ASES 2010

Havacılık Projelerinde Emniyet Odaklı Sistem Mühendisliği Uygulamaları

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

Özet

1960 ların sonunda yeni nesil hava araçlarında emniyet kritik fonksiyonların artması, bu fonksiyonların uçuş kritik kompleks sistemler tarafından yapılmasını gerektirmiştir. Hava aracı sistemlerinin geliştirilmesi için teknolojideki karmaşıklığın artması, hata durumlarının oluşma olasılıklarının veya etkilerinin belirlenmesinde mühendislik kararlarının tek yöntem olarak uygulanmasını zorlaştırmıştır. Bu nedenle tasarımın kabul edilebilirliğinin değerlendirilmesinde rasyonel olasılık değerlerinin belirlenmesi ve analiz tekniklerinin uygulanması kabul görmüştür [4]. Sivil hava araçlarında kullanılan bu yaklaşım ve ilgili standartlartlar askeri hava araçları içinde benimsenmiş ve askeri operasyonları ve ihtiyaçları da içine alaçak şekilde kapsamı genişletilmiştir.

Havacılıkta teknoloji hızla ilerlemektedir ve hava araçlarında kullanılan sistemler kısa zamanda demode olmakta müşteri ihtiyaçlarını karşılayamaz duruma gelmektedir. Bu durum, yeni sistemlerle donatılmış bir hava aracı almak yerine, maliyet etkin bir çözüm olan mevcut platformların yeni sistemlerle modernize edilmesi ihtiyacını doğurmuştur. Günümüzde, aviyonik modernizasyon projelerindeki artış ile platform üzerindeki eski teknoloji sistemler çıkarılıp, yerine daha yeni ve daha fazla kabiliyete sahip kompleks sistemler entegre edilmektedir.

Son yıllarda, askeri hava aracı aviyonik modernizasyon/ sistem entegrasyon projelerinde sözleşmeler aracılığı ile emniyet gereksinimleri ve ilgili rehber standartların kullanılması zorunlu hale getirilmiştir. Bu durum, modernize edilen hava araçlarının uçuşaelverişliliğinin ve benzer kategorideki hava aracı/sistemleri için tanımlanan emniyet hedeflerini sağladığının kabul edilebilir bir metedoloji ile gösterilmesini gerektirmiştir.

Sistem Mühendisliği standartlarında Özel Mühendislik Disiplinlerinden biri olarak bahsedilen emniyet, bu standartlarda detaylı olarak tanımlanmamakla birlikte havacılıkta geliştirme ve tasarım sürecini belirleyici en önemli faktör olarak ortaya çıkmaktadır.

Bu bildiride, bazı Sistem Mühendisliği aktivitelerinin emniyet analizleri sonucunda belirlenen sistem kritikliklerine göre nasıl ele alınacağı hakkında bilgi verilmektedir.

1. Giriş

Sistem Mühendisliği tüm disiplinlerin ve özel mühendislik gruplarının ürün geliştirme süreci içerisinde bir takım gibi çalışmasını sağlayan disiplinler arası bir yaklaşımdır. Sistem Mühendisliği, karmaşık sistemlerin belirli bir maliyet ve zaman kısıtı içerisinde müşteri/kullanıcı gereksinimlerini karşılayacak şekilde konsept tasarımdan operasyonuna kadar ki geliştirme sürecini yapılandırır. Müşterilerin ticari ve teknik ihtiyaçlarını göz önünde bulundurarak kullanıcı ihtiyaçlarını da karşılayacak kaliteli ürünleri hedeflemektedir. Havacılıkta ise tüm bu gereksinimlere ek olarak emniyetli havaaraçları tasarlamak, üretmek ve sürekli olarak uçuşa elverişliliğinin sağlanabilmesi hedeflenmektedir. Bu nedenle havacılık projelerinde Emniyet Mühendisliğinin diğer disiplinlerle arayüzü çok önem taşımaktadır.

Emniyetin tedarik sürecine sonradan dahil edilmesi finansal riskleri artırabilir. Bu nedenle emniyet gereksinimlerinin, tedarik sürecinin başlangıç aşamasında, sistemi satın almadan veya inşa etmeden ortaya koyulması gerekmektedir. Sistem emniyet süreci ile, erken safhada risklerin tanımlanması, analiz edilmesi, azaltılması ve kontrol altında tutulması amaçlanmaktadır. Riskler/tehlikeler, sistem geliştirme sürecinde değerlendirilmezse sistem bu potansiyel tehlikelerle tasarlanır. Eğer bu tehlikeler geliştirme sürecinde çok geç safhalara kadar tespit edilemez şekilde kalırsa; kişiler için daha büyük riskler, zayıf sistem performansı, pahallı tadilat/iyileştirmeler, yüksek

bütçe ve ulaşılamayan proje takvimi olarak geri döner [7].

Bu nedenle riskleri projenin erken evrelerinde analiz etmemiz ve tasarım değişiklikleri ile paralel bu analizlerimizi güncellememiz gerekmektedir.

