Research Paper

Journal of Aerospace System Engineering
Vol.16, No.4, pp.10-16 (2022)

EISSN 2508-7150
http://dx.doi.org/10.20910/JASE.2022.16.4.10

항공 시스템용 전자 하드웨어 개발을 위한 미국 및 유럽의 가이드라인 : RTCA DO-254와 ECSS-Q-ST-60-02C의 비교 분석 연구

김성훈[1,†] · 김현우[1] · 채희문[1] · 김기두[1]

[1]한국정보통신기술협회 항행안전시설성능적합증명센터

A study of U.S. and European electronic hardware guidelines for aviation system : RTCA DO-254 and ECSS-Q-ST-60-02C

Sung Hoon Kim[1,†], Hyun Woo Kim[1], Hee Moon Chae[1] and Ki Du Kim[1]

[1]Certification Center of Performance Suitability of Air Navigation Facilities, Telecommunication Technology Association

Abstract

Since aviation systems are developed as the complex form of software a hardware, the necessity to apply to relevant guidelines is increasing. It is however uncommon that international development guidelines regarding electronic hardware are applied to current domestic aviation systems. In this paper, we compare and analyze DO-254 and ECSS-Q-ST-60-02C, electronic hardware development guidelines with the case of KASS (Korea Augmentation Satellite System) Performance Suitability, based on the project of SBAS (Satellite Based Augmentation System) development and construction.

초 록

항공 시스템은 소프트웨어·하드웨어 복합 형태로 개발되므로, 관련 가이드라인의 적용 필요성이 증가하고 있다. 그러나 현재 국내의 항공 시스템에 전자 하드웨어와 관련한 국제 개발 가이드라인을 체계적으로 적용한 경우는 흔치 않다. 따라서, 본 연구에서는 초정밀 GPS 보정시스템(SBAS; Satellite Based Augmentation System) 개발·구축의 KASS(Korea Augmentation Satellite System) 성능적합증명 수행을 사례로 항공(우주)용 전자 하드웨어 개발 가이드라인인 DO-254와 ECSS-Q-ST-60-02C의 비교 분석 연구를 목적으로 한다.

Key Words : Electronic Hardware(전자 하드웨어), FPGA(프로그래밍 반도체 소자), Development Guideline (개발 지침서), DO-254, ECSS-Q-ST-60-02C

1. 서 론

항공 시스템은 기능이 고도화됨에 따라 소프트웨어와 하드웨어가 복합적으로 결합된 형태로 개발되며 [1], 시스템의 개발 및 제작단계에서 안전성 및 신뢰성을 검증하기 위한 관련 개발 가이드라인의 적용 필요성이 증가하고 있다. 개발 가이드라인을 의무 적용하면 단기적으로 개발에 소요되는 비용 및 시간이 증가할 수 있으나 체계화된다면 시스템 유지보수 비용 감소 효과와 안전성 및 신뢰성을 확보할 수 있을 것으로 판단된다. 그럼에도 불구하고, 현재 국내의 항공용 전자 하드웨어 개발은 안전성 및 신뢰성을 중요시 하는 규정 및 절차에 따라 개발이 진행되는 것이 아니라 기능 구현을 위해 기능을 테스트하는 방식으로 개발이 진행되고 있다[2]. 또한 항공용 소프트웨어와 하드웨어를 개발하고 테스트한 사례는 있으나, 체계적으로 국제 개발 가이드라인을 적용한 경우는 흔치 않다.

본 연구에서는 초정밀 GPS 보정시스템(SBAS) 개발·구축의 KASS 성능적합증명 수행을 사례로 항공(우주)용 전자 하드웨어 개발 가이드라인인 DO-254와

Received: Oct. 12, 2021 Revised: Jun. 14, 2022 Accepted: Jun. 15, 2022
† Corresponding Author
Tel: ***-****-**** E-mail: ksh10@tta.or.kr

ECSS-Q-ST-60-02C의 비교 분석 연구를 목적으로 한다.

2. RTCA DO-254 분석

2.1 DO-254 개요

DO-254(Design Assurance Guidance for Airborne Electronic Hardware)는 항공용 전자 하드웨어 설계 보증 가이드라인으로 RTCA가 2000년 4월에, FAA에서는 2005년 6월 AC 20-152로 채택하여 인증기준으로 활용하도록 하고 있다.

