Rafta Hazır Ticari Yazılımların Hava Aracı Tip Sertifikası Alım Sürecinde Alternatif Uyum Gösterim Yöntemleri

Tuğba Saraç

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

Özet. Rafta Hazır Ticari yazılımlar, belirli fonksiyonları yerine getirmek üzere daha önceden geliştirilmiş ve bir katalog listesinden satılan ticari uygulamalardır. Rafta Hazır Ticari yazılımlar (RAHAT) yüklenicilere sağladıkları takvim ve maliyet avantajları nedeni ile başta havacılık sektörü olmak üzere, nükleer enerji ve sağlık sektöründe giderek yaygın bir şekilde kullanılmaktadır. Yükleniciler RAHAT yazılımların hedef ortamdaki kullanılabilirliklerini, bulundukları sektörün gereksinimlerine göre kanıtlamakla yükümlüdür. Örneğin havacılık sektöründe sivil hava sahasında uçacak hava araçlarında, uyum gösterimi sertifikasyon otoriteleri tarafından kabul edilmiş yazılımlar kullanılabilir. Yazılım kapsamında uyum gösterimi, hava aracında kullanılacak yazılımların DO-178B rehber dokümanına veya sertifikasyon otoriteleri tarafından kabul görmüş başka bir uyum gösterim yöntemine göre geliştirildiğinin sertifikasyon otoritesi tarafından kabul edilmesi anlamına gelmektedir. Uyum gösteriminin temel amacı, yazılımın hava aracının uçuş emniyetini olumsuz yönde etkilemeyeceğini göstermektir. Bu çalışma, sivil hava sahasında uçacak hava araçlarında kullanılacak ve daha önce bir sertifikasyon otoritesinden uyum onayı olmayan RAHAT yazılımların uyum gösteriminde kullanılabilecek alternatif yöntemleri içermektedir. Ayrıca, RAHAT yazılımların seçimi ve hedef platform için uygunluğu ile ilgili yapılacak değerlendirmede dikkate alınması gereken hususlar ve değerlendirme sürecinde kullanılabilecek sorular sunulmuştur. İlave olarak, TUSAŞ tarafından geliştirilen ve/veya modernize edilen hava araçlarının sertifikasyon sürecinde, uyumu olmayan RAHAT yazılımların uyum gösteriminde izlenen yaklaşımdan ve yapılan çalışmalardan örnekler verilmiştir.

Anahtar Kelimeler: DO-178B Uyumu Olmayan RAHAT (Commercial Off-The-Shelf (COTS)) Yazılım, Sertifikasyon, RAHAT Yazılım Değerlendirme Süreci

1 Giriş

1980'li yılların başından itibaren yazılımlar hava araçlarında yaygın bir şekilde kullanılmaya başlanmıştır. Bununla birlikte, bu yazılımların uçuşa elverişlilik gereksinimlerinin karşılanması için kabul edilebilir bir yöntem belirlenmesi ihtiyacı doğmuş ve bu kapsamda RTCA (Radio Technical Commission for Aeronautics) tarafından DO-178B rehber dokümanı hazırlanmıştır. Bu rehber doküman, yazılım yaşam döngüsü süreçlerinin amaçlarını (objectives), bu amaçlara ulaşmak için tamamlanması gereken aktiviteleri ve üretilmesi gereken dokümanları tanımlamaktadır.

Sivil hava sahasında uçacak tüm hava araçlarının uçuşa elverişlilik gereksinimlerini karşılaması gerekir. Sivil havacılık otoriteleri (Amerikan Sivil Havacılık Otoritesi (Federal Aviation Administration(FAA)), Avrupa Sivil Havacılık Otoritesi(European Aviation Safety Agency (EASA)) gibi) tarafından bu gereksinimleri karşılayan hava araçlarına tip sertifikası verilmektedir. 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 ve geçerli düzenlemeleri içeren belgedir. Tip sertifikasını alabilmek için sağlanması gereken uçuşa elverişlilik gereksinimleri arasında hava aracında kullanılan yazılımlara yönelik gereksinimler de vardır. Yazılım ister yeni geliştirilsin, ister daha önceden geliştirilmiş RAHAT yazılım olsun, yazılımla ilgili uçuşa elverişlilik gereksinimlerini karşılaması ve gerekli kanıt dokümanların üretilerek otoriteye sunulması gerekmektedir [1,8]. Uçuşa elverişlilik gereksinimleri, DO-178B rehber dokümanına veya ilgili sertifikasyon otoritesi tarafından kabul edilen başka bir uyum gösterim yöntemine uyum olabilir. Bu çalışmada sunulan bilgiler ve metotlar DO-178B rehber dokümanına uyum gösterimi kapsamındadır.

DO-178B dokümanında yazılım ile ilgili emniyet seviyeleri tanımlanmıştır. Yazılımın yerine getireceği fonksiyonun, uçuş emniyeti üzerindeki etkisine göre ARP 4754A (Guidelines for Development of Civil Aircraft and Systems) dokümanında tanımlanan süreç çerçevesinde yazılım emniyet seviyeleri belirlenir. Bu seviyeler, Seviye A (Ölümcül), Seviye B (Tehlikeli), Seviye C (Önemli), Seviye D (Az Önemli) ve Seviye E (Önemsiz)'dir. DO-178B rehber dokümanında, Seviye D'den A'ya kadar ilave amaçların eklenmesi ile karşılanması gereken toplam 66 amaç vardır [1]. Doğrulama sürecinde uyulması gereken "Bağımsızlık" şartı da, atanan yazılım seviyesine göre değişmektedir.