2. Standartlar:

SAE-ARP-4754; havacılık otoriteleri tarafından kabul görmüş bir rehber doküman olarak hava aracının geliştirilmesi ve modifikasyonunda izlenmesi gereken süreci tanımlamaktadır. Sistem mühendisliği süreçleri ile ortak bir çok noktası olan standardın temel farkı emniyet odaklı olması ve aktivitelerin/analizlerin derinliğinin sistemin, donanımın ve yazılımın kritikliğine göre belirlenmesidir.

SAE-ARP-4761; Hava aracı, sistem ve ekipman seviyesi emniyet analiz tekniklerini tanımlamaktadır

MIL-STD-882; Sistem içerisindeki tehlikeleri tanımlayarak önleyebilecek yeterlilikte ve kapsamda bir sistem emniyet programı geliştirme ve gerçekleştirme için gereksinimleri sağlayan bir standarttır [5]. Havacılık dahil emniyetin önemli olduğu birçok sektörde (Nükleer, kimyasal, biyolojik, raylı Sistemler, vb.) uygulaması mevcuttur.

Temelde tüm emniyet standartlarının amacı; tehlikeleri, riskleri önceden tespit ederek, geliştirme süreci içerisinde bunları önleyebilecek veya etkisini kabul edilebilir seviye ve altında tutabilecek tasarım önlemlerinin alınmasını sağlayabilmektir [6].

Hava araçlarının çok maliyetli olması, kaza sonrası can ve mal kayıpları ve yüksek tazminat bedelleri hava aracı üreticilerininin bu standartlardaki gereksinimleri daha da sıkılaştıracak şekilde bir araya gelmelerine ve ihtiyacı karşılayacak şekilde standartları güncellemelerine neden olmaktadır.

3. Modifikasyon Etki Analizi:

Hava aracı ve/veya sistemlerine yapılacak bir modifikasyonda bakılması gereken en önemli konulardan biri modifikasyonun mevcut hava aracına etkisidir. Bu değerlendirme, modifikasyonun orjinal emniyet değerlendirmelerine etkisini de içermelidir. Dolayısıyla modifikasyonun, hava aracının emniyet ve operasyonel gereksinimlerine etkisi detaylı olarak değerlendirilmelidir.

Emniyetle ilgili aşağıdaki değişiklikler gözden geçirilmelidir:

- Mevcut hata durumu sınıflandırmalarında (kritikliklerinde) değişiklik
- Yeni hata durumlarının etkisi
- Geliştirme Teminat Seviyeleri
- Emniyet marjinlerinde azalma
- Mimari kabulleri
- Çevresel kalifikasyon test sonuçlarının geçerliliği
- Geçerli kılma ve doğrulama metod ve prosedürlerinin güncellenmesi

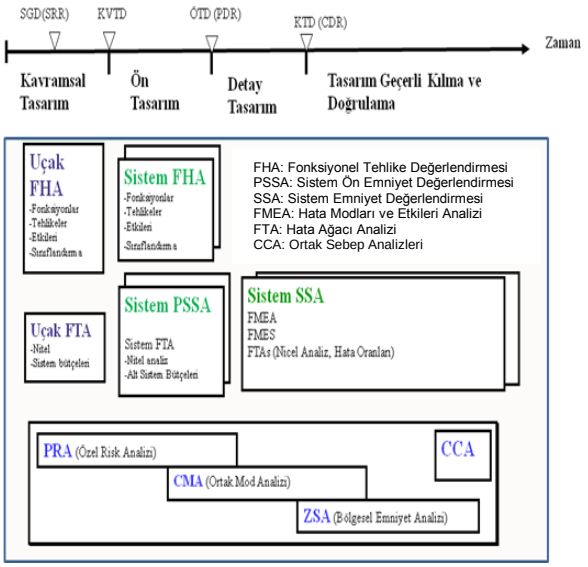
Operasyonel karakteristiklerdeki aşağıdaki değişiklikler gözden geçirilmelidir:

- Hava aracı operasyonel veya uçuşa elverişlilik karakteristikleri
- Uçuş personeli prosedürleri
- Pilot iş yükü artışı
- Durumsal farkındalık, ikaz ve uyarılar
- Pilota gösterilen bilgiler

4. Emniyet Hedefleri ve Emniyet Analizleri:

Hava aracı emniyeti, kişilere ve mallara gelebilecek zararlara ait risklerin, tehlikelerin kabul edilebilir seviyeye indirilmesi ve bu seviyede veya altında tutulabilmesidir. Hava aracının karşılaması gereken minimum emniyet gereksinimleri sertifikasyon standartlarında tanımlanmaktadır. Hava aracı sınıfına göre sayısal emniyet hedefleri geçmiş kaza istatistikleri temel alınarak belirlenmiş ve sertifikasyon standartlarına (CS/FAR 25, CS/FAR 23, vb) girilmiştir.

Şekil 1'de proje geliştirme fazlarına göre emniyet analizlerinin yeri uygulama sırasına göre verilmiştir. Emniyet analiz teknikleri için SAE-ARP-4761 havacılık otoriteleri tarafından kabul görmüş bir rehber doküman olarak kullanılmaktadır.



