기능안전성 표준 및 동향

- 201611293 전다윤 -
- 201611261민지호 -
- 201212519 김선우 -
- 201510624김용현 -

- 목차 -

- 기능안전성 이란?
  - 안전성 vs 기능안전성
- 자동차 분야 기능안전성 (ISO26262)
  - 정의 : 목록 및 개요
  - 파트 별 설명 (+ Life Cycle)
  - 국내 법
  - 인증기관 및 절차
- 항공 분야 기능안전성 (DO178)
  - 정의 : 목록 및 개요
  - Life Cycle
  - 기타 관련 표준
  - 개정 흐름
  - 인증 기관 및 절차

기능안전성이란? : 안전성 vs 기능안전성

Safety vs Functional Safety

안전성 : 자연재해 ,사고로 인한 피해의 원인이 될 수 있는 위험요소로 부터 막는 것

기능안전성 : 시스템이나 장비에 의해 결정되는 안전

전기 모터

안전성 : 절연체를 통해 안전유지

기능안전성 : 센서를 통해 과열이 발생하면 위험을 감지하고 동력 차단

▶ Fail Safe

ISO26262 : 정의 및 개요

ISO26262 이란?

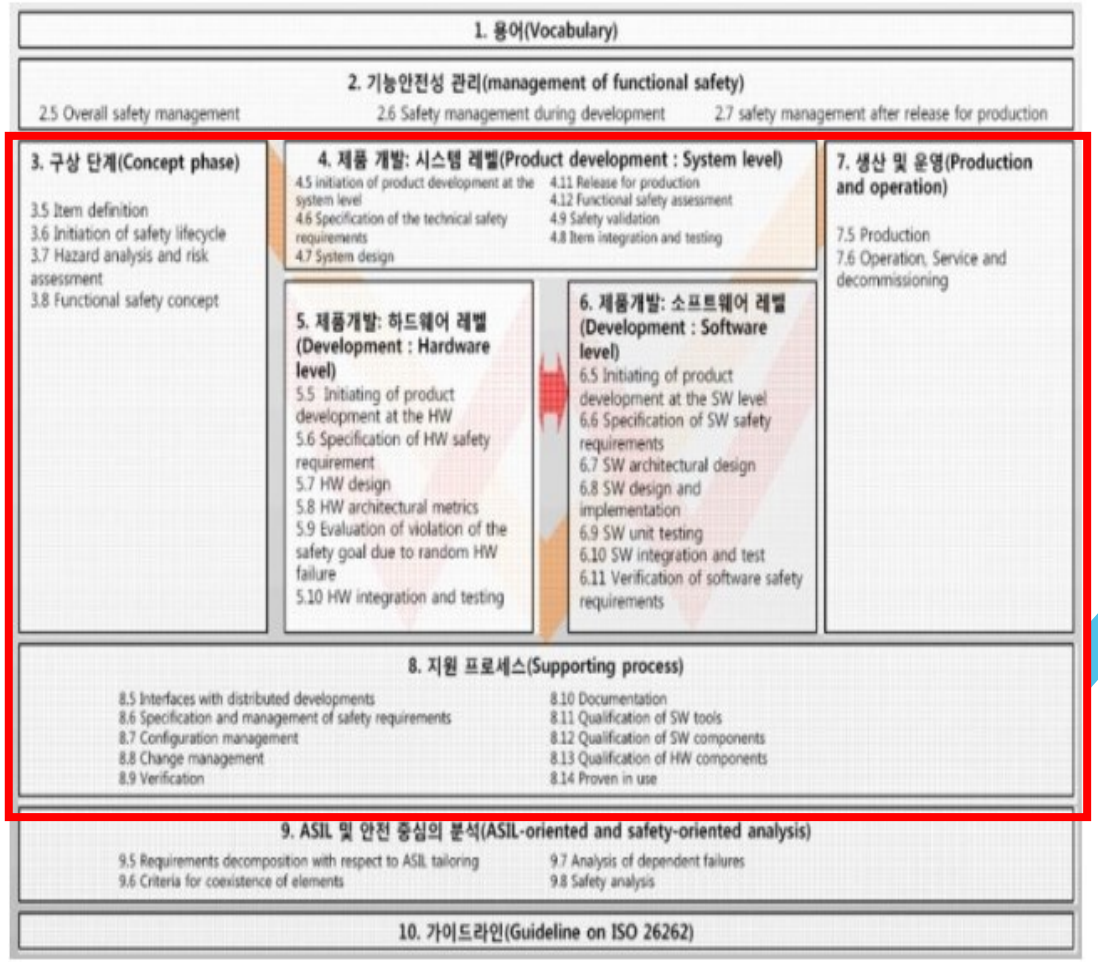
다른 말로는 자동차 기능 안정성 국제 표준이라 불리며 자동차의 안전 관련 전기/전자 장치에 적용되는 기능 안정성

국제 표준

ISO26262 개요 (Guideline)

- 단순한 규격만을 말하는 것이 아닌 프로세스 모델과 함께 요구되는 안전 프로세스, 유무형의 증거물, 그리고 개발과 생산에 사용되는 방식을 정의한다.
- ISO 26262는 자동차용 시스템의 개발부터 생산, 폐기까지 수명 전 주기에 걸쳐 적용 가능한 기능안전을 정의합니다

ISO26262 : definition



ASPICE (Automotive SPICE)

- 소프트웨어 개발 프로세스 및 관련된 비즈니스 관리 기능 전반에 관한 기술적 표준 (SPICE)을 자동차에 적용
- 자동차 개발의 여러 도메인 중, 소프트웨어 개발 도메인에 대해 프로세스 개선 역량을 결정하기 위한 모델
- 5단계 등급으로 나뉜다.
- ISO 26262 표준 인증을 위하여 CMMI, ASPICE 와의 통합이 필요하다.