Daha Önce Geliştirilen Yazılımlar, (Previously Developed Software(PDS)), belirli bir amaç kapsamında belirli fonksiyonları yerine getirmek üzere daha önceden geliştirilmiş yazılımdır. RAHAT yazılım ise, belirli fonksiyonları yerine getirmek üzere daha önceden geliştirilmiş, PDS'lerden farklı olarak genel bir katalog listesine girmiş ve o katalog listesinden satılan ticari uygulamalardır [1,2]. RAHAT yazılımlar özelleştirilmek veya yani fonksiyonlar eklemek amacı ile alınmazlar. Herhangi bir sözleşme ile özel bir uygulama kapsamında geliştirilen yazılımlar RAHAT yazılım kapsamına girmez. RAHAT yazılımlar da daha önceden geliştirildikleri için PDS sınıfında yer alırlar [2].

Havacılık sektöründe kullanılan RAHAT yazılımlara örnek olarak, A firması tarafından hava araçlarına takılmak üzere geliştirilmiş, Hava Veri Bilgisayarı

(HVB) üzerinde koşan ve hava aracının irtifa, dikey hız, sürat gibi bilgilerini hesaplayan yazılım verilebilir. Bu örnekte, HVB RAHAT cihaz, HVB üzerinden koşan yazılım ise RAHAT yazılımdır. Bu bildiride, RAHAT cihaz içinde koşan RAHAT yazılımlardan bahsedilmektedir.

Bildiri, üç bölümden oluşmaktadır. İlk bölümde, RAHAT yazılımları seçerken yüklenicinin dikkate alması gereken kriterler, ikinci bölümde RAHAT yazılımların uyum gösteriminde kullanılabilecek alternatif metotlar, üçüncü bölümünde ise referans verilen dokümanların içeriklerinden kısaca bahsedilmiştir.

2 RAHAT Yazılımların Seçim Kriterleri

RAHAT yazılımın hedef ortam için uygunluğunun değerlendirilmesinde dikkate alınması gereken üç temel konu vardır. Bunlar, RAHAT yazılımın seçimi, hedef platforma entegrasyonu ve uyum gösterim yöntemleri olarak sıralanabilir. RAHAT yazılımın hedef ortama entegrasyonu konusu bu bildirinin kapsamı dışında olup, çalışma kapsamında yapılan araştırmalarda konu ile ilgili olduğu değerlendirilen dokümanlar bilgi amaçlı son bölümde verilmiştir.

RAHAT yazılımlar, daha önceden geliştirilmiş yazılımlar oldukları için takvim ve maliyet avantajları nedeni havacılık sektöründe yaygın bir şekilde kullanılmaktadır. Bu yazılımları kullanmak her ne kadar yüklenicilere çok cazip gelse de, RAHAT yazılımlar bir takım bilinmeyenleri ve dezavantajları de beraberinde getirmektedir. RAHAT yazılımlar daha önceden geliştirildikleri için bu yazılımlara ait geliştirme ve doğrulama süreçleri ile bu süreçlere ait kanıtlara (örneğin yazılım gereksinimleri, tasarım, kaynak kod, yazılım doğrulama sonuçları, kalite güvence kayıtları) her zaman erişilemeyebilir. National Aeronautics and Space Administration (NASA) tarafından yayımlanan Software Safety Guidebook'da, RAHAT yazılımların soy ağacı her zaman tam olarak bilenemeyebileceği için, bu yazılımlar için SOUP (Software of Uncertain Pedigree) ifadesi kullanılmıştır [6].

RAHAT cihaz ve üzerinde koşan yazılım, daha önce başka hava araçlarında sorunsuz olarak kullanılmış olsa bile, bu cihazın teknolojisinin ve kabiliyetlerinin yeni kullanılacak hava aracı için uygunluğu, uçuş emniyetine ve sistem performansına etkisi, diğer cihazlarla olan ara yüzleri, yazılım geliştirme süreçlerinin ve üretilmiş dokümantasyonun yeterliliği sistematik bir şekilde değerlendirilmeli ve bu değerlendirme süreci firmalarda tanımlanmalıdır. Değerlendirmede dikkate alınması gereken hususlardan başlıcaları ve kullanılması faydalı olabilecek bir soru listesi aşağıda verilmiştir. Bu bilgiler, TUSAŞ'da yürütülen projelerde kazanılan deneyimlerden, konu ile ilgili yayımlanmış dokümanlardan ve paylaşılan sektör deneyimlerinden yola çıkılarak derlenmiştir.

RAHAT Yazılımın kabiliyetlerinin hedef platformun gereksinimlerini ne ölçüde karşıladığının değerlendirilmesi gerekir. Bu kapsamda, RAHAT cihazın daha önce kullanıldığı platform ile hedef platform arasındaki sadece benzerliklerin değil, farklılıkların da detaylı bir şekilde değerlendirilmesi gerekir. Konunun daha kolay anlaşılabilmesi için basit bir örnek vermek gerekirse, hava aracının irtifa, dikey hız, sürat gibi bilgilerini hesaplayan ve uçuş zarfı azami

20.000 ft olan bir platformda kullanılmak üzere geliştirilmiş bir HVB, uçuş zarfı 70.000 ft'de görev yapacak bir platform için yetersiz olacaktır.

