HÜRKUŞ Uçağı Sertifikasyon Yolculuğunda Yazılım ve Alınan 20 Ders

Tuğba Saraç

Türk Havacılık ve Uzay Sanayii, A.Ş., Uçuşa Elverişlilik ve Sertifikasyon Müdürlüğü, Ankara, Türkiye
tsarac@tai.com.tr

Özet. Bu bildiride, Türk Başlangıç ve Temel Eğitim Uçağı'nın (Hürkuş) tip sertifikasyonu yolculuğunda, uçak üzerindeki cihazların içindeki yazılımların "DO-178B" (Software Considerations in Airborne Systems and Equipment Certification) rehber dokümanına ve projenin sertfikasyon otoritesi "Avrupa Sivil Havacılık Otoritesi" (European Aviation Safety Agency (EASA)) tarafından açılan "Sertifikasyon İşlem Maddelerine" (Certification Review Item((CRI)) uyum gösterimi kapsamında izlenen süreçler, gerçekleştirilen aktiviteler ve alınan dersler anlatılmaktadır.

Anahtar Kelimeler. DO-178B, Yazılım, Sertifikasyon, EASA

1 Giriş

19 Ocak 2005 tarihinde yapılan Savunma Sanayi İcra Kurulu toplantısında Hv.K.K.lığının ihtiyacına yönelik Başlangıç ve Temel Eğitim Uçağı (BTEU) Projesi kapsamında Türk Başlangıç ve Temel Eğitim Uçağı Geliştirme Programı, 15 Mart 2006 tarihinde Savunma Sanayi Müsteşarlığı ve TUSAŞ arasında imzalanan sözleşme ile yürürlüğe girmiştir. Türk Başlangıç ve Temel Eğitim Uçağı Geliştirme Programı (TBTEU) ile özgün bir eğitim uçağı prototipinin tasarlanması, geliştirilmesi, test ve doğrulamasının yapılması, üretiminin ve sertifikasyonunun gerçekleştirilmesi, sisteme ait teknik veri paketinin oluşturulması hedeflenmiştir. Ayrıca projesi kapsamında yapılan tasarım, Avrupa Sivil Havacılık Otoritesi (European Aviation Safety Agency (EASA)) tarafından sivil tip sertifikası alacaktır.

Adını Türk Havacılık Tarihi'nin en önemli pilotlarından Vecihi Hürkuş'tan alan "Hürkuş" uçağı projesi kapsamında, TUSAŞ'da kurulan proje ekibi 2006 yılından beri özverili çalışmalarına aralıksız devam etmekte olup uçağın 33 dakika süren ilk test uçuşu, 28 Ağustos 2013 tarihinde Ankara Akıncı Hava Üssü'nde başarı ile gerçekleştirilmiştir.

Hürkuş Uçağı'nda yer alan sistemlerdeki yazılımların bir kısmı yeni geliştirilirken, bir kısmı da Rafta Hazır Ticari Ürün (RAHAT) (Commercial Off-The-Shelf (COTS)) olarak satın alınmıştır.

Bu bildiride, Hürkuş Uçağı üzerindeki yazılımların sertifikasyon otoritesine uyum gösterimi kapsamında yapılan çalışmalar, yürütülen süreçler ve kazanılan dersler anlatılmaktadır.

Bildiri kapsamında kullanılan temel kavramlar ve önemli noktalar aşağıda verilmiştir:

- Uçuşa Elverişlilik: Belirli bir hava aracı konfigürasyonunun, onaylanmış kullanım şartları ve sınırlandırmalar içerisinde, emniyetle uçuşunu başlatabilme, sürdürebilme ve sonlandırabilmesi özelliğidir.
- Tip sertifikası: Sivil / Askeri Havacılık Otoriteler tarafından yayımlanan ürün tip tasarımının ilgili uçuşa elverişlilik kural ve gereksinimlerine uyumunu gösteren ve tip tasarım, operasyon sınırlandırmaları, tip sertifikası bilgi sayfası (Type Certification Data Sheet(TCDS)), geçerli düzenlemeleri içeren belgedir ve yalnızca bir tip için verilir.
- Sertifikasyon: Ürün, servis, organizasyon ve, personelin; konuya ilişkin otorite gereksinimlerine uyumunun belirlenmesi için uygulanan Havacılık Otoriteleri tarafından belgelendirilmesi ile sonuçlanan sistematik süreçtir.

1980'li yılların başında yazılımların hava araçları ve motorlarında kullanımlarının artması ile birlikte, uçuşa elverişlilik gereksinimlerinin karşılanması için kabul edilebilir bir yöntem belirlenmesi ihtiyacı doğmuştur. DO-178B rehber dokümanı bu ihtiyacı gidermek üzere RTCA (Radio Technical Commission for Aeronautics) tarafından hazırlanmış rehber bir dokümandır. Bu rehber dokümanın, cihazın yazılımının uçuşa elverişlilik gereksinimlerine olan uyumunu kabul edilebilir bir emniyet seviyesinde sağlamak için endüstriye kılavuzluk etmesi hedeflenmiştir.

ABD'de Amerikan Sivil Havacılık Otoritesi, (Federal Aviation Administration(FAA)), Avrupa Birliği'nde ise Avrupa Sivil Havacılık Otoritesi, (European Aviation Safety Agency (EASA)) iki önemli sivil havacılık otoritesidir. Bunların haricinde, her ülkenin kendi ulusal sivil havacılık otoritesi bulunmaktadır. Sivil havacılık otoriteleri, sivil hava sahasında uçacak uçakların uçuşa elverişlilik gereksinimlerini karşılamalarını beklemekte, bu gereksinimleri karşılayan hava araçlarına da tip sertifikası vermektedir. FAA bu gereksinimleri Federal Avia-tion Regulations (FAR) dokümanlarında, EASA ise Certification Specifications (CS) dokümanlarında tanımlamıştır.

Hava araçları için FAA'nın FAR XX.1309 ve EASA'nın CS XX.1309 ve diğer yerel otoritelerin de eş değer emniyet gereksinimleri mevcuttur. Burada bahsedilen XX, hava aracı kategorisine göre değişmektedir. Örneğin FAR 23.1309 küçük uçaklar ile ilgili emniyet gereksinimlerini, FAR 25.1309 ise büyük uçaklar ile ilgili emniyet gereksinimlerini tanımlar. FAA, EASA veya yerel otoriteler, sivil hava sahasında uçacak uçakların bu kurallara uymasını beklemektedir. AC 1309, FAR 1309'da yer alan gereksinimler için gösterilebilecek kabul edilebilir uyum yöntemlerini anlatır ve hava aracı yazılımlarının uyum gösterim yöntemi kapsamında AC20.115B dokümanına referans verir. FAA tarafından 01 Kasım 1993 tarihinde yayınlanan AC20.115B'ye göre, DO-178B rehber dokümanı tek uyum yöntemi olmamakla beraber, hava araçlarında kullanılan yazılımlar için kabul edilebilir Uyum Yöntemi (Means of Compliance (MoC)) olarak belirlenmiştir. Bu kabulden sonra, FAA ve EASA dahil tüm sertifikasyon otoriteleri tarafından, havacılık sektöründe kullanılacak yazılımların uyum gösterim yöntemi olarak DO-178B'ye uyum şartı aranmaya başlanmıştır.

DO-178B, yazılım yaşam döngüsü süreçlerinin amaçlarını (objectives), bu amaçlara ulaşmak için tamamlanması gereken aktiviteleri ve amaçların sağlandığını göstermek için üretilmesi gereken kanıt dokümanları tanımlar.

DO-178B rehber dokümanının 1982 yılında yayımlanan ilk sürümünün (DO-178) ardından, yazılım teknolojisindeki hızlı gelişim ve bunun beraberinde getirdiği kritik konular ile ilgili ortak bir anlayış sağlayabilmek için, 1985 yılında DO-178A sürümü, 1992 yılında da DO-178B sürümü yayımlanmıştır. DO-178B sürümü, oldukça uzun süredir kullanılmış olup 2011 senesinde şu an geçerli son sürümü olan DO-178C yayımlanmıştır.

