『항공전자 S/W 안전』

2016년 11월 29일

한국항공우주산업(주)

목 차

I. 항공전자 소프트웨어 안전

I. 항공전자 소프트웨어 안전

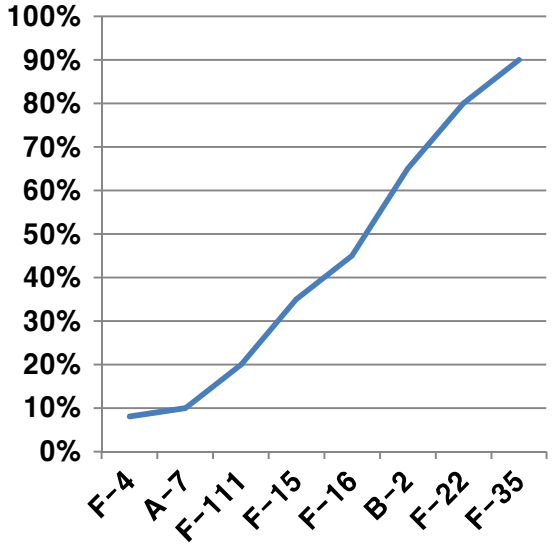
항공전자 소프트웨어

- **항공전자 S/W 특성**
  - 항공전자는 비행 보조 수단으로 항공기 성능에 중요한 요소
  - 기술 발전 추세와 함께 타 계통 기술보다 급속히 발전
  - 항공기 수명주기보다 항공전자 수명주기가 짧아 항공전자 성능개량 요구 증대
  - 항공전자 단일장비 성능보다 통합 성능 향상으로 발전

- **항공전자 소프트웨어 비중 증대**
  - 소프트웨어로 수행되는 비율 증가

기종	F-4	A-7	F-111	F-15	F-16	B-2	F-22	F-35
년도	1960	1964	1970	1975	1982	1990	2000	2007
비율	8%	10%	20%	35%	45%	65%	80%	90%

[The Method Framework for Engineering System Architectures(09)]



I. 항공전자 소프트웨어 안전

안전에 대한 정의

- MIL-STD-882 'System Safety Program Requirements'
  - 사망, 상해, 직업병, 또는 장비나 재산 또는 그 환경의 손상이나 손실을 일으키는 조건들로부터의 자유 (Freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment)

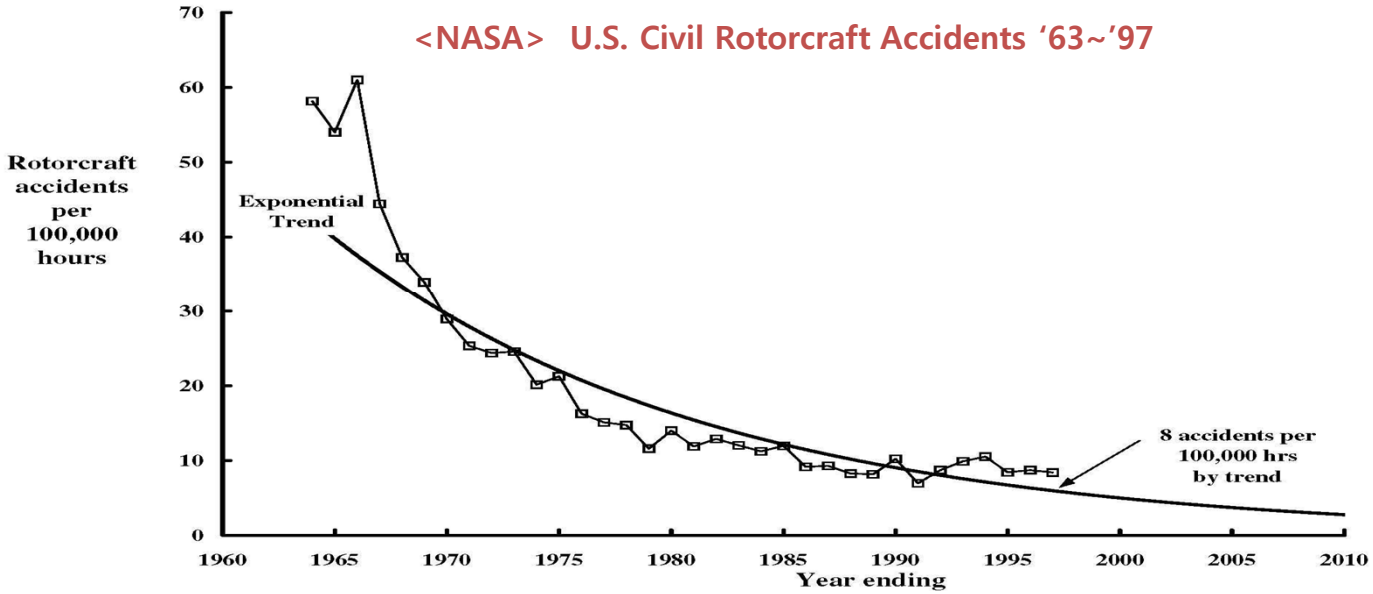
- 공군교리 (공교 1-2-26)
  - 위험에 대한 공포로부터의 해방을 말하며, 인사사고 요인, 물적 및 환경적 위험을 제거한 상태

