V&V 프로젝트 발표 1

기능 안전성 표준 및 관련 법/규정, 현황 조사

공민정
김태형
이규은
최지현

1-0. IEC 61508 (범용 기능 안전)

- 전기(Electrical), 전자(Electronic), 프로그래밍 가능한 전자 장비 (Programmable Electronic) 장비의 기능적 안전성을 위한 국제 표준
- 안전 생명 주기(safety life cycle)와 안전 무결성 기준(SIL: Safety Integrity Levels, 리스크 감소 차수 레벨)에 기반

Safety Integrity Level	Probability of failure on demand, average (Low Demand mode of operation)	Risk Reduction Factor
SIL 4	$>=10^{-5}$ to $<10^{-4}$	100000 to 10000
SIL 3	$>=10^{-4}$ to $<10^{-3}$	10000 to 1000
SIL 2	$>=10^{-3}$ to $<10^{-2}$	1000 to 100
SIL 1	$>=10^{-2}$ to $<10^{-1}$	100 to 10

Safety Integrity Level	Probability of dangerous failure per hour (Continuous mode of operation)
SIL 4	$>=10^{-9}$ to $<10^{-8}$
SIL 3	$>=10^{-8}$ to $<10^{-7}$
SIL 2	$>=10^{-7}$ to $<10^{-6}$
SIL 1	$>=10^{-6}$ to $<10^{-5}$

1-1. ISO 26262

- 모든 자동차 E/E 시스템의 안전관련 규약들을 표준화하기 위해 IEC 61508을 자동차 E/E 시스템에 적합하게 수정
- 시스템의 안전 정도를 법적으로 증명 가능

1-1. ISO 26262

1. 용어 정리(Vocabulary)

2. 기능 안전 관리(management of functional safety)

3~7. 자동차 안전 라이프사이클 단계에 맞는 요구사항

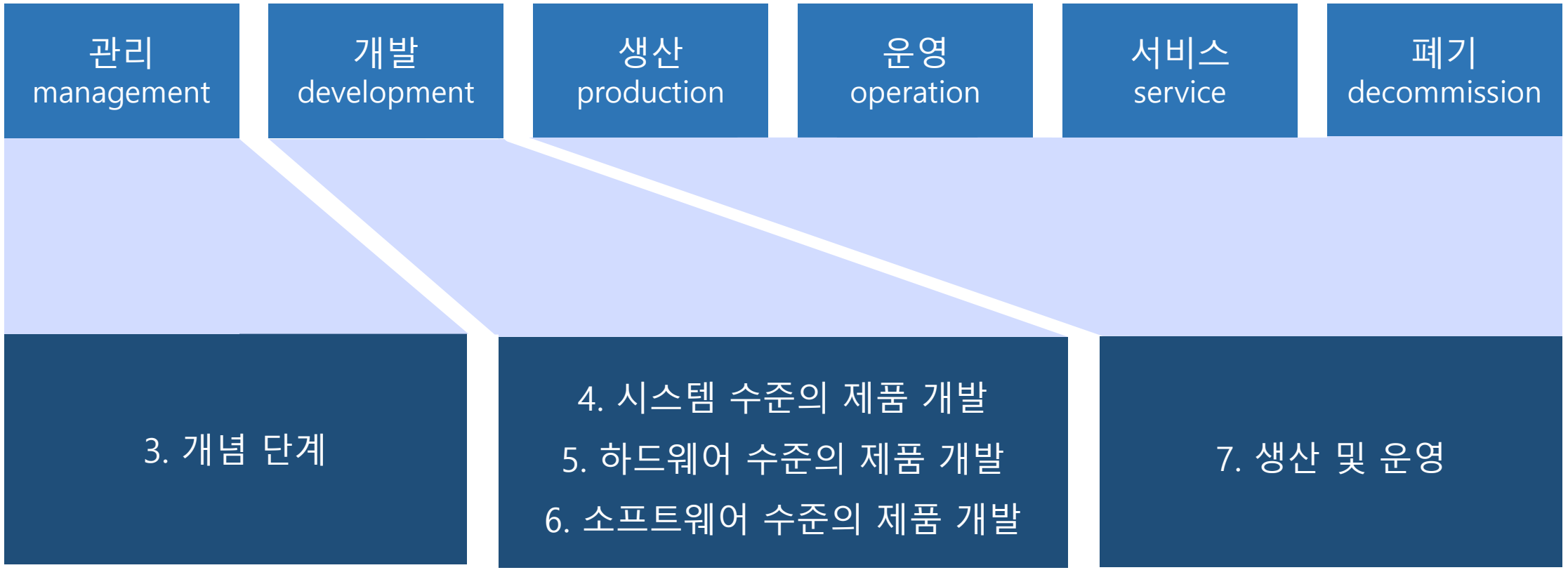
8. 지원 프로세스(Support process)

