacılık sektörünün sadece teknik operasyonlarını değil, aynı zamanda uluslararası terörizm ve suçla mücadele gibi geniş bir spektrumu kapsamasından kaynaklanır.

- Tanım: Güvenlik (İng. security), uçağın ve onunla ilişkili sistemlerin kasıtlı zararlı eylemlere karşı korunmasını ifade eder. Bu, siber saldırılara, terörizme ve diğer kasıtlı tehditlere karşı koruma anlamına gelir [49].
- Odak Noktası: Güvenlik, kasıtlı zararlı eylemlere karşı koruma sürecidir. Bu, sabotaj, terörizm, casusluk veya siber saldırılar gibi kasıtlı tehditlere karşı önlemleri içerir.
- Uygulama Alanları: Güvenlik, uçakların iletişim sistemleri, siber güvenlik, havaalanı güvenlik protokolleri ve yolcu tarama süreçlerini içerir.
- Örnekler: Güvenlik önlemleri arasında uçaklara yetkisiz erişimi önleme, siber güvenlik duvarları, personel güvenlik denetimleri ve havaalanı güvenlik taramaları bulunur.

2.3.1.3. Emniyet ve Güvenlik Karşılaştırması

- Odak: Emniyet, kazaları ve arızaları önlemeye odaklanırken, güvenlik kasıtlı zararlı eylemlere karşı korumaya odaklanmaktadır.
- Yaklaşım: Emniyet, tasarım ve operasyonel süreçlerde riskleri azaltmayı hedeflerken, güvenlik, tehditlere karşı savunma mekanizmaları geliştirmeyi hedeflemektedir.
- Uygulama: Emniyet, genellikle sistemsel bir yaklaşım gerektirir ve tasarım aşamasından itibaren entegre edilir. Güvenlik ise sürekli bir tehdit değerlendirmesi ve güncellenen güvenlik önlemleri gerektirmektedir.

2.3.2. Risk

Risk, belirsiz bir olayın gerçekleşmesi durumunda ortaya çıkabilecek olumsuz sonuçların bir kombinasyonu olup genellikle iki ana bileşenden oluşur [25, 27].

1. Olasılık: Bir olayın gerçekleşme ihtimali. Bu, bir olayın ne kadar sık meydana geldiği veya gelecekte meydana gelme ihtimali ile ilgilidir.

2. Şiddet: Eğer olay gerçekleşirse, ortaya çıkacak sonuçların ciddiyeti veya etkisi olarak tanımlanır. Bu, olayın sonuçlarının ne kadar zararlı veya ciddi olduğunu ifade eder.

SAE ARP 4761 ve MIL-STD 882'ye göre emniyet tanımları aşağıda yer almaktadır.

- ARP 4761'e göre risk: Bir tehlikenin gerçekleşme olasılığı ile bu tehlikenin yol açabileceği zararın şiddetinin birleşimi olarak değerlendirilir. Risk değerlendirmesi, hem olasılığı hem de sonuçları göz önünde bulundurarak yapılır [25].
- MIL-STD-882E'ye göre risk: Ön görülen tehlikeye ait kritiklik ve olasılığın kombinasyonudur. Risk yönetimi, bu riskleri azaltma veya kabul edilebilir seviyelere indirme süreçlerini içerir [27].

2.3.3. Tehlike

Tehlike, potansiyel bir zarar veya istenmeyen sonucun kaynağı olarak tanımlanabilir. Havacılık endüstrisinde, tehlike; uçuş emniyeti, yolcu emniyeti veya araç bütünlüğü için olası riskler oluşturan herhangi bir durum veya koşul olarak değerlendirilir. Tehlike, doğrudan bir kaza veya olaya yol açabilecek unsurlar içerir ve bu nedenle tespit edilmesi, analiz edilmesi ve yönetilmesi gereklidir [25, 27].

Havacılık sektöründe, bu tehlikeler genellikle uçuş emniyetini tehdit eden unsurlar olarak karşımıza çıkar. Hava araçları kapsamında başlıca tehlike türlerini şu şekilde sıralayabiliriz:

1. Mekanik Arızalar: Uçağın kritik bileşenlerinde (motorlar, kontrol sistemleri, hidrolik sistemler vb.) meydana gelen arızalar. Örneğin, bir motorun arızalanması veya hidrolik sistemlerdeki bir sızıntı, uçuş sırasında ciddi riskler oluşturabilir.
2. Hava Koşulları: Şiddetli hava koşulları (türbülans, fırtına, buzlanma vb.) uçuş emniyetini doğrudan etkileyen doğal tehlikelerdir. Örneğin, ani

hava değişimleri uçağın kontrolünü zorlaştırabilir veya görüş mesafesini düşürebilir.

3. İnsani Faktörler: Pilot hatası, ekipmanların yanlış kullanımı veya bakım ekiplerinin hataları gibi insan kaynaklı hatalar. Bu tür hatalar, yanlış kararlar veya dikkatsizlik sonucu meydana gelebilir.
4. Operasyonel Sorunlar: Hava trafik denetim hataları, yanlış rota planlaması veya acil durum yönetimi eksiklikleri gibi operasyonel faktörler de tehlike oluşturabilir.

SAE ARP4761 ve MIL-STD-882'ye göre tehlike tanımları aşağıda yer almaktadır.

- ARP4761: Tehlike, bir hava aracı sisteminin potansiyel olarak zararlı bir durum veya koşul oluşturabilecek özelliği olarak tanımlanır. Tehlikeler, sistem arızaları, operasyonel hatalar veya dış etkenlerden kaynaklanabilir [25].
- MIL-STD-882E: Tehlike, bir sistemin veya bileşenin işletilmesi sırasında yaralanma, ölüm, ekipman hasarı veya çevresel zarara yol açabilecek potansiyel bir durum olarak tanımlanır [27].

2.4. EMNİYETLİ SİSTEM GELİŞTİRME: HAVACILIK VE SAVUNMA SEKTÖRLERİNDE STANDARTLAR VE YÖNERGELER

Havacılık ve savunma endüstrileri, yüksek riskler barındıran ve karmaşık sistemlerin geliştirilmesi ve işletilmesini gerektiren sektörlerdir. Bu sektörlerde emniyet, sadece işletme maliyetlerini azaltmak ve düzenleyici uyumu sağlamakla kalmaz, aynı zamanda insan hayatını korumak ve mal kaybını önlemek için de kritik öneme sahiptir. Sistem emniyeti, bir sistemin beklenen işlevlerini kabul edilebilir risk seviyeleri içinde yerine getirme yeteneği olarak tanımlanır. Bu, potansiyel tehlikelerin tanımlanması, değerlendirilmesi ve azaltılması yoluyla gerçekleştirilir.

Emniyetli sistem geliştirme süreci, bir dizi standart ve kılavuz doküman tarafından desteklenir. Bu dokümanlar, SAE ARP4754A, SAE ARP4761, RTCA DO178B, RTCA DO254 ve MIL-STD-882E, sektördeki en iyi uygulamaları ve yöntemleri belirler. Bu standartlar, hem sivil hem de askeri uygulamalar için emniyetli sistem

geliştirme süreçlerini tanımlar ve bu süreçlerin uygulanmasında kritik bir rol oynamaktadır.

2.4.1. SAE ARP4754A: Sivil Havacılık Sistemlerinin Geliştirilmesi İçin Kılavuzlar

SAE ARP4754A, sivil havacılık sistemleri ve bileşenlerinin geliştirilmesi için kapsamlı bir çerçeve sunmaktadır [26]. Bu standart, sistem geliştirme sürecinin her aşamasında emniyeti entegre etmeyi amaçlar ve bu süreçlerin, donanım ve yazılım geliştirmedeki amaçları destekleyen RTCA DO178 ve DO254 standartları ile uyumlu olmasını sağlamaktadır.

SAE ARP4754A'nın temel amacı, sistem geliştirme sürecinde emniyetin sistem tasarımının her aşamasına entegre edilmesini sağlamaktır. Bu, hava araçlarının ve bileşenlerinin tasarım ve geliştirme sürecinde ortaya çıkabilecek riskleri azaltmayı ve böylece hava araçlarının emniyetli bir şekilde işletilmesini sağlamayı hedeflemektedir.

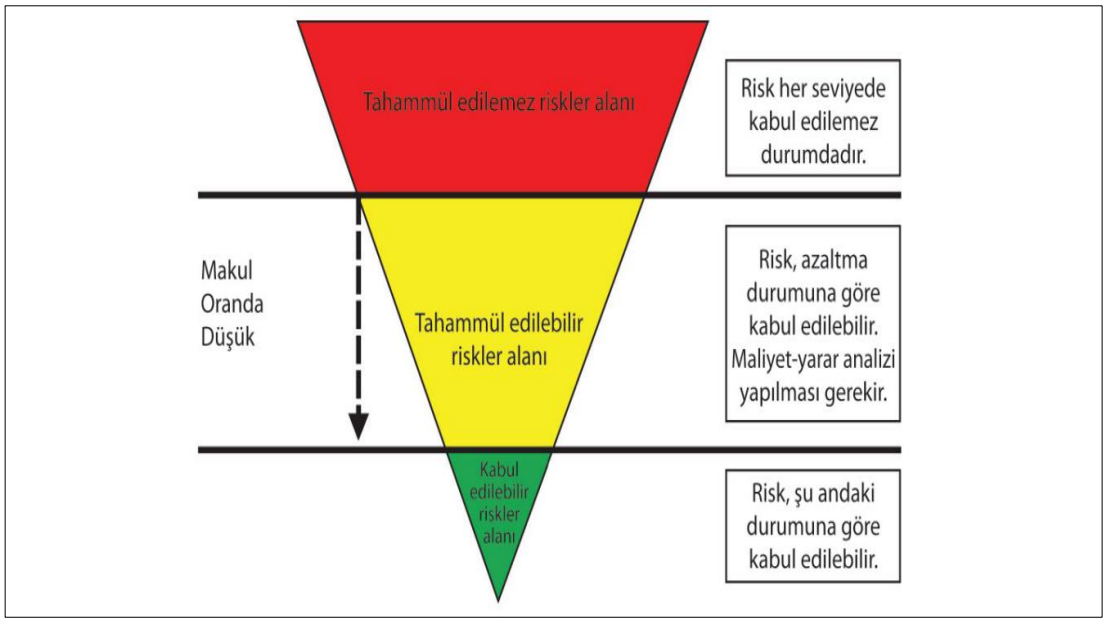
Sistem Geliştirme Sürecinin Aşamaları

1. Gereksinim Analizi: Projeye başlarken, sistem gereksinimlerinin belirlenmesi ve analiz edilmesi gerekmektedir. Bu aşama, sistemin ne yapması gerektiğini tanımlar.
2. Tasarım: Gereksinimler belirlendikten sonra, bu gereksinimleri karşılayacak sistem tasarımı yapılır. Tasarım aşaması, hem donanım hem de yazılım bileşenlerini kapsar.
3. Doğrulama ve Validasyon: Tasarlanan sistem veya bileşenlerin, belirlenen gereksinimleri karşılayıp karşılamadığı test edilir. Bu süreç, hem tasarımın doğruluğunu hem de emniyet gereksinimlerinin karşılanıp karşılanmadığını değerlendirir.
4. Emniyet Analizi: Sistem tasarımı sırasında ve sonrasında, potansiyel emniyet risklerinin analizi yapılır. Bu analiz, sistemdeki muhtemel hataların ve arızaların belirlenmesi ve değerlendirilmesi için kritiktir.

2.4.2.MIL-STD-882E: Askeri/ Savunma Sektöründe Sistem Emniyeti

MIL-STD-882E, ABD Savunma Bakanlığı tarafından geliştirilmiş bir emniyet standardıdır [25]. Bu standart, askeri ekipman ve tesislerin emniyet analizleri için gereklilikleri ve yönergeleri kapsar. Burada 'emniyet', askeri sistemlerin, ekipmanın ve tesislerin tasarımı, üretimi ve işletimi sırasında insan hayatını ve sağlığını koruma, mal kaybını önleme ve misyonun etkin bir şekilde yerine getirilmesini sağlama yeteneği olarak tanımlanır. MIL-STD-882E, özellikle risk yönetimi ve tehlike analizi konularında derinlemesine yönergeler sunmaktadır.

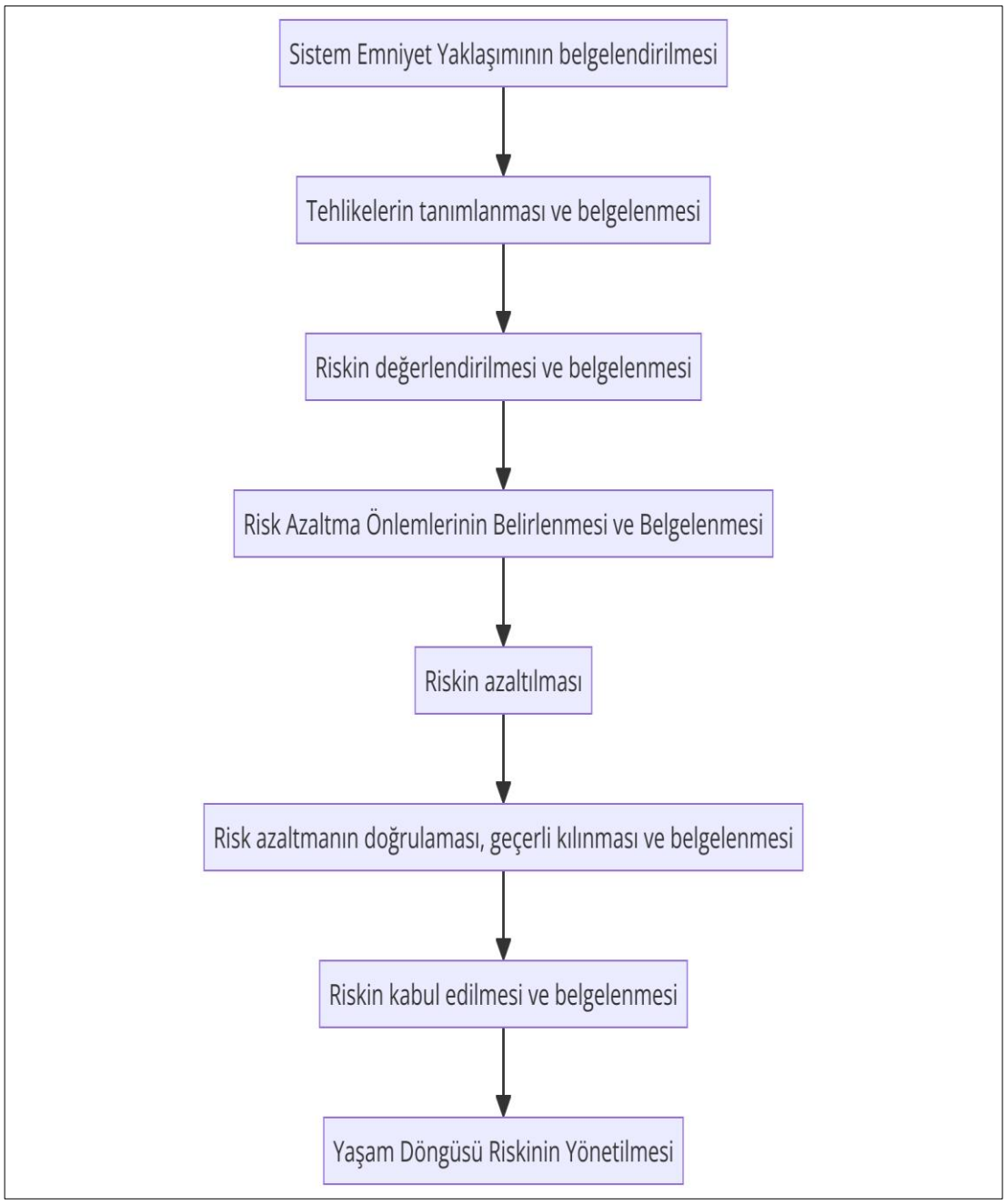
Risk azaltma süreçleri, tehlikelerin sonuçlarının büyüklüğüne göre şekillenmektedir. "Eğer ölçülmezse yönetilemez" mantığıyla, tehlike sonuçlarının öneminin belirlenmesi için ölçme faaliyetleri kritik önem taşımaktadır.



Şekil 2.1. Emniyet riski yönetiminde risk alanları.

Şekil 2.1 üzerinde emniyet riski yönetiminde kabul edilebilir ve edilemez türdeki risklerin alanları belirtilmiştir. Havacılık kuruluşlarının çevrelerinde bulunan emniyet risklerini kabul edilebilir alanda tutabilmek için ya tehlikenin sonuçlarının hasar verme olasılığını düşürmesi ya da bu mümkün değilse ilgili faaliyeti iptal etmesi gerekmektedir. MIL-STD-882E askerî standardı, tehlike analizi, risk değerlendirme ve

risk azaltma stratejilerinin uygulanmasını içeren ayrıntılı yönergeler sunmaktadır. Bu standart, Şekil 2.2 üzerinde yer alan sekiz temel adımı içermektedir.



Şekil 2.2. Sistem emniyeti sürecinin sekiz adımı.

Sistem Emniyet Yaklaşımının Belgelendirilmesi

Sistem mühendisliği içerisinde yer alan sistem emniyeti yaklaşımı, tehlikelerin yönetilmesi amacıyla aşağıdaki temel unsurları içerir:

- Sistem düzeyinde belirlenen emniyet hedefleri
- Uçak düzeyindeki emniyet hedefleri
- Proje için belirlenen emniyet gereksinimleri
- Tehlikeleri yönetme sürecinde kullanılacak analiz yöntemleri
- Risk yönetimi faaliyetlerinin kapsamı.

Tehlikelerin Tanımlanması ve Belgelenmesi

Tehlikelerin sistematik bir analiz yöntemiyle tanımlanması, donanım, yazılım, sistem arayüzleri, insan kaynaklı hatalar, çevresel ve operasyonel faktörler gibi çeşitli unsurların kapsamlı bir şekilde incelenmesini gerektirir. Bu süreçte, kullanıcıların bilgi, beceri ve yeteneklerinin yanı sıra, geçmişteki benzer sistemlerden edinilen tecrübeler de dikkate alınır. Tehlikelerin belirlenmesi için Fonksiyonel Tehlike Analizi, Hata Modu ve Etkileri Analizi, Özel Risk Analizi, Bölgesel Emniyet Analizi, Ortak Neden Analizi gibi yöntemler ve test sonuçları etkili araçlar olarak kullanılabilir. Ayrıca, tehlikeleri tanımlama sürecinde beyin fırtınası, standartlar ve prosedürlerin gözden geçirilmesi, uzman görüşleri ve anketler, tehlike raporlama sistemleri gibi çeşitli metotlar kullanılır.

Riskin Değerlendirilmesi ve Belgelenmesi

Potansiyel kazaların kritiklik ve olasılık dereceleri, her tehlike için Çizelge 2.1 ve Çizelge 2.2 ile belirtilen kriterlere göre incelenir. Bu inceleme sonucunda, tehlikenin etkileri, en uygun sınıflandırma seviyesine göre kategorize edilir.

Çizelge 2.1. Şiddet kategorisi [27].

Tanim	Seviye Kategorisi	Tehlike Sonuç Kriterleri
Ölümcül	1	Aşağıdakilerden bir veya daha fazlasına neden olabilir: • Ölüm, • Kalıcı tam sakatlık, • Geri dönüşü olmayan önemli çevresel etki, • 10 milyon ABD dolarına eşit veya daha fazla kayıp.
Kritik	2	• Kalıcı kısmi sakatlık, • En az üç personelin hastaneye kaldırılmasıyla sonuçlanabilecek • Yaralanma veya meslek hastalığı, • Geri dönüşümlü önemli çevresel etki, • 1 milyon ABD dolarına eşit veya bu tutarı aşan ancak 10 milyon ABD dolarından az parasal kayıp.
Marjinal	3	• Bir veya daha fazla iş gününün kaybedilmesine neden olan yaralanma veya mesleki hastalık, • Tersine çevrilebilir orta düzeyde çevresel etki, • Veya 100.000 ABD dolarına eşit veya bu tutarı aşan ancak 1 Milyon ABD dolarından az parasal kayıp.
Önemsiz	4	• İş günü kaybıyla sonuçlanmayan yaralanma veya mesleki hastalık, • Minimum çevresel etki, • Veya parasal kaybın 100.000 dolardan az olması.

Çizelge 2.1 üzerindeki uygun kısımlara, potansiyel kazaların olasılıkları yerleştirilir. Sayısal bir değer elde edilemiyorsa, olasılık seviyelerinin açıklamaları kullanılarak değerlendirme yapılmalıdır. Bir tehlikenin bir saatlik uçuş sürecinde meydana gelme ihtimali, risk değerlendirme sürecinde önemlidir ve bu, projenin emniyet amaçları doğrultusunda belirlenir. Örnek vermek gerekirse, Çizelge 3 ile verilen kategorilere göre uçak kaybı riski için, 100.000 uçuş saatine düşen tehlike olasılığının 0,1 ile 1 arasında olması kabul edilir, bu da riskin 10^{-5} ile 10^{-6} olasılık değerleri arasında bir yerde olduğunu gösterir.

Çizelge 2.2. Olasılık seviyesi [27].

Tanım	Seviye	Belirli Bireysel Öğe	Filo veya Envanter
Sık Sık	A	Ürünün yaşam süresi boyunca sıklıkla meydana gelecektir.	Sürekli olarak deneyimlenir.
Olası	B	Ürünün yaşam süresi boyunca birkaç kez meydana gelecektir.	Sıklıkla meydana gelecektir.
Rastgele	C	Ürünün yaşam süresi boyunca bazen meydana gelecektir.	Birkaç kez meydana gelecektir.
Pek Az	D	Ürünün yaşam süresi boyunca olası olmasa da, meydana gelmesi mümkündür.	Düşük ihtimalle de olsa, makul olarak beklenen bir durumdur
Olası Olmayan	E	Öylesine düşük bir ihtimal ki, ürünün yaşam süresi boyunca meydana gelmeyeceği varsayılabilir.	Olası bir şey olmamasına rağmen mümkün durumdur.
Elenmiş	F	Meydana gelme ihtimali olmayan. Bu seviye, potansiyel tehlikeler belirlendikten ve daha sonra ortadan kaldırıldıktan sonra kullanılır.	"Meydana gelme ihtimali olmayan. Bu seviye, potansiyel tehlikelerin belirlenip daha sonra ortadan kaldırıldığı durumlar için kullanılır.

Çizelge 2.3. Uçuş saatine göre tehlike olasığı sayısal sınırları [23].

Tanım	Frekans (100k Uçuş Saatinde)	Olasılık
Sık Sık	$100 < F$	$10^{-3} < P$
Olası	$100 \leq F < 10$	$10^{-4} < P \leq 10^{-3}$
Rastgele	$10 \leq F < 1.0$	$10^{-5} < P \leq 10^{-4}$
Pek Az	$1.0 \leq F < 0.1$	$10^{-6} < P \leq 10^{-5}$
Olası Olmayan	$0.1 \leq F$	$P \leq 10^{-6}$

İncelenen riskler, kritiklik ve olasılık seviyelerinin birleşiminden oluşan Risk Değerlendirme Kodu (Ing. Risk Assessment Code, RAC) ile tanımlanır. Çizelge 2.4 ile belirtildiği gibi, 2C için Risk Değerlendirme Kodu (RAC); "CİDDİ" kritiklik ve "RASTGELE" olasılık seviyelerinin bir araya gelmesinden oluşmaktadır. Örnek risk değerlendirme matrisi Çizelge 2.5 ile verilmiştir.

Çizelge 2.4. Risk değerlendirme matrisi [27].

	ÖLÜMCÜL	KRİTİK	MARJİNAL	ÖNEMSİZ
SIK SIK	YÜKSEK	YÜKSEK	CİDDİ	ORTA
OLASI	YÜKSEK	YÜKSEK	CİDDİ	ORTA
RASGELE	YÜKSEK	CİDDİ	ORTA	DÜŞÜK
PEK AZ	CİDDİ	ORTA	ORTA	DÜŞÜK
OLASI OLMAYAN	ORTA	ORTA	ORTA	DÜŞÜK
ELENMİŞ	ELENMİŞ			

Çizelge 2.5. Örnek risk değerlendirme matrisi [28].

RİSK DEĞERLENDİRME TABLOSU				
	ÖLÜMCÜL	KRİTİK	MARJİNAL	ÖNEMSİZ
SIK SIK	1	3	7	13
OLASI	2	5	9	16
RASGELE	4	6	11	18
PEK AZ	8	10	14	19
OLASI OLMAYAN	12	15	17	20

Çizelge 2.6 ile birlikte örnek risk çizelgesi verilmiştir.

Çizelge 2.6. Örnek risk değerlendirme çizelgesi [28].

KAZA (MISHAP) RİSK DEĞERLENDİRMESİ DEĞERİ	KAZA RİSK KATEGORİSİ
1-5	YÜKSEK
6-9	CİDDİ
10-17	ORTA
18-20	DÜŞÜK

Risk Azaltma Önlemlerinin Belirlenmesi ve Belgelenmesi

Öncelikle, tehlikeleri mümkün olan en üst düzeyde ortadan kaldırmak hedeflenmelidir. Eğer bu mümkün değilse, risklerin asgari seviyeye çekilmesi gerekmektedir. Bu süreç, maliyet, zaman ve performans gibi faktörler göz önünde bulundurularak, sistem emniyetini tasarım aşamasında öncelikler belirlenerek gerçekleştirilmelidir. Sistem emniyeti tasarımındaki bu öncelikler, çeşitli azaltma yöntemlerini tanımlar ve bunları etkinliklerine göre sıralar, böylece risk azaltma işlemi sağlanır. Kısacası, riski azaltma stratejileri aşağıdaki gibidir:

- Riski ortadan kaldırmak amacıyla tasarımın yeniden yapılması
- Tasarımın yeniden düzenlenerek riskin tehlike düzeyinin azaltılması
- İlave azaltma önlemlerinin alınması
- İzleme ve alarm sistemlerinin kurulması
- İşlem prosedürlerinin iyileştirilmesi ve eğitimlerin verilmesi
- Uyarı işaretleri ve notlar ekleyerek riskin asgari düzeye çekilmesi.

Riskin Azaltılması

Azaltma stratejileri, risk seviyelerini kabul edilebilir bir düzeye indirmek amacıyla seçilip uygulanmaktadır. Sistem Emniyeti ve Entegre Ürün Takımı (İng. Integrated Product Team, IPT) içerisinde, bu stratejilerin maliyeti, uygulanabilirliği ve etkisi dikkatle incelenir. Teknik inceleme toplantılarında, karşılaşılan tehlikeler, bu

tehlikelerin şiddeti ve olasılığına dair değerlendirmeler ile riski azaltma yöntemlerinin güncel durumu ele alınmaktadır.

Risk Azaltmanın Doğrulaması, Geçerli Kılınması ve Belgelenmesi

Seçilen her bir risk azaltma tedbirinin etkililiği, uygun analiz, test, gösterim veya değerlendirme metotlarıyla kanıtlanmalıdır. Bu doğrulama süreci ve sonuçları, hata takip sistemi üzerinde kaydedilerek resmiyet kazandırılmalıdır.

Riskin Kabul Edilmesi ve Belgelenmesi

Projeye başlamadan önce, insanlar, ekipmanlar veya çevre üzerinde olumsuz etkileri olabilecek bilinen sistem tehlikelerine ilişkin riskler, Çizelge 2.7 üzerinde yer alan kategorilere göre uygun yetkililer tarafından tanımlanmalı ve onaylanmalıdır. Resmi bir risk onayı kararını destekleyen sistem yapılandırması ve ilgili belgeler, sistemin kullanım ömrü boyunca saklanmak üzere müşteri veya yetkili kuruma teslim edilmelidir.

