Hava Aracı Tasarımında Emniyet Gereksinimlerine Uyumun Önemi

Sezgin DURAK
STM A.Ş. Sertifikasyon Müdürlüğü
sdurak@stm.com.tr

Nazan GÖZAY GÜRBÜZ
STM A.Ş. Sertifikasyon Müdürlüğü
ngurbuz@stm.com.tr

Hava aracı kazaları sonucunda can, mal kayıplarının yanında havacılık şirketlerinin itibarıda doğrudan etkilenmektedir. Kazaların direk ve dolaylı maliyetlerinin hava aracı maliyetlerinin çok üzerinde olması üreticilerin, hava aracı tasarım ve üretimlerinde emniyet kapsamında yaptıkları çalışmaları daha zorlayıcı hale getirmesine neden olmuştur. Ayrıca havacılık otoritelerinin koyduğu emniyet gereksinimlerine uyum gösterebilmek için rehber dokümanlar oluşturmalarına neden olmuştur.

Hava aracı geliştirme ve tasarım esnasında yapılabilecek değişikliklerin sürecin başlangıcından sonuna doğru ciddi bir şekilde maliyeti arttırdığı bilinmektedir. Literatürde “the rule of ten” ve ya “do it right the first time” olarak geçen tanımlara göre genel olarak her bir tasarım adımı arasında geri dönüş maliyetlerinde yaklaşık 10 katlık bir fark meydana gelmektedir. Bir projede konsept tasarım aşamasında yapılacak bir değişiklik ile, ön tasarım arasında yaklaşık 10 kat, kritik tasarım aşaması ile yaklaşık 100 katlık maliyet farkı oluşacaktır. Bu maliyetlerden kurtulmanın yolu tasarım geri dönüşlerini minumuma indirmek ve emniyet gereksinimlerini karşılayacak tasarım çözümlerini sağlayabilmektir.

Tasarlanan hava aracı tipine göre minimum emniyet gereksinimleri havacılık otoriteleri tarafından oluşturulan uçuşa elverişlilik standartlarında belirtilmektedir. Uçuşaelverişlilik ve kalifikasyon gereksinimleri karşılandığında müşteri ihtiyaçlarını karşılayan emniyetli bir hava aracı üretilmiş olmaktadır. Bir hava aracının kendisinden beklenen görev gereksinimlerini karşılayabilmesi için öncelikle uçuşa elverişli olması gerekmektedir. CSXX.1309 uçuşaelverişlilik standartları içersindeki bir çok gereksinimden biri olmakla birlikte tüm hava aracı sistemlerini ilgilendiren ve sistematik bir emniyet süreci sonucunda oluşturulan bir dizi emniyet analizi neticesinde karşılananbilen bir gereksinimdir. Bu makalede CS 25.1309 gereksiniminin zorunlu kıldığı emniyet çalışmalarının neler olduğu, bu çalışmaların ne zaman yapılması gerektiği ile ilgili süreç anlatılmaktadır. Bu gereksinimi karşılayabilmek için otoriteler tarafından kabul görmüş rehber standartlar SAE ARP 4761 ve 4754 dür. Bu rehber dokümanlarda uçuşa elverişlilik stanadartlarında yer alan emniyet gereksinimlerine tasarımda nasıl uyum gösterileceğine yönelikler yöntemler yer almaktadır.

Sonuç olarak maliyet etkin emniyetli bir tasarımın başarı ile tamamlanmasının en önemli yolu emniyet çalışmalarının projenin ilk aşamalarından başlayarak sonuna kadar sistematik bir süreç ile yürütülmesidir.

Uçuşa Elverişlilik Standartları

Hava araçları tasarımında emniyetin sağlanmasına yönelik uçak tipine göre değişen çeşitli standartlar bulunmaktadır. Bu standartlardan bazıları çizelge 1'de verilmiştir.

Çizelge 1: Hava araçları sertifikasyonunda kullanılan bazı standartlar

Kategori	UE STANDARTLARI EASA	FAA	ASKERİ
Hafif Uçaklar	CS VLA		MIL-HDBK-516B DEF-STAND
Hafif Döner Kanatlar	CS VLR		
Küçük Uçaklar	CS 23	FAR 23	
Büyük Uçaklar	CS 25	FAR 25	
Küçük Döner Kanatlar	CS 27	FAR 27	
Büyük Döner Kanatlar	CS 29	FAR 29	
Motor	CS E	FAR 33	
Pervane	CS P	FAR 35	

Bu çalışmada CS 25 kapsamına giren uçaklar için CS 25.1309 gereksinimine uyumun tasarım sürecinde nasıl ele alındığı değerlendirilmektedir.

CS 25.1309'a Uyum Gösterimi

CS 25 uçuşa elverişlilik standardı genellikle taşımacılık amacıyla kullanılan büyük uçakların sertifikasyonu için uyum gösterilmesi gereken gereksinimleri içermektedir.

Bu gereksinimler arasında sistem emniyetini doğrudan ilgilendiren gereksinim 1309'dur. Bu çalışmada 1309'a uyumun nasıl gösterilebileceği anlatılmaktadır.

1309'maddesi üç alt maddeden oluşmaktadır. Çizelge 2'de gereksinim alt maddelere bölünerek verilmiştir.

