기능안전성 표준 및 관련 법/규정과 현황

※ Contents

1. 기능안전성 표준 및 ISO 26262, DO-178C의 개요와 세부
2. 항공/자동차 분야의 기능안전성 관련 기타 표준
3. 기능안전성 관련 국내 법/규정
4. 국내외 인증 기관 및 인증 방법과 현황

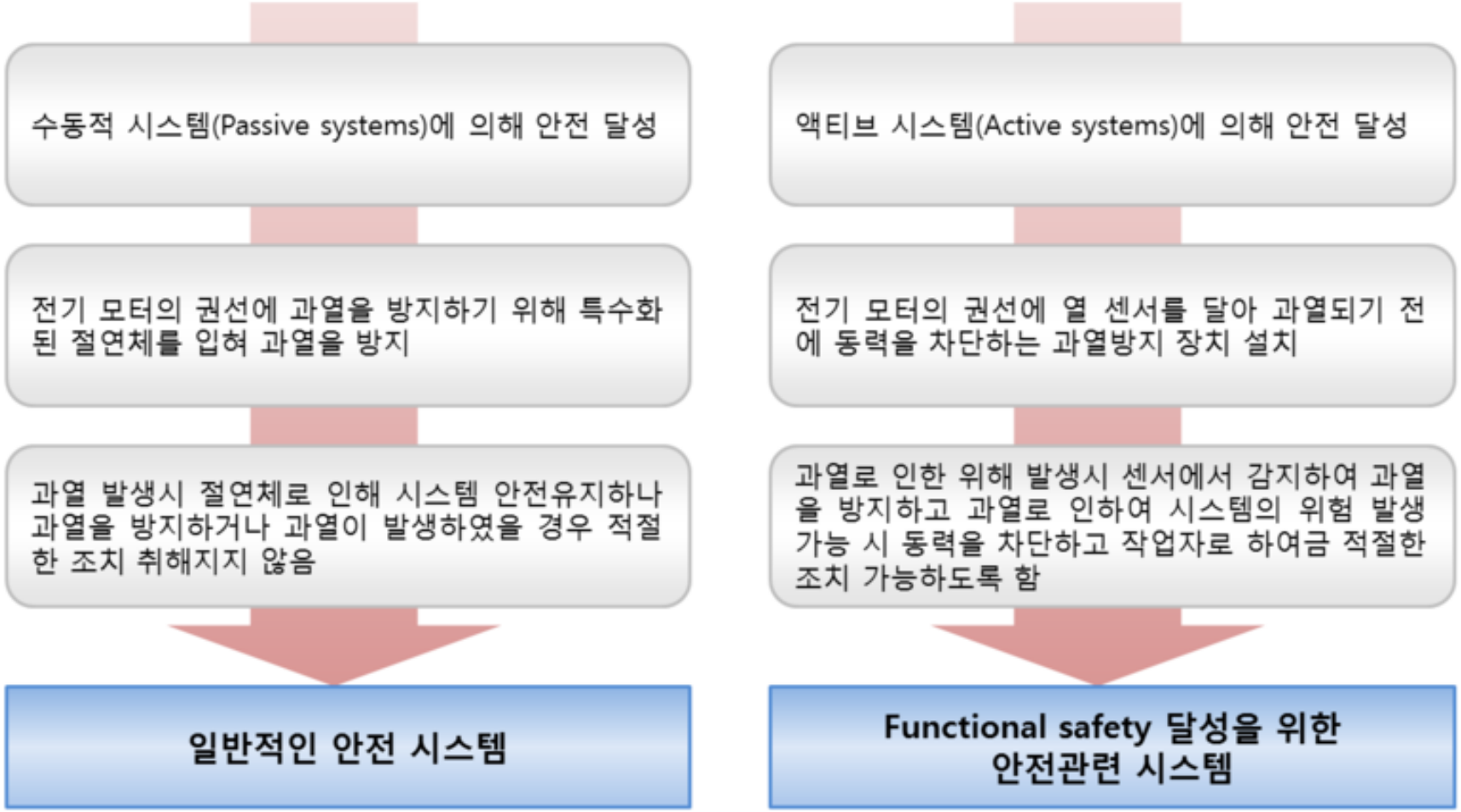
Team #1
201411273 박재범
201411295 이상훈
201510436 허윤아
201511244 김민우

DEPENDABLE SOFTWARE LABORATORY

1. 기능안전성 표준 및 ISO 26262, DO-178C의 개요와 세부

1. 기능안전(Functional safety)이란?

- 기능안전이란 **안전에 대한 진화된 개념**으로 IEC 61508(범용 기능안전) 국제표준에서 등장한 용어.
- 기능안전은 시스템이나 장비의 총체적 안전의 일환으로 하드웨어 고장, 소프트웨어 오류, 운영자 오류 그리고 환경적인 영향 등에 대한 안전 관리(management of safety)를 의미함.



※ 기능안전 =
기존 안전 평가 방법 보다
더 높은 수준의
안전 평가 방법

※ IEC 61508 =
전기, 전자, 또는
프로그램이 가능한 전자
(E/E/PE: Electric, Electronic or Programmable Elecronic)
시스템 및 제품의
전체 수명주기를 아우르는
포괄적인 기능안전 규격

2. IEC 61508에 대하여

HW와 SW가 융합된 시스템이 점점 많아지고 복잡해짐 -> 고도의 안전 평가 시스템 표준을 만듦(ISO, 1998)
IEC 61508에서는 **안전 수명 주기, 하드웨어, 소프트웨어** 세 가지에 대한 안전성 구현 및 검증 방법을 제시함.
안전 수명 주기에 따라 위험 분석 및 평가(위험 평가), 안전 무결성 수준(SIL: Safety Integrity Level)을 설정하고,
하드웨어와 소프트웨어를 목표 수준에 충족하도록 구현하며 설치, 운영, 유지보수, 변경, 폐기까지 관리해야 함.

