항공탑재용 소프트웨어 안전 소개 및 적용
: DO-178C 기반

2015. 12. 1

KARI Korea Aerospace Research Institute

한국항공우주연구원

목차

I. 개발동향

항공전자 장비(소프트웨어 탑재) 개발 동향

Aronca Model 7 Champion

항공전자 장비(소프트웨어 탑재) 개발 동향

Spaceshipone

지상 24Km => 지상 112km

[**Spaceshipone**]

항공전자 장비(소프트웨어 탑재) 개발 동향

New Piper- Meridian

항공전자 장비(소프트웨어 탑재) 개발 동향

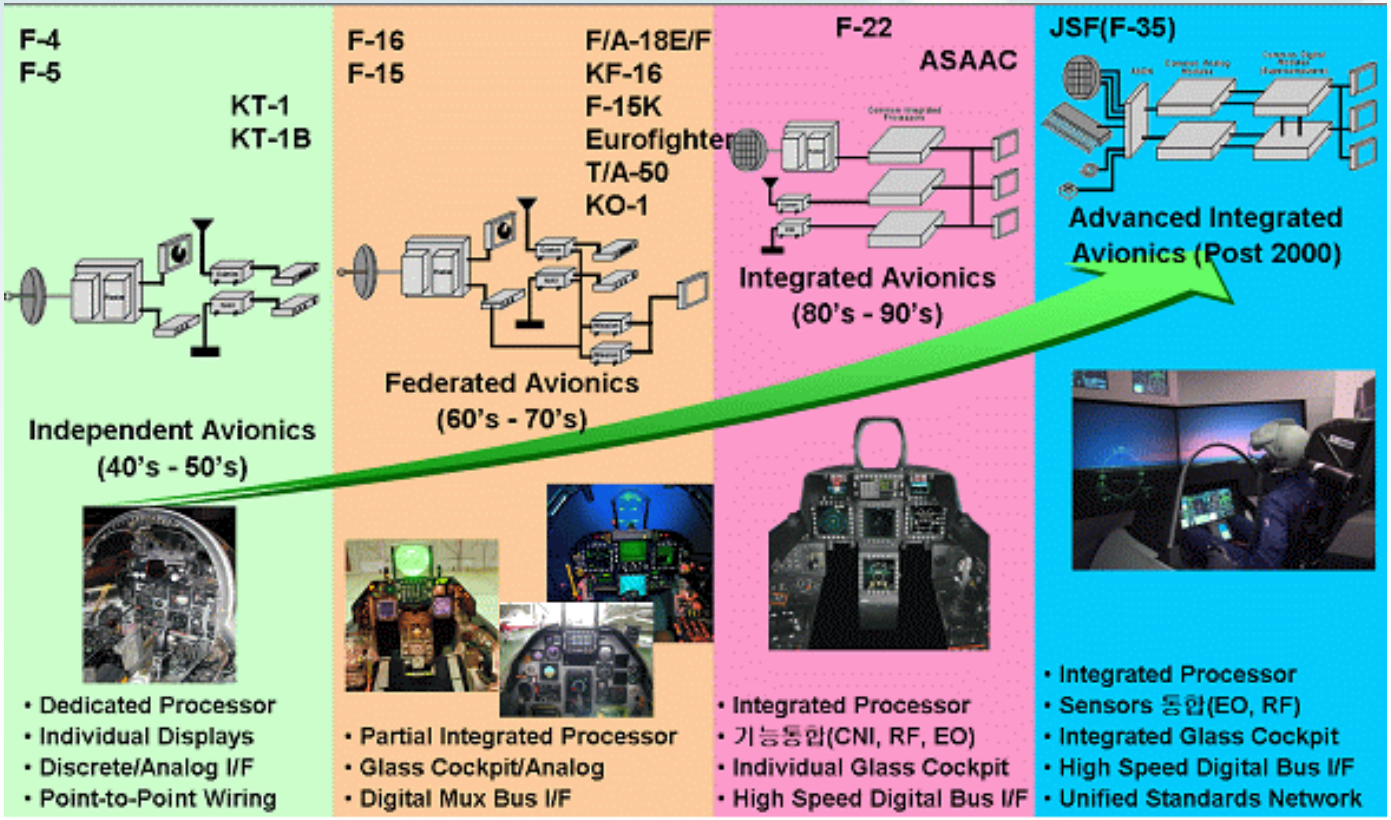
A-380 개발비 : 120억 유로
소프트웨어 개발(인증 포함) : 40억 유로

▪ 항공 탑재 소프트웨어 유형

- 비행 또는 임무 중요 소프트웨어 : fly-by-wire, engine control, radar, ADIRU, AP 등
- Health 및 안전 관련 : 환경 조정 계통(압력, 온도, 습도, 조명, 생명유지장치 등)
- 업무 부하 감소 : 정교한 디스플레이를 사용하는 Secondary System
- 항공기 안전과 종속되지 않는 소프트웨어: 항공기 내 설치된 오락장치, 승객 컴뮤니케이션 용