Şekil 1. Proje geliştirme fazlarında emniyet analizlerinin yeri [1]

Sistem Mühendisliği Yönetim Planı içerisinde ilave sistem mühendisliği aktiviteleri olarak tanımlanan Emniyet Planı emniyet analizlerini gerçekleştirebilmek ve kullanıcı, sistem, çevre ve halka gelebilecek riskleri değerlendirebilmek için izlenecek metotları ve yaklaşımı tanımlamaktadır [8].

MIL-STD-882C' de detaylı olarak tanımlanan Emniyet Program Planı genel hatları ile aşağıdakileri içermektedir;

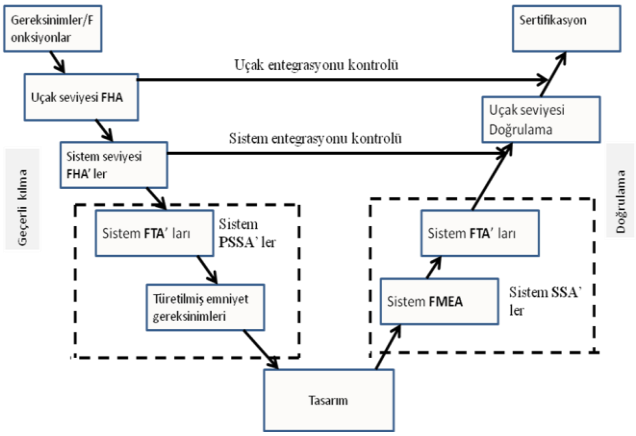
- Projede uygunacak emniyet standartları
- Proje emniyet organizasyonu ve sorumluluklar
- Proje emniyet organizasyonu içi ve dışı (alt yüklenicilerle, tedarikçiler, vb.) arayüzler
- Projede kullanılacak emniyet aktivite/analiz teknikleri
- Proje kilometre taşlarına göre emniyet analizlerinin çıktıları ve teslim tarihleri
- Emniyet gereksinimlerinin geçerli kılınması ve doğrulanması için yöntemler
- Emniyet Planının diğer planlarla arayüzü

Emniyet Program Planı proje planlama safhasında hazırlanmalı ve proje safhaları boyunca plana uyum denetlenmelidir.

Kavramsal tasarım aşamasında hava aracı seviyesi Fonksiyonel Tehlike Değerlendirmesi (FHA) ile üst seviye emniyet gereksinimleri ve üst seviye fonksiyonların kritiklikleri belirlenmektedir. Ön tasarım aşamasında sistem seviyesi fonksiyonların belirlenmesi ile birlikte herbir sistemin Fonksiyonel Tehlike Değerlendirmeleri yapılır ve detay sistem emniyet gereksinimleri çıkarılır. Bu gereksinimlere göre şekillenen ve önerilen sistem mimari çözümlerinin yeterliliği ve emniyet gereksinimlerini karşılayabilirliği Sistem Ön Emniyet Değerlendirmesi (PSSA) ile belirlenmektedir. PSSA ile alt sistem/yazılım /donanım parçalarının kritiklikleri ve tasarımın bu seviyesi için emniyet gereksinimleri belirlenmektedir. Sistem Emniyet Değerlendirmeleri (SSA) ise doğrulama analizleridir. Tamamlanmış sistemin emniyet gereksinimlerini karşıladığı bu analizlerle gösterilmektedir.

Projenin geliştirme fazları ile paralel yürütülen sistem seviyesi emniyet analizleri ile detay sistem emniyet gereksinimleri (nitel ve nicel emniyet hedefleri) ve yazılım/donanım kritiklikleri belirlenmektedir. Geliştirme Teminat Seviyesi A olan kritik bir sistem için uygulanacak süreç ile Geliştirme Teminat Seviyesi D olan minör bir sistem için izlenecek süreç ve yapılan analizler farklılık göstermektedir. Sistem için izlenecek geliştirme süreci SAE-ARP-4754' te tanımlanmaktadır. Yazılım ve donanım geliştirme seviyelerine göre izlenecek geliştirme süreci, RTCA-DO-178B ve RTCA-DO-254 standartlarında tanımlanmıştır.

Emniyet analizlerinin geçerli kılma-doğrulama diyagramında gösterimi Şekil 2' de verilmiştir.



Şekil 2. Emniyet Analizleri V diyagramı

4.1. Fonksiyonel Tehlike Değerlendirmesi

Fonksiyenel Tehlike Değerlendirmesi potansiyel fonksiyonel hataları değerlendirmek ve etkisini sınıflandırmak için hava aracı ve sistem fonksiyonlarını inceleyen bir analiz tekniğidir. Fonksiyenel Tehlike Değerlendirmesi uçak/sistem fonksiyonlarının ve bu

fonksiyonlardaki hata durumlarının sistematik ve kapsamlı bir şekilde değerlendirilmesidir. Bu analiz ile aşağıdakiler belirlenir:

a. Hata durumlarının tanımlanması

b. Hata durumlarının etkilerinin tanımlanması

c. Hata durumlarının etkilerinin sınıflandırılması (Ölümcül, Tehlikeli, Major, Minör, Emniyete Etkisi Yok). Sınıflandırmaların tanımları uçak tipine göre ilgili rehber dokümanlarda bulunmaktadır. (ör; AC 25.1309-1A, AC23.1309-1D, AMC 25.1309, vb.)