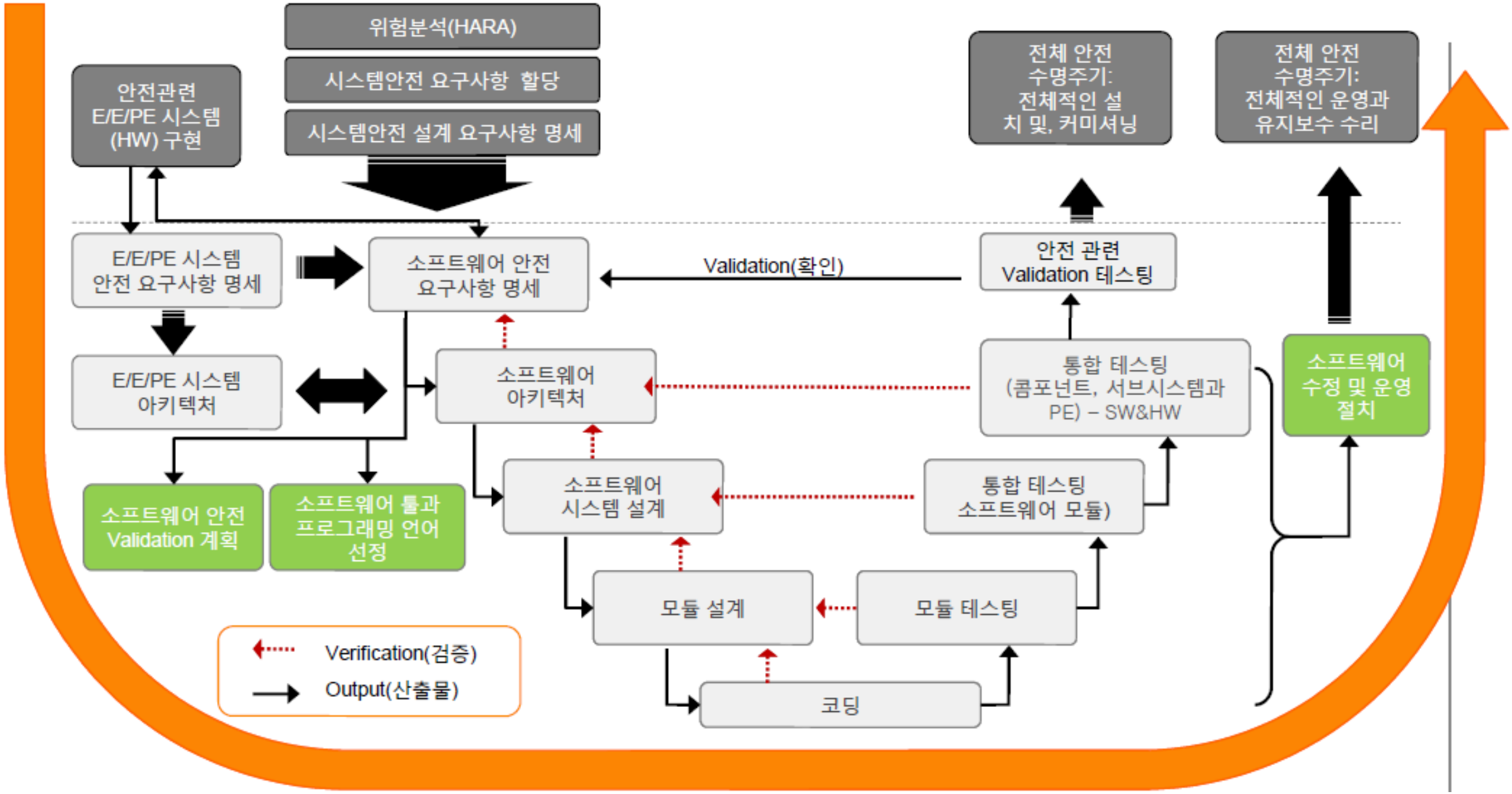
1. 안전 수명 주기
위험 평가, 안전 무결성 수준(SIL)을 만족하도록 설계하기 위해 필요한 것으로, 위해 요인 분석을 통해
위험 감소 대상을 식별하고 식별된 위험을 감소시키기 위해 어떤 활동을 해야 하는지 다루고 있음.

2. 하드웨어
IEC 61508에는 기능 안전이 구현된 하드웨어에 대한 요구사항 등이 정의되어 있음.
요구사항에 따라 하드웨어를 설계하고 구현하는 것과, 이에 대한 계획, 검증, 구조적 제한, 결함 탐지 능력,
시험 및 수정 시 영향 분석 등이 정의됨.

3. 소프트웨어
IEC 61508에는 또한 소프트웨어를 설계하는데 요구되는 활동 및 설계기술의 요구사항 등도 정의되어 있음.
소프트웨어의 경우 결합되는 하드웨어와 시스템에 대해 허용 가능한 고장률을 결정하고 이를 바탕으로
목표 안전 무결성 수준(SIL)을 설정한 뒤 알맞은 단계별 요구사항을 따르도록 함.

▶ **이 IEC 61508를 기반으로 각 세부 분야(자동차, 항공, 의료, 원자력 등)별 특성에 맞는 표준들이 만들어짐.
또한, 국가별 상황에 맞게 국제 표준을 일부 개정하여 사용하기도 함, 우리나라는 KS(국가기술표준원) 담당**

참고) V-Model 형태의 IEC 61508 소프트웨어 안전 수명 주기



3. ISO 26262란?

- **자동차(Automotive)**의 안전을 확보하기 위한 전기전자부품 및 시스템 개발절차에 대한 국제 규격.
- ISO에서 제정하였으며, 자동차에 특화된 총 **12개의 Part**로 나뉜 요구사항 및 권고사항으로 구성됨.
- IEC 61508에서 자동차의 특수성을 반영하지 못하는 부분을 보완하기 위해 따로 만들어진 표준.