ISO26262 : Part 2,3

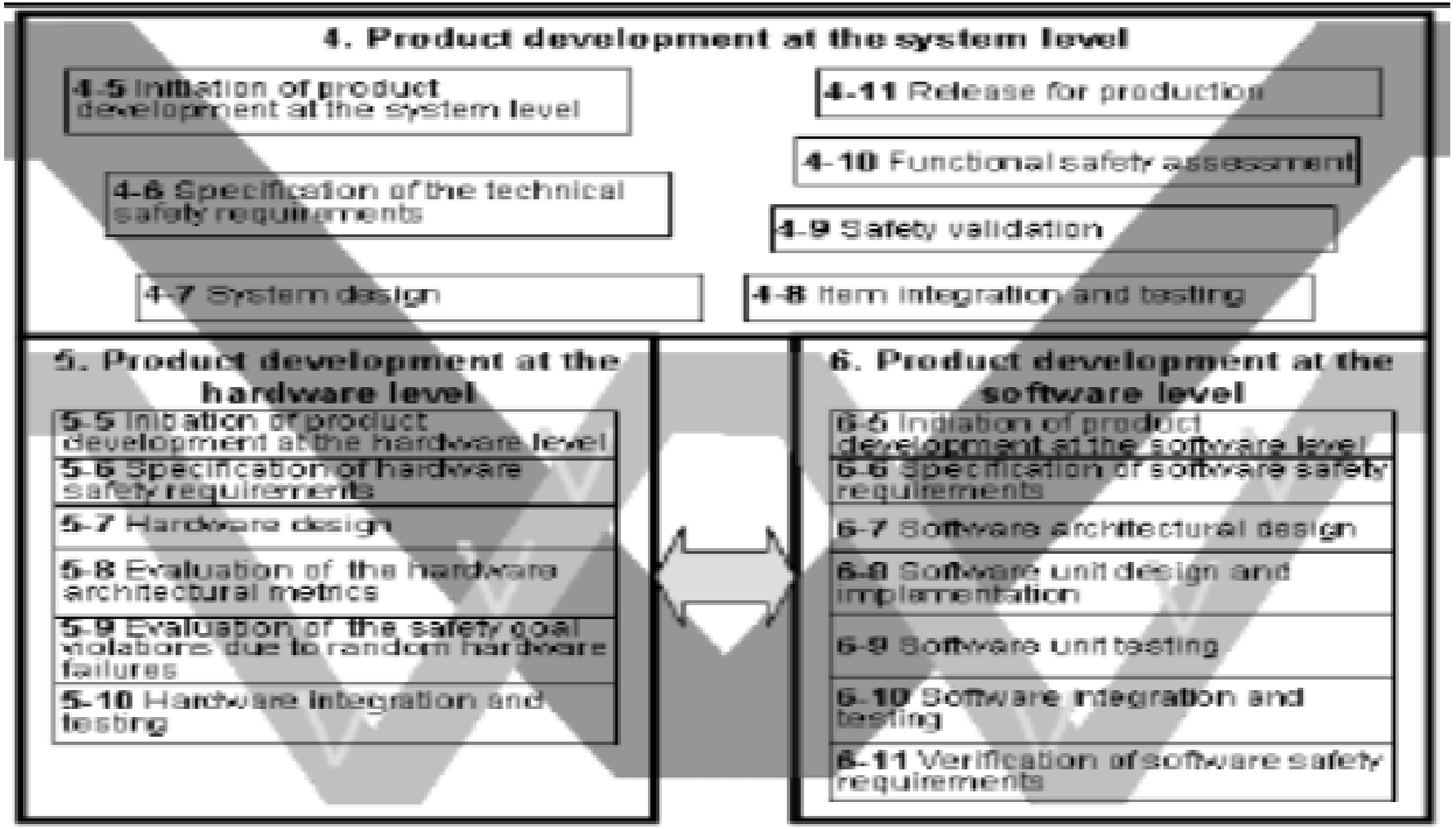
2-5. Overall safety management

안전생명주기를 책임지고 안정생명주기 활동을 수행하는 조직에 대한 요구사항을 정의한다.