DO-254의 적용대상은 전자 하드웨어로 FPGA(Field Programmable Gate Array), ASIC(Application Specific Integrated Circuit) 등이 포함된다.

DO-254는 ARP4761 및 ARP4754A 지침을 기반으로 시스템 안전성 평가 프로세스가 요구되며, 이 시스템 안전성 평가 프로세스에 의해 지정된 설계보증레벨(DAL; Design Assurance Level)에 따라 개발 엄격도가 정해지게 된다. 또한, 지정된 설계보증레벨에 따른 설계보증 목표를 만족하기 위해 설계보증 활동에 대한 지침을 제공하고 있다. 이와 같이 설계보증레벨에 따른 엄격도를 분류하여 요구조건들을 명시하며 이를 만족해야 하는 시스템 안전성 기반의 개발 가이드라인이다[3].

2.2 DO-254 개발 라이프 사이클

DO-254 개발 가이드라인에서 제시하는 개발 라이프 사이클은 크게 3가지로 분류할 수 있다. 계획 프로세스(Planning Process), 설계 프로세스(Hardware Development), 지원 프로세스(Supporting Process)로 분류되며 계획 프로세스를 완료하고 설계 프로세스를 시작할 수 있으며, 지원 프로세스는 개발 전 주기에서 수행된다.

계획 프로세스는 DO-254 개발 가이드라인에 따라 전자 하드웨어 개발 계획을 수립하고 이를 문서화하는 단계이다. 계획 프로세스에서는 하드웨어 설계 라이프 사이클 프로세스, 개발에 적용될 표준, 하드웨어 개발 및 검증 환경이 선택되고 제안된다. 또한 하드웨어 설계 보증 목표의 준수 방법이 인증당국에 제안된다.

설계 프로세스는 시스템 요구사항으로부터 하드웨어로 할당된 요구사항을 수행하는 하드웨어 아이템을 만들어 내는 단계이며, 요구사항 캡처 프로세스(Requirement Capture), 개념 설계 프로세스(Conceptual Design), 상세 설계 프로세스(Detail Design), 구현 프로세스(Implementation), 생산 전이 프로세스(Production Transition)로 구성되어 있다. 요구사항 캡처 프로세스는 파생 요구사항을 포함하여 요구사항이 식별되고 정의되며 문서화된다. 개념 설계 프로세스는 하드웨어 개념 설계가 식별되고 정의된 요구사항과 일치하게 개발되는지 확인한다. 상세 설계 프로세스는 하드웨어 요구사항과 개념 설계 데이터와 일치하게 상세 설계가 되는지 확인한다. 구현 프로세스는 하드웨어 상세 설계를 구현해 하드웨어 아이템을 생산한다. 생산 전이 프로세스는 하드웨어 아이템의 일관된 복제를 지원하기 위해 필요한 베이스라인이 형성된다. DO-254에서는 위의 5가지 프로세스 각각이 요구하는 목표(Objective)와 활동(Activities)를 명시하고 있으며, 하드웨어로 할당된 요구사항을 충족하는 하드웨어 아이템을 생성하는 과정으로 명시하고 있다.

지원 프로세스는 확인 및 검증 프로세스(Validation and Verification), 형상관리 프로세스(Configuration Management), 프로세스 보증 프로세스(Process Assurance), 인증연계 프로세스(Certification Liaison)을 수행한다. 확인 및 검증 프로세스는 하드웨어 개발과정에서 요구사항을 충족시키며 적합하게 검증되었는지를 확인하는 프로세스이다. 형상 관리 프로세스는 모든 변경사항의 이력 관리가 되었는지를 확인하는 프로세스이다. 프로세스 보증 프로세스는 라이프 사이클 목표를 만족하고 계획에 따라 개발이 되는지를 확인하는 프로세스이다. 인증연계 프로세스는 하드웨어 개발 라이프 사이클 동안 신청자와 인증 당국간의 소통과 이해를 만들기 위한 프로세스이다[3].