< ISO 26262의 배경>

기능안전의 등장

- 전자제어시스템(ECU) 개수 및 역할 증대
- 네트워크로 연결/상호작용
- ADAS (첨단운전자시스템)

ISO 61508 한계 보완

- 공급자 중심의 제품안전성
- 전기전자 장치 안전에 관한 포괄적 규격

< ISO 26262 의 주요내용>

- 자동차에 특화된 Lifecycle 반영
  - 초기-생산-폐기에 걸친 안전 관련 요구사항
- 소비자 관점의 안전성 증점
  - 재난노출가능성, 차량 통제 가능성 등 고려
- 자동차에 적합한 위해도 평가지표
  - **IEC** 61508의 SIL 보완 -> ASIL 등급 (A~D)

※ ISO 26262의 국내 적용 대상(KS R ISO 26262)
하나 이상의 전기 및/또는 전자 (E/E) 시스템을 포함하면서, 모페드(모터 달린 자전거)를 제외한 양산 도로 차량에 설치된 안전관련 시스템.

▶ ISO 26262는 자율주행차가 등장함에 따라 필요성이 더욱 증대되고 있음.

3. ISO 26262 개정 2판(2018) / 12개의 Part

Part	Topic	Argument
26262-01	용어	-
26262-02	기능안전 관리	모든 회사
26262-03	단계적 개념	OEM & Tier 1
26262-04	양산 개발: 시스템 레벨	OEM & Tier 1
26262-05	양산 개발: HW 레벨	Tier 1 & Tier 2
26262-06	양산 개발: SW 레벨	Tier 1 & Tier 2
26262-07	생산 & 작동 & 폐기	OEM & Tier 1 & Tier 2
26262-08	지원 프로세스	모든 회사
26262-09	ASIL 및 안전 분석	모든 회사
26262-10	ISO 26262 가이드 라인	참고용 (Informative)
26262-11	반도체 응용 가이드 라인	참고용 (Informative)
26262-12	Motorcycles에 대한 적용	-

3. ISO 26262 개정 2판(2018) / ASIL(Automotive SIL) 설정

다음 3가지 기준으로 위험 평가를 진행하고, 그 총점을 바탕으로 **ASIL(A~D)**을 설정
1. 노출성(Exposure)
2. 피해 정도(Severity)
3. 조작 가능성(Controllability)

※ Severity 기준

AIS 등급	상해 수준	
0	No injury	부상 없음
1	Minor	깊지 않은 상
2	Moderate	깊은 상처, 1
3	Serious	뇌 손상 없는 생명을 위협
4	Severe	최대 12시간 (생명 위협,
5	Critical	척수에 손상 부상 (생명 위
6	Maximum	척수에 손상 위험하거나

※ Controllability 기준

등급	Controllability 등급			
	C0	C1	C2	C3
내용	대개 제어 가능	간단히 제어 가능	보통의 경우 제어 가능	제어하기 어렵거나 제어 불가
제어 수준	-	모든 운전자, 교통 참여자의 99% 이상이 일반적으로 피할 수 있음	모든 운전자, 교통 참여자의 90% 이상이 일반적으로 피할 수 있음	모든 운전자, 교통 참여자의 90% 미만이 일반적으로 피할 수 있음
예시	-	• 조향 축이 잠긴 상태에서 감속 및 정지를 위한 제동	• 야간 중속 주행 시 전조등이 고장난 상태에서 갓길 정차 및 제동 수행	• 브레이크 고장 시 정지를 위한 제동

www.carcrash.org 또는 www.unfallforensik.de/body_lexikon.html)

3. ISO 26262 개정 2판(2018) / 안전 수명 주기에 따른 프로세스 진행

다음 3가지 기준으로 위험 평가를 진행하고, 그 총점을 바탕으로 **ASIL(A~D)**을 설정
1. 노출성(Exposure)
2. 피해 정도(Severity)
3. 조작 가능성(Controllability)

만약 총점이 **6 이하(QM, Quality Management) 등급**이 나오면
더 이상의 분석을 하지 않고 ISO 26262도 적용하지 않음.

	ASIL rating
6 이하	QM* (Quality Management)
7	A
8	B
9	C
10	D

설정된 **ASIL**의 안전요구사항에 맞추어
HW 및 SW 모두 **V-Model 개발 프로세스**를
따라 독립적으로 병행하여 수행.

이는 개발 초기부터 생산, 폐기에 이르는
전체 수명 주기에 영향을 미친다.

4. DO-178C란?

RTCA: 항공무선기술협회
EUROCAE: 유럽민간항공장비협회
FAA: 미연방항공국

- **항공 분야 소프트웨어**의 신뢰성 및 안전성을 보장하기 위한 주요 표준.
- RTCA, EURCAAE가 공동으로 제정하였고 FAA에서 수락 가능한 적합성 입증 방법으로 채택함.
- 최신 소프트웨어 개발 기술(기법)을 도입하여(MBD, FM, OO 등) 기존 DO-178B를 개정(2012)한 것.

기존 DO-178B의 **Tool-Qualification**(프로젝트에서 활용되는 SW Tool에 대한 신뢰성 확인)항목을 DO-330으로 별도 제정하였으며, 새롭게 추가된 각 기법들에 대한 보충 문서(DO-331, 332, 333) 또한 별도로 제정되었음.

〈그림 2〉 DO-178C 관련 표준 문서

- DO-330: 소프트웨어 도구 검증 고려(Software Tool Qualification Considerations)
- DO-331: 모델 기반 개발 및 검증(Model-Based Development and Verification Supplement to DO-178C)
- DO-332: 객체지향 기술 및 관련 기술 (Object-Oriented Technology and Related Techniques Supplement to DO-178C)
- DO-333: 정형 기법(Formal Methods Supplement to DO-178C)
- DO-248C: 추가 정보(Supporting Information for Development and Verification Supplement to DO-178C)

국방 분야 등에서도 항공기 안전에 대한 관심이 계속 높아지고 있으며, **Boeing 787의 소프트웨어 결함**에 의한 사고 등으로 항공기 소프트웨어 인증 필요성이 대두되었음.

