유럽 항행시스템 안전성 표준 및 유럽-국내 공동개발시스템 (KASS) 적용 사례

TTA 항행안전시설 성능적합증명센터
발표자 : 윤동환 선임연구원

발표일자 : 2018.11.29.

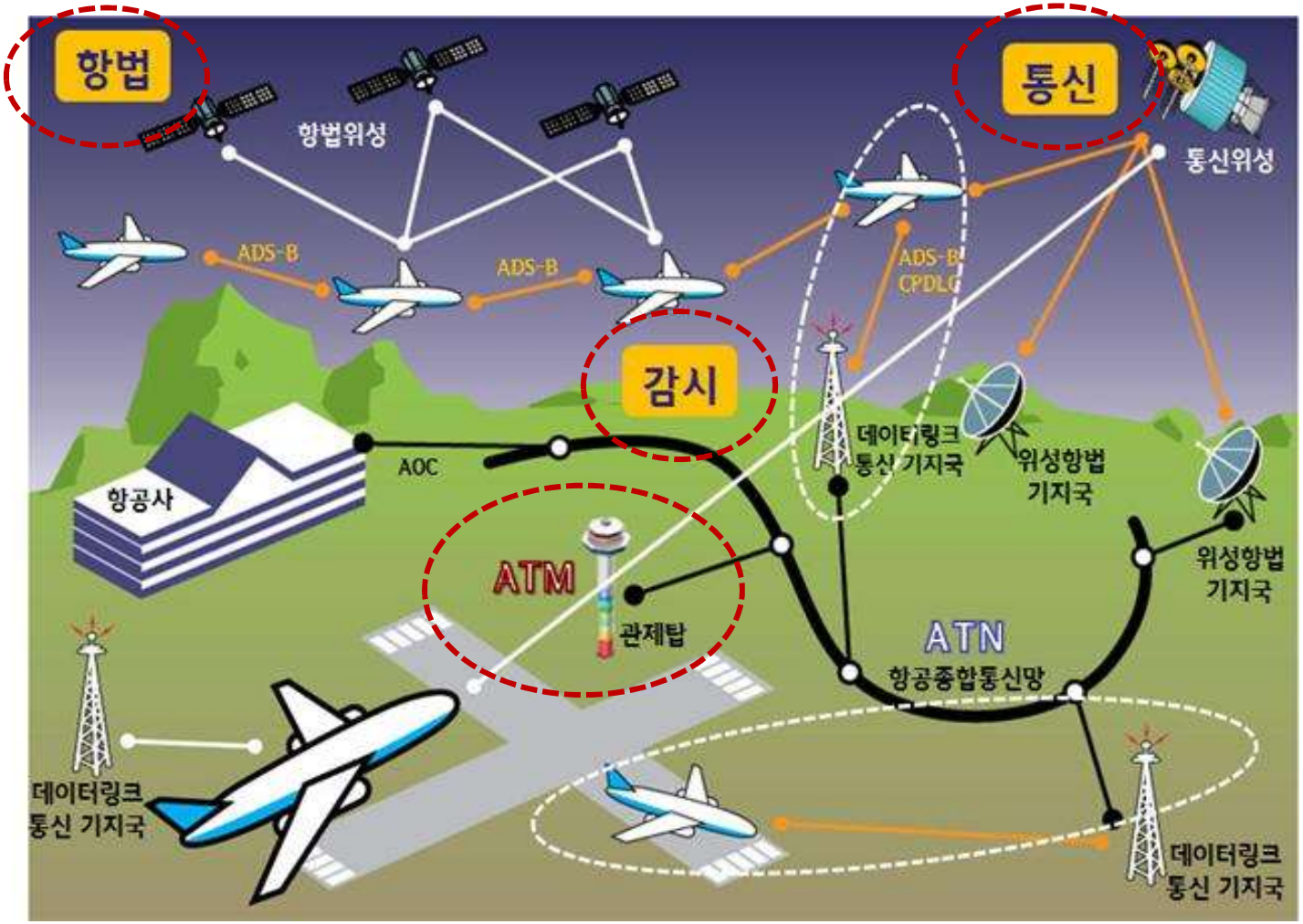
TTA 한국정보통신기술협회
Telecommunications Technology Association