I. 항공전자 소프트웨어 안전

항공기 사고 분석

- 전세계적으로 항공기 사고율은 감소되고 있음.
  - 엄격한 안전프로그램 도입으로 1950년대 이후 미공군 중사고율은 현격히 감소.
  - 80년대 중반까지는 사고율의 감소추세가 뚜렷하였으나, 이후 감소추세가 둔화 되고 있음

<NASA> U.S. Civil Rotorcraft Accidents '63~'97



- 전반적으로 사고율은 감소되고 있으나 항공기 운영대수 및 운항횟수의 증가로 년간 사고발생 건수와 치명도는 증가

I. 항공전자 소프트웨어 안전

항공기 안전의 필요성

- 항공기 사고 발생 시 인명 손상 , 자산 손실, 환경 파괴, 비용 유발 등 치명적 손상 초래

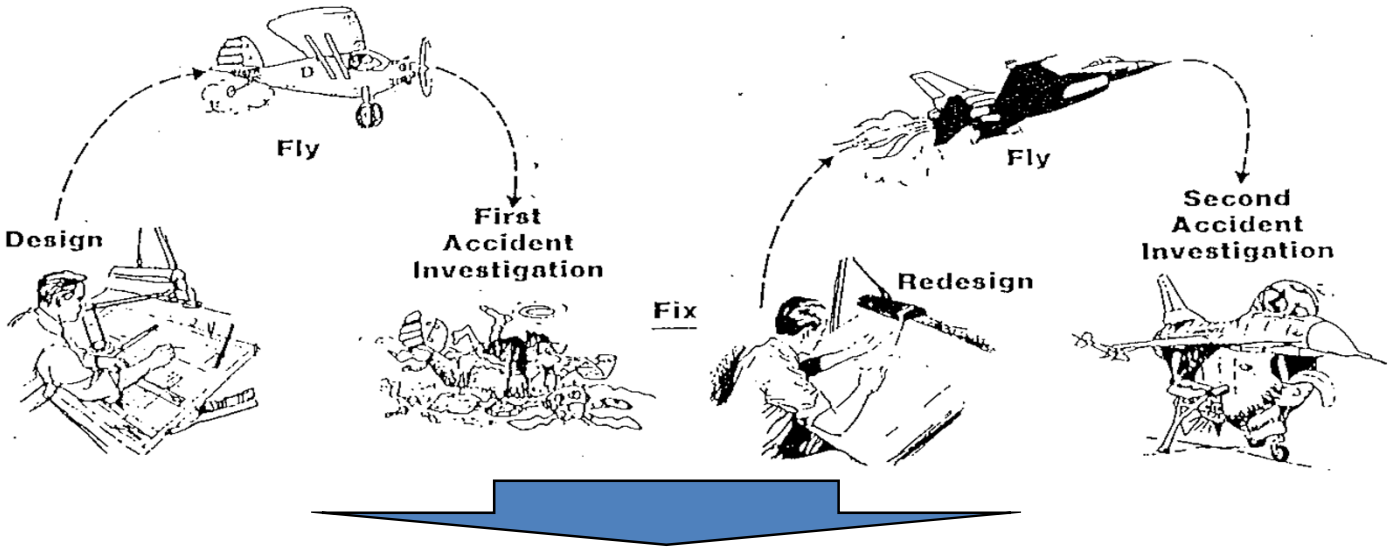
- 전체 개발 프로그램 비용 비교하여 크지 않은 비용 소요
  - 1대 항공기 손실을 방지하는 경우, 안전에 소요된 개발 비용 이상이 보상됨

- 설계단계에서 초기에 위험요소를 발견하고 조치를 하는 경우,
  - 필요 시 재설계를 할 수 있는 기회 획득
  - 공식 기술교범의 변경 행위 불필요
  - 지원장비 또는 예비부품의 변경 행위 불필요
  - 재시험이 불필요

