소프트웨어 V&V

기능 안정성 표준 및 동향

201511243 김동언
201511246 김상재
201511262 박우진
201711356 천세진

Index

Functional Safety

- **IEC 61508**
  - “Functional Safety of Electrical/Electronic Programmable Electronic Safety-related System” , 프로그래밍이 가능한 **전기/전자 시스템**의 기능 안전(Functional Safety) 표준 규격
  - 모든 종류의 산업에 적용 가능한 기본적인 기능안전 표준을 목적으로 작성
- **IEC 61508 에서 정의한 Functional Safety**
  - 프로그래밍 가능한 전기/전자 시스템의 정확한 기능, 다른 기술 안전 관련 시스템과 외부적인 위험 감소 설비에 의존하는 **제어 대상 장치와 제어 대상 장치를 제어하는 시스템** 관련된 부분적 또는 전반적인 안전

ISO 26262

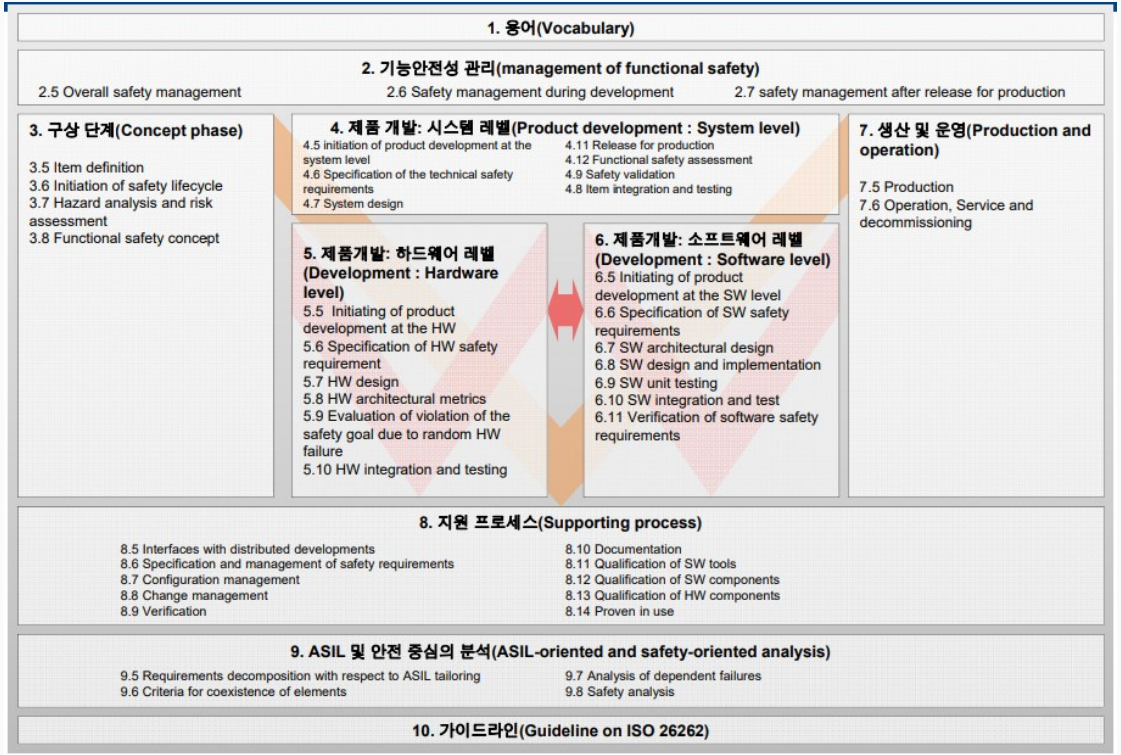
- **등장 배경 및 목적**
  - 자동차 산업이 날로 복잡해짐에 따라 **안전 향상을 위한 관련 규약**들을 증가하려는 노력을 지속적으로 하고 있음. 자동차 업계에서는 전자 시스템을 테스트하고 검증하는 것이 필요하게 됨.

    그러므로 ISO 26262의 목적은 **모든 자동차 E/E 시스템의 안전관련 규약들을 표준화**하는 것.