DO-178B'ye uyumlu geliştirilmiş yazılım, DO-178B'de yer alan ilgili emniyet seviyesine ait amaçların karşılandığı ve gerekli kanıtların geliştirildiği yazılım anlamına gelmektedir. Geliştirilmesi gereken kanıtlar DO-178B rehber dokümanının 11. Bölümünde (Yazılım Yaşam Döngüsü Verileri) tanımlanmıştır. Bu kanıtlara örnek olarak yazılım planları, yazılım gereksinimleri, yazılım tasarımı, kod, yazılım test prosdürleri, test sonuçları kalite ve konfigürasyon kayıtları verilebilir. DO-178B'de belirtilen her bir emniyet seviyesi için karşılanması gereken amaçlar farklıdır. Bu amaçlar DO-178B, Ek A Tablo 1-10'da belirtilmiştir. Buna göre, Seviye A yazılım (Ölümcül) için 66 amaç, Seviye B yazılım (Tehlikeli) için 65 amaç, Seviye C yazılım (Önemli) için 57 amaç ve Seviye D yazılım (Az Önemli) için 28 Amaçtır. Seviye E için karşılanması gereken herhangi bir amaç bulunmamaktadır. Bu seviyeler, yazılımın yerine getireceği fonksiyonun uçuş emniyeti üzerindeki etkisine göre ARP 4754A (Guidelines for Development of Civil Aircraft and Systems) rehber dokümanına göre belirlenir.

Bir yazılım ürünü, DO-178B rehber dokümanı yanısıra, IEEE 12207 Standardı gibi çeşitli standartlara uyumlu olarak da geliştirilebilir. Her ne kadar belirlenen bir rehber doküman veya standartlara uyumlu olarak yazılım geliştirmek sertifikasyon kapsamında gerçekleştirilen bir aktivite olsa da, "Yazılımın Sertifikasyonu" diye bir kavram yoktur. Yazılımın sertifikasyonu değil, yazılımın içinde bulunduğu bütün bir sistemin sertifikasyonu (Certified System) söz konusudur. Sistemin sertifikasyonu için de, yazılımın "Belgelendirilebilir" (Certifiable) olması gerekir. Yazılımın belgelendirilebilir olması demek, yazılımın DO-178B rehber dokümanı gibi bir dokümana uyumlu olarak geliştirilmesi ve bu uyumun bir sertifikasyon otoritesi tarafından onaylanması demektir. Sertifikasyon otoritesi yazılım emniyet seviyesine göre uygulanabilir DO-178B amaçlarının karşılanma durumunu, üretilen yazılım yaşam döngüsü süreçlerini ve verilerini, yazılım geliştirme süreçleri boyunca üretilen doğrulama, kalite ve konfigürasyon kayıtlarını inceleyerek / denetleyerek değerlendirilir.

Türk Başlangıç ve Temel Eğitim Uçağı Geliştirme Programı kapsamında da yazılımların uyum gösterim yöntemi olarak DO-178B rehber dokümanı ve EASA tarafından başlatılan Sertifikasyon İşlem Maddesi (SİM) (Certification Review Item (CRI)) belirlenmiştir. Buna göre, uçak üzerindeki tüm cihazların içindeki yazılımların belirlenen yazılım seviyesine göre DO-178B rehber dokümanı ve SİM'lerde belirtilen gereksinimleri karşılaması gerekmektedir. SİM, tanımlanması, takip edilmesi ve çözüm üretilmesi gereken önemli teknik ve idari problemlerle ilgili sertifikasyon konularıdır. Projede yazılım uyum gösterim yöntemi kapsamında DO-178B'ye ek olarak EASA tarafından yazılım kapsamında açılmış 7 adet SİM mevcuttur.

Bildirinin devamında, Hürkuş uçağındaki hava aracı yazılımların DO-178B ve SİM'lere uyum gösterimi kapsamında pratikte izlenen süreçler, tamamlanan çalışmalar, karşılaşılan sorunlar ve öneriler anlatılmaktadır. Bu kapsamda, öncelikle ilgili konu sonraki paragrafta da o konu ile ilgili alınan ders /dersler paylaşılmıştır.

2 Proje Uygulaması

Hava araçları, Oksijen Sistemi, Yakıt Sistemi, Gösterge ve Kayıt Sistemi, Elektrik Sistemi, Haberleşme Sistemi gibi sistemlerden meydana gelir. Hürkuş Uçağı'nda 18 farklı sistemde bulunan 24 farklı cihazda, 23 farklı yazılım mevcuttur. Bu yazılımların çok büyük bir çoğunluğu Seviye C, kalanları ise Seviye D şeklindedir.

Hürkuş Uçağı'na takılan cihazların içindeki yazılımlar proje kapsamında aşağıdaki şekilde sınıflandırılmış ve projenin başında, her bir sınıf için uyum gösterim kapsamında izlenecek süreçler ve üretilecek kanıt dokümanları belirlenerek EASA ile üzerinde anlaşma sağlanmıştır.

Sınıf 1: Yeni geliştirilen yazılımlar

Sınıf 2: Daha önceden geliştirilmiş ve DO-178B uyumu sertifikasyon otoritesi tarafından onaylanmış yazılımlar.

Sınıf 3: Daha önceden geliştirilmiş ve DO-178B uyumuna dair herhangi bir kanıtın olmadığı yazılımlar.

Bildirinin devamında her bir sınıf için, belirlenen yazılım emniyet seviyesine göre DO-178B ve SİM'lerde belirtilen amaçlara uyum gösterimi kapsamında yapılan çalışmalar, kazanılan deneyimler, sorunlar ve konu ile ilgili öneriler verilmiştir.

2.1 Sınıf 1: Yeni Geliştirilen Yazılımlar

Hürkuş Uçağı geliştirme projesi kapsamında, 3 ayrı alt yüklenici tarafından yeni geliştirilen 6 ayrı yazılım vardır. Her bir alt yüklenici, DO-178B ve SİM' lerde tanımlanan amaçlara ve aktivitelere göre gerekli olan yazılım yaşam döngüsü verilerini ve kayıtlarını oluşturmuştur. Bildiride yer alan "Yazılım Sertifikasyon Konuları Planı" ve "Yazılım Başarım Özeti" bu verilerinden bazıları olup, tüm yazılım yaşam döngüsü verileri ve kayıtları, DO-178B rehber dokümanı 11.Bölüm'ünde listelenmiştir. Başta yazılım plan ve standartları (gereksinim, tasarım ve kodlama standartları) olmak üzere, alt yükleniciler tarafından geliştirilen yazılım yaşam döngüsü verileri TUSAŞ tarafından gözden geçirilmiş / denetlenmiş ve varsa gerekli değişikliklerin doğrulanmasından sonra onaylanmıştır.

Yeni geliştirilen yazılımların DO-178B rehber dokümanına uyumu onayı, sertifikasyon otoritesi tarafından SOI (Stage of Involvement) adı verilen denetimlerden sonra yapılan değerlendirmeler ile gerçekleştirilmektedir. DO-178B rehber dokümanına uyumlu olarak geliştirilmiş yazılımların onayı süreci, FAA tarafından hazırlanan 8110.49 Software Approval Guidelines dokümanında yer almaktadır. Buna göre, yazılım yaşam döngüsünün 4 farklı aşamasında sertifikasyon otoritesi tarafından denetimler yapılarak, üretilen yazılım yaşam döngüsü süreç ve verilerinin, DO-178B amaçlarını karşılama durumu değerlendirilmektedir. Bu denetimler, SOI #1 Planlama Denetimi, SOI #2 Yazılım Geliştirme Denetimi, SOI #3 Doğrulama Denetimi ve SOI

#4 Nihai Denetimidir. Her bir SOI denetimine ait soru listesi FAA tarafından hazırlanan Job Aid (Conducting Software Reviews Prior to Certification) dokümanında mevcuttur. Her bir denetim için denetimden önce hazırlanarak konfigürasyon kontrolü altına atılması gereken yazılım yaşam döngüsü verileri, FAA Order 8110.49 Software Approval Guidelines dokümanında anlatılmaktadır.

Proje kapsamında EASA tarafından Aralık 2010 tarihinde hava aracı yazılım kapsamında tasarım organizasyonu onayı (Design Organization Approval (DOA)) denetimi gerçekleştirilmiştir. Bu denetim ile mevcut TUSAŞ alt yapısı, yazılım süreçleri, proje çalışanlarının yetkinliği ve DO-178B deneyimi EASA tarafından yeterli olarak değerlendirilerek 21J.367 DOA sertifikası kapsamında, seviye C ve altı hava aracı yazılımlarının DO-178B'ye ve SİM'lere uyum onayı Temmuz 2012 tarihinde EASA tarafından TUSAŞ'a delege edilmiştir. O tarihten itibaren, SOI denetimleri ve uyum onayı kararı EASA adına TUSAŞ tarafından gerçekleştirilmektedir. Proje boyunca referans alınan TUSAŞ yazılım süreçleri; Yazılım Planlama Süreci, Yazılım Geliştirme Süreci, Yazılım Doğrulama Süreci, Yazılım Kalite Güvence Süreci, Yazılım Konfigürasyon Yönetim Süreci ve Sertifikasyon İrtibat Sürecidir.