항공 분야의 사고는 심각한 인명 및 물질 피해를 야기하므로 이에 대한 안전성은 매우 중요한 이슈.

▶ **또한 DO-178C는 무인항공기(드론)가 등장함에 따라 그 필요성이 더욱 증대되고 있음.**

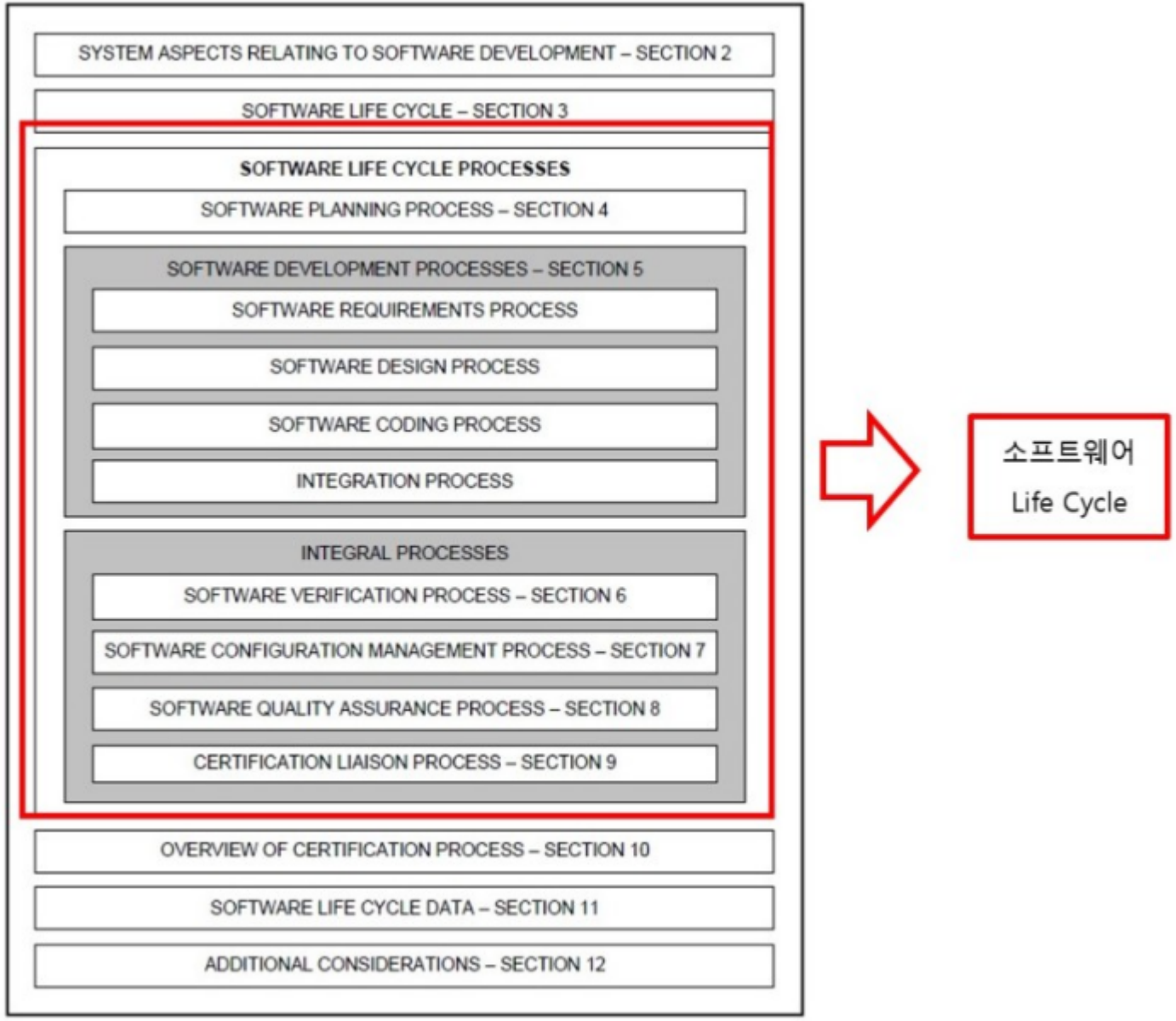
4. DO-178C / 소프트웨어 수명 주기 프로세스

DO-178C는 소프트웨어 개발을 **계획(Planning), 개발(Developement), 통합(Ingetral)** 3가지 수명 주기로 구분.

1. Planning Process
소프트웨어 개발 계획 수립에 대한 내용.

2. Development Process
요구 정의(Requirement), 설계(Design), 코딩(Coding), 통합 및 시험(Integration) 으로 구성.

3. Integral Process
검증(Verification ∋ Review, Testing, Analysis), 형상 관리(Configuration Management), 품질 보증(QA), 인증 지원(Certification Liaison) 세부 절차를 포함하며
검증은 마지막에만 하는 것이 아니라 프로젝트 시작부터 끝까지 병행하여 진행됨.