2.3 DO-254 산출물

DO-254는 하드웨어 보증 레벨 A부터 D까지 4단계의 하드웨어 개발 보증 레벨에 따라 만족시켜야 할 프로세스별 목표 및 활동의 엄격도가 달라지며 이에 대한 근거가 Table 1에 명시된 하드웨어 개발 라이프 사이클 산출물들에 포함되어야 한다. 또한 하드웨어 제어 카테고리 1(HC1)과 하드웨어 제어 카테고리 2(HC2)로 분류하여 하드웨어 개발 보증 레벨 및 산출

물 별 하드웨어 제어 카테고리를 다르게 할당하여 형상관리 활동의 차이점 및 엄격성을 구분짓고 있다.

Table 1 Output data according to DO-254

No.	Hardware Life Cycle Data	Level A	Level B	Level C	Level D
1	Plan for Hardware Aspects of Certification	HC1	HC1	HC1	HC1
2	Hardware Design Plan	HC2	HC2	HC2	NA
3	Hardware Validation Plan	HC2	HC2	HC2	NA
4	Hardware Verification Plan	HC2	HC2	HC2	HC2
5	Hardware Configuration Management Plan	HC1	HC1	HC2	HC2
6	Hardware Process Assurance Plan	HC2	HC2	NA	NA
7	Requirements Standards	HC2	HC2	NA	NA
8	Hardware Design Standards	HC2	HC2	NA	NA
9	Validation and Verification Standards	HC2	HC2	NA	NA
10	Hardware Archive Standards	HC2	HC2	NA	NA
11	Hardware Requirements	HC1	HC1	HC1	HC1
12	Conceptual Design Data	HC2	HC2	NA	NA
13	Detailed Design Data	NA*			
14	Top-Level Drawing	HC1	HC1	HC1	HC1
15	Assembly Drawings	HC1	HC1	HC1	HC1
16	Installation Control Drawings	HC1	HC1	HC1	HC1
17	Hardware/Software Interface Data	HC1	HC1	HC1	HC1
18	Hardware Traceability Data	HC2	HC2	HC2	HC2
19	Hardware Review and Analysis Procedures	HC1	HC1	NA	NA
20	Hardware Review and Analysis Results	HC2	HC2	HC2	HC2
21	Hardware Test Procedures	HC1	HC1	HC2	HC2
22	Hardware Test Results	HC2	HC2	HC2	HC2
23	Hardware Acceptance Test Criteria	HC2	HC2	HC2	HC2
24	Problem Reports	HC2	HC2	HC2	HC2
25	Hardware Configuration Management Records	HC2	HC2	HC2	HC2
26	Hardware Process Assurance Records	HC2	HC2	HC2	NA
27	Hardware Accomplishment Summary	HC1	HC1	HC1	HC1

* If the applicant references this data item in submitted data items, it should be available.

신청자는 인증당국의 요청 시 Table 1에 명시된 하드웨어 개발 라이프 사이클 산출물들을 인증당국에 제공하여야 하며, PHAC(Plan for Hardware Aspects of Certification), HVP(Hardware Verification Plan), TLD(Top-Level Drawing), HAS(Hardware Accomplishment Summary)은 필수 제출물에 해당된다[3].

3. ECSS-Q-ST-60-02C 분석

3.1 ECSS-Q-ST-60-02C 개요

ECSS-Q-ST-60-02C(ASIC and FPGA development)는 ECSS가 발행하였으며, ECSS는 유럽 우주 분야를 위해 표준을 개발하고 ESA(European Space Agency), NSA(National Space Agency) 및 EIS(European Industry Associations)와 협력하는 단체이다. ECSS-Q-ST-60-02C는 ASIC 및 FPGA와 같은 디지털, 아날로그 및 아날로그-디지털 혼합 회로 등의 개발을 위한 포괄적인 요구사항을 정의하며 초기 요구사항 설정부터 프로토타입 검사 및 배포까지 모든 활동을 포함하여 명시되어 있다.

ECSS-Q-ST-60-02C는 전자 하드웨어의 기능, 품질, 일정 및 비용 등의 요구조건 충족을 목표로 하는 임무에 중점을 둔 임무 기반의 개발표준이다. 특히, 우주 프로젝트와 같이 개발과정이 복잡하고 장기간 개발기간이 소요되는 프로젝트의 비용, 일정 및 기술적 성능 충족을 위해 중점적으로 언급하고 있다[4].