항공전자 장비(소프트웨어 탑재) 개발 동향

Avionics Architecture Trend

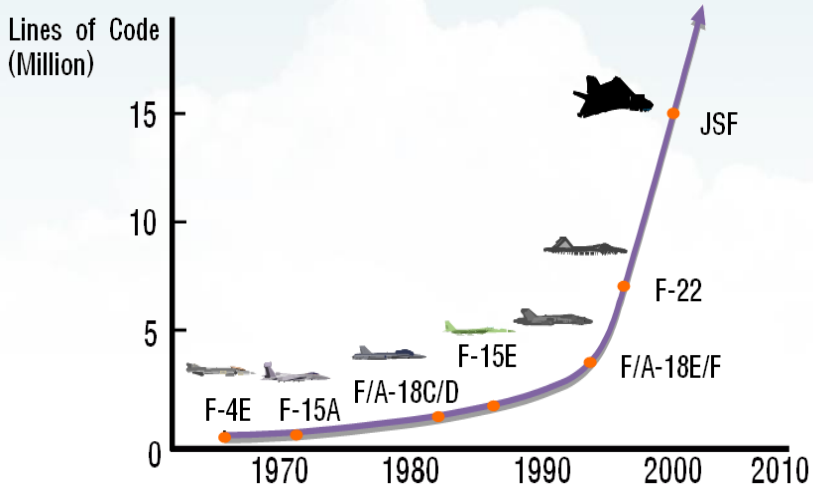


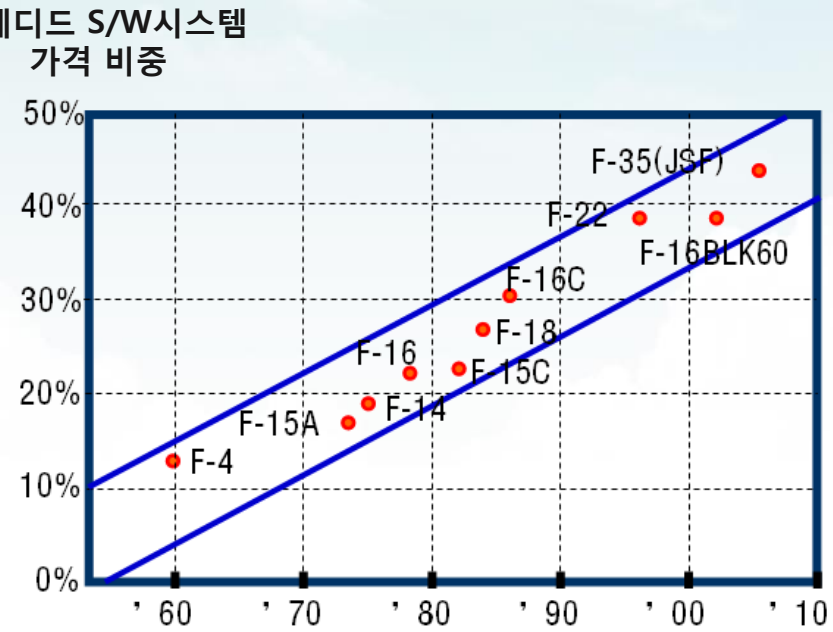
- 시스템 통합성
- 부품 모듈화
- 고속 디지털화
- 인터페이스 단순화
- 확장성 확보
- 고 신뢰성
- 고 정비성
- 저 비용
- 저 중량
- 저 전력

항공전자 장비(소프트웨어 탑재) 개발 동향

항공분야 S/W 발전

- 국방/항공 기술 발달과 더불어 항공탑재용 S/W 수요 증가
  - 항공기 탑재용 S/W 코드 복잡화 (코딩 라인 수 증가)
  - 전체 항공기 가격 대비 S/W 비율 증가

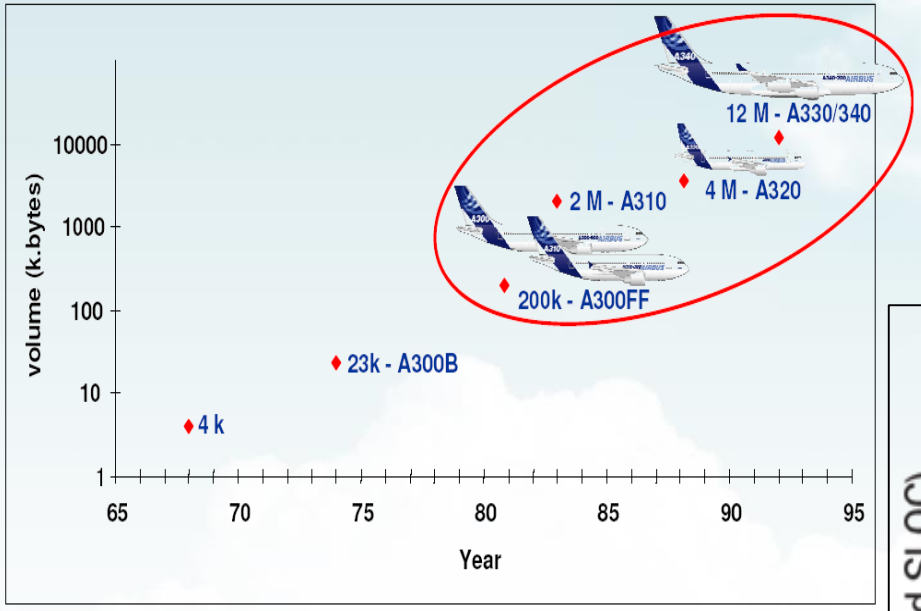


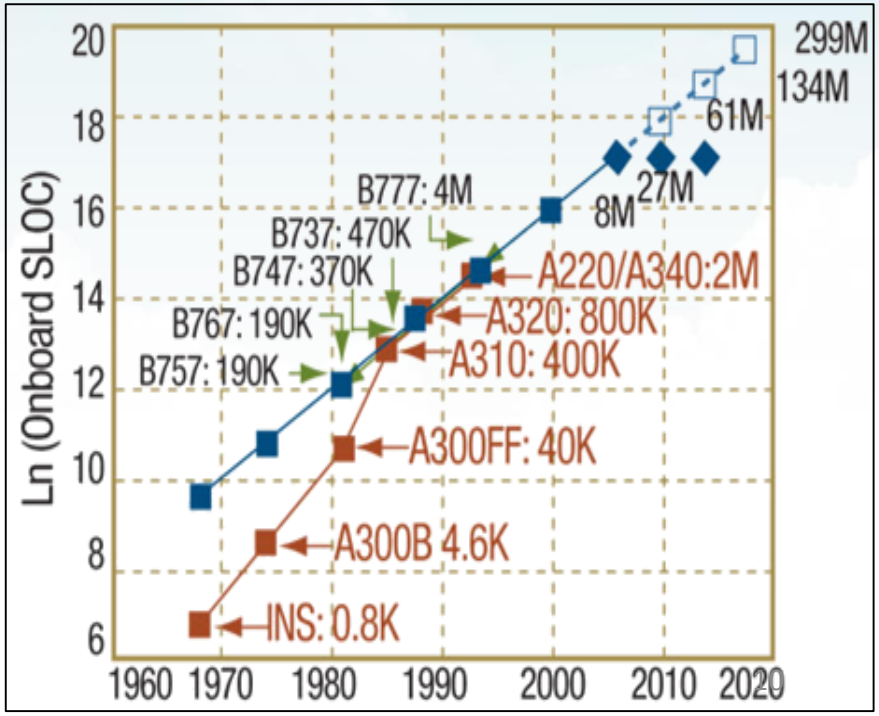


<자료 : Boeing사>

항공용 소프트웨어 사용량 증가 추세

- **항공분야 S/W LOC 증가 추세**





II. 사고 사례

S/W 오류 인한 사고 사례

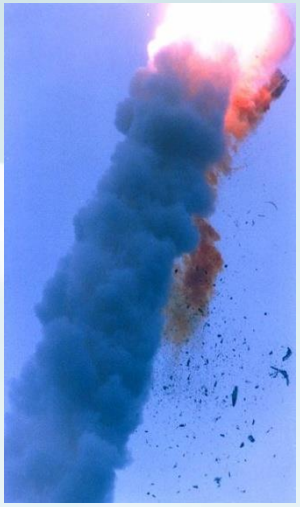
항공 관련(민간/군사)

- 항공 교통 컨트롤 시스템 (2004년 9월 14일)
  - 원인 : 카운트 다운 타이머 오류
    (카운트 다운 타이머가 4 billion milliseconds를 초과)
  - 결과 : 항공기 위치 추적 신호 통신 마비
  - 시스템 작동 중단을 막기 위해 수동 방법으로 재 부팅(30일 마다)
- 패트리어트 미사일 (1991년 1월 21일)
  - 원인 : 계산 미사일 위치 오차(약 600m)
  - 결과 : 사망자 발생 (군인 28명)
- F-22 (1992년, 2007년)
  - 원인 : 동시 다발적인 다중 컴퓨터 충돌