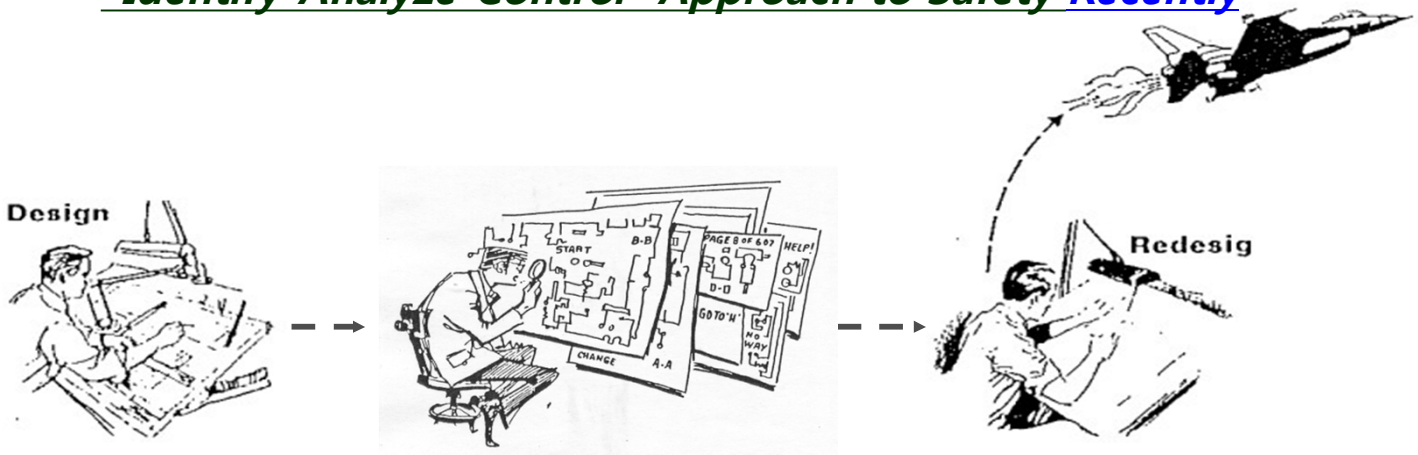
I. 항공전자 소프트웨어 안전

항공기 안전에 대한 방법론

"Fly-Fix-Fly" Approach to Safety in the Past



"Identify-Analyze-Control" Approach to Safety Recently



I. 항공전자 소프트웨어 안전

항공기 안전 프로그램

- 특정 항공기가 안전한지 어떻게 알 수 있나?
  - 체계적이고 엄격한 인증기준이 필요

- 항공기 안전에 관한 인증기준
  - 감항인증
    : 법률의 권한을 부여받은 감항당국이 항공기 또는 부품 제조자의 제품이 비행안전성에 적합한지를 확인하고 승인하는 법적 행위

    – 민수항공법에서 정의하는 감항성
      : 항공기가 안전하게 비행할 수 있는 성능
    – 군수항공기 비행안전성 인증에 관한 법률에서 정의하는 감항성
      : 군용항공기가 운용범위 내에서 비행안전에 적합

- 항공기 감항인증 기준
  - 민수 항공기 감항인증 기준
    – FAR(FAA), STANAG(NATO) 등
  - 군수 항공기 감항인증 기준
    – 표준감항인증기준 또는 승인된 기타감항인증기준을 기초로 해당 군용항공기 특성에 맞게 감항인증기준 수립

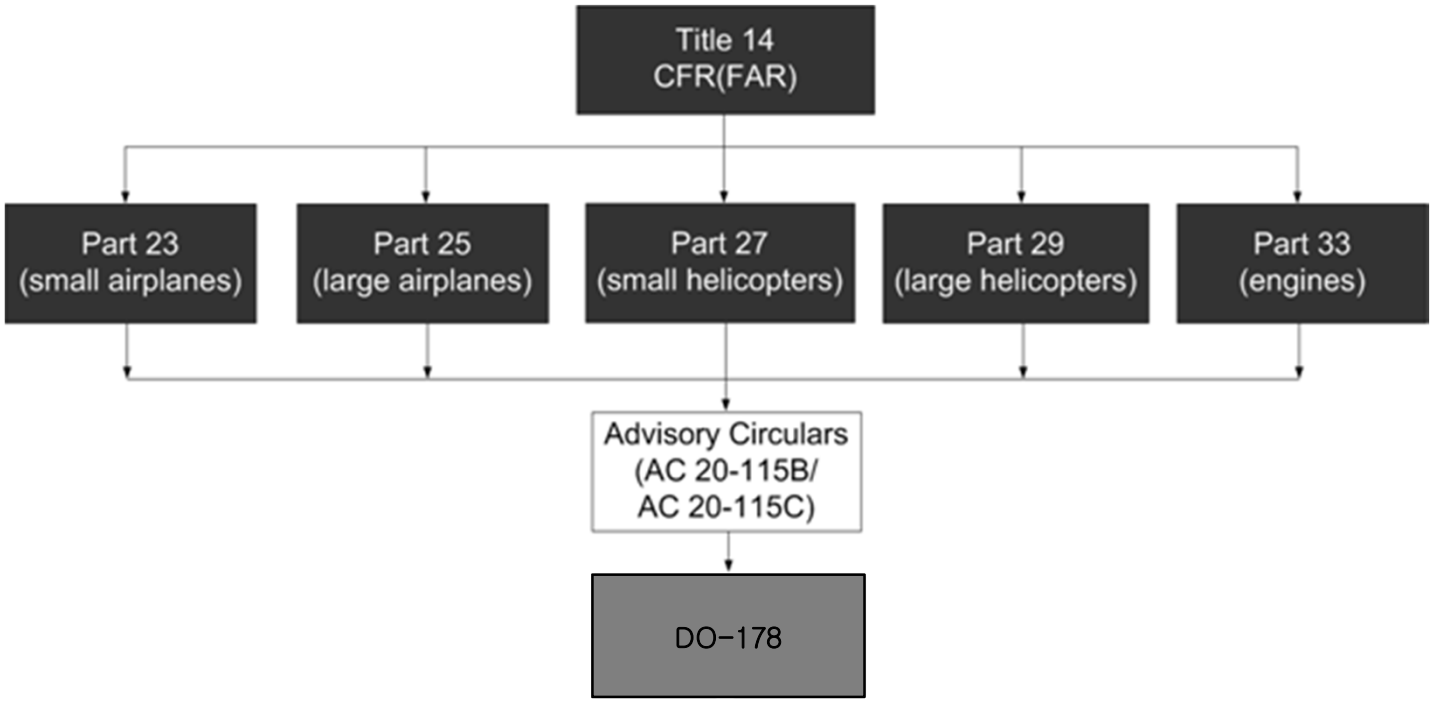
II. 민수 항공분야 소프트웨어 안전

II. 민수 항공분야 소프트웨어 안전

소프트웨어 안전 기준

➢ 민수 항공기 소프트웨어 인증

- DO-178B는 항공기 제조 업계의 의견수렴과 동의를 통해, 미국의 RTCA와 유럽의 EUROCAE에 의해 표준 인증 체계로 1992년 발표 및 권고되었으며, 미 항공국(FAA) 및 각국 정부에 의해 "Software considerations in Airborne Systems and Equipment Certification(항공기 및 항공 장비 인증시 소프트웨어 고려사항)으로 승인된 표준 인증 체계