Çizelge 2: CS 25.1309 gereksiniminin içeriği

CS 25.1309
(a) The aeroplane equipment and systems must be designed and installed so that: (1) Those required for type certification or by operating rules, or whose improper functioning would reduce safety, perform as intended under the aeroplane operating and environmental conditions. (2) Other equipment and systems are not a source of danger in themselves and do not adversely affect the proper functioning of those covered by sub-paragraph (a)(1) of this paragraph.
(b) The aeroplane systems and associated components, considered separately and in relation to other systems, must be designed so that; (1) Any catastrophic failure condition (i) is extremely improbable; and (ii) does not result from a single failure; and (2) Any hazardous failure condition is extremely remote; and (3) Any major failure condition is remote.
(c) Information concerning unsafe system operating conditions must be provided to the crew to enable them to take appropriate corrective action. A warning indication must be provided if immediate corrective action is required. Systems and controls, including indications and annunciations must be designed to minimize crew errors, which could create additional hazards.

Çizelge 2'de verilmiş olan 1309 gereksiniminin detaylı olarak analizi ve uyum gösterim yöntemleri aşağıdaki bölümlerde verilmiştir.

1309 (a) Gereksinimine Uyum Gösterilmesi

Gereksinimin ana maddesinde (a) uçak ekipman ve sistemlerinin (a)(1) ve (a)(2)'de verilmiş olan gereksinimleri karşılayacak şekilde tasarlanması ve uçağa entegre edilmesi gerektiği vurgulanmaktadır. (a)(1) ve (a)(2)'de ne istendiğine bakılmaksızın bu gereksinime uyumlu bir tasarımın otoriteye gösterilebilineceği ilk doküman sistem tanımlama dokümanlarıdır(SDD). SDD'lerde tasarım ve enstalasyon ile ilgili detaylar yer almaktadır. Ancak, burada yer alan bilgilerin doğrulanması amacıyla ihtiyaca göre analiz, test, ekipman özellik belgesi vb. de hazırlanarak SDD'lerden referans verilebilir.

(a)(1) gereksiniminde belirtilen uçak ekipman ve sistemlerinin en azından çizelge 3'deki üç gruptan birine giriyor olması gerekmektedir;

Çizelge 3: 1309 (a)(1) gereksinimine uyması beklenen ekipman / sistemler

No	Grup İçeriği
1	Tip Sertifikası için gerekli olan ekipman / sistemler (Uçağın teslim edilecek tip sertifikasında yazılı olacak ekipman / sistemler)
2	Operasyonel Kurallar için gerekli olan ekipman / sistemler (Havacılık kuralları ve uçağın yapacağı operasyonlara özgü kurallara göre gerekli olabilecek ekipman / sistemler)
3	Uygun olmayan(fonksiyon kaybı, fonksiyonun yanlış ve ya istemsiz çalışması) davranışının emniyeti etklileyeceği ekipman / sistemler (Emniyet analizleri neticesinde belirlenmiş olan ekipman / sistemler)

Gruplara bakılacak olursa bazı ekipmanlar birden fazla gruba girebilmektedir. Örneğin uçakta yer alması gereken dış haberleşme sistemi üç grup için de gereklidir. Ancak, iç haberleşme sistemi tasarıma göre değişmekle birlikte 1. ve 3. grupta yer alabilmektedir. Sonuç, olarak herhangibir ekipman ve ya sistem bu üç gruptan birine giriyorsa (a)(1)'de istenen gereksinime uygun bir şekilde tasarlanmalı ve uçağa entegre edilmelidir.

(a)(1) gereksinimi ile istenen ise belirlenmiş olan ekipmanların uçağın operasyonel ve çevresel koşulları altında kendilerinden beklenen performansı gösteriyor olmasıdır. Bu gereksinimin doğrulanabilmesi için uçağın operasyonel ve çevresel koşullarının belirlenmiş ve bu koşulların ekipman/sistem seviyesinde detaylandırılmış olması gerekmektedir. Uçağın hangi operasyonları hangi şartlarda gerçekleştireceğinin açıklandığı bir doküman hazırlanmalıdır. Bu dokümana çizelge 4'deki kaynaklardan girdi sağlanabilir;

Çizelge 4: Uçağın maruz kalacağı şartların ve ekipman / sistemlerin performans gereksinimlerinin belirlenebileceği kaynaklar

No	Grup İçeriği
1	Sözleşme gereksinimleri
2	Sertifikasyon gereksinimleri
3	Operasyonel kural gereksinimleri
4	İlk 3 maddede yeterli detayı bulunmayan gereksinimler için kullanıcı girdileri

Uçağın maruz kalacağı çevresel koşulların belirlenmesinden sonra, her bir ekipmanın takılacağı bölgede maruz kalacağı koşullar belirlenmelidir. Ekipman / sistemlerin kalifiye olduğu çevresel şartlar uçağın ömür döngüsü boyunca maruz kalabileceği(normal ve acil durum şartları) çevresel şartlardan daha zorlayıcı olmaldır. Ekipmanın takılacağı bölgelerdeki koşullar bazen kolaylıkla belirlenebildiği gibi (uçağın dışı güneşe maruz kalıyor, içi maruz kalmıyor vb.), bazı durumlarda analiz (sıcaklık, titreşim analizi), test (laboratuar, uçak üzeri) ve muayene(mantar oluşumu gözlenmesi) yapılması gerekebilir.