(F-22 crash landing 동영상)

S/W 오류 인한 사고 사례

우주 발사체



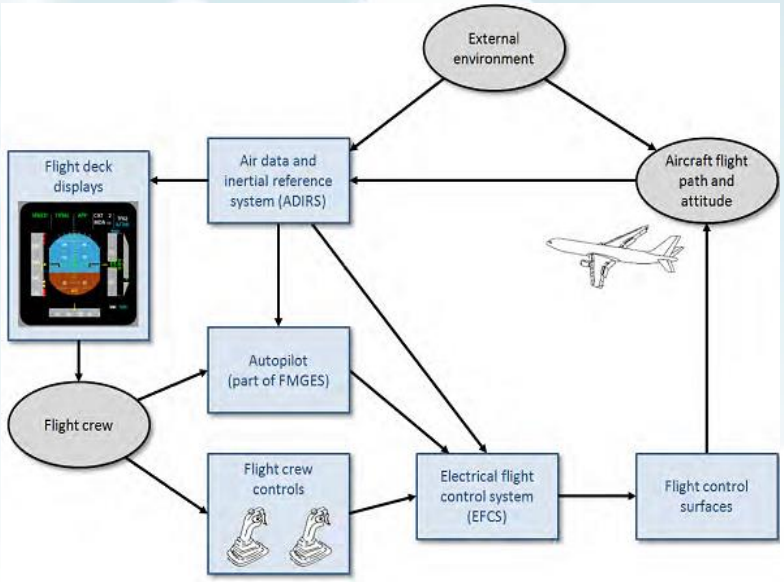
- 아리안 5호 로켓 (1995년 6월 4일)
  - 원인 : 숫자 단위 변환 에러
    (64 비트의 부동 소수점 -> 16 비트 정수 변환 과정)
  - 결과 : 발사 후에 37초 후 로켓 폭발
  - 소요 비용 : $ 7.5 billion
- NASA 화성 기후 궤도 탐사선 (1999년 11월 23일)
  - 원인 : 개발 팀간 단위 Unit 혼동
    미터법이 아닌 야드파운드법로 적용, 자세제어용 추력기에서 발생하는 힘을 실제보다 약 4.45배 적은 것으로 예측
  - 결과 : 화성 궤도 진입 후 40m 상공에서 폭발
  - 소요 비용 : $ 125 million

- NASA 화성 탐사선 (2006년 11월 2일)
  - 원인 : 하드웨어 구속조건을 초과한 입력에 의한 배터리 손실
  - 결과 : 전력 저하로 임무 조기 중단

항공기 운항 중 준사고사례_ 소프트웨어 안전성

항공기 준사고 사례 https://www.atsb.gov.au/media/24550/aair200503722_001.pdf

- 대상 항공기: 말레이시아 항공 Boeing 777-200ER
  - 2005년 호주 Perth에서 쿠알라룸푸르 운항
- 준사고 개요
  - AIDRU 고장에 따라 잘못된 데이터가 입력되어 항공기가 과도하게 기동하는 심각한 준사고
  - Low Airspeed, "PFD의 Slip/Skid 편향지시 속도 감속(270 Knots=> 158 Knots), 실속경보
  - 회복후 회항중, 항공기 노즈다운, 우측뱅크 발생



  - 자동조종장치 사용 포기하고 수동비행으로 안전하게 회항
- 호주 사고 조사위원회(ATSB) 결론
  - ADIRU 운용프로그램 소프트웨어(OPS)가 표준에 따라 시험하고 인증을 받았으나, 시험이 구성품의 표준요건에 한정하여 시험되어 OPS에 확인되지 않은 Anomaly 존재

㈜ ADIRU(Air Data Inertial Reference System) : 항공기의 주비행조종계통(PFC), 자동조종장치(AP)의 비행지시장치(FD), 비행관리시스템(FMS) 등에 대기정보(속도, 고도, 받음각)와 항행정보 제공

항공기 운항 중 준사고사례_ 소프트웨어 안전성

항공기 준사고 사례 (계속)

- 호주 사고 조사위원회(ATSB) 결론(계속)
  - 구성품 소프트웨어에 존재하는 Anomaly(비정상적인 작동)가 ADIRU 내의 고장난 가속도계로부터의 입력 허용
  - ADIRU에 잘못 입력된 데이터가 주비행컴퓨터, 자동조종장치 등의 항공기 시스템에서 사용됨. 그 결과 항공기 이상 기동현상 발생
  - 또한, 비행교범에 조종사가 항공기의 이상자세에서의 회복 절차를 제공하지 않음

- 시정조치
  - 미국 FAA(항공기 제작국가): AD 2005-18-51(감항개선지시서)를 통해 B777항공기에 ADIRU 신규 OPS 설치 및 비행교범의 Limitation 변경 조치
  - AIDRU 제작사 : 항공기 제작사와 함께 AIDRU OPS Hierarchy 검토 및 S/W 민감도 결정
  - 항공기 제작사 : ADIRU 신규 운용프로그램 설치, 운용매뉴얼 개정(이상자세 회복절차 등)
  - 항공기 운항사: AD 2005-18-51적용 및 개정 운용 매뉴얼 적용

III. 항공전자 시스템 개발

항공전자시스템 개발>>>> How

- **항공용 장비 요건: KAS/FAR 25.1309**

(a)비행기의 감항기준에 의거 소요 기능이 요구되는 장비 및 시스템 그리고 장비의 장착요건은 예상되는 모든 운용조건하에서 요구되는 기능을 제대로 발휘할 수 있도록 설계하여야 한다.