3-7. Harazd analysis and risk assessment

FTA(Fault tree analysis) or FMEA(Failure Modes and Effects Analysis) 를 이용한 위험 요인 분석 및 위험성 평가

ISO26262：Part 4,5,6



ISO26262 : Part 7(생산 및 운영)

Functional Safety Requirement

품목 생산을 위한 계획, 샘플생산, 양산, 서비스 등에 관한 요구사항 정의

1.Production

Objectives : 안전 관련 개발 품목의 생산 프로세스 개발 및 유지
Activities : 생산 계획 수립 및 생산 수행
-> 생산 계획서, 생산 통제 계획서, 통제 특정 보고서, 생산 프로세스의 역량 보고서

2.Operation service and decommissioning

Objectives : 고객 정보, 유지보수 지침 명세
Activities : 운영, 서비스, 폐기 계획 수립 및 수행
->유지관리 계획서, 수리 지침, 안전 관련 정보, 필드 조사 지침

ISO26262：Part 8(지원 프로세스)

안전 요구사항 명세 및 관리, 형상관리, 변경관리, 검증, SW 툴, HW의 자격 검증

1.Interfaces within distributed developments
2.Specification and management of safety requirements
3.Configuration management
4.Change management
5.Verification
6.Documentation
7.Confidence in the use of software tools
8.Qualification of software components
9.Qualification of hardware components

개발 이후의 생산 및 공급, 검증 등을 하는 단계

ASIL (Automotive Safety Integrity Level)

ASIL 이란?
ISO26262 내에서 HARA에 의해 정의되는 위험 등급 분류 체계

ISO26262：Part 9 (ASIL 분해)

ASIL 분해
상위 레벨에서 하위 레벨로 상세화할 때 ASIL을 적절히 배분하는 것

ASIL 분해를 하는 이유?

- 개발하려는 Item의 ASIL 등급이 높아서 기간내에서 수행하기 어려운 경우
- 기존에 개발한 부분을 통해서 신규 Item의 개발 시 활용이 가능한 경우

→ 개발 비용 감소

ISO26262：Part 9 (위험도 분석)

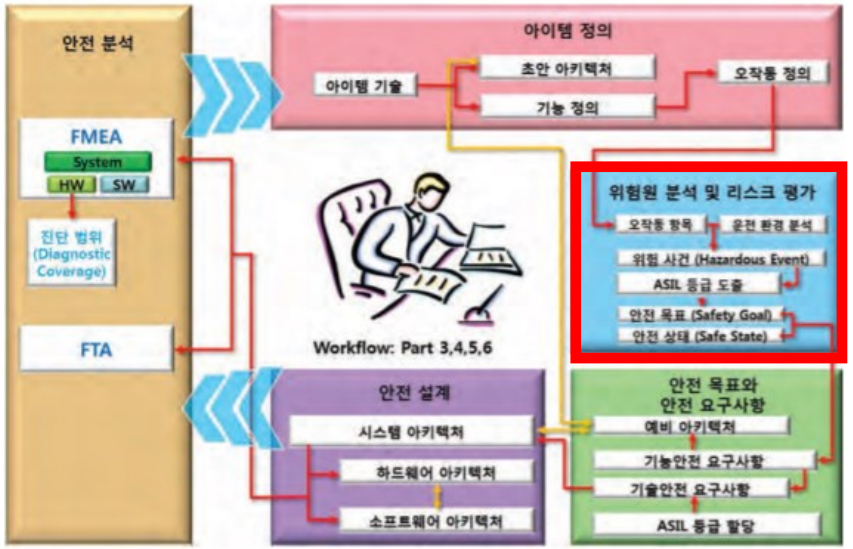
FTA (Fault Tree Analysis)

- 정량적 고장해석방법
- Top-down
- 트리 형태로 분석

FMEA (Failure Mode and Effects Analysis)

- 정성적 고장해석방법
- Bottom-up
- 표 형태로 정리

ISO26262 : 안전 활동관리 방안



〈그림 5〉 기능안전 프로세스상에서 안전 관리에 대한 "우경일&석민진 해석"

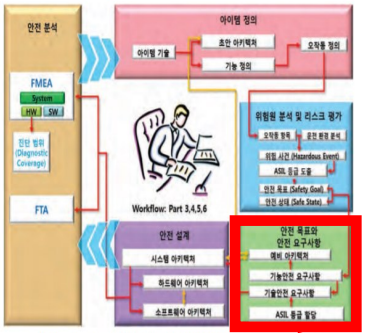
위험원 분석 및 리스크 평가(H&R) 단계

잠재적인 위험 사건(Hazardous Event)을 분석

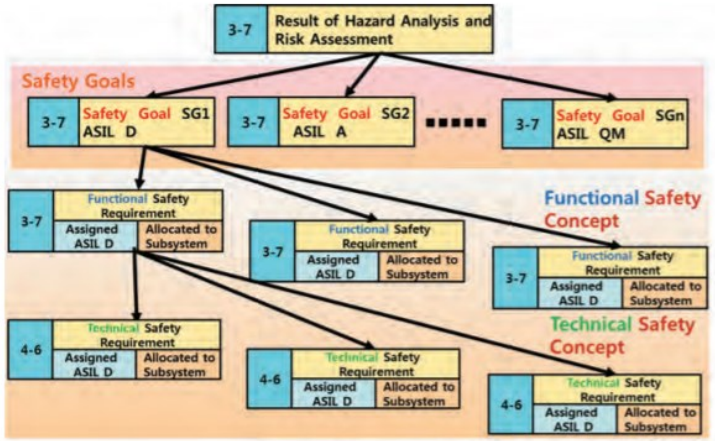
- 심각도 : 위험 사건 발생시, 사람에게 끼칠 수 있는 위험 정도
- 노출확률 : 위험사건이 발생하는 기간,상황 빈도
- 제어가능성 : 운전자의 적절한 대응을 통한 통제정도

⇒ ASIL 정도를 판단한다 엄격함의 정도 에 따라 QM A < B < C < D < E로 정해지며 A이상의 상태를 안전 상태 라고 한다.