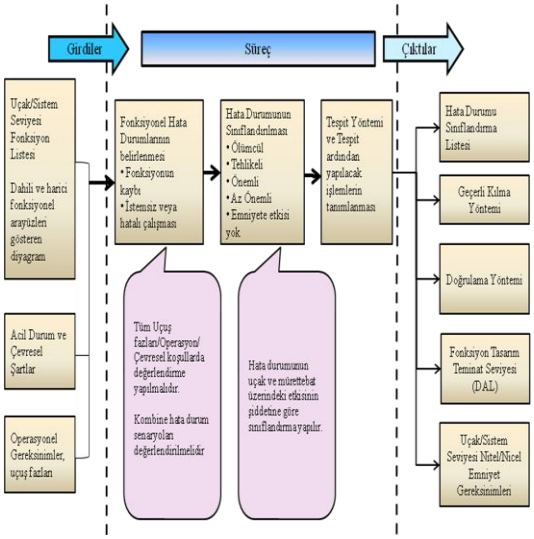
d. Hata durumlarının tespit yönteminin ve ardından yapılacak işlemlerin tanımlanması

e. Herbir hata durumunu değerlendirilirken yapılan varsayımlar ve kullanılan paremetrelerin tanımlanması (ör; uçuş fazları, zorlu operasyonel ve çevresel şartlar, vb.)

f. Hata Durumlarının geçerli kılma ve doğrulama metotlarının tanımlanması

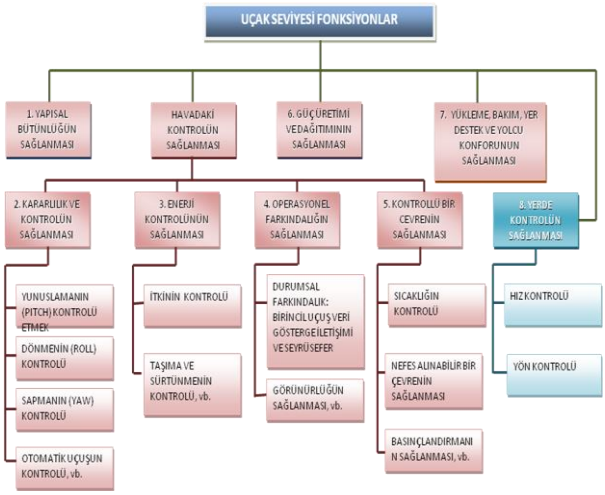
Fonksiyonel Tehlike Değerlendirmesinin temel amacı fonksiyonların dolayısıyla bu fonksiyonlarla ilgili sistemlerin kritikliğini belirleyerek emniyet hedeflerini oluşturmak ve bu hedefler doğrultusunda tasarımın şekillenmesini sağlayabilmektir. Fonksiyenel Tehlike Değerlendirmesinin hava aracı/sistem geliştirme veya modifikasyonunun başlangıç fazında gerçekleştirilmesi büyük önem taşımaktadır.

Hata durumlarının şiddetlerine göre sınıflandırılması her bir hata durumunun hava aracı ve mürettebat/yolcular üzerindeki etkisine göre yapılmaktadır. Fonksiyonel Tehlike Değerlendirmesi süreci ana hatları ile Şekil 3'te verilmiştir.

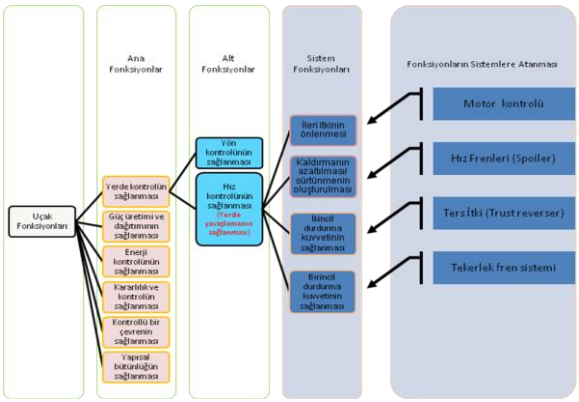


Şekil 3. Fonksiyonel Tehlike Değerlendirmesi Süreci

Hava aracı seviyesi fonksiyonlarına örnek Şekil 4'te verilmiştir. Üst seviye fonksiyonlar ve gereksinimler belirlendikten sonra ilgili sistemlere atamalar yapılmalıdır. Şekil 5' te "Yerde yavaşlamanın sağlanması" fonksiyonunun ilgili sistemlere atanması gösterilmektedir. Örneğimizde hava aracının yerde yavaşlamasının tekerlek fren sistemi, İtki Sistemi (trust reverse fonksiyonu) ve Hız Frenleri ile sağlanması öngörülmüştür ve üst seviye mimari bu şekilde tasarlanmıştır.