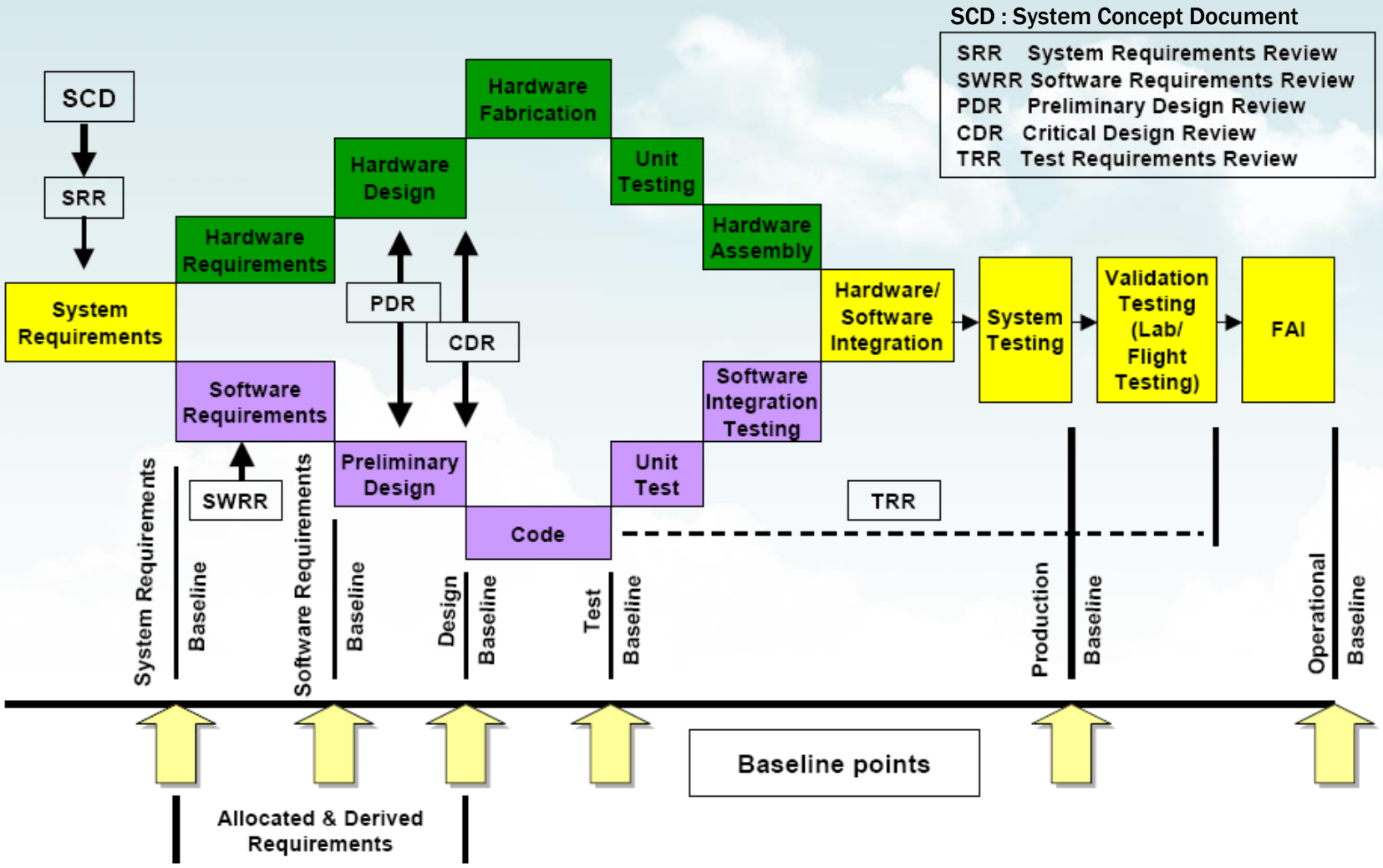
(b) 비행기의 시스템 및 관련되는 구성품은 다른 시스템과 개별적으로 그리고 연관하여 고려할 때 다음 사항에 적합하도록 설계하여야 한다.

(1) 비행기의 안전한 비행과 착륙을 방해하는 임의의 고장상태의 발생이 아주 없어야 한다(Extremely improbable)

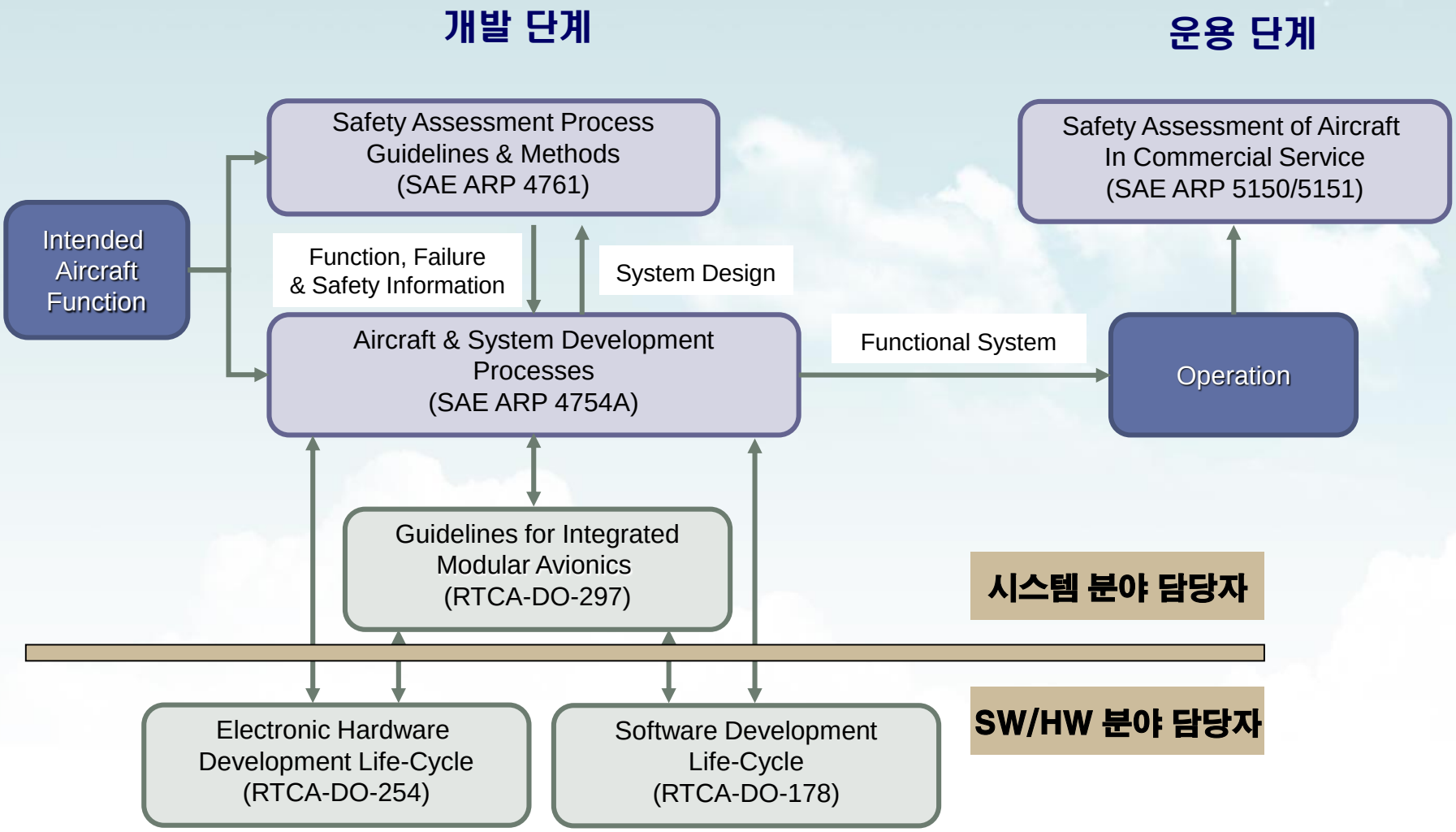
(2) 비행기의 성능 또는 조종사가 불리한 운항 상태를 극복하는 능력을 감퇴시키는 임의의 고장상태의 발생이 없어야 한다(improbable).