9. ASIL(Automotive Safety Integrity Level) 지향적이고 안전 지향적인 분석

10. ISO 26262 가이드 라인

1-1. ISO 26262

3~7. 자동차 안전 라이프사이클 (전체 생산 라이프사이클)



1-1. ISO 26262

ASIL(Automotive Safety Integrity Level)

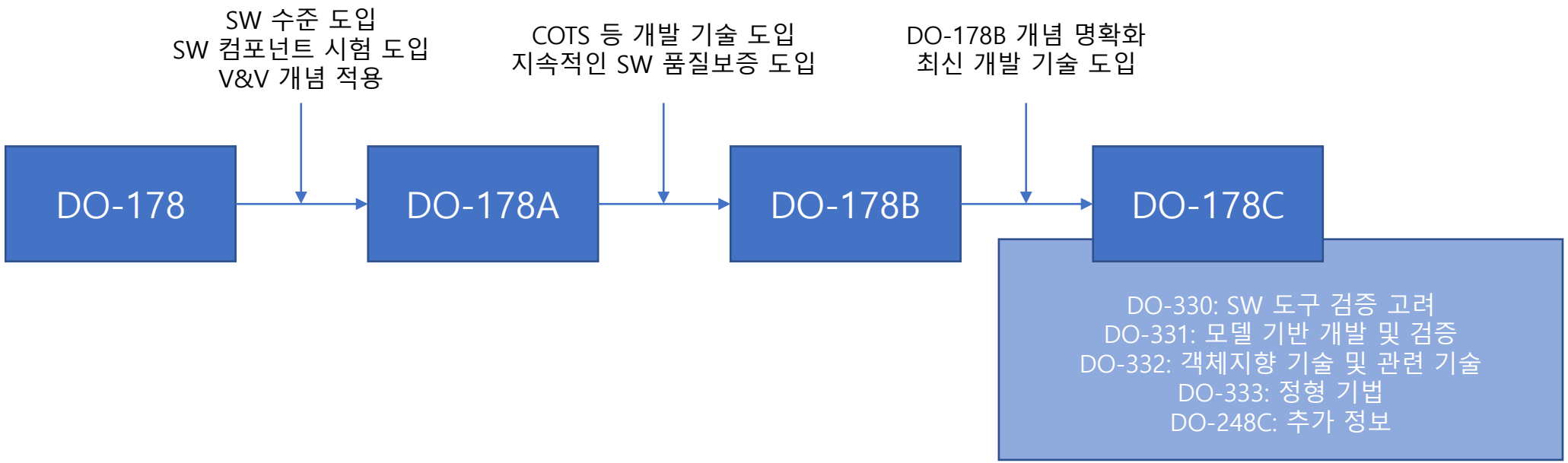
- SIL에서 파생되어 ISO 26262에서 정의된 리스크 분류 시스템
- 표준 달성에 필요한 검증 및 확인 조치까지 포함
- 3가지 기준으로 단계를 분류
  - 심각도(Severity: S0~S3): 운전자와 보행자에게 발생할 수 있는 사고의 유형
  - 발생 확률(Probability of Exposure: E0~E4): 차량이 위험에 노출되는 빈도
  - 통제력(Controllability: C0~C3): 운전자가 사고를 예방하기 위해 해야 하는 노력