ISO26262 : 안전 활동관리 방안



〈그림 5〉 기능안전 프로세스상에서 안전 관리에 대한 "우경임&석민진 ..."



〈그림 9〉 안전 목표 및 안전 요구사항 계층도

안전 목표 및 안전 요구사항 단계

part3, part4에서 언급하는 기술안전 개념 분석을 통해 안전 목표를 달성하기 위한 기능 ,기술, HW,SW 안전요구사항 명세

- 안전목표 : H&R 단계 최종 산출물, 최상위 안전 요구사항
- 기능안전 요구사항 : 안전 목표 달성을 위한 차상위 안전 요구 사항
- 기술안전 요구사항 : 기능안전 요구사항을 구현하기위한 시스템 레벨 안전 요구사항
- 시스템/HW/SW 안전 요구사항 : 기술 요구사항을 구현하기 위한 각 단계별 안전 요구사항

⇒ 요구사항, 엘리멘트간의 연관성을 설정하여 기능 /비기능을 포함한 아키텍처를 완성하고, 소프트웨어 하드웨어로 분리 한다. 이는 하드웨어 컴포넌트, 소프트웨어 유닛까지 영향을 끼친다.

ISO26262 : 안전 활동관리 방안

〈그림 5〉 기능안전 프로세스상에서 안전 관리에 대한 "우경일&석민진 해석"

안전 설계(Safety Design)와 안전 분석(Safety Analysis) 단계

시스템/하드웨어/소프트웨어 아키텍처를 구성하고, 동시에 검증을 위한 과정

- 시스템 아키텍처 : 안전 목표 ,안전 요구사항 단계 시스템 아키텍처를 구성하고 있는 엘리먼트들은 ASIL이 지정된 기술안전 요구사항들을 할당 받게 되고 이를 바탕으로 하드웨어 아키텍처와 소프트웨어 아키텍처를 구성한다.
- 하드웨어 아키텍처 : 소프트웨어 아키텍처와는 다르게 안전 관련된 컴포넌트들의 고장율(FailureRate)을 관리해야 한다.

=>안전 분석은 시스템/하드웨어/소프트웨어 아키텍처를 구성하면서 동시에 수행하는 단계이다.

ISO26262 : 안전 활동관리 방안

〈그림 5〉 기능안전 프로세스상에서 안전 관련에 대한 "우경일&석민진 해석"

안전 설계(Safety Design)와 안전 분석(Safety Analysis) 단계

ISO 26262 표준에서는 FTA를 통해 H&R 단계에서 도출된 안전 목표 (SafetyGoal)를 중심으로 안전

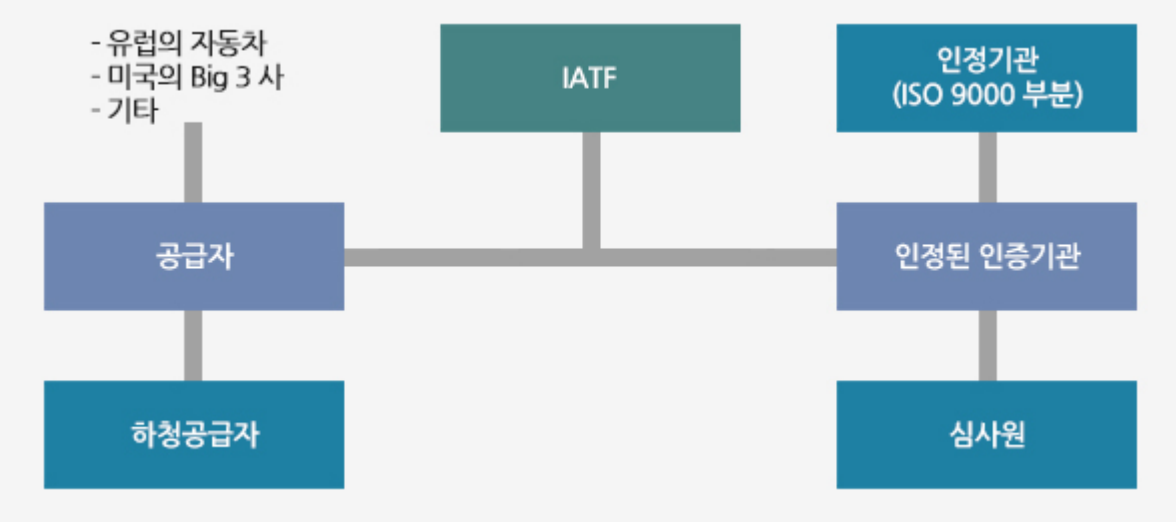
진단 범위 분석 활동은 하드웨어 컴포넌트들의 고장율을 계산하여 SPFM과 LFM을 산출하고, 구성하고 있는 하드웨어 아키텍처가 얼마만큼 단일점 결함 및 잔존 결함이 있는지를 나타내는 SPFM, 잠재 다중점 결함의 비율을 나타내는 LFM을 하고, 아이템에 부여된 ASIL 기준 내에 충족하는지를 검증한다.

