Software V&V

Functional Safety Standards per Automative/Aerospace Industry

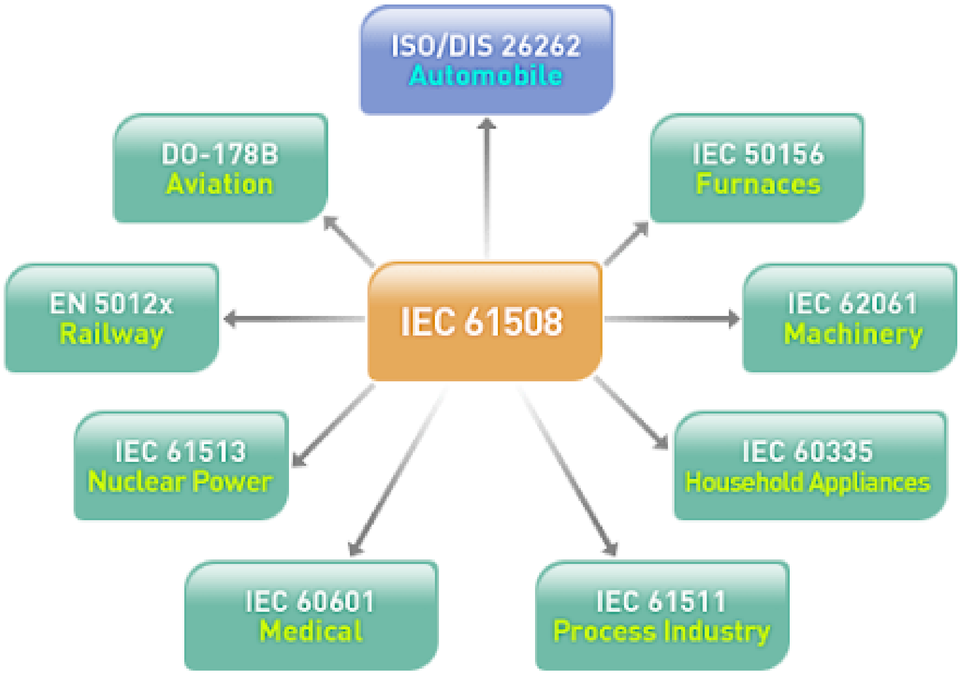
3팀
주재빈, 소경현, 이정우

ISO 26262 : 2018

Road vehicles – Functional safety

개요

- ISO 26262 또는 자동차 기능 안전성 국제 표준
- 자동차에 탑재되는 E/E (Electrical and/or Electronic) 시스템의 오류로 인한 사고방지를 위해 ISO에서 제정한 자동차 기능 안전 국제 규격
- 기능 안전 표준 IEC 61508을 자동차 전기/전자 시스템에 적용시킨 것



- 표준을 적용하는 것은 자율에 따르나 실제로는 점차로 더 많은 완성차 업체에서 그 부품공급업체들에게 새로운 프로젝트에 표준 적용을 요구하고 있다.

구성

1. Vocabulary
2. Management of functional safety
3. Concept phase
4. Product development at the system level
5. Product development at the hardware level
6. **Product development at the software level**
7. Production, operation **(service and decommissioning)**
8. Support processes
9. Automotive safety integrity level(ASIL)-oriented and safety-oriented analysis
10. Guidelines on ISO 26262
11. **(Guidelines on application of ISO 26262 to semiconductors)**
12. **(Adaptation of ISO for motorcycles)**

1. Vocabulary

2. Management of functional safety

- **2-5** Overall safety management
- **2-6** Project dependent safety management
- **2-7** Safety management regarding production, operation, service and decommissioning

3. Concept phase

- **3-5** Item definition
- **3-6** Hazard analysis and risk assessment
- **3-7** Functional safety concept

4. Product development at the system level

- **4-5** General topics for the product development at the system level
- **4-6** Technical safety concept
- **4-7** System and item integration and testing
- **4-8** Safety validation

7. Production, operation, service and decommissioning

- **7-5** Planning for production, operation, service and decommissioning
- **7-6** Production
- **7-7** Operation, service and decommissioning

12. Adaptation of ISO 26262 for motorcycles

- **12-5** General topics for adaptation for motorcycles
- **12-6** Safety culture
- **12-7** Confirmation measures
- **12-8** Hazard analysis and risk assessment
- **12-9** Vehicle integration and testing
- **12-10** Safety validation

5. Product development at the hardware level

- **5-5** General topics for the product development at the hardware level
- **5-6** Specification of hardware safety requirements
- **5-7** Hardware design
- **5-8** Evaluation of the hardware architectural metrics
- **5-9** Evaluation of safety goal violations due to random hardware failures
- **5-10** Hardware integration and verification

6. Product development at the software level

- **6-5** General topics for the product development at the software level
- **6-6** Specification of software safety requirements
- **6-7** Software architectural design
- **6-8** Software unit design and implementation
- **6-9** Software unit verification
- **6-10** Software integration and verification
- **6-11** Testing of the embedded software

8. Supporting processes

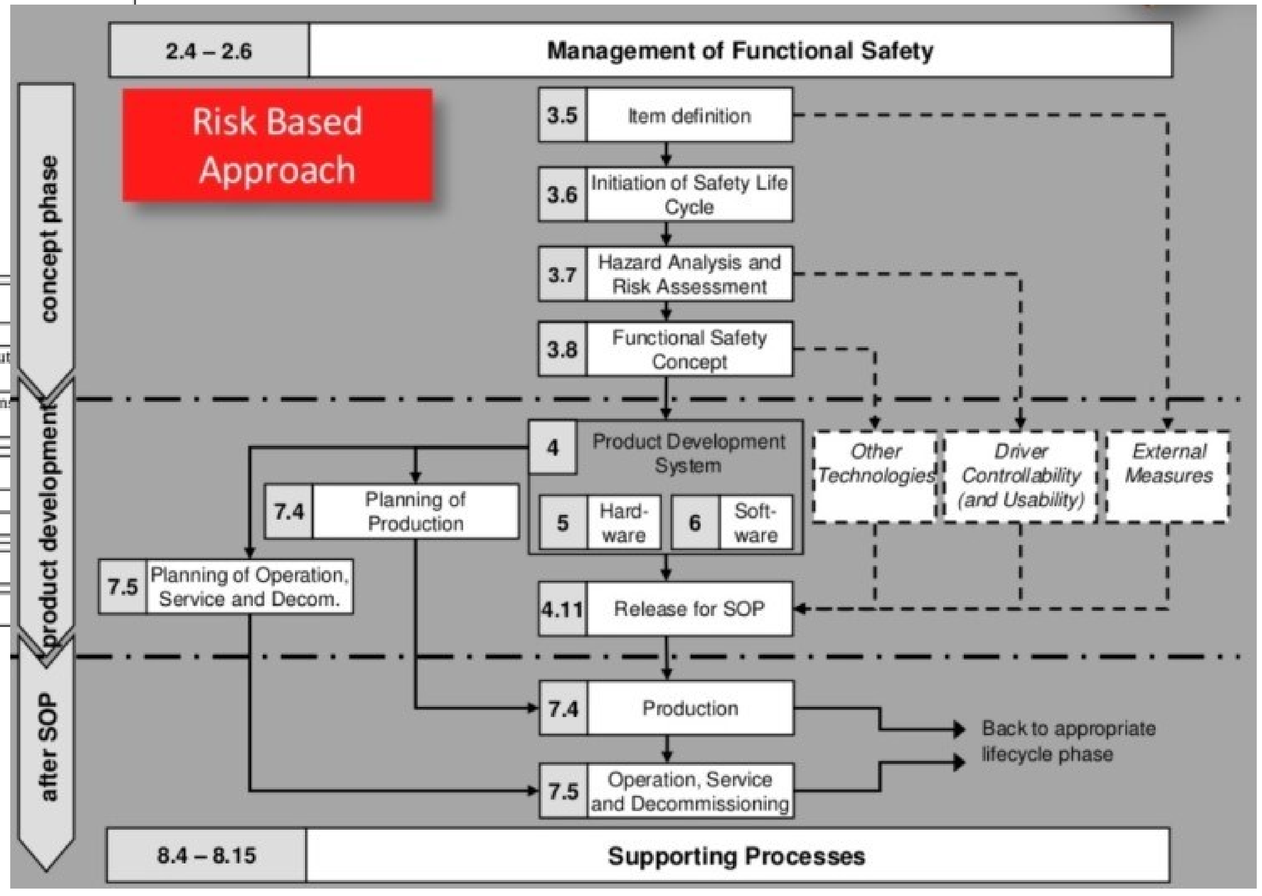
- **8-5** Interfaces within distributed developments
- **8-6** Specification and management of safety requirements
- **8-7** Configuration management
- **8-8** Change management
- **8-9** Verification
- **8-10** Documentation management
- **8-11** Confidence in the use of software tools
- **8-12** Qualification of software components
- **8-13** Evaluation of hardware elements
- **8-14** Proven in use argument
- **8-15** Interfacing an application that is out of ISO 26262
- **8-16** Integration of safety-related systems developed according to ISO 26262