Uçak üzerinde çok sayıda sistem olduğu ve her bir sistem de ayrı bir uzmanlık gerektirdiği için, genellikle o sistem ile ilgili uzmanlaşmış alt yüklenicilerden sistemin tedarik edilmesi yoluna gidilmiştir. Özellikle projede DO-178B'e uyum şartı var ise, doğru alt yüklenicinin seçilmesi projenin başarı için oldukça elzemdir. Alt yüklenici seçiminde, sözleşme bedeli önemli bir ölçüt olmakla birlikte, seçim kapsamında ilave ölçütlerin de dikkate alınmasının faydalı olduğu değerlendirilmektedir. Bu ölçütler arasında, firmanın yazılım geliştirme süreçlerinin ve alt yapısının DO-178B amaçlarını ne kadarını karşıladığı, firmanın sertifikasyon ve DO-178B uyumlu yazılım geliştirme deneyimi, daha önce geliştirilen yazılımın seviyesi ve karmaşıklık derecesi, yazılım kalite güvence ve yazılım konfigürasyon yönetimi alt yapısı sayılabilir. Bu ölçütlerin dikkate alınmadığı durumlarda, DO-178B amaçlarını karşılayan süreç ve verilerin çıkabilmesi için ana yüklenicinin planlanandan daha fazla dâhil olması gerekebileceği değerlendirilmektedir.

AD 1: *Alt yüklenicilerin seçiminden önce, alt yüklenicinin DO-178B amaçlarını karşılayacak süreçleri gerçekleştirme ve yazılım yaşam döngüsü verilerini üretebilme durumlarının (imkân varsa firma tesislerinde) yapılacak incelemeler ile değerlendirilmesi önerilmektedir. Değerlendirmenin olumlu olması durumunda, ana yüklenici alt yükleniciye belirlenen dokümanların onay yetkisi kapsamında delegasyon vererek kendi iş yükünü de azaltabilir. Değerlendirmenin olumsuz olması durumunda ise, tespit edilen iyileşmeye açık noktaların firma ile paylaşılması firmanın ve sektörün gelişimi için çok önemli bir fırsattır. Yeterli alt yapı ve deneyime sahip olmayan firmaların alt yüklenici olarak seçilmesi durumunda, tamamlanan süreçler ve üretilen veriler uyum kapsamında yetersiz olabilmekte, bu da ana yükleniciye ilave çalışmalar getirebileceği için planlanan iş gücü ve sertifikasyon takvimi olumsuz yönde etkilenebilmektedir.*

Projenin yürürlüğe girmesi ile birlikte, farklı başkanlıklara bağlı olan "Yazılım Mühendisliği Müdürlüğü ve Ürün Teminatı Şefliği", "Uçuşa Elverişlilik ve Emniyet Müdürlüğü" ve "Mühendislik Grup Müdürlüğü" çatısı altında Yazılım Teknik Lideri,

Yazılım Kalite Güvence Sorumlusu, Yazılım Uyum Doğrulama Mühendisi, Yazılım Uçuşa Elverişlilik Uzmanı ve Yazılım Konfigürasyon Yönetim Sorumlusundan oluşan bir yazılım ekibi kurulmuştur.

Akabinde, geliştirilen yazılımların DO-178B ve SİM'lere uyum gösterimi kapsamında TUSAŞ yazılım ekibi tarafından yürütülecek aktivitelerin, rollerin, görev ve sorumlulukların anlatıldığı "Yazılım Mühendisliği Aktiviteleri Planı" hazırlanmış ve yayımlanmıştır. EASA tarafından da onaylanan bu planda, Sınıf 1, Sınıf 2 ve Sınıf 3 kategorisindeki tüm yazılımların DO-178B'ye ve SİM'lere uyum gösterimi kapsamında izlenecek yöntemler, süreçler ve hem TUSAŞ tarafından hem de alt yükleniciler tarafından üretilecek yazılım yaşam döngüsü verileri anlatılmıştır.

AD 2: *Yazılım projeleri, diğer projelerde olduğu gibi planlama fazı ile başlamakta olup projenin başında yazılım planları üretilir. Yazılım geliştirme iş paketi, ana yüklenicinin yerine alt yüklenicinin sorumluluğunda olsa bile, proje kapsamında ana yüklenicide izlenecek süreçlerin, gerçekleştirilecek faaliyetlerin, kontrol noktalarının, üretilecek verilerin ve müşteri / sertifikasyon otoritesi ile irtibat sürecinin ve yönteminin ana yüklenici tarafından hazırlanacak bir planda tanımlanması önerilmektedir.*

EASA'nın TUSAŞ'a delegasyonu öncesinde, uyum gösterimi kapsamında gerçekleştirilen SOI denetimleri EASA tarafından gerçekleştirilmiştir. EASA tarafından gerçekleştirilen SOI denetimlerinden önce, TUSAŞ tarafından alt yüklenici firmalara yine aynı SOI soru listeleri kullanarak denetimler yapılmıştır. EASA'nın da talebi doğrultusunda, bu denetimler EASA'dan önce TUSAŞ tarafından geçekleştirilmiş ve böylelikle EASA denetimlerinden önce alt yüklenicilerde tamamlanan süreç ve üretilen yazılım yaşam döngüsü verilerindeki uygunsuzlukların tespit edilerek giderilmesi sağlanmıştır.

AD 3: *Sertifikasyon içeren projelerde, sertikasyon otoritesi tarafından yapılacak SOI denetimlerinden önce, sertifikasyon otoritesi tarafından tespit edilebilecek potansiyel uygunsuzlukların önüne geçmek için en az SOI sorularını kullanarak ana yüklenici tarafından denetimlerin gerçekleştirmesi ve bu kapsamda gerekli planlamanın proje planına dâhil edilmesi önerilmektedir.*

Bu denetimler, alt yüklenici tarafından üretilen verilerin ve yürütülen süreçlerin DO-178B gereksinimlerini karşılayıp karşılamadığını gösterdiği için, alt yüklenici iş paketlerinde sözleşme ödemeleri üretilen dokümanlarla birlikte, bu denetimlerin kapanmasına da bağlanabilir.

AD 4: *Yazılım iş paketi içeren sözleşmelerde ödemelerin, yalnızca yazılım yaşam döngüsü verilerine değil, ana yüklenici tarafından gerçekleştirilen denetimlerin başarısına da bağlanması konusunun da önerilmektedir.*

EASA'nın TUSAŞ'a delegasyonu sonrasında ise, alt yüklenici firmalarda tamamlanan yazılım geliştirme süreçleri ve üretilen yazılım yaşam döngüsü verileri kapsamında TUSAŞ tarafından SOI denetimleri gerçekleştirilmiştir. Denetimler son-

rasında, denetim raporları hazırlanarak EASA ile paylaşılmış ve denetimlerde açılan işlem maddeleri TUSAŞ tarafından takip edilerek kapatılmıştır.

SİM-F70 (Software Aspects of Certification, application of ED-12B/DO-178B, Field Loadable Software, User Modifiable Software, Use of COTS)'de her bir SOI denetiminin yapılabilmesi için sağlanması gereken ön şartlar ve konfigürasyon kontrolüne alınmış olması gereken yazılım yaşam döngüsü verileri belirtilmiştir. Proje kapsamında EASA tarafından özellikle SOI#2 (Geliştirme) ve SOI#3 (Doğrulama) denetimlerinin iki ayrı aşamada yapılması istenmiştir. Bunun nedeni, süreçte veya yazılım yaşam döngüsü verilerindeki olası önemli (majör) uygunsuzlukların ilgili fazının sonunda yapılan denetim ile tespit edilmesinin yaratacağı olumsuz etkidir. Çünkü süreç sonunda tespit edilen hataların düzeltilmesinin maliyeti, özellikle de hata sistematik veya önemli ise oldukça büyük olabilir. Ayrıca çözülmeyen hatalar proje ilerledikçe daha da karmaşıklaşarak çözülmesi imkânsız hale gelebilir. Örneğin, kodlama süreci resmi olarak tamamlandıktan sonra gerçekleştirilen SOI#2 denetiminde tespit edilen gereksinim geliştirme aşamasında yapılmış sistematik bir hatanın giderilmesi, yazılım gereksinimlerinin, yazılım tasarımının, kaynak kodun ve test prosedürlerinin değişmesine neden olabilir. Bu durum, yazılım yaşam döngüsü verilerinin güncellenmesi ve değişiklik yönetimi kapsamında yeni kayıtlarının üretilmesi ihtiyacını doğurur, bu da iş yükünün artmasına neden olur. Bu yaklaşımla ve EASA'nın da talebi doğrultusunda Proje kapsamında yazılım geliştirme ve yazılım doğrulama denetimleri iki ayrı aşamada (Geliştirme_Fazı_Bölüm1, Geliştirme_Fazı_Bölüm2 gibi) yapılmıştır.