Çizelge 2.7. Risk kabul örneği çizelgesi [28].

Kaza Risk Değerlendirme Değeri	Kaza Risk Kategorisi	Kaza Risk Kabul Seviyesi
1-5	Yüksek	Bileşen Satın Alma Yöneticisi
6-9	Ciddi	Program Yürütme Görevlisi
10-17	Orta	Program Müdürü
18-20	Düşük	Yönlendirildiği Gibi

Yaşam Döngüsü Riskinin Yönetilmesi

“Yaşam döngüsü" terimi, bir sistemin geliştirme, test, değerlendirme, kullanım, işletim ve destek gibi evrelerini ifade etmektedir. Sistem operasyonel hale geldikten sonra, sistem program ofisi, tehlikeleri belirlemek ve sistem emniyeti prosedürlerini kullanarak yaşam döngüsü boyunca hata takip sistemini yönetmek için çalışır. Bu süreç, arayüzler, kullanıcılar, donanım ve yazılım, yanlış bilgi, görevler veya profiller

ve sistem sağlık verileri gibi çeşitli faktörleri kapsar ve sadece bu örneklerle sınırlı değildir. Risk yönetimi ekibi, bu tür değişikliklerin farkında olup uygun prosedürleri, örneğin konfigürasyon denetimi sürecini, uygulayacak şekilde düzenlenmiştir. Program ofisi ve kullanıcı topluluğu arasında, ortaya çıkan yeni tehlikeleri ve riskleri tanımlayıp yönetmek üzere sürekli ve etkili bir iletişim kurulmalıdır.

2.5. SAE ARP4761: SİVİL HAVA SISTEMLERI VE EKİPMANINDA EMNİYET DEĞERLENDİRME SÜRECİNİN YÜRÜTÜLMESİNE İLİŞKİN KILAVUZ VE YÖNTEMLER

SAE ARP4761, SAE ARP4754A tarafından tanımlanan sistem geliştirme sürecine, aşağıda belirtilen emniyet değerlendirme metodolojilerini sunmaktadır.

Fonksiyonel Tehlike Analizi (İng. Fault Tree Analysis, FHA): Uçak ve Sistem seviyesinde olmak üzere çalışma gerçekleştirilebilmektedir. Genel olarak hata durumlarının belirlenmesi, bu hata durumlarına kritiklik atanması, bu hata durumlarına karşılık mürettebatın tespit yöntemleri ve uygulayacağı prosedürler belirlenmektedir.

Ön Sistem Emniyet Değerlendirmesi (Preliminary System Safety Assessment, PSSA): Tasarımın FHA çalışmasında belirlenmiş olan emniyet gereksinimleri karşılayabileceğinin öngörüldüğü çalışmadır. Hata ağacı analizleri (FTA) ile sistemin FHA'de belirlenmiş hata durumlarına ne şekilde sebebiyet verebileceği gösterilir. FTA'lar vasıtası ile alt seviye emniyet gereksinimleri (Sistem, ekipman, parça üzerine düşen) belirlenmiş olur.

Sistem Emniyet Değerlendirme Değerlendirmesi (İng. System Safety Assessment, SSA): FHA ve PSSA çalışmaları neticesinde oluşturulmuş olan emniyet gereksinimlerine sistemin uyum gösterdiği çalışmadır.

Ortak Sebep Analizleri (Common Cause Analysis, CCA): FTA analizleri ile yedeklenmiş olarak gösterilen ekipman / sistemlerin yedekliliğinin gerçekte varolduğunun gösterilmesi ve FHA'da belirlenmiş hata durumları haricinde oluşması muhtemel diğer hata durumlarının olasılıklarının kabul edilebilir seviyelerde

olduğunun gösterilmesi amacıyla hazırlanan Ortak Mod Analizi (CMA), Özel Risk Analizi (PRA) ve Bölgesel Emniyet Analizi (ZSA) çalışmalarından oluşmaktadır.

2.6. SAE ARP4761 VE MIL-STD-882E STANDARTLARI ARASINDAKİ İLİŞKİ

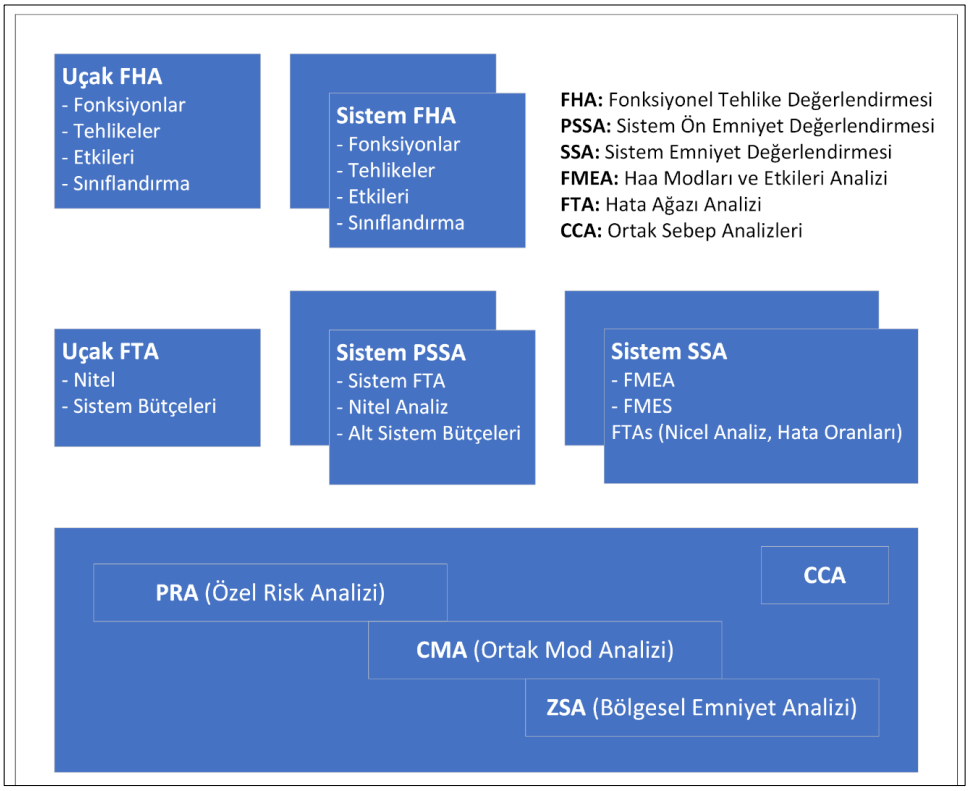
Her iki standart da, tehlikeleri belirlemek ve riskleri yönetmek için sistematik bir yaklaşım sunmakta olup her biri farklı uygulama alanlarına odaklanır: ARP4761 standardı genellikle sivil hava sistemleri ve ekipmanı için kullanılırken, MIL-STD-882 genellikle savunma sistemleri geliştirilirken göz önünde bulundurulur. Bu nedenle, hangi standardın kullanılacağına karar verirken, uygulamanın doğası ve gereksinimleri dikkate alınmalıdır. Her iki standart da, tehlikeleri belirlemek, riskleri değerlendirmek ve bu riskleri azaltmak için değerli araçlar ve yöntemler sunmaktadır.

2.7. SAE ARP4761 VE SAE ARP4754A STANDARTLARI ARASINDAKİ İLİŞKİ

SAE ARP4761 standardı, SAE ARP4754A'nın talep ettiği emniyet değerlendirmesi süreçlerini sağlamaktadır. Bu iki standart birlikte çalışarak, sistem geliştirme sürecinin her aşamasında emniyetin entegre edilmesini sağlar.

“ARP4754A bir ne yapılması gerektiği kitabıdır ve ARP4761 size bunun nasıl yapılacağına ilişkin adımları verir. Bize evet, günümüz uçaklarındaki sistem ve ekipmanların emniyetli olduğunu söyleyebilmemizi sağlayan süreç, yöntemler ve araçları sağlayan şey, önerilen bu iki uygulamanın birleşimiydi." —Eric M Peterson, Havacılık Sertifikasyonu Emniyet Uzmanı

2.8. SAE ARP4761: EMNİYET DEĞERLENDİRME YÖNTEMLERİ



Şekil 2.3. Proje geliştirme fazlarında emniyet analizlerinin yeri [25].

Uçak tasarımının kavramsal aşamasında, FHA aracılığıyla uçak seviyesindeki üst seviye emniyet gereksinimleri ve fonksiyonların kritiklik seviyeleri tespit edilmektedir. Bu aşama, tasarımın ilkelerini ve emniyet önceliklerini belirlemektedir. İlerleyen ön tasarım aşamasında, sistem seviyesinde fonksiyonlar belirlenir ve bu fonksiyonlara ait her bir sistem için ayrı ayrı FHA gerçekleştirilir. Bu değerlendirmeler, detaylı sistem emniyet gereksinimlerinin ortaya konulmasını sağlar.

Tasarlanan sistem mimarisinin ve önerilen çözümlerin emniyet gereksinimlerini ne derecede karşıladığının değerlendirilmesi, PSSA ile yapılır. PSSA, alt sistemlerin, yazılım ve donanım parçalarının kritiklik seviyelerini ve tasarımın bu evresi için gerekli emniyet gereksinimlerini belirlemektedir.

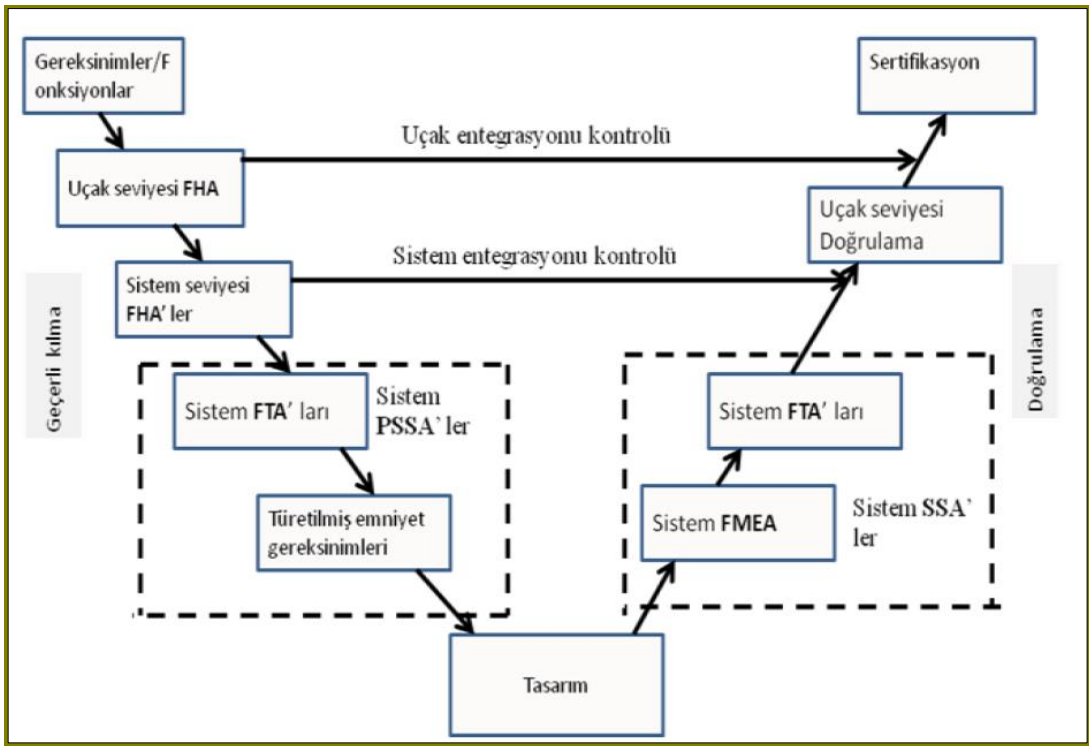
Sonrasında, SSA ile tamamlanmış sistemin emniyet gereksinimlerini karşılayıp karşılamadığı doğrulanır. SSA, temelde bir dizi doğrulama analizi olarak işlev görür ve sistemin emniyetini kanıtlar.

Projenin gelişim aşamalarına paralel olarak yürütülen sistem seviyesi emniyet analizleri, detaylı sistem emniyet gereksinimlerini (hem niteliksel hem de niceliksel emniyet hedeflerini) ve yazılım/donanımın kritiklik düzeylerini ortaya koymaktadır. Bu süreç, geliştirilen sistemin kritikliğine göre farklılık gösterir. Örneğin, Geliştirme Güvence Seviyesi (İng. Development Assurance Level, DAL) A olan kritik bir sistem için uygulanacak süreç ile DAL D olan çok daha az kritik bir sistem için izlenecek süreç ve analizler arasında önemli farklar bulunmaktadır.

Geliştirme sürecinin nasıl izleneceği, SAE ARP 4754 standardı ile belirlenmiştir. Bu standart, sistem geliştirme sürecinin genel çerçevesini ve uygulanacak emniyet yönetim süreçlerini tanımlamaktadır. Yazılım ve donanım geliştirme seviyelerine özgü süreçler ise sırasıyla RTCA-DO-178B ve RTCA-DO-254 standartları ile ifade edilmiştir. Bu standartlar, yazılım ve donanımın geliştirilmesi sırasında takip edilmesi gereken spesifik prosedürleri ve gereklilikleri içerir, böylece sistemin emniyet ve performans hedeflerine ulaşması sağlanır.

Bu bağlamda, kritiklik seviyesi yüksek olan sistemler için daha katı ve kapsamlı bir geliştirme ve doğrulama süreci gerekmektedir. DAL A seviyesindeki sistemler, can ve mal güvenliği üzerinde doğrudan etkisi olabilecek sistemler olduğundan, hata toleransları en düşük seviyede tutulmalı ve en yüksek doğrulama standartlarına tabi tutulmalıdır. Buna karşılık, DAL D gibi daha düşük bir kritiklik seviyesine sahip sistemler, daha az katı doğrulama gereksinimlerine tabidir, ancak yine de belirlenmiş standartlara uygun olarak geliştirilmelidir.

Emniyet Analizlerinin geçerli kılma-doğrulama diyagramında gösterimi Şekil 2.4 üzerinde verilmiştir.



Şekil 2.4. Emniyet analizleri V diyagramı.

2.8.1. Ön Sistem Emniyet Değerlendirmesi

PSSA, sistemin tasarım ve geliştirme aşamalarında potansiyel tehlikeleri ve bunların olası sonuçlarını önceden belirleyerek, riskleri azaltmak ve sistem emniyetini artırmak için stratejiler geliştirilmesini sağlamaktadır. PSSA sürecinde, hata modlarının ve etkilerinin analizi için hem nitel hem de nicel yöntemler kullanılır. Bu yöntemler arasında Hata Ağacı Analizi (İng. Fault Tree Analysis, FTA) ve Ortak Neden Analizi (İng. Common Cause Analysis, CCA) bulunur. FTA, FHA'daki hata durumları (FC) belirledikten sonra, her bir FC'ye neden olabilecek daha düşük seviyelerde hangi tekil hataların veya hata kombinasyonlarının (varsa) mevcut olabileceğini belirlemek için PSSA'nın bir parçası olarak uygulanabilir.

Bu analizler, sistemin emniyetini sağlamak için gereken tasarım değişikliklerini ve önlemleri belirlemek amacıyla yapılır.

PSSA sürecinde aşağıdaki çalışmalar gerçekleştirilir.

1. Emniyet Gereksinimlerinin Belirlenmesi:
    - Uçak ve sistem seviyesindeki emniyet gereksinimlerinin tam listesi oluşturulur.
    - FHA sürecinde belirlenen fonksiyonel tehlikeler temel alınarak hata koşulları tespit edilir.
2. Sistem Mimarisinin Değerlendirilmesi:
    - Önerilen mimari ve kavram (konsept) tasarımının emniyet gereksinimleri ve hedeflerini karşılayıp karşılayamayacağı değerlendirilir.
    - Sistem mimarisinin açıklaması, hata koşulları, sistem ekipmanının listesi, sistem arayüzleri ve ön CCA'lar dikkate alınır.
3. Alt Seviye Emniyet Gereksinimlerinin Türetilmesi:
    - Daha alt seviye öğeler için (donanım ve yazılım) emniyet gereksinimleri türetilir.
    - Sistem entegrasyonu ve operasyonları için emniyet gereksinimleri belirlenir.
4. Tasarım ve Mimari Kararların Değerlendirilmesi:
    - FTA veya benzeri yöntemler kullanılarak, öğe başarısızlıklarının nasıl birleştiği ve belirlenen hata koşuluna yol açtığı gösterilir.
    - Bağımsızlık iddiaları, CCA'lar ve gerekli testlerle değerlendirilir.
    - Gizli hatalar için bakım görevlerinin "Aşılmaması Gereken" aralıkları belirlenir.
5. Daha Alt Seviyedeki Öğelerin Tasarımı İçin Emniyet Gereksinimlerinin Uygulanması:
    - Sistem emniyet gereksinimlerinin, öğelere ve montaj tasarımına nasıl tahsis edileceği belirlenir.
    - Donanım ve yazılım için DAL seviyeleri ve emniyet bakım görevleri tanımlanır.

PSSA süreci, tasarım süreciyle paralel olarak ilerler ve yinelemeli bir doğaya sahiptir. Tasarım değişiklikleri veya yeni bilgiler ışığında, PSSA analizleri güncellenir ve gerektiğinde yeni emniyet önlemleri veya tasarım değişiklikleri önerilir. Bu yinelemeli

süreç, tasarımın tüm aşamalarında emniyet gereksinimlerinin karşılandığından emin olmayı amaçlar.

2.8.2. Fonksiyonel Tehlike Analizi

Bir Fonksiyonel Tehlike Analizi (FHA) uçak/sistem geliştirme sürecinin başında gerçekleştirilmelidir. Bu çalışma, fonksiyonların hata durumlarını önem derecelerine göre belirlemek ve netleştirmek için işlevlerin sistematik ve kapsamlı bir şekilde incelenmesi olarak tanımlanır. Hata durumu sınıflandırmaları, uçak/sistemin karşılaması gereken emniyet hedeflerini belirler. Hata durumları, uçuş aşaması ve ilgili olumsuz operasyonel veya çevresel koşullar veya harici olaylar göz önüne alındığında, bir veya daha fazla arıza veya hatanın neden olduğu veya katkıda bulunduğu, uçak ve/veya içindekiler üzerinde doğrudan veya sonuç olarak etkisi olan bir durumdur.

Fonksiyonel tehlike analizleri her iki seviyede (uçak/sistem) gerçekleştirilir ve aynı prensipleri kullanır.

Uçak seviyesi Fonksiyonel Tehlike Analizi (UFHA): UFHA, uçak işlevlerinin yüksek seviyeli, nitel bir değerlendirmesidir. UFHA'nın amacı, uçak seviyesi fonksiyonel hata durumlarını belirlemek, bunların etkilerini değerlendirmek ve ilişkili ciddiyeti belirleyerek buna bağlı gereksinimler çıkarmaktır. Bu hata durumlarının açıklanması sonrasında, uçağın karşılaması gereken emniyet gereksinimleri (veya türetilmiş emniyet hedefleri) belirlenir.

Sistem Seviyesi Fonksiyonel Tehlike Analizi (SFHA): SFHA, sistem fonksiyonlarının nitel bir değerlendirmesidir. SFHA'nın amacı, sistem seviyesi fonksiyonel hata durumlarını belirlemek, bu durumların operasyonel aşamalara ve işletme koşullarına göre etkilerini değerlendirmek ve bu etkiler için emniyet sınıflandırmasını belirlemektir. Bu hata durumlarının açıklanması, sistemin karşılaması gereken emniyet gereksinimlerini belirler.

FHA'nın amacı, fonksiyonların tamamen kaybı, kısmi kaybı, hatalı çalışması ve yanlışlıkla çalışması olarak değerlendirilen tüm hata durumlarını tanımlamaktır. Bu

şekilde, kritik fonksiyonlar ve fonksiyonu sağlayan ekipman sınıflandırılarak emniyet gereksinimleri oluşturulur ve tasarım ekiplerinin çalışmaların girdiler olarak iletilir.

Fonksiyonel Tehlike Analizi, kritik hata koşullarının türetilmesi için sistematik bir yaklaşım sağlar ve emniyet değerlendirme sürecini başlatır.

Hata durum senaryolarının tanımları aşağıda gösterilmiştir.

- Tam fonksiyon kaybı: Söz konusu fonksiyon yeteneğini tamamen kaybeder.
- Kısmi fonksiyon kaybı: Söz konusu fonksiyon yeteneğini kısmen kaybeder.
- Fonksiyonun hatalı çalışması: Söz konusu fonksiyon gerektiğinde hatalı çalışır.
- Fonksiyonun yanlışlıkla çalışması: Söz konusu fonksiyon gerekli olmadığı halde doğru çalışır.

Fonksiyonel Hatalar, etkilerinin şiddetlerine göre aşağıdaki kategoriler doğrultusunda sınıflandırılmaktadır.

Felaket (İng. Catastrophic): Normalde uçağın kaybıyla birlikte bir uçuş ekibi üyesinin ölümcül şekilde yaralanmasıyla sonuçlanacak hata durumudur.

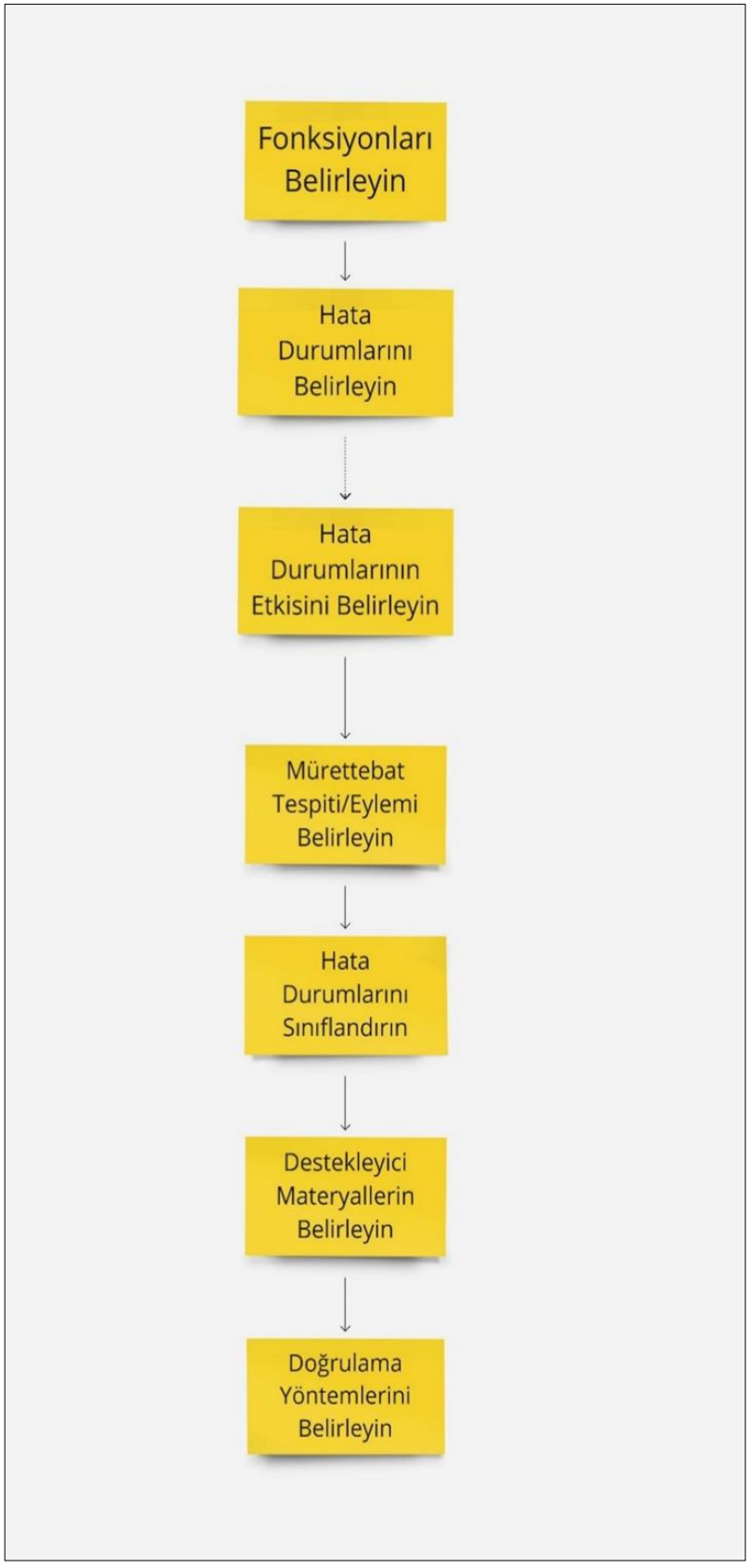
Tehlikeli (İng. Hazardous): Aşağıdaki durumlar, uçağın kabiliyetini veya mürettebatın olumsuz çalışma koşullarıyla başa çıkma kabiliyetini azaltabilecek hata durumlarıdır:
(a) Emniyet marjlarında veya fonksiyonel yeteneklerde büyük bir azalma; veya
(b) Uçuş ekibinin görevlerini doğru veya eksiksiz bir şekilde yerine getireceğine güvenilemeyecek kadar fiziksel sıkıntı veya aşırı iş yük içerir.

Büyük (İng. Major): Uçağın yeteneğini veya mürettebatın olumsuz işletim koşullarıyla başa çıkma kabiliyetini azaltacak şekilde, örneğin, emniyet marjlarında veya işlevsel yeteneklerde önemli bir azalma, mürettebatın iş yükünde veya mürettebatın verimliliğini bozacak koşullarda önemli bir artış, uçuş ekibine rahatsızlık veya yolculara veya kabin ekibine fiziksel sıkıntı, hatta yaralanmaları içerebilir.

Küçük (İng. Minor): Uçak emniyetini önemli ölçüde azaltmayacak ve mürettebatın kendi kabiliyetleri dahilindeki eylemlerini içeren hata durumlarıdır. Küçük hata durumları, emniyet marjlarında veya fonksiyonel kabiliyetlerde hafif bir azalma veya mürettebat iş yükünde hafif bir artış (rutin uçuş planı değişiklikleri gibi) içerebilir.

Etkisiz (İng. No Safety Effect): Emniyet üzerinde etkisi olmayacak hata durumlarıdır (yani, uçağın operasyonel kapasitesini etkilemeyecek veya mürettebatın iş yükünü artırmayacak hata durumlarıdır).

Genel olarak, FHA süreci, fonksiyonel hata durumlarını belirlemek, etkilerini değerlendirmek, bunların ciddiyetini sınıflandırmak ve sistem/alt-sistem tasarımcılarına gereksinimler çıkarmak için bir üstten aşağı yaklaşımdır. FHA çalışması Şekil 2.5 üzerinde yer alan görseldeki adımları takip ederek gerçekleştirilir.



Şekil 2.5. FHA süreci.

2.8.3. Hata Ağacı Analizi

FTA, karmaşık sistemlerde olası hata durumlarını ve bu hataların oluşum nedenlerini analiz etmek için kullanılan grafiksel bir araçtır. FTA, bir sistemin başarısızlığa uğramasına yol açabilecek hata kombinasyonlarını tanımlayan ve görselleştiren bir diyagramdır. Bu analiz, genellikle emniyet önlemleri ve risk yönetimi için kritik öneme sahiptir. FTA'nın uygulama alanları arasında sistem tasarımı, operasyonel emniyet, kazaların neden analizi ve bakım planlaması bulunmaktadır [25].

