8. ULUSAL HAVACILIK VE UZAY KONFERANSI
9-11 Eylül 2020, Türk Hava Kurumu Üniversitesi, Ankara

UHUK-2020-143

UZAY ARAÇLARI İÇİN GÜVENİLİRLİK, KULLANILABİLİRLİK, BAKIM VE GÜVENLİK TEMELLİ PLATFORM VERİ İŞLEME SİSTEMİ TASARIM YÖNTEMİ

Ahmet Burak KOÇ[1] ve Koray BAYRAKTAR[2]
Türksat A.Ş., Ankara

Hasan Hüseyin ERTOK[3]
Türksat A.Ş., Ankara

ÖZET

Uzay araçları tasarlama sürecinde başarı ihtimalini çok yüksek seviyelerde tutmak ve görevin başarısızlıkla sonuçlandığı durumda dahi uzay çevresine, başka uzay araçlarına veya insanlı görev icra eden uzay aracındaki insanlara zarar vermeden uzay aracının güvenli bir şekilde yeryüzüne inmesini sağlamak için güvenilirlik, kullanılabilirlik, bakım ve güvenlik analizleri yapılmaktadır. Uzay aracının yer istasyonundan aldığı komutlarla birlikte otonom olarak da görev yönetimini sağlayan, alt sistemleri görev modlarına göre yöneten ve yer istasyonuna gönderilecek telemetri verisini düzenleyen Platform Veri İşleme Sisteminin de bu analizlere uygun bir şekilde tasarlanması görev gereksinimlerini sağlamakta ciddi önem arz etmektedir. Bu bildiride, güvenilirlik, kullanılabilirlik, bakım ve güvenlik analizleri temel alınarak Platform Veri İşleme Sistemi tasarım yöntemi sunulmuştur. Tasarım yöntemi anlatılırken başlangıç noktası olarak acil durumda Uluslararası Uzay İstasyonu (ISS)'deki astronotları Dünya'ya getirecek bir kurtarma görevi örnek görev olarak değerlendirilmiştir.

KISALTMALAR

AOCS	: Attitude and Orbit Control System (Yönelim ve Yörünge Kontrol Sistemi)
ATV	: Automated Transfer Vehicle (Otomatik Transfer Aracı)
DHS	: Data Handling System (Platform Veri İşleme Sistemi)
ECLS	: Environment Control and Life Support (Çevre Kontrolü ve Yaşam Destek Sistemi)
ESA	: European Space Agency (Avrupa Uzay Ajansı)
FIT	: Failure In Time
GPS	: Global Positioning System (Küresel Konumlama Sistemi)
ISS	: International Space Station (Uluslararası Uzay İstasyonu)
MTBF	: Mean Time Between Failures (Arızalar Arası Ortalama Zaman)
NASA	: National Aeronautics and Space Administration (Ulusal Havacılık ve Uzay Dairesi)
PASO	: Product Assurance and Safety Office (Ürün Güvence ve Güvenlik Ofisi)
PCS	: Power Control System (Güç Kontrol Sistemi)
TCS	: Thermal Control System (Isıl Kontrol Sistemi)
TM / TC	: Telemetry and Telecommand (Telemetri ve Tele-komut Sistemi)

[1] Müh., Teknik Personel, Türksat A.Ş., E-posta: abkoc@turksat.com.tr
[2] Müh., Teknik Personel, Türksat A.Ş., E-posta: kbayraktar@turksat.com.tr
[3] Genel Müdür Yardımcısı, Türksat A.Ş., E-posta: hertok@turksat.com.tr

GİRİŞ

Platform veri işleme sistemi (DHS) sahip olduğu fonksiyonları sayesinde, uzay aracının alt sistemleri arasında düzenli bir veri akışını sağlamaktadır. Sistem gerekli şartlarda otonom kararlar verme, uzay aracının alt sistem durumlarının sürekli olarak gözlemlenmesi, tele-komutları uygulamak ve ilgili alt sistemlere dağıtmak ve veriyi depolamak gibi birçok sorumluluğa sahiptir. Bu sistemin karmaşıklık seviyesi, icra edilecek olan görevle ve uzay aracının sahip olduğu alt sistem çeşitliliğiyle doğrudan ilişkilidir. Bu durum sistemin tasarım sürecini kolaylaştırmak ve sistematikleştirmek adına bir tasarım yöntemi sunmayı zorunlu hale getirmektedir.

Uzay teknolojileri kapsamında hayata geçirilen insanlı projelere ve üretilen sistemlere, alt sistemlere ve ekipmanlara uzay ajanslarının geliştirdiği birtakım mühendislik, yönetim, sürdürülebilirlik ve kalite güvence standartları uygulanmaktadır. Uzay ajanslarının bu doğrultudaki hedefleri görevi ve insanların hayatlarını tehlikeye atabilecek olan tüm tehlike ve risklerin derin bir şekilde değerlendirilip, bunların hafifletilme planlarının yapılarak birinci sınıf bir güvenlik programı ortaya çıkarabilmektir. Ulusal Havacılık ve Uzay Dairesi (NASA)'nın insanlı uzay görevlerine uyguladığı standartlardan biri de NPR 8705.2 'Human-Rating Requirements for Space Systems' (Uzay Sistemleri için İnsan Derecelendirme Gereksinimleri)'dir [Jakhu ve Pelton, 2010]

NASA'nın uzay projelerindeki birçok sistemi 'İnsan Derecelendirme Sertifikasını' gerektirmektedir. ISS gibi bu sertifikayı gerektiren projeler için, NASA uzay görevlerinde mürettebat üyelerinin ve yolcuların güvenliğini teminat altına alan bu sistemleri üretmek için gerekli ek süreçleri, prosedürleri ve gereksinimleri uygulamaktadır (NPR 8705.2). Bu sertifikaya sahip sistemler, insan ihtiyaçlarını karşılar, insan yeteneklerini etkin bir şekilde kullanır, tehlikeleri sürekli olarak kontrol eder ve insanlı uzay uçuşu ile ilişkili güvenlik riskini yönetir. Ayrıca, gerektiğinde mürettebatı güvenli bir şekilde kurtarma kabiliyeti sağlar. 'NPR 8705.2' sistemin yaşam döngüsü boyunca tüm program faaliyetlerine (tasarım ve geliştirme, test & doğrulama, program yönetimi & kontrolü, uçuşa elverişlilik, görev operasyonları, bakım ve görev sonu prosedürleri) uygulanmaktadır.