II. 민수 항공분야 소프트웨어 안전

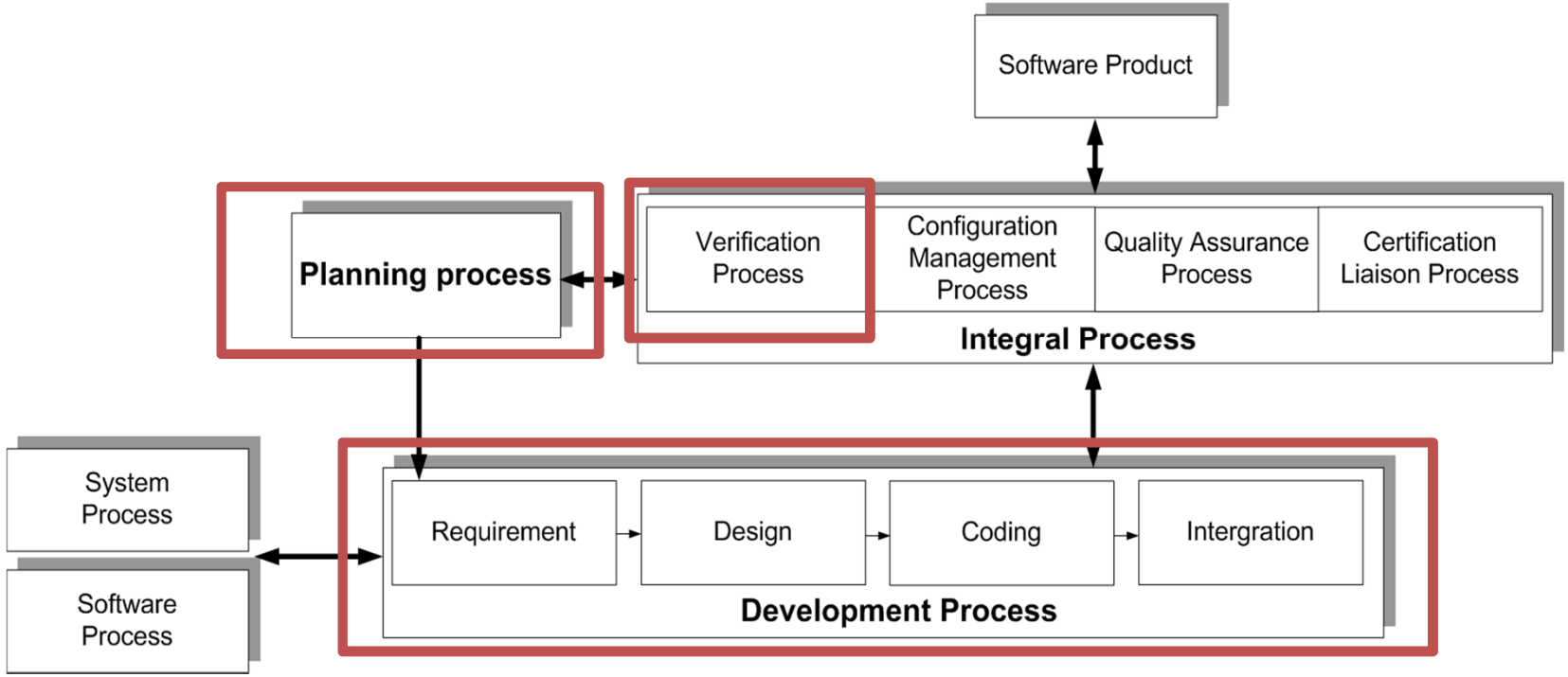
소프트웨어 인증 기술 발전 동향

규격	년도	Basis	주요 내용
DO-178	1980	498 & 2167A	기본적인 절차
DO-178A	1985	DO-178	소프트웨어 엔지니어링 관련 원칙 강화. • 소프트웨어 레벨 도입 • 소프트웨어 컴포넌트 테스팅 도입
DO-178B	1992	DO-178A	“어떻게” 보다는 “무엇을” 에 중점 • 다양한 소프트웨어 개발 기술 도입 (COTS 제품, 툴 도입) • 지속적인 소프트웨어 품질보증 도입 (전환기준)
DO-178C	2011	DO-178B	최신 소프트웨어 개발 기술 도입 • 모델기반 개발 및 검증 • 정형기법 • 객체지향 기술

II. 민수 항공분야 소프트웨어 안전

DO-178

- **DO-178에서 요구하는 소프트웨어 프로세스**
  - 계획 프로세스(Planning process)
  - 개발 프로세스(Development process)
    - 요구조건 단계, 설계 단계, 코딩 단계 및 통합/시험 단계
  - 통합 프로세스(Integral process)
    - 검증, 형상관리, 품질보증 및 인증 지원