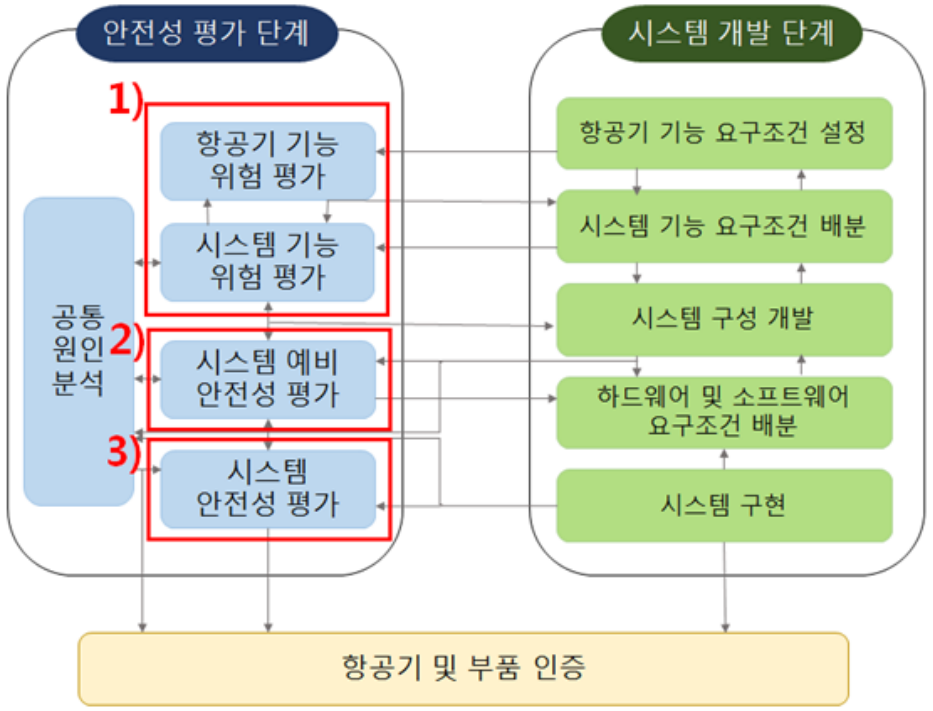
〈그림 1〉 DO-178C 문서 개요

4. DO-178C / DAL(Design Assurance Level)

DAL은 **시스템 안전성 평가 프로세스(System Safety Assessment Process)**를 통해 설정된다.

Objectives: 해당 단계에 해당하는 소프트웨어가 충족해야 하는 목표의 수.
With independence: 독립적으로 충족해야 할 목표의 수, **개발자가 아닌 개인**이 이에 대한 검증을 수행함.

Level A에 가까울수록 엄격하고 많은 목표를 만족해야 하며, 참고해야 할 문서의 양도 많음.
Level E로 설정되면 안전에 영향을 주지 않는 것으로 판단해 DO-178C의 지침을 적용하지 않음.



〈그림 2〉 시스템 개발 단계별 안전성 평가

Level	Failure condition	Failure rate	Objectives	With independence
A	Catastrophic	$\leq 1x10^{-9}$	71	33
B	Hazardous	$\leq 1x10^{-7}$	69	21
C	Major	$\leq 1x10^{-5}$	62	8
D	Minor	$1x10^{-5}$	26	5
E	No safety effects	N/A	0	0

Table 1: DO-178C Design Assurance Levels (DAL)

이후 설정된 DAL(Level E 제외)와 관련된 문서들을 적용하여
앞서 나온 **소프트웨어 수명 주기 프로세스**를 따라 개발을 진행함.
▶ **각 단계의 목표를 달성해야만 다음 프로세스로 전환할 수 있음.**

2. 항공/자동차 분야의 기능안전성 관련 기타 표준

1. 항공 분야

1. DO-254(ED-80) / Design Assurance Guidance for Airborne Electronic Hardware

항공 전자 Hardware의 개발을 위한 가이드 문서. DO-178이 Software 관련 기능 안전성 표준이라면, DO-254는 Hardware 기능 안전성 표준이다. 이 문서가 적용될 수 있는 전자 Hardware는 LRU, Circuit board assembly, FPGA나 ASIC 같은 Custom micro-coded component, COTS component 등이 있다. DO-178과 마찬가지로 failure가 실제로 미칠 영향을 A부터 E등급으로 나누어 관리한다. RTCA, EUROCAE에서 제정하였다.

2. ARP4761 / Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

민간 Airborne (비행 장비) 시스템 및 장비 안전도 평가 수행 지침 및 방법이다. 시스템의 Safety를 평가하기 위한 Modeling technique을 이용한 프로세스가 있다. DO-178이 항공 SW 기능 안전성 표준이라면 ARP4761은 SW 시스템 기능 안전성 표준이기 때문에 프로세스에서 더 범위가 넓고 다양한 위험 분석(Hazard Analysis)와 안전성 평가 (Safety Assessment)가 이루어진다. SAE International에서 제정하였다.

1. 항공 분야

3. ARP4754(ED-79) / Guidelines For Development Of Civil Aircraft and Systems

민간 Aircraft(항공기) system certification을 지원하는 개발 프로세스. 시스템 requirement부터 verification까지 완전한(complete) aircraft 개발 주기를 담고 있다. A 개정판 (ARP4761A)에서는 Safety process를 통합 개발 프로세스의 한 부분으로 수정했다. DAL (Development Assurance Level)이라는 Hardware와 Software의 development와 verification 활동의 적용에 대한 부분 또한 추가되었다. ARP4761과 결합하여 사용하기 위해 만들어졌고 DO-178이나 DO-254와 같은 다른 항공 기준과 같이 쓰인다. SAE International에서 제정하였다.

4. MIL-STD-882E

미국 국방부 산하 모든 군사부서 및 국방기관에서 사용 승인된 System Safety Standard.
국방 시스템을 개발, 테스트, 생산, 사용 및 폐기할 때 발견할 수 있는 Hazard와 관련된 risk를 식별하고 이를 평가 및 완화하는 표준 접근법. 항공 분야에 특화된 표준은 아니지만 항공 시스템의 system-level risk이 Software에 미치는 영향을 판별하기 위해 DO-178과 함께 쓰인다. 미 국방부는 이런 SW 엔지니어링 프로세스를 통해 hazard 식별 및 risk 완화를 위해 소방, 산업 보건, 환경 엔지니어와 같은 다른 기능분야 전문가에 의해서도 사용되어야 한다고 주장한다. Department of Defense (DoD)에서 제정하였다.

2. 자동차 분야

1. UNECE Regulations

World Forum for Harmonization of Vehicle Regulations (WP.29, 차량규정 조화를 위한 세계포럼)에서 제정된 규정. Vehicle safety, environment protection, energy efficiency, theft-resistance를 아우르는 규정이다. 1958년 "차량과 차량 장비와 부속품들의 획일적인 기술적 처방을 도입하고 이러한 처방에 기반한 승인의 상호 확인 조건을 위한 합의" 로 최초로 제정되었고 2015년 135개 조항이 추가되었다. 차량의 종류에 따라 규정이 나뉘어 있으며 승용차 규정은 램프부터 안전벨트, 전자기 저항성, 타이어나 바퀴 등과 관련된 조항을 포함한다.