- **정의**
  - **E/E 시스템**이 일으킬 수 있는 **오작동 행위**를 모두 분석하여 위험원이 될 수 있는 **요인들을 줄여나가는** 과정

ISO 26262

- ISO 26262 표준의 구조



ISO 26262

● ASIL (Automotive Safety Integrity Level)

○ Probability of exposure (발생 확률) + Controllability (통제력) + Severity of failure (심각성)

		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

S : Severity, E : Probability of Exposure, C : Controllability

ISO 26262

● Part 3 - 구상 단계(Concept Phase)

- ○ 개발 품목 정의를 기반으로 Hazard 분석 및 Risk 평가를 통해 ASIL 판정
- ○ 3.5 Item Definition
  - ■ 개발 품목, 다른 품목과의 의존성 정의
- ○ 3.6 Initiation of safety lifecycle
  - ■ 신규개발품목과 현존 품목의 구분, 안전 생명 주기에 대한 활동을 정의
- ○ **3.7 Hazard analysis and risk assessment**
  - ■ **개발 품목의 고장을 발생시키는 위험원 분류 및 식별**
  - ■ **위험원 분석 및 위험 평가서, 안전 목표, 위험원 분석 및 안전평가, 안전 목표에 대한 확인 리뷰 보고서를 제작**
- ○ 3.8 Functional safety concept
  - ■ 안전목표로부터 기능 요구사항 도출 및 각 기능 요구사항을 아키텍처에 할당

ISO 26262

● Part 4 - 제품 개발 : 시스템 레벨(Product development : System Level)

- ○ 4.5 Initiation of product development at the system level
  - ■ 시스템 개발의 각 서브 단계에서의 **기능 안전성 활동**의 **정의**
  - ■ 프로젝트 계획서, 안전 계획서, 개발 품목 통합 및 테스팅 계획서, 확인 계획서, 기능 안전성 평가 계획서
- ○ 4.6 Specification of technical safety requirements
  - ■ 기술적 **안전 요구사항 명세 및 분석** 검증
  - ■ 기술적 안전 요구사항 명세서, 시스템 검증 보고서, 확인 계획서
- ○ 4.7 System Design
  - ■ 개발 품목의 기능 **안전 요구사항** 및 이를 **기반한 시스템 설계** 및 기술 안전성 개념 개발
  - ■ 기술적 안전 개념, 시스템 설계 명세서, 하드웨어 소프트웨어 인터페이스 명세서, 시스템 검증 보고서, 안전 분석 보고서
- ○ 4.8 Item Integration and testing
  - ■ 각 안전 요구사항의 명세와 **ASIL 분류에 따른 테스트** 및 안전 요구사항의 시스템 설계 커버리지 검증
  - ■ 개발 품목 통합 및 테스트 계획서, 통합 테스팅 명세서, 통합 테스팅 보고서

ISO 26262

- **Part 4 - 제품 개발 : 시스템 레벨(Product development : System Level) (con't)**
  - 4.9 Safety Validation
    - 안전 목표 준수 근거 제공 및 안전 목표가 완전히 달성된 것에 대한 **근거 제공**
    - 확인 계획서, 확인 보고서
  - 4.10 Functional safety assessment
    - 개발 품목에 의해 달성된 **기능 안전성 평가**
    - 기능 안전성 평가 보고서
  - 4.11 Release for production
    - 개발 품목의 완전성에 대한 **생산 기준 릴리즈 명세**
    - 생산을 위한 릴리즈 보고서

ISO 26262

- **Part 5 - 제품 개발 : 하드웨어 레벨 (Product development : Hardware Level)**
  - 5.5 Initiation of product development at the hardware level
    - 하드웨어 개발 각 단계에서 기능 안전성 활동 계획 수립
    - 안전 계획서
  - 5.6 Specification of hardware safety requirements
    - 하드웨어 안전 요구사항 명세 및 하드웨어 안전 요구사항 검증
    - 하드웨어 안전 요구사항 명세서, 하드웨어 소프트웨어 인터페이스 명세서(HIS), 하드웨어 안전 요구사항 검증 보고서
  - 5.7 Hardware design
    - 시스템 설계 명세와 하드웨어 안전 요구사항에 따른 하드웨어 설계와 하드웨어 설계 검증
    - 하드웨어 설계 명세서, 하드웨어 안전 분석 보고서, 하드웨어 설계 검증 보고서

ISO 26262

- **Part 5 - 제품 개발 : 하드웨어 레벨 (Product development : Hardware Level)**
  - 5.8 Evaluation of the hardware architectural metrics
    - 하드웨어 아키텍처 측정 항목에 따른 아키텍처 평가
    - 아키텍처 효과성 분석서, 아키텍처 효과성 평가 검토 보고서
  - 5.9 Evaluation of violation of safety goals due to random hardware failures
    - 안전 목표에 위배되는 리스크의 평가 기준 수립
    - 안전 목표 위배 분석, 하드웨어 측정 명세, 안전 목표 위해 평가 리뷰 보고서
  - 5.10 Hardware integration and testing
    - 하드웨어 안전 요구사항의 준수 여부 보장
    - 하드웨어 통합 및 테스팅 보고서