*시스템,하드웨어 설계 검증 안전 분석기법 : FMEA와 FME(D)A

기타 관련 표준 (IATF 16949)

Another Standard

자동차 부품 관련 조직의 지속적 개선, 부적합 예방을 목적으로 IATF와 ISO에 의해 개발된 자동차 분야 품질경영 시스템 규격입니다. ISO 9001 규격을 기본으로 하여 추가적인 시스템 요구사항이 포함되어 있습니다.
ISO/ TS 16949 를 대체하기 위해 2016년 10월에 발표됨



IATF는 공급자인 GM, FORD 등 세계적인 자동차 생산기업들로 구성되어 있습니다.

ISO26262 : 국내 법

Certificate Authority and procedures

- 2012.12.07　국내 산업의 육성을 위하여 신속한 KS 부합화 사업이 필요하다. 2011년 10월 자동차 산업분야의 기능안전성 표준으로 ISO 26262가 제1부~제9부까지 총 9부가 발표됨. 파급효과가 큰 분야로 ISO 26262의 KS 부합화가 시급함

- 2015.06.24　국제표준(ISO)을 부합화한 국가표준(KS)의 용어 및 번역 내용 등을 업계 실정에 맞게 수정하여 활용될 수 있도록 하고, 2008년 개정된 KS 서식을 적용함

- 2019.12.30　국제표준(ISO, IEC, ITU) 개정내용 반영

ISO26262 : 인증 기관 및 절차

Certificate Authority and procedures

인증 기관

한국 : KAB

(한국인정지원센터)

미국 : ANAB

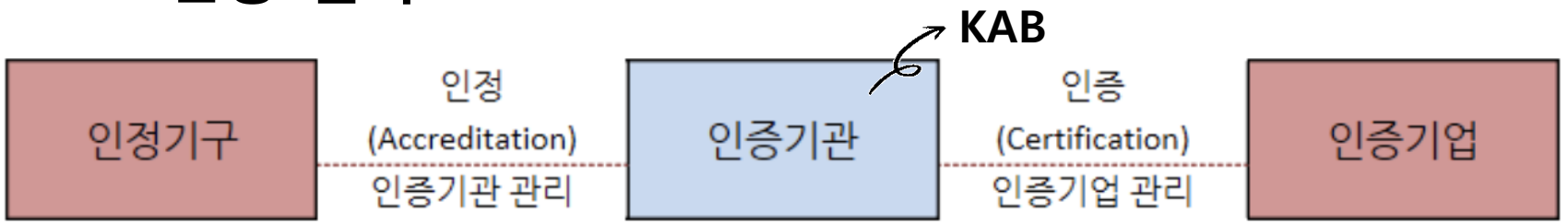
일본 : JAB

영국 : UKAS

독일 : TGA Gmbh

네덜란드 : RvA

ISO 인증 절차



1. 시스템 구축 (시스템 점검 , ISO에 따라 문서화 ,내부검토)
2. 인증의 신청 및 계약 체결 (상담 , 제안 요청 , 인증 제안, 인증 신청)
3. 인증 심사 (심사 계획 통보 , 예비 심사 , 본 심사)
4. 인증심사 부적합 시정 및 인증의 결정 (확인 심사 , 인증 심의 ,인증서 발급)
5. 사후 관리 심사 (최초 발급 후, 3년간 6개월~1년 주기로 심사)
6. 인증 갱신 (3년 주기로 갱신되어야 인증 유지)

DO178 : 정의 , 목록 및 개요

DO178 : Definition

DO178 이란?

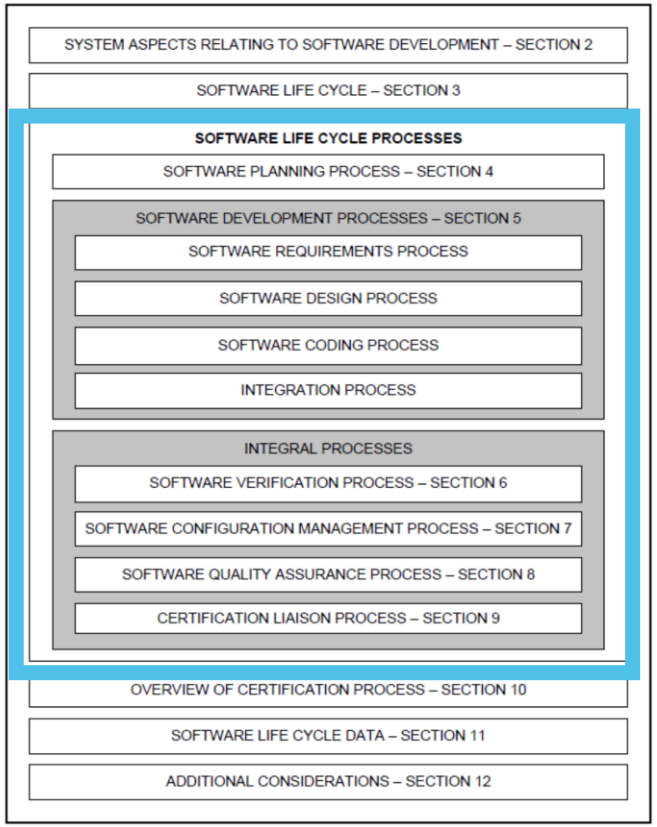
항공기 시스템 및 탑재 장비(감항) 인증 시 소프트웨어에 대해 고려할 사항