9. Automotive safety integrity level (ASIL)-oriented and safety-oriented analyses

- **9-5** Requirements decomposition with respect to ASIL tailoring
- **9-6** Criteria for coexistence of elements
- **9-7** Analysis of dependent failures
- **9-8** Safety analyses

10. Guidelines on ISO 26262

11. Guidelines on application of ISO 26262 to semiconductors



part 6. Product development at the software level : overview

< sw development phase model >

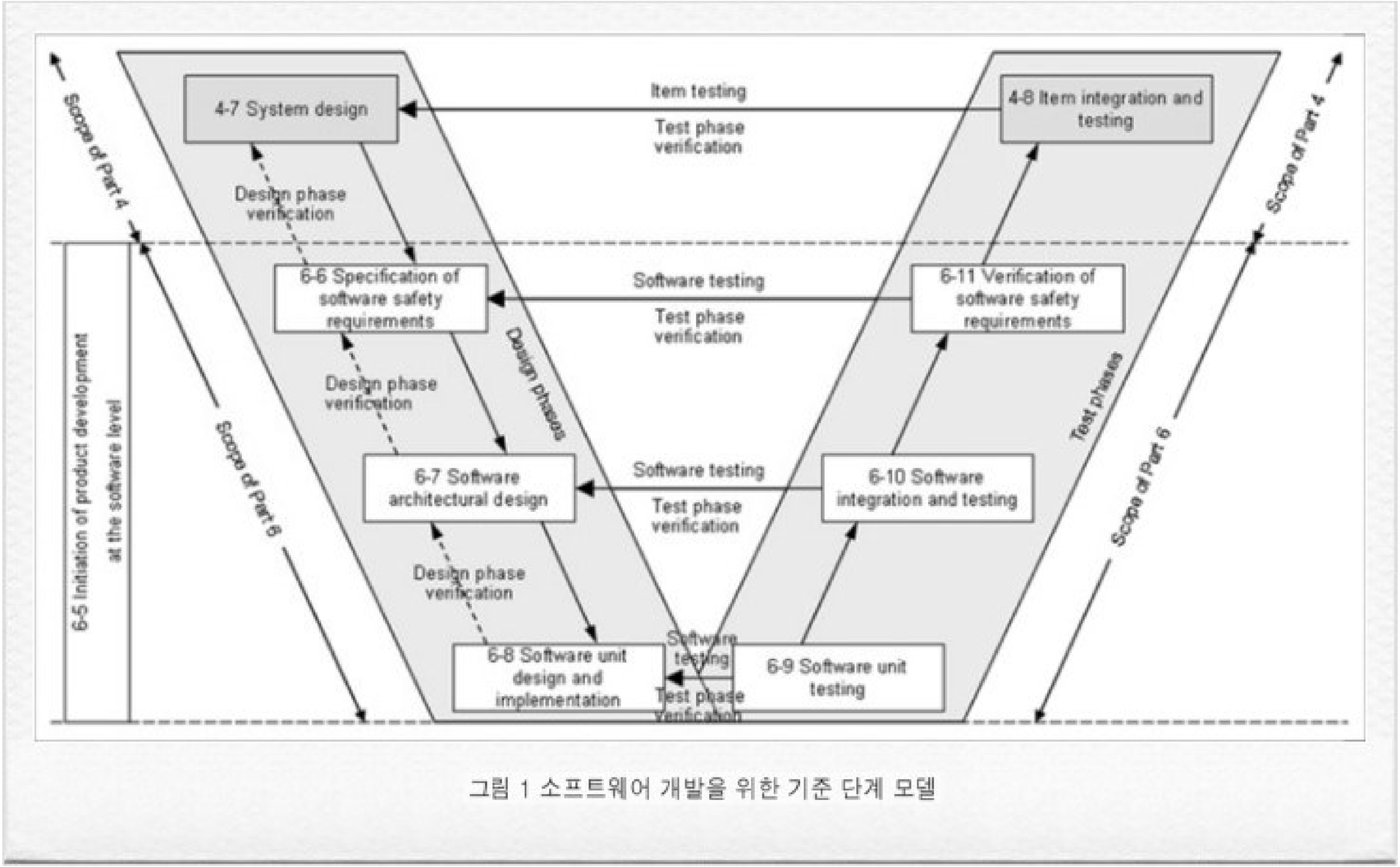


그림 1 소프트웨어 개발을 위한 기준 단계 모델

part 6. Product development at the software level : overview

< contents >

part 6. ISO 26262의 SW 검증단계

- Verification of software unit design (ISO 26262-6-8)
- Software unit testing (ISO 26262-6-9)
- Software integration and testing (ISO 26262-6-10)
- Verification of software safety requirements (ISO 26262-6-11)

part 6. ISO 26262의 SW 검증단계

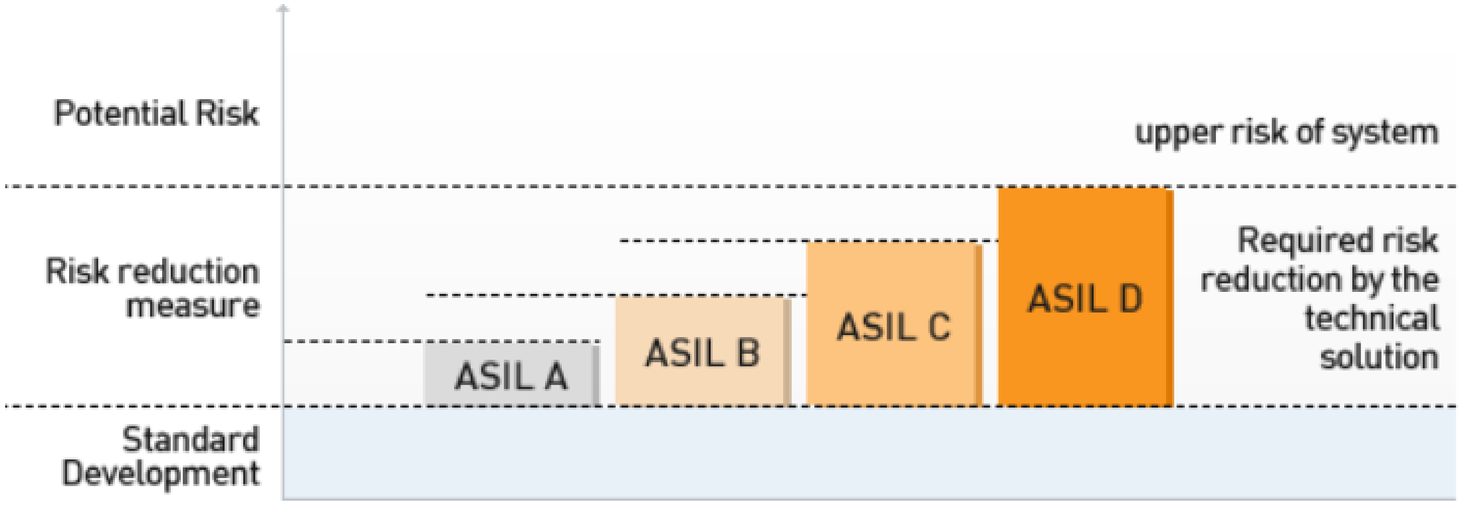
0) ASIL

- ASIL(Automotive Safety Integrity Level)
- A~D등급으로 나뉘며, D등급으로 갈수록 안전이 중요한 프로세스를 가진다는 것을 의미.