2. FMVSS

Federal Motor Vehicle Safety Standards의 준말. 미 연방의 자동차 디자인과 구성, 성능, 내구성 요구사항과 자동차 안전 관련 규정. 이와 유사한 캐나다 자동차 안전 표준인 CMVSS와 더불어 세계 UN 요구사항과 매우 다르기 때문에 북미 specification에 부합하여 제작되지 않은 외래 자동차는 이 표준과 다를 가능성이 매우 높다. 크게 충돌 회피, 충돌 내구성, 충돌 후 생존성 세 분류로 나뉜다. UN 규정과의 두드러지는 차이점은 승용차를 예로 들면 전자 제어 주행 안정 장치(Electronic Stability Control)에 관한 항목이 북미 표준에는 존재한다. NHTSA(National Highway Traffic Safety Administration, 미국 고속도로 안전관리국)에서 제정하였다.

2. 자동차 분야

3. Automative SPICE(A-SPICE)

ISO/IEC-12207 (Software life cycle process) 에서 파생된 SPICE (ISO/IEC-15504, Information technology-Process assessment) 모델을 자동차에 적용한 표준 프로세스 모델. 국제 표준이 아니고 대형 자동차 업계들이 합의하여 만든 표준 모델로 현재 산업계 de-facto 표준이다. SPICE는 자동차의 ECU (Engine Control Unit)의 Embedded SW 개발과 관련한 표준으로 ECU 개발 프로세스 및 품질에 관한 표준이다. ISO-26262 프로세스와 굉장히 유사하여 현재까지도 두 표준에 대한 Harmonized Integrated process 연구가 진행 중이다.

4. MISRA-C Standards

MISRA에서 제정되었다. MISRA는 차량용 임베디드 소프트웨어의 Safety 확보를 위한 협회이다. ISO-26262가 출시되기 전에 이 협회에서 자동차 산업을 위해 MISRA-C라는 C 코딩 규칙을 개발했다. 현재는 Safety가 요구되는 분야에 널리 사용되고 있다. C 언어의 모호성을 최소화하는데 목적이 있다. MISRA-C 표준 준수를 위한 static checking tools와 test suite를 제공해준다.

3. 특징 및 비교

항공	DO-254	ARP4761	ARP4754	MIL-STD-882E
설립 단체	RTCA, EUROCAE	SAE International	SAE International	미 국방부
목적	항공 전자 Hardware의 Functional safety 인증표준	민간 Airborne (비행 장비) 시스템 및 장비 안전도 평가 수행 지침 및 방법	민간 Aircraft(항공기) system certification을 지원하는 개발 프로세스	모든 국방 시스템에서의 Hazard 분석, 평가 및 완화
적용 범위	Airborne electronic Hardware	Civil Airborne System & Equipment	Civil Aircraft System	모든 미 국방 System 혹은 System-level risk를 식별해야 하는 System

자동차	UNECE Regulations	FMVSS	A-SPICE	MISRA-C Standards
설립 단체	UNECE 산하 WP.29	미국 고속도로 안전관리국	대형 자동차 업계	MISRA
목적	UN소속 국가들의 차량 안전 관련 획일화된 규정	미국의 환경에 맞는 UNECE 규정 상응 자동차 안전 규정.	ECU 개발 과정 상 품질 보장	C언어의 모호성을 완화하여 차량용 Embedded SW의 Safety 확보
적용 범위	UNECE에 가입된 나라의 모든 자동차 및 부속품	미국 내의 모든 자동차 및 부속품	ECU (Engine Control Unit), ECU Embedded SW	차량용 Embedded SW

3. 기능안전성 관련 국내 법/규정

1. 자동차관리법 및 항공안전법

국내 자동차/항공분야 **안전성**에 관한 법

법령 제정은 국토교통부 주관

- 자동차 및 자동차부품의 성능과 기준에 관한 규칙 [**국토교통부령** 제700호]

- 자동차관리법 제30조1항
  자동차를 제작·조립 또는 수입하려는 자는 **국토교통부령**으로 정하는 바에 따라 그 자동차의 형식이 자동차안전기준에 적합함을 스스로 인증하여야 한다.

- 항공안전법 제19조
  국토교통부장관은 항공기등, 장비품 또는 부품의 안전을 확보하기 위하여 다음 각 호의 사항을 포함한 기술상의 기준(이하 "항공기기술기준"이라 한다)을 정하여 고시하여야 한다.
  1. 항공기등의 감항기준
  2. 항공기등의 환경기준(배출가스 배출기준 및 소음기준을 포함한다)
  3. 항공기등이 감항성을 유지하기 위한 기준
  4. 항공기등, 장비품 또는 부품의 식별 표시 방법
  5. 항공기등, 장비품 또는 부품의 인증절차

우리나라의 실정에 맞추어진 **'기능안전성'**에 관한 법은 **미비**

2. 산업표준화법

KS R ISO 26262

한국산업표준(KS)이란?

"산업표준"이란 광공업품의 종류, 형상, 품질, 생산방법, 시험·검사·측정방법 및 산업활동과 관련된 서비스의 제공방법·절차 등을 통일하고, 단순화하기 위한 기준을 말한다. 산업통상자원부 장관은 **산업표준화법**에 의거하여 산업표준을 운영하며, 이에 따라 고시된 사업표준을 한국산업표준(KS)이라 한다.

산업표준화법이란?

제1조(목적) 이 법은 적정하고 합리적인 산업표준을 제정·보급하고 품질경영을 지원하여 광공업품 및 산업활동 관련 서비스의 품질·생산효율·생산기술을 향상시키고 거래를 단순화·공정화(公正化)하며 소비를 합리화함으로써 산업경쟁력을 향상시키고 국가경제를 발전시키는 것을 목적으로 한다.