항공전자시스템 개발>>>> How

- **시스템 개발 프로세스**



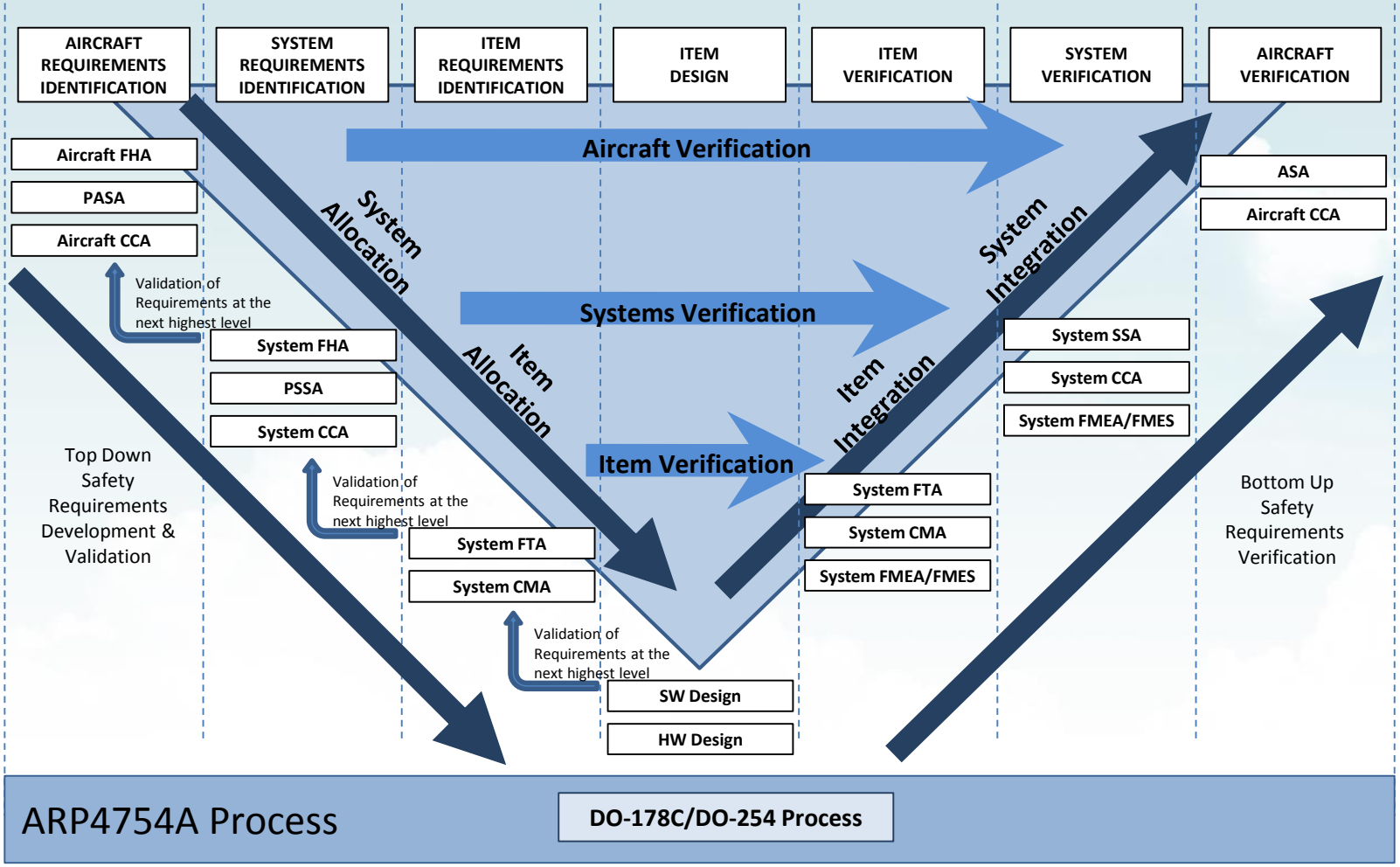
항공전자시스템 개발>>>> How



- **SAE ARP 4754 Guidelines for Development of Civil aircraft and System: 항공기 시스템에 대한 인증을 도움을 주기 위한 국제적 지침**
- **FAA AC 25.1309-1A System Design and Analysis은 인증방법론 설명**

항공전자시스템 개발>>>> How

- **안전성 프로세스(ARP 4754A)**



FHA : Functional Hazard Assessment
PASA : Preliminary Aircraft Safety Assessment
PSSA : Preliminary System Safety Assessment
SSA : System Safety Assess0ment

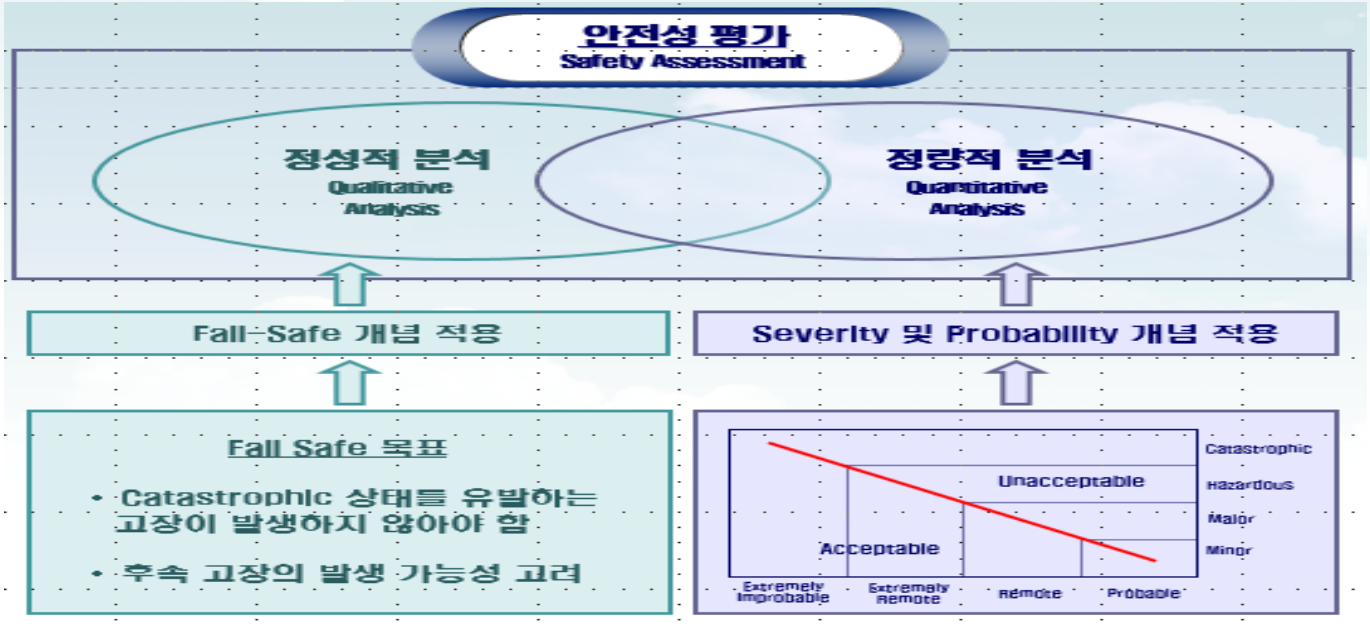
FTA : Fault Tree Analysis
FMEA : Failure Mode Effects Analysis
FMES : Failure Mode Effects Summary
CCA : Common Cause Analysis