RAHAT cihazın seçim çalışmalarından önce bu cihazın yer alacağı sistem ile ilgili emniyet çalışmalarının yapılarak, hedef platformda yazılıma atanan emniyet seviyesi de belirlenmelidir. Böylelikle, RAHAT yazılımın daha önce kullanıldığı platformlarda, yazılıma atanan emniyet seviyesi ile yeni kullanılacağı hava aracında yazılıma atanan emniyet seviyesi karşılaştırılabilir. Örneğin, RAHAT yazılımın kullanıldığı önceki platformdaki mimari ve yerine getirdiği fonksiyonlara göre yazılıma atanan seviye C iken, hedef platformda bu seviye B olarak atanmış olabilir. Bu durumda Seviye B ile gelen ilave DO-178B amaçları için ilave çalışmaların yapılması gerekebilir.

RAHAT yazılım üreticileri pazarda sağlayacağı rekabet avantajı nedeni ile çok fonksiyonlu ürünler geliştirmektedirler. Bu durum, hedef platformda hiç kullanılmayacak kabiliyetlerin hava aracına entegre edilmesi anlamına gelir. RAHAT yazılımda var olan ve hedef platform tarafından kullanılmayacak ilave fonksiyonları gerçekleştiren kodlar, hedef platformda hiç kullanılmayacak kodlardır. Bu kodların, her hangi bir anda istemsiz bir şekilde aktive olup sistem emniyetini tehlikeye atmayacağının kanıtlanması ve istemsiz aktivasyonu engelleyecek önlemlerin alınması gerekir. Bunun mümkün olmadığı durumlarda, kullanılmayacak bu fonksiyonların istemsiz çalışmasının sistem emniyetine ve hava aracının diğer fonksiyonlarına etkisinin (istemsiz aktivasyonun hava aracının başka fonksiyonlarının çalışmasına neden olup olmayacağı gibi) değerlendirmesi gerekir. Ayrıca, kullanılmayacak fonksiyonlara ait kodun bellekte ne kadar yer kapladığının ve bunun sistem performansına etkisinin de analiz edilmesi önemlidir. RAHAT yazılımın daha önce kullanıldığı sistemlerdeki veri iletim hızları, kullanılan fonksiyonları, operasyonel modları ve kesinlik derecesi gibi faktörler de dikkate alınarak eşdeğerliği karşılaştırılmalıdır [6,7]. Aşağıda, RAHAT yazılımların seçim sürecinde kullanılabilecek sorular verilmiştir;

1. RAHAT yazılım, kullanılacağı hedef ortamın gereksinimlerini karşılıyor mu? RAHAT yazılımın daha önce kullanıldığı platform ile kullanılacağı hedef platform arasındaki benzerlikler ve farklılıklar nelerdir? (HVB örneğindeki azami uçuş zarflarının farkı gibi)
2. RAHAT yazılım olgun ve kararlı hale gelmiş mi? Yeni sürümleri yayımlama ve hata çözme sıklıkları nedir?
3. RAHAT yazılım üreticisi yazılım güncellemelerinde kullanıcılarını bilgilendiriyor mu? Yazılım ile ilgili tespit edilen hataları yönetmek üzere bir süreç tanımlamış ve bunu işletiyor mu?
4. Rahat Yazılım ile ilgili henüz çözülmemiş açık hatalar nelerdir? Firmanın bu hataları çözme konusundaki planlaması nedir?
5. Yazılım geliştirme süreçleri ve yazılım yaşam döngüsü verileri mevcut mu? İhtiyaç halinde yüklenici firmaya sağlanabiliyor mu?
6. Kaynak kod mevcut mu ve gerekirse inceleme yapmak üzere açılabilir mi?
7. Yazılım doğrulama sürecinde kullanılan yöntemler nelerdir? Doğrulama kayıtları mevcut mu ve konfigürasyon kontrolü altında mı?
8. Doğrulama süreci bağımsız olarak yapılmış mı? Buna dair kanıtlar var mı?
9. Yüklenicinin RAHAT yazılımın önceki sürümünü satın alması durumunda, üretici bu sürümü halen destekleyebilir mi?

10. Yazılım içeren RAHAT cihazın diğer sistemlerle ara yüzü uyumlu mu? Ara yüzlere ait “Ara Yüz Tanımlama Dokümanı” var mı?
11. RAHAT yazılımda var olan ve hedef ortamda kullanılmayacak fonksiyonlar var mı? Varsa bu kabiliyetlerin aktivasyonu engellenebilir mi veya aktive olmayacağı kanıtlanabilir mi?
12. Yazılımın DO-178B Bölüm 12.3.5’de verilen kriterleri sağlayan servis geçmişi var mı? Bununla ilgili yeterli dokümantasyon mevcut mu?
13. Yazılım geliştirme ve doğrulama süreçlerinde araç kullanıldı mı? Kullanıldı ise DO-178B’de çizilen çerçeveye göre araç kalifikasyonuna ihtiyaç var mı? Var ise araç kalifikasyon bilgileri mevcut mu?
14. RAHAT yazılım üreticisinin süreçlerin yeterliliği ile ilgili fikir vermesi için ISO, SEI, CMMI gibi sertifikaları var mı?
15. İhtiyaç halinde ana yüklenici, RAHAT yazılım üreticisinin tesislerinde denetim yapabilme hakkında sahip mi?