- “ + + ”는 해당 방법이 식별된 ASIL에 대해 매우 권장

- “ + ”는 해당 방법이 식별된 ASIL에 대해 권장

- “o”는 해당 방법이 식별된 ASIL에 대해 권장사항이 없음



재난 요인별 심각도 분석

TABLE 1. 잠재적 재난이나 위험에 대한 심각도 등급

등급 (Class)	S0	S1	S2	S3
설명	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

재난 요인별 노출 가능성 분석

위험 및 재난의 노출 가능성 등급

등급 (Class)	E0	E1	E2	E3	E4
설명	Incredible	Very low probability	Low probability	Medium probability	High probability

재난 요인별 통제 가능성 분석

재난 통제 가능성 등급

등급 (Class)	C0	C1	C2	C3
설명	Controllable in general	Simply controllable	Normally controllable	Difficult to control to uncontrollable

ASIL 정의

ASIL Definition		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

QM(Quality Management)
: 기능안전과 무관

High ↓
ASIL A: 기능안전등급 A
ASIL B: 기능안전등급 B
ASIL C: 기능안전등급 C
ASIL D: 기능안전등급 D

part 6. ISO 26262의 SW 검증단계

1) Verification of software unit design(소프트웨어 단위 설계 및 구현의 검증)
: 소프트웨어 아키텍처 설계를 기반으로 소프트웨어 단위의 상세 설계가 진행
상세 설계 및 구현은 소프트웨어 단위 시험 단계를 진행하기 전에 정적으로 검증

Methods		ASIL			
		A	B	C	D
1a	Walk-through[a]	++	+	o	o
1b	Inspection[a]	+	++	++	++
1c	Semi-formal verification	+	+	++	++
1d	Formal verification	o	o	+	+
1e	Control flow analysis[b,c]	+	+	++	++
1f	Data flow analysis[b,c]	+	+	++	++
1g	Static code analysis	+	++	++	++
1h	Semantic code analysis[d]	+	+	+	+

표 1 소프트웨어 단위 설계 및 구현 검증 방법

part 6. ISO 26262의 SW 검증단계

2) Software unit testing(소프트웨어 단위 시험)
: 소프트웨어에서 소스 코드의 단위(일반적으로 함수로 정함)이 의도된 대로 작동하는지 검증하는 절차

Table 10 — Methods for software unit testing

Methods		ASIL			
		A	B	C	D
1a	Requirements-based test[a]	++	++	++	++
1b	Interface test	++	++	++	++
1c	Fault injection test[b]	+	+	+	++
1d	Resource usage test[c]	+	+	+	++
1e	Back-to-back comparison test between model and code, if applicable[d]	+	+	++	++

표 2 ISO 26262에서 명시하는 소프트웨어 단위 시험 방법

Methods		ASIL			
		A	B	C	D
1a	Analysis of requirements	++	++	++	++
1b	Generation and analysis of equivalence classes[a]	+	++	++	++
1c	Analysis of boundary values[b]	+	++	++	++
1d	Error guessing[c]	+	+	+	+

표 3 ISO 26262에서 명시하는 소프트웨어 단위 시험을 위한 테스트 케이스 생성 방법

part 6. ISO 26262의 SW 검증단계

2) Software unit testing(소프트웨어 단위 시험) con't

	Methods	ASIL			
		A	B	C	D
1a	Statement coverage	++	++	+	+
1b	Branch coverage	+	++	++	++
1c	MC/DC (Modified Condition/Decision Coverage)	+	+	+	++

표 4 ISO 26262에서 명시하는 소프트웨어 단위 수준의 구조적 커버리지 지표

part 6. ISO 26262의 SW 검증단계

3) Software integration and testing(소프트웨어 통합 시험)

- 통합 시험은 단위 시험과 전체적인 시험 방법 및 테스트 케이스 생성 방법이 같음.
- 차이점
  1. 단위시험 ; 소프트웨어 단위가 단위 설계 명세서와 부합한다는 것과 기능성 및 강건성을 증명
     통합시험 : 소프트웨어 아키텍처 설계에 대해 소프트웨어 단위 사이의 통합 수준과 인터페이스를 시험하기 위한 것
  2. ASIL C 등급의 결함 주입 시험(Fault injection test) 권장 사항 차이.
  3. 커버리지 지표

	Methods	ASIL			
		A	B	C	D
1a	Function coverage[a]	+	+	++	++
1b	Call coverage[b]	+	+	++	++

표 7 ISO 26262에서 명시하는 통합 시험 시, 소프트웨어 아키텍처 수준의 구조 커버리지 지표

part 6. ISO 26262의 SW 검증단계

4) Verification of software safety requirements(소프트웨어 안전 요구사항 검증)
: 소프트웨어가 소프트웨어 안전 요구사항을 충족하는지를 증명하는 절차

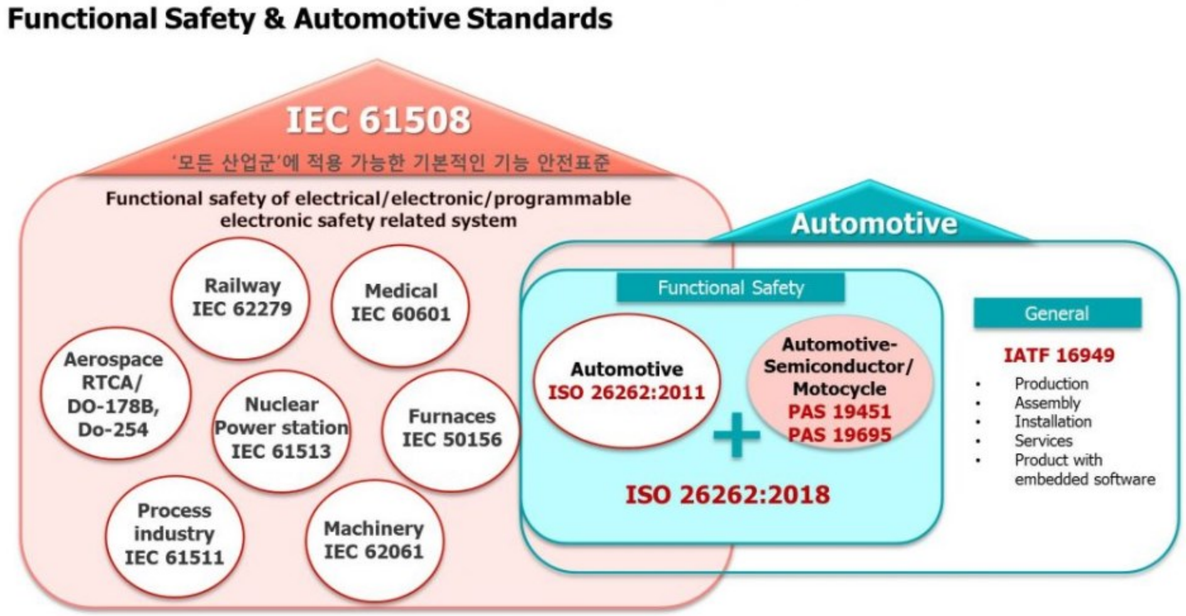
	Methods	ASIL			
		A	B	C	D
1a	Hardware-in-the-loop	+	+	++	++
1b	Electronic control unit network environments[a]	++	++	++	++
1c	Vehicles	++	++	++	++

표 8 ISO 26262에서 명시하는 소프트웨어 안전 요구사항 검증 실시를 위한 시험 환경

- 위 표에 나열된 시험 환경에서 시험을 실시해야함.
- 이미 기존에 있는 시험 케이스를 재사용하여 시험 할 수 있음.

자동차 기능 안전성과 관련된 기타 다른 표준

표준 명	개요	ISO 26262와의 차이점
ISO/PAS 19451 : 차량용 반도체 표준	ISO 26262 : 2011에서 제외된 차량용 반도체 기능 안전 설계 요구사항.	• Part 1 이 ISO 26262 : 2018 Part 11로 추가됨. • Part 2 이 ISO 26262 : 2018 Part 8에 부분적으로 추가됨
ISO/PAS 19695 : 모터사이클 기능안전성 표준	ISO 26262 : 2011에서 제외된 모터사이클 기능 안전 설계 요구사항.	• Part 1 이 ISO 26262 : 2018 Part 12로 추가됨
IATF 16949 : 자동차 품질경영시스템	기능안전 외에 자동차 산업에서는 일반적으로 가장 많이 활용되고 있는 표준	• 제품의 품질을 보장하기 위한 표준 • 자동차 산업 공급사슬 내 모든 기업의 품질시스템에 적용가능하다.



DO-178C

Software Considerations in Airborne Systems and Equipment Certification

항공 SW의 특징

기계나 하드웨어와 물리적 특성이 다르다

복잡성이 증가하여 SW결함을 중가시킨다

결함 시 심각한 사고를 초래할 수 있다

SW결함 -> SYSTEM결함-> 기능고장->사고

사전에 오류를 완벽 제거할 수 없다

안전성과 신뢰성이 엄격하게 요구되어 인증 을 거쳐야한다

항공기 탑재 급증

항공기 기체의 90%가 소프트웨어로 제어되고 있다

DO-178

(Software Considerations in Airborne Systems and Equipment Certification)

RTCA 제정, 항공안전SW를 위한 인증표준
- DO-178 : 항공 소프트웨어
- DO-254 : 항공 하드웨어

항공전자시스템에서 사용되는
안전 필수 소프트웨어의 안전성을 취급하는 지침.
기술적인 가이드이기는 하나
항공전자 소프트웨어 시스템을 개발하기 위한
사실상의 표준이다.