Analizin amacı, sistem operasyonu ve bakımı ile ilgili kişiler dahil olmak üzere, sistemin nasıl başarısız olabileceğini ve istenmeyen bir olaya yol açabileceğini belirlemektir. Ancak, en az bunun kadar önemli bir diğer amaç, analistin sistemin nasıl kullanılacağını anlamasıdır. Bu, uçuşların süresi ve tipi, beklenen stres seviyeleri, bakım konsepti, komuta ve kontrol, işletme ve bakım personelinin beklenen deneyim seviyesi gibi faktörleri içerir. Ayrıca, acil durum ve iptal prosedürlerinin planlanması gerekmektedir, böylece mürettebatın tepki verememe veya yanlış tepki verme olasılığı göz önünde bulundurulabilir.

Bu kapsamlı inceleme, sistemin ve bu sistemi yönetecek insan kaynağının potansiyel başarısızlık noktalarını belirleyebilmek için kritik öneme sahiptir. Bu analiz süreci, beklenen uçuş koşulları, bakım stratejileri, komuta ve kontrol sistemlerinin işleyişi, ve mürettebatın deneyim seviyesi gibi bir dizi faktörü dikkate alır. Ayrıca, acil durum ve iptal prosedürlerine olan hakimiyet, olası hatalı veya eksik tepkilerin önüne geçilmesinde önemli bir role sahiptir. Bu çerçevede, analistin, sistem ve onunla etkileşimde bulunacak insan unsurlarının tam bir anlayışına sahip olması gerekmektedir. Bu, sistemin emniyetli ve etkili bir şekilde işlemesini sağlamanın yanı sıra, olası hataları en aza indirgeyerek, istenmeyen olayların önlenmesine yönelik önlemlerin geliştirilmesinde hayati bir adımdır.

FTA, Hata Modu ve Etki Analizleri'nden (İng. Failure Modes and Effects Analysis, FMEA) farklı olarak, "Üstten Aşağı Analiz Yöntemi" olarak adlandırılır. Bu, çalışmanın ilk adımı, emniyet açısından kritik kabul edilen hata durumunun (örneğin, "xx" dereceden fazla kanat asimetrisi veya bir uçakta üretilen gücün tamamen kaybı)

tanımlanması anlamına gelir. Sonraki adım, kritik hata durumunu üreten hata modlarının kombinasyonlarına ulaşmak için tüm olası sistem hata durumlarını incelemektir. Kritik hata durumuna yol açan bu tür hata kombinasyonlarının minimum sayısı, Minimal Kesim Kümesi (İng. Minimum Cut Set) olarak bilinir. Daha sonra, türetilen denklemin Minimal Kesim Kümesini temsil ettiğinden emin olmak için Boolean Cebiri (İng. Boolean Algebra) kullanılmalıdır. Minimal Kesim Kümesindeki her bir hata modu için hata olasılıkları yerine konularak, Hata Durumunun meydana gelme olasılığı türetilebilir.

Minimal kesim kümesi (İng. minimum cut set), bir üst olayın meydana gelmesine neden olacak bileşen hatalarının en küçük kombinasyonu olarak tanımlanabilir. Bu tanıma göre, minimal kesim kümesi, üst olay için yeterli olan birincil olayların bir kombinasyonudur. Bu kombinasyon, üst olayın meydana gelmesi için gerekli olan tüm hataları içermekte olup kesim kümesindeki hatalardan biri meydana gelmezse, bu kombinasyonla üst olay gerçekleşmemektedir.

Her hata ağacı, o üst olay için benzersiz olan sınırlı sayıda minimal kesim kümesi içerir. Eğer varsa, tek bileşenli minimal kesim kümeleri, üst olayın gerçekleşmesine neden olacak tekil hataları temsil eder. İki bileşenli minimal kesim kümeleri, birlikte üst olayın gerçekleşmesine neden olacak çift hataları temsil eder. Bir n-bileşenli minimal kesim kümesi için, kesim kümesindeki tüm n bileşenin başarısız olması gerekir ki üst olay meydana gelebilsin.

Üst olay için minimal kesim kümesi ifadesi genel bir formda yazılabilir:

$$T=M1+M2+...+Mk \tag{2.1}$$

Burada T üst olayı ve M1, M2, …, Mk minimal kesim kümelerini temsil eder. Her minimal kesim kümesi, belirli bileşen hatalarının bir kombinasyonundan oluşur ve bu nedenle genel bir n-bileşenli minimal kesim şu şekilde ifade edilebilir:

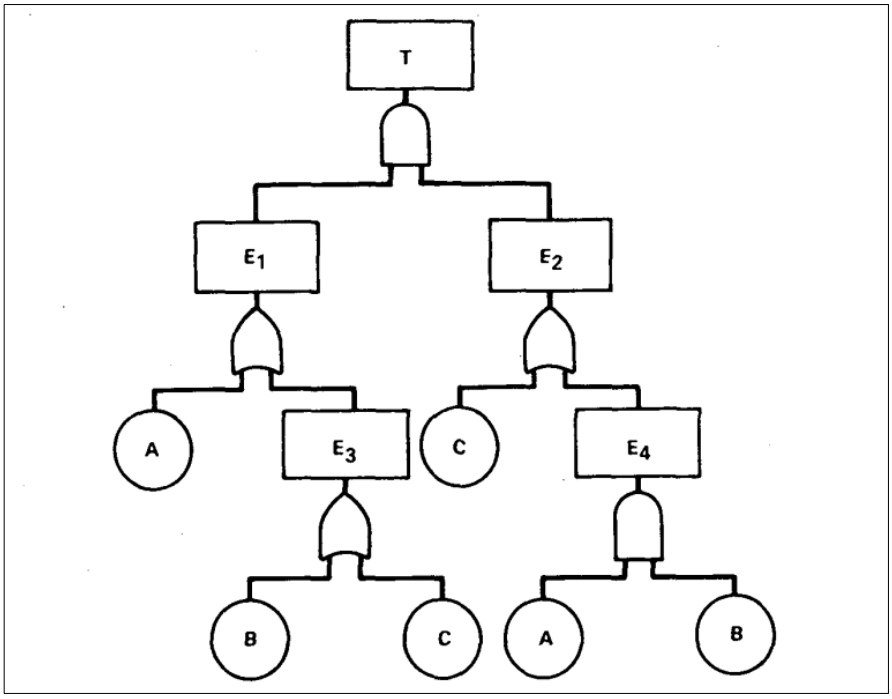
$$M2=X1\cdot X2\cdot...\cdot Xn \tag{2.2}$$

Burada X1, X2, …, ağaçtaki temel bileşen hatalarıdır. Üst olay ifadesinin bir örneği şu şekildedir.

$$T=A+B\cdot C \tag{2.3}$$

Burada A, B ve C, bileşen hatalarıdır. Bu üst olayın bir bileşenli minimal kesim kümesi (A) ve iki bileşenli bir minimal kesim kümesi (B·C) vardır. Minimal kesim kümeleri bir üst olay için benzersizdir ve aynı hata ağacının farklı eşdeğer formlarından bağımsızdır.

Boolean Cebiri, özellikle iki durumlu durumlarla ilgili olduğunda önemlidir: anahtarlar ya açık ya kapalıdır, valfler ya açık ya kapalıdır, olaylar ya gerçekleşir ya gerçekleşmez. Bir hata ağacı, en üst olayın gerçekleşmesine neden olan hata olayları arasındaki Boolean ilişkilerin görsel bir temsili olarak düşünülebilir. Aslında, bir hata ağacı her zaman tamamen eşdeğer bir Boolean denklemleri setine çevrilebilir. Böylece, Boolean cebirinin kurallarını anlamak, hata ağaçlarının inşası ve basitleştirilmesine katkıda bulunur. Bir hata ağacı çizildikten sonra, nitel ve nicel özelliklerini vermek için değerlendirilebilir. Bu özellikler, hata ağacından kendisinden elde edilemez, ancak eşdeğer Boolean denklemlerinden elde edilebilir.



Şekil 2.6. Basit bir FTA örneği.

Şekil 2.6 ile verilen FTA örneğine ait boolean denklemi aşağıda yer almaktadır.

$$T = E1 \cdot E2 \tag{2.4}$$

$$E1 = A + E3 \tag{2.5}$$

$$E3 = B + C \tag{2.6}$$

$$E2 = C + E4 \tag{2.7}$$

$$E4 = A \cdot B \tag{2.8}$$

Başlangıç Durumu:

Üst olay denklemi:

$$T = (A+E3) \cdot (C+E4) \tag{2.9}$$

1.Adım: İlk Yerine Koyma ve Genişletme

$$T=(A\cdot C) + (E3\cdot C) + (E4\cdot A) + (E3\cdot E4) \quad (2.10)$$

2. Adım: E3 için Yerine Koyma

$$E3 = B + C \quad (2.11)$$

Bu nedenle,

$$T = A \cdot C + (B+C) \cdot C + E4 \cdot A + (B+C) \cdot E4 \quad (2.12)$$

3.Adım: Denklemi Düzenleme ve İdempotent Yöntemi Uygulama

İdempotent Yöntemi: Bir olayın kendisiyle çarpımı, olayın kendisine eşittir:

$$(C \cdot C = C) \quad (2.13)$$

$$T = A \cdot C + B \cdot C + C + E4 \cdot A + E4 \cdot B + E4 \cdot C \quad (2.14)$$

4.Adım: Emilim Yöntemi (İng. Law of Absorption) Uygulama

Emilim Yöntemi: Bir olay ve onun bir başka olayla birleşimi, ilk olayı verir.

$$(A \cdot C + B \cdot C + C + E4 \cdot C = C) \quad (2.15)$$

Bu nedenle,

$$T = C + E4 \cdot A + E4 \cdot B \quad (2.16)$$

5. Adım: E4 için Yerine Koyma ve Emilim Yöntemi Uygulama

$$E4 = A \cdot B \quad (2.17)$$

$$T = C + (A\cdot B) \cdot A + (A\cdot B) \cdot B \quad (2.18)$$

Emilim Yöntemi uygulandığında,

$$T = C + A \cdot B \tag{2.19}$$

Minimal kesim kümesi ifadesi:

$$T = C + A \cdot B \tag{2.20}$$

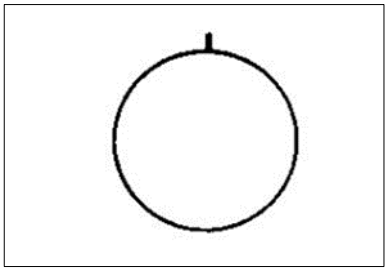
Bu sonuç, üst olayın gerçekleşmesi için gereken minimal bileşen hatalarının kombinasyonunu gösterir. Burada, C tek başına bir minimal kesim kümesi olarak ve A · B kombinasyonu da bir başka minimal kesim kümesi olarak belirlenmiştir.

2.8.3.1. Semboller Hata Ağacının Yapı Taşları

Olay Sembolleri

Basit Olay

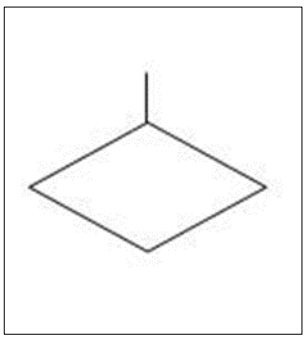
Daire, FTA'da bir hata olayının en temel seviyesini simgeler ve bu olayın altında daha fazla detayın incelenmesine gerek olmadığını gösterir. Bu, çalışmayı gerçekleştiren kişilere analizde odaklanılacak temel noktaları belirleme ve sistem üzerindeki etkileri değerlendirme konusunda rehberlik eder (Şekil 2.7).



Şekil 2.7. Basit olay.

Geliştirilmemiş Olay

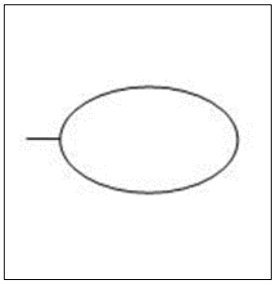
Elmas şekli, hata ağacı analizinde, daha fazla incelenmeye gerek duyulmayan belirli bir hata olayını simgeler. Bu sembol, ya olayın önemsiz olduğu için ya da ilgili bilgilerin eksik olduğu durumlarda kullanılır. Elmas, sistem üzerinde büyük bir etkisi olmayan veya yeterli detayı bulunmayan olayları işaret eder (Şekil 2.8).



Şekil 2.8. Geliştirilmemiş olay.

Koşullandırma Olayı

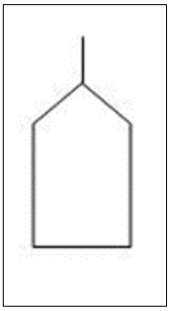
Elips şekli, hata ağacı analizinde, herhangi bir mantık kapısına uygulanan koşulları veya kısıtlamaları kaydetmek için kullanılır. Bu, özellikle INHIBIT (Engelleme) ve PRIORITY AND (Öncelikli VE) kapıları ile birlikte kullanılır. Elips, bu tür kapıların çalışmasını etkileyen özel koşulları veya gereksinimleri belirtmek için tasarlanmıştır (Şekil 2.9).



Şekil 2.9. Koşullandırma olayı.

Harici Olay

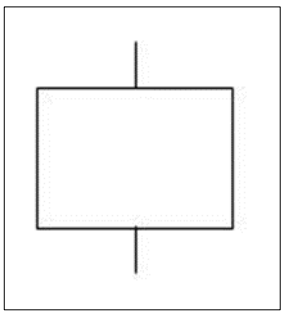
Hata ağacı analizinde, harici olay simgesi, genellikle olması beklenen, hata olarak değerlendirilmeyen olayları temsil eder (Şekil 2.10).



Şekil 2.10. Harici olay.

Ara Olay

Ara olaylar, bir veya daha fazla öncül nedenin mantık kapıları aracılığıyla etkisiyle meydana gelen hata olaylarıdır. Tüm ara olaylar dikdörtgenlerle simgelenir (Şekil 2.11).



Şekil 2.11. Ara olay.

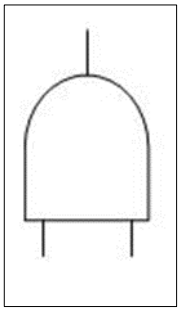
Kapılar

Hata Ağacı, "kapılar" olarak bilinen bir dizi öğeden oluşur. Bu kapılar, arıza mantığının ağaç yapısında yukarı doğru geçişini sağlar veya engeller. Kapılar, bir "üst" olayın meydana gelmesi için gereken olayların ilişkilerini gösterir. "Üst" olay, kapının "çıkışı"; "alt" olaylar ise kapının "girişleri" olarak kabul edilir. Kapı sembolü, çıkış

olayı için gerekli olan giriş olaylarının ilişki türünü belirtir. Bu bakımdan, kapılar bir elektrik devresindeki anahtarlar veya bir boru düzenindeki iki valf ile benzer işlevler görür. Hata ağacı analizinde temel olarak "VE (İng. AND)" ve "VEYA (İng. OR)" iki tür kapı (İng. GATE) vardır.

VE Kapısı

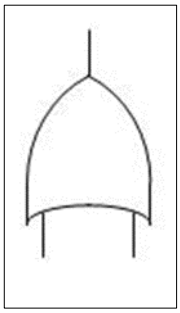
VE (İng. AND) kapısı, çıkış arızasının yalnızca tüm giriş hataları meydana geldiğinde oluştuğunu belirtmek için kullanılır. Bir AND kapısına istenilen sayıda giriş hatası olabilir (Şekil 2.12).



Şekil 2.12. VE kapısı.

VEYA Kapısı

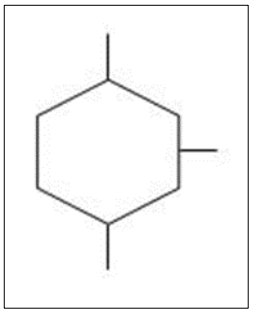
VEYA (İng. OR) kapısı, giriş olaylarından biri veya daha fazlası meydana geldiğinde çıkış olayının gerçekleşeceğini göstermek için kullanılır. Bir VEYA kapısına istenilen sayıda giriş olayı olabilir (Şekil 2.13).



Şekil 2.13. VEYA kapısı.

Engelleme Kapısı

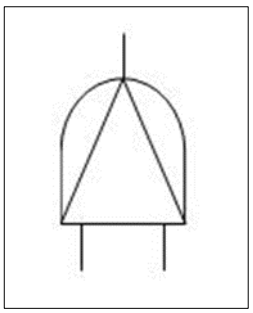
Engelleme (İng. INHIBIT) kapısı, altıgen ile temsil edilen ve ve kapısının özel bir durumu olan bir kapıdır. Çıkış, tek bir girişten kaynaklanır, ancak girişin çıkışı üretebilmesi için bazı belirleyici koşulların karşılanmış olması gerekir. Var olması gereken koşul, koşullu giriştir. Bu koşullu girişin açıklaması, kapının sağ tarafına çizilen bir elips içinde detaylandırılır (Şekil 2.14).



Şekil 2.14. Engelleme kapısı.

Öncelikli VE Kapısı

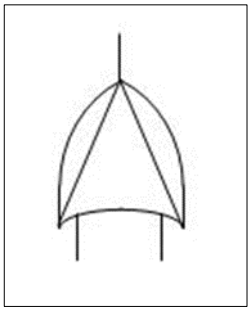
Öncelikli VE kapısı (İng. PRIORITY AND Gate), tüm giriş olaylarının belirlenen bir sırayla gerçekleşmesi durumunda çıkış olayının meydana geldiği, VE kapısının özel bir durumudur. Bu sıra genellikle, kapının sağ tarafına çizilen bir elips içinde gösterilir (Şekil 2.15).



Şekil 2.15. Öncelikli VE kapısı.

Özel VEYA Kapısı

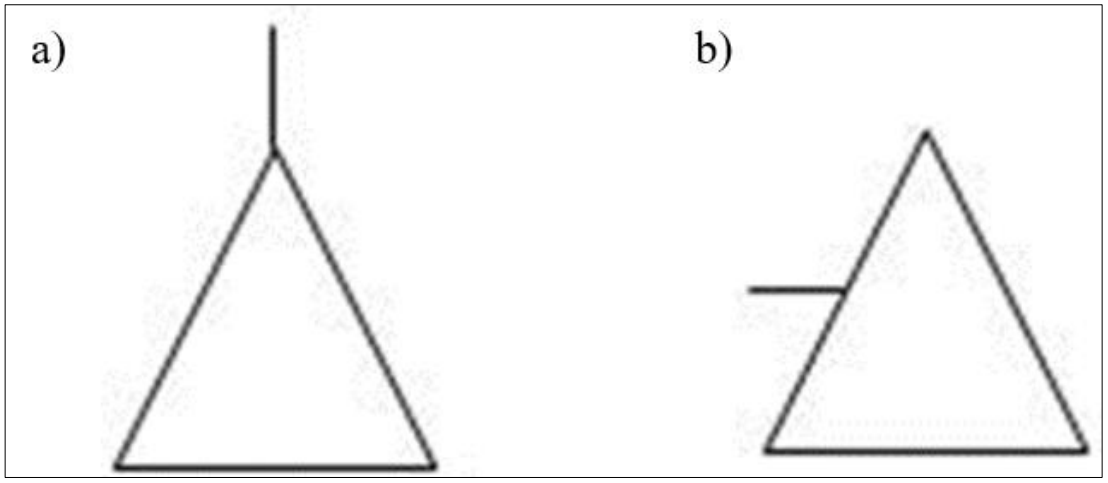
Özel VEYA kapısı (İng. EXCLUSIVE OR), yalnızca tam olarak bir giriş olayı gerçekleştiğinde çıkış olayının meydana geldiği, VEYA kapısının özel bir durumudur (Şekil 2.16).



Şekil 2.16. Özel VEYA kapısı.

Transfer Sembolleri

Üçgenler, hata ağacı içinde aşırı tekrarların önlenmesi amacıyla kolaylık sağlamak için transfer sembolleri olarak tanıtılır. Üçgenin tepe noktasından çıkan bir çizgi "içeri aktarım" (İng. transfer in), yan taraftan çıkan bir çizgi ise "dışarı aktarım" (İng. transfer out) anlamına gelir. Bir kapıya bağlı bir " içeri aktarım ", karşılık gelen "dışarı aktarım" ile bağlantı kurar. Bu "dışarı aktarım", belki başka bir kağıt üzerinde, kapıya giriş tanımlayan ağacın daha ileri bir kısmını içerir (Şekil 2.17).



Şekil 2.17. Transfer sembolleri a) İçeri aktarım b) Dışarı aktarım.

Hata Ağacı Değerlendirmelerinin Temelleri

Hata ağacı değerlendirmesi, sistem hatalarının analiz edilmesi ve değerlendirilmesi sürecinde önemli bir araçtır. Bu analiz yöntemi, sistemdeki potansiyel hataların ve bunların sonuçlarının belirlenmesinde kullanılır. Bu analiz, temelde nitel bir model olmakla birlikte, nicel olarak değerlendirilebilen ve genellikle de değerlendirilen bir yapıya sahiptir. FTA'nın niteliksel yönü, aslında hemen hemen tüm sistem modelleri için geçerli olan bir özelliktir. Hata ağacının niceliksel olarak değerlendirilmeye özellikle uygun bir model olması, modelin kendisinin niteliksel doğasını değiştirmez. Hata ağacı oluşturulduktan sonra, nitel ve/veya nicel sonuçlar elde etmek üzere değerlendirilebilir. Basit ağaçlar manuel olarak değerlendirilebilirken, karmaşık ağaçlar için bilgisayar kodlarından yararlanılması gerekmektedir.

Nitel Değerlendirmeler

Nitel değerlendirmeler kapsamında, minimal kesim kümeleri hata ağacının Boole indirgemesi ile elde edilir. Elde edilen minimal kesim kümeleri, sadece sonraki nitel değerlendirmelerde değil, tüm nicel değerlendirmelerde de kullanılır.

Nicel Değerlendirmeler

Minimal kesim kümeleri elde edildikten sonra, nicel sonuçlar isteniyorsa olasılık değerlendirmeleri yapılabilir. Nicel değerlendirmeler, genellikle bileşenlerin başarısızlık olasılıklarını belirleyerek başlanarak, ardından minimal kesim kümesi olasılıklarının ve nihayetinde sistem, yani üst olay, olasılığının belirlenmesi şeklinde sıralı bir şekilde en kolay gerçekleştirilir. Bu süreçte her kesim kümesinin ve her bileşenin önemine dair nicel ölçütler de elde edilebilir.

Başarısızlık oranları rastgele değişkenler olarak ele alınırsa, başarısızlık oranı varyasyonlarından kaynaklanan sistem sonuçlarındaki değişkenliklerin tahmin edilmesi için rastgele değişken yayılım teknikleri kullanılabilir.

İlgili hata modunun hata oranı ve risk süresinin birleşimi, Hata Olasılığı (İng. Probability of failure: Pf) olarak adlandırılan değeri meydana getirir. Bu olasılık, başarı oranı veya diğer adıyla güvenilirlik (İng. Probability of success: Ps) değerinin 1'den eksiltilmesiyle genellikle hesaplanır. Ps ve Pf arasındaki bağlantıyı ve hata olasılığının neden hata oranı ile risk süresinin çarpımına dayandığını açıklayan matematiksel formül ve gösterimler aşağıda yer almaktadır.

$$P_s = e^{-\lambda t} \tag{2.21}$$

$$P_f = 1 - e^{-\lambda t} \tag{2.22}$$

$$e^{-\lambda t} = 1 - \lambda t + \frac{\lambda^2 t^2}{2!} - \frac{\lambda^3 t^3}{3!} + \cdots] \tag{2.23}$$

$$P_f = 1 - [1 - \lambda t + \frac{\lambda^2 t^2}{2!} - \frac{\lambda^3 t^3}{3!} + \cdots] \tag{2.24}$$

$$Pf = \lambda t - \frac{\lambda^2 t^2}{2!} + \frac{\lambda^3 t^3}{3!} - \cdots] \tag{2.25}$$

λt küçük ise;

$$P_f \cong \lambda t \tag{2.26}$$

Hata ağacı değerlendirmesi sonucunda elde edilen bulgular, niteliksel ve niceliksel sonuçlar olmak üzere iki ana başlık altında incelenebilir.

Nitel Sonuçlar:

- Minimal Kesim Kümeleri: Sistem başarısızlığına yol açan bileşen hatalarının kombinasyonlarıdır. Bu kümeler, sistemin kritik zayıflık noktalarını belirlemekte kullanılır. Ortak neden/ortak mod değerlendirmeleri, ortak bir hassasiyet nedeniyle, tek bir arıza nedeniyle potansiyel olarak hepsi başarısız olabilecek birden fazla bileşeni içeren minimal kesme setlerini belirler.

- Nitel Önemler: Sistem başarısızlığına katkılarına göre bileşenlerin nitel olarak sıralanmasıdır. Bu sıralama, bileşenlerin sisteme olan etkilerinin göreceli önemini belirler.
- Ortak Sebep Potansiyelleri: Tek bir hata nedenine duyarlı olabilecek minimal kesim kümeleridir. Bu, birden fazla bileşenin aynı sebepten dolayı başarısız olma olasılığını ifade eder.

Nicel Sonuçlar:

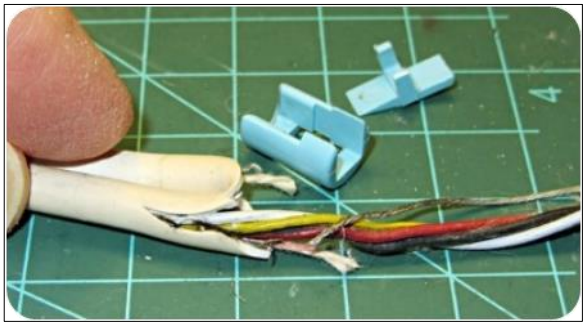
- Sayısal Olasılıklar: Sistem ve kesim kümesi başarısızlıklarının olasılıklarıdır. Bu değerler, sistem hatalarının ne sıklıkta meydana gelebileceğini belirlemek için kullanılır
- Nicel Önemler: Bileşenlerin sistem başarısızlığına katkılarının sayısal olarak sıralanmasıdır. Bu sıralama, her bir bileşenin sistemin genel performansı üzerindeki etkisinin büyüklüğünü gösterir.
- Hassasiyet Değerlendirmeleri: Modellerde ve verilerdeki değişikliklerin, hataların belirlenmesindeki etkileridir. Bu değerlendirmeler, sistemin belirli değişikliklere ve hatalara karşı hassasiyetini analiz eder.

2.8.4. Hata Modu ve Etkileri Analizi

FMEA, potansiyel sistem hata modlarını, nedenlerini ve hata modunun sistem işletimi üzerindeki etkilerini belirlemek için sistematik bir yaklaşımdır. FMEA, öngörülen hata modlarından tasarım gereksinimlerine ulaşılamaması durumunda kabul edilemez hata etkileri ile potansiyel sistem hatalarını belirleyen bir temel oluşturur. Bu, emniyetin değerlendirilmesi, bakım aktivitelerinin planlanması ve sistem için hata iyileştirme, hata toleransı ve hata tespit ve izolasyonu gibi tanımlamaların yapılmasını içerir. Ayrıca, bir sistemin üzerindeki arızanın etkisini tolere edilebilir bir seviyeye indirmek için gereken tasarım güncellemelerinin (modifikasyonlarının) ve düzeltici eylemlerin belirlenmesinde uygulanmaktadır. Bu tür analizler, etkilerinin şiddeti ve etkinin meydana gelme olasılığı açısından hata modunun karşılaştırılmasına genişletildiğinde, buna Hata Modu, Etkileri ve Kritiklik Analizi (İng. Failure Mode, Effects, and Criticality Analysis, FMECA) denir.