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

ASIL-A~D등급으로 분류

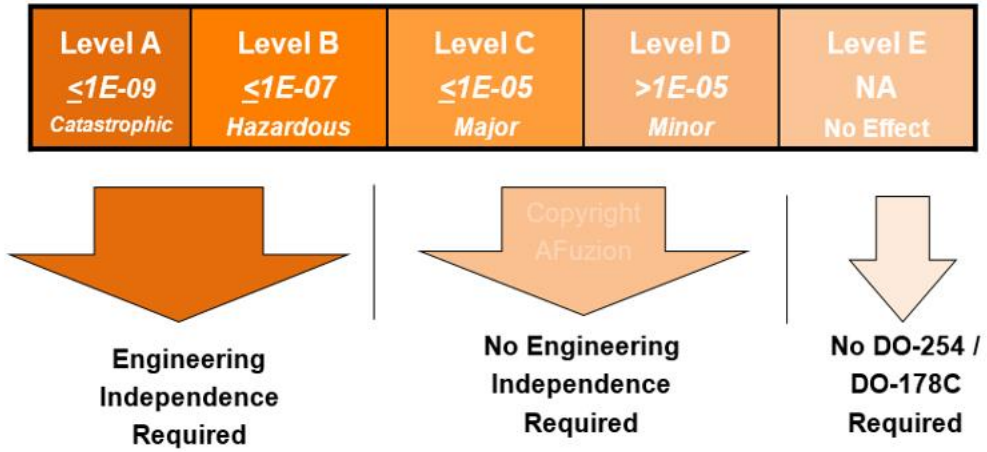
1-2. DO-178C

- 항공기, 엔진, 프로펠러 및 지역별 보조 동력 장치에 사용되는 항공기 탑재 장비 및 시스템 소프트웨어 제품 관련 인증
- 항공 분야의 소프트웨어 복잡도가 높아지고 그에 따른 결함이 늘어나면서, 신뢰성과 안전성을 확보하기 위해 등장