SW 생명주기 전체를 다루고 있다
- 계획 프로세스
- 개발 프로세스
- 인증지원 프로세스
- 검증 프로세스
- 품질보증 프로세스
- 형상관리 프로세스

1992년, FAA(미연방항공국) <권고회람 AC 20-115B>
형식증명/부가형식증명/기술표준품 과제에 대한
SW적합성을 입증하는 하나의 방법으로서 DO-178B 채택

2004년부터 DO-178B 개정작업→ DO-178C

2013년, FAA <권고회람 AC 20-115C>
DO-178C + 관련된 보충표준 전체를
항공용 SW 보증을 위한 하나의 체계로 인정

항공용 탑재 SW에 대한 적합성을 인증 받고 싶다면?

자신의 **개발방법론**에 적용되는 표준의 **목표**들을 전부 달성했다고 입증해야 한다

생명주기 프로세스에서 산출되는 **생명주기자료**
+ **보충표준**이 요구하는 **목표**의 달성을 입증한 자료

DO-178C : 구성

문서	내용
DO-178C	일반 원칙을 다루는 상위 규범
DO-330	툴에 관한 표준
DO-331	모델 기반 기법 (MB)
DO-332	객체 지향 (OO)
DO-333	포말 메소드 (FM)
DO-248C	자주 묻는 질문, 주제 관련 논의문서

DO-178C 개선사항

- 비일관적인 용어사용을 정리했다
- 모호한 묘사를 명확화
- 일반 원칙을 다루는 상위 규범에 더불어 다양한 방법론을 다루는 **보충문서**들을 제정했다

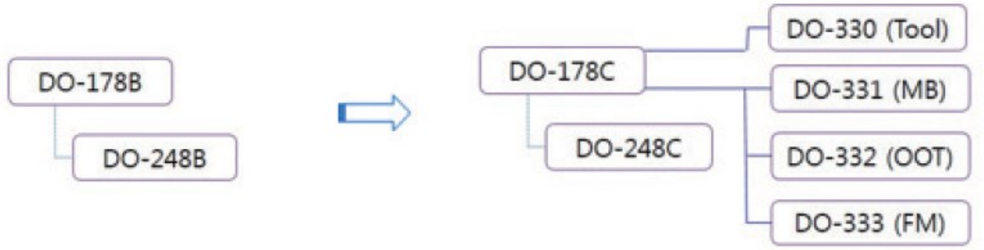
DO-178B는 별도의 보충 표준이 없었다

- 해석과 적용상의 의문이 있을 경우

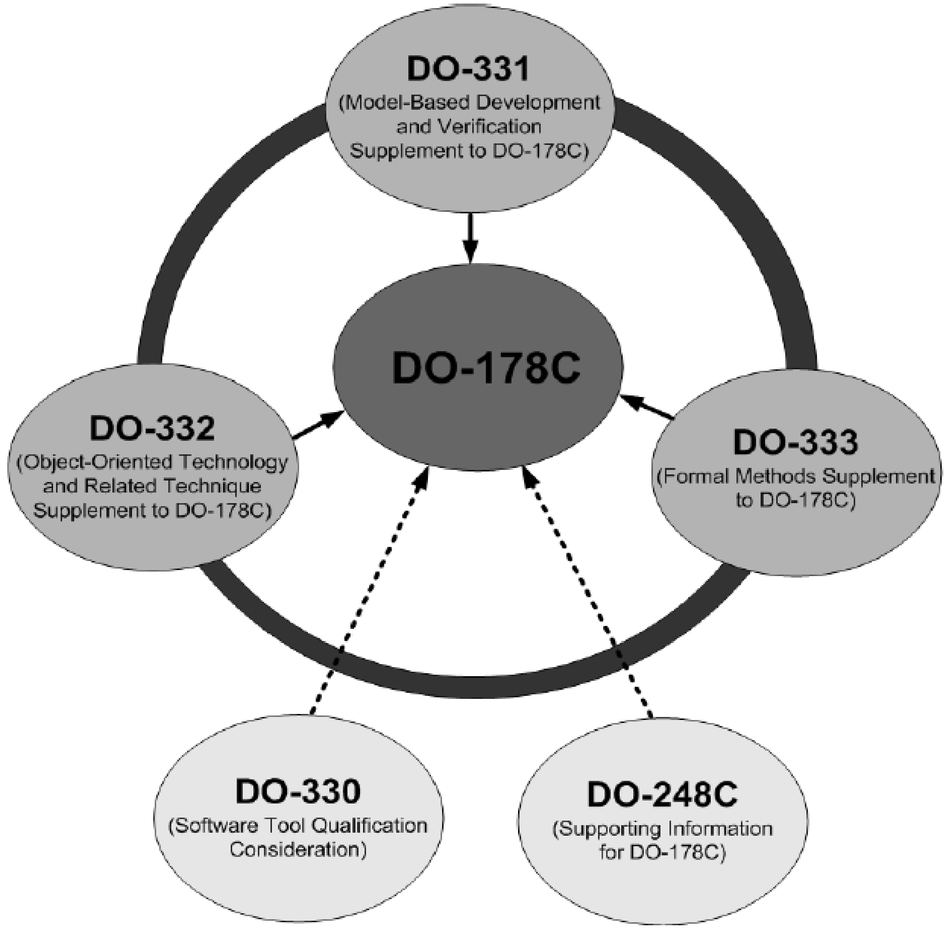
⇒개별 과제별로 Issue Paper 를 발행하여 인증당국과 협의

⇒CAST(인증당국SW팀)의 정책권고문서가 밝히는 인증당국의 입장을 적용

<DO-178C로의 개정 문서변화>



<DO-178C 문서구성>



DO-178C : 목표(Objectives)

적합성인증 신청자는 SW 적합성을 입증하기 위해
- **SW 레벨**에 의해 요구되는 모든 **목표**의 달성을 증명하는 **수명주기 자료**와
- (**보충 표준**이 **다루는 기법**을 적용했을 시) 보충표준이 요구하는 **목표**의 달성을 입증하는 자료를 제출하여야 한다

DO-178C의 철학
- **목표** 기반의 보증
- 기술과 **독립**적인 목표를 통한 보증

RTCA는 개발자가 DO-178C를 전부 이해하고 실제 개발에 적용할 문서로 활용하길 원함
- 부속서 A에서
- **목표** & 목표를 위해 수반되는 **활동**을 하이퍼링크로 제공

Table A-1 Software Planning Process

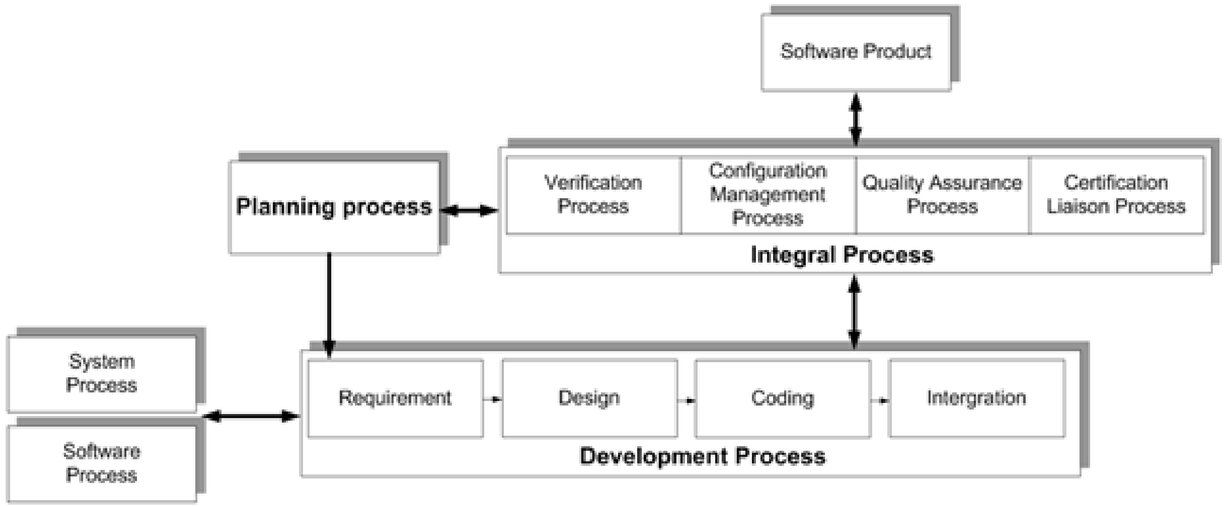
	Objective		Activity	Applicability by Software Level				Output		Control Category by Software Level			
	Description	Ref	Ref	A	B	C	D	Data Item	Ref	A	B	C	D
1	The activities of the software life cycle processes are defined.	4.1.a	4.2.a 4.2.c 4.2.d 4.2.e 4.2.g 4.2.i 4.2.l 4.3.c	O	O	O	O	PSAC SDP SVP SCM Plan SQA Plan	11.1 11.2 11.3 11.4 11.5	① ① ① ① ①	① ① ① ① ①	① ② ② ② ②	① ② ② ② ②
2	The software life cycle(s), including the inter-relationships between the processes, their sequencing, feedback mechanisms, and transition criteria, is defined.	4.1.b	4.2i 4.3.b	O	O	O		PSAC SDP SVP SCM Plan SQA Plan	11.1 11.2 11.3 11.4 11.5	① ① ① ① ①	① ① ① ① ①	① ② ② ② ②	