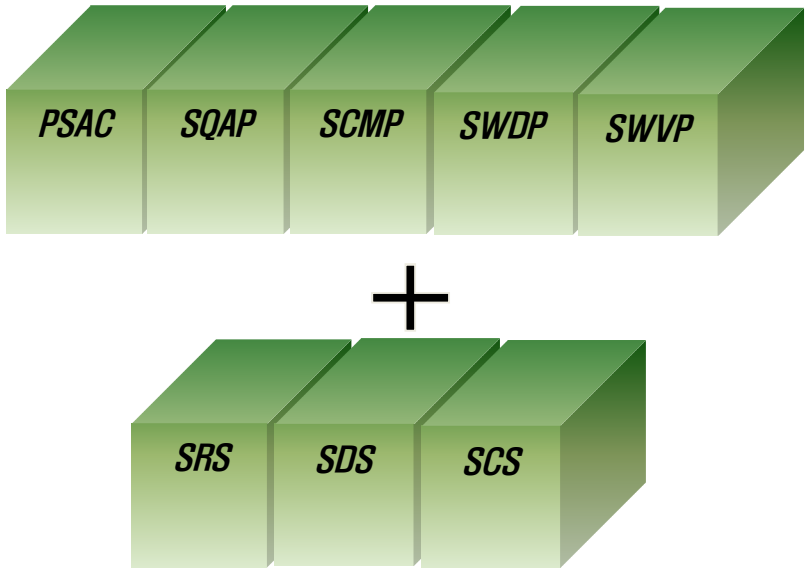
II. 민수 항공분야 소프트웨어 안전

DO-178 (Planning process)

- **소프트웨어 계획 PROCESS**
  - 시스템 요구 사항을 충족하고 소프트웨어 레벨에 대한 신뢰성을 만족하는 수단 정의

- **수행업무**
  - 시스템 요구 사항 할당
  - 소프트웨어 레벨 정의
  - 소프트웨어 라이프 싸이클 결정
  - 소프트웨어 개발 환경 정의

- **산출물**
  - **PSAC**(Plan for SW Aspects of Certification)
  - **SDP**(SW Development Plan)
  - **SVP**(SW Verification Plan)
  - **SCMP**(SW Configuration Management Plan)
  - **SQAP**(SW Quality Assurance Plan)
  - **SRS**(SW Requirements Standards)
  - **SDS**(SW Design Standards)
  - **SCS**(SW Code Standards)



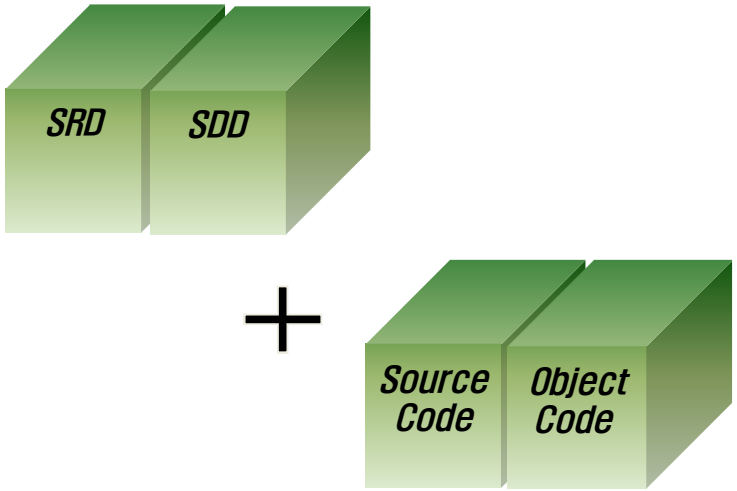
II. 민수 항공분야 소프트웨어 안전

DO-178 (Development process)

- 소프트웨어 개발 PROCESS
  - Software requirements process
  - Software design process
  - Software coding process
  - Integration process

- 수행업무
  - High-level requirements, Low-level requirements의 개발
  - Derived high-level requirements, Derived low level requirements의 개발
  - Software Architecture 및 Source Code 개발
  - Integration HW/SW

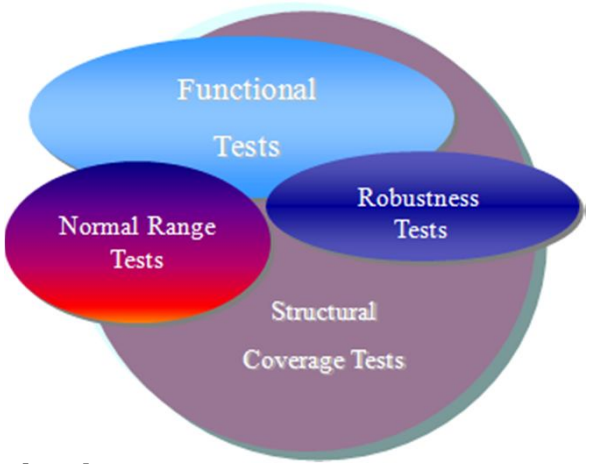
- 산출물
  - Software Requirement Data
  - Software Design Description
  - Source Code
  - Executable Object Code



II. 민수 항공분야 소프트웨어 안전

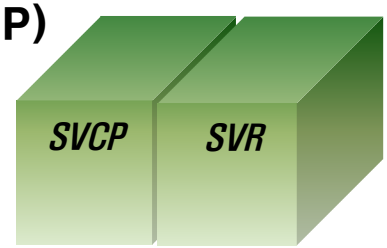
DO-178 (Verification process)