Ekipmanın bu tip sorulara göre değerlendirilerek seçilmesi, sertifikasyon sürecinin başarısı için önemlidir. Örneğin, DO-178B’nin kaynak kod ile ilgili amaçlarının uyum gösterimi kapsamında kaynak kodun incelenmesi ihtiyacı doğduğunda RAHAT yazılımı geliştiren firma buna izin vermez ise, yazılıma atanan seviye B iken bağımsız doğrulama kayıtları yok ise veya firma ekipman ile ilgili serviste aldığı hataları yönetmiyor ise sertifikasyon süreci orada tıkanabilir. O nedenle, RAHAT Yazılımın projenin gereksinimlerine göre belirlenen kriterlere göre değerlendirilerek seçilmesi oldukça çok önemlidir.

3 RAHAT Yazılımların Uyum Gösteriminde Alternatif Metotlar

Bu bölümde, DO-178B uyumu olmayan yazılımların, DO-248B dokümanında tanımlanmış alternatif uyum gösterim metotlarından ve bu metotların hangi DO-178B amacını karşılayabileceğinden bahsedilmektedir. DO-248 dokümanı, DO-178B rehber dokümanındaki amaçları detaylandırmak ve endüstri / sertifikasyon otoritelerinin uygulamada karşılaştıkları sorunları açıklayarak sektöre kılavuzluk etmek için “Special Committee 190” komitesi ve “European Organisation for Civil Aviation Equipment (EUROCAE) Working Group 52” çalışma grubu tarafından geliştirilmiş bir dokümandır.

DO-248 rehber dokümanın içerisindeki başlıklardan bir tanesi de, RAHAT yazılımların uyum gösterimi sürecinde kullanılabilecek potansiyel alternatif metotlar ile ilgili olan başlık DP#5 (Application of Potential Alternative Methods of Compliance for Previously Developed Software)’tir [2].

Buna göre, DO-178B uyumlu geliştirilmemiş RAHAT yazılımların uyum gösterim sürecinde yedi alternatif metot kullanılabilir. Bu metotlardan iki tanesi, DO-178B rehber dokümanında (Bölüm 12.3) belirtilen “Servis Geçmişi” ve “Formal Yöntemler”’dir [2]. DP#5’de ise bu metotlara ilave olarak endüstri deneyimlerinden yola çıkılarak oluşturulmuş 5 farklı metottan daha bahsedilmektedir. Bu metotlar aşağıda kısaca özetlenmiş olup, hangi metodun hangi DO-178B amaçlarını kullanılabileceği de çalışmanın devamında sunulmuştur.

Metot1:Process Recognition (PR) (Süreç Tanıma)
Bu metot, RAHAT yazılım geliştirme fazında tanımlanmış bir sürece uyulduğuna dair kanıtların olması durumunda kullanılabilecek bir metottur. RAHAT yazılım geliştirme fazında takip edilen süreçlerin yeterliliği, DO-178B amaçlarına göre değerlendirmekte ve karşılanan amaçlar bir matris ile sunulmaktadır.
Metot 2: Prior Product Certification (PPC) (Önceki Ürün Sertifikasyonu)
Bu metot, RAHAT yazılımın daha önce belgelendirilmiş veya kalifiye edilmiş bir sistemde bir sertifikasyon otoritesi tarafından onaylanmış olması durumunda kullanılabilir (Örneğin RAHAT yazılımın, sivil uçaklarda daha önce kullanılmış olması gibi). Bu yöntemde önemli olan husus, RAHAT yazılımın onaylandığı önceki sisteme ait sertifikasyonuna temeli ile hedef ortama ait sertifikasyon temeli arasındaki benzerlikler ve farklılıklardır. Bu karşılaştırmaya göre karşılanan ve karşılamayan DO-178B amaçları belirlenebilmektedir.
Metot 3: Reverse Engineering (RE) (Tersine Mühendislik)
Bu metotta mevcut yazılım yaşam döngüsü verilerinden, diğer yazılım yaşam döngüsü verileri üretilir. (Çalıştırılabilir nesne kodundan, kaynak kodu, yazılım test prosedürlerinden yazılım gereksinimleri üretmek gibi). Akabinde üretilen veriler incelenerek, DO-178B amaçlarını karşılama durumları değerlendirilir.
Metot 4: Restriction of Functionality (RF) (İşlevsellik Kısıtlaması)
Bu metotta, RAHAT yazılımın sahip olduğu fakat hedef platformda kullanılmayacak fonksiyonlar uçuş emniyetini etkilemeden kısıtlanabilirse (örneğin tasarımda veya kodda yapılacak bir değişiklik ile) kullanılmayacak fonksiyonlara ait yazılımlar için, uyum gösterimine ihtiyacı olmayacağından sertifikasyon sürecinde yüklenicinin harcayacağı iş gücü azaltılabilir.
Metot 5: Product Service History (PSH) (Ürün Servis Geçmişi)
Bu metot, RAHAT yazılımın önceki platformlardaki kullanımlarında elde edilen verilerin uyum gösterimi kapsamına kullanıldığı metottur. Örneğin, A firması tarafından üretilen HVB cihazının farklı hava araçlarında aynı fonksiyonlar ile t saat kullanımı sonucunda toplanan verinin (yazılımın hatasız çalışmış olması / varsa yazılım kaynaklı hatalar) hedef platformda kullanılacak yazılım uyum gösteriminde kullanımı gibi. Metot, RAHAT yazılım geliştirici firmada, tanımlı ve takip edilen yazılım konfigürasyon ve kalite yönetimi süreci varsa, yazılımın daha önce kullanıldığı platformlar, icra ettiği fonksiyonlar, toplam uçuş saati, önceki mimarilerde yazılım atanan seviye gibi konular değerlendirildikten sonra, özellikle seviye C ve D yazılımların uyum gösteriminde yaygın olarak kullanılan ve sertifikasyon otoriteleri tarafından da en çok kabul edilen metottur.
Metot 6: Formal Methods (FM) (Formal Metotlar)
Formal metotlar, sistem davranışının matematiksel modellerini oluşturmak, geliştirmek ve kanıtlamak için kullanılan tanımlayıcı simgeler ve analitik yöntemlerdir. (Örneğin UML formal gereksinim geliştirme metotlarındandır.) bu yöntem ile gereksinimlerin, algoritmaların, kaynak koddaki veri akış analizi de doğruluğu ve tamlığı ile matematiksel modeller ile kanıtlanarak uyum gösterimi yapılabilir.
Metot 7: Audits and Inspections (AI) (Denetim ve Muayene)
RAHAT yazılım geliştirme sürecinde kullanılan süreçlere, üretilen yazılım döngüsü verilerine (planlar, gereksinimler, tasarım, kalite ve konfigürasyon