DO178 개요 (Guideline)

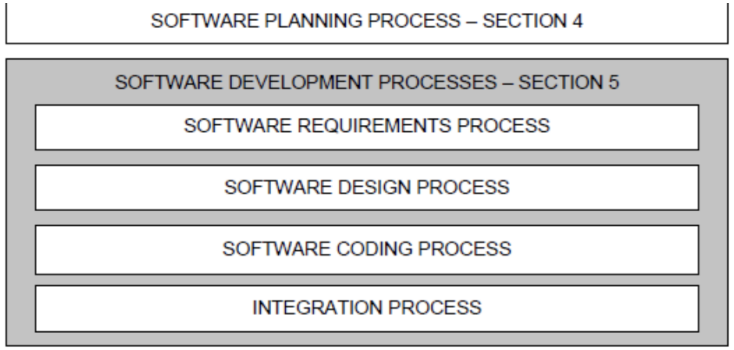
항공 시스템과 장비를 위한 소프트웨어 생산과 관련된 인증 특성

소프트웨어 Life Cycle (+ 시스템 Life Cycle의 일부)

소프트웨어
Life Cycle



DO178 : 소프트웨어 Life Cycle – 1,2



1. 소프트웨어 계획 프로세스 (Software Planning Process)

프로젝트에 대한 소프트웨어 개발과 필수 프로세스의 활동을
정의하고 조정

2. 소프트웨어 개발 프로세스 (Software Development Process)

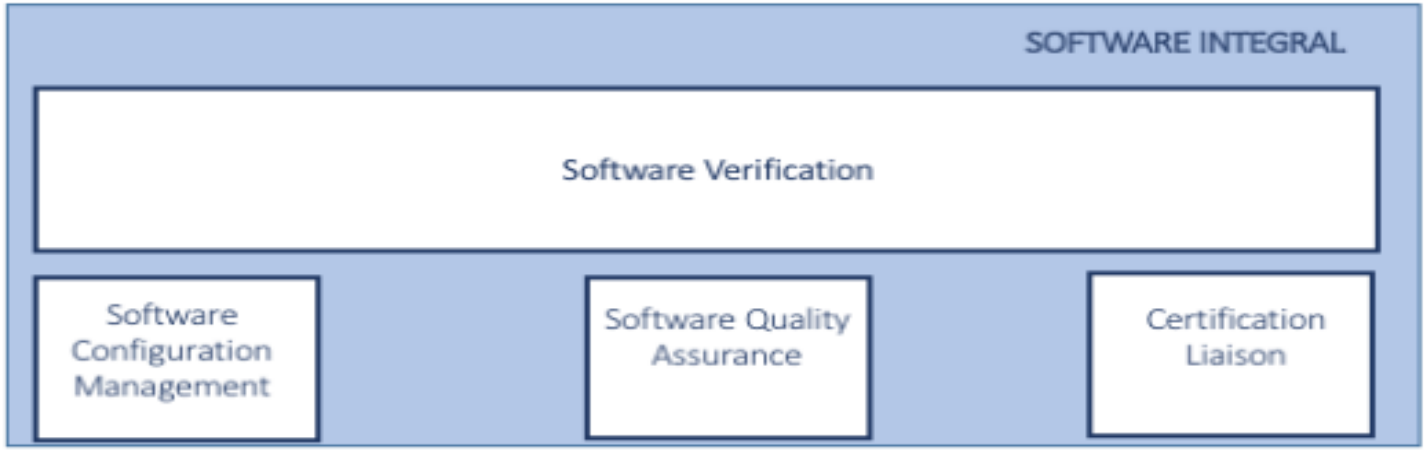
소프트웨어 제품을 생산하는 소프트웨어 개발 프로세스
소프트웨어 요구사항(Requirement) / 설계(Design) / 코딩(Coding), 통합(Integration) 프로세스가 존재

DO178 : 소프트웨어 Life Cycle - 3

3. 필수 프로세스 (Integral Process)

소프트웨어 라이프 사이클 프로세스와 출력에 대한 정확성과 컨트롤 그리고 신뢰를 보장하는 필수 프로세스

소프트웨어 검증(Verification) / 형상 관리(Configuration Management) / 품질 보증(Assurance Assurance), 인증 교섭(Certification Liaison) 프로세스가 존재



DO178 : 소프트웨어 Life Cycle - 3

3. 필수 프로세스 (Integral Process)

소프트웨어 검증 프로세스 (Software Verification Process)