3.2 ECSS-Q-ST-60-02C 개발 프로세스

ECSS-Q-ST-60-02C에서는 전체 개발단계를 정의 단계(Definition Phase), 아키텍처 설계(Architectural Design), 상세 설계(Detailed Design), 레이아웃(Layout), 시제품 구현(Prototype Implementation), 설계 검증 및 배포(Design Validation and Release)로 분류한다. 공급업체(Supplier)는 정의 단계 전에 ASIC 및 FPGA 제어 계획(ACP)을 수립해야 하며 정의 단계에서 ASIC 및 FPGA 요구사항 사양(Requirements Specification), 실행 가능성 및 위험 분석 보고서(Feasibility and Risk Analysis Report), ASIC 및 FPGA 개발 계획(ADP)을 수립해야 한다. 아키텍처 설계 단계는 칩(Chip) 아키텍처가 모든 의도된 기능, 인터페이스 및 상호 작용을 구현하는 기본 블록 수준까지 정의, 검증 및 문서화 되어야 하며, 이를 준수해야 한다. 상세 설계 단계에서 높은 수준의 아키텍처 설계가 구조적 설명으로 변환되며, 레이아웃 제약(Layout Constraints), 평면도(Floorplanning), 생산

테스트 프로그램(Production Test Program) 등과 같은 후속 개발 단계에 대한 추가 정보가 생성되며 문서화 된다. 레이아웃 단계는 설계 규칙(Design Rules), 타이밍(Timing) 및 기타 제약 조건을 충족하기 위해 배치(Placement) 및 라우팅(Routing) 정보를 생성한다. 또한 이러한 정보들을 레이아웃 생성 보고서에 문서화 한다. 시제품 구현 단계는 칩이 제조 및 패키징 되며 FPGA가 프로그래밍되고 시제품 테스트가 수행된다. 해당 단계는 테스트가 수행된 제품을 전달하는 것으로 종료된다. 설계 검증 및 배포단계는 모든 기능, 성능, 인터페이스 및 호환성 요구사항을 만족하는지 확인하기 위해 수행되며 초기에 수립된 계획에 따라 검증을 수행하며 문서화 된다[4].

Table 2 Output data according to ECSS-Q-ST-60-02C

No.	Documentation
1	ASIC and FPGA control plan
2	ASIC and FPGA requirements specification
3	Feasibility and risk analysis
4	ASIC and FPGA development plan
5	MoM of System Requirements Review
6	Architecture definition report
7	Verification plan
8	Architecture verification and optimization report
9	Preliminary data sheet
10	MoM of Preliminary Design Review
11	Design entry report
12	Netlist generation report
13	Netlist verification report
14	Updated data sheet
15	MoM of Detailed Design Review
16	Layout generation report
17	Layout verification report
18	Design validation plan
19	Updated data sheet
20	Draft detail specification
21	MoM of Critical Design Review
22	Production test results and reports
23	Burn-in or any other production test results
24	specification, pattern
25	Validation report
26	Radiation test report
27	Release report
28	Final data sheet
29	Final detail specification
30	Application note
31	Experience summary report
32	MoM of Qualification Review/Acceptance Review

3.3 ECSS-Q-ST-60-02C 산출물

ECSS 표준은 우주 프로그램 및 프로젝트를 수행하기 위하여 수요자와 공급자의 관계를 지원하고, 맞춤 설계된 구성 요소가 기능, 품질, 신뢰성, 일정 및 비용 측면에서 요구사항을 충족하는지 확인하는 것을 목표로 한다. 이에 따라 고객은 개발기간 동안 산출된 문서, 설계 키트(Design Kit) 등을 공급업체로부터 받을 수 있으며 독립적으로 확인할 수 있다.

위의 Table 2에서 명시하는 산출물은 고객과 공급업체의 합의를 통해 전달되며 추가 항목은 필요에 따라 정의될 수 있다[4].