FMEA, potansiyel sistem hata modlarını, nedenlerini ve hata modunun sistem işletimi üzerindeki etkilerini belirlemek için sistematik bir yaklaşımdır. FMEA, öngörülen hata modlarından tasarım gereksinimlerine ulaşılamaması durumunda kabul edilemez hata etkileri ile potansiyel sistem hatalarını belirleyen bir temel oluşturur. Bu, emniyetin değerlendirilmesi, bakım aktivitelerinin planlanması ve sistem için hata iyileştirme, hata toleransı ve hata tespit ve izolasyonu gibi tanımlamaların yapılmasını içerir. Ayrıca, bir sistemin üzerindeki arızanın etkisini tolere edilebilir bir seviyeye indirmek için gereken tasarım güncellemelerinin ve düzeltici eylemlerin belirlenmesinde uygulanmaktadır. Bu tür analizler, etkilerinin şiddeti ve etkinin meydana gelme olasılığı açısından hata modunun karşılaştırılmasına genişletildiğinde, buna Hata Modu, Etkileri ve Kritiklik Analizi (İng. Failure Mode, Effects, and Criticality Analysis, FMECA) denir.

Fiziksel veya kimyasal süreçler, tasarım hataları, kalite kusurları, parça yanlış kullanımı veya başarısızlığa neden olan temel sebep olan veya bozulmanın başarısızlığa ilerlemesine neden olan fiziksel süreci başlatabilecek diğer süreçlerdir [31]. Hata sebebi örneği Şekil 2.18 üzerinde verilmiştir.



Şekil 2.18. Hata sebebi (İng. Failure Cause).

Bir hatanın gözlemlendiği şekil, hatanıneydana gelme şeklini ve ekipman operasyonu üzerindeki etkisini tanımlar [31]. Hata modu örneği Şekil 2.Şekil 2.19 üzerinde verilmiştir.

Şekil 2.19. Hata modu (İng. Failure Mode).

Bir hata modunun, bir sistem veya ekipmanın işletimi, fonksiyonu veya durumu üzerindeki sonucudur [31]. Hata etkisi örneği Şekil 2.20 üzerinde verilmiştir.

Şekil 2.20. Hata etkisi (İng. Failure Effect).

Tasarım eksikliklerinin erken uyarısı, tasarım değişikliği gerekli olduğunda ekonomik bir etkiye sahiptir. Bir FMEA'nın amaçları ve kullanımları şunlardır:

- Tehlikeli durumlara neden olabilecek hata modlarını ortaya çıkararak sistem emniyetini iyileştirmek.
- Kritik ve/veya tespit edilemeyen hataların görevle ilgili etkisini değerlendirmek.
- Tasarımı, son ürünü etkileyen hata sayısını azaltacak şekilde etkilemek.
- Doğrulama süreçlerini desteklemek.
- Tasarım mühendisini operasyonel olarak başarılı olma olasılığı yüksek bir tasarım seçmeye yardımcı olmak.

- Etkili bir bakım desteği geliştirmeye yönelik veri sağlamak.

FMEA çalışması, projenin kavramsal tasarım aşamasında başlatılır ve gereksinimlerin yeterliliğini doğrulamak üzere ürünün Ön Tasarım aşamasına kadar devam eder. Ürün geliştirme sürecinin erken dönemlerinde, büyük bir belirsizlik söz konusudur. Bu dönemde, müşteri ihtiyaçları tam olarak anlaşılmamış, gereksinimler ve özellikler genellikle eksiktir. Bu aşamada yer alan belirsizlik, tasarımın kavramsal aşamadan tamamlanma aşamasına kadar olan sürecinde yavaş yavaş giderilir. Bu şekilde, tanımlanan iyileştirmeler tasarımın olgunlaşma sürecini takip eder. Ön Tasarım aşamasında, son ürünün fonksiyonel analizi, ürünün hem arızasız hem de arızalı durumlarda nasıl işlev gösterdiğinin değerlendirilmesi yoluyla tasarım belirsizliğinin azaltılmasına yardımcı olur. Detaylı tasarım aşamasında, tasarımın gereksinimlere uygunluğunun doğrulanması için bu analiz kullanılır.

Analize başlamadan önce, sistem gereksinimleri ve işletim konsepti bilindiği kadarıyla belirlenmelidir. Bunlar arasında sistem işletim modları ve fonksiyonları, gerekli performans seviyeleri, çevresel düşünceler ve emniyet veya düzenleyici gereksinimler yer alır. Sahada elde edilen raporlar, tasarım kuralları, denetim listeleri ve benzer sistemlerin tarihçesi veya analizleri üzerine kurulu derslerden çıkarılan diğer rehberler gibi veriler toplanır ve incelenir.

Analiz planlaması, analiz sonuçlarının tasarım rehberliği sağlamak üzere nasıl kullanılacağının belirlenmesi, belirlenen gereksinimleri ve tasarımın gereksinimlere uygunluğunu doğrulama prosedürleri için gerçekleştirilir. Analiz süreci, sürecin ve metodolojinin iç yönergeler ile belirlenen standartlar, gereksinimler ve hedeflerle nasıl uyumlu olduğunun kurulması için tanımlanmaktadır.

Her bir arızanın sonuçlarını değerlendirerek ve arızanın sistem emniyeti, hazırlığı, görev başarısı, bakım talebi veya lojistik destek üzerindeki etkisini inceleyerek potansiyel tasarım zayıflıkları belirlenir. Arızaların tespiti için yollar ve etkilerini hafifletmek için gerekli olan telafi edici önlemler veya tasarım değişiklikleri, her arızanın şiddeti ve oluşma olasılığına göre tanımlanır ve önceliklendirilir.

FMEA, hata modlarının nasıl varsayıldığına bağlı olarak;

- Fonksiyonel FMEA,
- Arayüz FMEA,
- Detaylı FMEA olarak sınıflandırılır.

Fonksiyonel FMEA: Fonksiyonel Hata Modu ve Etki Analizi (F-FMEA), kavramsal tasarım aşamasında, bir sistemin veya sürecin fonksiyonlarını, bu fonksiyonların başarısızlık modlarını ve bu başarısızlıkların sistem üzerindeki etkilerini analiz ederek, tasarımın geliştirilmesine yardımcı olmayı amaçlar. Bu analiz yöntemi, denetim sistemleri, süreçler, yazılımlar ve fonksiyonelliği işletim detaylarından daha kolay anlaşılır olan karmaşık sistemler gibi çeşitli uygulamalarda kullanılabilir. Fonksiyonel FMEA, donanım, yazılım veya süreç henüz oluşturulmadan önce, yani tasarım aşamasında uygulanarak, tasarımın iyileştirilmesine önemli katkılar sağlar.

Fonksiyonel FMEA'nin Ana Amaçları:

1. Hava aracı fonksiyonel incelemesi ve alt sistem fonksiyonel incelemesi için hangi fonksiyonların görev açısından kritik olduğunu belirler.
2. Her başarısızlık modunun sistem performansı üzerindeki etkilerini belirler.
3. Hata ağacı analizi geliştirmek için veri sağlar.
4. Başarısızlık kök nedenlerini belirlemek için bir temel oluşturur.
5. Tasarım alternatiflerinin yüksek güvenilirlikle değerlendirilmesine olanak tanır.
6. Test yöntemleri ve izolasyon tekniklerinin geliştirilmesine yardımcı olur.

F-FMEA Sonuçları:

1. Düzeltici eylem gerektiren fonksiyonel başarısızlıkları vurgular.
2. Her fonksiyonel başarısızlığı, başarısızlık etkisinin görev başarısı ve uçuş emniyeti üzerindeki ciddiyetine göre sınıflandırır.

3. Sistem ve/veya alt sistem fonksiyonel başarısızlık modlarını sıralar.
4. Güvenilirlik açısından kritik fonksiyonları tanımlar ve emniyet aktivitelerine geri bildirim sağlar.

F-FMEA Süreci: Analize başlamadan önce, analize yardımcı olacak mümkün olduğunca çok bilgi toplanmaktadır. Bu bilgiler arasında güncel çizimler veya şematikler, sistem fonksiyonları, işletim teorisi, olasılık sınıflandırmaları, varsayılan başarısızlık modları ve görev aşamaları bulunur.

- Fonksiyon ID: Fonksiyonun sistemdeki düzeyini ifade eder.
- Fonksiyon: Fonksiyonun kısa bir açıklamasını ifade eder.
- Uçuş Fazı: Ortak Veri Dokümanı'nda verilen uçuş fazlarını ifade eder.
- ID No: Her bir hata moduna atanan numarayı ifade eder.
- Hata Modu: Fonksiyonlarla birlikte kullanılan ortak hata modları seti, hata modlarının tanımlarını oluşturmak için kullanılır.
- Aşırı (İng. Over),
- Yetersiz (İng. Under),
- Yok (İng. No),
- Aralıklı (İng. Intermittent).
- Lokal Etki: Hatanın doğrudan etkilerini ifade eder.
- Bir Üst Etki: Sistem fonksiyonlarının hatadan nasıl etkilendiğini ifade eder.
- Son Etki: "Son Etki" sütunu hatanın uçak seviyesine nasıl etki ettiğini ifade eder.
- Şiddet Sınıflandırması: Bir hata modunun en kötü potansiyel sonucunu dikkate alır, Çizelge 8'e göre belirlenir.
- Oluşma Sıklığı: Grup içindeki (F-FMEA ve tasarım ekibi dahil olmak üzere) deneyime dayanır ve konsensüs yoluyla nitel bir terim seçilir.
- Kritiklik İndeksi: Kritiklik Matrisinin renklerine göre temsil edilen sütundur.

- Tespit Yöntemi: Bir hatanın, normal sistem işletim çalışması esnasında operatör tarafından veya bakım ekibi tarafından bazı tanısal işlemlerle keşfedilebileceği yöntem veya araç.
- Telafi Edici Önlemler: Operatörün bir sistemin üzerindeki hatanın etkisini yok etmek veya hafifletmek için kullanabileceği veya alabileceği eylemler.
- Açıklamalar: Çalışma sayfası satırındaki herhangi bir diğer sütunu açıklayan veya netleştiren herhangi bir önemli açıklama not edilir [30].

FMEA çalışması kapsamında şiddet sınıflandırması kategorileri Çizelge 2.8. Şiddet sınıflandırması ve açıklaması [30] ile birlikte verilmiştir.

Çizelge 2.8. Şiddet sınıflandırması ve açıklaması [30].

Kategori	RHS	Şiddet Sınıflandırması	Açıklaması
Cat 1	1	Kategori I Felaket (İng. Catastrophic)	Ölüme veya silah sistemi kaybına (yani uçak, tank, füze, gemi vb.) neden olabilecek bir hata.
Cat 2	2	Kategori II Kritik (İng. Critical)	Ciddi yaralanmalara, büyük maddi hasara veya görev kaybına neden olacak büyük sistem hasarına neden olabilecek bir hata.
Cat 3	3	Kategori III Önemsiz (İng. Marginal)	Küçük yaralanmalara, küçük maddi hasarlara veya sistemde küçük hasarlara neden olacak gecikmeye, kullanılabilirlik kaybına veya görev bozulmasına neden olabilecek bir hata.
Cat 4	4	Kategori IV Küçük (İng. Minor)	Yaralanmaya, maddi hasara veya sistem hasarına neden olacak kadar ciddi olmayan, ancak planlanmamış bakım veya onarımla sonuçlanacak bir hata.

Arayüz FMEA: Arayüz FMEA'sı, gereksinimlere uygunluğu doğrulamak için Fonksiyonel FMEA ile aynı şekilde gerçekleştirilir. Özellikle farklı tasarım grupları tarafından tasarlanmış olan alt sistemler arasındaki bağlantılar, varsayılan arıza modları için temel oluşturur. Ayrı bir Arayüz FMEA'nın avantajı, bağlantılı alt sistemlerin detaylı tasarımı mevcut olmadan gerçekleştirilebilmesidir. Sistem bağlantıları tanımlandığı anda, uygun arayüz protokollerinin tasarlandığından emin

olmak için başlanır. Bu analizin tipik çıktıları, arayüz tasarım değişiklikleriyle ortadan kaldırılması veya hafifletilmesi gereken arayüz arıza modlarıdır.

Arayüz FMEA, arayüzleme sistem elemanları arasındaki bağlantılardaki hataların özelliklerini belirleme ve kaydetme sürecidir. Arayüz FMEA, sistem elemanlarının arayüzlerine ilişkin bilgilerin toplanmasıyla başlar. Gösterildiği gibi, donanım elemanları arasındaki bağlantılar kablolar, teller, fiber optik hatlar, hidrolik hatlar veya pnömatik hatlar olabilir. Ayrıca, sistem elemanları arasındaki yazılım arayüzlerine ilişkin bilgiler de belirlenmelidir. Daha önce elde edilen veya üretilen birim arayüz diyagramları, arayüz gereksinimleri spesifikasyonları ve arayüz denetim dokümanları, belirli türdeki arayüzleri tanımlamak için incelenir. Arayüzlerle özgü hata modları tanımlanır ve özellikleri belirlenir.

Detaylı FMEA: Detaylı FMEA, bireysel sistem elemanları içindeki her bileşenin başarısızlıklarının özelliklerini belirleme ve belgeleme sürecidir. Bu elemanlar; küçük parçalar (İng. piece_parts), işlevsel parça grupları ve uygulamadaki yazılımları içerir. Her bir elemanın tasarımı olgunlaştıkça ve detaylı tasarım şematikleri, parça listeleri, detaylı yazılım tasarım dokümanları ve kaynak kodları mevcut hale geldikçe detaylı FMEA başlatılır. Bu analiz, mühendislik modeli üzerinde gerçekleştirilebilir ve sistem operasyonel modelinde yansıtılan değişiklikler için revize edilebilir. Detaylı analizi doğru bir şekilde gerçekleştirmek için kurulu bir başarısızlık modları seti hayati öneme sahiptir. İstenmeyen sonuçlara sahip herhangi bir tek nokta veya tespit edilmemiş başarısızlıklar, ilgili tasarım disiplini ile gözden geçirilir. Bulunan eksiklikler uygun tasarım grubu tarafından düzeltilir ve analiz buna göre yeniden düzenlenir.

Kritiklik Analizi (CA): Kritiklik Analizi (İng. criticality analysis, CA), her bir hata modunu ciddiyeti ve oluşma olasılığına göre sınıflandırmayı amaçlar. Bu sayede, ürünün mümkün olan tüm hata durumlarında tam olarak değerlendirilmesi sağlanabilir. Parça konfigürasyonu ve hata oranı verilerinin mevcudiyet düzeyi, kullanılacak analiz yaklaşımını belirlemektedir. Kritiklik analizi nitel ve nicel olmak üzere iki şekilde gerçekleştirilir.

Nitel Kritiklik Analizi: Hata sıklığı, hata oranına bağlı olduğundan ve bu tür analizlerde hata oranı kullanılmadığından, analistler beklenen olasılıkları tahmin etmek zorundadır. Sistem olgunlaştıkça, hata olasılık seviyeleri güncellenmelidir. Parça konfigürasyonu ve hata oranı verileri mevcut hale geldikçe, gerçek kritiklik numaraları niceliksel yaklaşım kullanılarak türetilmeli ve analize dahil edilmelidir.

Bu süreç, sistemin zamanla daha iyi anlaşılmasını ve hata yönetiminin daha etkili bir şekilde yapılmasını sağlar. Başlangıçta, eksik veri nedeniyle tahmini yöntemler kullanılsa da, zamanla elde edilen gerçek verilerle sistem daha doğru bir şekilde analiz edilebilir. Bu yaklaşım, sistem güvenilirliğinin artırılmasına ve beklenmeyen hataların minimize edilmesine katkıda bulunur. Olasılık tanımları
Çizelge 2.9 ile verilmiştir.

Çizelge 2.9. Olasılık Tanımları [30].

Olasılık Seviyesi	Olasılık	Olasılık Tanımı
1	Sık (İng. Frequent)	Her bir ekipman için birkaç kez meydana gelmesi beklenir.
2	Makul olarak Muhtemel (İng. Reasonably Probable)	Her bir ekipman için en az bir kez meydana gelmesi beklenir.
3	Ara Sıra (İng. Occasional)	Tüm ekipmanlar için birkaç kez meydana gelmesi beklenir, ancak her ekipman için meydana gelmesi beklenmez.
4	Uzak (İng. Remote)	Tüm ekipmanlar için en az bir kez meydana gelmesi beklenir.
5	Son Derece İmkansız (İng. Extremely Unlikely)	Meydana gelmesi beklenmez.

Nicel Kritiklik Analizi: Hata oranları (İng. Failure rates), MIL-HDBK-217, 217Plus, Elektronik Olmayan Parçaların Güvenilirlik Verileri (İng. Nonelectronic Parts Reliability Data) (NPRD-91) gibi kaynaklardan türetilebilir veya çıkarılabilir.

$$C_m = \beta \alpha \lambda_p t \tag{2.27}$$

C_m: " m^{th} " Hata Modu İçin Kritiklik Numarası (Bir bileşenin veya fonksiyonun hata durumları karşısında ne kadar kritik olduğunu nicel bir şekilde ifade eden bir ölçüttür.)

β: Hata Modu Oranı (belirli bir öğe için)

α: Koşullu Fonksiyon Kaybı Olasılığı

λ_p: Parça Hata Oranı (Hata / Milyon Saat)

t: Çalışma Süresi veya Çalışma Döngüsü Sayısı

Kritiklik Matrisi: Çizelge 2.10 üzerinde verilen kritiklik matrisi, bir ürün veya süreçteki potansiyel hata modlarının sistematik olarak değerlendirilmesini sağlayan, risk yönetimi ve güvenilirlik mühendisliği alanlarında temel bir araçtır. Ana amacı, her hata modunun şiddeti ve oluşma olasılığına dayanarak risk azaltma çabalarını önceliklendirmektir. İlgili risk sınıflandırması

Çizelge 2.11 ile gösterilmektedir.

Çizelge 2.10. Kritiklik matrisi.

Kritiklik Matrisi	**A** **SIK** **R_{POC} = 1** **FR_{POC} = 2**	**B** **MAKUL OLARAK MUHTEMEL** **R_{POC} = 2** **FR_{POC} = 3**	**C** **ARA SIRA** **R_{POC} = 3** **FR_{POC} = 4**	**D** **UZAK** **R_{POC} = 4** **FR_{POC} = 5**	**E** **SON DERECE İMKANSIZ** **R_{POC} = 5** **FR_{POC} = 6**
(I) **FELAKET** **R_{HS} = 1** **FR_{HS} = 2**	**1** **Risk = 4**	**2** **Risk = 6**	**3** **Risk = 8**	**4** **Risk = 10**	**5** **Risk = 12**
(II) **KRİTİK** **R_{HS} =2** **FR_{HS} = 4**	**3** **Risk = 8**	**5** **Risk = 12**	**6** **Risk = 16**	**7** **Risk = 20**	**8** **Risk = 24**
(III) **ÖNEMSİZ** **R_{HS} =3** **FR_{HS} = 8**	**6** **Risk = 16**	**8** **Risk = 24**	**9** **Risk = 32**	**10** **Risk = 40**	**11** **Risk = 48**
(IV) **KÜÇÜK** **R_{HS} =4** **FR_{HS} = 16**	**9** **Risk = 32**	**11** **Risk = 48**	**12** **Risk = 64**	**13** **Risk = 80**	**14** **Risk = 96**

RHS (Hata Şiddeti): Bir arızanın sisteme veya işletmeye olan etkisinin şiddetini ölçer. Bu, arızanın ne kadar ciddi olduğunu ifade eder.

FRHS (Hata Şiddeti Faktörü): Hata şiddetinin sayısal bir değerle ifadesidir ve bu değer, RHS değerinin iki katı alınarak hesaplanır. Bu, hata şiddetinin risk hesaplamalarında nasıl ölçeklendirildiğini gösterir.

RPOC (Meydana Gelme Olasılığı): Bir hatanın meydana gelme ihtimalini ifade eder. Bu, hatanın ne kadar sık yaşandığının bir göstergesidir.
FRPOC (Meydana Gelme Olasılığı Faktörü): Meydana gelme olasılığının sayısal bir değerle ifadesidir. Bu değer, risk hesaplamalarında kullanılır.

FRHS = 2*RHS

Risk = FRPOC * FRHS

Çizelge 2.11. Risk sınıflandırması.

KRİTİKLİK ENDEKSİ	**SONUÇ**
1 ile 5 arası (A)	KABUL EDİLEMEZ Zorunlu olarak yeniden tasarım gerekir
6 ile 8 arası (B)	İSTENMEYEN Yeniden tasarım tercih edilir, aksi takdirde hafifletici önlemler gerekli olacaktır.
9 ile 10 arası (C)	KABUL EDİLEBİLİR Yeniden tasarım istenebilir, aksi takdirde hafifletici önlemler gerekli olabilir.
11 ile 14 arası (D)	KABUL EDİLEBİLİR Daha fazla işleme gerek yoktur.

2.8.5. Geliştirme Güvence Seviyesi

Uçak sistem tasarımında Geliştirme Güvence Seviyesi (İng. Development Assurence Level, DAL), sistem emniyetinin temel taşlarından biridir. Bu seviyeler, sistemlerin ve bileşenlerin, olası arızalarının uçak üzerindeki potansiyel etkisine göre sınıflandırılmasını sağlamaktadır. Bu yaklaşım, havacılık endüstrisindeki emniyet standartlarını karşılamak ve yolcu ile mürettebat emniyetini en üst düzeye çıkarmak için kritik öneme sahiptir.

Bir uçak/sistem fonksiyonunun veya öğesinin Geliştirme Güvence Seviyesi, sadece bu uçak/sistem fonksiyonunun veya öğesinin geliştirme sürecine değil, aynı zamanda incelenen fonksiyon veya öğeyi etkileyebilecek diğer tüm uçak/sistem fonksiyonları veya öğeleriyle olan arayüzlerin geliştirilmesine de uygulanır.

Geliştirme Güvence Seviyesi, Başarısızlık Durumlarının şiddet sınıflandırmasına bağlı olarak atanır ve geliştirme hatalarının sonuçlarını sınırlayabilecek geliştirme süreçleri arasındaki olası bağımsızlık göz önünde bulundurularak belirlenir. Başarısızlık Durumu Sınıflandırması ne kadar ciddiyse, Başarısızlık Durumunu hafifletmek için gerekli olan Geliştirme Güvence düzeyi o kadar fazla olur.

DAL belirlenmesi, ilgili uçak seviyesi fonksiyonlarıyla ilişkilendirilen en ciddi hata durumunun sınıflandırmasına dayalıdır. Bu sınıflandırma, hataların potansiyel ciddiyetine bağlı olarak A'dan E'ye kadar değişiklik gösterir.

Uçak Seviyesi Başarısızlık Durumlarının şiddet sınıflandırmasını dikkate alarak DAL ataması aşağıdaki şekilde gerçekleştirilmektedir.

Felaket Bir Başarısızlık Durumu Söz Konusu Olduğunda:

- Eğer bir uçak/sistem fonksiyonu veya öğesinde olası bir geliştirme hatası sonucu Felaket bir Başarısızlık Durumu (FC) oluşabilecekse, ilişkili DAL A seviyesi atanır.
- Eğer iki veya daha fazla bağımsız geliştirilmiş uçak/sistem fonksiyonları veya öğeleri arasında olası geliştirme hatalarının bir kombinasyonu sonucunda Felaket bir Başarısızlık Durumu oluşabilecekse, ya bir DAL A seviyesi atanır ya da iki Geliştirme Güvence sürecine en az B seviyesi atanır. Diğer bağımsız geliştirilmiş uçak/sistem fonksiyonları veya öğeleri en düşük DAL olarak C seviyesi atanır. İki veya daha fazla bağımsız geliştirilmiş uçak/sistem fonksiyonlarının veya öğelerinin gerçekten bağımsız olduğunu belirleyen DAL A seviyesinde kalmalıdır.

Tehlikeli Bir Başarısızlık Durumu Söz Konusu Olduğunda:

- Eğer bir uçak/sistem fonksiyonu veya öğesinde olası bir geliştirme hatası sonucu Tehlikeli/Ciddi Büyük bir Başarısızlık Durumu oluşabilecekse, ilişkili DAL en az B seviyesi atanır.
- Eğer iki veya daha fazla bağımsız geliştirilmiş uçak/sistem fonksiyonları veya öğeleri arasında olası geliştirme hatalarının bir kombinasyonu sonucunda Tehlikeli Başarısızlık/Ciddi Büyük Durumu oluşabilecekse, ya bir Geliştirme Güvence sürecine en az B seviyesi atanır ya da iki Geliştirme Güvence sürecine en az C seviyesi atanır. Diğer bağımsız geliştirilmiş uçak/sistem fonksiyonları veya öğeleri en düşük DAL olarak D seviyesi atanır. İki veya daha fazla bağımsız geliştirilmiş uçak/sistem fonksiyonlarının veya öğelerinin gerçekten bağımsız olduğunu belirleyen Geliştirme Güvence süreci B seviyesinde kalmalıdır.

Büyük Bir Başarısızlık Durumu Söz Konusu Olduğunda:

- Eğer bir uçak/sistem fonksiyonu veya öğesinde olası bir geliştirme hatası sonucu Büyük bir Başarısızlık Durumu oluşabilecekse, ilişkili geliştirme güvence sürecine C seviyesi atanır.
- Eğer iki veya daha fazla bağımsız geliştirilmiş uçak/sistem fonksiyonları veya öğeleri arasında olası geliştirme hatalarının bir kombinasyonu sonucunda Büyük bir Başarısızlık Durumu oluşabilecekse, ya bir geliştirme güvence sürecine en az C seviyesi atanır ya da iki geliştirme güvence sürecine en az D seviyesi atanır. İki veya daha fazla bağımsız geliştirilmiş uçak/sistem fonksiyonlarının veya öğelerinin gerçekten bağımsız olduğunu belirleyen Geliştirme Güvence süreci C seviyesinde kalmalıdır.