Ekipmanların / sistemlerin maruz kalacağı çevresel koşullar belirlendikten sonra, her bir ekipman / sistemden istenilen performans kriterlerinin belirlenmesi gerekmektedir. Bu kriterler yine çizelge 4'de yer alan kaynaklardan temin edilebilir.

(a)(2) gereksiniminde ise, (a)(1) gereksiniminde belirlenmiş olan kritik ekipman / sistemlerin maruz kalacağı operasyonel ve çevresel şartlara uygun olarak tasarlandığının ve uçağa entegre edildiğinin doğrulanması esnasında, diğer ekipman / sistemlerin de (a)(1) maddesindeki kritik ekipman / sistemlere olumsuz etkisinin olmadığının ispatlanması gerektiği vurgulanmaktadır. Diğer ekipmanlar belirlenirken çizelge 3'deki gruplar gözönünde bulundurulur. Emniyet kritik ekipmanlar hava aracı tasarımı süresince uygulanan emniyet analizleri sonucunda belirlenmektedir. 1309 (b) ve (c) maddeleri bu analizlerin yapılmasını zorunlu kılmaktadır.

Belirlenmiş olan bu ekipman / sistemlerin çevresine fiziksel zarar vermedikleri içsel tehlike analizi (IHA) ile gösterilebilir. Ancak, IHA analizine göre halen risk oluşturan ekipman / sistemler var ise yapılacak olan Özel Risk Analizi (PRA) ve Bölgesel Emniyet Analizi (ZSA) çalışmaları ile bu riskin kabul edilebilir seviyelere indirgendiği gösterilmelidir.

1309 (b) Gereksinimine Uyum Gösterilmesi

Gereksinimin ana maddesinde (b) uçak ekipman ve sistemlerinin ayrı olarak ve diğer sistemlerle olan bağlantılarına göre (b)(1), (b)(2) ve (b)(3)'de verilmiş olan gereksinimleri karşılayacak şekilde tasarlanması gerektiği vurgulanmaktadır. Bu gereksinimde herhangi bir ekipman / sistem ayrımı yapılmamış olup, uçak üzerindeki tüm ekipman / sistemlerin değerlendirilmesi gerektiği belirtilmektedir. Tüm ekipman / sistem tasarım bilgilerinin elde edilebileceği Sistem Tasarım Tanımlama dokümanları uyum gösterimi için kullanılan dokümanlar arasında yer almaktadır. SDD içinde verilen bilgilerin doğrulanması amacıyla (a) gereksinimine uyum gösteriminde olduğu gibi ihtiyaca göre analiz, test, ekipman özellik belgesi vb. de hazırlanarak SDD'lerde referans verilebilir.

(b)(1)(2)(3) gereksinimlerinde uçak sistemlerinin kendi içlerinde ve birbirleri ile olan bağlantıları nedeniyle oluşabilecek hata durumlarının meydana gelme olasılıklarının kabul edilebilir seviyelerde olması gerektiği vurgulanmaktadır. Dolayısı ile uçak tasarımına bağlı olarak oluşabilecek tüm hata durumları belirlenmeli ve hata durumu kritikliklerine göre oluşma olasılıklarının kabul edilebilir seviyelerde olduğunun ispat edilmesi gerekmektedir. Bu durum doğru ve planlı bir şekilde işletilen emniyet süreci ile yürütülebilir.

Yapılan bir çok uçak tasarım projesinde rehber olarak kullanılan SAE ARP 4761 ve 4754 dokümanlarında emniyet süreci örnekleri ile açıklanmaktadır. SAE ARP 4761 ve 4754'e göre (b) maddesine uyum için asgaride çizelge 5'de yer alan dokümanlar hazırlanmış olmalıdır.

Çizelge 5: 1309 (b) gereksinimine uyum gösterimi için hazırlanması gereken asgari doküman listesi

No	Doküman
1	**Emniyet Planı:** Emniyet sürecinin kimler tarafından, ne zaman ve nasıl işletileceğinin anlatıldığı dokümandır.
2	**Ortak Bilgi Dokümanı (CDD):** Emniyet analizleri esnasında uçağa ait kullanılacak tüm bilgilerin yer aldığı dokümandır. Bu doküman emniyet analizleri haricinde yürütülen tüm çalışmalarda da kullanılmalıdır. Emniyet Planı'nın içeriğinde de verilebilir.
3	**Fonksiyonel Tehlike Değerlendirmeleri (FHA):** Uçak ve Sistem seviyesinde olmak üzere hazırlanabilir. Genel olarak hata durumlarının belirlenmesi, bu hata durumlarına kritiklik atanması, bu hata durumlarına karşılık mürettebatın tespit yöntemleri ve uygulayacağı prosedürler belirlenmektedir. Ayrıca, 1309 (b) maddesine göre ilk emniyet gereksinimlerinin oluşturulduğu dokümandır.
4	**Ön Sistem Emniyet Değerlendirilmesi(PSSA):** Tasarımın FHA çalışmasında belirlenmiş olan emniyet gereksinimleri karşılayabileceğinin öngörüldüğü dokümandır. 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.
5	**Sistem Emniyet Değerlendirmesi(SSA):** FHA ve PSSA çalışmaları neticesinde oluşturulmuş olan emniyet gereksinimlerine sistemin uyum gösterdiği bu dokümanda verilmektedir.
6	**Ortak Sebep Analizleri (CCA):** FTA analizleri ile yedeklenmiş olarak gösterilen ekipman / sistemlerin yedekliliğinin gerçekte varolduğunun gösterilmesi ve FHA'de 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) dokümanlardan oluşmaktadır. FTA çalışmalarında ekipmanların belli koşullar (sıcaklık, titreşim, nem vb.) çalıştığı kabulüne göre MTBF değerleri atanmaktadır. Bu koşulların uçağın ömrü boyunca değişmeyeceği PRA ve ZSA çalışmaları neticesinde teminat altına alınır.