목 차

목 차

1 서론

➢ 항행안전시스템


항법
항법위성
통신
통신위성
ADS-B
ADS-B
ADS-B
CPDLC
감시
데이터링크
통신 기지국
위성항법
기지국
위성항법
기지국
AOC
항공사
ATM
관제탑
ATN
항공종합통신망
데이터링크
통신 기지국
데이터링크
통신 기지국

1 서론

➢ 안전성(Safety)

[ECSS-Q-ST-40C Rev.1 - Safety Risk]
Measure of the threat to safety *posed by the* ***hazard scenarios*** *and their consequences*

▶ 위험 시나리오(Hazard Scenarios) 및 안전성 위협 척도(Measure of the threat to safety)

EUROCAE ED-78A

Hazard Class	1 (most severe)	2	3	4	5(least severe)
Effect on Operations	Normally with hull loss. Total loss of flight control, mid-air collision, flight into terrain or high speed surface movement collision.	Large reduction in safety margins or aircraft functional capabilities.	Significant reduction in safety margins or aircraft functional capabilities.	Slight reduction in safety margins or aircraft functional capabilities.	No effect on operational capabilities or safety.
Effect on Occupants	Multiple fatalities.	Serious or fatal injury to a small number of passengers or cabin crew.	Physical distress, possibly including injuries.	Physical discomfort.	Inconvenience.
Effect on Air crew	Fatalities or incapacitation.	Physical distress or excessive workload impairs ability to perform tasks.	Physical discomfort, possibly including injuries or significant increase in workload.	Slight increase in workload.	No effect on flight crew.
Effect on Air Traffic Service	Total loss of separation.	Large reduction in separation or a total loss of air traffic control for a significant time.	Significant reduction in separation or significant reduction in air traffic control capability.	Slight reduction in separation or slight reduction in air traffic control capability. Significant increase in air traffic controller workload.	Slight increase in air traffic controller workload.

1 서론

➢ 항행안전시스템 개발 표준(사실 표준)

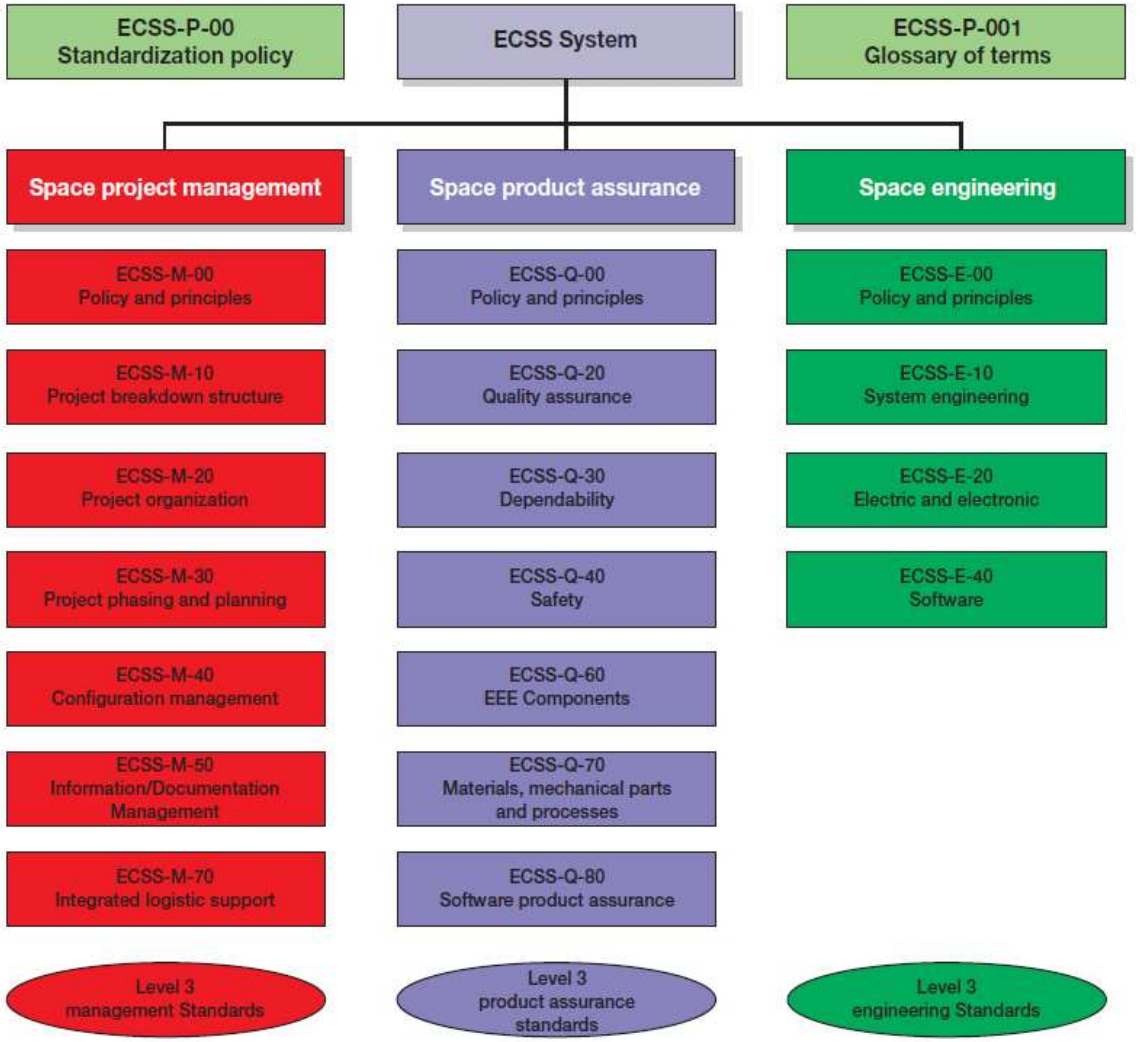
	미국	유럽	대한민국
시스템 개발	ARP-4754A	ECSS-E-10 ED-79A	
안전성 평가	ARP-4761	ECSS-Q-40 ED-135	
SW Assurance	DO-178B/C	ED-12B/C ECSS-Q-80	
프로젝트 관리	ARP-4754A	ECSS-M ED-79A	