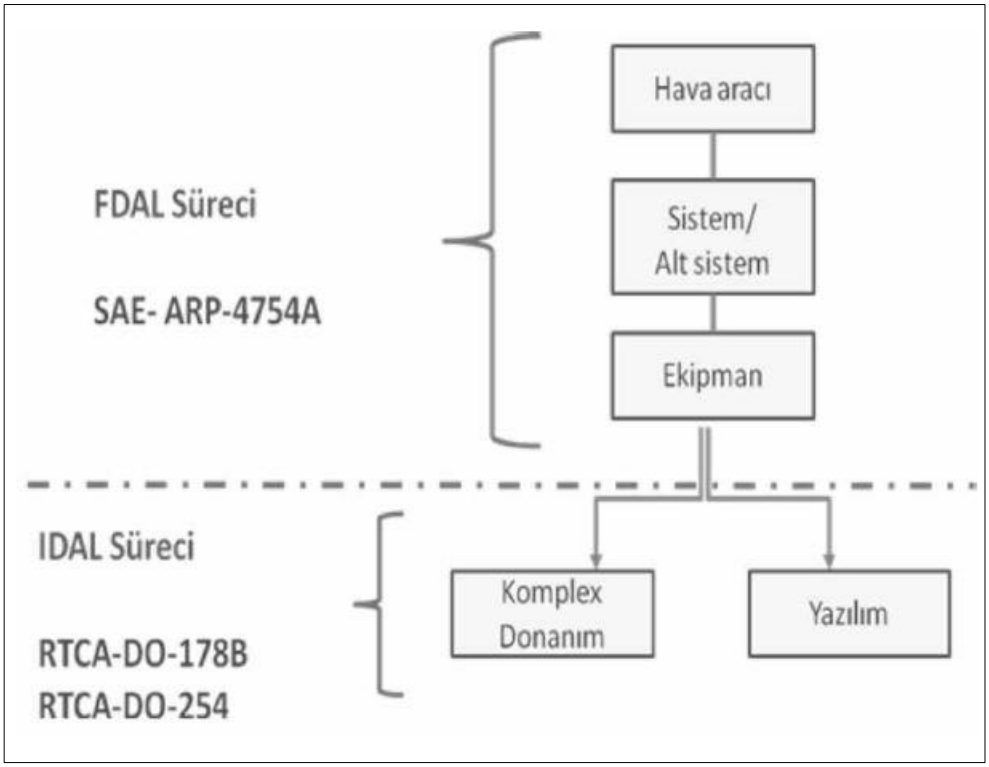
Küçük Bir Başarısızlık Durumu Söz Konusu Olduğunda:

- Eğer bir uçak/sistem fonksiyonu veya öğesinde olası bir geliştirme hatası sonucu Küçük bir Başarısızlık Durumu oluşabilecekse, ilişkili geliştirme güvence sürecine en az D seviyesi atanır.
- Eğer iki veya daha fazla bağımsız geliştirilmiş uçak/sistem fonksiyonları veya öğeleri arasında olası geliştirme hatalarının bir kombinasyonu sonucunda Küçük bir Başarısızlık Durumu oluşabilecekse, bir geliştirme güvence sürecine en az D seviyesi atanır.

Geliştirme sürecinde uygulanacak temel ilkeleri incelemek üzere, fonksiyon geliştirme ve öğe geliştirme olmak üzere iki ayrı aşama tanımlanmıştır.
Fonksiyon Geliştirme Aşaması (FDAL): Bu aşamada, Fonksiyonlar için gereksinimler geliştirilir ve öğelere tahsis edilir. Gereksinim geliştirme süreci, gereksinim setinin tamamlanma ve doğruluk güvencesini (validasyon) içerir. Fonksiyon gereksinimi geliştirme sürecinin titizlik düzeyi, Fonksiyonun Geliştirme Güvence Seviyesi tarafından belirlenir ve burada FDAL (Fonksiyon Geliştirme Güvence Seviyesi) olarak adlandırılır.

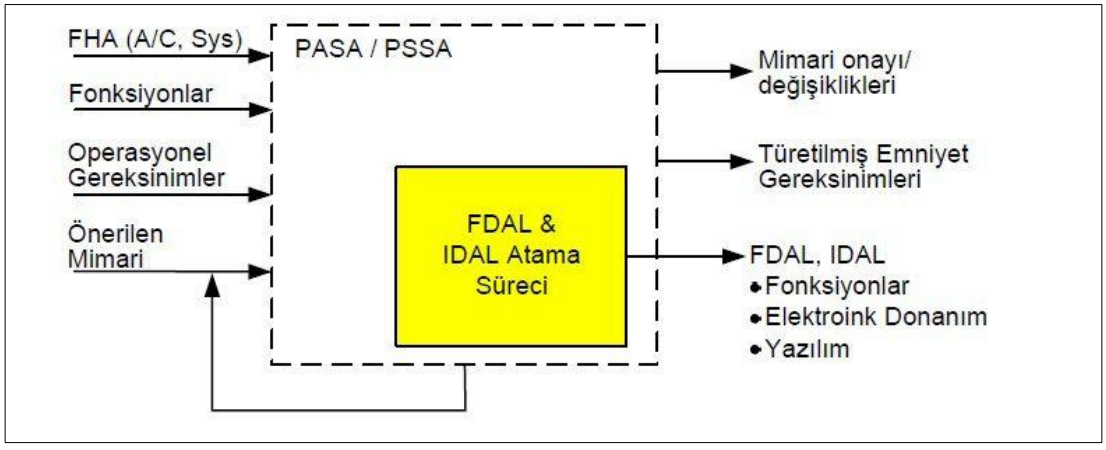
Öğe Geliştirme Aşaması (IDAL): Bu aşamada öğeler geliştirilir. Öğelerin geliştirme sürecinin titizlik düzeyi, elektronik donanım veya yazılım güvence seviyesi olan ve burada IDAL (Öğe Geliştirme Güvence Seviyesi) olarak adlandırılan seviye tarafından belirlenir. IDAL ataması bağlamında, bir öğe kendisi içinde potansiyel geliştirme hatalarını hafifletmek için kredi olarak kullanılacak mimari özellikler içermez.

Şekil 2.2121 ile belirtilen DAL seviyelerine göre hangi geliştirme standartlarının uygulanacağı gösterilmiştir.



Şekil 2.21. DAL-standart ilişkisi [24].

Fonksiyonlar, ilgili Hata Durumu Sınıflandırmaları, sistemler ve madde gereksinimleri arasındaki ilişkiler ve bunlara karşılık gelen DAL atamaları, Şekil 2.22 üzerinde özetlenmiştir.



Şekil 2.22. FDAL/IDAL atama süreci [26].

DAL atama süreci, uçağın ve/veya sistemlerin FHA Başarısızlık Durumlarına (burada Üst Seviye Başarısızlık Durumları olarak adlandırılır) dahil olan Fonksiyonlara FDAL

atamasıyla başlar. En ciddi Üst Seviye Başarısızlık Durumu Sınıflandırmasına dayanarak, üst seviye Fonksiyona bir FDAL atanır. Bu atama Çizelge 2.12 ile verilene uygun olarak, uçak ve sistem FHA'lerdeki her fonksiyon için gerçekleştirilir.

Çizelge 2.12. Üst düzey fonksiyon FDAL ataması [26].

Üst Düzey Hata Durumu Şiddet Sınıflandırması	**İlişkili Üst Düzey Fonksiyon FDAL Ataması**
Felaket	A
Tehlikeli / Ciddi Büyük	B
Büyük	C
Küçük	D
Emniyet Etkisi Yok	E

Belirli bir Başarısızlık Durumunun ciddiyetine göre, Fonksiyonel Emniyet Sistemlerindeki elemanlara FDAL değerlerinin nasıl tahsis edileceği Çizelge 2.13 ile belirtildiği şekilde ilerlemektedir.

Çizelge 2.13. Fonksiyonel başarısızlık kümesi üyelerine DAL ataması [26].

EN ÜST DÜZEY BAŞARISIZLIK DURUMU SINIFLANDIRMASI	GELİŞTİRME GÜVENCE SEVİYESİ (DAL)		
	TEK ÜYELİ FONKSİYONEL BAŞARISIZLIK KÜMELERİ	BİRDEN FAZLA ÜYESİ OLAN FONKSİYONEL BAŞARISIZLIK KÜMELERİ NOT 2 VE NOT 4	
		SEÇENEK 1 NOT 3	**SEÇENEK 2**
Sütun 1	Sütun 2	Sütun 3	Sütun 4
Felaket	FDAL A NOT 1	Bir üye için FDAL A düzeyi, ek üyelerin gelişim süreçlerindeki hataların en ciddi etkileri için geçerli tüm başlıca başarısızlık durumlarında, en ağır bireysel etkileriyle uyumlu seviyede katkıda bulunur. Ancak, ek üyeler için bu seviye C'den daha düşük olamaz.	İki üye için FDAL B, en üst düzeydeki Başarısızlık Koşuluna yol açar. Diğer üye(ler) ise, geliştirme süreçlerindeki bir hatanın en ciddi bireysel etkileriyle ilişkili seviyede, tüm uygulanabilir en üst düzey Başarısızlık Koşulları için yer alır (ancak ek üye(ler) için bu seviye C'den daha düşük olamaz).
Tehlikeli / Ciddi Büyük	FDAL B	Bir üye için FDAL B, ek üye(ler)in geliştirme süreçlerindeki bir hatanın en şiddetli bireysel etkileriyle ilişkili seviyede, tüm uygulanabilir en üst düzey Başarısızlık Koşullarına katkıda bulunmasıyla sağlanır (ancak ek üyeler için bu seviye D'den daha düşük olamaz).	İki üye için FDAL C, en üst düzey Başarısızlık Koşuluna yol açar. Diğer üyeler, geliştirme süreçlerindeki bir hatanın en ciddi bireysel etkileriyle ilişkili seviyede, tüm uygulanabilir en üst düzey Başarısızlık Koşulları için yer alır (ancak ek üyeler için bu seviye D'den daha düşük olamaz).
Büyük	FDAL C	Bir üye için FDAL C, ek üye(ler)in geliştirme süreçlerindeki bir hatanın en şiddetli bireysel etkileriyle ilişkili seviyede, tüm uygulanabilir en üst düzey Başarısızlık Koşullarına katkıda bulunmasıyla sağlanır.	İki üye için FDAL D, en üst düzey Başarısızlık Koşuluna yol açar. Diğer üyeler, geliştirme süreçlerindeki bir hatanın en ciddi bireysel etkileriyle ilişkili seviyede, tüm uygulanabilir en üst düzey Başarısızlık Koşulları için yer alır.
Küçük	FDAL D	Bir Üye için FDAL D, ilgili tüm üst düzey Arıza Koşulları için geliştirme süreçlerindeki bir hatanın en şiddetli bireysel etkileri ile ilişkilendirilen düzeydeki tüm ek Üyelerin katkıda bulunduğu durumda geçerlidir.	
Emniyet Etkisi Yok.	FDAL E	FDAL E	

NOT 1: Eğer bir FFS'nin tek bir Üyesi varsa ve sistematik hatalar için azaltma stratejisi yalnızca FDAL A ise, başvuru sahibi, o Üyenin geliştirme sürecinin, felaket etkisi olan potansiyel geliştirme hatalarının giderilmiş veya hafifletilmiş olduğundan emin olmak için yeterli bağımsız doğrulama/teyit aktivitelerine, tekniklerine ve tamamlama kriterlerine sahip olduğunu kanıtlamak zorunda kalabilir.

NOT 2: Yapılan fonksiyonel ayrıştırma sayısı ne olursa olsun aynı sırada kalınması gerekmektedir (örneğin, Felaket Başarısızlık Koşulu için, en üst FDAL A FFS'den yapılan herhangi bir ayrıştırma derecesi en az bir FDAL A veya iki FDAL B Üyesi içermelidir).

NOT 3: Fonksiyonel Başarısızlık Setindeki Üyelerin sayısal bulunabilirliğinde büyük bir fark varsa, genellikle daha yüksek bulunabilirliğe sahip Üyeye daha yüksek seviyede FDAL atanmalıdır.

NOT 4: 14CFR Bölüm 23 /CS-23 hava araçlarının bazı sınıflarında, Tablo 3'te gösterilenden daha düşük FDAL'ler bulunmaktadır. Özel yönlendirmeler için güncel FAA AC23.1309 ve eşdeğer EASA politikasına bakınız.

2.8.6. Ortak Neden Analizi

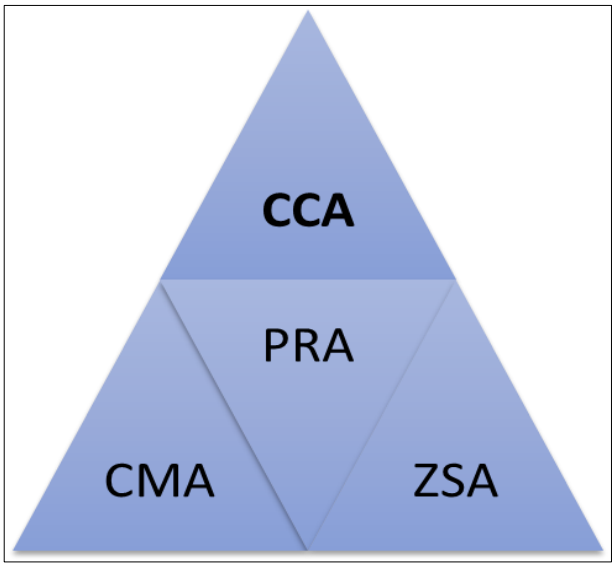
SAE-ARP-4761[25]'e göre tanımlandığında, Ortak Neden ifadesi, yedekliliği veya bağımsızlığı geçersiz kılan veya yanıltan bir olay veya başarısızlıktır.

CS 25.1309b(1)(ii) gerekliliklerine göre, bir sistemin tek bir bileşeninin, parçasının veya unsurunun arızalanması sonucunda bir Felaket Hata Durumu meydana gelmemelidir. Felaket Hata Durumlarını engellemek amacıyla tek bir arızanın etkilerinin yayılmasını sınırlamak için sistem tasarımı tarafından hata önleme sağlanmalıdır. Buna ek olarak, hem tek bir bileşeni, parçayı veya unsuru hem de arıza önleme hükümlerini etkileyebilecek ortak bir hata nedeni olmamalıdır [29].

Bu nedenle emniyet gerekliliklerini karşılamak için fonksiyonlar, sistemler veya öğeler arasında bağımsızlık gerekmektedir. Bu tür bir bağımsızlığın mevcut olduğundan veya bağımlılıkla ilişkili riskin kabul edilebilir olduğundan emin olunması gerekmektedir. Ortak Neden Analizi, bu bağımsızlığı doğrulamak veya belirli bağımlılıkları tanımlamak için araçlar sağlar.

Şekil 2.23 ile gösterilen Ortak Neden Analizi, Fonksiyonel Tehlike Analizleri (FHA) çalışmalarının tamamlanması ile başlar.

Başlangıçta Özel Risk Analizleri (PRA) gerçekleştirilir ve geliştirilen bazı gereklilikler Ortak Mod Analizi (CMA) ve Zonal Emniyet Analizi (ZSA) için uygulanır.



Şekil 2.23. Ortak neden analizi ilişkisi.

2.8.6.1. Ortak Mod Analizi

Ortak Mod Analizi; Hata Ağacı Analizi (FTA), Bağımlılık Diyagramları (DD) ve Markov Analizindeki (MA) VE'li olayların gerçekten bağımsız olduğunu doğrulamak için gerçekleştirilir. Tasarım uygulamasının, üretim ve bakım hatalarının ve yedekli tasarım ilkelerini bozan sistem bileşenlerinin arızalarının etkileri analiz edilmelidir. Genel olarak, CMA gerektiğinde bağımsızlık ilkelerinin uygulandığının doğrulanmasına katkıda bulunur.

Ortak Mod Analizinde Asgari olarak aşağıdaki modlara bakılmalıdır:

- Geliştirme Süreci Ortaklığı (Donanım, Yazılım Gereksinim, DAL vb.)
- Üretim Hattı Ortaklığı
- Yerleşim/Montaj Ortaklığı
- Çevresel Faktörlerin Ortaklığı (Sıcaklık, Nem, Titreşim vb.)
- Düzeltici/Önleyici Bakım Süreci Ortaklığı

- Operasyon Ortaklığı
- Teknoloji Ortaklığı
- Rotalama (kablaj vb.) Ortaklığı
- Dış Kaynakların Ortaklığı (Güç Beslemesi vb.).

2.8.6.2. Özel Risk Analizi (PRA)

"Özel riskler, ilgili sistemlerin dışında kalan olaylar veya etkiler olarak tanımlanır. Örnekler arasında yangın, sıvı sızıntısı, kuş çarpması, lastik patlaması, yüksek yoğunluklu yayılan alanlara maruz kalma, yıldırım, yüksek enerjili dönen makinelerin denetimsiz arızası vb. yer almaktadır. Her risk, eşzamanlı veya kademeli etkileri incelemek ve belgelemek için özel bir çalışmanın konusu olmalıdır." [29].

Bazı Özel Riskler mutlaka Ortak Nedenli Arıza ile sonuçlanmasa da, genellikle çok kanallı sistemleri tehlikeye atma potansiyeline sahip olduklarından herhangi bir Ortak Neden Analizinde dikkate alınmaları gerekir**.**

- Yüksek enerjili dönen cihazlardan salınan enkaz (Motor Dışı Sınırlama)
- Basınçlı gemilerden salınan döküntüler
- Yüksek Basınçlı Hava Kanalı Kopması
- Yüksek Sıcaklık Hava Kanalı Kopması
- Lastik Enkazı
- Sallanan Lastik Sırtı
- Tekerlek Enkazı
- Pist Enkazı
- Yangın
- Sızdıran Sıvılar
- Yakıt
- Hidrolik Yağ
- Akü Asidi
- Su
- Kuş Çarpması

- Dolu, Buz, Kar
- Yıldırım Çarpması
- Elektromanyetik Girişim.

Kuş Çarpmaları

Tasarım boyunca, sistemlerin tek bir kuş çarpmasının hayati sistemlerin arızalanmasına yol açmayacak şekilde yönlendirilmesine dikkat edilmektedir. Ancak, çarpma olasılığını etkileyen birçok faktör olduğundan, uçak gövdesine kuş çarpması olasılıkları değerlendirilirken zorluklarla karşılaşılabilir. Bu faktörler arasında uçak hızı, rakım, saldırı açısı, havaalanı konumu, günün saati, yılın zamanı, yerel hava trafiği yoğunluğu, havaalanı kuş önleyici tedbirler, kuşun boyutu vb. yer alır.

Bununla birlikte, hizmet içi kayıtların analizinden, Avrupa'da faaliyet gösteren uçaklara kuş çarpmalarının ortalama olarak 10.000 hareket başına 3,5 oranında meydana geldiği görülmektedir. Çarpmaların %1'inden azı 4 lb'den büyük kuşları içermektedir ve yaklaşık %85'i 8000 feet'in altında meydana gelmektedir. Bununla birlikte, mevcut çalışmalar daha büyük kuşların ve özellikle de Islıkçı Kuğuların çarpma sıklığının son yıllarda arttığını göstermektedir.

Kuş çarpması hasarına ilişkin EASA CS-25 gereklilikleri şu şekildedir: *"Uçak, 4 lb'lik bir kuşa çarptıktan sonra, uçağın hızı (uçağın uçuş yolu boyunca kuşa göre) deniz seviyesinde VC'ye eşit olduğunda, uçağın sürekli güvenli uçuş ve iniş kabiliyetini sağlayacak şekilde tasarlanmalıdır veya 2438 m'de (8000 ft) 0,85 VC, hangisi daha kritikse." [29].*

"Tasarımın ilk aşamalarında, kontrol sistemi bileşenleri gibi temel hizmetlerde yer alan öğelerin ve hasar görmesi halinde elektrikli ekipman gibi tehlikeye neden olabilecek öğelerin kurulumuna dikkat edilmelidir. Mümkün olduğu sürece bu tür eşyalar kuşların çarpabileceği alanların hemen arkasına yerleştirilmemelidir." [29].

Kuş çarpmaları bağımsız olmayan olayların klasik bir örneğidir. Kuşlar sürüler halinde toplanma eğiliminde olduğundan, ayrılmış çok kanallı sistemlerin bile birden fazla

kuşun çarpması nedeniyle kritik hasara uğrama riski vardır. Kuş sürüleri, Ortak Sebepli Arızanın çok önemli bir şeklidir ve birçok çoklu motor alevlenmesi vakasıyla sonuçlanmıştır. Kuş çarpmasına ait görüntü Şekil 2.24 üzerinde yer almaktadır.

Şekil 2.24. Kuş çarpması görseli.

Bir Boeing 737 uçağında meydana gelen kazaya ilişkin aşağıdaki açıklama, kuş çarpmalarının uçağın kritik sistemlerinde arızaya neden olma potansiyelini göstermektedir:

“28 Kasım 2004 Pazar günü bir Boeing 737-400, dönüş sırasında burun iniş takımı bölgesine kuş çarpması yaşadı. Soruşturmada, kazanın muhtemelen kalkış sırasında uçağın burun tekerleği yönlendirme sisteminin kablolarından birinin kuş çarpması sonucu kırılması ve diğerinin sıkışması sonucu burun tekerleklerinin temas ettiğinde sola dönmesi nedeniyle meydana geldiği belirlendi. İniş sırasında aşağı indi ve uçak yavaşlarken lövyenin tam sapması ile durdurulamayan sola doğru bir sapmaya neden oldu. Uçak büyük hasar gördü. İçeridekilerde ciddi veya ölümcül bir yaralanma olmadı.” [34].

Lastik Enkazı

Tork mili kırılmaları ve lastik sırtının dökülmesi gibi çok kanallı sistemlere yönelik diğer potansiyel çevresel tehlikeler, tasarım aşamasında "Bölgesel Emniyet Analizi" aracılığıyla dikkate alınır. Çoğu Hata Analizi tekniği her sistemi ayrı ayrı ele alır; ancak Bölgesel Emniyet Analizinin amaçlarından biri farklı sistemlerin etkileşimini dikkate almaktır. Örneğin, kapaklı tork tüpünün kırılması, arızalı şaftın sallanması nedeniyle bitişikteki elektrik kablolarında, hidrolik borularda ikincil hasara neden olabilir. Benzer şekilde, alt takımın yakınına yerleştirilen ekipman, lastik sırtının dökülmesi veya patlaması nedeniyle hasar görebilir. Hata durumları belirlendikten sonra, mümkün olan yerlerde bunları ortadan kaldırmak için uygun düzeltici eylem gerçekleştirilmelidir. Ancak bazı durumlarda kritik sistem bileşenlerini potansiyel lastik döküntü alanlarından tamamen izole etmek mümkün olmayabilir ve risk seviyesinin değerlendirilmesi, motor döküntüsü için kullanılana benzer bir teknik kullanılarak yapılabilir.

Lastik hasarından kaynaklanan ve uçağın diğer sistemlerine hasara yol açan bir senaryoya ait görsel Şekil 2.25 ile verilmiştir.

Şekil 2.25. Lastik enkazını anlatan bir görsel.

Aşağıdaki lastik enkazı modeli, risk değerlendirmesi için kullanılanların tipik bir örneğidir:

Enkaz Boyutu ve Kütlesi: kenarları lastiğin genişliğine eşit olan bir kareye uygun boyutlarda lastiğin bir parçası olarak alınır. (Hizmet sırasındaki gerçek lastik sırtı olaylarından elde edilen verilere dayanmaktadır ve aynı zamanda FAR 33'ün önceki standartlarında önerilen boyuta da karşılık gelmektedir) [34].

Hız: Tipik bir iniş/kalkış hızı olarak alınan hız ifadesidir [34].

Serbest Bırakma Noktası: Çevre üzerindeki yerle temas halinde olmayan herhangi bir nokta için olasılığın sabit olduğu varsayılmaktadır [34].

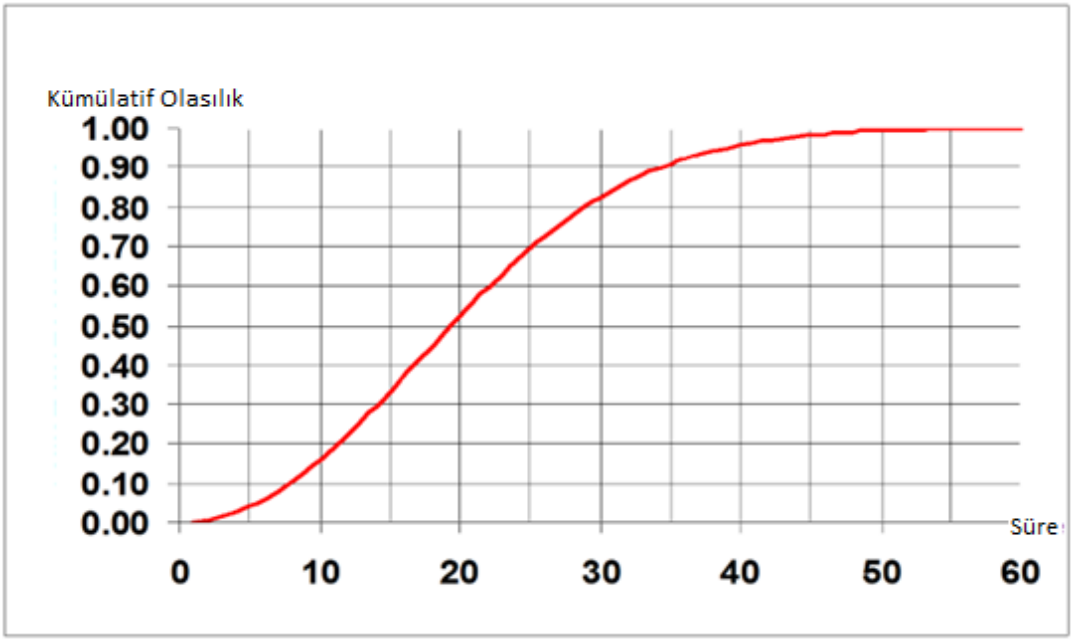
Yörünge: Sönmüş bir lastik için zemin/lastik temas noktasından çıkan bir noktada, lastiğin her iki yanında dikeyden 10° olarak alınır. (Dinamometre test sonuçlarına göre) [34].

Lastik enkaz modellerinin, değişen hızlar ve lastik enkaz boyutları gibi faktörlere uyum sağlamak üzere uçağa özel olması gerektiği açıktır. Bir uçak üreticisi, maksimum enkaz boyutunun 3 kilograma kadar olduğunu ve Gauss dağılımına yakın bir yörüngenin ± 15° olduğunu varsaymaktadır.

Yangın

Uçak sistemlerinin kurulumu planlanırken kanalların ayrılmasına ve olası yangın kaynaklarına göre konumlarına özel dikkat gösterilmelidir.

FAA için gerçekleştirilen geçmiş kazalara ilişkin bir araştırmaya dayanarak, potansiyel olarak felaket etkisine sahip (katastrofik) bir uçuş sırasında yangının sürdürülemez hale gelmesi için değerlendirilen zaman dağılımı Şekil 2.26. üzerinde gösterilmiştir.



Şekil 2.26. Uçuş sırasında meydana gelen bir yangının ardından kullanılamaz hale gelme süresinin Kümülatif Olasılık Dağılımı [34].

Aşağıdaki kazalar, uçaktaki yangınların uçağın emniyetini ciddi şekilde tehlikeye atma potansiyelini göstermektedir:

"2 Eylül 1998 tarihinde, Swissair'in 111 sefer sayılı uçağı, 215 yolcu ve 14 mürettebatıyla İsviçre'nin Cenevre kentine gitmek üzere tarifeli seferle ABD'nin New York kentinden doğu yaz saati uygulamasına göre 2018'de havalanmıştır.

Kalkıştan yaklaşık 53 dakika sonra, 330 uçuş seviyesinde seyir halindeyken, uçuş ekibi kokpitte anormal bir koku hissetmiştir. Daha sonra dikkatleri arkalarında ve üstlerinde belirsiz bir alana çekildi ve kaynağı araştırmaya başladılar. Başlangıçta gördükleri şeyin kısa bir süre sonra artık görünür olmadığını algılamışlardır. Anomalinin kaynağının klima sistemi olduğu konusunda hemfikir olmuşlardır. Gördükleri ya da görmekte oldukları şeyin kesinlikle duman olduğunu değerlendirdiklerinde, yön değiştirmeye karar verdiler. Başlangıçta Boston'a doğru dönmeye başladılar; ancak hava trafik hizmetleri alternatif bir havaalanı olarak Halifax, Nova Scotia'dan bahsedince, rotayı Halifax Uluslararası Havaalanı olarak değiştirdiler.
Uçuş ekibi Halifax'a inişe hazırlanırken uçağın ön kısmında tavana doğru yayılan bir yangının farkında değildi. Anormal kokunun tespit edilmesinden yaklaşık 13 dakika

sonra uçağın uçuş veri kaydedicisi, uçak sistemleriyle ilgili arızaları hızlı bir şekilde kaydetmeye başladı. Uçuş ekibi acil durum ilan etti ve acilen iniş yapılması gerektiğini belirtti. Yaklaşık bir dakika sonra, uçakla olan radyo iletişimi ve ikincil radar bağlantısı kesildi ve uçuş kayıt cihazları çalışmayı durdurdu. Yaklaşık beş buçuk dakika sonra uçak, Şekil 2.27 üzerinde görselleştirildiği üzere, Peggy's Cove, Nova Scotia, Kanada'nın yaklaşık beş deniz mili güneybatısında okyanusa düştü ve maalesef kurtulan olmadı [35].