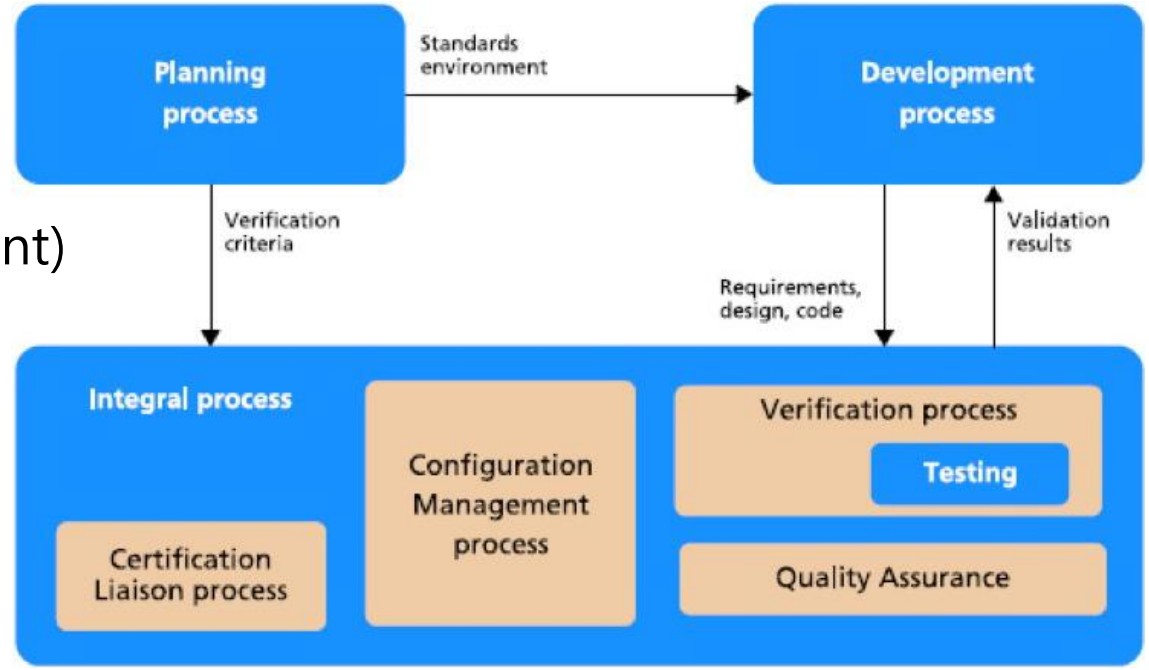
1-2. DO-178C

- DAL(Design Assurance Level) 또는 IDAL(Item DAL)로 소프트웨어 레벨 측정
  - Level A: Catastrophic(추락의 위험을 갖는 고장 위험)
  - Level B: Hazardous(성능 또는 안전에 큰 부정적 요소를 갖거나 물리적 변형 또는 과도한 업무 부하로 인해 조종사가 비행을 유지할 수 없는 위험)
  - Level C: Major(심각한 수준이지만 위험하지는 않은 상태)
  - Level D: Minor(고장 상태가 보이지만 Major보다는 덜한 상태)
  - Level E: No Effect(안전, 비행 조정 또는 조종사 과부하에 영향을 미치지 않은 고장)



1-2. DO-178C

- 소프트웨어 개발을 3가지 생명 주기(Life Cycle)로 구분
  - 기획 절차(Planning process)
  - 개발 절차(Development process)
  - 통합 절차(Integral process)
    - 검증(verification)
    - 형상 관리(configuration management)
    - 품질 보증(quality assurance)
    - 인증 절차(certification liaison)



2-1. 자동차 분야 기능 안전성과 관련된 기타 다른 표준
- ISO/PAS 19451

- 제정 배경 및 계기

- ISO 26262 part10의 부록A: microcontrollers만 언급하며 다른 종류의 반도체 포함하지 않음
  -> 이에 대한 혼란 우려
- 자동차 산업에서 향후 자동차의 안전,보안,친환경,편의성 구현을 위해 반도체의 중요성 인식 및 강조

- IOS/PAS 19451

- ISO 26262를 충족하기 위한 반도체 분야에 대한 세부적 내용
- 반도체 부품에 ISO26262 적용할 경우, 권장사항 및 모범사례 제공
  -> 사용자에게 유익한 지침 제공
- 목적: 차량용 반도체 ISO 26262 충족 위한 전문가들의 Best Practice 내용을 담은 가이드라인 제공

2-1. 자동차 분야 기능 안전성과 관련된 기타 다른 표준 조사
- ISO/PAS 19451

- ISO 26262와 ISO/PAS 19451의 공통점

  - 귀납적, 연역적 방법론인 FTA, RBD, FMEA 등의 안전 분석 기법을 사용

  -> 기능 및 안전 요구사항, 고장형태, 고장의 영향을 파악, 재검토 및 검증을 요구

- Part 1과 Part 2로 구성됨
- Part1
  - 아날로그 반도체 (Analogue/mixed signal components and ISO 26262)
  - 지적 재산(IP: Intellectual property and ISO 26262)
  - MC(Multi-core components and ISO 26262)
  - PLD(Programmable logic devices and ISO 2626)
  - 기본 고장율(BFR: Base failure rate estimation and ISO 26262)
  - 종속고장 분석(DFA: Semiconductor dependent failure analysis and ISO 26262)

2-1. 자동차 분야 기능 안전성과 관련된 기타 다른 표준 조사
- ISO/PAS 19451

- Part 2

- ISO 26262에서 요구하는 하드웨어 부품의 자격인정(Qualification of hardware component)
- 표준 인정(Standard Qualification)과의 차이점
- 자격 인정이 필요한 이유
- 인정을 받아야 하는 시기
- 인정을 할 경우 해야 할 것
- 자격 인정 시 고려할 사항
- 향후 문제 발생 경우, DIA(Development Interface Agreement:협력개발)를 통한 완성차 또는 고객과의 해결방안