CMA : Common Mode Analysis
ASA : Aircraft Safety Assessment

항공전자시스템 개발>>>> How

시스템 안전성 평가

- 항공기 설계에 대한 평가를 통해 현재의 안전 기준을 충족하는지 확인하기 위한 절차
- 필요하다면 고장 발생 가능성을 더 낮추거나 고장으로 인한 영향을 감소시키기 위한 조치의 필요성을 판단
- Risk 개념을 적용하여 발생 가능성과 이로 인한 를 평가하고, 허용안전수준에 따라 설계요건 및 관리기준을 적용함.



항공전자 시스템 개발>>>> How

시스템 – 소프트웨어 – 전자하드웨어 관계

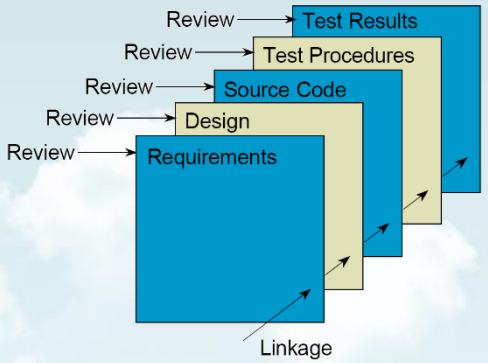
- SAE ARP 4761는 보증 수준(Assurance Level)을 정의하고 있는 개발기준으로 안전성평가를 다룸
- 보증 수준은 기능적인 고장 조건에 상응하는 프로세스의 엄격한 적용 수준을 설정
- SAE ARP 4754A, RTCA DO-178C 및 DO-254는 시스템에 대해 잠재된 시스템 안전성과 상위 시스템에서 도출된 요구조건의 시스템 요구조건 영향성 평가 필요성 강조
- 이는 안전성에 영향을 미칠 수 있는 개발과정의 실수가능성을 배제하기에 충분한 정화된 방식으로 완성이 가능하게 함
- 서로간에 모두 의존하며 Objectives-based Tables 사용
- 항공전자 LRU(Line Replaceable Unit)
  - PLD, ASIC 및 FPGA 구성품 형태의 전자 하드웨어 포함

Ⅳ. RTCA DO-178C 적용

항공용 소프트웨어 개발 및 DO-178C

소프트웨어 안전

- 소프트웨어가 안전한지 어떻게 아는가?
  - 모른다
- 소프트웨어 안전성?
  - 적절한 프로세스 준수
  - 코드에 대한 내부로부터의 검증 및 점검…점검…점검



※ 소프트웨어 오류는 개수와 유형을 평가하는 것이 실현불가능하며, 만약 오류가 존재하는 경우 시스템 설계, 개발 및 시험 완료후에도 존재할 수 있음.

- 인증과정에서 시스템 수준에서의 육안으로 확인 가능성이 탑재 시스템에 장착되는 소프트웨어를 평가하고 통제하기 위해 감항당국의 수락가능한 지침 및 내용을 규정하고 이에 따른 평가를 통해 안전성 확보

항공용 소프트웨어 개발 및 DO-178C

DO-178C의 인증 적용성

▪ **FAA AC 20-115C (2013.7)**

"An Applicant for a TSO authorization, TC, or STC for any electronic equipment or system employing digital computer technology may use considerations outlined in RTCA Document *RTCA DO-178C* as a means, but not the only means, to secure FAA approval of digital computer software."

※ FAA에서 CAST를 통해, DO-178 적용에 대한 논의사항을 문서로 정리(현재는 총 33건)"
예: 소프트웨어 구획분할/보호 구조에 대한 평가 지침, 인증에서의 미해결 문제 보고서 관리 등
https://www.faa.gov/aircraft/air_cert/design_approvals/air_software/cast/cast_papers/

DO-178 History

문서	년도	주요내용
DO-178	1982	기본적인 절차 (산출물, 문서, 추적성, 시험)
DO-178A	1985	프로세스, 시험, 구성품, 안전수준, 검토, Waterfall methodology 도입
DO-178B	1992	통합, 단계 전이 기준(Transition Criteria), 다양한 개발 방법, 데이터, 툴
DO-178C	2011	DO-178B 개념 명확화, 최신 소프트웨어 개발 기술도입

항공용 소프트웨어 개발 및 DO-178C

DO-178 주요 특성

- 감항 요구조건의 적합성을 만족하는 안전성과 신뢰 수준으로 의도한 기능을 수행하는 항공용 시스템 및 장비의 소프트웨어 지침 : S/W에 대해 단독 지침은 아님
- 소프트웨어 안전수준을 결정하기 위해, 안전성 평가가 요구됨
- 프로젝트 기반으로 개발활동을 통한 오류 제거
- 라이프사이클 활동과 관련된 목표와 그 산출물을 제시
- 다른 S/W 표준 대비 특이사항 : S/W 레벨 개념 도입, 커버리지 분석 요구
- DO-178은 주로 프로세스중심의 문서
  - 지정된 프로세스 (계획, 개발, 검증 등)와 이들 결과물에서의 요구조건 집합
- 항공기의 지속적인 안전한 비행과 착륙을 저해할 수 있는 모든 고장 조건의 발생 가능성이 없음을 입증
  ⇒ 요구조건을 충족시키는 증거는 소프트웨어 안전(Criticality) 수준에 따라 변함

항공용 소프트웨어 개발 및 DO-178C

- **DO-178B=> DO-178C 개정에 따른 변경 및 추가 사항**
  - 주요 변경 내용
    - 툴 검증(Tool Qualification) – [DO-330]
    - 모델기반 설계(Model-Based Development Supplement) – [DO-331]
    - 객체지향 기술(Object-Oriented Technology) – [DO-332]
    - 정형기법(Formal Method) – [DO-333]

DO-178B → 보완 & 수정 → DO-178C

DO-178B	DO-178C
• S/W 개발 툴 • S/W 검증 툴	• S/W 개발 툴 • S/W 검증 툴 : 다른 개발/검증 통합 • S/W 검증 툴(Only)

추가 보충 문서

DO-330 - 툴 검증(Tool Qualification)

- DO-331 모델 기반 설계 (Model-Based Development Supplement)
- DO-332 객체 지향 기술 (Object-Oriented Technology)
- DO-333 정형 기법 (Formal Method)