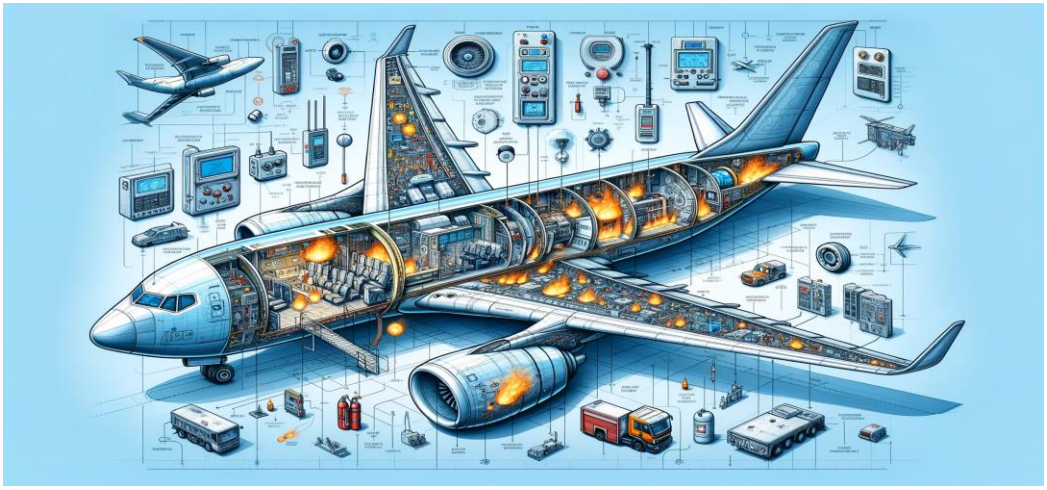
Şekil 2.27. Yangın kazasını anlatan bir görsel.

Delta – Boeing 727: Bu yangınla ilgili kaza yerde meydana geldi ve neyse ki personele herhangi bir yaralanmaya yol açmadı. Ancak, yangın uçuş sırasında gerçekleşseydi, koşullar biraz farklı olabilirdi.

14 Ekim 1989'da Delta Havayolları'na ait bir Boeing 727-232 uçağı ABD'nin Utah eyaletindeki Salt Lake City'nin kapısına park edilmişti. Mürettebat boğuk bir patlama duydu ve 3D numaralı koltuğun yakınındaki havalandırma deliğinden gelen alevleri gördü. Yangın, mürettebatın kazayı, yangını ve kurtarmayı bildirmek için kokpite dönmesini engelledi. Yolcular ve mürettebat uçağı tahliye etti. En son ayrılan ikinci memur, duman nedeniyle çıkış bulmakta zorlandıktan sonra arka hava merdivenlerine ulaşamadı ve acil durum penceresi çıkışından dışarı çıktı. Bir tamirci, uçuş öncesi sırasında yolcu oksijen kaynağının düşük olduğunu fark etti ve oksijen tüplerini değiştirdi. Elektrik ekipmanı bölmesinden çıkarken tamirci, oksijen sistemi akış

kontrol ünitesini beyaz bir ışığın sardığını gördü. El telsizini kullanarak kaza, yangın ve kurtarma ekiplerine yangını bildirme girişiminde bulundu ancak sonuç alamadı. Yolcu oksijen sistemi, önceki 30 gün boyunca altı adet düşük oksijen miktarı bakım raporuna sahipti ancak şirketin otomatik trend analiz programı tarafından "işaretlenmedi". Delta'nın filosunun incelenmesi, diğer uçaklarda 35 oksijen sistemi sızıntısını ortaya çıkardı. Kazada, uçakta 22 yolcu bulunuyordu ve yolcuların tamamı yara almadan kurtuldu [36].

Uçakların tasarımında yangına karşı göz önünde bulundurulması gereken senaryoları gösteren görsel Şekil 2.28 üzerinde gösterilmiştir.



Şekil 2.28. Bir uçağın yangına karşı önlemlerinden bir kesit.

Bu kazalardan yola çıkarak alınması gereken başlıca tasarım önlemleri özetle aşağıdaki gibi sıralayabiliriz.

- Tüm malzemelerin gerekli yanıcılık gereksinimlerini karşıladığına dair onaylı olması gerekmektedir.
- Kurulum, normal veya müteakip sistem arızalarında (örneğin yakıt veya hidrolik boru sızıntısından kaynaklanan) karşılaşılabilecek yanıcı akışkanların yakınında potansiyel tutuşma kaynakları olmayacak şekilde yapılmalıdır.
- Kritik sistemler yangına maruz kalabilecek alanlarda konumlandırılmamalıdır.

2.8.6.3. Bölgesel Emniyet Analizi

Bölgesel Emniyet Analizi (İng. Zonal Safety Analysis, ZSA)'nin amacı, uçağın her bir bölgesindeki ekipman kurulumlarının, tasarım ve kurulum standartları, sistemler arası müdahaleler ve bakım hataları açısından yeterli bir emniyet standardında olmasını sağlamaktır. Uçağın, birden fazla sistemin ve bileşenin yakın mesafede kurulduğu alanlarında, bölgesel analizin, tek başına sürdürülebilir olarak kabul edilen ancak yan yana bulunan diğer sistemleri veya bileşenleri olumsuz etkileyerek daha ciddi etkilere neden olabilecek herhangi bir hatayı veya arızayı tespit etmesi gerekmektedir [25].

Uçak bölgeleri; kullanım, basınçlandırma, sıcaklık aralığı, şiddetli hava koşullarına ve yıldırım çarpmalarına maruz kalma ve ateşleme kaynakları, yanıcı sıvılar, yanıcı buharlar veya dönen makineler gibi içerdiği tehlikeler açısından farklılık gösterir. Buna göre kurulum kuralları bölgeye göre farklılık gösterir. Örneğin, kablolama için kurulum gereklilikleri, kablonun yangın bölgesine, rotor patlama bölgesine veya kargo alanına kurulmasına bağlıdır.

ZSA, bir sistem ekipmanının ve ara bağlantı tellerinin, kablolarının ve hidrolik ve pnömatik hatlarının, tanımlanmış kurulum kurallarına ve ayırma gerekliliklerine uygun olarak kurulduğunun doğrulanmasını içerir. ZSA, ekipman girişimi potansiyelini değerlendirir. Aynı zamanda sistemler üzerinde kademeli bir etkiye sahip olabilecek arıza modlarını ve bakım hatalarını da dikkate alır. Örneğin:

- Sallanan tork mili
- Oksijen sızıntısı
- Akümülatör patlaması
- Sıvı sızıntısı
- Rotor patlaması
- Gevşek bağlantı elemanı
- Hava kaçağı
- Aşırı ısınmış tel
- Bağlayıcı anahtarlama hatası.

19 Temmuz 1989'da, bir McDonnell Douglas DC-10-10 olan United Airlines Flight 232, 2 No'lu motor aşaması 1 fan rotor diski tertibatında denetlenemeyen bir arıza yaşadı. Motor parçaları 1 ve 3 numaralı hidrolik sistem hatlarını kopardı. Motor arızasından kaynaklanan kuvvetler 2 No'lu hidrolik sistem hattını kırdı. Hidrolik güçle çalışan üç uçuş kontrol sisteminin de kaybedilmesiyle emniyetli iniş imkânsız hale geldi. Üç hidrolik sistemin bağımsız olmaması, fiziksel olarak izole edilmiş olmasına rağmen, birbirlerine yakın olmaları nedeniyle onları tek bir arıza olayına karşı savunmasız bıraktı. Bu bölgesel bir tehlikeydi. Uçak, Sioux City, Iowa'daki Sioux Gateway Havaalanına saptıktan sonra düştü; 111 ölüm, 47 ciddi yaralanma ve 125 hafif yaralanma meydana geldi [37].

12 Ağustos 1985'te, bir Boeing 747-SR100 olan Japan Air Lines Flight 123, Japonya'nın Tokyo kentindeki Haneda Havaalanından 24.000 feet yükseklikte kalkıştan 12 dakika sonra kabinde basınç kaybı yaşadı. Dekompresyon, daha önce onarılan arka basınç bölmesindeki arızadan kaynaklandı. Kabin havası basınçsız gövde boşluğuna hücum etti, bölgede aşırı basınç oluştu ve yardımcı güç ünitesi (APU) güvenlik duvarının ve dikey kanat için destekleyici yapının arızalanmasına neden oldu. Dikey kanatçık uçaktan ayrıldı. Arka gövdede bulunan hidrolik bileşenler de koparak dört hidrolik sistemin tamamının hızla tükenmesine yol açtı. Dikey kanatçığın kaybı, dört hidrolik sistemin tamamının kaybıyla birleştiğinde, uçağın üç eksende de kontrol edilmesini imkânsız olmasa da son derece zor hale getirdi. Dört hidrolik sistemin tek bir arıza olayından bağımsız olmaması bölgesel bir tehlikeydi. Uçak, kalkıştan kırk altı dakika sonra bir dağa çarptı; 520 kişi öldü ve 4 kişi hayatta kaldı [38].

2.8.7. Sistem Emniyet Değerlendirmesi

SSA, bir sistemin, mimarisinin ve kurulumunun emniyet gereksinimleriyle uyumunu göstermek için sistemli bir incelemedir. Her PSSA için karşılık gelen bir SSA olmalıdır. En üst düzey SSA, sistem düzeyindeki SSA'dır. Analiz edilen her sistem için SSA, uçağa olan etkileriyle birlikte tüm önemli arıza koşullarını özetlemektedir. Uyumun gösterilmesi için kullanılan analiz yöntemleri nitel veya nicel olabilir. SSA süreci, tasarımın emniyet standartlarına ve hedeflerine uygunluğunun alttan üste bir

metodoloji ile teyit edilmesini sağlamaktadır. Bu süreç aşağıdaki adımları içermektedir:

- Sistem Seviyesi FHA tarafından tanımlanan tasarım kriterlerinin karşılandığının denetlenmesi
- Uçak seviyesindeki potansiyel etkilerin sınıflandırılmasının doğrulanması
- Uçak tasarımının gereksinim ve amaçlarına dayanarak belirlenen emniyet kriterlerinin yerine getirildiğinin onaylanması
- CCA prosedürü ile tanımlanan tasarım şartlarının yerine getirilmesinin doğrulanması
- Sistem seviyesindeki SSA'nın, uçak seviyesindeki FHA ile olan ilişkisinin incelenmesi.

2.9. MODEL TABANLI EMNİYET ÇALIŞMALARI

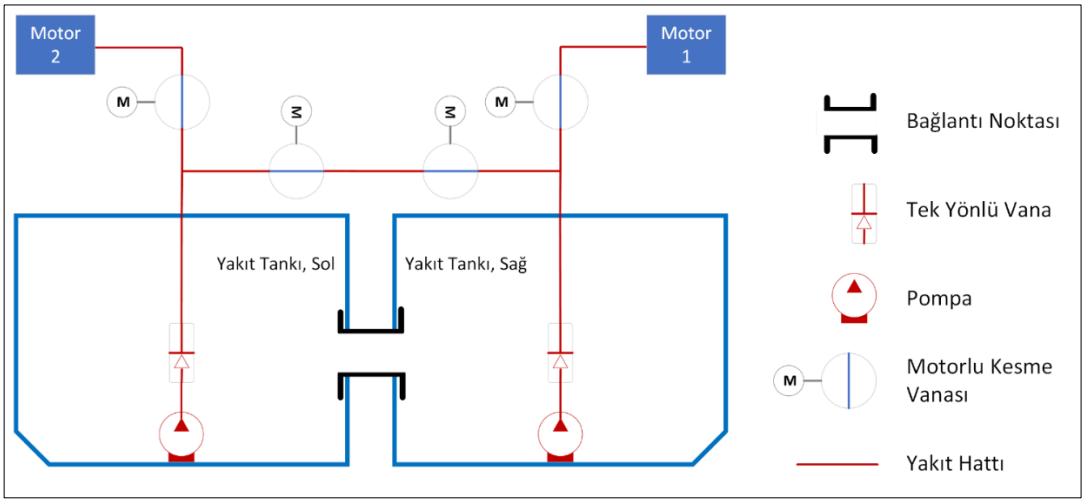
Daha önceki bölümlerde teorik temelleri atılan emniyet çalışmaları, bu bölümde Model Tabanlı Emniyet Çalışmaları (MBSE) metodolojisi ile Ansys Medini yazılımı kullanılarak derinlemesine uygulanmaktadır. Bu yaklaşım, hava araçlarının yakıt sistemlerinin emniyet ve güvenilirlik analizlerinde kritik bir dönüm noktası teşkil etmektedir. MBSE'nin, yakıt sisteminin motorları besleme fonksiyonunun emniyetini değerlendirme süreci, bu metodolojinin nasıl entegre edildiğini ve emniyet süreçlerinin nasıl detaylandırıldığını örnekleyen bir vaka çalışması olarak sunulmaktadır. Süreç, Motor Besleme Mimarisi'nin tasarımından başlayarak, Fonksiyon Mimarisi oluşturma, FHA, Nitel FTA ve en nihayetinde kesme vanasının FMECA analizine kadar geniş bir spektrumu kapsamaktadır. FMECA'dan elde edilen veriler, daha sonra SSA kapsamında Nicel FTA için bir temel oluşturmuştur.

Bu bölümdeki Ansys Medini programı ile gerçekleştirilen analizler, Model Tabanlı Emniyet Çalışmalarının, geleneksel emniyet analiz yöntemlerine göre nasıl daha üstün bir detay seviyesi ve kapsamlılık sunduğunu gözler önüne sermektedir. MBSE kullanımı, yakıt besleme sistemi gibi kritik sistemlerin emniyetini artırmanın yanı sıra, erken tasarım aşamalarında potansiyel risk ve hataların tanımlanmasına olanak

tanıyarak, etkili çözüm stratejilerinin geliştirilmesine imkan vermektedir. Bu yaklaşım, hava araçlarının tasarım ve işletme süreçlerinde bir paradigma değişikliği yaratmayı amaçlamakta, böylelikle araçların daha güvenli ve emniyetli bir şekilde kullanımını mümkün kılmaktadır.

MBSE'nin bu derinlemesine uygulaması, emniyet çalışmalarının sadece teorik bir çerçeveden ibaret olmadığını, aynı zamanda pratikte de uygulanabilir ve etkili sonuçlar doğurabilecek bir metodoloji olduğunu kanıtlamaktadır.

2.9.1. Sistem Mimarisi



Şekil 2.29. Sistem mimarisi.

Hava araçlarının emniyetli ve etkin bir şekilde işletilmesinde, yakıt sisteminin rolü hayati öneme sahiptir. Bu sistem, çok çeşitli kritik görevleri yerine getirirken, özellikle motor besleme fonksiyonu, yakıt sisteminin en kritik bileşenlerinden biri olarak öne çıkmaktadır. Motorun sürekli ve güvenilir bir şekilde yakıt ile beslenmesini sağlayan bu fonksiyon, hava aracının performansı ve emniyeti açısından temel bir unsur olarak Kabul edilmektedir.

Bu bölümde Şekil 2.29 ile birlikte gösterilen motor besleme sisteminin genel mimarisi incelenmektedir. Analiz edilen mimari, iki adet yakıt tankı, iki adet pompa, iki adet tek yönlü vana (İng. non-return valve, NRV) ve dört adet kesme vanası ile birlikte normal besleme ve çapraz besleme hattı içermektedir.

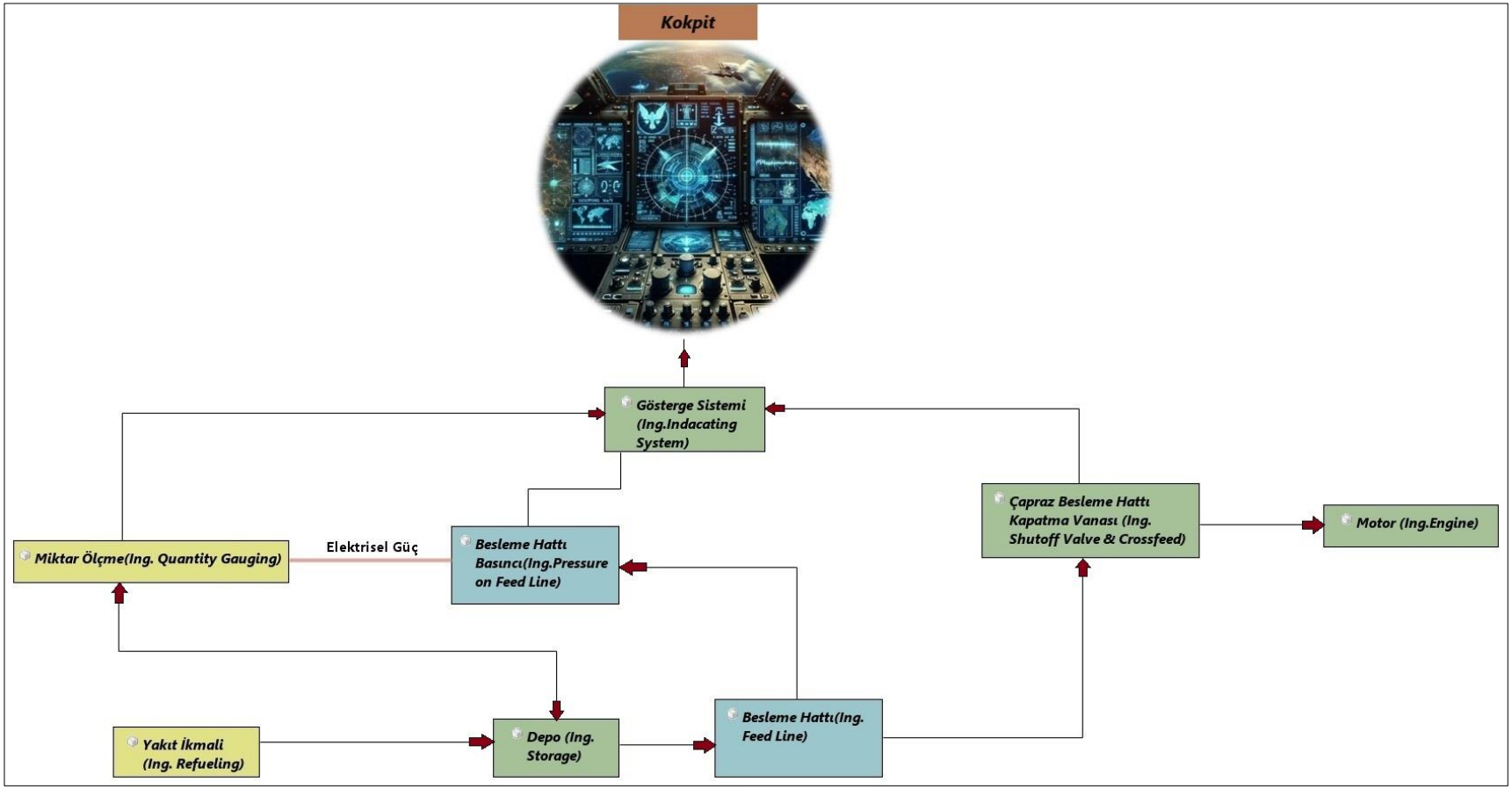
Motorlar (Motor 1 ve Motor 2): Sistemde iki motor bulunmaktadır. Bunlar, sol tarafta "Motor 2" ve sağ tarafta "Motor 1" olarak etiketlenmiştir. Bu motorlar, aracın itiş gücünü sağlarlar ve yakıtı yakarak mekanik enerji üretirler.

- Yakıt Tankları (Sağ Tank ve Sol Tank): Her bir motorun yanında birer yakıt tankı bulunmaktadır. Bu tanklar, motorların ihtiyacı olan yakıtı depolar.
- Pompalar (M ile işaretlenmiş daireler): Her bir yakıt hattında, yakıtı tanklardan motorlara taşıyan pompalar bulunmaktadır.
- Boru Hatları ve Bağlantılar (Kırmızı hatlar): Kırmızı hatlar, yakıtın tanklardan motorlara taşındığı boru hatlarını temsil eder. Ayrıca, bu hatlar arasındaki bağlantılar, yakıtın her iki tanktan da her iki motora ulaşabilmesine olanak tanır, bu da yakıtın dengeli bir şekilde tüketilmesini ve gerektiğinde bir tanktan diğerine transfer edilmesini sağlar.

Kesme Vanaları ve Tek Yönlü Vanalar: Yakıt hatlarında, akışı denetlemek ve yönlendirmek için çeşitli vanalar bulunur. Şekil ’de görüldüğü üzere kırmızı hatlar üzerinde vanalar bulunmaktadır. Bu vanalar, yakıt akışını düzenlemek veya durdurmak için kullanılır.

Tasarımın genel amacı, her iki motorun da çalışmasını sağlayacak şekilde yakıtın emniyetli ve güvenilir bir şekilde dağıtılmasını sağlamaktır. Ayrıca, bu tür bir tasarım esneklik sağlar; eğer bir motor veya yakıt hattı arızalanırsa, diğer tanktan yakıt sağlanarak motorun çalışmaya devam etmesi sağlanabilir. Tasarımın bir diğer önemli özelliği de, her iki tanktan da her iki motora yakıt akışına izin veren çapraz bağlantılardır. Bu, bir yakıt tankındaki olası bir sorun durumunda diğer tanktan her iki motora da yakıt sağlanabilmesine olanak tanır.

2.9.2. Fonksiyonel Blok Diyagramı



Şekil 2.30. Fonksiyonel blok diyagramı.

Şekil 2.30 üzerinde verilen diyagram, bir uçağın yakıt sisteminin genel fonksiyonlarını temsil etmektedir. Bu fonksiyonların temel bileşenleri aşağıda yer almaktadır.

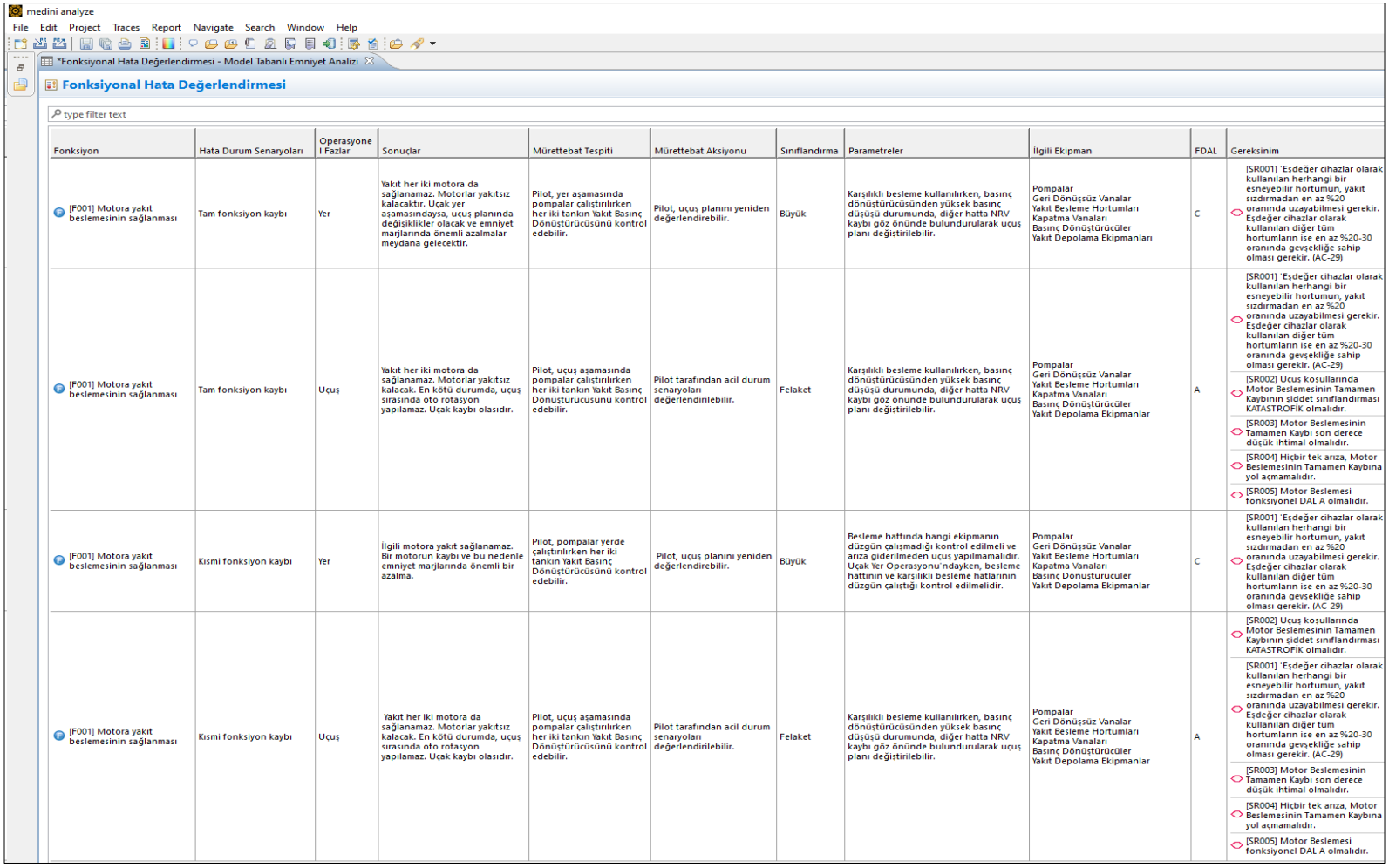
1. Yakıt İkmal (İng. Refueling): Sistemin ilk adımı yakıtın depolanmasını sağlar. Bu, yakıtın tanka doldurulduğu yerdir.
2. Depolama (İng. Storage): Yakıtın depolandığı yer, genellikle uçağın kanatları içinde bulunan yakıt tanklarıdır.
3. Yakıt Hattı (İng. Feed Line): Depolanan yakıt, motorlara ulaşana kadar bu hatlar üzerinden sevk edilir.
4. Yakıt Kesme ve Çapraz Besleme (İng. Fuel Shutoff & Crossfeed): Yakıt akışını denetleyen vanalar bulunur. Bunlar, yakıtın gerektiğinde kesilmesini veya motorlar arasında çapraz beslenme yapılmasını sağlar.
5. Motor (İng. Engine): Yakıt, yanma için motorlara ulaştıktan sonra güç üretilir.
6. Miktar Ölçümü (Quantity Gauging): Tanklardaki yakıt miktarını ölçer ve bu bilgi kokpite iletilir.
7. Gösterge Sistemi (İng. Indicating System): Pilotlar, bu sistem aracılığıyla yakıt miktarını ve basınç gibi diğer parametreleri görebilir.
8. Yakıt Hattı Üzerinde Basınç (İng. Pressure on Feed Line): Yakıt hatlarında uygun basıncın oluşmasını sağlar, bu da yakıtın motorlara düzgün bir şekilde sevk edilmesine yardımcı olur.

Bu sistemin genel çalışma prensibi, yakıtın ikmalinden itibaren motorlara kadar olan yolculuğunu ve bu süreçteki çeşitli denetleme noktalarını içerir. Pilot, gösterge sistemi aracılığıyla yakıt seviyesini ve basıncını izleyebilir ve yakıt kesme vanalarını kullanarak yakıt akışını yönetebilir.