Şekil 4. Hava aracı üst seviye fonksiyonları –Örnek



Şekil 5. Fonksiyonların sistemlere atanması- Örnek

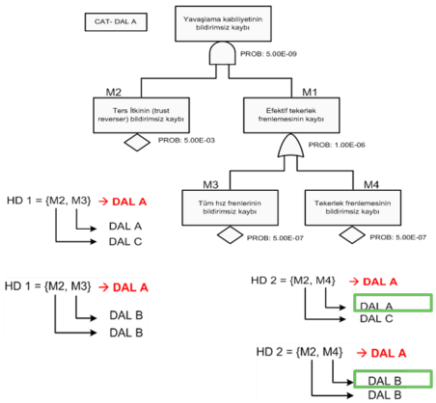
Hava aracı seviyesi Fonksiyonel Tehlike Değerlendirmesi sonucunda belirlenen hava aracı seviyesi bazı hata durumları aşağıdaki gibidir;

- İniş fazında "*Yavaşlama kabiliyetinin bildirimsiz kaybı"* Ölümcül (CAT) olarak sınıflandırılmıştır. Çünkü Pilot, aşırı hızdan dolayı uçağı yavaşlatamaz ve uçak pist dışına çıkabilir.
- İniş fazında *"Yavaşlama kabiliyetinin bildirimli kaybı"* Tehlikeli (HAZ) olarak sınıflandırılmıştır. Çünkü Pilot daha uygun bir hava sahasını seçebilir ve acil yer destek ekibine durumu bildirebilir. Gerekli yer hazırlıkları yapılabilir.
- Kalkış fazında *"V1 Hızından sonra istemsiz yavaşlama" "* Ölümcül (CAT) olarak sınıflandırılmıştır. Çünkü Pilot, yüksek takatta frenleme yüzünden kalkışı yapamaz ve yüksek hızda pistin dışına çıkabilir.

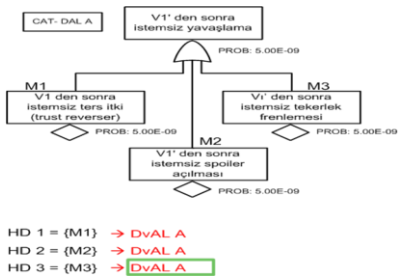
Tekerlek Fren Sistemi Fonksiyonel Tehlike Değerlendirmesi sonucunda belirlenen sistem seviyesi bazı hata durumları;

- İniş fazında *"Tekerlek fren sisteminin bildirimsiz kaybı"* Tehlikeli (HAZ) olarak sınıflandırılmıştır. Çünkü Pilot, frenleri devreye sokmaya çalışırken hatayı farkeder. Spoiler ve Thrust Reverser'ları kullanabilir. Buna rağmen uçak pistten çıkabilir.

Yavaşlama kabiliyetinin bildirimsiz kaybının Hata Ağacı Analizi (FTA) aşağıdaki gibi basitleştirilebilir. Tekerlek fren sistemi ve Ters İtkinin birlikte kaybı hata durumuna neden olmaktadır. Bu hata ağacına göre Tekerlek Fren Sistemi' nin Geliştirme Teminat Seviyesi A veya B olabilir.



V1 hızından sonra istemsiz yavaşlama hata durumunun Hata Ağacı aşağıdaki gibi basitleştirilebilir. Bu hata ağacına göre Tekerlek Fren Sistemi' nin geliştirme Teminat Seviyesi A olarak belirlenmektedir. Geliştirme Teminat Seviyelerinin doğru belirlenebilmesi için tüm hata durumları değerlendirmeli ve en yüksek seviye atanmalıdır.

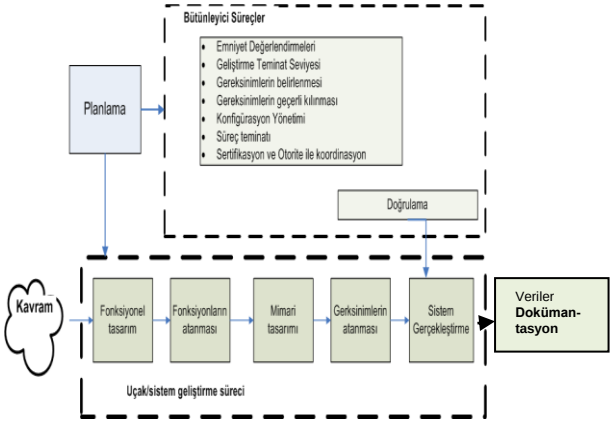


Emniyet analizleri sonucunda Tekerlek Fren Sistemini' nde oluşabilen bazı hataların hava aracının kaybına yol açabileceği değerlendirilmiş ve Geliştirme Teminat Seviyesi olarak en yüksek seviye "seviye A" atanmıştır. Bu seviyenin anlamı, bu sistemin ve yazılımının/donanımının geliştirilmesinde izlenecek planlama, geliştirme, geçerli kılma, doğrulama, konfigürasyon yönetimi, süreç teminatı, vb. gibi süreçlerin daha sıkı ve bağımsız kontrollü olmasıdır.