4. RTCA DO-254와 ECSS-Q-ST-60-02C의 비교 분석

2절에서 분석한 DO-254와 3절에서 분석한 ECSS-Q-ST-60-02C를 비교하여 차이점을 분석하였다. 처음으로 개발 단계별로 산출되어야 하는 산출물들을 Table 3에 명시하였다.

Table 3 Comparison of the Output data at ECSS-Q-ST-60-02C and DO-254

Phase	ECSS-Q-ST-60-02C	DO-254
	Output	Output
Planning	- A/F control plan	- Plan for Hardware Aspects of Certification - Hardware Design Plan - Hardware Validation Plan - Hardware Verification Plan - Hardware Configuration Management Plan - Hardware Process Assurance Plan - Requirements Standards - Hardware Design Standards - Validation and Verification Standards - Hardware Archive Standards

Development	- A/F requirements specification - Feasibility and risk analysis - A/F development plan - Architecture definition report - Verification plan - Architecture verification and optimization report - Preliminary data sheet - Design entry report - Netlist generation report - Netlist verification report - Updated data sheet - Layout generation report - Layout verification report - Design validation plan - Updated data sheet - Draft detail specification - Production test results and reports - Burn-in or any other production test results, specification, pattern - MoM of SRR, PDR, DDR, CDR	- Hardware Requirements - Conceptual Design Data - Detailed Design Data - Top-Level Drawings - Assembly Drawings - Installation Control Drawings - Hardware/Software Interface Data
Validation & Verification	- Validation report - Radiation test report - Release report - Final data sheet - Final detail specification - Application note Experience summary report - MoM of QR/AR	- Hardware Traceability Data - Hardware Review and Analysis - Procedure Hardware Review and Analysis - Results Hardware Test Procedures - Hardware Test Results - Hardware Acceptance Test - Criteria Problem Reports - Hardware Configuration Management Records - Hardware Process Assurance Records - Hardware Accomplishment Summary

다음으로 각 표준에서 명시하고 있는 요구조건들의 특징을 비교하여 Table 4에 제시하였다. DO-254는 시스템 안전성 평가 프로세스 수행을 통해 정해진 설계보증레벨에 따라 만족시켜야 할 요구조건이 다른 안전성 기반의 개발표준이며 의도한 기능을 안전하게 수행할 수 있도록 항공기 탑재 전자 하드웨어에 대한 명확하고 일관적인 지침을 제공한다. ECSS-Q-ST-02-60C는 우주 프로젝트에서 사용되는 설계요소가 기능, 품질, 일정 및 비용 등의 요구조건 충족하는지 확인하는 것을 목표로 하는 임무에 중점을 둔 임무 기반의 개발표준이다. 위와 같이 각 표준의 특성에 따라 요구조건에 차이가 존재한다. 세부내용은 아래와 같다.

첫째로, DO-254는 SAE(Society of Automotive Engineers) International의 항공 시스템 안전성 평가 프로세스 및 항공 시스템 개발 프로세스에 관한 가이드라인인 ARP 4761, ARP4754A 문서를 기반으로 시스템 안전성 평가 프로세스 수행이 요구된다. 이에 따라 설계보증레벨이 정해지게 되는데, DO-254에서는 설계보증레벨에 따라 만족시켜야 할 목표(Objective) 수와 독립성 수준이 다르며 설계보증레벨에 따라 만족시켜야 할 요구조건을 명시하고 있다. 시스템 안전성 평가 프로세스를 수행함에 따라서 설계보증레벨이 높을수록 하드웨어 기능의 오작동이나 결함이 항공기의 안전성 및 승무원의 정상적인 업무수행에 중대한 영향을 미칠 수 있음을 의미한다. 이와 반대로 설계보증레벨이 낮을수록 기능의 오작동이나 결함이 항공기 운용이나 승무원의 업무부하에 영향을 주지 않음을 나타낸다. 또한, DO-254는 하드웨어의 안전성을 입증하기 위한 방법으로 기능고장경로분석(Functional Failure Path Analysis)를 제시한다. 기능고장경로분석은 구조화된 Top-Down 분석 방법이며 각 하드웨어 컴포넌트들 간의 기능 경로를 분석하고, 하드웨어 아키텍처 및 구현이 안전 요구사항을 준수하는지 확인하기 위해 고장 모드와 영향성 분석을 한다. 해당 분석 방법은 하드웨어 품목의 일부분에 대해 낮은 설계보증레벨을