DO-178C : SW 생명주기 프로세스

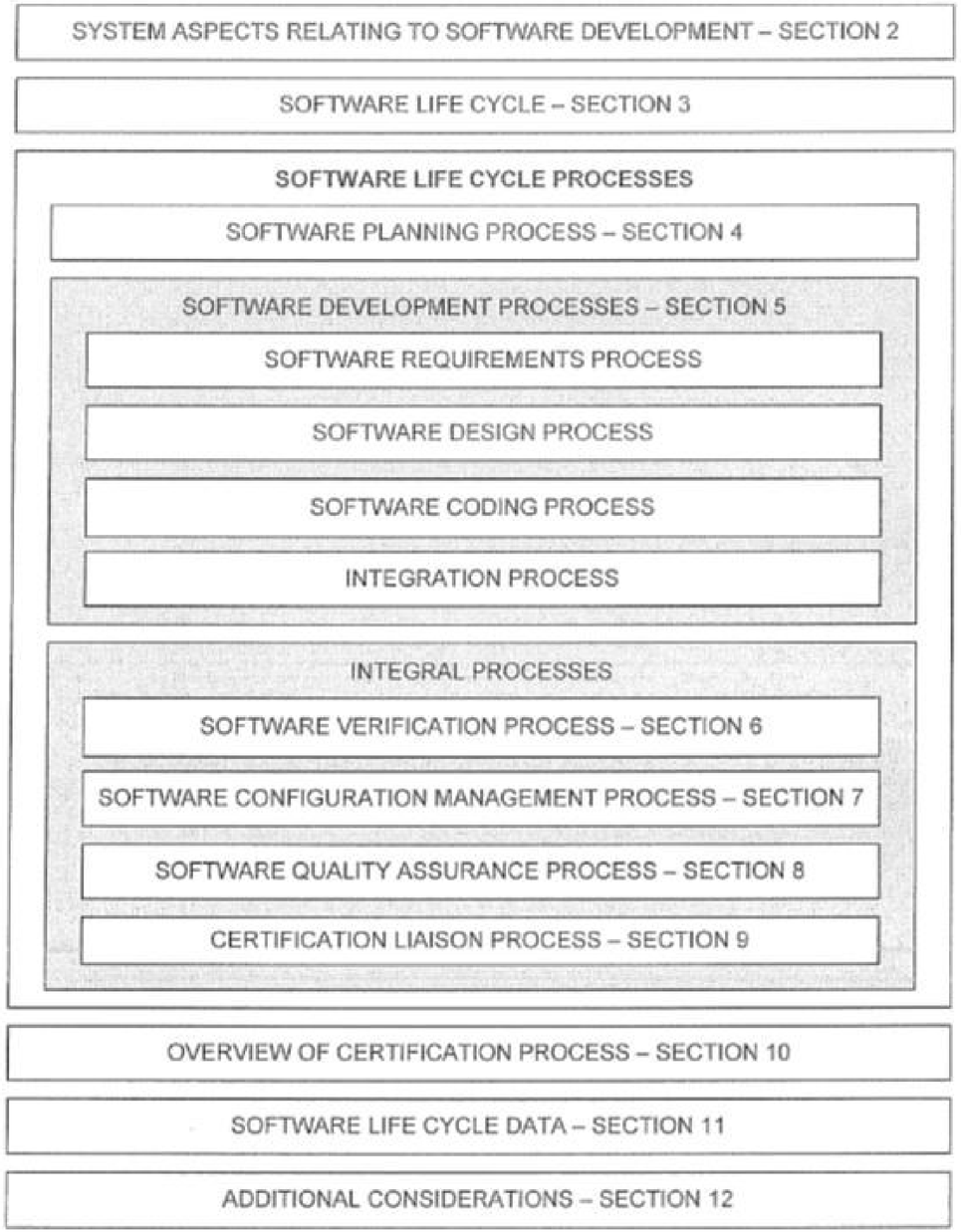
큰 틀의 SW 생명주기 프로세스 3가지
- 계획/개발/통합 프로세스

SW 생명주기 프로세스
- 소프트웨어의 탄생부터 죽음에 이르는 **생명주기**동안 진행하는 모든 활동
- 생명주기 프로세스를 거치면 소프트웨어 **생명주기 데이터**가 생성

생명주기 데이터는 인증 교섭 프로세스를 지원하기 위해 활용



<DO-178C 문서의 챕터>



DO-178C : SW 생명주기 프로세스 (1) 계획 프로세스

산출하는 생명주기 데이터

소프트웨어 인증 양상 계획
(Plan for Software Aspects of Certification; PSAC)
- 인증 고려사항, 소프트웨어
- 생명 주기 및 데이터, 인증을 위한 검사 일정,
- 등을 정의한다

소프트웨어 개발 계획
(Software Development Plan; SDP)
- 소프트웨어 개발 프로세스와 활동과
- 생명주기를 제시한다.
- 요구사항, 설계 그리고 코드에 대한 소프트웨어 표준
- 소프트웨어 개발 환경 등을 정의한다

소프트웨어 검증 계획
(Software Verification Plan; SVP)
- 조직의 책임, 소프트웨어 생명 주기와의 인터페이스,
- 독립된 검증 방법, 장비 설명과 시험/분석 도구의 활용 등을 정의한다.

소프트웨어 품질 보증 계획
(Software Quality Assurance Plan; SQA)
- SQA 환경, SQA 기관과 책임, 문제 보고, 추적, 보정 등의 활동에 관련된 생명 주기 전반에 걸친 SQA 활동과
- 활동 시점에 대해 정의한다.

소프트웨어 형상 관리 계획
(Software Configuration Management Plan; SCM)
- 절차, 도구, 표준, 책임, 형상 식별자, 기준선, 추적 가능성, 문제 보고, 변경 통제, 변경 검토, 형상 상태 등을 정의한다
- SCM에서는 각 소프트웨어 생명주기 데이터 항목에 대한 통제 카테고리 (Control Category; **CC**)를 결정한다

소프트웨어 요구사항

설계 및 코드 표준

소프트웨어 검증결과

DO-178C : SW 생명주기 프로세스 (2) 개발 프로세스

산출하는 생명주기 데이터

프로세스	입력	출력
요구사항	- 시스템 요구사항 - 시스템 안전성 요건 - 시스템 정의서	**상위수준 요구사항**
설계	- 고수준 요구사항	**하위수준 요구사항** **소프트웨어 구조 명세**
코딩	- 저수준 요구사항	**소스 코드**
통합	- 소스코드 - Compiling/Linking/Loading 데이터	**Executable Object Code** **매개변수 데이터 항목**
추적성	- 시스템 요구사항 - 고/저수준 요구사항 - 소스 코드	**추적 데이터**

<소프트웨어개발 하위 프로세스의 입출력>

매개변수 데이터 항목(Parameter Data Item)

매개변수는 실행 시 참조가 되어 SW의 Beahavior에 영향을 주기 때문에 별도의 형상항목으로 관리하도록 함

추적 데이터(Trace Data)

추적성 데이터는 추적성을 입증하는 생명주기자료임.
DO-178C는
1) 시스템 요구사항 ↔ 상위수준 요구사항 ↔ 하위수준 요구사항 ↔ 소스코드
2) 소프트웨어 요구사항 ↔ 테스트 케이스
3) 테스트 케이스 ↔ 시험절차
4) 시험절차 ↔ 시험결과 간 양방향 추적성을 요구
이를 통해서 불용코드와 미아코드가 존재하지 않음을 입증해야 함.