(1) 목적: 소프트웨어 개발 프로세스 동안에 주입될 수 있는 에러를 탐지하고 레포트하는 것

(2) 개요

Input: 시스템 요구사항, 소프트웨어 요구사항 및 아키텍처, 추적 데이터, 소스 코드, 실행가능 오브젝트 코드, 소프트웨어 검증 계획

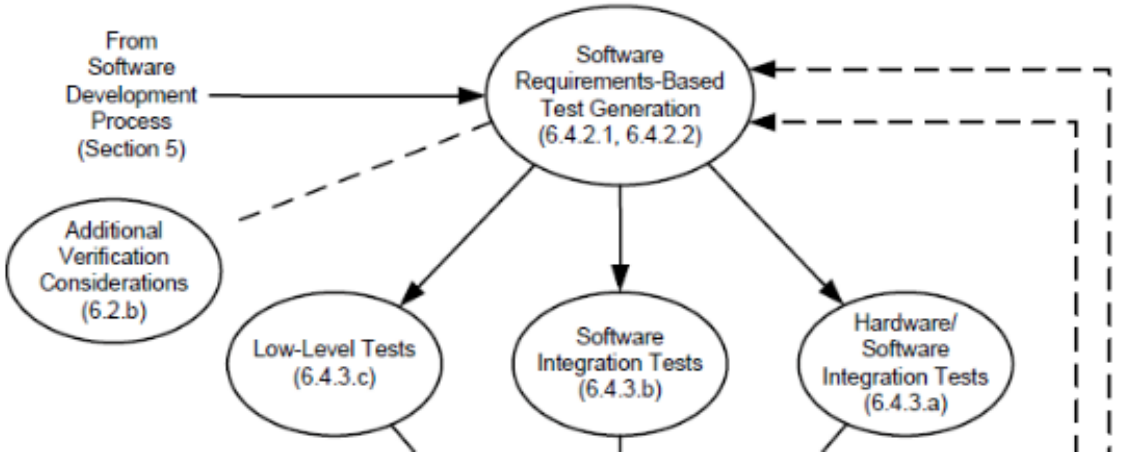
Output: 소프트웨어 검증 케이스 및 절차, 소프트웨어 검증 결과, 관련된 추적 데이터

DO178 : 소프트웨어 Life Cycle - 3

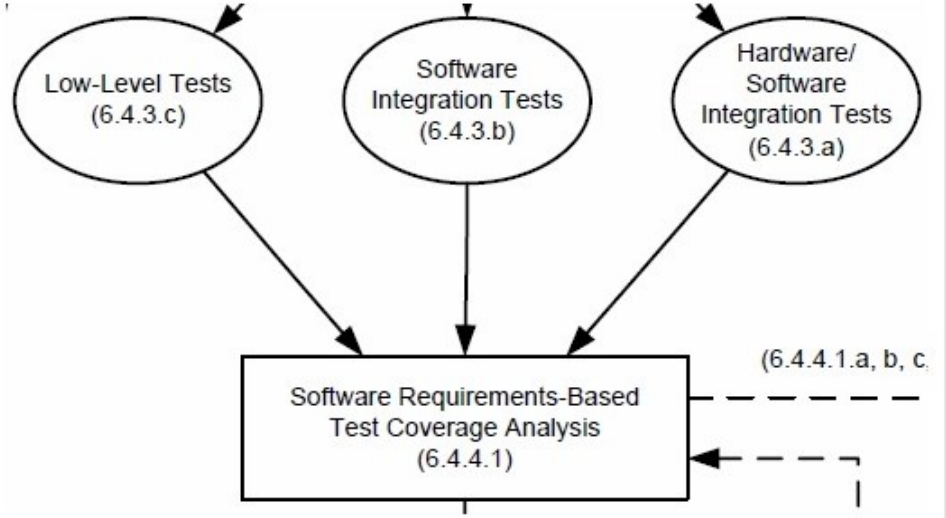
DO178 : SW Life Cycle

(3) 소프트웨어 리뷰 및 분석

- **상위레벨 요구사항**의 리뷰 및 분석 시스템 요구사항과의 연계성 중요
- **하위레벨 요구사항**의 리뷰 및 분석: 상위레벨 요구사항과의 연계성 중요
- **소프트웨어 아키텍처**의 리뷰 및 분석: 많은 수의 컴포넌트와 그들의 관계로 이루어지는 아키텍처 중심 검증
- 소스 코드의 리뷰 및 분석: 하위레벨 요구사항, 소프트웨어 아키텍처, 소프트웨어 코드 표준과 일치해야함
- **통합 프로세스의 출력**에 대한 리뷰 및 분석: 통합 프로세스에서 나오는 출력에 대해 리뷰와 분석