→ 국제 기능안전성 표준과 마찬가지로, 강제성은 없다

3. 국제 표준과 국내 표준

ISO 26262 vs. KS R ISO 26262

ISO 26262 규격을 구성하는 12개의 파트는 다음과 같다.

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 decommissionir
8. Support processes
9. Automotive safety integrity level(ASIL)-oriented an
10. Guidelines on ISO 26262
11. Guidelines on application of ISO 26262 to semicor
12. Adaptation of ISO for motorcycles

https://ko.wikipedia.org/wiki/ISO_26262

ISO 26262 – 11, 12는 KS R ISO 26262 - 10에 포함

KS R ISO26262-1	도로 차량 — 기능안전 — 제 1 부: 용어	2019-12-30	2019-0547	기계융합산업표준과
KS R ISO26262-10	도로차량 — 기능안전 — 제 10 부: KS R ISO26262에 대한 지침	2019-12-30	2019-0547	기계융합산업표준과
KS R ISO26262-2	도로 차량 — 기능안전 — 제 2 부: 기능안전 관리	2019-12-30	2019-0547	기계융합산업표준과
KS R ISO26262-3	도로 차량 — 기능안전 — 제 3 부: 개념 단계	2019-12-30	2019-0547	기계융합산업표준과
KS R ISO26262-4	도로 차량 — 기능안전 — 제 4 부: 시스템 수준의 제품 개발	2019-12-30	2019-0547	기계융합산업표준과
KS B ISO26262-5	도로 차량 — 기능안전 — 제 5 부: 하드웨어 수준의 제품 개발	2019-12-30	2019-0547	기계융합산업표준과
KS R ISO26262-6	도로 차량 — 기능안전 — 제 6 부: 소프트웨어 수준의 제품 개발	2019-12-31	2019-0579	기계융합산업표준과
KS R ISO26262-7	도로 차량 — 기능안전 — 제 7 부: 생산 및 운영	2019-12-30	2019-0547	기계융합산업표준과
KS R ISO26262-8	도로 차량 — 기능안전 — 제 8 부: 지원 프로세스	2019-12-30	2019-0547	기계융합산업표준과
KS R ISO26262-9	도로 차량 — 기능 안전 — 제 9 부: 자동차 안전무결성 수준 (ASIL) 및 안전 기반 분석	2019-12-30	2019-0547	기계융합산업표준과

https://standard.go.kr/KSCI/standardIntro/getStandardSearchList.do

4. 항공 분야의 국내 표준?

한국의 DO-173C?

항공분야에 관련된 **'기능안전성'**에 대한 **국내 표준**은 아직까지 **존재하지 않는다.**

감항성 또는 감항능력(Airworthiness) 요구되는 유지보수 활동이 이루어지고 있는지
유지보수를 통해 안전한 비행이 가능함을 보일 수 있는지
안전한 비행을 하기 위해 적합한 비행기인지를 측정하는 지표

Airworthiness is the measure of an aircraft's suitability for safe flight. Certification of airworthiness is conferred by a certificate of airworthiness from the state of aircraft registry national aviation authority, and is maintained by performing the required maintenance actions.

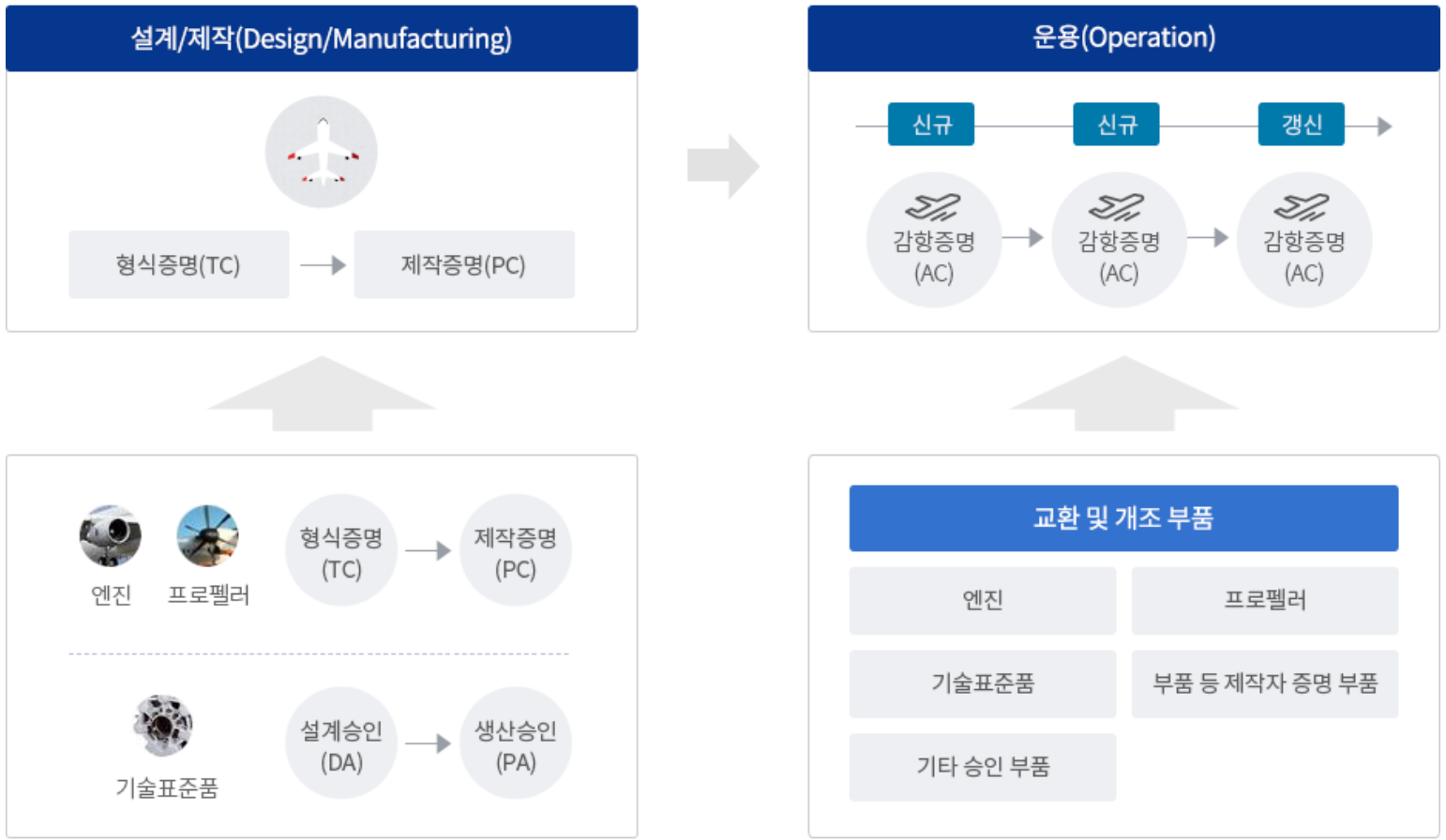
https://en.wikipedia.org/wiki/Airworthiness