정당화하거나 제품 서비스 이력(Product Service History) 등으로 구현된 다른 기능을 수용하기 위해 사용될 수 있다. ECSS-Q-ST-60-02C는 DO-254에서 적용하는 설계보증레벨과 같이 수준에 따른 개발 엄격성을 구분하여 요구하지 않는다. ECSS-Q-ST-60-02C는 이와 유사한 개념으로 위험 분석이나 위험 평가 보고서를 요구하고 있으나 DO-254와 같이 인명손실 관련 장애 또는 설계 결함 방지를 목적으로 하는 것보다 임무 수행에 필요한 제품의 품질 등을 위해서 위험 분석 및 평가가 필요하다는 관점으로 명시되어 있다. 또한 시스템 안전성 평가 수행 후 할당된 설계보증레벨에 따라 개발을 수행하는 DO-254와는 달리 ECSS-Q-ST-60-02C의 경우 위험 분석 및 평가를 개발활동과 동시에 수행한다.

둘째로, DO-254는 개발과정에서 요구사항, 설계, 테스트케이스 및 절차 등은 작성자와 검토자 간의 독립성 확보가 되어야 한다는 것을 명시하고 있다. 예를 들면 설계자가 개발한 테스트 케이스 및 절차는 다른 사람이 검토하며 설계자가 분석을 수행하면 다른 사람이나 팀이 분석 결과를 검토를 해야 한다고 명시하고 있다. 또한 시스템 안전성 평가 프로세스 수행에 따라 할당된 설계보증레벨 별로 독립성 확보 조건을 다르게 설정하여 요구하고 있다. ECSS-Q-ST-60-02C의 경우에는 하드웨어 개발단계를 분류하며 단계별 요구 조건들을 명시하고 있으나 특별히 개발수준에 따른 개발 독립성 확보는 요구하지 않는다.

셋째로, DO-254는 하드웨어의 개발 요구사항 변경에 따른 설계 요구사항 구현 및 검증에 대한 정보를 포함해 모든 변경사항이 이력 관리가 되어야 한다는 것을 의미하는 형상 관리 프로세스에 대한 내용을 별도로 분류하여 목표 및 활동을 명시하고 있으며 하드웨어 제어 카테고리 1(HC1)과 하드웨어 제어 카테고리 2(HC2)로 분류하여 하드웨어 제어 카테고리에 따른 형상관리 활동의 차이점 및 엄격성을 구분지어 명시하고 있다. 예를 들면 하드웨어 인증 계획서(PHAC)는 하드웨어 제어 카테고리 1로 분류되어 있으며 이는 DO-254에서 요구하는 형상관리 활동인 형상식별, 베이스라인 수립, 베이스라인 추적성 확립, 문제 보고서 작성 및 관리 등을 모두 수행해야 한다.
ECSS-Q-ST-60-02C의 경우에는 DO-254와 같이 특정 기준에 따라 형상관리 활동의 차이점 및 엄격성을 구분 짓지는 않으며 ECSS-Q-ST-60-02C에서 참조하고 있는 문서인 ECSS-M-ST-40(Space Project Management – Configuration and Information Management)에서 형상관리 관련 내용을 명시하고 있다. 해당 표준에서는 우주 프로그램 또는 프로젝트에서 제품의 형상을 관리하기 위한 일반적 요구사항을 제공한다.

넷째로, DO-254는 인증 교섭 프로세스에 대한 내용을 명시하여 인증 당국과의 구체적인 소통 방안을 명시하고 있다. DO-254에 따르면, 하드웨어 인증 계획서를 인증 당국에 제출하고, 인증 당국에 의해 식별된 이슈가 해결되어야 하며 하드웨어 인증 계획서의 동의를 확보하여야 한다 등의 구체적인 절차가 명시되어 있다. 또한 하드웨어 인증 계획서, 하드웨어 검증 계획서, 상위 수준 도면, 하드웨어 달성 요약서는 인증당국에 필수로 제출되어야 한다고 명시되어 있다. ECSS-Q-ST-60-02C에서 개발 결과물의 경우, 고객이 요청 할 경우 독립적으로 검증할 수 있도록 제공하여야 한다고 비교적 간략하게 명시되어 있다.