ISO 26262

- **Part 6 - 제품 개발 : 소프트웨어 레벨 (Product development : Software Level)**
  - 6.5 Initiation of product development at the software level
    - 소프트웨어 개발 각 단계에서의 기능 안전성 활동 계획 수립
    - 안전 계획,소프트웨어 검증 계획,설계 및 코딩 가이드라인,툴 적용 가이드라인
  - 6.6 Specification of software safety requirements
    - 소프트웨어 안전 요구사항 명세 및 소프트웨어 안전 요구사항 검증
    - 소프트웨어 안전 요구사항 명세서,소프트웨어 검증 계획서,소프트웨어 검증 보고서
  - 6.7 Software architectural design
    - 소프트웨어 아키텍처 설계 개발
    - 소프트웨어 아키텍처 명세서, 안전 계획서, 소프트웨어 안전 요구사항 명세서, 소프트웨어 검증 보고서
  - 6.8 Software unit design and implementation
    - 소프트웨어 단위 명세 및 구현, 정적 검증
    - 소프트웨어 단위 설계 명세서, 소프트웨어 단위 구현, 소프트웨어 검증 보고서

ISO 26262

- **Part 6 - 제품 개발 : 소프트웨어 레벨 (Product development : Software Level)**
  - 6.9 Software unit testing
    - 소프트웨어 단위의 기능적 수행 확인
    - 소프트웨어 검증 계획서, 소프트웨어 검증 명세서, 소프트웨어 검증 보고서
  - 6.10 Software integration and testing
    - 소프트웨어 개발 품목 통합 및 아키텍처 설계 검증
    - 소프트웨어 검증 계획서, 소프트웨어 검증 명세서, 소프트웨어 검증 보고서, 임베디드 소프트웨어
  - 6.11 Verification of software safety requirements
    - 임베디드 소프트웨어의 소프트웨어 안전 요구사항 수행 확인
    - 소프트웨어 검증 계획서, 소프트웨어 검증 명세서, 소프트웨어 검증 보고서

ISO 26262

- **소프트웨어 검증 단계에서의 ASIL 적용**
  - 6.9 Software unit testing 및 6.10 Software integration and testing 단계에서 ASIL 등급에 따라 검증 방법이 다름

++ : Mandatory, + : Recommended

[표 1] 단위 테스트 방법

테스트 방법		ASIL 등급			
		A	B	C	D
1a	요구사항 기반 테스트	++	++	++	++
1b	인터페이스 테스트	++	++	++	++
1c	결함 주입 테스트	+	+	+	++
1d	자원 사용량 테스트	+	+	+	++
1e	모델과 코드의 백-투-백 비교 테스트 (가능한 경우)	+	+	++	++

[표 2] 테스트 케이스 도출 방법

테스트 케이스 도출 방법		ASIL 등급			
		A	B	C	D
1a	요구사항 분석	++	++	++	++
1b	동등 클래스 생성 및 분석	+	++	++	++
1c	경계 값 분석	+	++	++	++
1d	에러 추정	+	+	+	+

[표 3] 소프트웨어 단위 테스트의 구조 커버리지 지표

구조 커버리지		ASIL 등급			
		A	B	C	D
1a	구문 커버리지	++	++	+	+
1b	분기 커버리지	+	++	++	++
1c	MC/DC (변경 조건/결정 커버리지)	+	+	+	++

6.9 Software unit testing

[표 4] 소프트웨어 통합 테스트 방법

테스트 방법		ASIL 등급			
		A	B	C	D
1a	요구사항 기반 테스트	++	++	++	++
1b	인터페이스 테스트	++	++	++	++
1c	결함 주입 테스트	+	+	++	++
1d	자원 사용량 테스트	+	+	+	++
1e	모델과 코드의 백-투-백 비교 테스트 (가능한 경우)	+	+	++	++

[표 5] 소프트웨어 통합 테스팅의 테스트 케이스 도출 방법

테스트 케이스 도출 방법		ASIL 등급			
		A	B	C	D
1a	요구사항 분석	++	++	++	++
1b	동등 클래스 생성 및 분석	+	++	++	++
1c	경계 값 분석	+	++	++	++
1d	에러 추정	+	+	+	+