Bu aşamaların belirlenebilmesi için, ilgili faza ait (örneğin gereksinim geliştirme fazı) yazılım yaşam döngüsü verilerinin (örneğin yazılım gereksinimleri) % 40'nın üretilerek konfigürasyon kontrol altına alınması, ikinci aşaması için de benzer şekilde verilerin %75'nin üretilerek konfigürasyon kontrol altına alınması ölçüt olarak belirlenmiştir. Bu rakamlar bu projenin özelinde, yazılımın atanmış emniyet seviyesine, üretilmesi planlanan yazılım yaşam döngüsü verilerinin içeriğine, yazılımın karmaşıklığına ve alt yüklenici firmanın DO-178B uyumlu yazılım geliştirme deneyimine göre Proje kapsamında TUSAŞ tarafından belirlenmiş ve EASA tarafından da onaylanmış rakamlar olup herhangi bir istatistiksel bir değer taşımamaktadır.

AD 5: *Yazılım geliştirme süreçlerini süreç tamamlandıktan sonra izlemek, olası sistematik veya önemli hataların süreç tamamlandıktan sonra tespit edilmesine neden olur. Bu durum, hatanın giderek karmaşıklaşmasına ve etkilenen yazılım yaşam döngüsü verilerinin ve süreçlerinin artmasına neden olabilir. O nedenle, yazılım ister alt yüklenicide ister ana yüklenicide geliştirilsin ana yüklenicinin ilgili yazılım yaşam döngüsü süreci tamamlanmadan süreci izleyecek şekilde bir alt yapı kurması önerilmektedir.*

Proje kapsamında alt yüklenicilerde gerçekleştirilen yazılım testlerine TUSAŞ tarafından Yazılım Mühendisliği Aktiviteleri Planı'da belirlenen oranda katılım (test witness) sağlanmıştır. Bu katılım EASA tarafından da talep edilmiş olup, katılımın amacı ana yüklenici olarak sürecin onaylanan yazılım planlarına göre yürütüldüğünü teminat altına almak / alındığını kontrol etmektir. Alt yüklenicilerdeki resmi yazılım testlerine başlamadan önce, teste başlanabilirlik durumu Teste Hazırlık Gözden Geçirme (THGG) Ölçüt Listesi ile değerlendirildiğine dair kanıtlar aranmıştır. THGG

ölçüt listesinde, teste girecek yazılıma ait; yazılım gereksinimleri, yazılım tasarım, kod, test prosedürleri konfigürasyon kontrolünde olup olmadığına, ana hat çekilip çekilmediğine, bu verilerin sürümlerinin birbiri ile senkronize olup olmadığına, test ortamının ilgili plan ya da prosedürde tanımlandığı gibi kurulup kurulmadığına, yazılımın emniyet seviyesine göre bağımsızlık şartı sağlanmış olup olmadığına dair sorular mevcuttur. Resmi yazılım testlerine başlanabilirlik durumunu bu ölçütlere göre değerlendirilerek testlere başlanmıştır / testlere başlandığı yapılan denetimlerle sorgulanmıştır.

AD 6: *Sözleşmelere veya alt yükleniciler tarafından oluşturulan yazılım planlarına, resmi yazılım testlerine başlama durumunun belirli ölçütlere göre değerlendirilmesini sağlayacak şekilde ölçütlerin eklenmesi önerilmektedir. Örneğin, test prosedürlerine, koda, gereksinimlere ana hat çekilmeden yapılacak resmi yazılım testleri SİM-F70 Bölüm 2.5.3'ye göre geçerli sayılamayacağı için projenin başında sözleşme veya yazılım planları aracılığı ile değerlendirme ölçütlerin eklenmesi testlerin tekrar koşulmasının önüne geçecektir.*

AD 7: *Yazılım ister alt yüklenicide ister ana yüklenicide geliştirilmiş olsun, ana yüklenicinin yazılım test koşularına belirli oranlarda katılım sağlayarak sürecin teminat altına alınması için proje takvimine gerekli aktiviteleri eklemesi önerilmektedir. TUSAŞ bünyesinde tamamlanan ve devam edem projelerde de, ana yüklenicinin belirli oranlarda testlere katılım sağlamasının sertifikasyon otoriteleri tarafından şart koşulduğu görülmüştür.*

Yazılım testlerinde olduğu gibi, sistem seviyesinde gerçekleştirilen testlere yönelik de THGG ölçüt listesinin oluşturulması, THGG değerlendirmesinin daha nesnel yapılmasına olanak verir. Sistem seviyesinde yapılacak THGG için ölçütlerden birisi de, o sistem içinde koşacak yazılıma ait ölçütler olmalıdır. THGG'ye konu olan sistemindeki yazılıma ait varsa açık işlem maddelerinin, uygunsuzlukların ve hataların sistemin emniyeti üzerindeki etkisinin değerlendirilmesi gerekir.

AD 8: *Sistem THGG'leri için hazırlanan ölçüt listesine, sistem üzerinde koşacak yazılıma ait varsa açık işlem maddelerinin, hata ve uygunsuzlukların sistem emniyetine etkilerinin değerlendirilmesine yönelik ölçütlerin eklenmesi önerilmektedir.*

DO-178B uyum denetimlerinden sonuncusu, SOI#4 nihai yazılım denetimidir. Bu denetimin amacı, üretilen yazılım yaşam döngüsü verilerinin DO-178B rehber dokümanına uyumunu, planlarda hedeflenen yaşam döngüsü süreçlerinin tamamlanarak planlanan verilerin ve kayıtların üretildiğini göstermektir.

AD 9: *Resmi uçuş testlerinden veya motor çalıştırmadan önce, sertifikasyon otoriteleri tarafından uçuşta / motor çalıştırma esnasında kullanılacak yazılımların en az SOI#3 Yazılım Doğrulama Denetiminin tamamlanması beklendiği için ana yüklenicilerin bu şekilde planlama yapması önerilmektedir. SOI#4 denetimlerinin de, testlerde çıkabilecek olası yazılım hataları nedeni ile*

uçuş testlerinden sonra gerçekleştirilmesi ve sözleşmenin bu şekilde hazırlanması önerilmektedir.

DO-178B rehber dokümanına göre tüm türetilmiş yazılım gereksinimlerinin emniyet değerlendirmesinin gerçekleştirilmesi gerekir. Türetilmiş gereksinim, yazılım geliştirme süreçleri boyunca üretilen ve üst seviye bir gereksinime izlenebilirliği olmayabilen ilave gereksinimlerdir. Türetilmiş yazılım gereksinimlerinin DO-178B'e göre emniyet sürecine gönderilmesi ve neden türetildiğine dair gerekçenin (rational) belirtilmesi gerekir. Bu değerlendirmenin amacı, türetilmiş yazılım gereksiniminin uçak emniyetine olumsuz bir etkisinin olup olmadığının değerlendirilmesidir. Proje kapsamında yazılım geliştirme faaliyeti alt yüklenicilerde gerçekleştirildiği için, bu emniyet değerlendirmesi aktivitesi alt yükleniciler tarafından geliştirilen yazılım planlarına ekletilmiştir. Ayrıca, yazılım gereksinim standartlarında da türetilmiş gereksinimlerin etiketleneceğine ve gerekçenin belirtileceğine dair kuralların ilave edilmesi sağlanmıştır. Bu gereksinimlerin emniyet değerlendirmesi, önce alt yüklenici tarafından sistem seviyesinde, sonra da TUSAŞ tarafından uçak seviyesinde gerçekleştirilmiştir. TUSAŞ'da bu süreç, ilgili rol ve sorumluluklar ile birlikte tanımlanmış ve değerlendirme bu sürece göre gerçekleştirilmiştir. Bu kapsamda bir veri tabanı oluşturulmuş ve tüm türetilmiş gereksinimlerin emniyet değerlendirme süreci bu veri tabanı üzerinden takip edilmektedir.