kayıtları gibi) ve yürütülen aktivitelerin onaylanan planlara uyumuna dair kanıtlar, DO-178B amaçlarına uyum gösterim sürecinde kullanılabilir.

DO-178 rehber dokümanında karşılanması gereken amaçlar, DO-178B Ek-A'da verilen 10 ayrı tabloda sıra ile belirtilmiştir. Bildirinin bu bölümünde uyum gösterimi çalışmalarında, hangi amaçların uyum gösteriminde hangi metotların kullanılabileceği ile ilgili bilgiler verilmiştir.

Method \Tablo	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
PR	✓	✓	✓	✓	✓	X	✓	X	X	X
PPC	✓	✓	✓	✓	✓	X	✓	X	✓	X
RE	X	✓	✓	✓	✓	X	X	X	X	X
RF	X	✓	✓	✓	✓	X	✓	X	X	X
PSH	X	✓	✓	✓	X	X	✓	X	X	X
FM	X	✓	✓	✓	✓	X	X	X	X	X
AI	✓	✓	✓	✓	✓	X	✓	X	✓	X

Tablo 1. Alternatif Yöntemlerin Tablolardaki (A1-A10) Uygulanabilirliği

Tablo 1'de, DO-178B amaçları ile bu amaçları karşılamak üzere kullanılabilecek metotlar arasında bir referans verilmiştir. Tablo 1'de bahsedilen sütunlar yukarıda bahsedilen metotları, satırlar ise DO-178B Ek A'da verilen ve amaçlarının yer aldığı tabloları göstermektedir. Ek A'da verilen bu tabloların başlıkları aşağıda listelenmiştir;

Tablo **A-1**: Planlama Süreci
Tablo **A-2**: Yazılım Geliştirme Süreçleri
Tablo **A-3**: Yazılım Gereksinim Süreci Çıktılarının Doğrulanması
Tablo **A-4**: Yazılım Tasarım Süreci Çıktılarının Doğrulanması
Tablo **A-5**: Kodlama ve Entegrasyon Süreci Çıktılarının Doğrulanması
Tablo **A-6:** Entegrasyon Süreci Çıktılarının Testi
Tablo **A-7**: Doğrulama Süreci Çıktılarının Doğrulanması
Tablo **A-8:** Yazılım Konfigürasyon Yönetim Süreci
Tablo **A-9:** Yazılım Kalite Güvence Süreci
Tablo **A-10:** Sertifikasyon İrtibat Süreci

Yukarıdaki tabloya göre, örneğin **RE** metodu Tablo A-1 için "DO-178B amaçlarını karşılamak üzere kullanılabilir bir yöntem değil iken, **PPC** metodu (önceki sertifikasyon kapsamında hazırlanmış olan plan ve standartlar olduğu için) uyum gösterim sürecinde kullanılabilir bir metottur.

Tablo 1'de hangi metotlar ile hangi DO-178B süreci amaçlarının karşılandığı (✓) işareti ile listelenmiştir.

PSH metodunda yeterli ve kabul edilebilir bir servis geçmişi ile alt seviye yazılım gereksinimlerinin hazırlanması, üst seviye yazılım gereksinimleri ile hedef ortam arasındaki uyumluluk, yazılım tasarımı, kullanılan algoritmaların doğruluğu, alt seviye gereksinimler ile hedef ortamın uyumluluğu kapsamındaki DO-178B amaçları karşılanabilir.

DO-178B Tablo **A-6** ile ilgili amaçların karşılanmasında, yukarıda bahsedilen yöntemler her zaman uygulanabilir olmamakla beraber, koşturulabilir nes-

ne kodu ile hedef ortamın uyumu ile ilgili amaç kapsamında servis geçmişi kullanılabilir. DO-178B Tablo **A-7** ile ilgili amaçlardan bir tanesi olan yapısal kapsama analizi [1] ile ilgili amacın karşılanmasında da bahsedilen yöntemler genellikle kullanılamaz.

DO-178B Tablo **A-8** ilgili amaçlar kapsamında alternatif metotlar genellikle uygulanabilir değildir. RAHAT yazılımı hava aracında kullanan yüklenici, Rahat Yazılımın konfigürasyon kontrolü mekanizmasını kurmakla ve idame etmekle yükümlüdür.