2-2. 항공 분야 기능 안전성과 관련된 기타 다른 표준 : ARP-4754A

- 시스템 요구사항, 요구사항 검증, 시스템 설계 및 검증을 다루는 항공기 개발 국제 표준

  (시스템 엔지니어링 측면을 다룸)

- 항공용 시스템* 에 대한 개발 주기, 시스템의 인증 및 품질 보증을 위한 요구사항이 정확한지 확인(validation), 이 요구사항이 설계에 대해 제대로 소프트웨어 아이템과 전자 하드웨어 아이템으로 할당돼 구현됐는지 검증(verification) 포함.

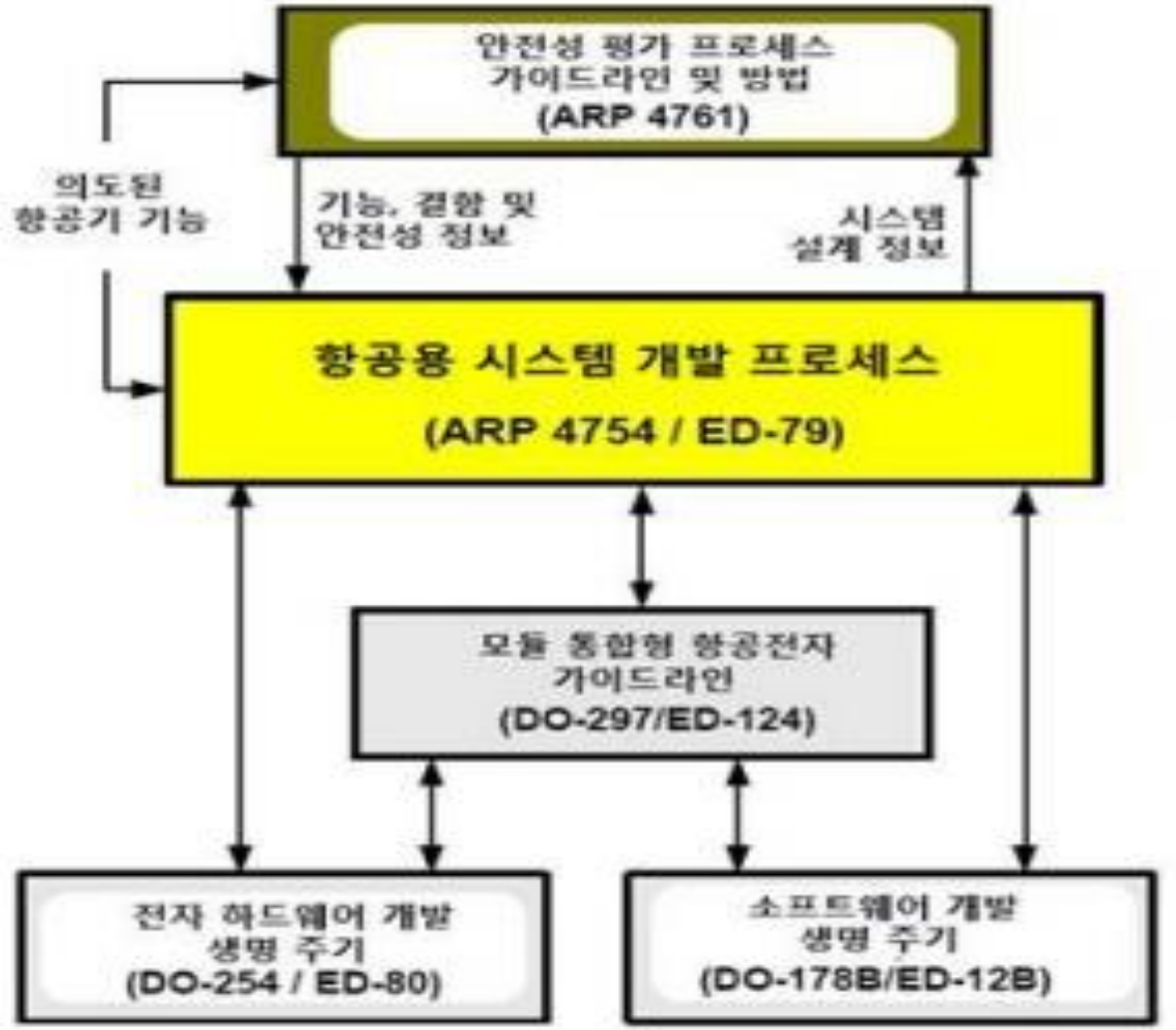
*시스템: 항공기 수준의 기능을 지원하고 항공기의 안전성에 영향 미칠 가능성 있는 고장모드를 갖는 시스템 의미함.