AD 10: *DO-178B'e göre türetilmiş yazılım gereksinimlerinin emniyet değerlendirmesine sağlanması gerektiği için, disiplinler arası olan bu sürecin tanımlanması ve gerekli alt yapının kurulması önerilmektedir. Alt yüklenicilerde yazılım geliştirme iş paketi olması durumunda ise, orada da konu ile ilgili süreç ve alt yapının kurulmasının sağlanması önemlidir.*

DO-178B rehber dokümanına göre, yazılım yaşam döngüsü süreçleri için Geçiş Ölçütü (Transition Criteria) tanımlanması gerekir. DO-178B rehber dokümanında geçiş ölçütlerinin tanımlanması Seviye A,B ve C için sağlanması gereken amaçlardan birisidir. Geçiş Ölçütü, bir yazılım yaşam döngüsü sürecine başlamak için sağlanması gereken minimum şartlar kümesidir. Örneğin, yazılım tasarımına başlamak için ilgili yazılım gereksinimleri konfigürasyon kontrolünde olmalıdır. Bu örneğe göre yazılım tasarım sürecinin geçiş ölçütlerinden birisi olarak, ilgili yazılım gereksinimlerinin konfigürasyon kontrolü alınması şartı tanımlanabilir.

Proje kapsamında yeni geliştirilen yazılımlar için geçiş ölçütünün alt yükleniciler tarafından geliştirilen planlarda tanımlanması sağlanmıştır. TUSAŞ tarafından gerçekleştirilen SOI denetimleri ile de, süreçler arasından geçişlerin, tanımlanan geçiş ölçütlerine göre gerçekleştirilip gerçekleştirilmediği ilgili kalite kayıtlarına ve üretilen yazılım yaşam döngüsü süreç ve verilerine bakılarak doğrulanmıştır.

AD 11: *Yazılım yaşam döngüsü süreçleri için geçiş ölçütünün tanımlanması, DO-178B rehber dokümanına göre karşılanması gereken bir amaçtır. Geçiş ölçütleri, yazılım geliştirme süreçlerinin belli noktalarda kontrol edilmesine imkân verdiği için tanımlanması veya alt yüklenicilerde tanımlatılması çok önemlidir. Bu ölçütlerin tanımlanması bir sonraki sürece, tanımlanan ön şart-*

lar, bir başka deyişle planlanan olgunluk sağlandığında geçilmiş olacağı için, yazılım yaşam döngüsünün ilerleyen fazlarında çıkabilecek potansiyel hatalar da azalacaktır.

Hürkuş Uçağı geliştirme projesi kapsamında her ne kadar TUSAŞ içerisinde bir yazılım geliştirme aktivitesi gerçekleştirilmemiş olsa da, sözleşme kapsamında alt yüklenicilerden gelen yazılım yaşam döngüsü verileri TUSAŞ bünyesinde konfigürasyon kontrolü altına alınmaktadır. O nedenle, proje kapsamında yalnızca alt yüklenici denetimi yapılmamış, TUSAŞ bünyesinde de, yazılım konfigürasyon yönetimi gibi tüm diğer entegre süreçleri de kapsayacak şekilde iç denetimler gerçekleştirilmiştir.

AD 12: *Yazılım geliştirme iş paketi, ana yüklenici firma yerine alt yüklenici firmalarda da gerçekleştirilebilir. Böyle bir modelde, yüklenicinin yalnızca alt yüklenicilerde gerçekleştirilen yazılım geliştirme süreçlerine yönelik denetim planlaması değil, aynı zamanda başta konfigürasyon yönetimi süreçleri olmak üzere ana yüklenicide yürütülecek tüm entegre süreçleri de kapsayacak şekilde iç denetimlerin de planlaması önerilmektedir.*

Yazılım geliştirme projelerinde, yazılım yaşam döngüsü verilerinin etkin bir şekilde gözden geçirilmesi ve gözden geçirme kayıtlarının konfigürasyon kontrolü altında saklanması kritiktir. Gözden geçirmelerin soru listeleri gibi belirli ölçütlere göre gerçekleştirilmesi gözden geçirmelerin daha nesnel bir zeminde gerçekleştirilmesine katkıda bulunur. DO-178B ve SİM'lerde belirtilen doğrulama sürecine yönelik amaçların karşılandığını gösteren kanıtların başında gözden geçirme süreçleri ve bu süreçte üretilen kayıtlar gelir. O nedenle gözden geçirme sürecinin, ölçütlerinin ve sonuçlarının konfigürasyon kontrolü altında olması çok önemlidir.

AD 13: *Yazılım yaşam döngüsü verilerini gözden geçirirken soru listelerinin kullanılması, soru listelerinin DO-178B ve SİM amaçları ile SOI sorularının referans alarak hazırlanması ve üretilen kayıtların konfigürasyon kontrolü altına alınması önerilmektedir. Geliştirdikleri yazılıma ileride DO-178B uyum onayı almak gibi vizyonu olan firmalar için, soru listeleri kullanılarak gerçekleştirilen gözden geçirmeler ve konfigürasyon kontrolünde olan gözden geçirme kayıtları, sertifikasyon aşamasında tamamlanmış bu süreçlerden kredi almanın yolunu açacaktır. Kredi almak, DO-178B'de belirtilen bir amacın karşılandığını gösteren süreç, ürün veya kanıtın sertifikasyon otoritesi tarafından kabul edilmesi anlamına gelir.*

Gözden geçirme sürecinde kapsamında "Bağımsızlık (Independence)" konusuna da kısaca değinmekte fayda var. Bağımsızlık, nesnel bir değerlendirmenin sağlanması için sorumlulukların ayrılması anlamına gelir. Bağımsızlığın yansıması, doğrulama sürecine ve yazılım kalite güvence süreçlerine olmaktadır. Doğrulama sürecinde bağımsızlık, doğrulama aktivitesinin, doğrulanan ürünü geliştirenden farklı bir kişi tarafından yapılması olarak düşünülebilir. Yazılım Kalite Güvence sürecinde bağımsızlık ise, proje organizasyonundan bağımsız bir kalite organizasyonu anlamına gelir. Sağlanması gereken bağımsızlık yazılımın seviyesine göre değişmektedir. Sağlanması gereken bağımsızlık şartları seviye bazında DO-178B rehber

dokümanının Ek A bölümünde verilen Tablo A.1–10'de belirtilmiştir. Buna göre, Seviye A ve B yazılımlar için doğrulama süreci kapsamında bağımsızlık şartı aranırken, yazılım kalite güvence organizasyonu kapsamında Seviye A, Seviye B, Seviye C ve Seviye D yazılımlar için bağımsızlık şartı aramaktadır.

Yazılım yaşam döngüsü boyunca dikkat edilmesi gereken en önemli faktörlerden birisi de izlenebilirliktir. İzlenebilirlik, yazılım yaşam döngüsü verileri arasındaki ilişkiyi gösteren kanıtlardır. Üretilen bir yazılım yaşam döngüsü verisi ve sürümünün, hangi verinin hangi sürümünden üretildiğinin izlenebilir olması gerekmektedir. Örneğin hangi sistem gereksinimleri setinin hangi sürümünden, hangi yazılım gereksinim setinin hangi sürümünün üretildiğinin takip edilebilir olması ve bu izlenebilirliğin de konfigürasyon kontrolü altına alınması gereklidir. Kurulması gereken izlenebilirlik atanan yazılım seviyesine göre değişmekte olup, detaylar DO-178B rehber dokümanının Ek A bölümünde verilen tablolarda ve Bölüm 5.5 "İzlenebilirlik"' başlığı altında verilmiştir. Proje kapsamında yeni geliştirilen yazılımlar için ilgili sistem gereksinimleri alt yüklenicilerin sözleşmelerine dâhil edilmiştir. Yazılım gereksinimleri ile sistem gereksinimleri arasında izlenebilirlik kurulmuş ve kurulan izlenebilirliklerin doğruluğu ve tamlığı TUSAŞ tarafından gerçekleştirilen gözden geçirmeler ve denetimlerle teminat altına alınmıştır.