[표 6] 소프트웨어 아키텍처 레벨의 구조 커버리지 지표

구조 커버리지		ASIL 등급			
		A	B	C	D
1a	함수 커버리지	+	+	++	++
1b	호출 커버리지	+	+	++	++

6.10 Software integration and testing

ISO 26262

- **Part 7 - 생산 및 운영 (Product and Operation)**
  - 7.5 Production
    - 안전 관련 개발 품목의 생산 프로세스 개발 및 유지
    - 생산 계획서, 생산 통제 계획서, 통제 특정 보고서, 생산 프로세스의 역량 평가 보고서
  - 7.6 Operation, service (maintenance and repair), and decommissioning
    - 고객 정보, 유지보수 지침 명세
    - 유지관리 계획서, 수리 지침, 안전 관련 정보, 필드 조사 지침

ISO 26262

● Part 9 - ASIL 및 안전 중심의 분석(ASIL-oriented and safety-oriented analysis)

- ○ 9.5 Requirements decomposition with respect to ASIL tailoring
  - ■ 높은 ASIL 등급을 요하는 Safety Requirement를 낮은 ASIL 등급의 **여러 개의 요소로 분리**
- ○ 9.6 Criteria for coexistence of elements
  - ■ 중복되는 요소들에 대한 **기준들을 생산**
  - ■ ASIL 등급이 커지는 것을 피할 수 있음
- ○ 9.7 Analysis of dependent failures
  - ■ Safety Requirement를 준수하기 위해 요구되는 품목의 요소들 간의 간섭이 발생하는 단일 사건 혹은 **원인을 찾는 단계**
- ○ 9.8 Safety analysis
  - ■ 구조, 기능 및 행동에 관련한 항목이나 요소에 대한 결함과 **실패의 영향을 설명**
  - ■ 안전 목표 또는 안전 요구사항을 위반할 수 있는 조건 및 원인에 대한 정보를 제공
  - ■ 위험원 분석과 위험 평가중 이전에 고려되지 않았던 새로운 function 혹은 non-funcional 위험원의 식별에 기여

DO-178C

- **DO-178**
  - 항공기, 엔진, 프로펠러, 보조 파워장비 등과 같은 **항공용 시스템과 장비**에 활용되는 **소프트웨어의 인증**을 위한 문서
  - 시스템 안전평가(ARP 4761)를 통해 소프트웨어 등급이 결정됨(Design Assurance Level)

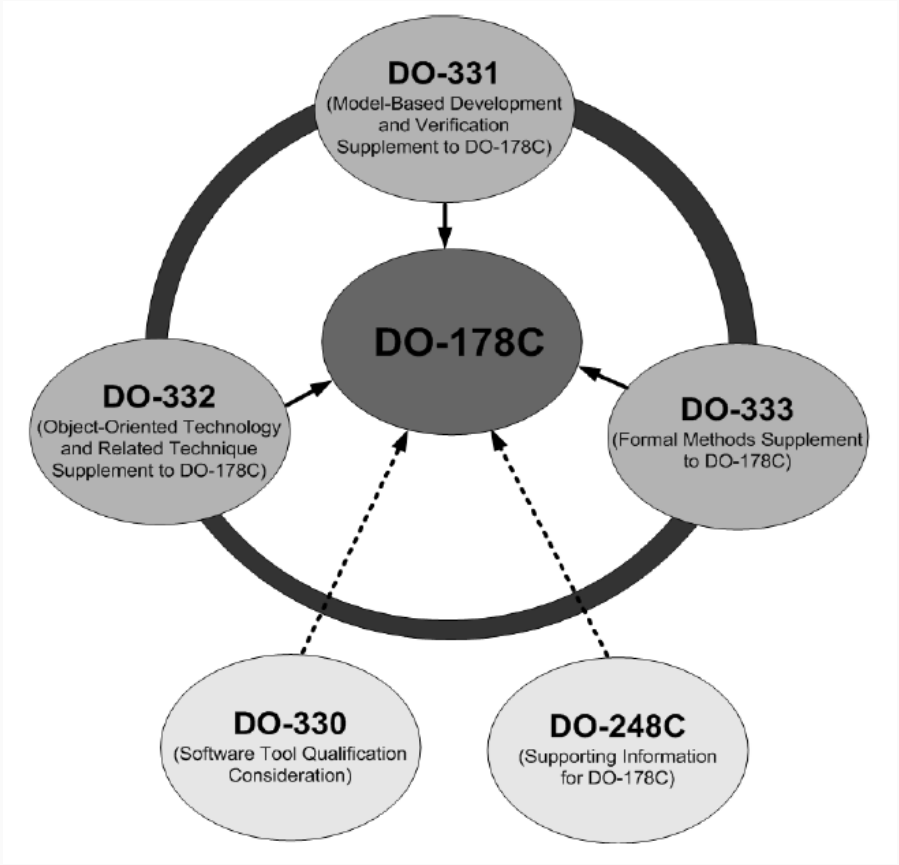
Level	Failure condition	Failure rate	Objectives	With independence
A	Catastrophic	$\leq 1x10^{-9}$	71	33
B	Hazardous	$\leq 1x10^{-7}$	69	21
C	Major	$\leq 1x10^{-5}$	62	8
D	Minor	$1x10^{-5}$	26	5
E	No safety effects	N/A	0	0