(b)(1)(i) gereksinimi meydana gelebilecek ölümcül (Catastrophic) bir hata durumunun son derece ihtimal dışı (extremely improbable) bir olasılığa sahip olması gerektiğini vurgulamaktadır. Hata durumunun kritikliğinin (Örneğin catastrophic) ve bu kritikliğe karşılık kabul edilebilir olasılık seviyesinin (Örneğin extremely improbable) belirlenmesinde AMC 25.1309'da verilmiş tablo kullanılmaktadır. Bu tablo çizelge 6'da verilmiştir.

Bu gereksinime uyum için çizelge 5'de verilmiş olan FHA dokümanı hazırlanarak tüm ölümcül hata durumları belirlenir ve bu hata durumları birer emniyet gereksinimine dönüştürülür. Örnek çizelge 7'de verilmiştir.

Çizelge 6: Hata durumlarının kritikliği ve olasılıkları arasındaki ilişki

Effect on Aeroplane	**Effect on Occupants excluding Flight Crew**	**Effect on Flight Crew**	**Allowable Qualitative Probability**	**Allowable Quantitative Probability:** ***(Average Probability per Flight Hour on the Order of)***	**Classification of Failure Conditions**
No effect on operational capabilities or safety	Inconvenience	No effect on flight crew	No Probability Requirement	No Probability Requirement	No Safety Effect
Slight reduction in functional capabilities or safety margins	Physical discomfort	Slight increase in workload	Probable	10^{-3}	Minor
Significant reduction in functional capabilities or safety margins	Physical distress, possibly including injuries	Physical discomfort or a significant increase in workload	Remote	10^{-5}	Major
Large reduction in functional capabilities or safety margins	Serious or fatal injury to a small number of passengers or cabin crew	Physical distress or excessive workload impairs ability to perform tasks	Extremely Remote	10^{-7}	Hazardous
Normally with hull loss	Multiple fatalities	Fatalities or incapacitation	Extremely Improbable	10^{-9}	Catastrophic

Note 1: A numerical probability range is provided here as a reference. The applicant is not required to perform a quantitative analysis, nor substantiate by such an analysis, that this numerical criteria has been met for Minor Failure Conditions. Current transport category aeroplane products are regarded as meeting this standard simplyby using current commonly-accepted industry practice.

(b)(1)(ii) gereksinimi de ölümcül bir hata durumunun sistemde meydana gelebilecek tek hatadan oluşmadığının ispatını istemektedir. (b)(1)(i) gereksinimine uyum gösteriminde olduğu gibi, FHA'de ölümcül olarak belirlenmiş hata durumlarından ilgili emniyet gereksinimi oluşturulur. Örnek, çizelge 7'de verilmiştir.

(b)(2) ve (b)(3) gereksinimlerine uyum gösterimi için de benzer yol izlenmektedir. Örnek çizelge 7'de verilmiştir.

Çizelge 7: FHA'de oluşturulmuş 1309 (b) kapsamındaki emniyet gereksinimleri örneği

Hata Durumu ve İlgili Emniyet Gereksinimi Numaraları	**Hata Durumu ve Emniyet Gereksinimi İçeriği (Seviye 1)**
Hata Durumu X	Bildirimsiz hatalı yükseklik bilgisinin pilota gösterimi uçağın yere ve ya başka bir uçağa çarpmasına sebebiyet verebilir. Dolayısı ile bu hata durumunun etkisi ölümcül olacaktır.
Emniyet Gereksinimi X (b)(1)(i)	*Bildirimsiz hatalı yükseklik bilgisinin pilota gösterimi son derece ihtimal dışı olmalıdır.*
Emniyet Gereksinimi X (b)(1)(ii)	*Bildirimsiz hatalı yükseklik bilgisinin pilota gösterimi tek hatadan kaynaklanmamalıdır.*
Hata Durumu Y	Bildirimli hatalı yükselik bilgisinin pilota gösterimi pilotun iş yükünde çok önemli bir artışa sebebiyet verebilir. Dolayısı ile bu hata durumunun etkisi tehlikeli olacaktır.
Emniyet Gereksinimi Y (b)(2)	*Bildirimli hatalı yükselik bilgisinin pilota gösterimi son derece uzak ihtimal olmalıdır.*
Hata Durumu Z	Yükseklik bilgisinin sadece birincil göstergelerden kaybı pilotun iş yükünde önemli bir artışa sebebiyet verebilir. Dolayısı ile bu hata durumunun etkisi önemli olacaktır.
Emniyet Gereksinimi Z (b)(3)	*Yükseklik bilgisinin sadece birincil göstergelerden kaybı uzak ihtimal olmalıdır.*

Oluşturulmuş emniyet gereksinimlerinin tasarım tarafından karşılanabileceği öncelikli olarak PSSA analizinde gösterilmektedir. Bu analizde her bir emniyet gereksinimine karşılık FT(Hata Ağacı) çizilmektedir. PSSA aşamasında birden fazla tasarım alternatifi olabilir. Dolayısı ile emniyet ve maliyet unsurları gözönünde bulundurularak kullanıcı isterlerini asgaride sağlayan tasarım alternatifleri denenerek, en iyi çözüm seçilmiş olur.