2.9.3. Fonksiyonel Hata Değerlendirmesi

Şekil 2.31. ile gösterilen FHA çalışmasında, mimari ve fonksiyonel blok diyagramlarından seçilen motor besleme fonksiyonuna odaklanarak, bu fonksiyon üzerinden kapsamlı bir hata değerlendirmesi gerçekleştirilmiştir. Emniyet analizi sürecinde, öncelikle fonksiyonel hata değerlendirmesi yapılarak genel hata modları incelenmiştir. Bu hata modları; fonksiyonun tamamen kaybı ve kısmi kaybı şeklinde tanımlanmıştır.

Değerlendirme sürecinde, hava aracının çeşitli operasyonel fazları göz önünde bulundurulmuş, özellikle yer ve uçuş fazları detaylı bir şekilde değerlendirilmiştir. FHA yapılırken, analiz edilen operasyonel fazlarda en kötü senaryolar dikkate alınmış ve bu senaryoların etkileri ayrıntılı bir şekilde incelenmiştir. Elde edilen bulgulara göre, mürettebatın potansiyel hata durumlarını tespit edebilme kapasitesi ve bu durumlarda alınacak aksiyonlar belirlenmiştir.

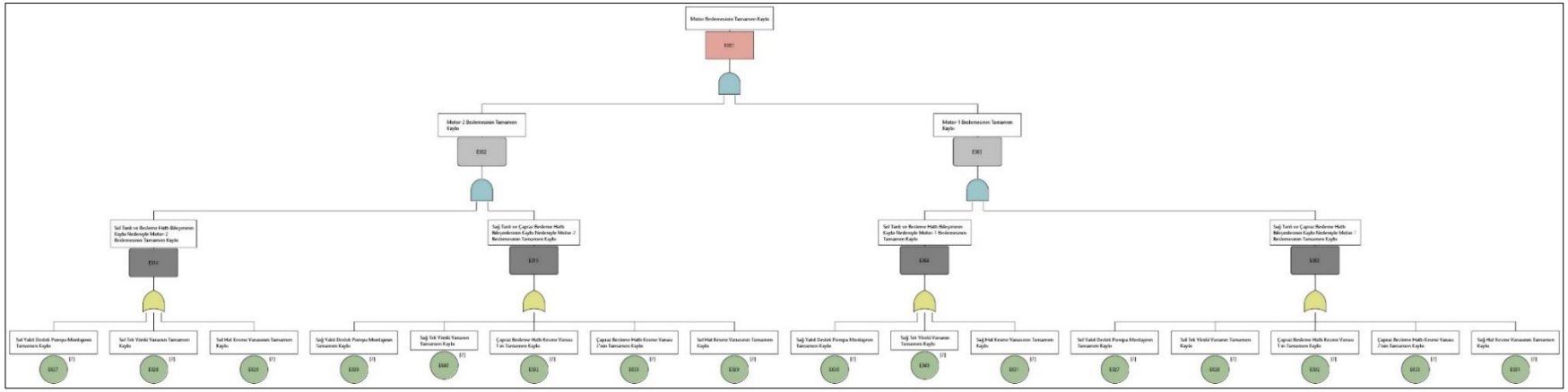


Fonksiyon	Hata Durum Senaryoları	Operasyonel Fazlar	Sonuçlar	Mürettebat Tespiti	Mürettebat Aksiyonu	Sınıflandırma	Parametreler	İlgili Ekipman	FDAL	Gereksinim
[F001] Motora yakıt beslemesinin sağlanması	Tam fonksiyon kaybı	Yer	Yakıt her iki motora da sağlanamaz. Motorlar yakıtsız kalacaktır. Uçak yer aşamasındaysa, uçuş planında değişiklikler olacak ve emniyet marjlarında önemli azalmalar meydana gelecektir.	Pilot, yer aşamasında pompalar çalıştırılırken her iki tankın Yakıt Basınç Dönüştürücüsünü kontrol edebilir.	Pilot, uçuş planını yeniden değerlendirebilir.	Büyük	Karşılıklı besleme kullanılırken, basınç dönüştürücüsünden yüksek basınç düşüşü durumunda, diğer hatta NRV kaybı göz önünde bulundurularak uçuş planı değiştirilebilir.	Pompalar Geri Dönüşsüz Vanalar Yakıt Besleme Hortumları Kapatma Vanaları Basınç Dönüştürücüler Yakıt Depolama Ekipmanları	C	[SR001] 'Eşdeğer cihazlar olarak kullanılan herhangi bir esneyebilir hortumun, yakıt sızdırmadan en az %20 oranında uzayabilmesi gerekir. Eşdeğer cihazlar olarak kullanılan diğer tüm hortumların ise en az %20-30 oranında gevşekliğe sahip olması gerekir. (AC-29)
[F001] Motora yakıt beslemesinin sağlanması	Tam fonksiyon kaybı	Uçuş	Yakıt her iki motora da sağlanamaz. Motorlar yakıtsız kalacak. En kötü durumda, uçuş sırasında oto rotasyon yapılamaz. Uçak kaybı olasıdır.	Pilot, uçuş aşamasında pompalar çalıştırılırken her iki tankın Yakıt Basınç Dönüştürücüsünü kontrol edebilir.	Pilot tarafından acil durum senaryoları değerlendirilebilir.	Felaket	Karşılıklı besleme kullanılırken, basınç dönüştürücüsünden yüksek basınç düşüşü durumunda, diğer hatta NRV kaybı göz önünde bulundurularak uçuş planı değiştirilebilir.	Pompalar Geri Dönüşsüz Vanalar Yakıt Besleme Hortumları Kapatma Vanaları Basınç Dönüştürücüler Yakıt Depolama Ekipmanlar	A	[SR001] 'Eşdeğer cihazlar olarak kullanılan herhangi bir esneyebilir hortumun, yakıt sızdırmadan en az %20 oranında uzayabilmesi gerekir. Eşdeğer cihazlar olarak kullanılan diğer tüm hortumların ise en az %20-30 oranında gevşekliğe sahip olması gerekir. (AC-29) [SR002] Uçuş koşullarında Motor Beslemesinin Tamamen Kaybının şiddet sınıflandırması KATASTROFİK olmalıdır. [SR003] Motor Beslemesinin Tamamen Kaybı son derece düşük ihtimal olmalıdır. [SR004] Hiçbir tek arıza, Motor Beslemesinin Tamamen Kaybına yol açmamalıdır. [SR005] Motor Beslemesi fonksiyonel DAL A olmalıdır.
[F001] Motora yakıt beslemesinin sağlanması	Kısmi fonksiyon kaybı	Yer	İlgili motora yakıt sağlanamaz. Bir motorun kaybı ve bu nedenle emniyet marjlarında önemli bir azalma.	Pilot, pompalar yerde çalıştırılırken her iki tankın Yakıt Basınç Dönüştürücüsünü kontrol edebilir.	Pilot, uçuş planını yeniden değerlendirebilir.	Büyük	Besleme hattında hangi ekipmanın düzgün çalışmadığı kontrol edilmeli ve arıza giderilmeden uçuş yapılmamalıdır. Uçak Yer Operasyonu'ndayken, besleme hattının ve karşılıklı besleme hatlarının düzgün çalıştığı kontrol edilmelidir.	Pompalar Geri Dönüşsüz Vanalar Yakıt Besleme Hortumları Kapatma Vanaları Basınç Dönüştürücüler Yakıt Depolama Ekipmanlar	C	[SR001] 'Eşdeğer cihazlar olarak kullanılan herhangi bir esneyebilir hortumun, yakıt sızdırmadan en az %20 oranında uzayabilmesi gerekir. Eşdeğer cihazlar olarak kullanılan diğer tüm hortumların ise en az %20-30 oranında gevşekliğe sahip olması gerekir. (AC-29)
[F001] Motora yakıt beslemesinin sağlanması	Kısmi fonksiyon kaybı	Uçuş	Yakıt her iki motora da sağlanamaz. Motorlar yakıtsız kalacak. En kötü durumda, uçuş sırasında oto rotasyon yapılamaz. Uçak kaybı olasıdır.	Pilot, uçuş aşamasında pompalar çalıştırılırken her iki tankın Yakıt Basınç Dönüştürücüsünü kontrol edebilir.	Pilot tarafından acil durum senaryoları değerlendirilebilir.	Felaket	Karşılıklı besleme kullanılırken, basınç dönüştürücüsünden yüksek basınç düşüşü durumunda, diğer hatta NRV kaybı göz önünde bulundurularak uçuş planı değiştirilebilir.	Pompalar Geri Dönüşsüz Vanalar Yakıt Besleme Hortumları Kapatma Vanaları Basınç Dönüştürücüler Yakıt Depolama Ekipmanlar	A	[SR002] Uçuş koşullarında Motor Beslemesinin Tamamen Kaybının şiddet sınıflandırması KATASTROFİK olmalıdır. [SR001] 'Eşdeğer cihazlar olarak kullanılan herhangi bir esneyebilir hortumun, yakıt sızdırmadan en az %20 oranında uzayabilmesi gerekir. Eşdeğer cihazlar olarak kullanılan diğer tüm hortumların ise en az %20-30 oranında gevşekliğe sahip olması gerekir. (AC-29) [SR003] Motor Beslemesinin Tamamen Kaybı son derece düşük ihtimal olmalıdır. [SR004] Hiçbir tek arıza, Motor Beslemesinin Tamamen Kaybına yol açmamalıdır. [SR005] Motor Beslemesi fonksiyonel DAL A olmalıdır.

Şekil 2.31. FHA program görüntüsü.

2.9.4. PSSA Kapsamında FTA

Şekil 2.32.Şekil 2.32. ile gösterilen FTA çalışmasında, motor besleme fonksiyonunun kaybının nedenlerini ve bu nedenlerin birbirleriyle olan ilişkilerini incelemektedir. Fonksiyon kaybının ciddiyeti, FHA çalışmasında "Felaket (İng. catastrophe)" olarak değerlendirilmiş, bu sebeple bir hata ağacı analizi yapılmıştır. Hata ağacının en tepesinde yer alan ana (birincil hata) olay, motor beslemesinin tamamen kaybıdır ve bu ana hata olayı detaylı bir şekilde incelenmektedir. Hata ağacının alt kısımlarında, bu ana olayın meydana gelmesine neden olabilecek hata bileşenleri ve alt olaylar ayrıntılı bir şekilde ele alınmaktadır. Diyagramda kullanılan “VE” ve “VEYA” kapıları, belirli hata olaylarının bir arada (VE) veya tek başlarına (VEYA) gerçekleşmelerinin ana olayın meydana gelmesine nasıl yol açtığını göstermektedir. Her bir olay ve bileşen için özel hata durumları belirtilmiştir.



Şekil 2.32. Nitel FTA program görüntüsü.

2.9.5. Hata Modu, Etkileri ve Kritiklik Analizi

Bu aşamada, yakıt kesme vanası gibi kritik bir sistem bileşeninin güvenilirliği ve emniyeti üzerine odaklanan FMECA çalışmasının önemi ve etkisi ele alınmaktadır. FMECA, sistem emniyeti ve güvenilirliğinin artırılması amacıyla kritik bir analiz yöntemi olarak öne çıkar. Bu çalışma, FHA sürecinin bir parçası olarak, motor besleme fonksiyonunun hayati ekipmanlarından biri olan yakıt kesme vanasının potansiyel hata modlarını ve bu hataların sistem üzerindeki etkilerini derinlemesine incelemektedir.

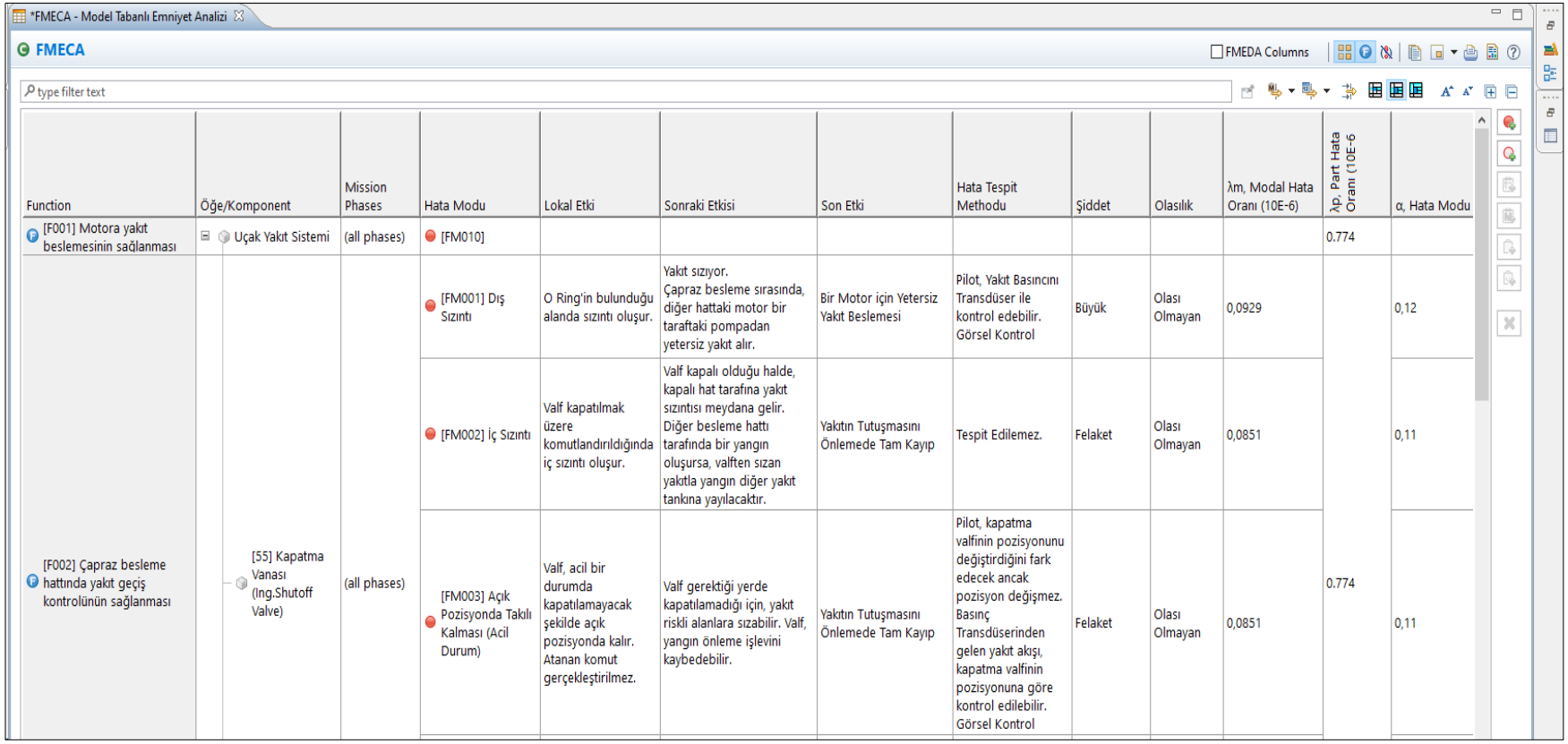
Özellikle iç sızıntı gibi belirli arıza modlarına yönelik önerilen risk azaltma önlemleri, sistem performansının korunması ve olası zararların en aza indirilmesi açısından büyük önem taşımaktadır. Bu önlemler, hata olasılığını düşürmek ve sistem güvenilirliğini artırmak amacıyla tasarlanmıştır.

FMECA çalışması, hata modlarının şiddetini ve olasılığını değerlendirerek, hangi hataların öncelikli olarak ele alınması gerektiği konusunda rehberlik sağlamaktadır. Bu yöntem, kaynakların en etkili biçimde kullanılmasını sağlayarak, en kritik risklerin azaltılmasına odaklanmaktadır. Çalışmada belirtilen felaket etkisine sahip yüksek şiddetli hatalar, acil müdahale gerektiren durumlar olarak dikkat çekmektedir.

Bu çerçevede, FMECA analizinin değerlendirilmesi, sistem tasarımı ve bakım stratejilerinin geliştirilmesinde önemli bir rol oynamaktadır. Risk azaltma önlemlerinin uygulanması, sistemin genel güvenilirliğini ve performansını önemli ölçüde iyileştirebilir. Ayrıca, bu analiz gelecekteki tasarım iyileştirmeleri için değerli bilgiler sağlayarak potansiyel hata noktalarını erken bir aşamada belirleme imkânı sunmaktadır.

Şekil ile gösterilen çalışmada kritiklik analizi ve nicel FTA için gerekli olan veriler, yakıt kesme vanasının hata oranlarının Quenterion programı aracılığıyla hesaplanmasıyla elde edilmiştir. Bu programda hata oranı hesaplanırken, vananın kullanıldığı ortamın özellikleri ve bu ortamın analiz için uygunluğu dikkate alınmaktadır. Program, FMECA çalışmasında kullanılan hata modu oranlarını sağlayarak, her bir hata modunun modal hata oranını hesaplamaktadır.

Sonuç olarak, FMECA çalışması, yakıt kesme vanası gibi kritik sistem bileşenlerinin güvenilirliğini ve emniyetini artırmada temel bir adımı temsil etmektedir. Hata modlarının, etkilerinin ve şiddetlerinin detaylı analizi, riskleri azaltma ve sistem performansını optimize etme yolunda önemli bir rehber sunmaktadır. Bu çalışma, sistemin uzun vadeli güvenilirliğini sağlamak amacıyla gereken iyileştirmelerin ve önlemlerin belirlenmesinde kilit bir kaynak olarak kabul edilmelidir.



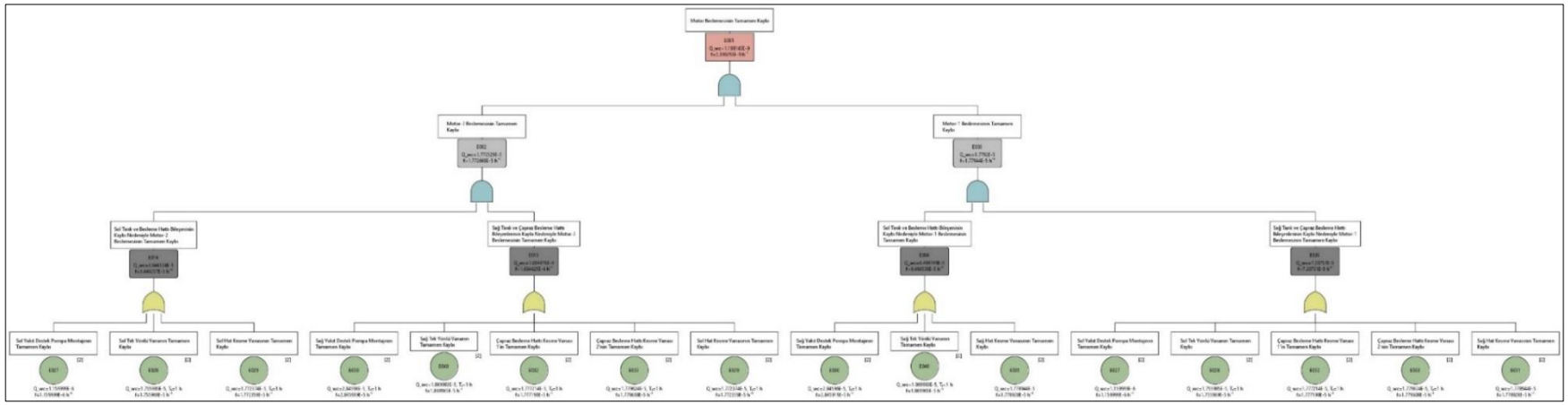
Function	Öğe/Komponent	Mission Phases	Hata Modu	Lokal Etki	Sonraki Etkisi	Son Etki	Hata Tespit Methodu	Şiddet	Olasılık	λm, Modal Hata Oranı (10E-6)	λp, Part Hata Oranı (10E-6	α, Hata Modu
[F001] Motora yakıt beslemesinin sağlanması	Uçak Yakıt Sistemi	(all phases)	[FM010]								0.774	
[F002] Çapraz besleme hattında yakıt geçiş kontrolünün sağlanması	[55] Kapatma Vanası (Ing.Shutoff Valve)	(all phases)	[FM001] Dış Sızıntı	O Ring'in bulunduğu alanda sızıntı oluşur.	Yakıt sızıyor. Çapraz besleme sırasında, diğer hattaki motor bir taraftaki pompadan yetersiz yakıt alır.	Bir Motor için Yetersiz Yakıt Beslemesi	Pilot, Yakıt Basıncını Transdüser ile kontrol edebilir. Görsel Kontrol	Büyük	Olası Olmayan	0,0929	0.774	0,12
			[FM002] İç Sızıntı	Valf kapatılmak üzere komutlandırıldığında iç sızıntı oluşur.	Valf kapalı olduğu halde, kapalı hat tarafına yakıt sızıntısı meydana gelir. Diğer besleme hattı tarafında bir yangın oluşursa, valften sızan yakıtla yangın diğer yakıt tankına yayılacaktır.	Yakıtın Tutuşmasını Önlemede Tam Kayıp	Tespit Edilemez.	Felaket	Olası Olmayan	0,0851		0,11
			[FM003] Açık Pozisyonda Takılı Kalması (Acil Durum)	Valf, acil bir durumda kapatılamayacak şekilde açık pozisyonda kalır. Atanan komut gerçekleştirilmez.	Valf gerektiği yerde kapatılamadığı için, yakıt riskli alanlara sızabilir. Valf, yangın önleme işlevini kaybedebilir.	Yakıtın Tutuşmasını Önlemede Tam Kayıp	Pilot, kapatma valfinin pozisyonunu değiştirdiğini fark edecek ancak pozisyon değişmez. Basınç Transdüserinden gelen yakıt akışı, kapatma valfinin pozisyonuna göre kontrol edilebilir. Görsel Kontrol	Felaket	Olası Olmayan	0,0851		0,11

Şekil 2.33. FMECA çalışması program görüntüsü.

[F002] Çapraz besleme hattında yakıt geçiş kontrolünün sağlanması		[55] Kapatma Vanası (Ing.Shutoff Valve)	(all phases)	[FM003] Açık Pozisyonda Takılı Kalması (Acil Durum)	Valf, acil bir durumda kapatılamayacak şekilde açık pozisyonda kalır. Atanan komut gerçekleştirilmez.	Valf gerektiği yerde kapatılamadığı için, yakıt riskli alanlara sızabilir. Valf, yangın önleme işlevini kaybedebilir.	Yakıtın Tutuşmasını Önlemede Tam Kayıp	Pilot, kapatma valfinin pozisyonunu değiştirdiğini fark edecek ancak pozisyon değişmez. Basınç Transdüserinden gelen yakıt akışı, kapatma valfinin pozisyonuna göre kontrol edilebilir. Görsel Kontrol	Felaket	Olası Olmayan	0,0851		0,11
				[FM004] Açık Pozisyonda Takılı Kalması (Besleme Durumu)	Valf, besleme durumunda açık pozisyonda kalacak ve kapatılamayacak. Atanan komut gerçekleştirilmez.	Motor besleme durumunda Valf açık kalsa bile operasyonel bir etkisi olmayacak.	Operasyonel bir etkisi yoktur.	Pilot, kapatma valfinin pozisyonunu değiştirdiğini fark edecek ancak pozisyon değişmez. Basınç Transdüserinden gelen yakıt akışı, kapatma valfinin pozisyonuna göre kontrol edilebilir. Görsel Kontrol	Emniyet Açısından Etkisi Yoktur.	Olası Olmayan	0,0851	0.774	0,11
				[FM005] Kapalı Pozisyonda Takılı Kalması (Besleme Durumu)	Besleme durumunda, vana kapalı konumda kalır ve açılmaz.	Çapraz besleme sırasında, diğer hatta bulunan motor bir tarafın pompasından beslenemez.	Motor Beslemesinin Kısmi Kaybı Tespit Edilemeyen Yanlış Yakıt Sistemi Durumu Geri Bildirimi	Pilot, kapatma vanasının pozisyonu değişse de pozisyonun değişmediğini fark edecek. Basınç Transdüserinden yakıt akışı, kapatma vanasının pozisyonuna göre	Büyük	Olası Olmayan	0,0851		0,11
[F002] Çapraz besleme hattında yakıt geçiş kontrolünün sağlanması		[55] Kapatma Vanası (Ing.Shutoff Valve)	(all phases)	[FM006] Kapalı Pozisyonda Takılı Kalması (Acil Durum)	Acil bir durumda vana kapalı konumda kalır	Acil bir durumda vana kapalı olduğundan operasyonel bir etki olmayacak.	Operasyonel bir etkisi yoktur.	Pilot, kapatma vanasının pozisyonu değişse de pozisyonun değişmediğini fark edecek. Basınç Transdüserinden yakıt akışı, kapatma vanasının pozisyonuna göre kontrol edilebilir. Görsel Kontrol	Emniyet Açısından Etkisi Yoktur.	Olası Olmayan	0,0851		0,11
				[FM007] Aşırı Basınç Düşüşü	Vana, motoru yakıtla besleme işlevini kısmen kaybeder.	Akış hızı ve basınç azalır.	Motor Beslemesinin Yetersiz Olması	Pilot, kapatma vanasının pozisyonu değişse de pozisyonun değişmediğini fark edecek. Basınç Transdüserinden yakıt akışı, kapatma vanasının pozisyonuna göre kontrol edilebilir. Görsel Kontrol	Büyük	Olası Olmayan	0,0851	0.774	0,11
				[FM008] Kırık	Yapısal bütünlük bozulur.	Yakıt sızıntısı yapar. Çapraz besleme sırasında, diğer hatta bulunan motor bir tarafın pompasından yetersiz beslenir.	Bir Motor İçin Yetersiz Yakıt Beslemesi	Pilot, kapatma vanasının pozisyonu değişse de pozisyonun değişmediğini fark edecek. Basınç Transdüserinden yakıt akışı, kapatma vanasının pozisyonuna göre kontrol edilebilir.	Büyük	Olası Olmayan	0,0851		0,11

Şekil 2.33. (devam ediyor).

2.9.6. SSA Kapsamında FTA



Şekil 2.34. Nicel FTA program görüntüsü.

Nicel FTA kapsamında, her bir ekipmanın hata oranı, MEDINI programı kullanılarak hesaplanıp ağaca dahil edilmiştir. Şekil 2.34. ile gösterilen Sistem Emniyet Değerlendirmesi (SSA) kapsamındaki bu analizin temel amacı, incelenen sistemin emniyet ve güvenilirlik hedeflerinin karşılanabilirliğini ve doğrulanmasını sağlamaktır. Analizde belirtildiği üzere, "VE" kapısının altında yer alan olayların hata oranları çarpılırken, "VEYA" kapısının altındaki olayların hata oranları toplanmaktadır. Bu hesaplamaların sonucunda, ağacın en üstünde yer alan olayın hata oranı, 2.396×10^{-9} olarak hesaplanmıştır.