- **DO-178C의 등장 배경**
  - 항공 분야에서 발생 하는 사고는 인명 및 물질적 피해가 크기 때문에 안전을 최우선으로 고려해야함
  - 현대 소프트웨어 크기와 복잡성 증가로 인해 DO-178B의 효율성 의문 및 결함 사례 검출 증가
  - 급진한 현대 SW 기술 발전으로 DO-178B에서 다루지 못한 개발, 검증 기술 방법 제시 필요
  - 2012년 개정

- **DO-178C에서 핵심 개정 내용**
  - 최신 소프트웨어 개발 기술 도입(모델 기반 개발 및 검증, 정형기법, 객체지향 기술)
  - DO-178B 개념 명확화

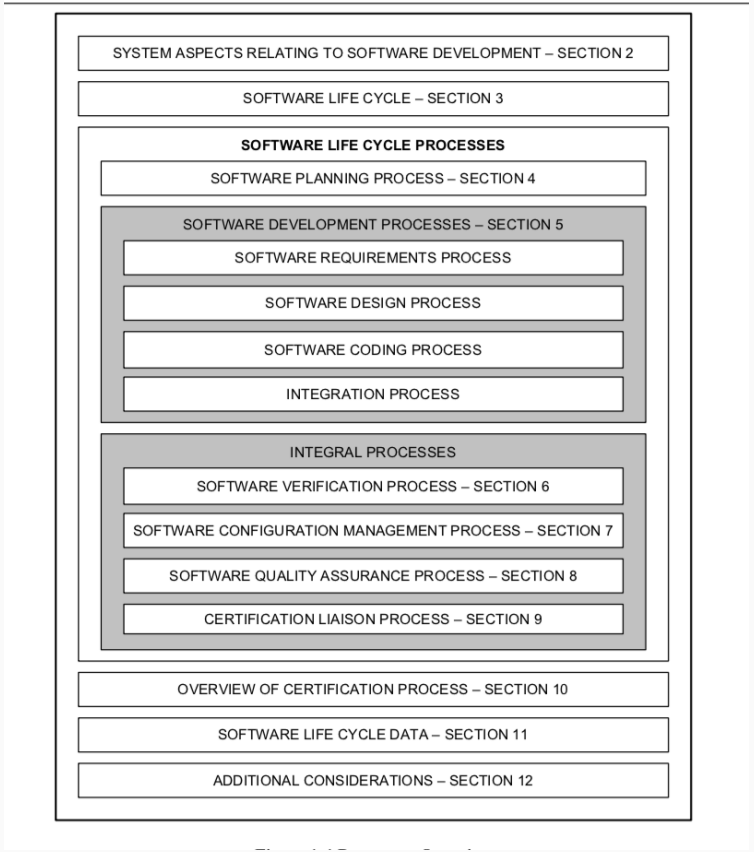
DO-178C

- DO-178C는 기본적으로 DO-178B의 텍스트를 대부분 유지하나 보충 문서들을 추가함
  - DO-330 (소프트웨어 도구 검증 고려)
    - 인증된 항전 소프트웨어 개발에 사용되는 도구에 필요한 도구 적격성 목표를 명확히 하고, 도구 적격성을 위한 특정 지침을 제공
  - DO-331 (모델기반 개발 및 검증)
    - 매핑 문제를 해결하기 위한 모델 기반 개발 및 검증을 위한 보충 문서
  - DO-332 (객체지향 기술 및 관련 기술)
    - 객체지향 기술에 대한 소개와 가이드라인을 혼합하여 기술
  - DO-333 (정형 기법)
    - 소프트웨어의 규격, 개발 및 검증을 위한 수학적 기반 기법



DO-178C

- DO-178C는 소프트웨어 개발을 계획, 개발, 통합 총 3가지의 Life Cycle 로 구분함
  - Software Planning Process - Section 4
  - Software Development Process - Section 5
  - Integral Process - Section 6