AD 14: *Tüm yazılım projelerinde, yazılım yaşam döngüsü verileri, veriler ile verilerin üretildiği süreçler, süreçler ile süreç çıktıları arasındaki ilişkiyi gösteren kanıt dokümanlarının oluşturulması ve izlenebilirliğin takip edilebileceği bir alt yapının kurulması önerilmektedir. Kurulan sağlıklı bir izlenebilirlik, yazılım yaşam döngüsü verilerinde olabilecek değişikliklerin üretilmiş veriler üzerindeki etki analizinin doğru bir şekilde gerçekleştirmesine ve yalnızca etkilenen süreç ve verilerin doğru ve hızlı bir şekilde tespit edilmesine olanak verir. Bu kapsamda kurulmuş sağlıklı bir alt yapı (süreç ve araç), değişiklik sürecinin maliyetini azaltan önemli faktörlerden birisidir.*

Hürkuş Uçağı'daki yazılımlar ile ilgili bir başka önemli konuda, cihazın hangisi sürümü üzerinde yazılımın hangi sürümünün koştuğunu takip etme konusudur. Cihaz üreticileri ekipman ve ekipman üzerinde koşan yazılımın sürümünü takip etmek için farklı yöntemler kullanmaktadır. Örneğin uçaktaki bazı cihazların üreticileri yazılımın sürüm bilgisini, cihazın üzerine ayrı bir etiket olarak yapıştırırken, bazıları da cihazın numarası ile yazılımın sürüm bilgisini içeren tek bir numara ile bu takibi yapmaktadırlar. Bazı üreticiler ise, ekipman numarası ile yazılım sürümünü kendi konfigürasyon yönetimlerinde takip ettikleri için, yazılımın sürüm bilgisini ekipman üzerinde bulundurmamaktadır. Özellikle ikinci ve üçüncü durumlarda, yazılımın hangi sürümünün cihazın hangi sürümünde koştuğunu takip etmek daha da kritik bir hale gelmektedir.

Projede bu kapsamda özel bir alt yapı kurulmuştur. Buna göre, cihazların üzerinde koşan yazılımların sürümleri, proje kapsamında kullanılan veri yönetim aracındaki ürün ağaçlarında cihaz ve cihaza bağlı yazılım ürün ağaçları ile yönetilmektedir. Bu kapsamda uçağa takılacak cihaza, içinde koşan yazılım tanımlaması (identification) ve sürümü ile ilişkilendirilerek yayımlanmaktadır. Böylelikle veri yönetim aracında cihaz yayımlandığında, cihazın parça numarası, seri numarası, sürümü ve satıcı parça

numarası, cihaz içinde koşan yazılım tanımlaması ve sürüm bilgisi ilişkilendirilmiş olmaktadır.

İster yeni geliştirilen yazılımlar olsun, ister RAHAT yazılımlar olsun genellikle cihazın içindeki yazılımın sürümünü bir ekrana (Multi Function Display(MFD) gibi) bağlayarak tespit etme imkânı bulunmamaktadır. O nedenle, satın alınan yazılımın sürüm bilgisini içeren dokümantasyonunun cihazla ilişkilendirilerek konfigürasyon kontrolü altına alınması elzemdir.

AD 15: *Yazılımın sürüm takibi çok kritik bir konu olduğu için, cihazın içindeki yazılımın sürümünün cihazın üzerinde ayrı bir etiket olarak basılması ve sözleşmelerin bu şartı gerçekleştirecek şekilde hazırlanması önerilmektedir. Ayrıca, yeni geliştirilen yazılımlar için cihazın içindeki yazılımın sürümünü, cihazı bir ekrana (Multi Function Display(MFD) gibi) bağlayarak tespit edebilmeye imkân verecek şekilde olması ve bu kapsamda özel yazılım gereksinimlerinin tanımlanması önerilmektedir.*

Proje kapsamında işletilen EASA tarafından da başlatılan SİM-F72'de de detayları verilen bir başka süreç de Açık Hata Raporlarının (AHR)(Open Problem Report (OPR)) yönetilmesi sürecidir. AHR, sertifikasyon aşamasında halen çözülememiş yazılım ile ilgili hata raporlarıdır. Bütün AHR'ler motor çalıştırma ve uçuş öncesinde TUSAŞ tarafından değerlendirilmektedir. Bu değerlendirmenin amacı, halen çözülmemiş olan bir hata raporunun motor çalıştırma veya uçuşa emniyetine etkisinin olup olmadığını tespit etmektir. Bu konu ile ilgili EASA tarafından açılan SİM-72 (Management of Open Problem Reports for Airborne Software and Airborne Electronic Hardware)'ye göre TUSAŞ'da ilgili süreç tanımlanmış ve AHR'lerin yönetimi için bir veri tabanı oluşturulmuştur. Hürkuş Uçağı'na takılan cihazlara ait AHR'ler, tanımlanan sürece göre ilgili veri tabanında emniyet, sistem, tasarım ve yazılım sorumlularının katılımı ile değerlendirilmiştir.

AD 16: *AHR'ler uçağın uçuş konfigürasyonuna göre sınırlandırma (limitation), hafifletme (mitigation) ve tasarım değişikliğine neden olabilir. O nedenle, cihazı satın alırken mümkünse açık hata raporu olmayan cihazların satın alınması, hataların olması durumunda da, bu hataların cihaz alım aşamasında değerlendirilerek ilgili tasarımcılarla gerekli geri beslemenin sağlanması önerilir.*

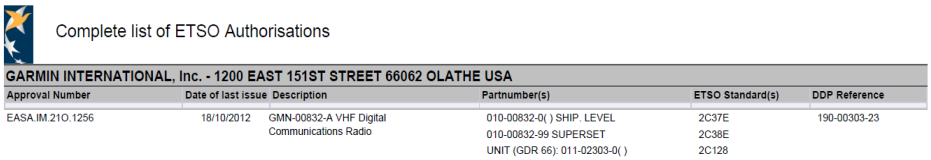
AD 17: *Cihaz alım aşamasında AHR'ler bir değerlendirme ölçütü olarak eklenmesi, mevcut AHR'lerin ilgili tasarımcıya aktarılması da dahil tüm sürecin tanımlanması ve AHR'lerin yönetimi için bir veri tabanının yaratılması / alt yüklenicilerde yaratılması önerilmektedir.*

2.2 SINIF 2: Daha Önceden Geliştirilmiş ve DO-178B Uyumu Sertifikasyon Otoritesi Tarafından Onaylanmış Yazılımlar

Bu sınıfa giren yazılımlar, DO-178B rehber dokümanına uyumlu olarak geliştirilmiş ve bu uyumun da EASA / FAA gibi bir sertifikasyon otoritesi tarafından onaylandığı yazılımlardır. Bu yazılımların üreticileri, yazılım geliştirme fazı boyunca

üretmiş oldukları yazılım yaşam döngüsü verileri ve DO-178B'ye uyum beyanlarını taahhüt ettikleri dokümanlar (Declaration of Design and Performance (DDP)) ile sertifikasyon otoritelerine başvurmaktadır. DDP'lerde, yüklenici firmanın adı, sistemin oluşturan alt bileşenler ve bu bileşenlerin numaraları, yazılıma ait sürüm ve tanımlama bilgileri, yazılım geliştirme seviyesi, uygulanabilir spesifikasyonlar, yeterlilik (qualification) test raporlarına referanslar gibi başlıklar yer almaktadır. Sertifikasyon otoriteleri DDP'leri inceleyerek ve gerek görürse firma tesislerinde gerekli incelemeleri yaparak geliştirilen yazılımın DO-178B'ye uyumlu geliştirilip geliştirilmediğini değerlendirir. Eğer değerlendirme olumlu ise, yazılımın uyumunu onaylayarak EASA/FAA web sitesinde onaylı cihazlar listesine ekler. Konunun görselleştirilebilmesi için bir örnek seçilmiştir. Proje kapsamında sertifikasyon otoritesi EASA olduğu için, EASA internet sayfasında1 yer alan cihazlardan bir örnek seçilmiştir.

Figür 1'de verilen örnek, EASA tarafından onaylanmış cihaz listesinde yer alan bir cihazdır. Bu cihaz Hürkuş Uçağı'nda yer almayıp, konunun anlaşılması için rastgele seçilmiş bir cihaza ait bir kayıttır.



Complete list of ETSO Authorisations

GARMIN INTERNATIONAL, Inc. - 1200 EAST 151ST STREET 66062 OLATHE USA

Approval Number	Date of last issue	Description	Partnumber(s)	ETSO Standard(s)	DDP Reference
EASA.IM.21O.1256	18/10/2012	GMN-00832-A VHF Digital Communications Radio	010-00832-0( ) SHIP. LEVEL 010-00832-99 SUPERSET UNIT (GDR 66): 011-02303-0( )	2C37E 2C38E 2C128	190-00303-23

Şekil 1. European Technical Standard Order (ETSO) Onaylı Cihaz

Proje kapsamında EASA tarafından onaylanarak listeye girmiş ve TUSAŞ tarafından belirlenen yazılım seviyesini de karşılayan 8 yazılım vardır. Bu yazılımlara ait onayların proje kapsamında geçerliliği, yukarıda verilen EASA internet sayfasından, proje kapsamında satın alınan cihaza ait DDP'ler incelenerek gerçekleştirilmiştir.