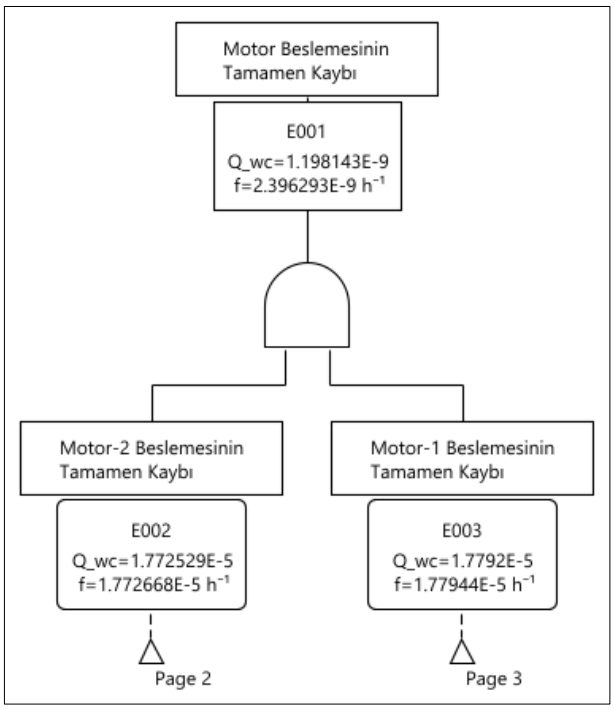
Şekil 2.34 üzerinde yer alan hata ağacının aşamalı olarak gösterilimi Şekil 2.35-2.41 üzerinde gösterilmiştir. Bu hata ağacı genel olarak aşağıda yer alan bilgileri özetleyen bir nitelik taşımaktadır.

1. Şekil 2.35 ile gösterilen En Üst Seviye Olay (Motor Beslemesinin Tamamen Kaybı - E001):
    - Bu olayın gerçekleşme olasılığı *QWC* ve beklenen sıklığı (frekans) *f*, alt sistemlerin birleşik etkisiyle hesaplanmıştır. Bu değerlerin hesaplanmasında "VE" kapıları kullanılmıştır. Çünkü bu kapılar, bağlı olayların tümünün gerçekleşmesi gerektiğini gösterir.
    - Motor beslemesinin kaybının olasılığı, alt sistemlerdeki hataların birleşik etkisine bağlıdır ve bu da sistemdeki kritik bağımlılıkları göstermektedir.
2. Şekil 2.36 ve Şekil 2.37 ile gösterilen İlk Seviye Alt Olaylar (Motor-2 ve Motor-1 Beslemesinin Kaybı - E002 ve E003):
    - Her motor beslemesinin kaybı için olasılık ve frekans değerleri, bu motorların bağımsız sistemler olduğunu ve ayrı ayrı değerlendirilmesi gerektiğini göstermektedir.
    - Bu seviyedeki alt olaylar genellikle "VE" kapıları ile bağlanır, çünkü bu olayların her biri en üst seviye olayın (Motor Beslemesinin Tamamen Kaybı - E001) gerçekleşmesine doğrudan katkıda bulunmaktadır.

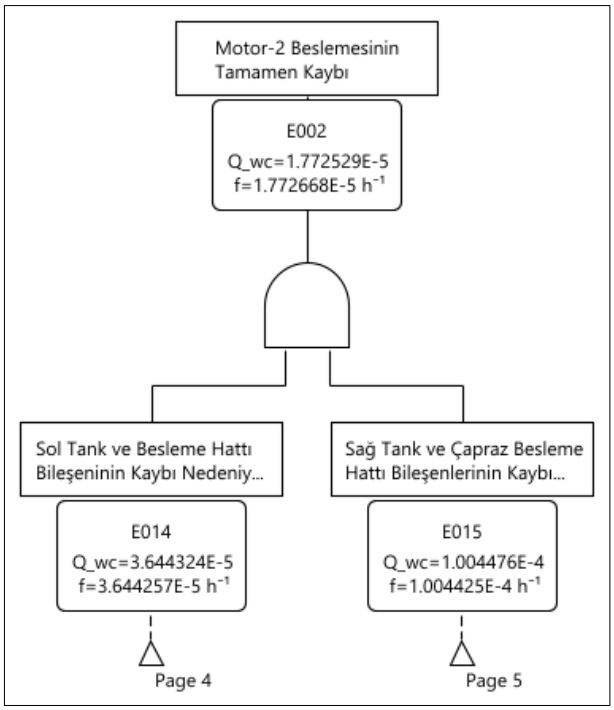
3. Şekil 2.38 ve Şekil 2.39 ile gösterilen İkinci Seviye Alt Olaylar (Sol ve Sağ Tank/Besleme Hattı Bileşenlerinin Kaybı - E014, E015, E004, E005):
    - İkinci seviyedeki alt olaylar, daha spesifik hata modlarının incelendiği yerdir. Buradaki her bir alt olayın gerçekleşmesi, ilgili üst seviye olayın olasılığını artırmaktadır.
    - Bu seviyede, "VEYA" kapıları kullanılarak bir üst seviye olayın birden fazla alt seviye olayın birleşiminden kaynaklanabileceği gösterilmektedir.
4. Şekil 2.40 ve Şekil 2.41 ile gösterilen Ayrıntılı Alt Olaylar (Örneğin: E027, E028, E030, E031, E032, E033, E040):
    - Bu seviyedeki her olay, belirli bir alt sistem veya bileşenin hatasını temsil etmektedir.
    - Arızaların olasılık (*QWC*) ve frekans (*f*) değerleri, genellikle detaylı istatistiksel verilere ve geçmiş olaylara dayanmaktadır.
    - Her bir bileşenin olasılığı ve frekansı, genel sistem performansı üzerindeki etkisini değerlendirmede kullanılır ve bu değerler, bu bileşenlerin düzenli bakım veya değişim ihtiyacını ortaya koymaktadır.

Genel olarak, bu FTA çalışması aşağıdaki bilgileri içerir:

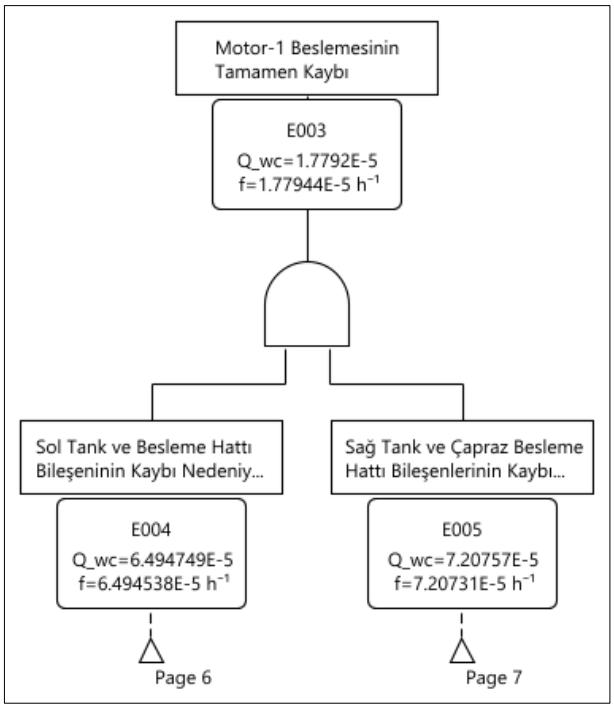
- Sistemdeki her bir bileşen ve alt sistemlerin hata modları detaylı bir şekilde tanımlanmıştır.
- Her bir hata modunun olasılığı ve sisteme etkisi, yani frekansı, nitel olarak ifade edilmiştir.
- Bu değerler, her bir bileşenin sistem güvenilirliğine olan katkısını ve risk seviyesini belirlemede yardımcı olur.
- Motor beslemesinin tamamen kaybı gibi bir en üst olay, çoklu alt sistem ve bileşen hatalarının birleşiminden kaynaklanabilir.
- Sistemin daha emniyetli hale getirilmesi için hangi bileşenlerin riskini azaltmaya odaklanılması gerektiği, bu analiz ile belirlenmektedir.



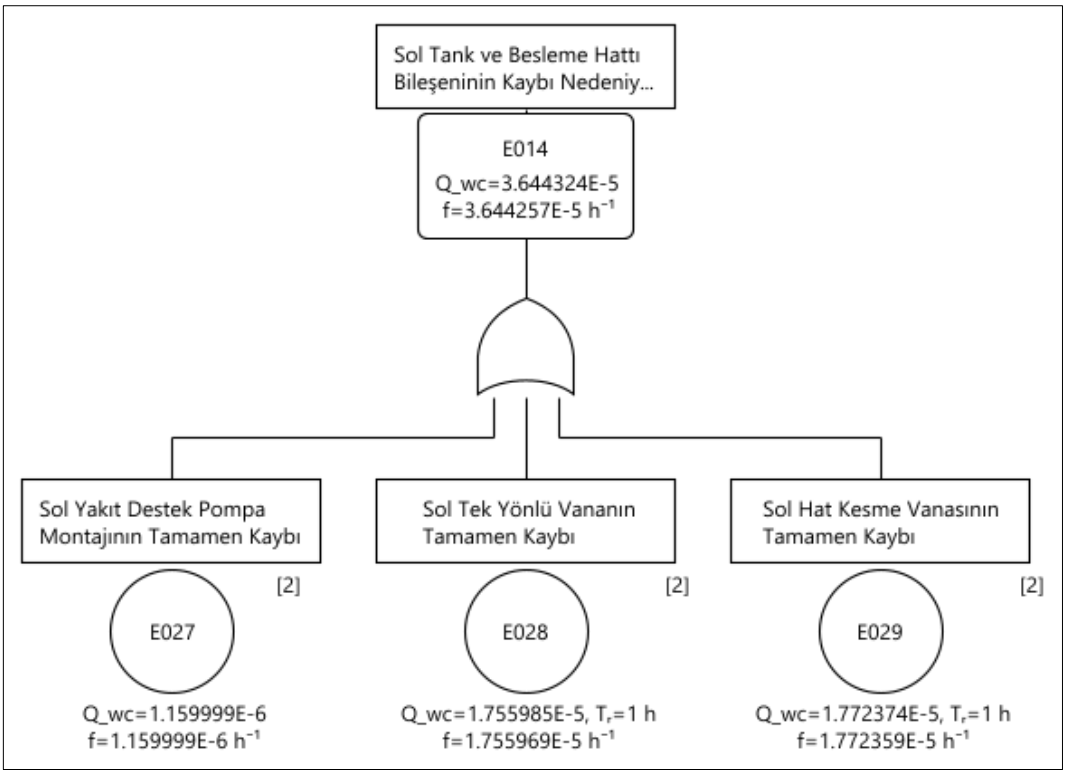
Şekil 2.35. Nicel FTA 1. Bölüm.



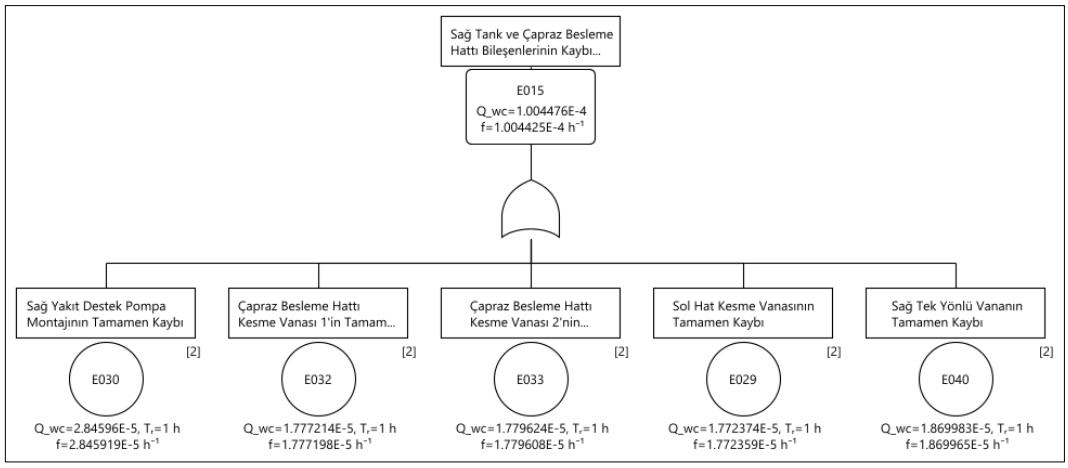
Şekil 2.36. Nicel FTA 2. Bölüm.



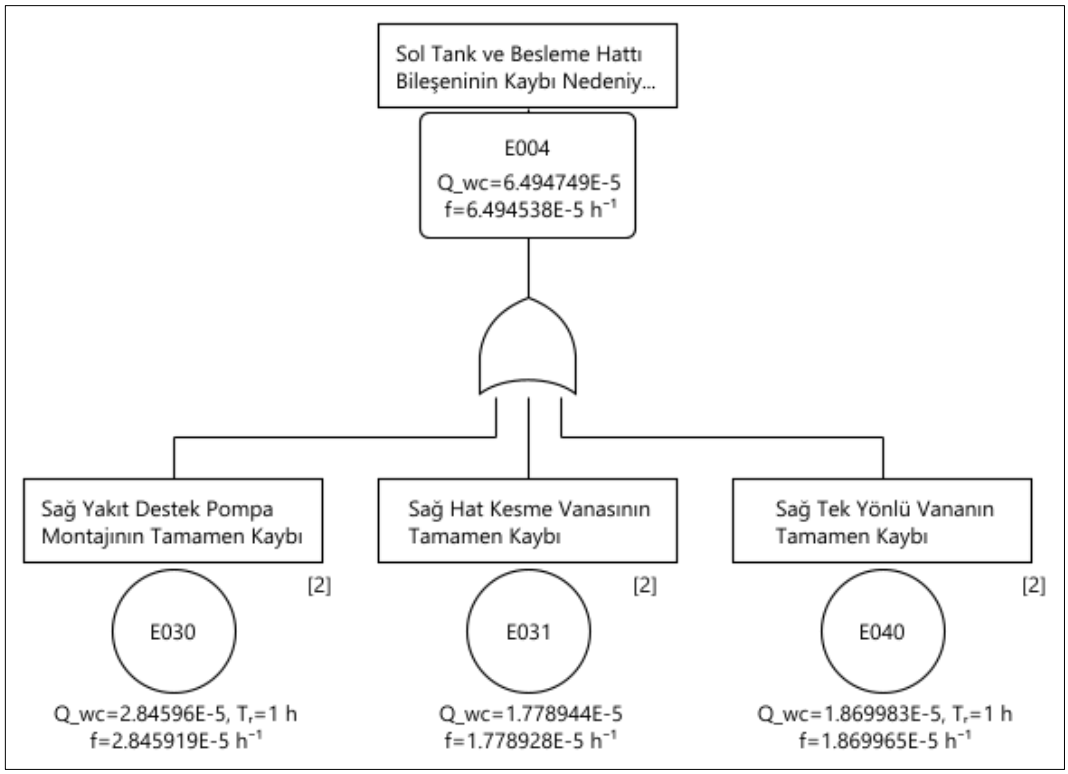
Şekil 7 Nicel FTA 3. Bölüm.



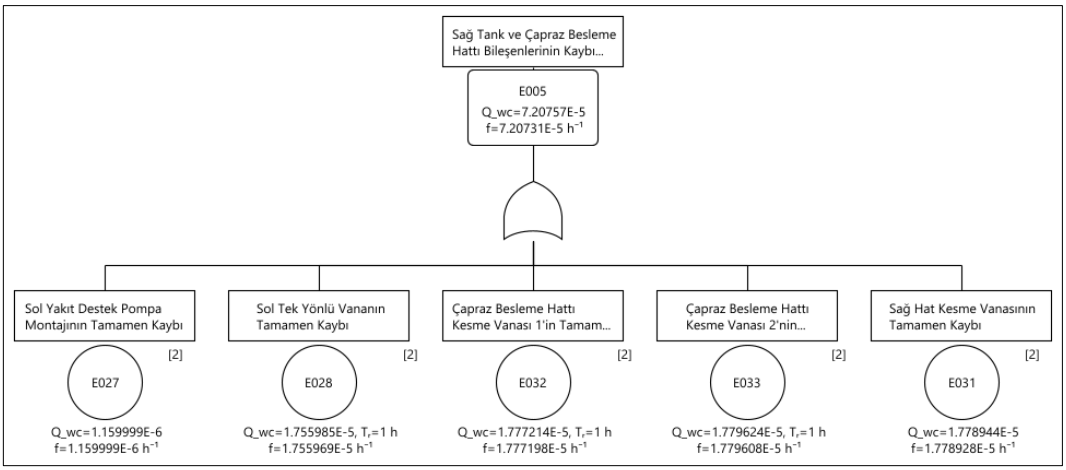
Şekil 2.38. Nicel FTA 4. Bölüm.



Şekil 2.39. Nicel FTA 5. Bölüm.



Şekil 2.40. Nicel FTA 6. Bölüm.



Şekil 2.41. Nicel FTA 7. Bölüm.

BÖLÜM 3

TARTIŞMA VE SONUÇ

Bu çalışma, hava araçlarının yakıt sistemlerinin emniyet ve güvenilirlik analizlerinde Model Tabanlı Emniyet Çalışmaları (MBSE) metodolojisinin ve Ansys Medini programının uygulanabilirliğini derinlemesine incelenmiştir. MBSE yaklaşımının entegrasyonu, emniyet analiz süreçlerinde kapsamlılık ve detay seviyesinde önemli iyileştirmeler sağlamıştır. Motor Besleme Mimarisi ve ilgili Fonksiyon Mimarisi'nin oluşturulmasından FHA, Nitel FTA, ve FMECA ve Nicel FTA analizlerine kadar genişletilen süreçler, emniyet değerlendirme metodolojisinin nasıl detaylandırıldığını ve entegre edildiğini somut örneklerle göstermiştir.

Analizler, özellikle yakıt sistemi gibi kritik sistemlerde, geleneksel yöntemlere kıyasla MBSE'nin sunduğu üstünlükleri ortaya koymuştur. Emniyet ve güvenilirlik analizlerindeki bu metodolojik ilerleme, erken tasarım aşamalarında potansiyel risklerin ve hataların tespit edilmesini mümkün kılmakta, bu sayede etkili çözüm ve önlem stratejilerinin geliştirilmesine olanak tanımaktadır. Bu yaklaşım, hava araçlarının tasarım süreçlerinde, daha yüksek emniyet standartlarına ulaşılmasını destekleyen bir paradigma değişikliğini teşvik etmektedir.

Sonuç olarak, bu tez, MBSE ve Ansys Medini programının kullanımıyla, hava araçlarının yakıt sistemlerinin emniyet ve güvenilirlik değerlendirmelerinde sağladığı katkıları kanıtlamaktadır. Bu çalışma, emniyet analiz süreçlerinde metodolojik bir ilerleme sunarken, aynı zamanda hava araçlarının daha emniyetli ve güvenilir kullanımı için kritik bir adımı temsil etmektedir. Bu nedenle, emniyet çalışmalarının teorik temellerin ötesine geçerek pratikte de uygulanabilir ve etkili sonuçlar doğurabilecek bir metodoloji olduğu açıkça gösterilmiştir.

KAYNAKLAR

1. Hu, B., Liang, Q., Zhong, D. and Wang, H. “The safety assessment process of carrier aircraft's control system”, ***2016 Prognostics and System Health Management Conference (PHM-Chengdu)***, Chengdu, 1-4 (2016).

2. Sun, Q. “Safety Assessment of Civil Aircraft Lighting System”, ***2022 IEEE 2nd International Conference on Data Science and Computer Application (ICDSCA)***, Dalian, 830-833 (2022).

3. Yu, B., Wu, S., Jiao, Z., Shang, Y. and Zhou, Y. “Safety analysis of actuation system of more electric aircraft”, ***CSAA/IET International Conference on Aircraft Utility Systems (AUS 2018)***, Guiyang, 1511-1516 (2018).

4. Haider, S. “Applying Model Based Safety Assessment for Aircraft Landing Gear System Certification”, ***2020 Annual Reliability and Maintainability Symposium (RAMS)***, Palm Springs, 1-7 (2020).

5. Jiang, Y., Bai, N., Yang, H., Zhang, H., Wang, Z. and Liu, X. “MBSE-based functional hazard assessment of civil aircraft braking system”, ***2020 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE)***, Harbin, 460-464 (2020).

6. Xiao, N., Wang, P., Tian, Y. and Ma, Z. “Research and application of Preliminary System Safety Assessment on civil airborne systems”, ***2011 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering***, Xi'an, 562-566 (2011).

7. Biswaws, P. and Shrimali, S.C. “Safety assessment of modern aircraft-a case study”, ***Annual Reliability and Maintainability Symposium. 2001 Proceedings. International Symposium on Product Quality and Integrity*** (Cat. No.01CH37179), Philadelphia, 365-371 (2001).

8. Caldwell, R.E. and Merdgen, D.B. “Zonal analysis: the final step in system safety assessment (of aircraft)”, ***Annual Reliability and Maintainability Symposium. 1991 Proceedings***, Orlando, 277-279 (1991).

9. Ye, Q. and Lu, P. “Comprehensive Design and Investigation of Civil Aircraft Reliability/Maintainability/Safety/Testability Engineering”, ***2021 Global Reliability and Prognostics and Health Management (PHM-Nanjing)***, Nanjing, 1-5 (2021).

10. Rong, H. and Dong, H. “Incorporating Model Based Safety Design into Development Process of Civil Aircraft Systems”, ***2019 IEEE 19th International Conference on Communication Technology (ICCT)***, Xi'an, 1291-1295 (2019).

11. Xiao, N. and Zhang, Y. “Comparative study on the safety assessment technology between civil airborne system and railway signal system”, ***The Proceedings of 2011 9th International Conference on Reliability, Maintainability and Safety***, Guiyang, 538-543 (2011).

12. Salihler, S.G. “System safety analysis as decision making tool for aircraft systems”, ***2016 Annual Reliability and Maintainability Symposium (RAMS)***, Tucson, 1-4 (2016).

13. Gradel, S., Aigner, B. and Stumpf, E. “Model-based safety assessment for conceptual aircraft systems design”, ***CEAS Aeronautical Journal***, 13, 281–294 (2022).

14. Tye, W. and Lloyd, T. “Is it Safe? The Safety Assessment of Aircraft Systems”, ***Aircraft Engineering and Aerospace Technology***, Vol. 53 No. 2, pp. 15-17 (1981).

15. Yoo, S. and Kim, I.-G. “A Study on the Implementation of Aircraft System Safety Assessment using Probabilistic Analysis of Failure Data”, ***Journal of Aerospace System Engineering***, 14(spc), 31–38 (2020).

16. Koo, M.-S. “A Study on the Application of Operational Experience in the Stage of Aircraft System Design and Safety Assessment”, ***Journal of the Korean Society for Aviation and Aeronautics***. The Korean Society for Aviation and Aeronautics (2014).

17. Kang, M.S., Cheon, Y.S., Koh, D.W. and Choi, N.S. “System Safety Assessment for KC-100 Civil Aircraft”, ***Journal of the Korean Society of Systems Engineering***, 1-13 (2010).

18. Lee, K.-C., Lee, J.-H., Yi, B.-J. and Yoo, S.-W. “A Study on the System Safety Assessment of Aircraft”, ***Journal of Applied Reliability***, 89-100 (2007).

19. Lee, K., Yoo, S.-W. and Kim, K.-S. “Safety Assessment for Aircraft Engines”, ***Journal of the Korean Society of Propulsion Engineers***, 26-34 (2007).

20. Ustaömer, T.C. ve Şengür, F. “Havacılıkta Emniyet Kültürü: Reason'ın Emniyet Kültürü Modelinin İncelenmesi”, ***Anemon Muş Alparslan Üniversitesi Sosyal Bilimler Dergisi***, 8(1), 95-104.

21. Yılmaz, A.K. “Havacılıkta Emniyet açısından Risk yönetimi Ve havacılık örgütlerinden Uygulama örnekleri”, ***Anadolu Üniversitesi***, Türkiye (2003).

22. Akdağ, M.S. “Türkiye’de Hava Araci Sertifikasyon Süreçleri –Hürkuş Örneği”, Yüksek Lisans Tezi, ***İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü***, İstanbul, 30-40 (2015).

23. Ayyıldız, P. “MIL-STD-882E’ye Dayalı Risk Değerlendirme Metodolojisi”, ***Ix. Ulusal Uçak, Havacılık ve Uzay Mühendisliği Kurultayı Bildiriler Kitabı***, Ankara, 122-134 (2017).

24. Gözay, N.G. “Sivil Havacılıkta Ürün ve Organizasyonların Sertifikasyonu”, ***VII. Ulusal Uçak, Havacılık ve Uzay Mühendisliği Kurultayı***, Eskişehir, 197-208 (2013).

25. SAE. “Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment,” ***ARP 4761***, (Dec. 1996).

26. SAE. “Guidelines for Development of Civil Aircraft and Systems”, ***ARP 4754A***, (2010).

27. “Department of Defence Standard Practice: System Safety.” ***MIL-STD-882E***, (2012).

28. “Department of Defence Standard Practice For System Safety”, ***MIL-STD-882D***, (2000).

29. “Certification Standard Large Aircraft and AMC25.1309.”

30. SAE. “Recommended Failure Modes and Effects Analysis (FMEA) Practices for Non-Automobile Applications”, ***ARP 5580*** (2020).

31. “Military Standard: Procedures for Performing A Failure Mode, Effects, And Criticality Analysis”, ***MIL-STD-1629A*** (1980).

32. RTCA. “Software Considerations in Airborne Systems and Equipment Certification”, ***DO-178B*** (1992).

33. RTCA and EUROCAE. “Design Assurance Guidance for Airborne Electronic Hardware”, ***DO-254***, Washington (2000).

34. Rgwcherry And Associates, *“System Safety Assessment Course”,* Cranfield University (2019).

35. SAE, "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment", ***ARP 4761***, United States of America (1996).

36. Australian Government Civil Aviation Authority, ***AC 21-39 Design and Fitting of Gaseous Oxygen Systems*** Version 1.0, Australia (2015).

37. National Transportation Safety Board, "Aircraft Accident Report, United Airlines Flight 232, McDonnell Douglas DC-10-10, Sioux Gateway Airport, Sioux City, Iowa, July 19, 1989," **NTSB/AAR-SO/06**. Retrieved 2011-02-19

38. Federal Aviation Administration, "Japan Airlines Flight 123, Boeing 747-SR100, JA8119", 12 August 1985. Retrieved 2013-09-10.

39. Stratejik Araştırmalar Merkezi, "Havacılığın İlk Yılları Üzerine", **https://strasam.org/** (2024).

40. İnternet: Wikipedia, "International relations (1919–1939)", **en.wikipedia.org** (2023).

41. İnternet: Vikipedi, "II. Dünya Savaşı", **tr.wikipedia.org** (2023).

42. İnternet: Vikipedi, "Havacılık tarihi", **tr.wikipedia.org** (2023).

43. İnternet: Allianz, "How aviation safety has improved", **commercial.allianz.com** (2023).

44. İnternet: Aero Crew News, "The Evolution of Aviation Safety", **aerocrewnews.com** (2023).

45. İnternet: RD Aero Systems, "The History of Aviation Safety", **www.hrd-aerosystems.com** (2023).

46. İnternet: Britannica, "Tenerife airline disaster", **www.britannica.com** (2023).

47. İnternet: Britannica, "Air France flight 4590", **www.britannica.com** (2023).

48. İnternet: International Civil Aviation Organization, "Safety Management", **icao.int** (2023).

49. İnternet: RTCA/DO-356, "Airworthiness Security Process Specification," RTCA, Inc., United States of America (2014) (2023).

ÖZGEÇMİŞ

Sergen OĞUZ İlköğretim ve Lise eğitimini Ankara'da tamamladı. 2013 yılında Karabük Üniversitesi Mühendislik Fakültesi Raylı Sistemler Mühendisliği bölümüne başladı ve 2018 yılında mezun oldu. 2024 Yılı Ocak ayı itibari ile "Uçak Tasarım Aşamasında Model Tabanlı Emniyet Analizi Süreci" isimli tez çalışması ile yüksek lisans derecesi onandı.