[ICT응용] 자율주행 시대의 차량의 안정성 확보를 위한 ISO 26262 기능안전 표준

1. ISO 26262 자동차 기능안전 표준개요

ISO 26262는 자동차에 탑재되는 전기전자시스템의 오작동으로 인한 사고방지를 위해 ISO에서 제정한 자동차 분야의 기능안전 국제표준으로 공식 명칭은 Road vehicles – Functional safety 이다. 이 표준이 대두한 배경은 다음과 같다. 첫째, 기존에 전기전자제어시스템을 위한 안전성 표준인 IEC 61508을 자동차 분야에 적용하려 하였지만 IEC 61508은 모든 산업분야에서 범용적으로 적용되는 기능안전 표준이다 보니 자동차 분야의 특성을 반영하는 데 한계가 있었다. 둘째, 자동차 개발 기간은 점점 단축되고 있으며, 신규 차종의 증가 및 전기전자제어시스템의 탑재가 증가하고 있다. 하지만, 현재의 테스팅 기술로는 복잡한 전기전자제어시스템의 안전성을 확인하는데 어려움이 있었다. 이에 독일, 프랑스, 일본 등 10개국 27개 자동차 OEM 및 부품 업체는 기능안전 표준인 ISO 26262를 개발하였고, 2011년 11월 ISO 국제표준으로 공식 발표하였다. 2017년 1월 현재 2nd edition 작업이 진행 중에 있다.

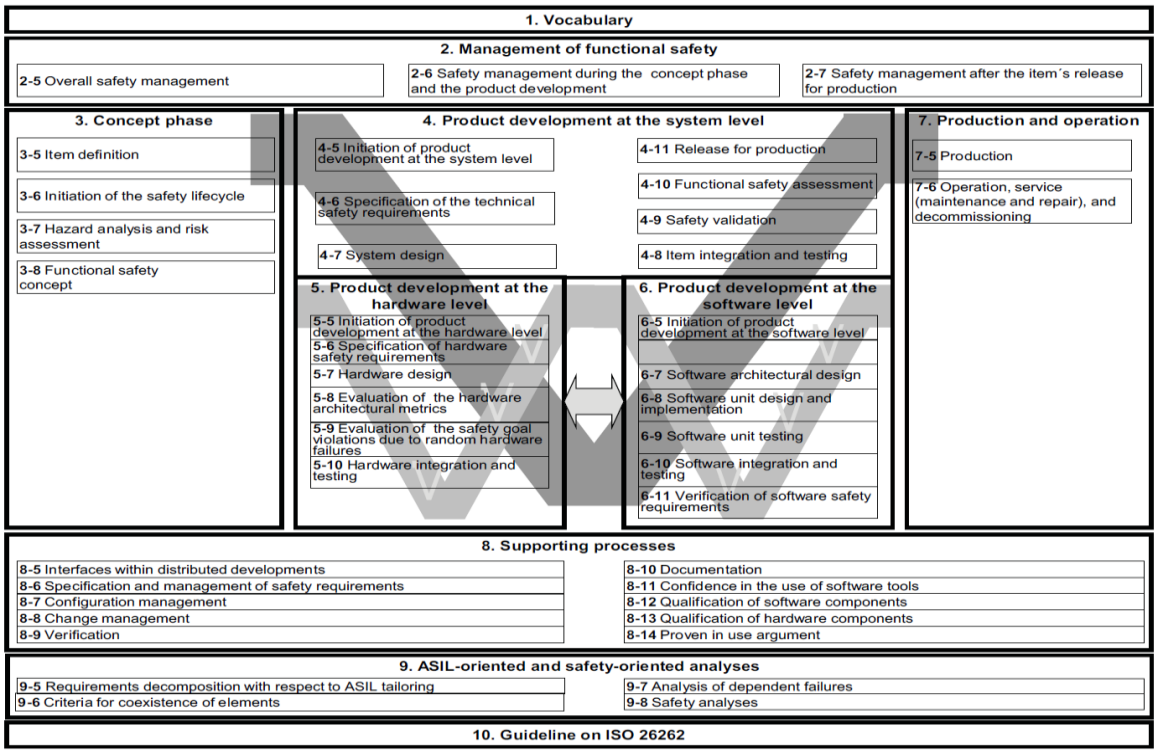
ISO 26262는 3.5t 이하 승용차의 에어백 시스템, 브레이크 제어시스템 등에 적용되며, [그림 1]과 같이 총 10개 파트, 43개 요구사항으로 구성되어 있다. 주요 내용은 다음과 같다.