DO-178C : SW 생명주기 프로세스 (3) 통합 프로세스

인증교섭 프로세스
(Certification Liaison Process; CLP)

신청자와 인증기관 사이의 소통과 이해를 수립하여 인증프로세스 지원
생명주기 데이터 & 인증당국으로부터의 검토사항을 활용함

- 소프트웨어 성과 요약 (Software Accomplishment Summary; **SAS**)
- PSAC
- 소프트웨어 형상항목 (Software Configuration Index; **SCI**)을 생성
- PSAC은 소프트웨어 생명주기 이전에 인증당국에 제출되어 검토받음
- 검토사항을 반영하여 SAS와 SCI를 제출함

소프트웨어 품질 보증
(Software Quality Assurance; SQA)

각 소프트웨어 생명주기 프로세스와 산출된 데이터를 평가함

- 각 요건들이 요구사항에 만족되는가?
- 결함이 검출/평가/추적/해결 되는가?
- 각 생명주기 데이터가 인증 요구사항을 따르는가?

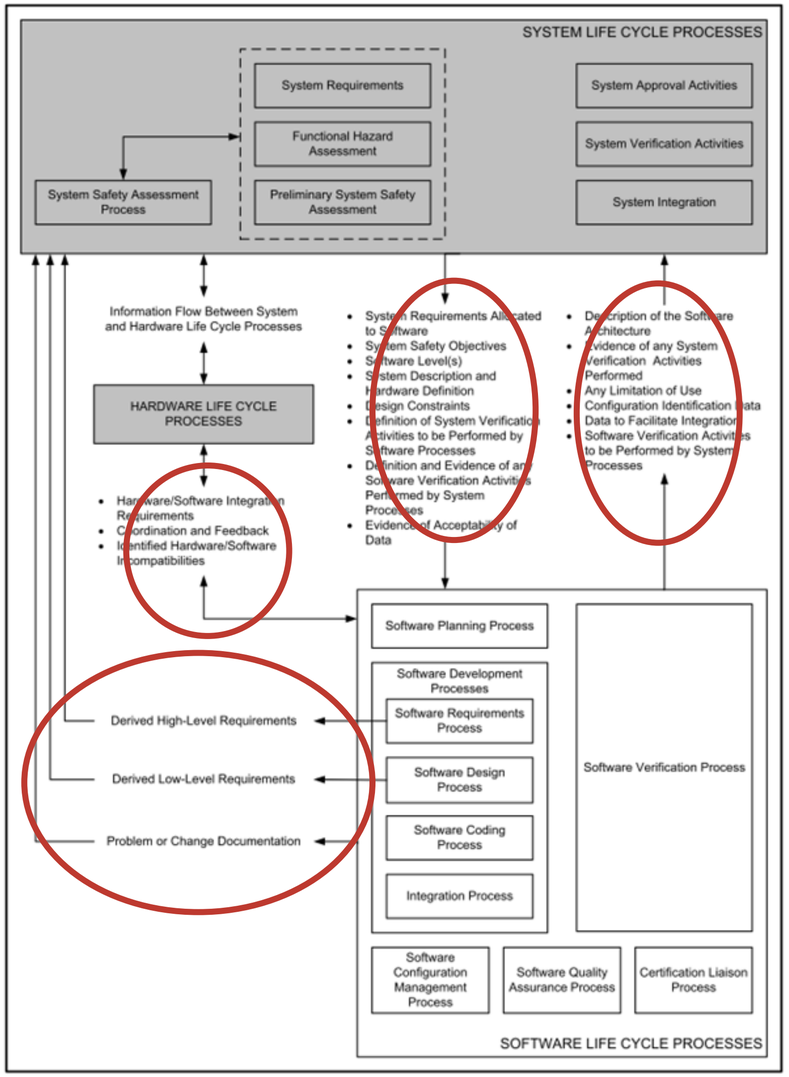
소프트웨어 검증 프로세스
(Software Verification Process; SVP)

- 소프트웨어 개발 과정에서 나타날 수 있는 오류를 찾고 보고하는 활동
- 크게 Review, Analysis, Test으로 나뉨
- 소프트웨어 검증 사례(case)와 절차
- 소프트웨어 검증 결과, 문제 보고, 추적 데이터를 산출

소프트웨어 형상관리 프로세스
(Software Configuration Management Process; SCMP)

- 결함보고 및 변경과 관련된 활동을 정의하고 통제하는 프로세스
- **SCM**에서 할당된 **CC**에 따라 각 형상 항목들을 관리함

DO-178C : 시스템 생명주기 프로세스 / SW 생명주기 프로세스 / HW 생명주기 프로세스 간 메시지



Section2 <소프트웨어 개발과 관련된 시스템 측면>
2절 <시스템 및 소프트웨어 생명주기 프로세스 간의 정보흐름>

DO-178C에서 시스템이란
하드웨어와 소프트웨어의 총합을 의미
시스템, 소프트웨어, 하드웨어 생명주기 프로세스 사이에는 정보 흐름이 있음

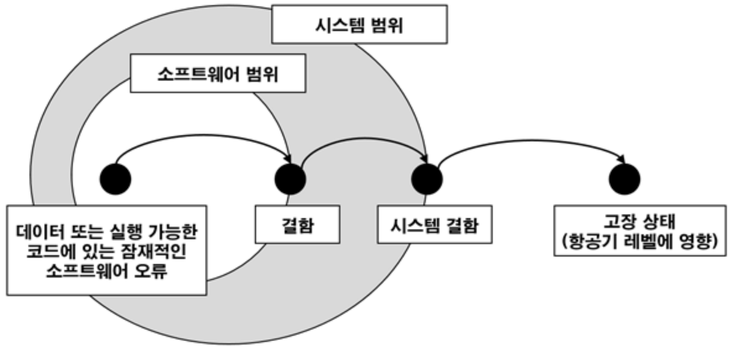
DO-178C는
시스템, 하드웨어, 소프트웨어 생명주기 프로세스의 연관성을 강화함
- 시스템과 소프트웨어 간 교환 자료 추가
- 시스템 안전성 평가로의 파생 요구 조건 제공
- 하드웨어와의 연계성 강화

시스템 요구사항과 이를 할당 받은 소프트웨어/하드웨어 프로세스는
- 요구사항을 충족해 나가는 과정에서
- 요구사항에 대한 적정성과 안정성에 대해 개발과 검증과정을 반복 수행.

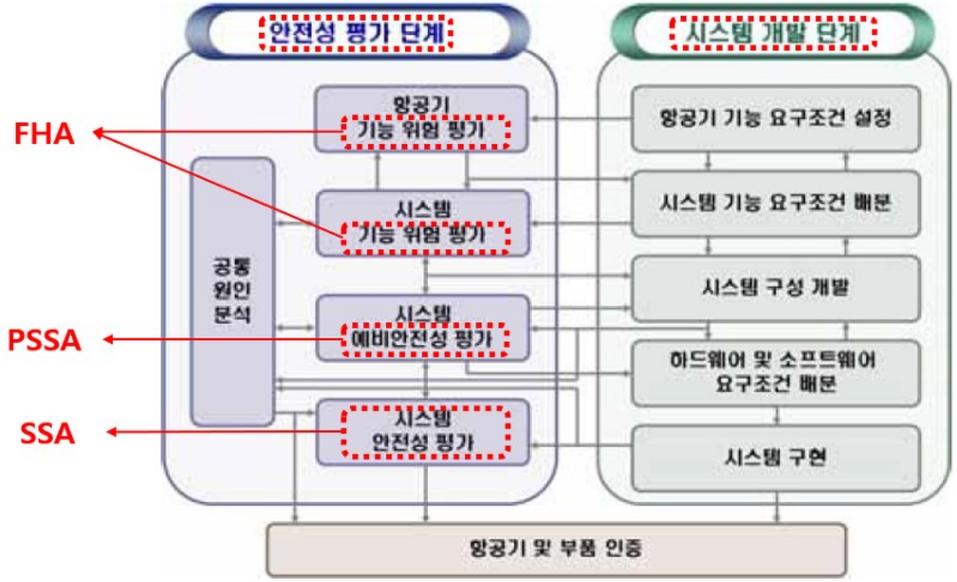
프로세스 간에 반복적으로 정보의 교환과 적용으로
각 프로세스의 생명주기가 결정됨 => 하나의 안정적인 시스템으로 통합