DO-178C

- **소프트웨어 계획 프로세스(1)**
  - 소프트웨어 인증 양상 계획 (PSAC, Plan for Software Aspects of Certification)
    - 인증기관이 제안된 소프트웨어 생명 주기가 요구되는 **소프트웨어 치명도 레벨에 상응하는지를 결정**하기 위해서 활용
    - 시스템 개요, 소프트웨어 개요, 인증 고려사항, 소프트웨어 생명 주기, 소프트웨어 생명 주기 데이터, 일정 등을 포함
  - 소프트웨어 개발 계획 (SDP, Software Development Plan)
    - 소프트웨어 개발 프로세스와 활동 그리고 생명 주기를 제시
    - 요구사항, 설계, 코드에 대한 소프트웨어 표준 정의, 소프트웨어 개발 환경 정의
  - 소프트웨어 검증 계획 (SVP, Software Verification Plan)
    - 조직의 책임, 소프트웨어 생명 주기와의 인터페이스, 독립된 검증 방법, 장비 설명과 시험 및 분석 도구의 활용, 이동 조건, 분할화 고려사항 무결성 정의
    - 인증 양상 계획에서 수립한 **치명도 레벨**에 따라 검증 방법의 차이 존재

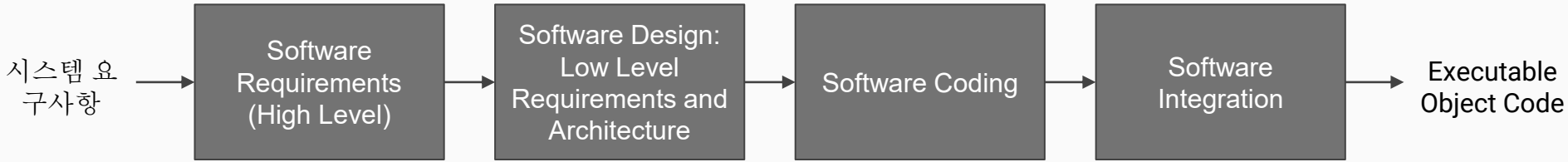
DO-178C

- **소프트웨어 계획 프로세스(2)**
  - 소프트웨어 형상 관리 계획 (SCMP, Software Configuration Management Plan)
    - 형상관리 환경 기술
      - 절차, 도구, 표준, 책임, 형상 식별자, 기준선, 추적 가능성, 문제보고, 변경 통제, 변경 검토, 형상 상태 정의
    - 형상관리 수행 활동
      - 형상 구분, 베이스라인과 추적성, 문제점 리포트, 변경 컨트롤 및 리뷰 등을 포함

  - 소프트웨어 품질 보증 계획 (SQAP, Software Quality Assurance Plan)
    - SQA 환경, SQA 기관과 책임, 문제 보고, 추적, 보정 등의 활동에 관련된 생명 주기 전반에 걸친 SQA 활동과 SQA 프로세스 활동 시점에 대해 정의
      - SQA 환경
        - 범위, 조직의 책임, 인터페이스 표준, 절차, 툴 등을 정의
      - SQA 활동
        - 소프트웨어 생명주기에 대한 리뷰, 감사 등의 품질 보증, 문제점 리포트, 추적, 수정 시스템 활동 기술

DO-178C

- **소프트웨어 개발 프로세스**
  - 소프트웨어 요구사항 (SRP, Software Requirement Process)
    - **시스템 요구사항, 안전성 요건, 정의서**를 통해 **고수준 요구사항** 도출
  - 소프트웨어 설계 (SDP, Software Design Process)
    - **고수준 요구사항**을 통해 **저수준 요구사항**, 소프트웨어 구조 명세 도출
  - 소프트웨어 코딩 (SCP, Software Coding Process)
    - **저수준 요구사항**을 통해 **소스코드** 도출
  - 소프트웨어 통합 (SIP, Software Integration Process)
    - **소스코드, Compile, Linking, Loading 데이터**를 통해 **Executable Object Code, Parameter Data 항목 파일** 도출



DO-178C

● 소프트웨어 통합 프로세스(1)

○ 소프트웨어 검증 프로세스 (SVP, Software Verification Process)

■ 소프트웨어 개발 과정에서 나타날 수 있는 오류를 찾고 테스트를 통해 요구사항을 이행했는지 확인.