Sertifikasyonun önemli ögeleri aşağıdaki gibi özetlenebilir;

- Sertifikasyon için referans görevin tanımı
- Referans görevin her fazı için mürettebatın hayatta kalma stratejilerinin sistem kabiliyetlerine göre değerlendirilmesi
- Sistem geliştirme ve tasarımına etki edecek güvenlik analizlerinin yapılması
- İnsanın sisteme dahil edilmesi ve insan kaynaklı hataların yönetilmesi
- Kritik sistemlerin performansının sağlaması, doğrulaması ve testi
- Uçuş test programı ve testin hedefleri
- Sistem konfigürasyon yönetimi ve sertifikanın gerektirdiği ilgili bakım-onarım

Avrupa'da ise Avrupa Uzay Ajansı (ESA)'ya bağlı Ürün Güvence ve Güvenliği Ofisi (PASO) insanlı uzay uçuşları için güvenlik standartlarından sorumludur. Bu kapsamda sertifikasyon ve gereksinimler süreci Otomatik Transfer Aracı (ATV)'ye yüklenecek faydalı yükleri, kargo malzemelerini ve ISS'de kulanılacak malzemeleri içermektedir. ESA tarafından kullanılan ISS güvenlik standartları genellikle ISS'nin Amerikan ve Rus ortakları tarafından kullanılan standartlar olmakla birlikte, ESA PASO genel olarak iki kategoride kargo ve insan güvenliği standartlarından sorumludur: ATV Gereksinimleri ve Kourou Yer Güvenlik Gereksinimleri [Jakhu ve Pelton, 2010].

Bu çalışmada sunulan metodun ilk basamağı görev gereksinimlerini doğru bir şekilde idrak edip, görevin analizini yapmak olarak verilmiştir. Görev analizi yapıldıktan sonra, sunulan yöntemin ikinci adımında veri yönetimi sistemi analizi yapılmıştır. Yöntem kapsamında, üçüncü ana adımda uzay aracının işlevsel zincirlerinin temel mimari tasarımının yapılması olmuştur. Yöntemin dördüncü adımında işlevsel zincirler arası bağlantılar da yapılarak tüm DHS mimarisi oluşturulmuştur. Son adımda oluşturulan mimari kütle, güç tüketimi, maliyet yönünden iyileştirilerek güncellenebilir. (Şekil 1).

Şekil 1: DHS Tasarım Yöntemi Akış Şeması

TASARIM YÖNTEMİ VE UYGULAMALARI

DHS sahip olduğu telekomut ve telemetri fonksiyonları, operasyonel ve göreve göre değişiklik gösterebilen alt sistem fonksiyonları ve hata tespit-çözüm fonksiyonları açısından uzay aracı için kayda değer bir önem arz etmektedir. Bu fonksiyonlar, DHS sorumluluğunda çeşitli ekipmanlar ve yazılımlar vasıtasıyla gerçekleşmektedir. Görev ve uzay aracının sağlığı açısından çok kapsamlı fonksiyonel özellikleri barındıran bir sistem olan DHS, beraberinde zorlu gereksinimleri de tetiklemektedir. Bu gereksinimlerin kapsamı; yüksek radyasyon toleransı, güvenilirlik ve kullanılabilirlikten başlayarak protokol güvenlik faktörlerini içeren uzay aracı ve yer istasyonu arasındaki veri haberleşme protokollerine kadar uzanmaktadır. Sistem tasarlanırken göz önünde bulundurulması gereken önemli hususlar ise aviyonik mimarinin, veri ağı ve yollarının belirlenmesidir. Bu amaç doğrultusunda, temel olarak ilgili görevin gereksinimlerinin iyi anlaşılması, görevin analizinin doğru bir şekilde yapılması, veri yönetim sistemi analizinin gerçekleştirilmesi, işlevsel zincirlerin temel mimarisinin oluşturulması ve her bir alt sistem için detaylı hata toleranslarının hesaba katılmasını kapsayan bir yöntem geliştirme ihtiyacı ortaya çıkmaktadır.

İyi bir tasarıma giden yolda görev gereksinimlerinin doğru bir şekilde anlaşılması önem arz etmektedir. Aksi takdirde, tasarımda katastrofik hatalar kaçınılmaz hale gelebilmektedir.

Görev Analizi

Görev analizinin ilk adımında görev fazları belirlenir ve tanımlanır. Bu fazların sayısı ve çeşitliliği, icra edilecek uzay göreviyle doğrudan ilişkilidir. Varsayılan örnek görev gereksinimlerine göre görev fazları ve tanımları yapılmıştır.

İkinci adımda, her bir görev fazının azami olarak ne kadar süreceği tespit edilmiştir. Fazların süresi, o fazda görev yapacak her bir ekipmanın güvenilirlik tespit çalışmalarını doğrudan etkilemesi açısından önem arz etmektedir. Fazların süresi uzadıkça ekipmanların hata verme olasılığı arttığı için güvenilirlik hesaplamaları en kötü duruma göre yani fazların maksimum sürelerine göre hesaplanacaktır.

Görev analizi kapsamında yapılması gereken son işlem; her bir görev fazını başlatan ve sonlandıran olayların belirlenmesidir. Bu olayların tespiti, uzay aracının merkezi bilgisayarının modları (kalkış, kilitlenme, serbest uçuş vs.) arasındaki geçişler açısından son derece önemlidir. Bu nedenle, olayların somut olarak merkez bilgisayarda tanımlanabilecek şekilde belirtilmesi gerekmektedir.