- 정확한 개발보증레벨(Development Assurance Level; DAL)을 할당하는 방법론 제공
- 세 부분의 가이드라인

  1. 개발 계획 프로세스
  2. 시스템 개발 프로세스
  3. 통합 프로세스

2-2. 항공 분야 기능 안전성과 관련된 기타 다른 표준 : ARP-4754A

- 항공 소프트웨어를 다루는 DO-178C와 항공 하드웨어를 정의하는 DO-254로 분류되는 체계적인 개발 흐름으로 이어지게 됨.
- 시스템 개발에서의 위치



3. SW 품질 인증의 기준

- 소프트웨어산업 진흥법 (약칭: 소프트웨어산업법)

[시행 2018. 8. 22.] [법률 제15371호, 2018. 2. 21., 일부개정]

제9조의2(품질인증기준) ① 법 제13조제3항에 따른 소프트웨어품질인증의 기준은 다음 각 호와 같다. <개정 2013. 3. 23., 2017. 7. 26.>

1. 소프트웨어의 기능을 정확하게 실행할 것
2. 소프트웨어의 신뢰성·효율성·사용과 유지·보수의 편의성 및 이식의 용이성이 과학기술정보통신부장관이 정한 수준 이상일 것

② 제1항에 따른 소프트웨어품질인증의 세부기준은 과학기술정보통신부장관이 정하여 고시한다. <개정 2013. 3. 23., 2017. 7. 26.>

[본조신설 2008. 8. 7.]

3. SW 품질 인증의 기준

- 소프트웨어산업 진흥법 시행규칙

제3조의3(품질인증 등급) 법 제13조제1항에 따른 품질인증은 1등급과 2등급으로 구분한다.

- 소프트웨어 품질인증의 세부기준 및 절차

[시행 2018. 6. 22.] [과학기술정보통신부고시 제2017-31호, 2017. 12. 22., 일부개정]

제8조(품질인증기관) ① 품질인증기관(이하 "인증기관"이라 한다)은 법 제13조, 시행령 제9조 및 시행규칙 제3조의3에 따라 과학기술정보통신부장관이 지정한 기관을 의미한다.

…

제9조(품질인증 신청) ① 품질인증을 받고자 하는 자(이하 "신청인"이라 한다)는 시행규칙 별지 제6호 서식에 다음 각 호의 구비서류를 첨부하여 인증기관의 장에게 신청하여야 한다.

3-1. 자동차 관련 국내법

- 운전자보조시스템(ADAS)

- 자율주행자동차

구분	ADAS	자율주행
차-운전자와의 관계	운전자를 지원	운전자를 대체
미 도로교통안전국 자동차 자동화 단계	레벨0 → 레벨3	레벨3 → 레벨4
기술개발 접근 방식	점진적(Evolutionary)	혁명적(Revolutionary)
운전자 필요 여부	반드시 필요	불필요

[표1: ADAS와 자율주행차의 주요 차이점]

3-1. 자동차 관련 국내법

- UNECE 자동차 기준 조화 포럼(WP29) 산하 자동/자율·커넥티드 차량 실무그룹(GRVA)에서 만든 합의안(19.2.12)