Eğer satın alınan cihaza ait DDP, EASA'nın onayladığı DDP sürümünden yeni ise, EASA onayından sonra üretici firma tarafından yazılım kapsamında bir değişiklik yapılmış olabilir. Bu durumda DDP'ler incelenerek yapılan değişikliklerin yazılım kapsamında olup olmadığı incelenir. Eğer değişiklik yazılım kapsamında ise değişikliğin içeriğinin, değişiklikten etkilenen yazılım yaşam döngüsü verilerinin ve değişiklik sonrasında üretilen doğrulama sonuçlarının incelenerek mevcut uyumun geçerliliğine veya uyumun devam edebilmesi için yapılması gereken ilave çalışmaların neler olduğuna karar verilmesi gerekir.

AD 18: *Uçağa takılacak cihazların seçimini yaparken, alternatif cihazların üzerinde koşan yazılımlara ait sertifikasyon bilgilerinin cihaz seçimi aşamasında seçim ölçüt listesine eklenmesi önerilir. Bu bilgiler;*

a. Yazılım içeren cihaz EASA/FAA gibi bir sertifikasyon otoritesi tarafından onaylanmış mı?

[1] http://www.easa.europa.eu/certification/docs/etso-authorisations/etsoa.pdf

b. *Uçağa takılacak cihaz, EASA/FAA tarafından onaylanan cihaz mıdır? (Bu kontrol, satın alınan cihaza ait DDP numarası, tarihi ve sürümü ile birlikte EASA internet sayfasından yapılabilir)*
c. *Onaylanan cihazın içindeki yazılımın seviyesi nedir?*
d. *Proje kapsamında yapılan emniyet çalışmalarına göre belirlenmiş yazılım seviyesi nedir?*
e. *Onaylanan cihazın içindeki yazılım seviyesi, proje kapsamında belirlenen yazılım seviyesini karşılamakta mıdır? (Örneğin onaylanan cihazdaki yazılım geliştirme seviyesi B iken, projede gerçekleştirilen emniyet çalışmalarına göre atanan yazılım seviyesinin B, C veya D olması gibi)*

Yazılım içeren cihazın seçiminin, emniyet değerlendirmesi sonrasında belirlenen yazılım emniyet seviyesine göre yapılması, sertifikasyon takviminin ve maliyetinin gerçeğe daha yakın planlanmasına katkıda bulunur. Örneğin, projenin başında DO-178B seviye C uyumlu geliştirilmiş yazılım içeren bir cihaz satın alınmış iken, proje kapsamında gerçekleştirilen emniyet çalışmalarında o cihazın içindeki yazılımın emniyet seviyesi B olarak belirlenebilir. Bu durum, yeni bir SİM açılarak ilave aktivitelerin gerçekleştirilmesi ve yeni dokümanların üretilmesi ile sonuçlanabilir. Ayrıca bu aktivitelerin tamamlanması, yazılımın DO-178B'e uyum kapsamında sertifikasyon otoritesi tarafından onaylanacağını da garanti altına almaz. Böyle bir durumda, yazılıma atanan emniyet seviyesinin düşürülmesi için sistemde değişiklikler yapılması bile gerekebilir. Projenin ilerleyen fazında bu mümkün olmayabilir veya çok büyük ilave maliyetler getirebilir. Her ne kadar Hürkuş Uçağı'nda, atanan yazılım seviyeleri ile satın alınmış cihazın içindeki yazılım geliştirme seviyesi kapsamında herhangi bir uyumsuzluk yaşanmamış olsa bile, bu konu proje ve sertifikasyon takvimini olumsuz yönde etkileyebilecek önemli konulardan birisi olduğu için bu konuya bu bildiride dikkat çekilmek istenmiştir.

AD 19: *Cihaz seçimi aşamasında, yazılım seviyesinin belirlenmiş olması ve projenin yazılım, sertifikasyon ve emniyet sorumlularının sürece dâhil edilmesi önerilmektedir.*

2.3 SINIF 3: Daha Önceden Geliştirilmiş ve DO-178B Uyumuna Dair Herhangi Bir Kanıtın Olmadığı Yazılımlar

DO-178B rehber dokümanına göre, daha önce geliştirilmiş ve uyum onayı olmayan tüm yazılımların belirlenmiş yazılım seviyesinin gerektirdiği DO-178B ve SİM'lerin tüm amaçlarını karşılaması gerekir.

Sınıf 3'e giren yazılımlar, DO-178B rehber dokümanının önceki sürümü DO-178A ile uyumlu geliştirilen yazılımlar ve uyuma ait herhangi bir kanıtın olmadığı yazılımlar olmak üzere iki grupta değerlendirilebilir.

Grup 1: DO-178A (Legacy) Uyumlu Geliştirilmiş Yazılımlar

Bu gruba giren yazılımlar, DO-178B rehber dokümanının önceki sürümü olan DO-178A ile uyumlu olarak geliştirilen ve uyumun daha önceden EASA/FAA gibi bir sertifikasyon otoritesi tarafından onaylandığı yazılımlardır. Bu yazılımlarda, eğer yazılımda bir değişiklik yok ise yazılımın mevcut onayı halen geçerlidir. Değişiklik olması durumunda da, değişikliğin büyüklüğüne ve değişiklik kapsamında yapılacak aktivitelerin çıktılarına göre mevcut onayın geçerliği ilgili sertifikasyon otoritesi tarafından değerlendirilir. DO-178A uyumlu geliştirilmiş yazılımların, DO-178B uyumu gerektiren projelerde kredi alabilmesi için, yazılıma atanan emniyet seviyesine göre denkliğinin (equivalence) gösterilmesi gerekir. Denkliğin gösterilebilmesi için SİM-70'de belirtilen ve aynı zamanda da FAA Order 8110.49 Software Approval Guide dokümanında yer alan aşağıdaki Tablo-1 kullanılmaktadır. Tablonun kullanımının kolay anlaşılabilmesi için bir örnek verilmiştir.

Örneğin tabloya göre DO/178A Seviye 2 (Level 2)'ye uyumlu geliştirilmiş bir yazılım, DO-178B Seviye A uyumlu geliştirilmiş bir yazılım ile denklik gösteremezken (No olarak görünmekte), DO-178B Seviye 1 (Level 1)'e uyumlu geliştirilmiş bir yazılım, DO-178B Seviye B uyumlu geliştirilmiş bir yazılım ile denklik gösterebilir (Yes olarak görünmekte). Tablo 1'e göre denkliğin sağlandığı yazılımlar için ilave bir aktivite ihtiyacı olmadan uyum gösterilebilir. Tabloda da görüldüğü gibi, bazı seviyeler arasında da bir takım analizler yapılarak denklik gösterilebilmektedir.

Bu tabloya göre göre denklik gösterilmişse veya uyumun ilave bir takım aktiviteler ile gösterilmesi planlanıyor ise, bu durumun tarafından Yazılım Sertifikasyon Konular Planı, (Plan for Software Aspects of Certification(PSAC)) dokümanında belirtilerek sertifikasyon otoritesi ile anlaşma sağlanması gerekir.

Tablo 1. Yazılım Denklik Tablosu

	Legacy System Software Level per ED-12/ED-12A		
ED-12B SW Level Required by the Installation	**Critical/Level 1**	**Essential/Level 2**	**Non-essential/ Level 3**
A	Possibly YES after Analyse	NO	NO
B	YES	NO/Analyse	NO
C	YES	YES	NO
D	YES	YES	NO
E	YES	YES	YES

Hürkuş Uçağı'na takılan cihazların içinde bu sınıfa giren bir yazılım vardır. Bu yazılım, DO-178A Level 2 uyumlu olarak geliştirilmiş bir yazılım olup, proje

kapsamında TUSAŞ emniyet süreçlerine göre yazılım için atanan seviye C'dir. Bu durumda, Tablo 1'e göre herhangi bir ilave çalışma ihtiyacı olmadan denklik gösterilmiştir. Bu kapsamda uyum dokümanı olarak, alt yüklenici firma tarafından Yazılım Sertifikasyon Konular Planı ve Yazılım Başarım Özeti (Software Accomplishment Summary(SAS)) hazırlanmış, TUSAŞ tarafından da incelenerek gerekli güncellemelerin doğrulanması ile onaylanmıştır.