DO-178B Tablo **A-9** ile ilgili amaçlar kapsamında, RAHAT yazılımın geliştirme sürecinde daha önce gerçekleştirilen kalite aktiviteleri ve üretilen kanıtlardan uyum gösterimi sağlanabilir.

DO-178B Tablo **A-10** ile ilgili amaçlar kapsamında alternatif metotlar genellikle kullanılabilir değildir. RAHAT yazılımın uyum gösterimi kapsamında yukarıdan belirtilen metotlar bir arada kullanarak da uyum gösterimi yapabilir. Burada önemli olan, uyum gösterimi kapsamında izlenecek yolun, kullanacak metotların ve üretilecek yazılım yaşam döngüsü verilerinin "Yazılım Sertifikasyon Konuları Planı"'nda (YSKP) tanımlanması ve sertifikasyon otoritesi ile anlaşma sağlanması hususudur. Projenin sonunda da, YSKP dokümanında taahhüt edilen çalışmaların sonuçları, varsa sapmalar ve uyum beyanını içeren Yazılım Başarım Özeti dokümanı üretilmelidir. Yüklenicinin, projenin başından sonunda kadar belirli aralıklarda sertifikasyon otoritesi ile görüşerek ilerlemeleri / varsa problemleri zamanında paylaşması sertifikasyon sürecinin başarısı için oldukça önemlidir.

Uyum gösterimi kapsamındaki bir diğer konu da, DO-178B rehber dokümanının önceki sürümü olan DO-178A ile uyumlu olarak geliştirilen ve uyumun daha önceden gibi bir sertifikasyon otoritesi tarafından onaylanan 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 seviyesine göre denkliğinin (equivalence) gösterilmesi gerekir [5]. Denkliğin gösterilebilmesi için FAA tarafından yayımlanan "Order 8110.49 Software Approval Guide" dokümanında yer alan aşağıdaki Tablo-2 kullanılmaktadır. Tablo-2'ye göre örneğin, DO-178A Seviye 2'ye uyumlu geliştirilmiş bir yazılım, DO-178B Seviye A uyumlu geliştirilmiş bir yazılım ile denklik gösteremezken (Hayır olarak görünmekte), DO-178B Seviye 1'e uyumlu geliştirilmiş bir yazılım, DO-178B Seviye B uyumlu geliştirilmiş bir yazılım ile denklik gösterebilir (Evet olarak görünmekte). Tabloda da görüldüğü gibi, bazı seviyeler arasında da bir takım analizler yapılarak denklik gösterilebilmektedir. Bu durum da YSKP dokümanında belirtilerek sertifikasyon otoritesi ile anlaşma sağlanması gerekir.

---

[1] Yapısal kapsama analizi, kodun yapısının istenen emniyet seviyesine göre doğrulandığını, kodun içerisinde istenmeyen (unintended) fonksiyonların bulunmadığını ve gereksinim tabanlı yapılan testlerin kodu kapsama ölçüsünü göstermek üzere yapılan bir analizdir.

	DO-178/DO178A		
DO-178B Yazılım Seviyesi	**Seviye 1**	**Seviye 2**	**Seviye 3**
A	Analiz Sonrası "Evet" olabilir	Hayır	Hayır
B	Evet	Hayır/Analiz	Hayır
C	Evet	Evet	Hayır
D	Evet	Evet	Hayır
E	Evet	Evet	Evet

Tablo 2. Yazılım Denklik Tablosu [5]

TUSAŞ'da, aviyonik modernizasyon projesi olan Erciyes Projesi'nde uçağa entegre edilen ve DO-178B uyumlu geliştirilmemiş RAHAT yazılımların uyum gösterimi kapsamında sertifikasyon otoritesi tarafından Sertifikasyon İşlem Maddesi (SİM) F-07 başlatılmıştır. SİM, tanımlanması, takip edilmesi ve çözüm üretilmesi gereken önemli teknik ve idari problemlerle ilgili sertifikasyon konularıdır. SİM F-07 kapsamında, uyumu olmayan yazılımlar için Amerikan Savunma Bakanlığı tarafından yayımlanan Joint Software Systems Safety Engineering Handbook (JSSS) dokümanının EK-D (COTS and Non-Developmental Item Software) bölümünde detaylandırılan çalışmaların ve analizlerin yapılması istenmiştir. Bu kapsamda, uyumu olmayan tüm yazılımlar için yazılımın mevcut dokümantasyonu, geliştirildiği süreçlerin olgunluğu, servis geçmişi, konfigürasyon yönetim süreci, kalite güvence süreci, emniyet faktörleri, test edilebilirlik, entegrasyon gereksinimleri, mevcut hata raporları, bu hataların sistem emniyetine etkileri ve RAHAT yazılımın daha önce kullanıldığı platformlar ile Erciyes Projesi'ndeki uçak arasındaki benzerlikler ve farklılıklar değerlendirilmiş, elde edilen kanıtlar JSSS dokümanında tariflendiği gibi "Yazılım Emniyet Durumu" (Software Safety Case) dokümanında sertifikasyon otoritesine sunulmuştur. Sertifkasyon otoritesi yapılan çalışmaları ve kanıt dokümanları yeterli bularak Erciyes Projesi kapsamında uyumu olmayan RAHAT yazılımların uyum gösterimini kabul etmiştir.