Bu bildiride belirlenen örnek görev fazlarının (Tablo 1) belirlenmesinde, özellikle ISS'e yaklaşma ve ayrılma fazlarında, ESA'nın ATV görev profilinden ve manevra planlarından yararlanılmıştır. ATV'nin Jules Vernes Uzay aracı'nın görev profilinde S(-1/2) noktası ISS'in 39 km arkasında, 5 km altında tanımlanmaktadır. S(-1/2) noktasında bir sonraki görev fazına (buluşma ve kenetlenme) geçilmekte ve bu fazda manevralar uzay aracının ISS referansına göre bağıl konumu kullanılarak yapılmaktadır. Buluşma ve kenetlenme manevraları sırasıyla S(0), S(1), S(2) ve S(3) noktalarından geçerek tamamlanmaktadır. Ayrılmadan sonra ise S(3) noktasına kadar ISS'ten uzaklaşıldıktan sonra kaçış manevrası yapılmaktadır [Labourdette, Julien, Chemama ve Carbonne, 2009]. Görev

fazları arasındaki geçişlerin somut olarak merkez bilgisayarda tanımlanabilmesi için kullanılacak sensörler de belirlenmiştir. Örnek olarak, serbest uçuş fazında GPS verisi ile alınan konum ölçümlerine göre S(-1/2) konumuna ulaşıldığında merkezi bilgisayar buluşma & kenetlenme fazına geçişi yapacaktır.

Tablo 1: Görev Fazlarının Başlangıç ve Bitiş Olayları

Faz Adı	Maksimum Süre	Başlangıç Olayı	Bitiş Olayı	Bitiş Olayının Tespitinde Kullanılacak Yöntem	Açıklama
Fırlatma	40 dk	Ateşleme	Ayrılma	Ayrılma sensörü verisi	Uzay aracının fırlatıcıdan ayrılması
Serbest Uçuş	20 gün	Ayrılma	S(-1/2) konumuna varış	GPS verisi	-
Buluşma & Kenetlenme	30 dk	S(-1/2) konumuna varış	Kilitlenme	Piezo elektrik sensör verisi	-
Bekleme	< 10 yıl	Kilitlenme	Alarm	Telekomut (Otonom alarm)	Periyodik sistem kontrolü yapılır
Ayrılmaya Hazırlık	< 2 sa	Alarm	"Hazır" komutu	Telekomut (Operatör komutları)	-
Ayrılma	30 dk	"Hazır" komutu	S3 + "Hazır" komutu	GPS verisi ve Telekomut	Uzay aracının ISS'ten ayrılması
Serbest Uçuş	2 sa	S3 + "Hazır" komutu	İniş	-	Serbest uçuş ve atmosfere giriş
İniş sonrası		-	-	-	-

Veri Yönetim Sistemi Analizi

Tasarım fazında yapılması gereken bir çalışma ise kapsamlı bir veri yönetim sistemi analizidir. Analiz sürecinin ilk adımı, sistemin fonksiyonel zincirlerinin tanımlanmasını içerir. Bu zincirlerin belirlenmesinde icra edilen uzay görevi ve tasarlanan uzay aracının alt sistemleri önemli bir rol oynamaktadır. Uzay aracının sahip olduğu alt sistem çeşitliliği işlevsel zincir alt kırılımlarını doğrudan etkilemektedir. Alt sistemler arasındaki işlevsel zincir dallanmaları gerçekleştirildikten sonra, her bir alt sistemin her görev fazındaki önem dereceleri belirlenir. Bu bildirideki örnek tasarım için ilgili görev fazındaki faydalı ancak kullanılması zorunlu olmayan alt sistem fonksiyonları için 1 rakamı, kullanılması zorunlu fakat kısıtlı performansta da yeterli olacak alt sistem fonksiyonları için 2 rakamı, tam performansta kullanımı zorunlu olan fakat hata durumu için kurtarma süresinde yüksek derece zaman kısıtlaması olmayan alt sistem fonksiyonları için 3 rakamı, 1 dakikanın altında zaman kısıtlaması olan alt sistem fonksiyonları için 4 rakamı ve 1 saniyenin altında zaman kısıtlaması olan alt sistem fonksiyonları için 5 rakamı kullanılmıştır (Tablo 2).

AOCS, uzay aracının ISS'e yakın olduğu ve ayrılıp atmosfere giriş yapacağı fazlarda gerçek zamanlı manevra kontrolleri yapacağı için alt sistemin kritiklik seviyesi bu fazlarda 5 olarak belirlenmiştir.

TM/TC alt sistemi için uzay aracının yönetilebilir durumda olmadığı fırlatma, bekleme (ISS'e kenetlenmiş durumda) gibi görev fazlarında yüksek zaman kısıtlaması yoktur fakat araç sağlığının doğru bir şekilde gözlemlenebilir olması gerekmektedir. Bu nedenle, kritiklik seviyesi 3 olarak belirlenmiştir. Uzay aracının aktif olduğu görev fazlarında, güvenilirlik ve güvenlik gereksinimlerini karşılaması için telemetri verisini hızlı ve hatasız işlemesi ve telekomutlara hızlı ve doğru tepki vermesi gerekmektedir. Bu nedenle aktif görev fazlarında kritiklik seviyesi 4 olarak belirlenmiştir.

PCS, bütün alt sistemlere güç sağlayacak olan alt sistemdir. Eğer yüksek kritiklik seviyelerinde bir alt sistem varsa, PCS'te yaşanacak problem sonucu bu kritik alt sistemde bir güç kesintisi yaşanmaması için PCS'in de aynı kritiklik seviyesinde çalışması gerekmektedir. Bu nedenle, PCS kritiklik seviyesi, görev fazlarındaki en kritik alt sisteme göre belirlenmiştir.