5. Geliştirme Sürecinin Emniyet Süreci ile İlişkisi

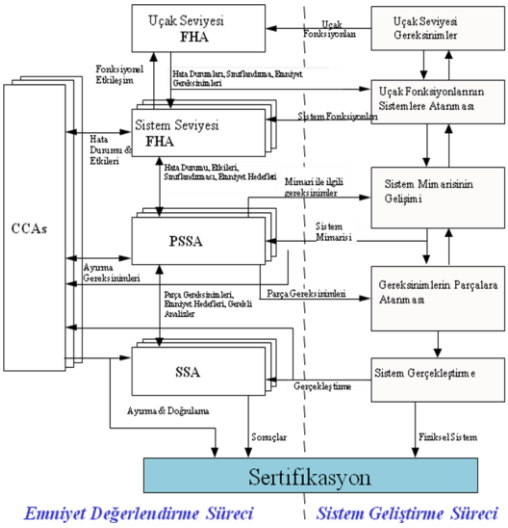
Geliştirme projelerinde fonksiyonel mimarinin doğru tanımlanması büyük bir önem taşımaktadır. Özellikle modernizasyon projelerinde, hava aracına yeni

kazandırılan ve modifiye edilen fonksiyonların doğru tanımlanması ve arayüzlerin doğru kurulması gerekmektedir. Hava aracına yeni kazandırılan kabiliyetler kapsamında yapılan modifikasyonun, hava aracının mevcut sistemlerini olumsuz yönde etkilememesi için gerekli emniyet değerlendirmeleri yapılmalı ve önlemler tasarım içerisinde alınmalıdır. Şekil 6' da hava aracı/sistem geliştirme süreci genel hatlarıyla gösterilmektedir.



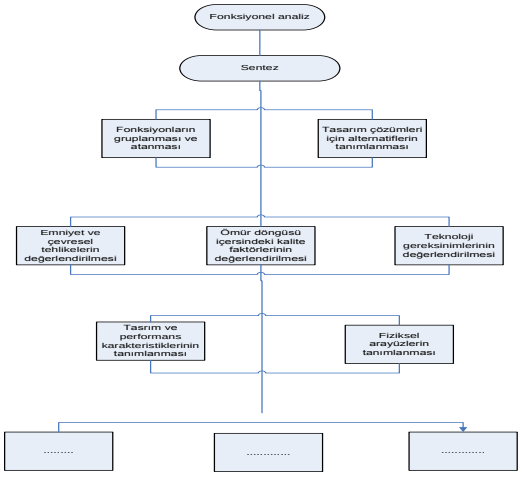
Şekil 6. Hava aracı / sistem geliştirme süreç modeli [3]

Geliştirme sürecinin emniyet süreci ile ilişkisi Şekil 7' de verilmiştir. Paralel yürümesi gereken bu aktiviteler arası arayüzler doğru ve zamanında kurulup yönetilmezse proje içerisinde çok fazla geri dönüşler olabilir.



Şekil 7. Emniyet ve Geliştirme Süreci İlişkisi [2]

Şekil 8' deki gibi IEEE 1220 standardı da, Şekil 7 de verilen ARP-4754 standardındaki süreçle benzer yaklaşımla fonksiyonel mimari oluşturulduktan sonra emniyet değerlendirmelerinin başlaması gerekliliğine dikkat çekmektedir.



Şekil 8. Sentez Süreci [8]

5.1. Gereksinim Analizi

Hava aracı geliştirme döngüsü içerisinde en üst seviye aktivite hava aracı fonksiyonlarının ve bu fonksiyonlarla ilgili gereksinimlerin tanımlanmasıdır. Hava aracı fonksiyonları, fonksiyonel arayüzler ve ilgili emniyet gereksinimleri hava aracı/sistem mimarisini oluşturmak için temel oluşturur. Mimarinin seçilmesi ile birlikte, mimarinin tamamlanması için gerekli olan ilave gereksinimler oluşturulur. Projenin erken safhalarında operasyonel gereksinimlerinin ve operasyon şartlarınında doğru ve yeterli düzeyde tanımlanması mimari tasarımının müşteri/kullanıcı beklentilerini karşılayabilecek potansiyelde olmasını sağlayacaktır.

Aşağıda verilen gereksinimler geliştirme sürecinin değişik safhalarında (fonksiyon, sistem, ekipman, yazılım/donanım vb.) dikkate alınmalıdır [2];

- Operesyonel gereksinimler
- Fonksiyonel gereksinimler
- Emniyet gereksinimleri
- Sertifikasyon gereksinimleri
- Performans gereksinimleri
- Fiziksel ve enstalasyon gereksinimleri
- İdameedilebilirlik gereksinimleri
- Arayüz gereksinimleri
- Türetilmiş gereksinimler, vb.

Sistem Mühendisliğinin ilk adımı process girdilerinin analiz edilmesidir. Gereksinim analizi aşamasında müşteri gereksinimlerinden fonksiyonel ve performans gereksinim seti geliştirilir ve tasarım kısıtları belirlenir. [10]. Müşterinin, kullanıcının ve yüklenicininin gereksinimler üzerinde aynı anlayışa sahip olması gerekmektedir. Bu nedenle gereksinimler açık, anlaşılır , tam ve doğru olmalıdır. Sistem Gereksinimleri Gözden

Geçirmesi bu ortak anlayışın ve ihtiyacın doğru ortaya koyulabilmesi için çok önemli bir kilometre taşıdır.