  - 한국과 일본, 유럽연합(EU) 등 40개 나라에서 생산하는 차량에 긴급제동장치(AEBS) 탑재를 의무화,

  - 한국은 2022년부터 전면 실행

- 미래자동차 산업 발전 전략: 2030년을 목표로 자율주행자동차의 완전자율주행 제도와 인프라(주요도로), 상용화를 달성 계획

3-1. 자동차 관련 국내법

- 자율주행자동차의 안전운행요건 및 시험운행 등에 관한 규정

(국토교통부 고시 제2018-24호)

- 자율주행자동차 상용화 촉진 및 지원에 관한 법률

[시행 2020. 5. 1.] [법률 제16421호, 2019. 4. 30., 제정]

- 자율주행 자동차 산업 발전의 필요성에 따라 관련 법률들이 제정
- 안전성에 대한 문제보다는 데이터의 가공/도로 주행의 여부 등 개발 관련 정책에 치중

3-1. 기업 차원의 자동차 안전

- 현대자동차, 현대모비스, 만도 등 대기업 대부분은 국제표준(ISO 26262)을 만족하는 전장부품 연구개발프로세스 구축·운영하고 공급자에게도 기능 안전 준수를 요구하고 있음.

- 국내 중소기업의 경우 SW안전 확보 활동은 차치하더라도 50% 정도만 SW개발 절차를 보유하고 있는 상태

(국민대 산학협력단, '18년)

3-2. 항공 관련 국내법

- 감항인증
  - 군용: 군용항공기 안전성확보에 대한 정부 인증
    - 생존, 기동성, 무장기능 중시
    - 미국방부 감항인증기준(MIL-HDBK-516B) 준용
  - 민간: 비행안전 확보 상태에서 성능 발휘 증명
    - 승객안전, 기체안전성 중시
    - 미연방항공청 감항인증기준(FAR) 적용

3-2. 항공 관련 국내법

- **군용항공기 표준 감항인증기준에 관한 고시**

UL.31 소프트웨어 개발 보증 수준

UAS에 통합되어 있는 소프트웨어는 다음의 요구도를 충족하는 안전 신뢰수준으로 의도한 기능을 수행해야 한다.

UL.31.1 소프트웨어 안전 계획은 안전한 소프트웨어 엔지니어링에 대한 소프트웨어 개발 보증 증거(예를들면, 소프트웨어의 경우 RTCA/DO-178B) 이나 AOP-52 그리고 펌웨어의 경우는 RTXA/DO254)와 하드웨어 설계 범위 내에서의 안전한 사용 분석을 제공하여야 한다(예, 미 국방부 합동소프트웨어 시스템안전위원회 시스템안전교범 MIL-STD-822 또는 STANAG 4404 내의 지침 활용).

3-2. 항공 관련 국내법

- **항행안전시설 성능적합증명 검사 기술기준**

제3조(적용기준) ① 항행안전무선시설의 기술기준은 항행안전무선시설 설치 및 기술기준(국토교통부 고시)중에서 기술기준을 적용한다.

② 항공정보통신설의 기술기준은 항공정보통신시설 설치 및 기술기준(국토교통부 고시)중에서 기술기준을 적용한다.

③ 제1항 또는 제2항의 검사 시 ICAO 기술 기준은 필수로 하고 해당 시설이 소프트웨어를 포함하는 경우 미국 또는 유럽의 공인화 된 항공관련 소프트웨어 개발 기술기준 최소 1개를 적용한다. 다만, 미국 또는 유럽 기술기준의 경우는 성능적합증명 검사 신청자의 선택으로 한다.

3-2. 기업 차원의 항공 안전

- 해외 수출 시 반드시 SW안전관련 국제표준 준수 필요.

- KAI, LIG Nex1, 한화 시스템 등 대부분의 대기업에서는 이를 고려해 핵심 SW에 대해서는 국제 표준(DO-178, DO-248, ARP 4754등) 준수함.

- 하지만 중소기업들의 SW안전 검증은 아직 미흡한 실정.