ECLS, kurtarılacak astronotlara yaşayabilecekleri ortamı sağlayacak olan alt sistemdir. Uzay aracı ISS'e otonom olarak ulaşacağı için, içinde sadece ISS'ten ayrılma fazı ve sonrasında astronot bulunmaktadır. ISS'e ulaşmadan önce uzay aracında astronot bulunmadığı için bu alt sistemin yüksek bir kritikliği yoktur. Astronotlar uzay aracındayken de uzay aracının iç koşulları (oksijen seviyesi, sıcaklık vs.) ani değişiklik gösteremeyeceği için 3 olarak belirlenmiştir.

Uzay aracı ekipmanlarının sıcaklık değerleri ani değişiklik gösteremeyeceği için TCS'in kritiklik seviyesi de 3 olarak belirlenmiştir.

Görev Yönetimi'nin kritiklik seviyesi de fonksiyonu zorunlu olduğu fakat ciddi bir zaman kısıtlaması olmadığı için 3 olarak belirlenmiştir.

Tablo 2: Görev Fazı / Alt Sistem Kritiklik Seviyeleri

Faz \ Alt Sistem	AOCS	TM/TC	PCS	ECLS	TCS	Görev Yönetimi
Fırlatma	1	3	3	1	3	3
Serbest Uçuş	4	4	4	1	3	3
Buluşma & Kenetlenme	5	4	5	1	3	3
Bekleme	1	3	3	3	3	3
Ayrılmaya Hazırlık	3	3	3	3	3	3
Ayrılma	5	4	5	3	3	3
Serbest Uçuş	5	4	5	3	3	3
İniş sonrası	1	3	4	3	3	3

İşlevsel Zincir Temel Mimarisi

Veri yönetim sistemi analiz çalışmalarını, işlevsel zincirlerin temel mimarisinin oluşturulması adımı takip etmektedir. Buna istinaden, önceden belirlenmiş olan uzay aracına ait her bir alt sistem için ekipman seçimleri yapılır. Ekipman seçimlerinde görev isterlerine uygunluk, performans, fiziksel özellikler ve maliyet gibi ana parametreler önemli rol oynamaktadır.

Bu bildiride örnek olarak AOCS ekipmanları belirlenmiştir (Tablo 3).

Tablo 3: AOCS Ekipmanları ve Adetleri

Ekipman	Adet	Açıklama
Yıldız Takipçisi (STR)	1	3-eksende yönelim ölçümü
Dinamik olarak ayarlanmış jiroskop (DTG)	4	Açısal hız ölçümü (3-eksen konfigürasyonu)
İvmeölçer (ACC)	6	İvme ölçümü
Vidyometre (VM)	1	ISS'e göre yönelim ve pozisyon ölçümü
GPS alıcısı	1	Konum ölçümü
Tepki Tekeri (RW)	4	Yönelim eyleyicisi (3-eksen konfigürasyonu)
İtici (THR)	12	3-eksende ötelenme ve dönme için itki
Bilgisayar	1	Sensör verisi işleme ve eyleyici komutlarının hesaplanması

Listedeki ekipmanlar yedeklilik hesaba katılmadan uzay mirasına sahip ve çeşitli görevlerde kullanılmış olan ekipmanlar göz önünde bulundurularak belirlenmiştir.

Ekipmanlar belirlendikten sonra sırasıyla kullanılabilirlik, güvenilirlik ve güvenlik analizleri yapılarak bütün işlevsel zincirler için DHS ön tasarımı gerçekleştirilir. Bu fazdaki tasarım kapsamında ekipman sayıları ve DHS mimarisi kabaca belirlenebilir. Ekipman sayıları ve bilgisayar sayıları belirlendikten sonra, güvenilirlik, kullanılabilirlik ve bakım ihtiyaçlarını sağlayacak şekilde işlevsel zinciri kontrol edecek bilgisayarlar karakterize edilir. Bu bildirideki örnekte her 6 ayda bir uzay aracının bakımı yapılacaktır.

Alt sistem işlevinin kritiklik seviyesine göre kullanılabilirlik analizi yapılır ve yedeklilik tipi (aktif yedeklilik, pasif yedeklilik) belirlenir. Örneğin, pasif yedeklilik kullanılan bir alt sistemde yedek ekipman pasif durumdan aktif duruma geçmesi zaman aldığı için kritiklik 5 seviyesine sahip bir alt sistemde pasif yedeklilik kullanılamaz. Bu bildirideki örnek görev için tasarlanacak AOCS, özellikle ISS'e yakın olduğu görev fazlarında 5 kritiklik seviyesine sahiptir. Kullanılabilirlik analizi sonucu AOCS bilgisayarlarının 3 aktif bilgisayar olacak şekilde yedeklilik gerektiği belirlenmiştir. Böylece, işlevsel zincirde meydana gelecek bir hata hızlı bir şekilde tespit edilebilecek ve hatalı bilgisayar devre dışı bırakılabilecektir.

Güvenilirlik analizi için güvenilirlik blok diyagramları oluşturulur. Bu bildirideki örnek görevde insanlı uçuş olacağı için yüksek güvenilirlik ihtiyacı bulunmaktadır ve 0.99 olarak varsayılmıştır. Her parçanın görev boyunca aktif olduğu süre ve hata verme sıklığı gibi karakteristikleri ($\boldsymbol{\lambda_{aktif}}, \boldsymbol{\lambda_{pasif}}$) göz önünde bulundurularak güvenilirlik hesabı yapılır. $\boldsymbol{\lambda}$(t) zamana bağlı olarak değişken olmakla birlikte pratik uygulamalarda genellikle sabit bir $\boldsymbol{\lambda}$ değeri olarak alınır. Örnek çalışmada

bilgisayarların hata verme sıklığı 8000 FIT olarak alınmıştır. Hata verme sıklığı aktif ekipmanda pasif ekipmana göre 10 kat fazla olarak alınmıştır. (1)'deki eşitliğe göre $\boldsymbol{\lambda}$ değerleri aktif ve pasif ekipmanlar için (2)'deki şekilde hesaplanmıştır [Birolini, 2007].

$$1\ FIT = 10^{-9}\ \frac{hata}{saat(h)} \tag{1}$$

$$\lambda_{on} = 8 * 10^{-6}\ h^{-1}, \qquad \lambda_{off} = 8 * 10^{-7}\ h^{-1} \tag{2}$$

Aktif ve pasif olduğu süreler sırasıyla t_{on} ve t_{off} olan ekipmanın güvenilir bir şekilde çalışma olasılığı (3)'te verilen denkleme göre hesaplanır.