항공용 소프트웨어 개발 및 DO-178C

소프트웨어 안전 수준 분류

SW 수준	고장 상태	고장상태의 분류
A	계속적인 안전 비행과 착륙을 막는 고장 상태	Catastrophic
B	아래와 같은 혹심한 운용 조건을 대처해 나가는 항공기 또는 승무원의 조종 능력을 떨어뜨리는 고장 상태 (1) 안전여유 또는 기능적 성능의 상당한 감쇄 (2) 승무원이 임무를 정상적으로 완전하게 수행할 수 없는 물리적 재난 또는 과도한 조종 부하 (3) 소수의 승객에게 심각하거나 잠재적 치명 상해와 같은 혹심한 영향이 있는 상태	Hazardous
C	승무원의 조종부하의 상당한 증가, 승무원의 능률이 저하되는 상태 또는 승객에게 부상이 발생하는 불편함과 같은 안전여유 감소 또는 항공기의 성능저하와 같은 혹심한 운항조건에 대처해 나가는 항공기의 성능 또는 승무원의 능력을 감쇄시키는 상태	Major
D	항공기의 안전을 현저하게 감쇄시키는 상태로서 승무원의 능력범위 안에서 수습 가능한 상태	Minor
E	항공기의 운용 성능을 떨어뜨리지 않으며 조종 부하를 증가시키지 않는 고장 상태	No Effect

항공용 소프트웨어 개발 및 DO-178C

소프트웨어 Level에 따른 DO-178C 목표

	Level A	Level B	Level C	Level D	Level E
Failure Condition due to S/W Anomalous behavior	Catastrophic	Hazardous	Major	Minor	No effect
# of objectives	71	69	62	26	-
# of objectives with independence	30	18	5	2	-

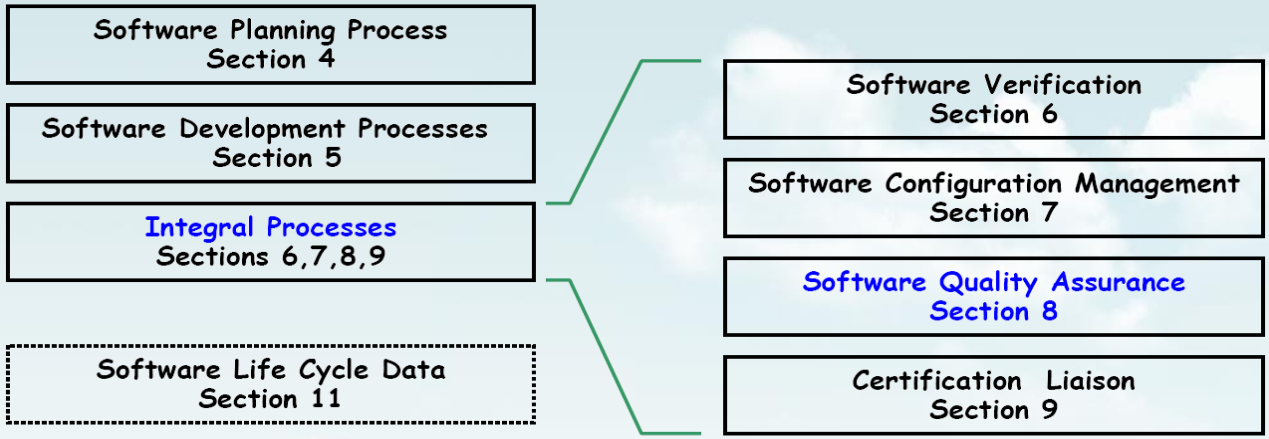
	Objective		Applicability by SW level				Output		Control category by SW level			
	Description	Ref.	A	B	C	D	Description	Ref.	A	B	C	D
1	Test procedures are correct.	6.3.6b	●	❍	❍		Software Verification Cases and Procedures	11.13	②	②	②	

LEGEND

●	The objective should be satisfied with independence.
❍	The objective should be satisfied.
Blank	Satisfaction of objective is at applicant's discretion.
①	Data satisfies the objectives of Control Category 1 (CC1).
②	Data satisfies the objectives of Control Category 2 (CC2).