5.2. Gereksinimlerin Geçerli Kılınması

Geçerli kılma faaliyeti, tanımlanan gereksinimlerin hava aracı/sistem/ekipman tasarımcısının yanında müşteri, kullanıcı, bakımcı ve sertifikasyon otoritelerinin ihtiyaçlarını karşılayacak şekilde doğru ve tam olmasını sağlayan bir süreçtir. Emniyet analizleri sonucuna göre belirlenen sistem kritiklikleri, geçerli kılma faaliyetlerinin derinliğini belirlemektir. Tablo 1' de Geliştirme Teminat Seviyelerine göre yapılması tavsiye edilen faaliyetler verilmiştir.

Metotlar ve Veriler	**Geliştirme Teminat Seviyesi**			
	A ve B	**C**	**D**	**E**
PSSA	R	R	A	N
Geçerli kılma planı	R	R	A	N
Geçerli kılma matrisi	R	R	A	N
Geçerli kılma özeti	R	R	A	N
Gereksinimlerin izlenebilirliği	R	A	A	N
Gereksinimlerin Gerekçesi (Türetilmiş Gereksinimler)	R	A	A	N
Analiz, modelleme, test	R	Biri	A	N
Benzerlik (Servis Deneyimi)	A		A	N
Mühendislik Gözden Geçirmeleri	R		A	N

Tablo 1. Gereksinimleri Geçerli Kılma Metotları ve Veriler [3]

R – Sertifikasyon için tavsiye edilir, A – Sertifikasyon için müzakere edilir, N – Sertifikasyon için gerekli değildir

Gereksinimlerin geçerli kılınması projelerde önemli kilometre taşlarından biridir. Geliştirme projelerinde ana ve alt süreçler birbiriyle yakından ilişkilidir ve bir sürecin çıktısı diğer bir sürecin girdisini oluşturmaktadır. Dolayısıyla süreçler arası ilişkilerin doğru tanımlanması gerekmektedir. Projelerde gereksinimlerin yazılması ve geçerli kılınması faaliyetlerinin doğru ve tam yapılamaması diğer tasarım süreçlerininin vaktinde ve yeterli olgunlukta yürütülmesini büyük ölçüde engellemektedir.

Herbir gereksinimin hangi metotla geçerli kılınacağı aşağıdaki temel yöntemler kullanılarak belirlenebilir;

- İzlenebilirlik
- Analiz
- Modelleme
- Test
- Benzerlik
- Mühendislik gözden geçirmesi

Emniyet analizleri sonucunda Tekerlek Fren Sistemine atanmış olan Geliştirme Teminat Seviyesi A 'ya göre uygulanması tavsiye edilen geçerli kılma faaliyetleri;

- Hava aracı, sistem, ekipman gereksinimlerinin tamlık ve doğruluğu (süreç bağımsızlığı gereklidir)
- Kabullerin ispatlanması ve geçerli kılınması (süreç bağımsızlığı gereklidir)
- Türetilmiş gereksinimlerin ispatlanması ve geçerli kılınması (süreç bağımsızlığı gereklidir)
- Gereksinimlerin izlenebilirliğinin sağlanması
- Geçerli kılma kanıtlarının (Geçerki kılma matrisi ve özeti) sağlanması

5.3. Sistem Doğrulama

Doğrulama süreci ile tanımlanmış ve geçerli kılınmış gereksinimlere göre sistemin tamamlanması güvence altına alınır. Hava aracı, sistem ve ekipmanların doğrulanabilmesi aşağıdaki temel yöntemler ile sağlanabilir;

- Mühensislik değerlendirmeleri
    - Uyum beyanı
    - Tasarımın gözden geçirilmesi
    - Hesaplama ve analiz
    - Emniyet Değerlendirmeleri
- Testler veya gösterim
    - Laboratuvar testleri

- Yer testleri
- Uçuş testleri
- Simülasyon

- Kontrol/muayene
- Ekipman kalifikasyonu
- Servis tecrübesi

Doğrulama faaliyetlerinin sıkılığı emniyet analizleri sonucunda belirlenmiş olan Geliştirme Teminat Seviyesine bağlı olarak Tablo 2' de verilmiştir.

Metot ve Veriler	Geliştirme Teminat Seviyesi			
	A ve B	C	D	E
Doğrulama Matrisi	R	R	A	N
Doğrulama Planı	R	R	A	N
Doğrulama Prosedürleri	R	R	A	N
Doğrulama Özeti	R	R	A	N
Sistem Emniyet Değerlendirmeleri	R	R	A	N
Muayene, Gözden geçirme, Analiz, veya Test	Test ve diğer metotlardan biri	Metotlardan biri	A	N
Servis Tecrübesi	A	A	A	A

Tablo 2.Doğrulama Metotları ve Veriler [3]

Emniyet analizleri sonucunda Tekerlek Fren Sistemine atanmış olan Geliştirme Teminat Seviyesi A 'ya göre uygulanması tavsiye edilen doğrulama faaliyetleri;