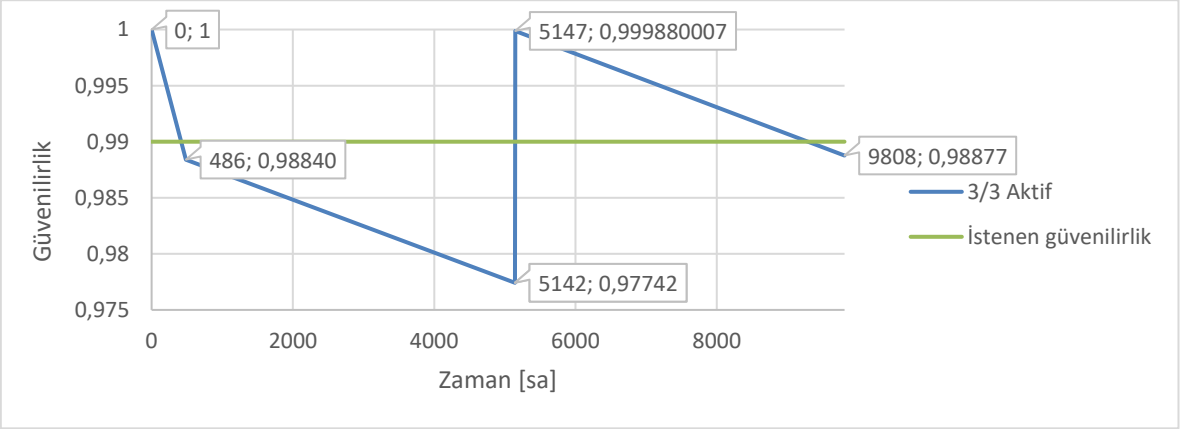
$$P_1(t) = e^{-\lambda_{on} t_{on}} * e^{-\lambda_{off} t_{off}} \tag{3}$$

Bu bildirideki örnekte 3 bilgisayar eş zamanlı aktif olacağı için güvenilirlik (4)'teki şekilde hesaplanır.

$$P_3(t) = P_1^3(t) \tag{4}$$

Tablo 1'deki verilen görev fazlarının maksimum sürelerine göre bilgisayarların aktif veya pasif olduğu süreler değişmektedir. ISS'e kenetlenmeden önceki süreçte 3 bilgisayar aktif olacaktır ve ISS'e kenetlendikten sonra bilgisayarlar pasif olacaktır. Bu nedenle, en kötü senaryoda güvenilirlik değerleri zamanla Şekil 2'deki gibi değişecektir.

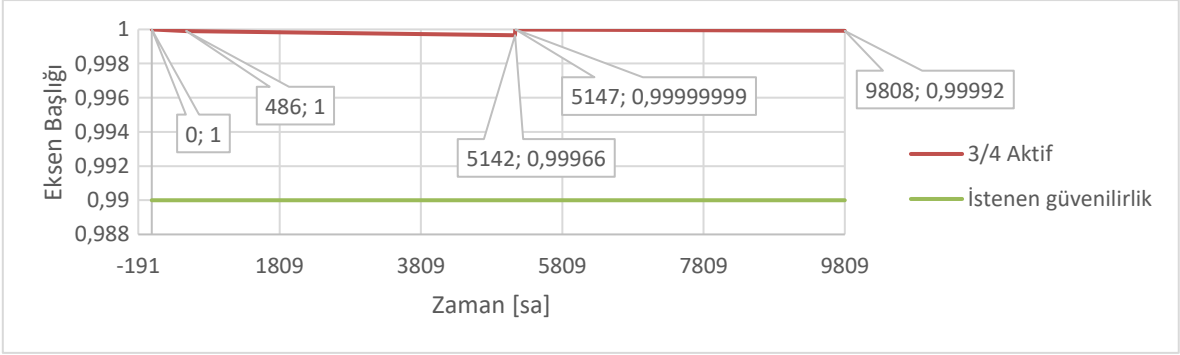
Örnek hesaplamalarda her 6 ayda yapılan bakımlarla güvenilirlik seviyesi tekrar 1'e çekilmiştir.



Şekil 2: Başarı Olasılık Grafiği (3 bilgisayar)

Güvenilirlik analizi sonuçlarına göre 3 aktif bilgisayardan bir bilgisayarın hata vermesi durumunda sistemin kullanılabilirlik gereksinimi karşılanamayacaktır. Bu nedenle, 3 aktif bilgisayarın yanında 1 pasif bilgisayar daha yedek olarak tasarıma eklenmiştir. 3 aktif ve 1 pasif bilgisayarlı sistemin güvenilirlik analizi (5)'teki şekilde hesaplandığında güvenilirlik gereksinimi karşılanmış olur (Şekil 3).

$$P_{3/4}(t) = P_1^4(t) + 4 * \big(1 - P_1(t)\big) * P_1^3(t) \tag{5}$$



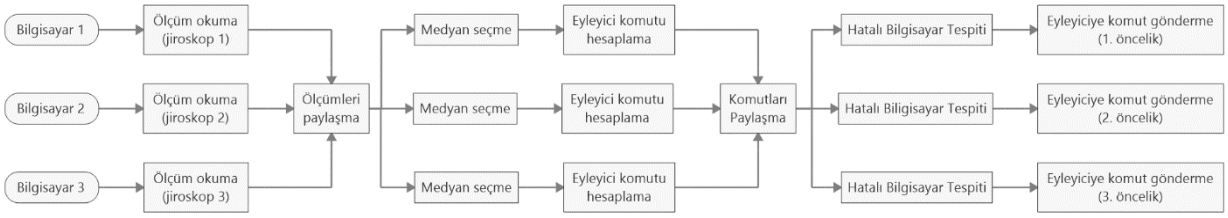
Şekil 3: Başarı Olasılık Grafiği (3 bilgisayar + 1 yedek bilgisayar)