“Emniyet Gereksinimi X (b)(1)(i)” ve “Emniyet Gereksinimi X (b)(1)(ii)”’ gereksinimleri bir alt seviyeye kırılarak ekipman / parçalara indirgenecek emniyet hedeflerinin elde edilmesi sağlanmış olur. Kırılım çizelge 8’de verilmiştir.

Çizelge 8: FHA'de oluşturulmuş emniyet gereksinimlerinin bir alt seviyeye kırılmış örnekleri

Emniyet Gereksinimi Numaraları	**Emniyet Gereksinimi İçeriği (Seviye 1 'den 2 'ye)**
Emniyet Gereksinimi X (b)(1)(i)	Bildirimsiz hatalı yükseklik bilgisinin pilota gösterimi son derece ihtimal dışı olmalıdır.
Emniyet Gereksinimi X (b)(1)(i).1	*Bildirimsiz hatalı yükseklik bilgisinin pilota gösterim olasılığı 10^{-9} /uçuş saati'nden düşük olmalıdır.*
Emniyet Gereksinimi X (b)(1)(i).2	*Yükseklik bilgisinin ve bu bilginin doğruluğu statüsünün aynı anda pilota iletilmesi fonksiyonunun FDAL'ı A olmalıdır.*
Emniyet Gereksinimi X (b)(1)(ii)	Bildirimsiz hatalı yükseklik bilgisinin pilota gösterimi tek hatadan kaynaklanmamalıdır.
Emniyet Gereksinimi X (b)(1)(ii).1	*Yükseklik bilgisinin ve bu bilginin doğruluğu statüsünün aynı anda pilota iletilmesi fonksiyonu birbirinden bağımsız en az iki kaynak tarafından sağlanmalıdır.*
Emniyet Gereksinimi X (b)(1)(ii).2	*Yükseklik bilgisinin ve bu bilginin doğruluğu statüsünün aynı anda pilota iletilmesi fonksiyonu sağlayan bağımsız kaynakların ortak bir dış etken nedeniyle aynı anda hata yapma olasılığı son derece ihtimal dışı olmalıdır.*

FT'lerın tekbaşına nicel ve nitel değerlendirmelerde kullanılması uygun değildir. Özellikle hata ağacında "tekrarlayan olaylar (repeated event)" var ise hata durumunu ifade eden "Minimum Cut Set (MCS)" elde edilmeli ve değerlendirmeler MCS üzerinden yapılmalıdır.

MCS'lerin elde edilmesi ile ilgili detaylı bilgi SAE ARP 4761 dokümanında bulunmaktadır. Şekil 1'de çizilmiş olan FT'nin MCS'i çizelge 9'da verilmiştir.

Burada verilen örnekler makalenin uzamaması için kısa tutulmuştur. Daha detaylı örnekler SAE ARP 4761 dokümanında bulunabilir. Şekil 1'de oluşturulmuş FT SDD yardımıyla oluşturulmuştur.

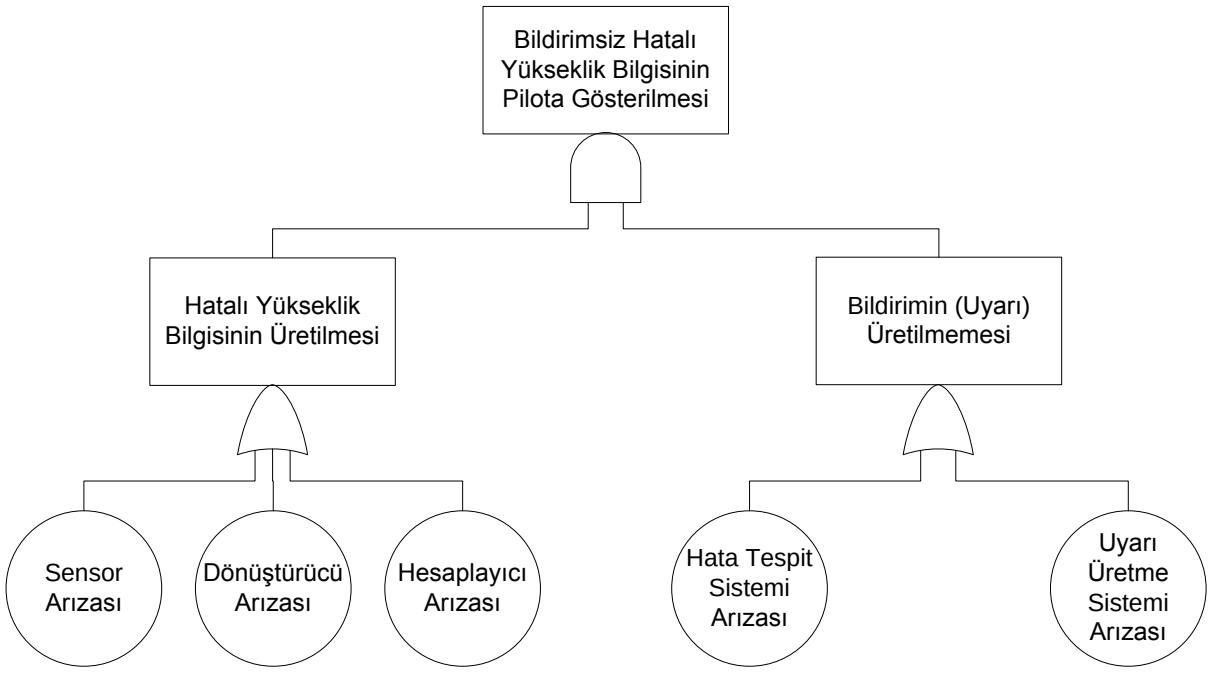
Ekipmanlara ait özellikler ve fonksiyonlar çizelge 9'da verilmiştir. PSSA aşamasında ekipman / sistemler için alternatifler olabileceği için çizelge 9'da sensör, hesaplayıcı ve hata tespit sistemi için iki seçenek sunulmuştur. FTA analizi neticesinde asgari emniyet seviyesini sağlayan ekipmanlar seçilmiş olacaktır. Ayrıca, ekipman farklılığının yanı sıra sistemin çalışma mantığı da farklı olabilir. Ancak, örneğin basit tutulması adına sistem çalışma mantığı tek tip olarak belirlenmiştir.