(1). 소프트웨어 요구사항 기반 시험 생성 및 수행



(2) 시험 커버리지 분석

(4) 소프트웨어 시험

- 목표: 실행가능 오브젝트 코드가 상위/하위레벨 요구사항을 충족하고 강건성(Robust)를 가져야함

1. 소프트웨어 요구사항 기반 시험 생성 및 수행

2. 시험 커버리지(Test Coverage) 분석

= 요구사항 기반 커버리지 분석: 정상(Normal)/비정상 입력과 조건에 응답하는 소프트웨어의 능력

+ 구조적 커버리지 분석: 컴포넌트간의 인터페이스를 포함해서 어떤 코드 구조가 요구사항 기반 시험 절차에 의해서 실행되지 않았는지를 결정

DO178 : 소프트웨어 Life Cycle - 3

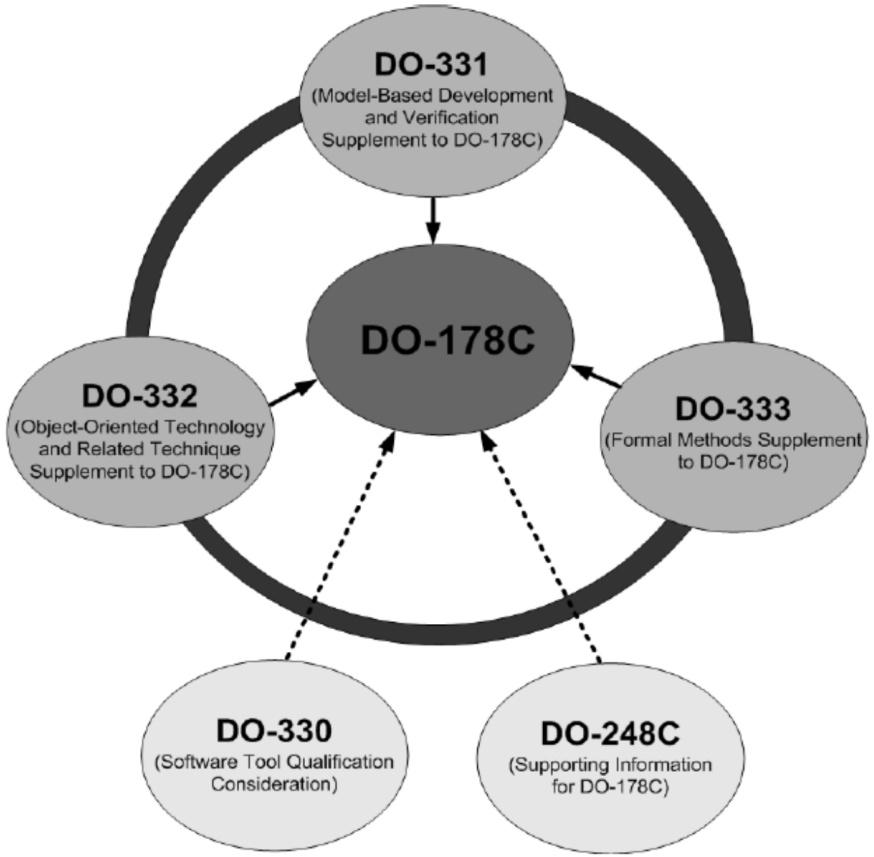
(5) 소프트웨어 검증 프로세스 **추적성**

소프트웨어 요구사항 – 시험 케이스 간, 시험 케이스 – 시험 절차 간, 시험 절차 – 시험 결과 간의 양방향 연결성을 보여주는 추적성 데이터 개발

(6) **파라미터 데이터 아이템**에 대한 검증

파라미터 데이터 아이템을 포함한 기능이 정상적으로 수행되는지 확인

DO178 : 관련 표준



DO-330: 소프트웨어 도구 검증 고려

DO-331: 모델 기반 개발 및 검증

DO-332: 객체지향 기술 및 관련

DO-333: 정형 기법

DO-248C: 추가 정보

DO178 : 개정 흐름

DO178 : Flow of Revision

규격	주요 내용	연도
DO-178	· 기본적인 절차	1980
DO-178A	· 소프트웨어 수준 도입, 소프트웨어 컴포넌트 시험 도입 · 검증(Verification) 및 인증(Validation) 개념 적용	1985
DO-178B	· '어떻게' 보다는 '무엇을'에 중점 · 다양한 소프트웨어 개발 기술 도입(COTS 제품, 도구 도입) · 지속적인 소프트웨어 품질 보증 도입(전환기준)	1992
DO-248	· DO-178B 관련 FAQs 및 명확화	2001
DO-278	· 지상용 소프트웨어에 대한 DO-178B 적용 관련	2002
DO-178C	· 최신 소프트웨어 개발 기술도입(모델 기반 개발 및 검증, 정형기법, 객체지향 기술) · DO-178B 개념 명확화	2012

FAA(미연방항공국)에서 FAR에 대한 적합성 인증 방법으로 DO-178B를 채택함으로써 항공분야 소프트웨어 인증의 주요 표준으로 자리 잡았다

▶ **소프트웨어의 복잡성이 높아짐에 따라 신뢰성, 안전성 확보가 필요**

DO178 : 관련 법 및 인증 절차

DO178 : Law and Certification Procedure

형식증명
항공기 기술기준 적합여부에 대한 증명

제작증명
형식증명을 만족할 기술, 설비, 관리체계에 대한 증명

감항증명
감항성에 대한 증명

※ 군용항공기의 경우, 안전 인증에 관한 법령이 따로 존재한다.

DO178 : 인증 기관

Certificate Authority and procedures

인증 기관

한국 : KIAST
(항공안전기술원)

미국 : FAA
(미국연방항공청)

세계 : ICAO
(국제 민간 항공기구)

- **KIAST** (한국안정기술원)

  ACS(Aircraft Certification System) 항공인증 시스템을 사용한다

- **FAA** (미국연방항공청)

  IASA(International Aviation Safety Assessment Program) 이라는 독립적 시스템을 가지고 있으며, 각 항공사, 항공기에 대해 따로 평가하는 것이 아닌 그 항공사가 소속된 국가를 대상으로 평가한다.

- **ICAO** (국제민간항공기구)

  UN의 전문기구로서 비행의 안전확보, 항공로/공항의 발전을 목표로 하고 있다.

감사합니다