Güvenilirlik gereksinimi de karşılandıktan sonra güvenlik analizi yapılmaktadır. Eğer donanım veya yazılımda yapılmış fakat tespit edilememiş kronik bir hata varsa bütün tasarım başarısızlıkla sonuçlanabilir. İnsanlı bir uzay görevi olduğu için en kötü durumda bile uzay aracının ISS'teki veya kendi bünyesindeki insanlara zarar vermemesi için güvenlik önlemleri alınmalıdır. Bu durum, asıl tasarıma ek olarak tamamen bağımsız yeni bir hata modu bilgisayarını gerekli kılar. Bu nedenle, tasarıma Bilgisayar 5 ve Bilgisayar 6 tamamen bağımsız donanım ve yazılıma sahip olarak eklenmiştir.

Güvenilirlik blok diyagramlarının planlanan şekilde çalışması ve istenen güvenilirlik seviyesinin sağlanması bilgisayarların karakterizasyonuna bağlıdır. Öncelikle, bilgisayarların tasarımındaki gereksinimler (bütün bilgisayarların senkron çalışması, aynı donanıma ve aynı yazılıma sahip olması vs.) belirlenmektedir. Ardından, ekipmanlardaki hatayı tespit edip düzeltmeyi yaparak eyleyicilere doğru komutu gönderecek şekilde bilgisayar işlemlerinin zamanlaması planlanmaktadır.

Bu bildirideki örnek tasarımda AOCS bilgisayarının sensör verisi toplama ve eyleyiciye komut gönderme işlemleri Şekil 4'de gösterilmiştir. Bu örnekte sensör verileri toplanıp diğer bilgisayarlarla paylaşıldıktan sonra, en doğru veriyi seçmek için ölçümlerin medyan değeri seçilir. Ardından bütün bilgisayarlar aynı girdiyle eyleyiciye gönderilecek komutları hesaplar. Komutlar paylaşıldıktan sonra 3 komutun aynı olması beklenir. Eğer komutlarda farklılık varsa aynı olan 2 komut doğru, farklı olan komut yanlış olarak değerlendirilir ve yanlış komutu hesaplayan bilgisayar hatalı olarak tespit edilir. Bilgisayar 1'de hata tespit edilirse diğer bilgisayarlar PCS'e Bilgisayar 1'in gücünü kesme komutu yollarlar ve eyleyici kontrolü sırasıyla Bilgisayar 2 ve Bilgisayar 3'e geçer.

Haberleşme, veri yolları (bus) üzerinden gerçekleşir ve her veri yolunun ana birimi ve yardımcı birimleri de bu aşamada belirlenir.



Şekil 4: Bilgisayar işlem algoritması

Detaylı Arıza-Kaldırır Mimari

Bu adımda, işlevsel zincirler arası bağlantılar oluşturulur ve arıza durumlarında toleransları kontrol edilerek detaylı bir arıza-kaldırır mimari oluşturulur.

Sensörler, eyleyiciler, merkezi bilgisayarlar, veri yolları ve uzay aracının çeşitli alt sistemleri arasında işlevsel zincir ara bağlantısı oluşturulurken yedeklilik hususunun itinayla göz önünde bulundurulması gerekmektedir. Bu durum, DHS kapsamında kullanılacak veri yolu sayısını ve mimarisini doğrudan etkilemektedir. Geliştirilen yöntem bünyesinde, arıza-kaldırabilir mimari tasarımının son adımı her bir ekipman için güç veri yolunun mimarisinin tasarlanmasıdır. Bilgisayar karakterizasyonunda bahsedilen yöntemle bilgisayarlardan birinde hata tespit edildiğinde PCS'e bu yönde telemetri gönderilecek ve PCS hatalı bilgisayarın gücünü kesecektir.

Mimarinin son durumu AOCS işlevsel zinciri için oluşturulmuştur (Şekil 5).