Çizelge 9: Örnek gösterge sistemi için ekipmanların özellikleri

Ekipman / Parça	MTBF Değeri (saat)	Hata Oranı (/saat)	DAL Seviyesi	Fonksiyonları
Sensör1	100.000	$1x10^{-5}$	Non-Complex	Uçağın yer ile mesafesini tespit ederek analog bir veri üretir.
Sensör2	1.000.000	$1x10^{-6}$	Non-Complex	
Dönüştürücü	250.000	$4x10^{-6}$	Non-Complex	Sensör'den aldığı analog veriyi, hesaplayıcının algılayabildiği formata dönüştürür.
Hesaplayıcı1	10.000	$1x10^{-4}$	DAL-B	Dönüştürücüden aldığı veriyi bünyesindeki algoritma yardımı ile yükseklik verisine dönüştürerek pilotun izlediği ekranlara gönderir.
Hesaplayıcı2	100.000	$1x10^{-5}$	DAL-B	
Hata Tespit Sistemi1	100.000	$1x10^{-5}$	DAL-C	Hesaplayıcıdan aldığı verileri kendi bünyesindeki algoritma yardımı ile değerlendirerek hata tespiti yapar. Hata tespit etmiş ise bir uyarı sinyali üreterek uyarı üretme sistemine gönderir.
Hata Tespit Sistemi2	100.000	$1x10^{-5}$	DAL-B	
Uyarı Üretme Sistemi	100.000	$1x10^{-5}$	Non-Complex	Hata tespit sistemi'nden aldığı sinyali sesli ve görsel olarak pilota iletir.

FTA hesaplamalarında MTBF(Mean Time Between Failure) değerleri yerine hata oranı (1/MTBF) değeri kullanılmaktadır.

Şekil 1: 1309 (b) gereksinimine uyum gösterimi için çizilen FTA



Çizelge 10: Şekil 1'de çizilmiş FTA'nın MCS'si

MCS No	Olay 1		Olay 2
1	Sensor arızası	**X**	Hata tespit sistemi arızası
2	Sensor arızası	**X**	Uyarı üretme sistemi arızası
3	Dönüştürücü arızası	**X**	Hata tespit sistemi arızası
4	Dönüştürücü arızası	**X**	Uyarı üretme sistemi arızası
5	Hesaplayıcı arızası	**X**	Hata tespit sistemi arızası
6	Hesaplayıcı arızası	**X**	Uyarı üretme sistemi arızası

Seçilebilecek ekipman alternatiflerine göre tasarımın emniyet gereksinimlerini karşılama durum özeti çizelge 11'de verilmiştir. Çizelge 11 şu şekilde hazırlanmıştır. Olasılık hesabı yapılırken çizelge 10'daki tüm MCS'ler dikkate alınarak alternatifi olmayan dönüştürücü ve uyarı üretme sistemi tek bir değer üzerinden hesaba katılırken, sensör, hesaplayıcı ve hata tespit sistemi (HTS) seçimlerinde çizelge 11'de verilen alternatifler üzerinden hesaplama yapılmıştır.

DAL (Development Assurance Level) atamalarının doğruluğunun hesaplanması için MCS'de her iki olayı da "Complex" olan MCS No.5 dikkate alınmıştır. Diğer MCS'lerde en az bir ekipman non-complex olduğu için DAL atamalarının değerlendirmesinde bir etkiye sahip olamamışlardır.

Çizelge 11:Şekil 1'de çizilen hata ağacının Minimum Cut Set'i

Alternatif No	Sensör Seçimi	Hesaplayıcı Seçimi	HTS Seçimi	Olasılık Değeri	DAL Atamaları
1	1	1	1	$2{,}28 \times 10^{-9}$	B x C
2	1	1	2	$2{,}28 \times 10^{-9}$	B x B
3	1	2	1	$0{,}48 \times 10^{-9}$	B x C
4	1	2	2	$0{,}48 \times 10^{-9}$	B x B
5	2	1	1	$2{,}10 \times 10^{-9}$	B x C
6	2	1	2	$2{,}10 \times 10^{-9}$	B x B
7	2	2	1	$0{,}30 \times 10^{-9}$	B x C
8	2	2	2	$0{,}30 \times 10^{-9}$	B x B

FTA ve MCS kullanılarak hangi tasarımın emniyet gereksinimlerini karşılayabileceğinin kontrolü çizelge 12'de verilmiştir. FDAL'ın karşılanması için DAL atamasının nasıl yapılacağı ile ilgili detay bilgiler SAE ARP 4754 dokümanında mevcuttur. Örnek özelinde özetlemek gerekirse FDAL A'yı karşılayabilmek için birbirinden bağımsız ve birbirinin benzeri olmayan

yedekli ekipman kullanılıyorsa her bir ekipman için DAL B seviyesi yeterli olacaktır. Bir ekipmanın DAL A, diğerininse DAL C olması ikinci bir alternatiftir.