① 안전 문화 및 조직 체계 수립을 위한 안전관리 요구사항

② 시스템, 소프트웨어, 하드웨어 개발 및 양산/폐기 단계별 절차 및 기법

③ ASIL(Automotive Safety Integrity Level) 기반의 설계, 테스팅, 안전분석 등의 기법 별 적용 기준

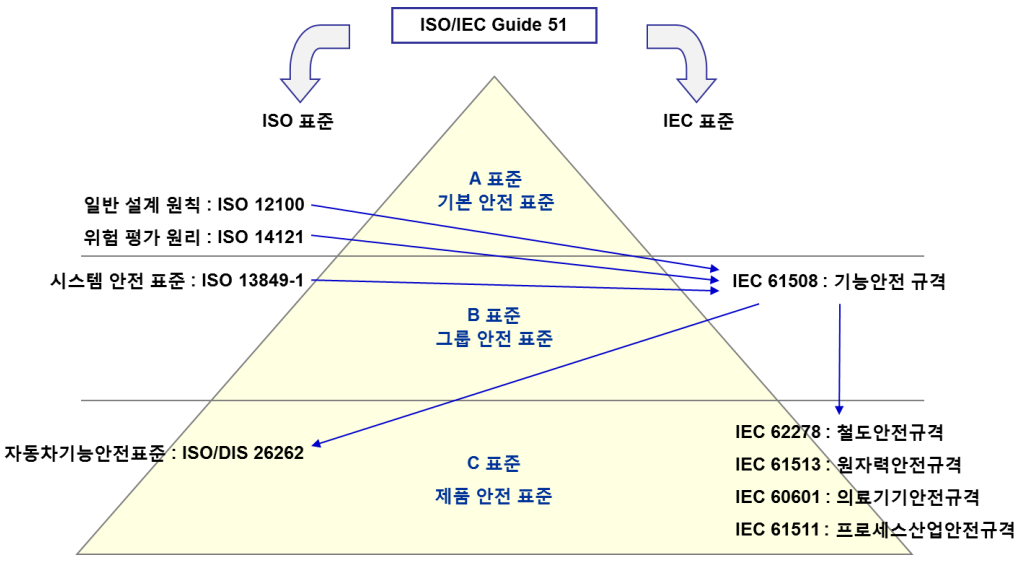
④ 형상관리, 변경관리, 문서화 등의 지원(Supporting) 프로세스



[그림 1] ISO 26262 자동차 기능안전 표준의 구성

2. ISO 26262의 상위 표준인 IEC 61508와 산업별 기능안전 관련 표준

ISO 26262의 상위 표준은 일반 전기전자제어시스템을 위한 안전성 표준인 IEC 61508 이다. 마찬가지로 IEC 61508을 기준으로 [그림 2]와 같이 산업별 특화된 기능안전 표준이 제/개정되고 있다.



[그림 2] IEC 61508과 산업별 기능안전 표준

3. ISO 26262 표준화 동향 및 향후 계획

ISO 26262 표준은 TC22/SC32/WG08에서 다루고 있다. TC22는 Road Vehicles, SC32는 Electrical and Electronic Equipment, WG16은 Functional Safety를 의미한다. ISO 26262 표준의 제정 현황은 다음과 같다.

① 2009년 7월 DIS(Draft International Standard) 배포

② 2011년 4월 FDIS(Final Draft International Standard) 배포

③ 2011년 11월 15일 Part 1~9 국제표준으로 확정

④ 2012년 8월 1일 Part 10 국제표준으로 확정

⑤ 2018년 1월 2nd edition 공식 배포 예정

ISO 26262 표준은 2011년 국제표준으로 제정된 이후 현재 2nd edition 작업이 진행 중에 있다. 2nd edition에서 주요 개정사항은 다음과 같다.

① 차량에 탑재되는 반도체 수의 증가에 따른 반도체 기능안전성 확보를 위해 ISO/PAS 19451 표준 통합 *PAS는 Publicly Available Specification의 약자로, 국제표준 발행 전에 중간단계 임시 규격을 의미함

② 기존 3.5t 이하 승용차에서 트럭/버스/모터사이클로 확대 적용 요구를 반영하여 ISO/PAS 19695 표준 통합

③ 차량 보안(Security)에 대한 중요성 증가에 따른 TARA(Threat Analysis and Risk Assessment) 등 Cyber Security 관련 요건 추가

4. 참고문헌

① ISO 26262 : Road vehicles – Functional safety, ISO, 2011

② 김병철 외 2인, ISO 26262 기본 실무가이드, 한국품질재단, 2012

③ SAFE (Safe Automotive soFtware architEcture) http://www.safe-project.eu/

도성룡 (현대오트론 품질팀 선임, SungRyong.Do@hyundai-autron.com)