DO-178C : 시스템 안전성 평가 프로세스 & 소프트웨어 레벨

SW에러 → 항공기 고장



ARP-4754/4761 시스템 안전성 평가 프로세스



<그림 4> 시스템 개발 단계별 안전성 평가

시스템 안전성 평가(SSA) 프로세스는
- **FHA**, **PSSA**에서 수행한 고장조건의 원인&영향력 분석을 토대로

기능ID	기능	단계	고장 조건	고장 영향	분류
36-401.1	휠 제동	착륙, RTO	모든 휠 제동 상실	활주로에 있는 항공기를 멈추게 하는 승무원의 능력이 크게 감소됨	Hazardous
36-401.2	자동 제동	착륙, RTO	자동 제동의 탐지되지 않은 상실	승무원은 항공기를 멈추기 위한 수동 절차를 사용해야 함	Major

소프트웨어 고장이 발생했을 시의 영향력을 분석하여
5가지의 **소프트웨어 레벨** 중 하나를 결정한다

DO-178C : 소프트웨어 레벨 & 목표/독립성

레벨	설명	고장상태	예시	**목표/독립성**
Level A	항공기에 치명적인 고장이 발생할 수 있습니다.	**Catastrophic**	항공기의 비행 및 조종 시스템	**71/30**
Level B	항공기에 위험한 고장이 발생할 수 있습니다.	**Hazardous**	연료 관리 장치	**69/18**
Level C	항공기에 주요 고장이 발생할 수 있습니다.	**Major**	조종사와 항공 교통관제 장치의 통신	**62/5**
Level D	항공기에 경미한 고장이 발생할 수 있습니다.	**Minor**	비행 데이터 기록계	**26/2**
Level E	항공기 운영 능력이나 파일럿 작업에 영향을 미치지 않고 시스템 기능의 고장이 발생합니다.	**No Safety Effect**	엔터테인먼트 시스템	**0**

독립성을 요구하는 목표

- 산출자와 산출물을 검증하는 사람이 명확히 분리될 것을 요구

치명도 Level E인 소프트웨어

- DO-178C의 생명주기 프로세스를 따르지 않는다

DO-178C : 보충문서

DO-330 : Software Tool Qualification Consideration Consideration

소프트웨어 툴

- [
-

툴 사용시 주의점

표 3. 소프트웨어 등급 및 분류에 따른 툴 검정 등급 표

소프트웨어 등급 (Software Level)	분류(Criterion)		
	1	2	3
Level A	TQL – 1	TQL – 4	TQL – 5
Level B	TQL – 2	TQL – 4	TQL – 5
Level C	TQL – 3	TQL – 5	TQL – 5
Level D	TQL – 4	TQL – 5	TQL – 5

유입

해가능

툴 검증과 관련한 DO-330 지침을 제정

- 검증된 툴만 사용하도록 요구
- 툴을 3가지 Criterion으로 나누고 5가지 Level(TQL)로 분류
- SW레벨과 Criterion에 따라 TQL이 달라지며 달성해야 할 목표도 달라진다

DO-331 : Model-Based Development and Verification

모델기반 설계 시 해야할 일들

- 모델 시뮬레이션이 허용되는 15개 목표를 알아야 함
- 테스트 케이스에 대해 검증 하여야 함 (MB.A-4의 목표 8, 9, 10)
- 검증 절차에 대해 검증 하여야 함 (MB.A-4의 목표 14, 15, 16)
- 결과의 정확성을 따져야 함 (MB.A-7의 목표 10, 11, 12)

인증당국과 합의되지 않은 사항들이 있음

- 명세 모델과 설계 모델에 대한 엄격한 분리
- 모델의 일관성과 유지보수성
- 시뮬레이터에 대한 **크레디트** 부여 가능성
- 자동 코드 테스팅의 인정 여부

DO-178C : 보충문서

DO-332 : Object-Oriented Technology and Related Technique Supplement to DO-178C

항공SW와 객체지향

- 항공 분야는 다른 산업분야보다
  소프트웨어 결정성을 강하게 요구하는 바
  객체지향이 일반적으로 사용되지 않는다고 함

계획/개발/검증 단계에서 추가적인 활동을 요구

⇒ 가상화 사용시 계획서에 반영하기
⇒ 컴포넌트 재사용시 어떻게 개발 과정에서 통합 것인 지에 대하여 설명하기
  타입 일치, 요구조건 매핑, 예외 처리 전략 등)
⇒ 취약성 분석을 어떻게 충족할 것인지 밝히기

DO-333 : Formal Methods Supplement to DO-178C

정형기법

- 시스템 행동을 수학적인 모델로 구성하고,
  개발하고, 검증하는 노테이션과 해석법.

- 안전관련 기능 및 속성에 대한 시스템 설계와 구현
  을 정형적인 방법으로 검증하는 것

장단점

- 수학적으로 정의되어 모호성이 없다는 특징
- 정형모델에 의한 정형분석은 요구조건과, 수명주기의 정
  확성을 강력하게 검증함
- 전문가, 지침, 툴 부족 상태
- 필요 수준 이상의 신뢰성 제공 가능성

⇒ 일부 분야 국한되어 사용

주요 항공 표준들

국가 or 기관	감항성	소프트웨어	하드웨어	지상시설
FAA	FAR	DO-178	DO-254	DO-278
유럽 EASA/JAA/CAA	JAR, CS	ED-12	ED-80	ED-109
미군	MIL-HDBK-516	MIL-STD-882 MIL-STD-498	-	-
ICAO	Annex 8(감항성), 19(항공안전관리)	-	-	-
우리나라	KAS(항공기기술기준)	-	-	-
NATO	STANAG 4671	-	-	-
NASA	-	NPD 1000.0 (거버넌스 모델) →NPR 7150.2 (소프트웨어 공학 요구사항) →NPR-STD-8719.13 (소프트웨어 안전)	-	-

<우리나라가 채택한 군용항공기 감항인증기술기준>

- 표준감항인증기준(MIL-HDBK-516) : FA-50, T-50i
- FAR Part 23 : KT-1B(인도네시아), KT-1T(터키)
- FAR Part 29 : KUH, KUH-1P(경찰청)
- STANAG 4671 : MUAV, 사단급, 군단급 UAV
- KAS Part 33. KUH
- KAS Part 36. KUH

기능안전 관련 국내 법규
및 인증기관

기능안전성 관련 국내 법규

Automotive

〈출처 : 국토해양부〉

기능안전성 관련 국내 법규

Automotive

제29조(자동차의 구조 및 장치 등) ① 자동차는 대통령령으로 정하는 구조 및 장치가 안전 운행에 필요한 성능과 기준(이하 "자동차안전기준"이라 한다)에 적합하지 아니하면 운행하지 못한다.

② 자동차에 장착되거나 사용되는 부품 · 장치 또는 보호장구(保護裝具)로서 대통령령으로 정하는 부품 · 장치 또는 보호장구(이하 "자동차부품"이라 한다)는 안전운행에 필요한 성능과 기준(이하 "부품안전기준"이라 한다)에 적합하여야 한다.

③ 국토교통부령으로 정하는 캠핑용자동차 안에 취사 및 야영을 목적으로 설치하는 액화석유가스의 저장시설, 가스설비, 배관시설 및 그 밖의 사용시설은 「액화석유가스의 안전관리 및 사업법」에 적합하여야 하며, 전기설비 및 캠핑설비는 국토교통부령으로 정하는 안전기준에 적합하여야 한다. <신설 2015. 8. 11., 2019. 8. 27.>