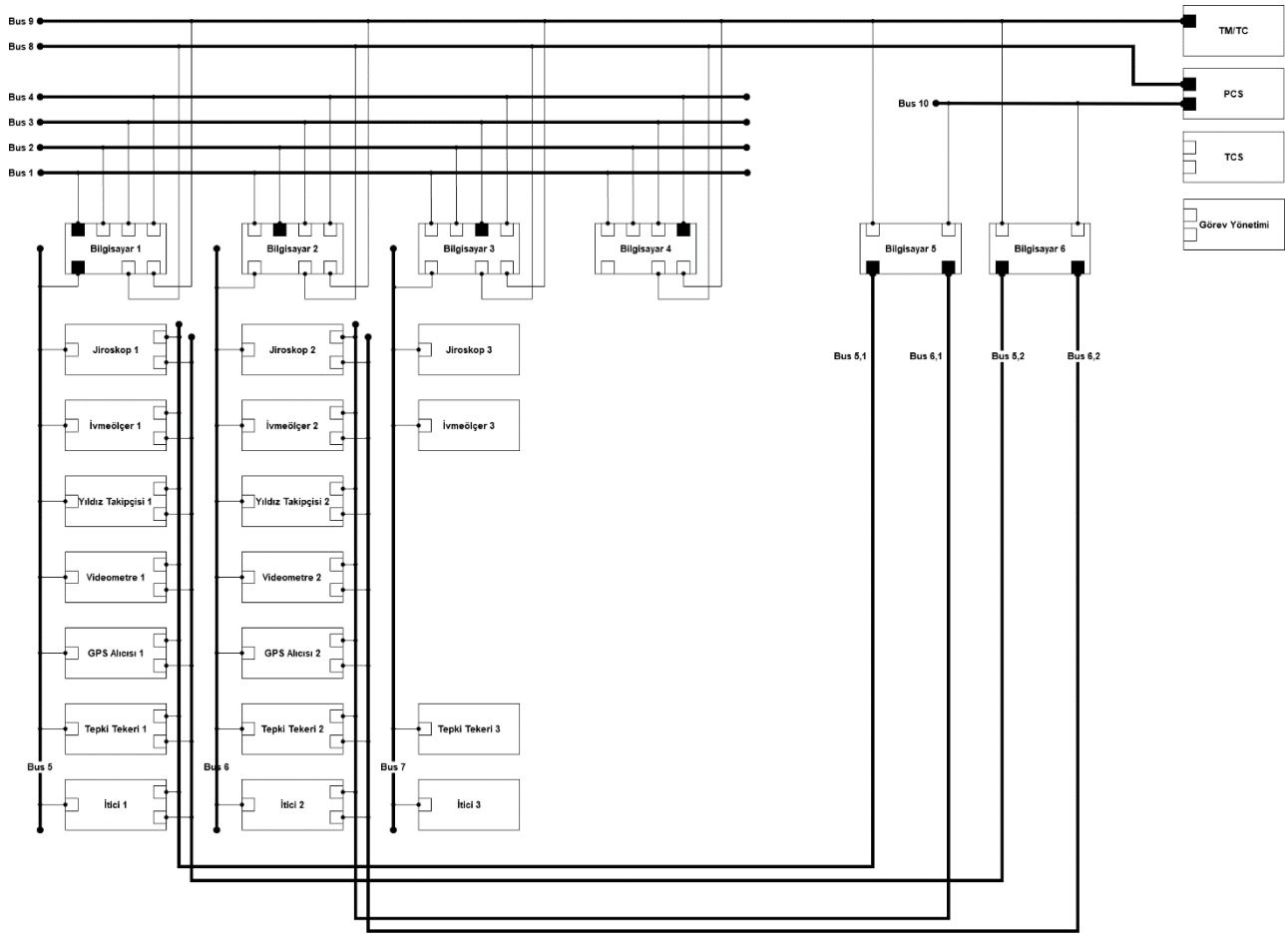
İyileştirme

Bu bildiride anlatılan tasarım yöntemindeki tasarım adımları işlevsel zincirlerin RAMS analizleri temelinde ilerlemektedir. Bu nedenle; tasarımın kütle, güç tüketimi ve maliyet bağlamında verimsizlikleri mevcut olabilir. Her işlevsel zincir için detaylı mimari oluşturulduktan sonra kütle, güç tüketimi ve maliyet yönlerinden iyileştirmeler yapılmaktadır.

Örnek olarak, 3 eksende 4 tepki tekerli piramit konfigürasyonunda herhangi bir tepki tekeri hata verdiğinde diğer 3 tepki tekeri 3 eksende yönelim kontrolü sağlayabilmektedir. Bu şekilde 6 tepki tekerine göre ciddi kütle ve maliyet iyileştirmesi yapılabilir.

Bilgisayar donanım ve yazılımında gerçek zamanlı işlem algoritması ve zaman çizelgelemesi iyileştirilerek bilgisayarlar birden fazla işlevsel zincirde kullanılabilir böylelikle kütle, güç tüketimi ve maliyetten kazanç elde edilebilir.

Ekipmanların güç yönetimi ve pasiflik-aktiflik durumları iyileştirilerek güç tüketiminden kazanç sağlanabilir.



Şekil 5: Uzay Aracının Arıza-Kaldırabilir Platform Veri İşleme Sistem Mimarisi

SONUÇ

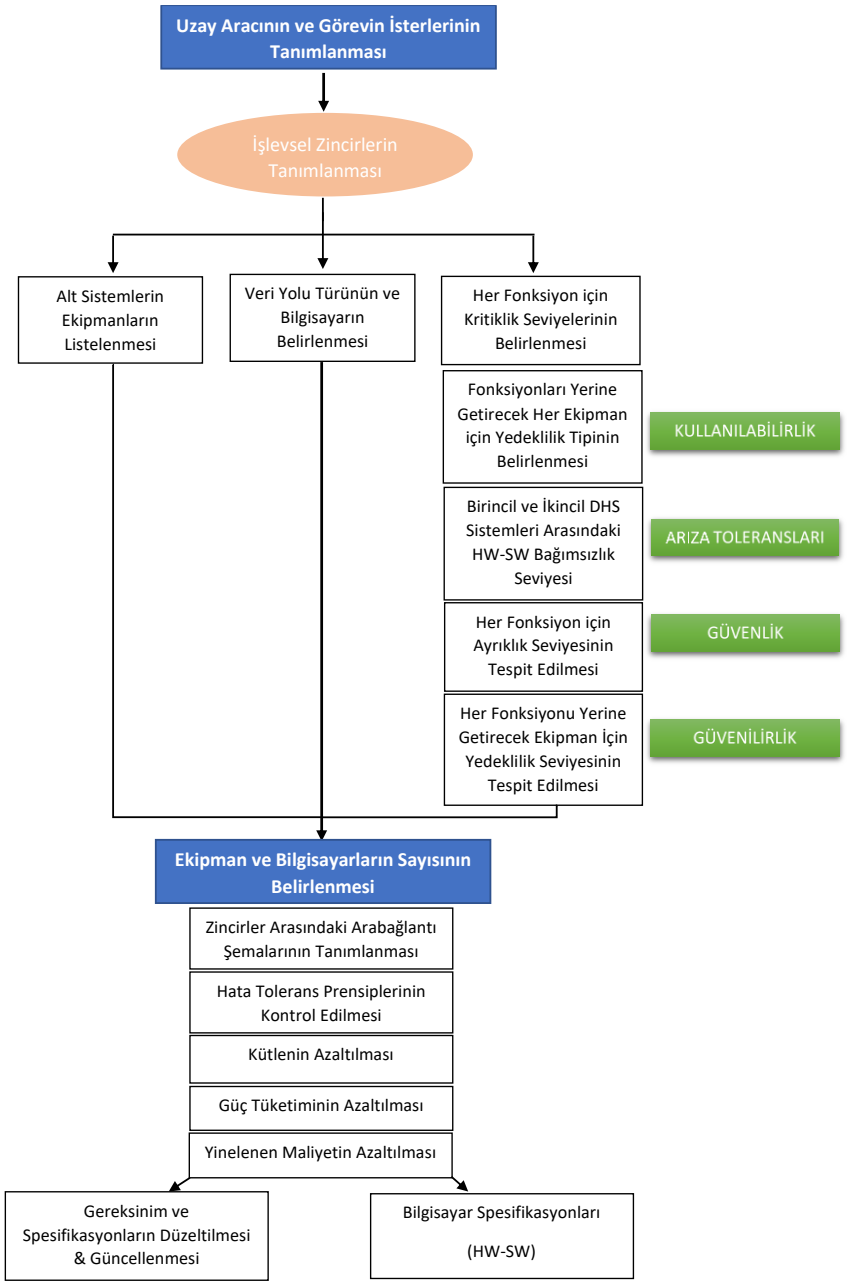
Çalışmada örnek görev olarak ISS'den olası bir kurtarma operasyonu incelenmiştir. Kenetlenme, ayrılma gibi ISS'e zarar verme ihtimali olan kritik manevralar yapacağı için ve insanlı uçuş yapacağı için yüksek güvenilirlik, kullanılabilirlik ve arıza-kaldırma ihtiyaçları bulunan bir uzay aracının platform veri işleme sistemi mimarisinin tasarımı örneği üzerinden güvenilirlik, kullanılabilirlik, bakım ve güvenlik analizlerine dayalı bir tasarım yöntemi sunulmuştur.