항공용 소프트웨어 개발 및 DO-178C

DO-178 프로세스

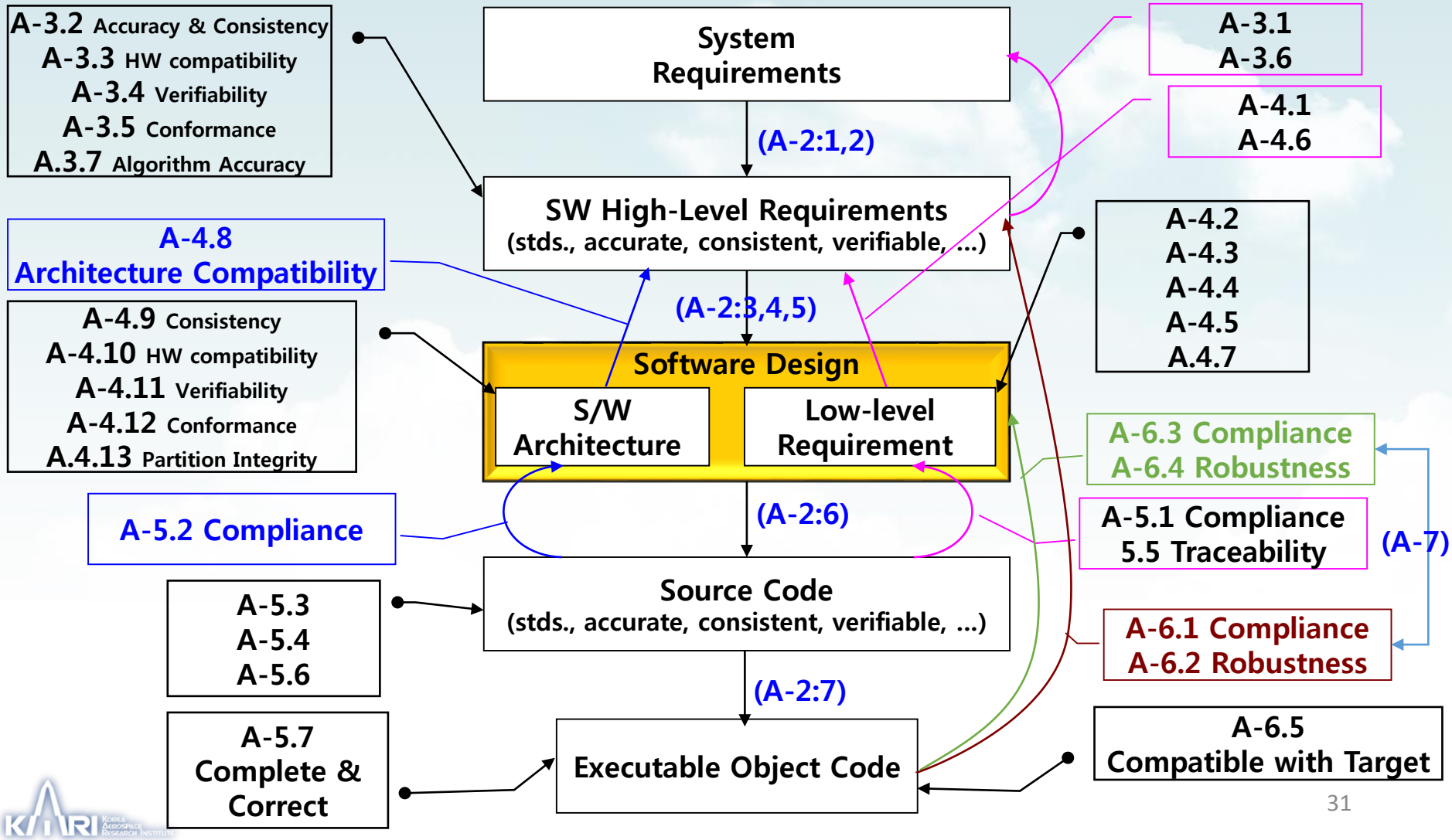


DO-178C 검증프로세스

- DO-178의 가장 중요한 Section
  - Workload 가중(A380의 경우, 임베디드 코드 1 line 에 대해 4 lines 시험)
- 개발과정에 발생되는 오류를 탐지하고 식별하기 위해 사용된 모든 프로세스에 적용
- 접근 방법
  - 분석(정량적 조사)
  - 검토(정성적 검사)
  - 시험(기능 및 구조 커버리지)

항공용 소프트웨어 개발 및 DO-178C

DO-178C 검증 프로세스

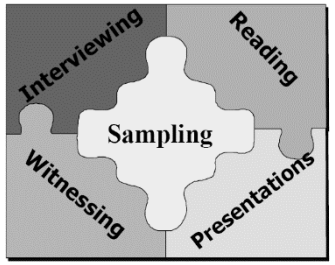


항공용 소프트웨어 개발 및 DO-178C

항공전자장비 인증 관점

- DO-178C 에서 인증 이해와 소통에 대한 개념을 정의 (Certification Liaison)
  - 인증을 받고자 하는 신청자와 감항당국간의 소통과 이해를 효과적으로 추진
- 목적 및 방법
  - 효과적인 이해와 소통을 위해 가능한 조기에 인증계획서(PSAC) 제출
  - 경험 및 능력을 고려하여 인증당국이 원하는 만큼 독립적인 검토 실행하되, 적시에 기술적 문제를 언급, 적합성 자료의 확인, 계획과 절차 준수, 위임자 감독
    - SOI #1: 계획서, 표준, 점검표 등 완료 및 형상관리를 적용 한 후(계획단계 종료 시점)
    - SOI #2 :개발단계에서 Source Code 완료 시점(복잡한 S/W인 경우, 50% 완료 후)
    - SOI #3: 검증단계완료 후(복잡한 S/W인 경우, 50% 완료 후)
    - SOI #4: 개발완료 시 수행

    ※ FAA Order 8110.49 및 국토부 지침서(항공용 소프트웨어 승인 지침) 참고
  - 소프트웨어 형상 색인(Software Configuration Index) 제출
  - 소프트웨어 구현 요약서(Software Accomplishment Summary) 제출



Ⅴ. 국내 항공용 소프트웨어 개발사례

국내 항공전자 개발 사례

항공용 소프트웨어 개발 사례(기술표준품 형식승인)

대 상 품	적용 KTSO (S/W Level)	신청자	승인서 번호 (교부일)
ADC (Air Data Computer)	KTSO-C106 (Level A)	퍼스텍	KTSO 2012001 (2012.5.25)
MFD (Multi-Functional Display)	KTSO-C113 (Level B)	LIG 넥스원	KTSO 2013001 (2013.10.25)
통합항전장비 (Integrated Flight Display System)	KTSO-C113a 외 부분 KTSO 21종 (Level B/C/D)	LG CNS	KTSO-1201 (2012.8~진행중)

국내 항공용 소프트웨어 개발 사례

ADC(Air Data Computer)

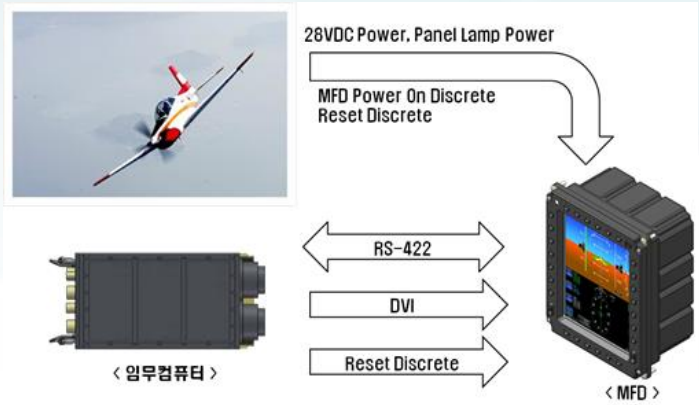
- 개발자 : 퍼스텍㈜
- 장비명: 대기자료 컴퓨터(Air Data Computer, ADC)

  Air Data Probe로부터 전압(Pt), 정압(Ps), 온도(Tt) 등의 대기자료를 수집하여 속도, 고도, 고도 상승률 등의 정보를 계산하여 항법계통에 전송
- 적용 규격
  - 기술표준품 표준서: KTSO-C106
  - 최소성능표준: SAE AS 8002 (Rev. A
  - 소프트웨어: RTCA DO-178B, Level
  - 전자하드웨어: RTCA DO-254, Level
  - 환경규격: RTCA DO-160 (Rev. E)

국내 항공용 소프트웨어 개발 사례

MFD(Multi-Functional Display)

- 개발자: LIG 넥스원㈜
- 장비명: 다기능 시현기(Multi Function Display, MFD)
  - 조종사의 임무에 필요한 항법, 통신, 식별, 항공기 상태 정보 등을 임무환경에 맞도록 시현하는 장치
- 적용 규격
  - 기술표준품 표준서: KTSO-C113
  - 최소성능표준: SAE AS 8034 (Rev. A)
  - 소프트웨어: RTCA DO-178B, Level B
  - 환경규격: RTCA DO-160 (Rev. F)



국내 항공용 소프트웨어 개발 사례

통합항전장비디스플레이(Integrated Flight Display, IFD)

- 개발자 : LG CNS㈜
- 대상품 : 12.1” 스마트타입 MFD(KTSO-C113a 외 22)
  - 적용 규격
    - 기술표준품 표준서: KTSO-C113 외 26
    - 최소성능표준: SAE AS 8034A 외 26
    - 소프트웨어: RTCA DO-178B, Level B/C/D
    - 전자하드웨어: RTCA DO-254, Level B
    - 환경규격: RTCA DO-160 (Rev. G)

Item	Failure	S/W level
Altitude	HAZ	B
Moving map	MAJ	C
Chart display	MIN	D
…	…	…

감사합니다