Çizelge 12: Emniyet gereksinimlerinin tasarım alternatiflerine göre karşılanma durumu

Emniyet Gereksinimi	Gereksinimi Karşılayan Alternatifler
Emniyet Gereksinimi X (b)(1)(i).1	3, 4, 7 ve 8
Emniyet Gereksinimi X (b)(1)(i).2	2, 4, 6 ve 8
Emniyet Gereksinimi X (b)(1)(ii).1	Tümü
Emniyet Gereksinimi X (b)(1)(ii).2	CCA analizi sonuçlarına göre belirlenecektir

FTA analizi sonucunda Emniyet Gereksinimi X (b)(1)(ii).2 haricindeki diğer üç gereksinime uyum konusunda PSSA kapsamında bir tasarım kararına varılabilir. Alternatif 4 ve alternatif 8 tasarımları üç emniyet gereksinimine uyum göstermede başarılı olacağı tespit edilir. Artık bu noktada maliyet unsurları düşünülerek tasarım seçimi tamamlanabilir.

Eğer ekipmanlar satın alınmak yerine yeni olarak tasarlanacak ise veya satın alınan bir ekipmana yeni bir yazılım/donanım yüklenecekse FTA ve MCS metodu ile yaklaşık MTBF değerleri ve DAL seviyesi hedefi atanabilir. Bu değerler sistem / ekipmanlar için emniyet hedefine dönüşmelidir. Örnekler çizelge 13'de verilmiştir.

Çizelge 13: FTA ve MCS yöntemini kullanarak ekipman / sistemlere atanan emniyet hedefleri

Emniyet Gereksinimi Numaraları		**Emniyet Gereksinimi İçeriği (Seviye 2 'den 3 'e)**
Emniyet Gereksinimi X (b)(1)(i).1		Bildirimsiz hatalı yükseklik bilgisinin pilota gösterim olasılığı 10^{-9} /uçuş saati'nden düşük olmalıdır.
Emniyet Gereksinimi (b)(1)(i).1.1	*X*	*Hesaplayıcı ekipmanının MTBF değeri 100.000 saat'ten az olmamalıdır.*
Emniyet Gereksinimi (b)(1)(i).1.2	*X*	*Hata Tespit Sisteminin MTBF değeri 100.000 saat'ten az olmamalıdır.*
Emniyet Gereksinimi X (b)(1)(i).2		Yükseklik bilgisinin ve bu bilginin doğruluğu statüsünün aynı anda pilota iletilmesi fonksiyonunun FDAL'ı A olmalıdır.
Emniyet Gereksinimi (b)(1)(i).2.1	*X*	*Hesaplayıcı ekipmanının HW / SW DAL seviyesi asgari B olmalıdır.*
Emniyet Gereksinimi (b)(1)(i).2.2	*X*	*Hata Tespit Sisteminin HW / SW DAL seviyesi asgari B olmalıdır.*
Emniyet Gereksinimi (b)(1)(i).2.3	*X*	*Hesaplayıcı ekipmanı ve Hata Tespit Sisteminin Yazılımları birbirinden bağımsız olmalıdır.*

FHA ve PSSA çalışmasının tasarımın ilk safhalarında tamamlanıyor olması maliyet etkin emniyetli tasarım çözümünün üretilmesinde önem arz etmektedir. PSSA çalışmalarının sağlıkli bir şekilde tamamlanabilmesi için ekipman / sistem adaylarının ve tasarım alternatiflerinin tasarımın ilk aşamalarında belirlenmiş olması gerekmektedir.

1309 (b) gereksinimine uyum gösterimi, bu gereksinimden türetilmiş emniyet gereksinimlerine SSA'lerde uyum gösterimi yapılarak tamamlanmış olur. SSA'lerin içeriği hakkında detaylı bilgi SAE ARP 4761 dokümanınıda mevcuttur.

1309 (c) Gereksinimine Uyum Gösterilmesi

Gereksinimin genel olarak FHA'lerde belirlenmiş olan uçuş ekibi hata tespit yöntemleri ve uygulanacak prosedürlerle ilgilidir.

Bir hata durumu meydana geldiğinde uygun prosedürün zamanında uygulayabilmesi için uçuş ekibi bilgilendirilmelidir. FHA'de yer alan "uçuş ekibi tespit yöntemleri" eğer bir Uyarı / İkaz / Tavsiye'ye(W/C/A) işaret ediyorsa, bu tespit yönteminin W/C/A Listesinde yer aldığı ve tasarımın bu uyarıyı doğru bir şekilde üretebildiği doğrulanmalıdır. Hatanın tespit edilmesi bir

W/C/A haricindeki durum ile (hissetme, göstergelerdeki değişimin gözlenmesi vb.) tespit edilebiliyorsa bu tespitin yapılabilirliği doğrulanmalıdır. Hatayı tespit etmiş olan uçuş ekibinin uygulayacağı prosedürün Uçuş El Kitabında yer aldığı ve prosedürün yeterliliği doğrulanmalıdır. 1309 (c) gereksinimi FHA'de yer alan hata durumu değerlendirmeleri yardımıyla alt seviyelere kırılabilir. Örnek çizelge 14'de verilmiştir.