④ 자동차안전기준과 부품안전기준은 국토교통부령으로 정한다. <개정 2013. 3. 23., 2015. 8. 11.>

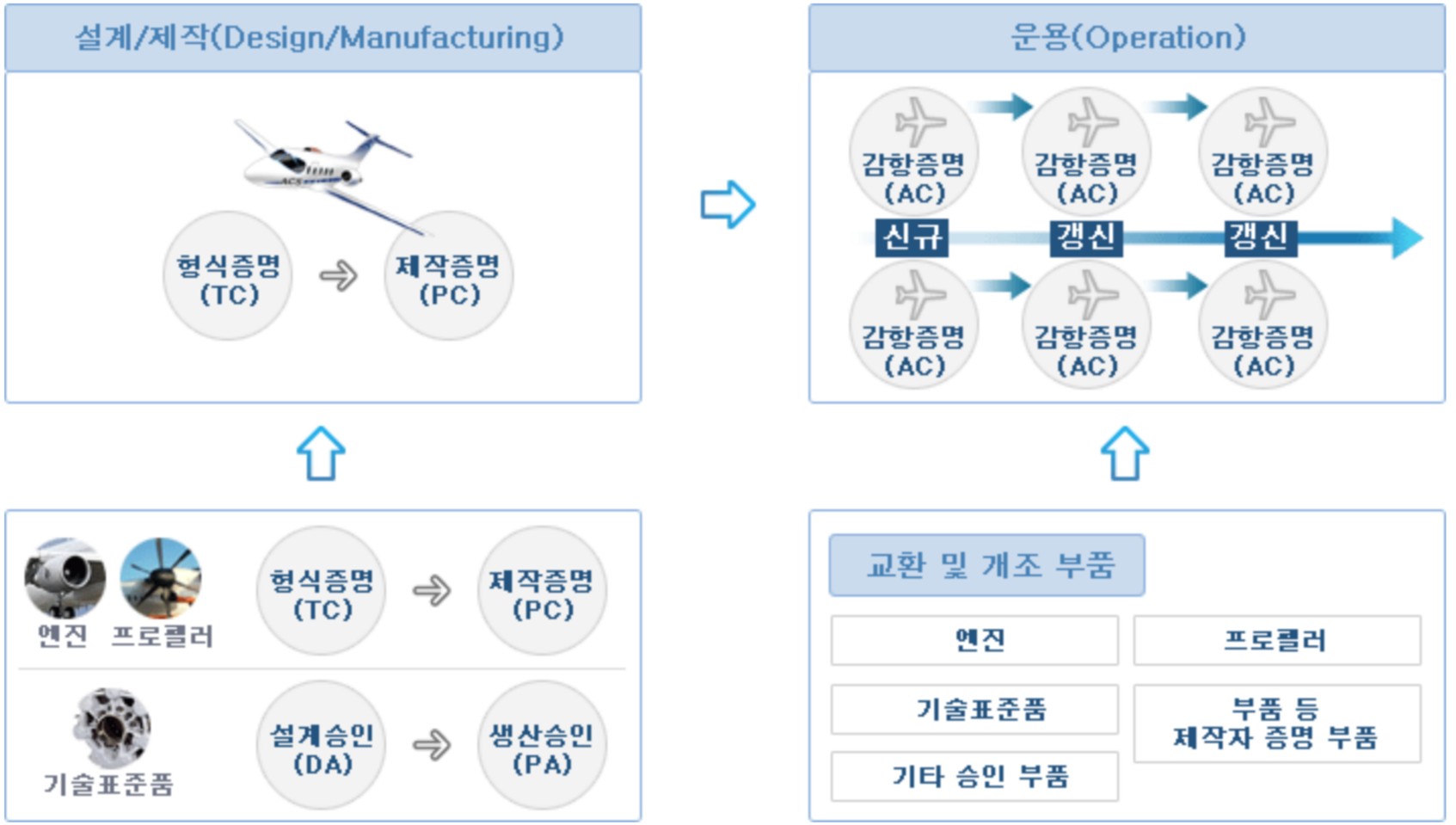
[전문개정 2009. 2. 6.]

자동차 안전기준에 관한 규칙 (http://www.law.go.kr/lsEfInfoP.do?lsiSeq=137717#)

자동차 및 자동차부품의 성능과 기준에 관한 규칙 (http://www.law.go.kr/법령/자동차및자동차부품의성능과기준에관한규칙)

기능안전성 관련 국내 법규

항공



기능안전성 관련 국내 법규

항공(민간)

감항증명 -> 항공기 기술기준

제15조(감항증명)

⑤ 국토교통부장관은 제3항 각 호에 따른 감항증명을 할 때에는 항공기가 제17조제2항에 따른 기술기준에 적합한지를 검사한 후 그 항공기의 운용한계(運用限界)를 지정하여야 한다. 이 경우 다음 각 호의 어느 하나에 해당하는 항공기의 경우에는 국토교통부령으로 정하는 바에 따라 검사의 일부를 생략할 수 있다. <개정 2012. 1. 26., 2013. 3. 23.>

제1조(목적) 이 규정은 항공법 제15조제5항에 의한 항행의 안전을 확보하기 위한 기술상의 기준(이하 "기술기준"이라 한다)에 관한 기술자료의 검토, 기술기준 및 특수기술기준의 제·개정 관리절차를 규정함으로서 최신 기술기준을 유지하는 것을 그 목적으로 한다.

제5조(기본방침) ①국토해양부장관은 기술기준(KAS)이 국제민간항공기구(ICAO)에서 발행하는 부속서 8(Airworthiness of Aircraft) 및 부속서 16(Environmental Protection)의 '표준 및 권고안' (SARPs) 요건에 적합하도록 유지·관리한다.

②국토해양부장관은 기본적으로 미국연방항공청(FAA)의 감항기준과 동등성을 유지하도록 하며, 유럽항공안전당국(EASA)의 인증규격(Certification Specification) 등을 참고하여 보완할 수 있다.

기능안전성 관련 국내 법규

항공(군용)

감항인증 -> 표준감항인증기

제3조(표준감항인증기준의 고시) ① 방위사업청장은 군용항공기 사업 계획의 수립 및 사업추진 단계별로 군용항공기의 비행안전성을 확보하기 위하여 사업관리기관의 장이 군용항공기 사업을 추진하는 경우에 일반적으로 지켜야 할 기술기준 등(이하 "표준감항인증기준"이라 한다)을 정하여 고시하여야 한다. <개정 2012. 12. 18.>

② 표준감항인증기준의 작성 및 변경 절차 등에 필요한 사항은 국방부령으로 정한다.

군용기 표준감항인증기준에 관한 고시 - 일부발췌

참고문서(References)

JSSG-2008 Appendix A: 3.1.7 - 3.1.12 System Architecture, Unique Function Integration, Failure Immunity and Safety, Failure Transients, Integration Management, Redundancy; 3.3.1 Processing Architecture

MIL-STD-882: Task 203 of MIL-STD-882 E (see also MIL-STD-882D: A.4.3.1; A.4.3.2 Safety Performance Requirements; A.4.3.3 Safety Design Requirements)

DoD JSSSEH: 4.3.5 addresses defining safety requirements for software systems

USAF Weapon Systems Software Management Guidebook: G.2.1; G.2.2; G.2.3

NASA-STD-8719.13B: 4.4.2 software safety requirements designated; 6.2.2.2.f

RTCA DO-178: 2.1 of RTCA DO-178C addresses how system design drives safety related requirements that flow to software (see also RTCA DO-178B: 2.1.1)

SAE ARP4754A: 4.1.6

FAA AC 20-115C: provides guidance on the use of RTCA DO-178C, RTCA DO-330, RTCA DO-331, RTCA DO-332, RTCA DO-333 (NOTE: FAA AC 20-115B was the companion guidance issued with RTCA DO-178B)

DOT/FAA/AR-07/48: A.6

전문

http://www.law.go.kr/LSW//conAdmrulByLsPop.do?&lsiSeq=208446&joNo=0003&joBrNo=00&datClsCd=010102&dguBun=DEG&lnkText=%25EA%25B3%25A0%25EC%258B%259C%25ED%2595%2598%25EC%2597%25AC%25EC%2595%25BC%2520%25ED%2595%259C%25EB%258B%25A4&admRulPttninfSeq=5243

인증 기관

인증기관 vs. 교육 및 컨설팅 기관

교육 및 컨설팅 기관

- 해당 기업의 시스템을 구축하는데 필요한 구체적인 방법 등을 제시하는 기관

인증기관

- 구축된 시스템이 해당 요구사항에 적합한지 아닌지를 평가하는 기관

인증 기관

ISO 26262 관련 인증기관과 교육 및 컨설팅 기관

인증기관

- TUV SUD

교육 및 컨설팅 기관

- 솔루션 링크
- 브이웨이
- KTL
- 슈어소프트
- 한컴 MDS etc.

인증 기관

DO-178C 관련 인증기관과 교육 및 컨설팅 기관

- FAA 에서 ODA(Organization Designation Authorization)시스템으로 위임업체들이 인증을 진행
  https://www.faa.gov/other_visit/aviation_industry/designees_delegations/designee_types/media/ODADirectory.pdf *(위임업체)*
- 항공기의 감항인증은 각 나라마다 별도 수행

인증기관(DO-178C)

-

인증기관(감항)

- 국토교통부, 방위사업청
- 국제민간항공기구 (ICAO)
- 유럽항공안전청 (EASA)

교육 및 컨설팅 기관

- 모아소프트
- 한컴 MDS etc.