■ 소프트웨어 검증 사례, 절차, 검증 결과, 문제보고, 추적 데이터 도출

● DAL : Design Assurance Level
● SC : Statement Coverage
● DC : Decision Coverage
● MC/DC : Modified condition/Decision coverage

DAL	Coverage requirements
Level E	-
Level D	100% requirements coverage
Level C	Level D + data/control coupling and 100% SC
Level B	Level C + 100% DC
Level A	Level B + 100% MC/DC coverage and verification of source-to-binary correlation

표1. Software verification coverage requirements by DAL

Coverage criteria	SC	DC	MC/DC
Every statement in the program has been invoked at least once	✔		
Every point of entry and exit in the program has been invoked at least once		✔	✔
Every decision in the program has reached all possible outcomes at least once		✔	✔
Every condition in a decision in the program has reached all possible outcomes at least once			✔
Every condition in a decision has been shown to independently affect that decision's outcome			✔

표2. Criteria for coverage as defined in DO-178C

DO-178C

- **소프트웨어 통합 프로세스(2)**
  - 소프트웨어 형상관리 프로세스 (SCMP, Software Configuration Management Process)
    - 형상 식별, 기준선 및 추적성, 문제보고, 변경 통제 및 검토, 형상 상태 감시 등의 활동을 통해 결함보고 및 변경과 관련된 활동을 정의하고 관리
    - 형상관리 프로세스에서 할당된 관리 범주에 따라 각 형상 항목들을 관리
  - 소프트웨어 품질 보증 프로세스 (SQAP, Software Quality Assurance Process)
    - 각 소프트웨어 생명 주기 프로세스와 산출된 데이터가 요구사항에 만족되는지, 결함이 검출/평가/추적/해결 되는지, 각 생명 주기 데이터가 인증 요구사항을 따르는지 평가
  - 인증 연계 프로세스 (CLP, Certification Liaison Process)
    - 신청자와 인증기관(Certification Authority)간에 인증 진행을 어떻게 할 것인지 정의하고 협의하는 단계
    - 인증 기관이 Planning, Developement, Verification, Final Review를 수행하고 신청자는 인증기관이 제기한 이슈를 해결.
    - 신청자는 PSAC(Plan for Software Aspects of Certification), SAS(Accomplishment Summary), SCI(Configuration Index)를 제출

자동차 분야 안전성 관련 다른 표준

- FMVSS
  - 자동차, 자동차 안전 관련 부품 및 시스템에 대한 설계, 제작, 성능 및 내구성 요구 사항에 대한 규정.
  - 충돌 방지(100 series), 충돌 안전도(200 series), 충돌 후 생존 가능성(300 series) 및 기타 항목으로 구성
  - 제조업자의 **자가인증 방식**이며 강제인증 및 국가 규격
  - 시장에서 판매되고 있는 제품을 무작위로 선택하여 해당 규격에 대한 최소한의 요건을 시험

- ISO-26262
  - 차량의 전기전자장치에 대한 기능 안전성 관련 요구사항을 정의한 표준
  - 자동차 분야의 특성을 반영해 차량의 전기전자장치의 기능안전성 요건 정의
  - ASIL(Automotive Safety Integrity Level)과 시스템 중심의 안전생명주기 도입

항공 분야 안전성 관련 다른 표준

- RESSAC
  - DO-178C 의 경우 새로운 기술이나 기법들의 도입이 어렵다. 이를 위하여 기존의 복잡한 절차들은 단순화시키고, **시스템과 소프트웨어를 아우르는** 인증 절차
  - **무인기 개발 인증에 과도한 부담을 줄이기 위해 EASA와 FAA가 추진함**
- DO-178C
  - RTCA에서 만들고 FAA, EASA에서 승인
  - **소프트웨어 안전성에 관한 표준**
  - 민간 유인 항공기 및 150kg 이상 무인기의 소프트웨어 개발 표준