- **미국과 유럽의 경우, 직접 사실 표준화에 참여하여** SoS(System of Systems) **개발 기준에 대한 프로세스 적용, 개발 산출물 작성, 품질 측정 등에 대한 이해도가 매우 높음**

목 차

2 유럽 항행시스템 안전성 표준

➢ 유럽 안전성 표준 구조도



2 유럽 항행시스템 안전성 표준

➢ ECSS (European Cooperation for Space Standardization)주요 표준

▶ Space Product Assurance

- ✓ ECSS-Q-ST-80C, Software Product Assurance
- ✓ ECSS-Q-HB-80-03A, Software Dependability and Safety
- ✓ ECSS-Q-ST-30C, Dependability
- ✓ ECSS-Q-ST-40C. Safety
- ✓ ECSS-Q-ST-30-02C, Failure Modes, Effects and Criticality Analysis (FMECA/FMEA)
- ✓ ECSS-Q-ST-30-09C, Availability Analysis
- ✓ ECSS-Q-ST-40-21C, Fault Tree Analysis (FTA) – Adoption notice ECSS/IEC 61025

▶ Space Engineering

- ✓ ECSS-E-ST-10C, Space Engineering
- ✓ ECSS-E-ST-40C, SW General Requirement
- ✓ ECSS-E-HB-40A, Software Engineering

2 유럽 항행시스템 안전성 표준

➢ ECSS-Q-ST-40C, Safety 문서 구조

Safety Programme

Safety Programme Plan, Safety Organization, Safety Risk Assessment and Control, Safety Critical Items, Safety Documentation

Safety Engineering

Safety Requirements Identification and Traceability, Safety Design Objectives, Safety Risk Reduction and Control, Identification and Control of Safety Critical Functions

Safety Analysis and Requirements Techniques

Assessment and Allocation of Requirements, Safety Analyses during the project life cycle, Safety Analyses

Safety Verification

Hazard Reporting and Review, Safety Verification Methods, Verification of Safety Critical Functions

2 유럽 항행시스템 안전성 표준

➢ 안전성 프로그램(Safety Programme)

▶ 안전성 관리자 (Safety Manager)