Benzer şekilde Hürkuş Projesi kapsamında da, DO-178B uyumlu geliştirilmemiş yazılım içeren cihazlar vardır. Bu cihazlar için de, DO-248'de belirtilen metotlardan, "Önceki Ürün Sertifkasyonu", "Ürün Servis Geçmişi", "Tersine Mühendislik" ve "Denetim ve Muayene" metotları ile gerekli kanıtlar sağlanarak uyum gösterimi yapılmış ve uyum gösterimi Avrupa Sivil Havacılık Otoritesi tarafından da kabul edilmiştir.

Ayrıca TUSAŞ'da yürütülen projelerin sözleşme aşamalarında, DO-178B uyumu olmayan yazılımların geliştiricilerinden DO-178B amaçlarına uyumlarını değerlendirdikleri bir fark analizi çalışması istenmektedir. Bu çalışma ile, RAHAT yazılımın hali hazırdaki kanıt dokümanları ile uyum gösterdiği ve gösteremediği DO-178B amaçları hakkında bir ön bilgi elde edilmektedir. Bu bilgi, RAHAT yazılımların seçim sürecinde kullanılan kriterlerinden birisidir. Örneğin hali hazırdaki uyum dokümanları ile bazı DO-178 amaçlarını karşılayan

RAHAT yazılım, hiç karşılamayan RAHAT yazılıma göre yüklenici açısından daha avantajlı olabilir. Yüklenicinin karşılanan ve karşılanamayan DO-178B amaçları hakkında projenin başında bilgi sahibi olması, proje boyunca yürütülecek sertifikasyon faaliyetleri kapsamında ayıracağı iş gücü ve kaynak planlaması için de oldukça önemlidir. Ayrıca, seçimi tamamlanan RAHAT yazılım üreticisi ile yapılan sözleşmeye, DO-248 dokümanında belirtilen "Audit&Inspection" metodu ile uyum gösterimi yapma seçeneğine karşın, TUSAŞ'ın RAHAT yazılım üreticisinin tesislerinde (gerektiğinde sertifikasyon otoritesi temsilcisi ile) denetim ve inceleme yapma hakkı ile ilgili sözleşme maddesi eklenmektedir.

4 Referans Dokümanların İçerikleri Hakkında Genel Bilgiler

4.1 Requirements for Safety Related Software in Defence Equipment

Bu doküman (DEF-STAN 00-55) İngiltere Savunma Bakanlığı tarafından 1997 yılında emniyet kritik sistemlerde kullanılacak yazılımların geliştirme sürecini anlatmak üzere yayımlanmış bir standarttır. Standart, yazılım geliştirme süreçlerinde dikkate alınması gereken kurallar (Requirements) ve bu kuralların uygulamasını anlatan bilgiler (Guidance) olmak üzere iki bölümden oluşmaktadır. Birinci bölümde "30. Use of Previously Developed Software" ve ikinci bölümde yer alan Ek-E "E.4.3 Previously Developed Software" bölümlerinde daha önce geliştirilmiş yazılımların uyum gösterimi ile ilgili gereksinimler ve yapılması gereken çalışmalar açıklanmıştır. Bu dokümana göre, yazılımın uçuş emniyetine olan etkisinin ve istenen tüm çalışmaların sonuçlarının "Yazılım Emniyet Durumu" (Software Safety Case) dokümanında otoriteye sunulması beklenmektedir [4]. Yazılım Emniyet Durumu dokümanı, sisteme ve tasarıma genel bakış, yazılım emniyet gereksinimleri, yazılım tanımı ve mimarisi, emniyet, yazılım geliştirme süreçleri, değişiklik yönetimi, uyum beyanı, servis geçmişi ve yazılım tanımlaması konularından oluşmaktadır.

4.2 Joint Software Systems Safety Engineering Handbook

Bu doküman, Amerikan Savunma Bakanlığı tarafından 2010 yılında, kabul edilebilir bir emniyet seviyesinde çalışabilecek yazılımların geliştirme süreçlerine kılavuzluk etmek amacıyla yayımlanmıştır. Dokümanın Ek D "COTS and Non-Developmental Item (NDI) Software" bölümünde, RAHAT yazılımların genel karakteristikleri, avantaj ve dezavantajları, aday yazılımların belirli bir sistem için uygunluğunu değerlendirmek üzere yapılması gereken aktiviteler, sisteme entegrasyonu kapsamında dikkate alınması gereken hususlar, risk azaltma metotları, yazılım emniyet durumu dokümanı içeriği ve konu ile ilgili bir örnek yer almaktadır [3].

4.3 *Commercial Off-The-Shelf Avionics Software Study*

Bu doküman Amerikan Sivil Havacılık Otoritesi, Havacılık Araştırma Ofisi tarafından 2001 yılında hazırlanmış olup, emniyet kritik sistemlerde RAHAT yazılımların endüstrideki kullanımları ile ilgili, endüstri temsilcileri ile yapılan görüşmelerden derlenen bilgileri içermektedir. Bu dokümanda, RAHAT cihaz üreticisi ile yüklenici arasındaki ara yüz, yazılım kaynaklı hata raporlarının yönetimi, bu süreçte tarafların sorumlulukları, RAHAT yazılımın kullanıldığı önceki ortam (environment) ve operasyonel profilinin, hedef ortam ile karşılaştırılması, kullanılmayan veya istenmeyen fonksiyonlar (unsued & unintended function) kapsamında yapılması gereken aktiviteler, RAHAT yazılıma ait versiyon kontrolü ve versiyonlar arasındaki izlenebilirliğin önemi, yeni yazılım sürümlerin sisteme etkileri, RAHAT yazılım geliştirme fazı boyunca tamamlanan süreçler, bu süreçlerin çıktıları ve geliştirme süreçlerinin uyumlu olduğu (ISO, CMMI) standartlara ait kanıtların kullanımı ile ilgili bilgiler içermektedir. Dokümanın son bölümde, RAHAT yazılımların emniyet seviyeleri ile DO-178B amaçlarını karşılama durumu hakkında, endüstri temsilcileri ile yapılan görüşmelerden elde edilen bilgiler sunulmuştur [7]. Buna göre;