기능안전성 관련 국내 법/규정

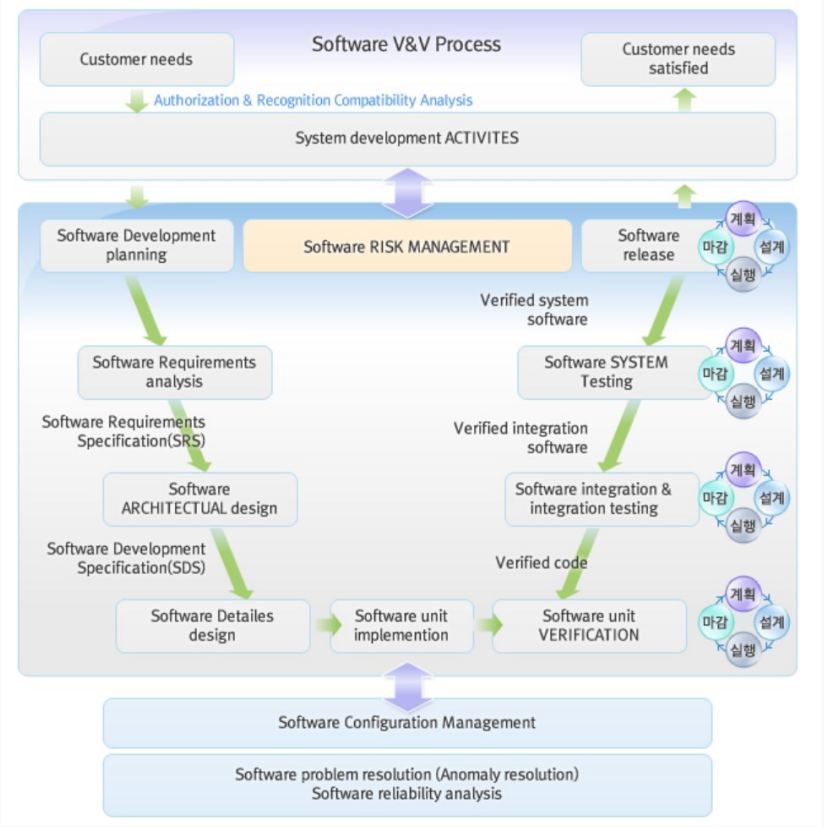
- **국내 자동차 기능 안전성 인증에 관한 법률**
  - 제작자동차 인증 및 검사 방법과 절차 등에 관한 규정
    - 제작자동차의 인증 및 검사 방법과 절차 등을 구체화
    - 시행과 관련하여 필요한 사항을 규정
    - 배출가스 및 소음, 내구성, 자기진단장치 및 배출가스저감장치에 관련한 인증 및 시험 절차임.
    - 자동차 내부 소프트웨어보다 장치, 하드웨어의 안전성에 초점이 맞춰져 있음.
  - 소프트웨어 산업진흥법
    - 소프트웨어 위험분석, 개발 및 검증 방법에 관하여 나와있음
    - 자동차에 특화된 소프트웨어 기능 안전성에 관한 법률은 나와있지 않음

기능안전성 관련 국내 법/규정

- **국내 항공 기능 안전성 인증에 관한 법률**
  - 군용 항공기에 관한 법률
    - 군용항공기 비행안전성 인증에 관한 법률
    - 군용항공기 비행안전성 인증에 관한 법률 시행령
    - 군용항공기 비행안전성 인증에 관한 법률 시행규칙
    - 군용항공기 비행안전성 인증에 관한 업무규정
  - 항공안전법
    - 항공안전법 제 9장 경량항공기 제 108조 안전성인증
    - 항공안전법 제 10장 초경량비행장치 제 124조 안전성인증
  - 항공 소프트웨어 개발 관련 국내 기준
    - 항공법, 항공법 시행령, 항공법 시행 규칙을 기준으로 훈령, 고시, 지침서/안내서 체계로 구성

국내 Certification 기관, 방법 및 현황

- **KTL (Korea Testing Laboratory)**
  - 사용자의 요구사항이 충족되었음을 객관적인 증거의 제공을 통하여 확인 (Verification), 사용자의 요구 및 사용 목적에 일치함을 객관적으로 입증 (Validation) 진행
  - 소프트웨어 전반적인 Life cycle에 걸쳐 수행함
  - IEEE 1012, EME 3100 표준 기반
  - 발전소, 의료, 철도, 항공, 산업플랜트 분야를 대상으로 함
- 이외에도 한국건설생활환경시험연구원, 한국기계전기전자시험연구원, 한국화학융합시험연구원 등의 기관들이 있음



국내외 Certification 기관, 방법 및 현황

- **인증기관**
  - 자동차
    - NHTSA
      - 자동차 제조사에 FMVSS를 준수하게 하는 기관
      - 도난 방지, 연료 효율 들에 대한 규정 제정 및 시험 평가를 수행
  - 항공
    - FAA(Federal Aviation Administration)
      - 미국 교통부 예하 항공 전문 기관
      - 항공수송의 안전 유지를 담당함
      - 항공기 개발, 제조, 수리, 운행 허가 등의 승인 기관

- **교육 기관**
  - ISO-26262
    - SPID, TUV-SUD, BizPeer, SLEXN
  - DO-178C
    - MOASOFT, SLEXN