- 소프트웨어 확인 PROCESS
  - 소프트웨어 개발 오류에 대한 확인 및 제거



- 수행업무
  - 소프트웨어 Review & Analyses
  - 소프트웨어 테스트
    - Low Level testing
    - SW integration testing
    - HW/SW integration testing
    - SW Requirements-Based Test Coverage Analysis
    - SW Structural Coverage Analysis

- 산출물
  - Software verification cases and procedures (SVCP)
  - Software verification results (SVR):
    - Review of all requirements, design and code
    - Testing of executable object code
    - Code coverage analysis



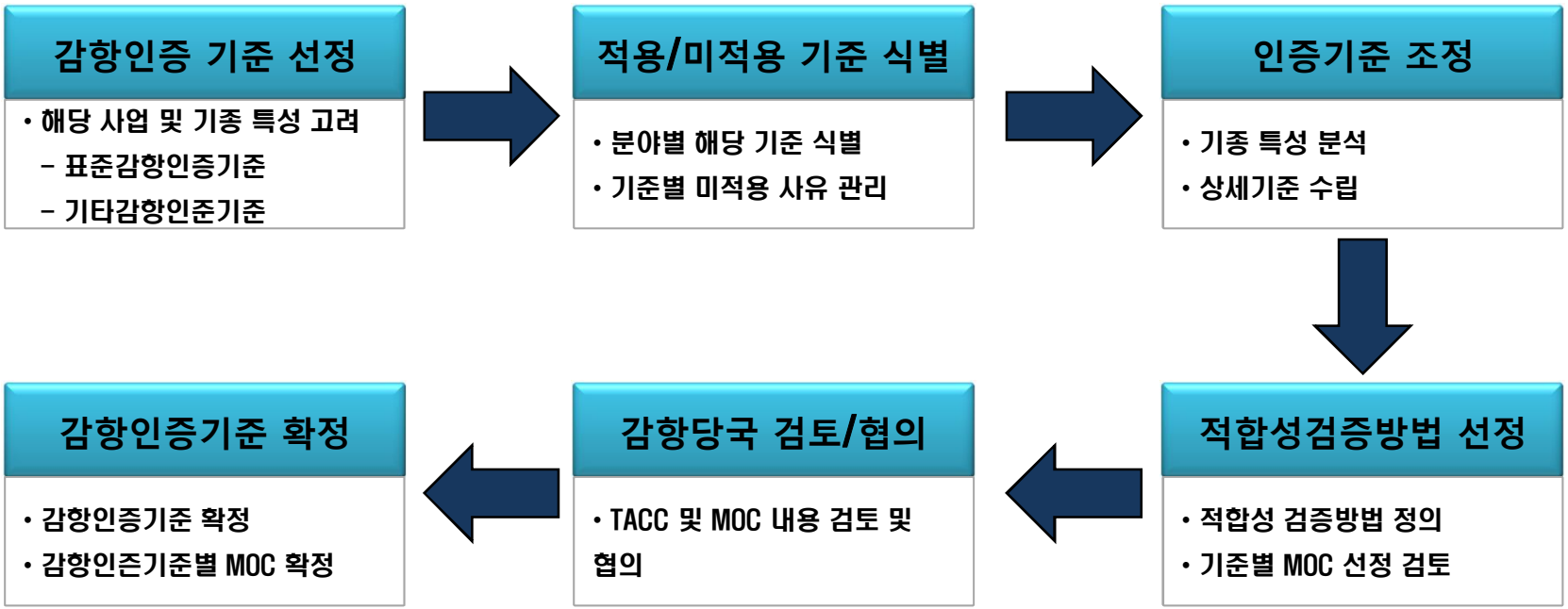
  - Analysis of all code and traceability from tests and results to all requirements is typically required (depending on software level)

III. 군수 항공분야 소프트웨어 안전

III. 군수 항공분야 소프트웨어 안전

소프트웨어 안전 기준

➢ 군수 항공기 소프트웨어 인증
- 방위사업청 고시에 따라 '군용항공기 표준감항인증기준' 에 따라 MIL-HDBK-516B으로 제정
- 표준감항인증기준 또는 기타감항인증 기준을 기초로 하여 해당 군용항공기 사업의 특성에 맞게 기종별 감항인증기준(TACC)를 수립



TACC (Tailored Airworthness Certification Criteria) : 감항인증 기준
MOC (Means Of Compliance) : 적합성 검증방법

III. 군수 항공분야 소프트웨어 안전

표준감항인증기준

➢ **군용항공기 개발사업 시 항공기의 비행안전성을 확보하기 위해 미 국방실 무치침서 ‘MIL-HDBK-516’을 바탕으로 설계, 제작, 시험 등에 적용하는 인증기준**

구 분		기준 수
Section 4	시스템 엔지니어링	17
Section 5	구조	32
Section 6	비행기술	201
Section 7	추진, 추진체 장착	88
Section 8	세부계통	259
Section 9	승무원 시스템	72
Section 10	진단계통	7
Section 11	항공전자	34
Section 12	전기 계통	23
Section 13	전자기 환경효과	13
Section 14	시스템 안전	31
Section 15	컴퓨터 자원	27
Section 16	정비	21
Section 17	무장/무장 장착물	20