- ✓ 프로젝트 안전성 요구사항을 위해 필요한 안전성 프로그램을 수립하고 유지 및 관리
- ✓ 안전성 프로그램 계획에 따라 소프트웨어를 포함한 시스템 설계의 안전성 보증활동을 관리

▶ 안전성 문서 산출물(Safety Documentation)

- ✓ Safety Analysis Report
- ✓ Supporting Analysis
- ✓ Safety Risk Assessment
- ✓ Hazardous ground operation list and procedures
- ✓ Safety Verification Tracking Log (SVTL)

2 유럽 항행시스템 안전성 표준

➢ 안전성 공학(Safety Engineering)

▶ 안전성 요구사항 식별 및 추적성

- ✓ 프로젝트 안전성 요구사항을 위해 필요한 안전성 프로그램을 수립하고 유지 및 관리
- ✓ 안전성 프로그램 계획에 따라 소프트웨어를 포함한 시스템 설계의 안전성 보증활동을 관리

▶ 안전성 설계 목표 (Safety Design Objectives)

- ✓ 안전성을 위한 설계 방법 선택(Design Selection)
  - Fail Safe Design Solutions
  - Damage Control, containment and isolation of potential hazard
- ✓ 위험 제거 절차(Hazard Reduction Precedence)
  - Hazard Elimination
  - Hazard Minimization
  - Hazard Control

2 유럽 항행시스템 안전성 표준

➢ 안전성 공학(Safety Engineering)

▶ 안전성 위험 제거 및 통제 (Safety Risk Reduction and Control)

✓ 안전성 심각도 분류(Severity Categories)

구분	단계	결과 유형(Type of Consequences)	
		Dependability	Safety
Catastrophic	1	Failure propagation	• Loss of life, life-threatening or permanently disabling injury or occupational illness • Loss of system • Loss of an interfacing manned flight system • Loss of launch site facilities • Severe detrimental environmental effects
Critical	2	Loss of mission	• Temporarily disabling but not life-threatening injury, or temporary occupational illness • Major damage to an interfacing flight system • Major damage to public or private property • Major detrimental environmental effects
Major	3	Major mission degradation	-
Minor or Negligible	4	Minor mission degradation or any other effect	-

2 유럽 항행시스템 안전성 표준

➢ 안전성 공학(Safety Engineering)

▶ 안전성 위험 제거 및 통제 (Safety Risk Reduction and Control)

✓ 안전성 관련 기능의 치명도 분류

구분	기능 치명도	기능 치명도 분류에 대한 할당 기준
Catastrophic (Level 1)	I	A Function that if not or incorrectly performed, or whose anomalous behavior can cause one or more hazardous events resulting in catastrophic consequences
Critical (Level 2)	II	A function that if not or incorrectly performed, or whose anomalous behavior can cause one or more hazardous events resulting in critical consequences

✓ 안전성 위험 제거 및 통제를 위한 고려 사항

- Failure Tolerance Requirements
- Design for Minimum Risk

2 유럽 항행시스템 안전성 표준

➢ 안전성 공학(Safety Engineering)

▶ 안전성 위험 제거 및 통제 (Safety Risk Reduction and Control)

✓ 소프트웨어에 할당된 기능 치명도 분류

기능 치명도	기능 치명도 분류에 대한 할당 기준
I	Criticality category A if the software product is the sole means to implement the function
	Criticality category B if, in addition, at least one of the following compensating provisions is available - A hardware implementation - A software implementation; this software implementation shall be classified as criticality A - An operational procedure
II	Criticality category B if the software product is the sole means to implement the function
	Criticality category C if, in addition, at least one of the following compensating provisions is available - A hardware implementation - A software implementation; this software implementation shall be classified as criticality B - An operational procedure

2 유럽 항행시스템 안전성 표준

➢ 안전성 분석 요구사항 및 기법

▶ 안전성 평가 및 요구사항의 할당

- ✓ Safety Requirements
- ✓ Additional Safety Requirements
- ✓ Define safety requirements – functions
- ✓ Define safety requirements – subsystems
- ✓ Justification
- ✓ Functional and subsystem specification

▶ 안전성 분석 (Safety Analyses)

- ✓ Hazard Analysis
- ✓ Safety Risk Assessment
- ✓ Supporting Assessment and analysis