4. 국내 시험기관의 인증기관 KOLAS

- (한국) KOLAS(Korea Laboratory Accreditation Scheme) 에서 국가표준기본법 및 ISO/IEC 17011의 규정에 따라, 시험기관, 검사기관의 인정업무를 수행.

- KOLAS에서 인증 받은 국내 시험기관은 국가인증기관으로서 공인 받음.

- KOLAS는 상호인정협정(MRA, Mutual Recognition Arrangement)을 통해 상대국의 공인성적서를 상호 수용함

- MRA를 맺은 기관은 APAC(아시아 태평양 인정 협력체) 28개국 46개 기구, ILAC(국제 시험기관 인정협력체) 104개국 102개 기구 있음.

- 시험기관은 각 표준(ISO 26262 등) 을 기준으로 시험대상이 얼마나 규격을 준수하였는지 평가하여 공인 시험성적서를 발급할 수 있음.

4. 국내 ISO 26262, DO-178C 시험기관

인정번호 (ACC.NO)	기관명 (Organization Name)	공인유효기간 (Accreditation Period)	시도 (City)	마크사용 (Mark)	인정상태 (Status)	ISO 26262 시험여부	DO-178C 시험여부
KT571	슈어소프트테크(주)	2017-07-06 ~ 2021-07-05	서울특별시		유효	O	O
KT190	(재)한국조선해양기자재연구원	2020-01-04 ~ 2024-01-03	부산광역시	사용	유효	O	X
KT122	한국에스지에스(주) 동탄시험소	2018-02-26 ~ 2022-02-25	경기도		유효	O	X
KT009	한국산업기술시험원	2018-09-30 ~ 2022-09-29	경상남도	사용	유효	O	X

4. 국외 ISO 26262 시험기관 TUV SUD

- TUV SUD korea : 1992년 한국시장에 진출한 이래로 자동차, 배터리, 철도, 전기전자, 의료기기 등 다양한 산업분야에 걸쳐 시험, 인증, 교육 등의 서비스 제공

- 시험뿐만 아니라 검사, 교육 등의 서비스 또한 제공하고 있다.

4. 평가 방법 (국내 슈어소프트테크 기준)

- 일반 시험(비공인)와 공인 시험(국제표준규격)서비스를 제공

- 일반 시험에서는 정부R&D과제 정량적 목표 및 고객요구사항에 대해 시험

- 공인 시험의 경우 국제표준규격을 적용하여 Code Inspection, Code Coverage 측정시험을 거침

- 발급절차

- 1. 시험 의뢰서 접수
- 2. 시험대상 코드 수령 : 보안을 위해 암호화된 코드를 수령한다.
- 3. 시험 계획 및 설계 : 구체적인 시험대상을 파악하여 시험수행을 위한 상세 계획 수립 적용 규칙 및 커버리지, 제약사항 등과 함께 종결기준 수립.
- 4. 시험 수행 및 결과 분석
- 5. 성적서 발급
- 6. 성적서 위변조 방지 및 진위 확인 시스템

4. 국제표준 교육현황

- 앞의 슈어소프트테크, TUV SUD 같이 시험기관이 교육 및 자문을 병행하는 경우가 많음

- 반드시 시험기관이 아니더라도 컨설팅을 전문으로 하는 사설업체에서 교육 서비스를 제공

슈어소프트테크에서 제공하는 ISO 26262 컨설팅 절차

4. 국내외 시험기관 현황 요약

- 국제표준 시험은 인정업무를 수행하는 기관(국내의 경우 KOLAS)에서 인증 한 사설 기관에서 수행

- 교육은 별도의 인증을 거치지 않은 사설 기관에서도 교육 가능

- ISO 26262: 인증(Certification) 대신 시험의 개념
  -> 반드시 인증 받을 필요 없음

- 비록 인정기관의 인증을 받았더라도 사설기관에서 시험이 치루어 지기 때문에 부정 시험이 치뤄지는 등의 사례가 있음
  -> 시험기관인정 이후에도 지속적인 감시가 필요할 것