Sunulan yöntem kapsamında uzay aracının ve görevin isterleri iyice anlaşıldıktan sonra alt sistemlere ait işlevsel zincirler tanımlanmıştır. Bu adımı müteakiben, örnek teşkil etmesi açısından bu çalışmada kurtarma görevini icra edecek olan uzay aracının AOCS alt sisteminde yer alacak ekipmanlar (sensörler ve eyleyiciler) tespit edilmiştir. Bu adıma paralel olarak veri yolu türleriyle birlikte uzay aracında kullanılacak bilgisayarlar belirlenmiştir. Tanımlanan işlevsel zincirler sayesinde, görevin farklı fazları için her bir alt sistemin kritiklik seviyesi tespit edilmiştir. Kullanılabilirlik incelemeleri kapsamında, örnek niteliği taşıyan AOCS alt sistemine ait olan tüm ekipmanlar için yedeklilik tipine dair tespit çalışmaları yürütülmüştür. Daha sonra, arıza toleransları

düşünülerek uzay aracında nominal olarak kullanılacak olan tüm bilgisayarların kaybedilmesi varsayılarak, görevin başarılı bir şekilde tamamlanması için ikincil DHS'e ait bilgisayar tespit çalışmaları yapılmıştır. Güvenlik çalışmaları kapsamında ise, alt sistemlere ait olan fonksiyonlar için ayrıklık seviyeleri incelenmiştir. Örnek alt sistem olan AOCS için ekipman ve DHS sistemi için bilgisayar sayıları tespit edilmeden önce son adım olarak güvenilirlik çalışmaları kapsamında, her ekipman için yedeklilik seviyeleri tespit edilmiştir. Son olarak, zincirler arasındaki arabağlantı şemaları tanımlanarak çalışma sonlandırılmıştır (Şekil 6).

Bu bildiride sunulan tasarım yönteminin son adımında, ön tasarımı tamamlanmış DHS mimarisi iyileştirilerek kütle, güç tüketimi ve maliyetleri düşürülmektedir. Böylece tasarlanan DHS mimarisi, uzay aracına daha maliyet-etkin bir şekilde uygulanabilir.

Bu çalışmada sunulan yöntemle birlikte daha güvenilir alt sistemler, sistematik olarak ve maliyet-etkin şekilde geliştirilebilir. Şüphesiz ki yöntem deneme yanılma veyahut daha detaylı numerik çalışmalarla birlikte geliştirilmeye ve optimize edilmeye muhtaçtır. Bu çalışmayla verimli ve etkin bir DHS tasarım yöntemi geliştirilip sunulmasının yanı sıra, yöntemin ülkemizin uzay çalışmaları kapsamında tasarlanacak olan ilgili uzay araçlarının DHS alt sistem çalışmalarına katkı sağlayacağı hedeflenmiştir.



Şekil 6: DHS Tasarım Süreci

Kaynaklar

Birolini, A., 2007, Springer-Verlag, Reliability Engineering Theory and Practice 5th Edition, s.1-35.

Jakhu, R. Ve Pelton J., (2010). Space Safety Regulations and Standarts

Labourdette, P., Julien, E., Chemama, F. ve Carbonne, D., 2009, International Symposium on Space Flight Dynamics, Toulouse, Fransa, 28 Eylül – 2 Ekim.

Mosnier, A., (2019). *CRV Data Management System.* Alain Mosnier' ait 2018-2019 dönemi ders notları. AIRBUS DS, Toulouse.

Moury, G. ve Mosnier, A., (2019). *On Board Data Handling*. Gilles Moury ve Alain Mosnier' ait 2018-2019 dönemi ders notları. ISAE-SUPAERO – Department of Space Systems Engineering, Advanced Master, Toulouse.

Moury, G., (2019). *On-Board Data Handling: Functions, Architectures & Flight Software.* Gilles Moury'e ait 2018-2019 dönemi ders notları. CNES – Directrice des Systèmes Orbitaux / Architecture, Validation et Intégration, Toulouse.