2 유럽 항행시스템 안전성 표준

➢ 안전성 검증(Safety Verification)

▶ 위험 보고 및 리뷰 (Hazard reporting and review)

- ✓ Hazard Reporting System
- ✓ Safety Status Review
- ✓ Documentation

▶ 안전 중요 기능의 검증 방법

- ✓ 확인(Validation)
- ✓ 품질보증(Qualification)
- ✓ 고장 시험(Failure Tests)
- ✓ 설계 혹은 운영 특성 검증(Verification of design or operational characteristics)

목 차

3 유럽-국내 공동개발시스템(KASS)

➢ 한국형 초정밀 GPS 보정시스템(KASS)

▶ 개요

- ✓ 대한민국의 위성기반 보강 시스템(SBAS, Satellite Based Augmentation System)의 개발 구축을 위해 설계
- ✓ 항공안전 향상을 주 목적으로 하며 GNSS 위성 배열에 기초하여 다음 서비스를 최종 사용자에게 제공
  - ▪ 일반 위성항법 신호 대비 향상된 위치정보 제공
  - ▪ 위치 서비스에 대해 무결성(Integrity), 연속성(Continuity), 가용성(Availability) 보장

▶ 주요 성능 요구사항

- ✓ ICAO SARPs Annex 10 Vol. 1에 제시된 SIS(Signal In Space)
- ✓ 서비스 범위는 인천 FIR (Flight Information Region) 전체를 대상으로 함

3 유럽-국내 공동개발시스템(KASS)

➢ 한국형 초정밀 GPS 보정시스템(KASS)

구분		검사 기준
기능 및 성능	국내외 기술 기준	항행안전무선시설 설치 및 기술기준 고시
	국제 최소 성능 기준(MOPS)	RTCA DO-229 change2
시스템 보증	SW 보증 기준	RTCA DO-178B / EUROCAE ED-12B (SW) ECSS-Q-ST-60 (HW)
	안전성 기준	ECSS-Q-ST-40 Safety ECSS-Q-ST-30 Dependability

3 유럽-국내 공동개발시스템(KASS)

➢ 한국형 초정밀 GPS 보정시스템(KASS)

▶ 인증기준(CRB, Certification Regulatory Basis)