Table 4 Comparison of features of DO-254 and ECSS-Q-ST-60-02C

features	DO-254	ECSS-Q-ST-60-02C
Safety and Risk Assessment Process	- 안전성 평가 수행에 따라 설계보증레벨 할당 및 이에 따른 개발 수행 - 설계보증레벨에 따른 산출물 작성 및 관리 요구 - 인명 손실 및 설계 결함 방지를 위해 안전성 분석 및 평가 요구	- 개발과 동시에 위험 분석 및 평가 수행 - 위험 분석 및 위험 평가 보고서 요구 - 제품의 품질 등을 위해 위험 분석 및 평가 요구
Independence	- 설계보증레벨 별 개발 독립성 확보 요구	- 개발수준에 따른 개발 독립성 확보 요구하지 않음
Configuration Management	- 하드웨어 제어 카테고리에 따른 수준별 형상 관리 활동 요구	- 참조문서인 ECSS-M-ST-40를 통해 일반적 요구사항 명시
Certification	- 인증당국에 전체 개발 산출물 제공 - 인증당국에 하드웨어 인증계획서 및 달성 요약서 제출 및 승인 요구	- 고객이 요청할 경우 개발 산출물 제공

5. 결 론

본 연구에서는 항공(우주)용 전자 하드웨어 개발 가이드라인인 DO-254와 ECSS-Q-ST-02-60C의 전반적인 문서 구성 및 내용을 분석하였다. DO-254는 시스템 안전성 평가 프로세스 수행을 통해 정해진 설계보증레벨에 따라 만족시켜야 할 요구조건이 다른 안전성 기반의 개발표준이며, ECSS-Q-ST-02-60C는 기능, 품질, 일정 및 비용 등의 요구조건 충족을 목표로 하는 임무에 중점을 둔 임무 기반의 개발표준이다. 또한 기타 프로세스에서도 각 표준에서 요구하는 중요도에 차이가 있었으며, 각 가이드라인에서 요구하는 사항에 따른 차이점을 확인하였다. DO-254는 시스템의 기능 복잡도 및 안전성 등에 따라 설계보증레벨을 구분하고 요구조건의 엄격도가 다른 안전성 기반의 개발표준이다. 따라서 특정 기능의 결함으로 인명손실을 야기할 수 있는 시스템의 경우에는 ECSS-Q-ST-02-60C보다 DO-254를 적용하는 것이 효율적이라고 판단된다. 항공(우주) 시스템은 기능이 고도화됨에 따라 소프트웨어와 하드웨어가 복합적으로 결합된 형태로 개발되며, 시스템의 개발 및 제작단계에서 안전성 및 신뢰성을 검증하기 위한 관련 개발 가이드라인의 적용 필요성이 증가하고 있다. 현재 국내의 항공(우주)용 전자 하드웨어 개발은 특정 규정 및 절차에 따라 개발이 진행되는 것이 흔치 않다. 관련 기술 확보를 위해 국제적으로 준용하는 가이드라인을 비교 분석하여 개발 시스템의 특성에 따라 선택 적용하는 것이 필요할 것으로 판단된다.

후 기

본 논문은 국토교통부 및 국토교통과학기술진흥원의 초정밀 GPS 보정시스템(SBAS) 개발구축 사업(KASS 성능적합증명 시스템 보증검사 수행, 21ATRP-A087579-08)으로 지원된 연구결과입니다.

References

[1] W. K. Youn, B. J. Yi and Y. K. Jin, “Comparison Study of Software and Hardware Quality Assurance for the Safety of Avionic System,“ *Current Industrial and Technological Trends in Aerospace*, Vol. 10, no. 2, pp. 112-121, Dec. 2012.

[2] J. A. Choi, “Avionics Hardware Certification based on DO-254,“ *Master’s degree of HanYang University*, Aug. 2018.

[3] RTCA, "Design Assurance Guidance for Airborne Electronic Hardware," *DO-254*, Apr. 2000.

[4] ECSS, “Space Product Assurance(ASIC and FPGA development,“ *ECSS-Q-ST-60-02C*, Jul. 2008.