[MIL-HDBK-516B]

군용항공기 표준 감항 인증 기준 개정을 통해 최신 소프트웨어 발전 추세를 반영
(MIL-HDBK-516C)

[컴퓨터 자원]

[컴퓨터 시스템 및 SW]

III. 군수 항공분야 소프트웨어 안전

표준감항인증기준 (소프트웨어 개발 프로세스)

➢ **소프트웨어 개발 프로세스에 대한 기준, 표준, 적합성 검증방안 제시**

표준감항인증기준	기 준
15.4 소프트웨어 개발 프로세스 (Software development processes)	-
15.4.1 소프트웨어 프로세스(Software processes)	안전지원 소프트웨어요소(SSSE)를 위한 소프트웨어 개발 절차가 모두 문서화(예 : 소프트웨어 개발 계획(SDP), 소프트웨어 안전 계획(SSP))되고, 이를 준수하며, 안전필수기능(SCF)을 지원하는 소프트웨어를 생산하는데 충분히 적합함을 검증하라.
15.4.2 추적성(Traceability)	각 안전지원 소프트웨어요소(SSSE)는 요구도(성능 및 인터페이스), 설계, 소스 코드, 시험 데이터에 대한 충분한 양방향 추적성이 설정되어 있음을 검증하라.
15.4.3 형상관리 (Configuration management)	형상/변경 통제 관리 절차가 완전히 문서화되고, 준수되며, 안전필수기능(SCF) 지원 소프트웨어 통제에 충분히 적합함을 검증하라.

III. 군수 항공분야 소프트웨어 안전

표준감항인증기준 (소프트웨어 아키텍쳐와 설계)

➢ **소프트웨어 아키텍쳐와 설계에 대한 기준, 표준, 적합성 검증방안 제시**

표준감항인증기준	기 준
15.5 소프트웨어 아키텍쳐와 설계 (Software architecture and design)	
15.5.1 소프트웨어 아키텍쳐 (Software architecture)	소프트웨어 구조와 설계가 정의되고, 시스템/소프트웨어 요구도가 올바르게 구현되었으며, 안전함을 검증하라.
15.5.2 소프트웨어 통제 구조와 실행률 (Software control structure and execution rates)	각 안전지원 소프트웨어요소(SSSE)에 있어 실행/통제구조(우선순위 지정과 인터럽트 설계를 고려)에 의해 제공되는 실행률이 일정하게 획득 가능하고 모든 지원되는 안전필수기능(SCF) 요구 성능을 안전하게 제공하는데 충분함을 검증하라.
15.5.3 소프트웨어 아키텍쳐 속성과 성능 (Software architecture attributes and performance)	모든 안전지원 소프트웨어요소(SSSE)에 대한 초기화, 동기화, 타이밍, 데이터 흐름, 통제 흐름, 인터럽트 구조, 데이터 구조를 포함한 소프트웨어 구조 및 설계가 안전하고 모든 지원되는 안전필수기능(SCF)의 요구 처리성능을 뒷받침하는데 충분함을 검증하라.
15.5.4 동적 운용 (Dynamic operation)	모드 입력, 운영 비행 모드, 고장 감시 및 탐지 기술, 고장 관리 기능, 중복여유 관리, 보팅 정책(voting scheme), 자체검사(Self-check), 자체진단시험(BIT), 안전 인터록 작동구조(Safety Interlock Mechanization), 안전필수기능(SCF) 인터페이스, 건전 상태(Health status) 인터페이스, 재구성(reconfiguration) 능력, 명령 및 통제 데이터링크 전환 사항들이 모든 예상되는 동적 조건 하에서 안전작동을 위해 설계됨을 검증하라..

III. 군수 항공분야 소프트웨어 안전

표준감항인증기준 (소프트웨어 아키텍쳐와 설계)

➢ **소프트웨어 아키텍쳐와 설계에 대한 기준, 표준, 적합성 검증방안 제시**

표준감항인증기준	기 준
15.5 소프트웨어 아키텍쳐와 설계 (Software architecture and design)	
15.5.5 고장 관리 및 중복여유 관리 (Failure management and redundancy management)	자체진단시험(BIT), 중복여유 관리, 고장 관리 알고리즘의 안전한 작동을 검증하라.
15.5.6 디지털 시스템 고장 (Digital system failures)	안전지원 소프트웨어요소(SSSE)가 디지털 시스템 고장을 탐지하고 수용하는데 충분하게 설계됨을 검증하라.
15.5.7 재시작과 리셋 능력 (Restart and reset capabilities)	안전지원 소프트웨어요소(SSSE) 설계가 비행중에 안전하게 시스템 재시작 및(또는) 리셋이 가능한 필요 준비를 가지고 있음을 검증하라.
15.5.8 불안전한 기술 (Unsafe techniques)	안전지원 소프트웨어요소(SSSE)가 불안전한 기술이나 속성(예 : 패치, 비활성 코드, 시험실시험 기능성)을 활용 또는 포함하지 않음을 검증하라.
15.5.9 자원용량 (Resource capacity)	모든 프로세서, 데이터 채널(I/O, 버스 등), 데이터 저장 장치에 충분한 용량과 설계 여유가 있음을 검증하라.
15.5.10 안전지원 소프트웨어 성능(Safety Supporting Software Elements (SSSE) performance)	모든 안전지원 소프트웨어요소(SSSE)가 수용 가능한 성능과 안전을 제공함을 검증하라.