Çizelge 14: FHA'de Oluşturulmuş 1309 (c) kapsamındaki Emniyet Gereksinimleri Örneği

Hata Durumu ve İlgili Emniyet Gereksinimi Numaraları	**Hata Durumu ve Emniyet Gereksinimi İçeriği (Seviye 1)**
Hata Durumu Y	Bildirimli hatalı yükselik bilgisinin pilota gösterimi pilotun iş yükünde çok önemli bir artışa sebebiyet verebilir. Dolayısı ile bu hata durumunun etkisi tehlikeli olacaktır. **Hata Durumu Tespit Yöntemi:** W/C/A ekranında üretilen sesli ve görsel "TBD" uyarısı ile **Uçuş Ekibi Düzeltici Hareketi:** Pilot, uçağı ATC kontrol koordinesiyle emniyetli irtifaya çıkartır. Diğer uçaklar telsiz vasıtasıyla uyarılır. Otopilot kullanılmaz. Pilot mümkün olan en yakın meydana ATC koordinesiyle yaklaşarak, uçağı görerek ve manuel olarak indirir.
Emniyet Gereksinimi Y (c).1	*Yükseklik verisinin güvenilir olmayan bir değere ulaşması durumunda pilot sesli ve görsel olarak "TBD" uyarısı ile bilgilendirilmelidir.*
Emniyet Gereksinimi Y (c).2	*Yükseklik verisinin güvenilir olmayan bir değere ulaşması durumunda uçağın emniyetini tehlikeye atmayacak bir şekilde düzeltici işlem pilota verilmelidir.*

Emniyet Gereksinimi Y (c).1'e uyum gösterimi için çeşitli yöntemler uygulanabilir. Öncelikle bu gereksinimde yer alan uyarının varlığı, W/C/A'ları içeren SDD dokümanının ilgili paragrafı referans verilerek gösterilebilir. Bir başka ifadeyle emniyet gereksinimleri ile belirlenmiş W/C/A'ların tasarımda uygulandığının izlenebilirlliği sağlanmaldır.

Bu uyarının güvenilir olmayan yükseklik verilerinde çalıştığı laboratuar testleri ile doğrulanabilir. Yükseklik verisinin hangi durumlarda güvenilir olmayacağı, analiz ve simulasyon metodları ile belirlenebilir.

Emniyet Gereksinimi Y (c).2'ye uyum gösterimi için ise varolan düzeltici işlemin Uçuş El Kitabındaki ilgili paragrafı referans verilebilir. Bu düzeltici işlemin uygun ve yeterli olduğu, uçağın emniyetini mevcut durumdan daha düşük seviyeye götürmediği analiz ve simulasyon yöntemleri ile doğrulanabilir. Her iki gereksinim için örnek uyum metodları çizelge 15'te verilmiştir.

Çizelge 15:1309 (c) kapsamında türetilmiş olan emniyet gereksinimlerini doğrulamak amacıyla kullanılabilecek uyum metodlarına örnekler

Emniyet Gereksinimi	**Uyum Metodları**	**Amaç**
Emniyet Gereksinimi Y (c).1	W/CA SDD	Uyarının varlığının ispatlanması
	W/C/A Analizi	Sınır değerlerin uygun bir şekilde belirlendiğinin ispatlanması
	W/C/A Simulasyonu & Analizi	Sınır değerlerin geçerli kılınması
	W/C/A Laboratuar Test Sonuçları	Uyarının beklendiği şekilde çalıştığının ispatlanması
Emniyet Gereksinimi Y (c).2	Uçuş El Kitabı	Prosedürün varlığının ispatlanması
	Acil Durum Prosedürleri Analizi	Prosedürün uygulanabilir olduğunun ispatlanması
	Acil Durum Prosedürleri Simulasyonu & Analizi	Prosedürün istenilen sonuçları verdiğinin ispatlanması

Sonuç olarak, bir hava aracının ömür döngüsü boyunca emniyetli uçuşunu gerçekleştirebilmesi ve hava aracı sistemlerinden kaynaklı teknik sebeplerden dolayı oluşan ölümcül kaza risklerinin kabul edilebilir seviyelere indirgenebilmesi için üreticilerin sistematik bir emniyet süreci işletmeleri gerekmektedir.

Ayrıca hava aracı tip sertifikasyonu kapsamında 1309 gereksinimine uyum gösterebilmek için üreticiler, efektif ve etkin çalışan bir emniyet organizasyonunu kurup emniyet süreçlerine uygun olarak tasarım faaliyetlerini yürütmek zorundadırlar. Emniyet süreci ve tasarım geliştirme süreçleri paralel yürütülmesi gereken süreçlerdir. Bu süreçleri iyi yöneten organizasyonlarda maliyetli tasarım geri dönüşleri minumuma indirgenmekte ve projenin öngörülen takviminde tamamlanması sağlanabilmektedir.