Level A: Seviye A için DO-178B rehber dokümanında toplam 66 amaç vardır. Seviye A olan RAHAT yazılımların uyum gösterimi ile ilgili endüstrideki mevcut durum, bu yazılımların genellikle DO-178B amaçlarından birisi olan "Uyarlanmış Koşul/Karar Kapsaması" amacını karşılayamadığıdır. Ayrıca, 66 gereksinimden 25 tanesi bağımsızlık gerektiren gereksinimler olup, bu bağımsızlığı kanıtlayabilecek yeterli veriler genellikle elde edilememektedir.

Level B: Seviye B'de ise DO-178B rehber dokümanına göre 65 amaç vardır. Endüstrideki mevut durum Seviye A'ya benzer şekilde, DO-178B amaçlarından birisi olan "Karar Kapsaması" amacını karşılayamadığıdır. Burada da, 65 amacın 15 tanesinin bağımsız bir şekilde tamamlanmış olması gerekirken, genellikle bunu da gösteren yeteri kadar kanıt olmamaktadır.

Seviye C ve **Seviye D** RAHAT yazılımlar, aviyonik sektörde endüstri tarafından en çok kullanılan ve alternatif metotlar ile uyum gösteriminin genellikle otoriteler tarafından da en çok kabul edildiği yazılımlardır.

5 Sonuç

Bu bildiride, hava araçlarında kullanılan ve DO-178B uyumlu geliştirildiğine dair kanıtı olmayan RAHAT yazılımların, uyum gösterim sürecinde kullanılabilecek alternatif metotlar ve bu metotlar ile karşılanabilecek DO-178B amaçları hakkında bilgiler verilmiştir. Ayrıca, RAHAT yazılımların seçim sürecinde dikkate alınması gereken konular ve bu süreçte kullanılabilecek bir soru listesi sunulmuştur. Tedarik edilecek RAHAT yazılımların, sistem emniyeti ve performansı üzerinde oluşturacağı etki nedeni ile detaylı bir şekilde değerlendirilmesi hususunun altı çizilmiş, projelerinde RAHAT yazılım kullanmayı planlayan firmalara öncelikle, gerekli tüm rollerin (sistem mühendisi, emniyet sorumlusu, sistem tasarımcısı, yazılım lideri gibi) dahil olacağı, kriterleri belli olan sistematik bir değerlendirme süreci tanımlaması önerilmiştir.

RAHAT yazılım kullanacak yüklenicilere, yazılım tedarikçilerinden DO-178B amaçlarını karşılama durumlarını değerlendirdikleri “Fark Analizi Çalışması”’ istemleri tavsiye edilmektedir. Fark analizi çalışması, yüklenicinin sertifikasyon sürecinde ayıracağı kaynak planlaması için de önemlidir.

Uyumu onayı olmayan RAHAT yazılımlar için, yüklenicinin uyum gösterim sürecinde kullanmayı planladığı alternatif metotları YSKP dokümanında açıklaması ve sertifikasyon otoritesi ile projenin erken safhalarında anlaşma sağlaması sertifikasyon sürecinin başarısı için elzemdir.

Daha önce DO-178B ile ilgili bir deneyimi olmayan ve misyonunda sivil hava sahasında uçacak hava araçlarına RAHAT yazılım üretmek olan firmalara, işletmelerinde DO-178B ile ilgili gerekli alt yapıyı kurmaları ve yazılım geliştirme süreçlerinde DO-178B amaçlarını dikkate almaları önerilmektedir. Bu durumun, RAHAT yazılım üreticisine piyasada çok ciddi rekabet avantajı sağlayacağı değerlendirilmektedir. RAHAT yazılım üretimini tamamlamış firmalara ise, DO-178B amaçlarını karşılama durumlarını değerlendirerek, uyumu gösteriminde kullanılabilecek kanıt dokümanlarını analiz etmeleri ve varsa eksik kanıt dokümanlarını üretmeleri önerilmektedir. Bu analiz, olası bir yazılım kaynaklı hatanın uçuş emniyetini olumsuz etkilememesi için üretilmiş yazılım yaşam döngüsü verilerinin (gereksinimler, tasarım, kod, kontrol ve veri akışları, kapsama analizleri gibi) bir kez daha incelenmesi için bir fırsattır.

Referanslar

1. Radio Technical Commission for Aeronautics (RTCA), DO-178B, (1992)
2. DO-248, Final Report for Clarification of DO-178B “Software Considerations in Airborne Systems and Equipment Certifıcation, RTCA, 2001
3. Joint Software Systems Safety Engineering Handbook, Department of Defence USA, 2010
4. DEF-STAN 00-55, Requirements For Safety Related Software In Defence Equipment, Part 1:Requirements & Part 2:Guidanece, United Kingdom Ministry of Defence,1997
5. Order 8110.49 - Software Approval Guide, FAA, 2003
6. Software Safety Guidebook, NASA, 2004
7. COTS Avionics Software Study, FAA Office of Aviation Research, 2001
8. 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