The FAA approved AC 20-115C on 19 Jul 2013, making **DO-178C** a recognized "**acceptable means, but not the only means, for showing compliance with the applicable airworthiness regulations for the software aspects of airborne systems and equipment certification**."

https://en.wikipedia.org/wiki/DO-178C

5. 국내의 항공기 인증 예

항공기 인증이란?
항공기의 항행안전성을 확보하기 위하여 설계 생산, 운용의 전 과정에서 비행**안전성** 요구사항에 대한 적합성을 기술적으로 판단하고 평가하는 것



https://www.kiast.or.kr/kr/sub03_01_01.do

4. 국내외 인증 기관 및 인증 방법과 현황

1. ISO 26262 인증을 받는 방법

- ISO에서 직접 받는 것이 아님.ISO는 표준을 정하는 기관이며 표준의 이행을 평가하는 기관을 정하는 역할도 담당

- ISO 26262 인증을 필요로 하는 기업이나 개인(expert)을 위해 인증 그 자체나 교육을 진행할 수 있는 업체를 선정함

- 해당 인증은 꼭 외부기관에 의해서만 발급받아야 하는 것이 아님, 기업 자체적으로 전문가를 보유하고 있다면 자체적으로 팀을 구성해 기능 안전성을 확보할 수 있음

2. ISO 26262 국내외 인증 기관 및 인증 과정

- 국내에는 에이비앤아이, 에스피아이디(spid) 등의 인증기관이 존재함
- AB&i 에이비앤아이(주) ADVANCED BUSINESS & INNOVATION maxim integrated
- 국외 인증 기관으로는TUV SUD, Exida, Maxim integrated 이 있음
- TÜV SÜD exida spid
- 각 기관에 따라 제품 개발 전 과정(whole process)에 대한 통합 프로세스를 제공하거나 전문가 양성 교육을 진행하기도 함
- 인증을 받고자 하는 모델이 기능안전 요구사항에 따라 개발되었는지(ISO26262 기준을 따랐는지) 확인하는 방법은, 기관마다 차이는 있지만 크게 확인검토, 심사, 평가의 세가지 단계로 나뉨

3. DO-178C 인증을 받는 방법

- DO-178C 인증 또한 ISO 26262 와 마찬가지로, standard를 제정하는 항공 무선기술협회(RTCA)와 유럽 민간항공장비협회(EUROCAE)에서 직접 인증 과정을 거치지 않음. 해당 기관에서는 스탠다드에 대한 교육과 전문가 양성만을 도와주고 있음

- 특이하게 미국은 국가적 차원에서 인증을 진행함. 미국연방항공국(FAA)에서는 자국내 항공용 부품에 쓰이는 소프트웨어의 신뢰성과 안전성을 DO-178C 표준을 이용해 검증함

4. DO-178 국내외 인증기관 및 인증 과정

- 국내에서는 모아소프트가 해당 표준에 대한 교육과 인증을 담당하는 대표적인 기업임
- MOASOFT
- 국외에서는 앞서 언급한 것처럼 미국연방항공국(FAA)와 Ansys라는 기업이 존재함. Ansys는 항공 및 임베디드 시스템 개발시 DO-178C 표준을 따라 개발할 수 있는 환경을 제공함.
- Federal Aviation Administration Ansys
- ISO 26262와 마찬가지로 standard를 제정한 기관과 다양한 기관에서 해당 표준에 대한 교육을 실시하고 있음.

- DO-178C 표준은 소프트웨어 개발에 대한 가이드라인으로

  planning (계획수립) – development (개발) – verification (확인 및 검증) – configuration management (CM과정) - quality assurance (QA) - certification liaison (autority로부터의 검증)

  의 과정을 따라 진행됨

5. ISO 26262 및 DO-178C 인증 현황

- 일본과 유럽 등의 국가에서는 국가적 차원에서 해당 표준에 올바르게 대응하기 위해 가이드라인을 구축하고 있음

- 기업들은 외부기관에 의존하는 것이 아니라 해당 표준을 담당하는 전담팀을 구성해 자체적으로 해결하는 모습을 보임

- 국내에서 활동하는 약 100여개의 인증기관 중 2/3이상이 외국계 기업으로, 인증업체의 부실 심사를 감독할 수단이 없어 기업과 국가에 신뢰도 하락으로 이어질 가능성이 있음

- ISO 26262 표준을 따라 개발을 진행 함으로서 신뢰성과 안전성을 어느 정도 보장할 수 있지만, 그것이 꼭 외부기관에 의한 인증일 필요가 없음. 내부적으로 구성된 팀이나 전문가 초빙 등의 방법으로 실현가능. 오히려 공신력 있는 외부기관에서 받은 인증으로 인증 자체를 부각시켜 마케팅으로 활용하는 수단이 될 수 있음

- 최근 소프트웨어 기술의 비약적 발전으로, 기존 DO-178B가 커버하지 못하는 기술적 문제들을 담아내기 위해 DO-178C가 2012년 등장함