✓ 국내 기준

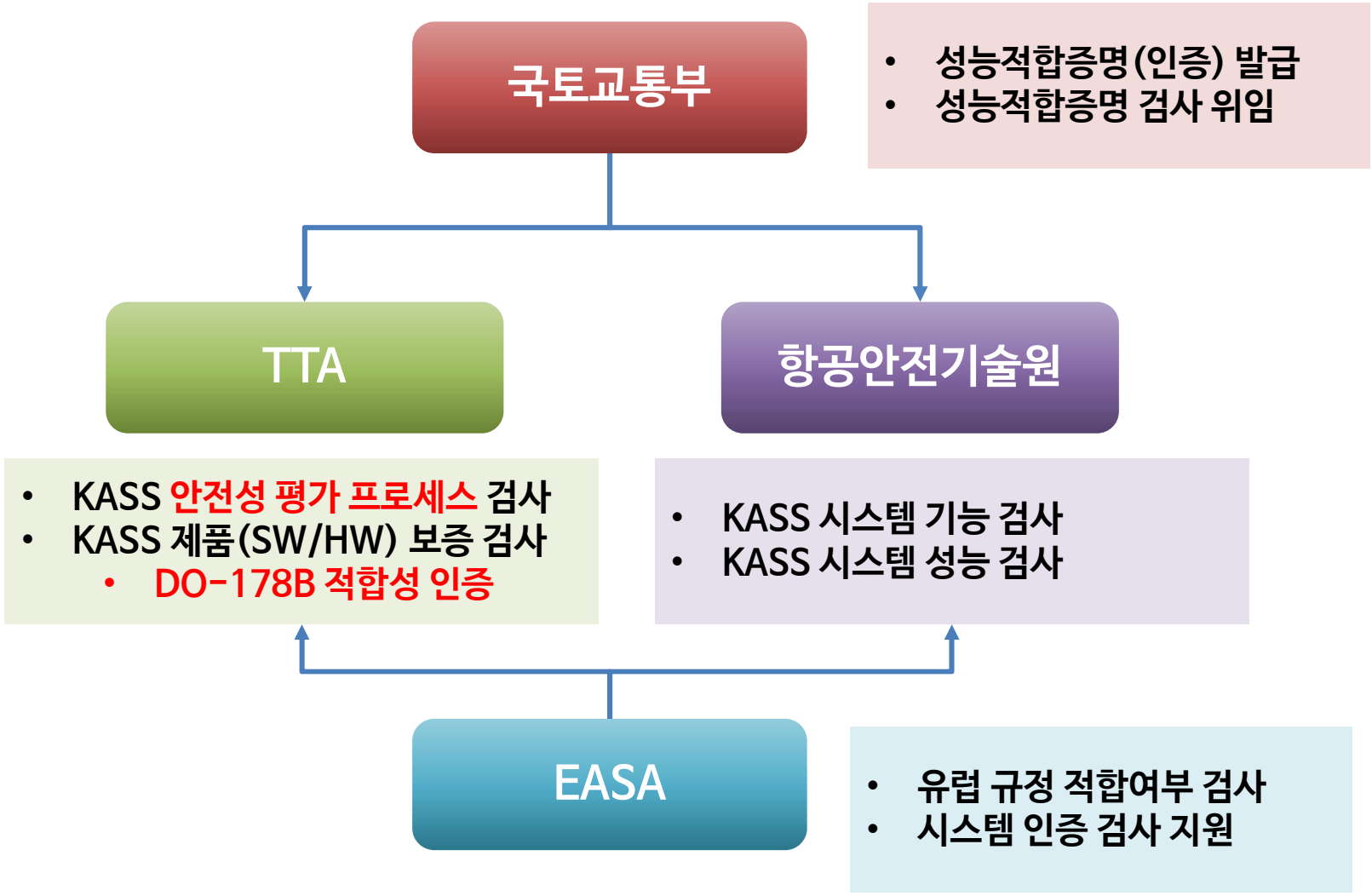
- 국토교통부 고시 제2016-122호(항행안전시설 성능적합증명 검사 기술기준)

조문	조문 내용
제3조 1항	항행안전무선시설의 설치 및 기술기준(국토교통부 고시 제 2016-205호)을 적용
제3조 3항	미국 또는 유럽의 공인화된 항공관련 소프트웨어 개발 기술기준 최소 1개를 검사 신청자가 선택하여 적용(KASS의 경우, 신청자 선택에 따라 RTCA DO-178B 적용)

- 국토교통부 고시 제2016-205호(항행안전무선시설의 설치 및 기술기준)
  - ❖ SBAS에 관련된 부분 발췌 적용
  - ❖ 고시 내 규정되지 않은 부분은 ICAO SARPs Annex 10 Vol. 1을 기준으로 적용

2 KASS 성능적합증명 검사 수행

➢ KASS 성능적합증명(인증) 검사 체계



목 차

4 결언

▶ 항행안전시스템을 비롯해 항공우주분야 개발에서 안전성 표준 적용은 필연적 흐름

- ✓ Mission Critical System인 우주 발사체, 우주선에도 재사용이 강조되며 안전성 표준이 점차 적용되고 있음
- ✓ NASA, FAA, EASA, ESA 등에서 Safety 관련 기법에 대한 가이드, 관련 연구들이 꾸준히 공유되고 있음

▶ 안전성 평가에 직접 참여하여 기술적 이해도를 높이려는 노력이 국내에도 필요함

- ✓ DO-178C SW Level A로 무조건 개발하는 것보다 더 저렴하게 더 안전성 있게 개발하려는 노력이 필요

참고 : https://www.theverge.com/2018/5/24/17388680/spacex-falcon-9-rocket-block-5-commercial-crew-nasa-copv

감사합니다

THANK YOU

한국정보통신기술협회
Telecommunications Technology Association

한국정보통신기술협회
Telecommunications Technology Association
[463-824] 경기도 성남시 분당구 분당로 47(서현동 267-2)
47, Bundang-ro, Bundang-gu, Seongnam-si, Gyeonggi-do,
463-824, Rep. of KOREA
http://sw.tta.or.kr