- Test veya gösterim prosedürlerinin doğruluğunun kontrolü (süreç bağımsızlığı gereklidir)
- Fonksiyonun yerine getirildiğinin ve niyet edilmeyen fonksiyonun emniyeti olumsuz etkilemediğinin gösterilmesi (süreç bağımsızlığı gereklidir)
- Gerçekleştirilen ürünün, hava aracı,sistem,ekipman gereksinimleri ile uyumluluğunun doğrulanması (süreç bağımsızlığı gereklidir)
- Emniyet gereksinimlerinin doğrulanması (süreç bağımsızlığı gereklidir)
- Doğrulama uyum kanıtlarının (Doğrulama Matrisi, Doğrulama Özeti) oluşturulması
- Eksiklik/yetersizliklerin emniyet üzerindeki etkilerinin değerlendirilmesi ve belirlenmesi

Doğrulama faaliyetleri, gereksinim geçerli kılma çeklistlerinde belirlenen metotlara göre geçerli kılma süreci içerisinde başlamaktadır. Geçerli kılma ve doğrulama süreci sertifikasyon sürecini büyük ölçüde desteklemektedir. Doğrulama faaliyetlerinde en kritik soru "Ne kadar doğrulama faaliyetinin ürünü doğrulamak için yeterli olduğudur" Kesin olan daha fazla testin tatmin edici olduğudur. Fakat proje maliyeti ve zaman düşünüldüğünde efektif bir çözüm değildir. Sistemi geliştirenin dağrulama faaliyetlerine karar vermesi gerekmektedir[9].

6. Süreç Teminatı

Süreç teminatı, hava aracı/sistem geliştirme süreçlerinden bağımsız bir disiplinde aşağıdaki temel aktiviteleri yürütmelidir;

- Ürünün geliştirilmesi için gerekli planların geliştirilmesi ve hava aracı, sistem, ekipman geliştirme döngüsü boyunca sürdürülmesini güvence altına almak
- Tüm geliştirme aktivitelerinin bu planlara uygun yürütülmesini sağlamak
- Planlara uyumluluğun kanıtlarını oluşturmak

Proje planlama aşamasında projede uygulanacak süreç teminat faaliyetleri de Süreç Teminatı Planı 'nda tanımlanmalıdır.

7. Sonuç

Emniyet analizleri sonucunda hazırlanan emniyet dokümantasyonu, projenin kavramsal tasarım aşamasında başlayan ve ürün teslimatından sonra bile herhangi bir olay kaza sonrası gözden geçirilerek güncellenmesi gerekebilen yaşayan dokümanlardır. Emniyet analizlerinin geliştirme aktivitelerine paralel yürütülmesi tasarım içerisindeki tehlikelerin ve emniyetsiz durumların zamanında tespit edilmesi ve maliyetli geri dönüşleri engellemek için büyük önem taşımaktadır.

Havacılık projeleri maliyeti yüksek emniyet kritik projelerdir. Havacılık projelerinde amaç, sadece uçabilen bir hava aracı tasarlamak ve üretmek değil, ömür döngüsü boyunca emniyetli uçuşunu sürdürebilecek ve kendisinden beklenen görev gereksinimlerini tanımlanan tüm operasyonlarda ve operasyonel koşullarda emniyetli bir şekilde yerine getirebilecek bir hava aracı tasarlayıp üretebilmektir. Amaçlanan bu gereksinimleri maliyet ve takvim sınırları içerisinde yürütebilmek için yetkin bir tasarım ve üretim organizasyonu, iyi bir planlama, doğru ve yeterli geliştirme ve emniyet süreç/prosedürleri, deneyimli personel gereklidir.

Standartlara bütünde bakıldığında mükerrer uygulamalar olmakla birlikte bir çoğunun birbirlerini tamamladığı görülmektedir. Dolayısıyla etkin ve efektif bir sistem kurup yönetebilmek için bu standartlara hakimiyet ve doğru yorumlayabilmek büyük önem taşımaktadır.

8. Kaynaklar

8.1. SAE-ARP-4761: Guidelines and methods for conducting the safety assessment process on civil airborne systems and Equipment

8.2. SAE-ARP-4754: Certification Considerations For Highly-İntegrated Or Complex A/C System

8.3. SAE S-18 "Aircraft Development and Safety Assessment Committe " Changes on ARP-4754 dated 1996

8.4. CS 25 Certification Standard Large Aircraft and AMC25. 1309

8.5. MIL-STD-882 C System Safety Program Requirements

8.6. Avionic Systems Standardisation Committee Systems Engineerıng Subcommittee, Comparison Of Defence Standard 00-56 And ARP 4761 / 4754 , ASSC/330/6/2 – Issue 1

8.7. System Safety Approach to Acquisition Risk and Cost Management, http://safetycenter.navy.mil/acquisition/systemsafety/default.htm

8.8. IEEE 1220 IEEE Standard for Application and Management of the Systems Engineering Process

8.9. Eushiuan Tran,Verification/Validation/Certification, Carnegie Mellon University 18-849b Dependable Embedded Systems Spring 1999

8.10. System Engineering Fundemental, January 2001, Defense Acquisition University