III. 군수 항공분야 소프트웨어 안전

표준감항인증기준 (소프트웨어 인증 및 설치)

➢ **소프트웨어 인증 및 설치에 대한 기준, 표준, 적합성 검증방안 제시**

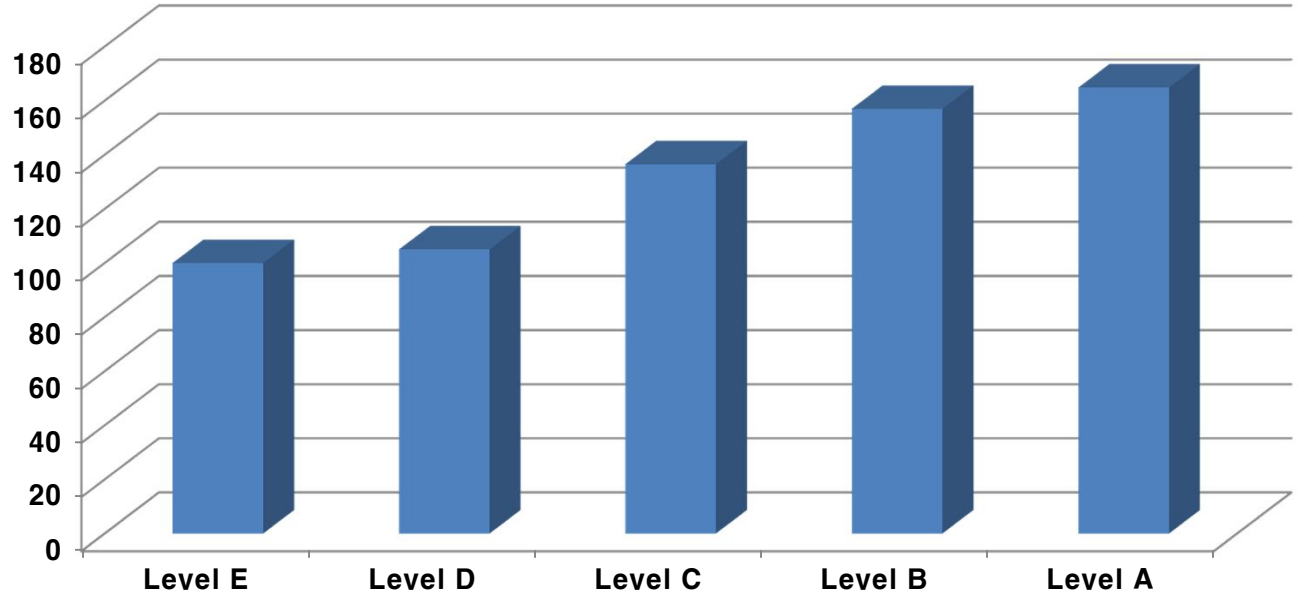
표준감항인증기준	기 준
15.6 소프트웨어 인증 및 설치 (Software qualification and installation)	
15.6.1 소프트웨어 시험방법 (Software test methodology)	각 안전지원 소프트웨어요소(SSSE)가 소프트웨어 구성품 단계에서부터 통합된 시스템 단계까지 다단계 접근법으로 시험되고 통합되며, 각 시험 단계에서 시험 범위가 충분함을 검증하라.
15.6.2 소프트웨어 전체 인증 (Full qualification of software)	비행을 위해 배포된 모든 안전지원 소프트웨어요소(SSSE)가 모두 인증되었음을 검증하라.
15.6.3 소프트웨어 빌드 프로세스 (Software build process)	비행을 위해 배포된 모든 안전지원 소프트웨어요소(SSSE)가 모두 인증되었음을 검증하라.
15.6.4 소프트웨어 장입 호환성(Software load compatibility)	적합한 형상관리 통제가 항공 시스템에서의 목적된 사용을 위한 올바르고 기능적으로 호환성 있는 소프트웨어 장입을 보장는 것이 적절한지를 검증하라.
15.6.5 소프트웨어 장입 (Software load process)	모든 소프트웨어에 대한 소프트웨어 장입 및 장입 검증 절차가 안전하고 정확함을 검증하라.

IV. 결론

IV. 결론

- 어떤 경우든 위험은 아주 낮아질 수 있지만 결코 ZERO가 되지 않음

- 소프트웨어 안전 등급에 따라 시스템 및 소프트웨어 개발 비용이 증가하므로 최적의 소프트웨어 안전 등급 결정 필요함



[DO-178 등급별 일반비용]

IV. 결론

- 민수 항공전자 소프트웨어의 경우, DO-178을 고려하여 개발
- 군수 항공전자 소프트웨어의 경우, 표준감항인증기준 또는 기타감항인증 기준을 기초로 하여 해당 군용항공기 사업의 특성에 맞게 수립된 감항인증기준(TACC)을 고려하여 개발
- 군수 항공전자 소프트웨어의 경우, 방사청 '무기체계 소프트웨어 개발 및 관리 매뉴얼' 을 고려하여 개발

※ 무기체계 소프트웨어 개발 및 관리 매뉴얼
방위력개선사업 무기체계 소프트웨어의 체계적인 개발 및 관리를 위한 프로세스와 산출물 작성 표준 등을 규정

감사합니다

Q & A