Yazılım Sertifikasyon Konuları Planında, yazılıma ve yazılımın dahil olduğu sisteme genel genel bakış, sertifikasyon kapsamında göz önünde bulundurulacaklar, uyum gösterim yöntemi, yazılım yaşam döngüsü süreç ve verileri, varsa servis geçmişi, yazılım geliştirme / doğrulama sürecinde kullanılan araçların yeterliliği (qualification) gibi konuların anlatılarak otorite ile doküman üzerinde anlaşma sağlanması gerekir.

Yazılım Başarım Özeti (SAS) dokümanında ise, Yazılım Sertifikasyon Konular Planı'nda verilen bilgilere ilaveten yazılım karakteristikleri (kaynak sınırlamaları, çalıştırılabilir nesne kodunun boyutu gibi), yazılım tanımlaması, varsa yazılım değişiklik tarihçesi, varsa sertifikasyon sırasında çözülemeyen hata raporlarının statüsü, bu hatalara bağlı olarak oluşturulan varsa sınırlandırmalar (limitation) ve DO-178B'ye uyum beyanı bulunur.

Grup 2: DO-178B Uyumuna Dair Herhangi Bir Kanıtın Olmadığı Yazılımlar

Bu gruba giren yazılımlar, cihazın içindeki yazılımın DO-178B'ye uyumlu geliştirildiğine dair herhangi bir resmi kanıtın veya onayın olmadığı RAHAT yazılımlardır.

Bu yazılımlar için EASA tarafından SİM-F70'de de belirtildiği gibi, en az Yazılım Sertifikasyon Konular Planı, Yazılım Konfigürasyon İndeksi (Software Configuration Index(SCI)) ve Yazılım Başarım Özeti dokümanlarının üretilmesi gerekir.

Yazılım Sertifikasyon Konular Planı ve Yazılım Başarım Özeti dokümanlarından Grup 1'de kısaca bahsedilmişti. Yazılım Konfigürasyon İndeksi dokümanı ise, yazılım ürünü, çalıştırılabilir nesne kodu, her bir kaynak kod bileşenleri, yazılım yaşam döngüsü verileri, çalıştırılabilir nesne koduna ait kurulum talimatı gibi bilgileri içerir.

RAHAT ürünün daha önceden üretilmiş olduğu mevcut süreç çıktıları, DO-178B'ye göre üretilmesi gereken yazılım yaşam döngüsü verilerini ve içeriklerini tam olarak karşılamıyor ise, tamamlanması gereken ilave aktivitelerin ve varsa üretilecek yeni yazılım yaşam döngüsü verilerinin hazırlanacak Yazılım Sertifikasyon Konular Planında belirtilmesi beklenmektedir. Bu sınıfa giren yazılımlar, yazılımın servis geçmişinden kredi alabilir. Bu durum, yazılımın içinde bulunduğu cihazın uçtuğu platform, yazılımın uçtuğu saat, uçuşlar boyunca varsa açılan hata raporunun sayısı, hata raporlama sürecinin yeterliliği gibi ölçütlere bağlı olarak sertifikasyon otoritesi tarafından değerlendirilir.

Projede bu kapsama giren 2 yazılım vardır. Bu yazılımların geliştirme fazı boyunca üretilmiş yazılım yaşam döngüsü verileri incelenerek yazılıma atanan seviyeye göre DO-178B ve SİM'lerde belirtilen amaçların ne kadarını karşıladığını gösteren fark analizi çalışmaları yapılmıştır. Fark analizleri çalışmalarına göre, tedarikçi firmalarda üretilmiş mevcut yazılım yaşam döngüsü verilerini, doğrulama, kalite ve konfigüra-

syon kayıtlarını incelemek üzere firma tesislerinde denetimler gerçekleştirilmiştir. Denetimlerde, DO-178B ve SİM'lerde belirtilen amaçları karşılamak için gerçekleştirilmesi gereken ilave aktiviteler ve hazırlanması gereken ilave yazılım yaşam döngüsü verileri tespit edilmiş ve ilgili Yazılım Sertifikasyon Konular Planında bu bilgiler belirtilmiştir.

AD 20: *DO-178B uyumu gerektiren projelerde RAHAT yazılım ve daha önceden geliştirilmiş yazılım içeren tasarım çözümlerinde, proje sertifikasyon otoritesinin onayladığı yazılımların seçilmesi proje sertifikasyon takvimini olumlu yönde etkilemektedir. Bununla birlikte, onaylanmış yazılımların maliyetleri genellikle daha yüksek olduğu için, başta maliyet olmak üzere çeşitli kısıtlamalar nedeni ile projelerde uyumu resmi olarak onaylanmamış yazılımlar ile ilerlemek durumunda kalınabilmektedir. Bu durumlarda, alternatif ürünler arasında seçim yapılırken, aday tedarikçilerin ISO 9001:2008, CMMI, AQAP, ISO 12207 sertifikalarının, yapılabilecek bir ön değerlendirme ile firmanın yazılım geliştirme süreçlerinin DO-178B amaçlarını ne ölçüde karşıladığının ve mevcut kalite ve konfigürasyon alt yapısının değerlendirilmesi önerilmektedir. Bu değerlendirme, projenin sertifikasyon takviminin gerçeğe daha yakın planlanmasına yardımcı olacaktır.*

3 Sonuç

Bu bildiride, Hürkuş Uçağını üzerinde bulunan cihazların içindeki yazılımların DO-178B rehber dokümanına ve EASA tarafından açılan Sertifikasyon İşlem Maddelerine uyum gösterimi kapsamında izlenen süreçler, gerçekleştirilen aktiviteler ve alınan dersler paylaşılmıştır. Bu paylaşımın amacı, yeni projelerde benzer süreçleri yaşayacak firmalara kazanılan tecrübeleri ve alınan dersleri aktararak benzer sorunlar ile tekrar karşılaşılmaması için gerekli çalışmaların planlanmasına katkıda bulunmaktır.

Proje kapsamında kazanılan deneyimler bildirinin ana metninde verilmiştir. Bunların dışında, sertifikasyon içeren projelerde sertifikasyon otoritesi ile etkin ve verimli bir iletişim yönteminin projenin en başında kurulması ve özellikle sözleşmelerde yer alan gözden geçirmeler, resmi testlerin başlangıcı gibi önemli kilometre taşlarından önce mutlaka sertifikasyon otoritesi ile zamanında iletişime geçerek, ilgili kilometre taşları için beklentilerinin neler olduğu bilgisinin alınması önemlidir. Özellikle uyum gösterimini etkileyebilecek problemlerle karşılaşıldığında, bu problemlerin sertifikasyon otoritesi ile zamanında paylaşılmasının sertifikasyon sürecini olumlu yönde etkilediği tecrübe edilmiştir.

Özellikle sertifikasyon içeren projelerde, ürün veya bir iş paketi kapsamında alt yüklenici seçimini yaparken, yalnızca maliyet faktörü göz önünde bulundurulduğunda, her ne kadar başlangıçta yapılan düşük maliyetli sözleşme kârlı gibi görünse de, projenin ilerleyen aşamalarında bu kâr, ürün / alt yüklenici tarafından üretilen veriler sertifikasyon gereksinimlerini karşılayamaz ise zarara dönüşmektedir. O nedenle, seçim yaparken, ürünün sertifikasyon bilgileri ve bunun DO-178B amaçlarını

karşılama durumu, alt yüklenicinin mevcut alt yapısı, sertifikasyon ve DO-178B deneyimi mutlaka dikkate alınmalıdır.

Son olarak da, sertifikasyon otoritelerinin projelerde başlattığı SİM'ler ve bu SİM'lerin kapatılması sürecinde yapılan çalışmalar, sonraki benzer projeler için çok önemli girdiler olduğundan, sektördeki tüm SİM'ler ve ilgili çözüm yöntemlerinin sektör kullanıcılarına açık bir veri tabanına aktarılmasının çok faydalı olacağı değerlendirilmektedir.

Kaynaklar

1. Radio Technical Commission for Aeronautics (RTCA), DO-178B, (1992)
2. Federal Aviation Administration, FAA Order 8110.49 - Software Approval Guide, (2003)
3. Federal Aviation Administration, Job Aid, Conducting Software Reviews Prior to Certification, (1998)
4. European Aviation Safety Agency, CRI-F71(SİM-70) Software Aspects of Certification, application of ED-12B/DO-178B, Field Loadable Software, User Modifiable Software, Use of COTS, (2008)
5. European Aviation Safety Agency, CRI-F72(SİM-72) Management of Open Problem Reports for Airborne Software and Airborne Electronic Hardware, (2008)