

ISO26262 (Road vehicles - Functional safety) 개요

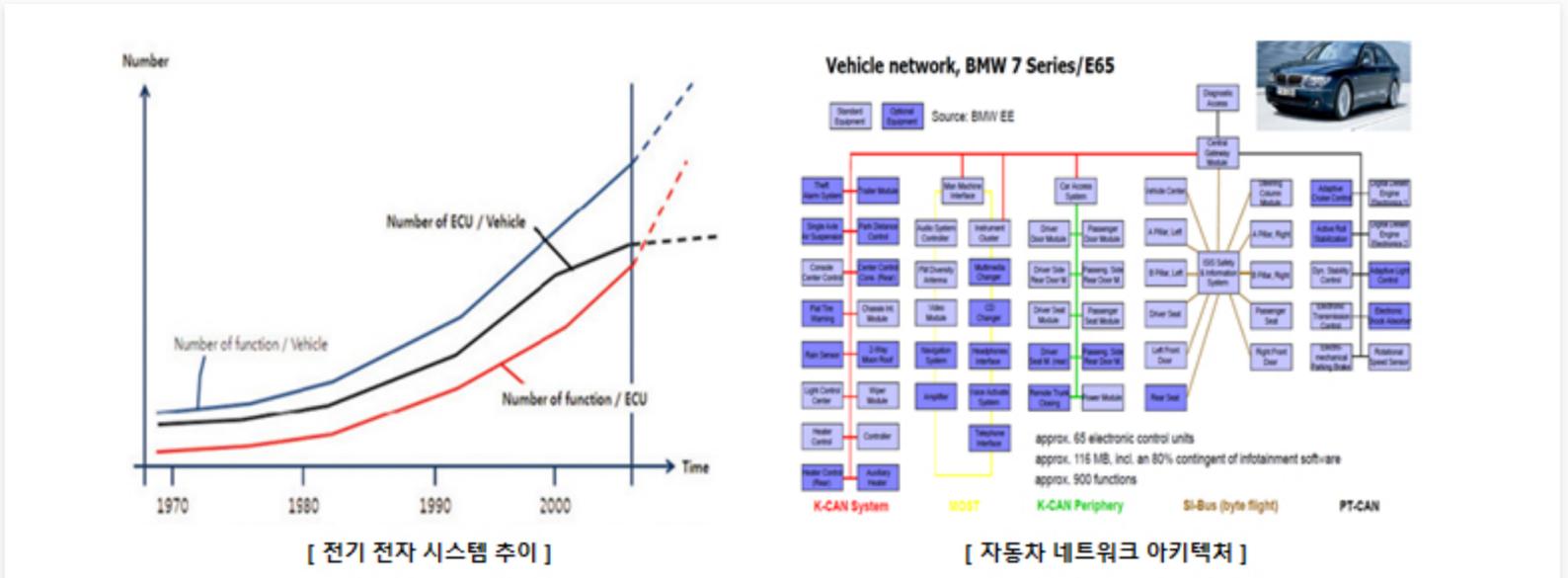
ISO26262 란,

자동차에 탑재되는 전기 전자 시스템(E/E, Electric & Electronic)의 오류로 인한 사고의 방지를 위해서 ISO에서 제정한 자동차 기능안전 국제 규격입니다. ISO 26262는 프로세스 모델과 함께 요구되는 활동, 유 무형의 산출물, 그리고 개발과 생산에 사용되는 기법을 정의합니다. ISO 26262는 2011년도에 1st edition이 발표 되었으며, 2018년에 ISO 26262 2nd edition이 발표될 예정입니다.



ISO26262의 등장 배경

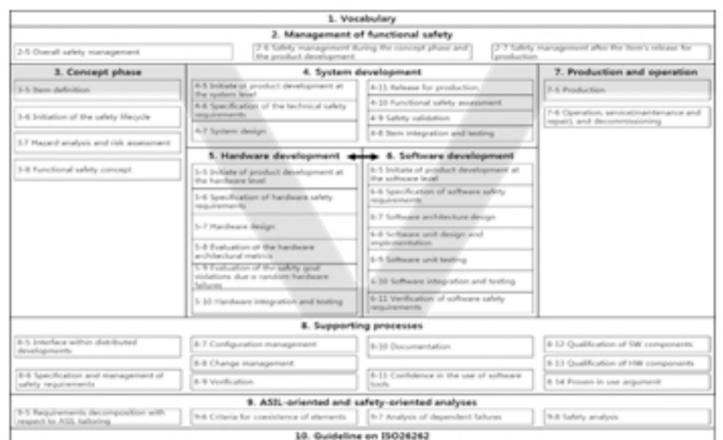
- 자동차 전기/전자 시스템의 복잡도 증가, 친환경 이슈로 인해 전자제어장치(ECU) 증가
- 전기/전자 시스템이 증가하고, 서로 연결(network)되어 동작함에 따라 해당 시스템의 안전 확보가 중요한 문제로 대두됨
- 이에, 자동차 분야의 특성을 반영해 전기/전자 시스템의 기능 안전성 요건 정의 및 ASIL(Automotive Safety Integrity Level)과 시스템 중심의 안전 생명 주기를 도입
- 이동성을 전제로 하는 차량의 특성을 반영하여 제어시스템과 안전 메커니즘 통합
- 시스템 개발 시 리스크 분석과 표준에 따른 기능 안전성 평가 수행



ISO26262의 구조

ISO26262는 V 모델 생명주기 모형을 따르고 있으며, 시스템/하드웨어/소프트웨어 개발이 독립적으로 병행될 수 있는 구조로 구성되어 있습니다.

- Part 1. Vocabulary**
- ISO 26262에 사용된 용어 및 약어에 대한 정의
- Part 2. Management of Functional Safety**
- 기능안전 관련 프로젝트의 관리 활동과 안전관리 요건 정의
- 개발 활동 계획, 조정, 추적
- 조직 차원에서 필요한 안전 문화
- 아이템 개발부터 생산 이후까지 걸친 안전관리 요건 정의
- Part 3. Concept Phase**
- Item 정의, hazard 분석 및 risk assessment를 통한 ASIL 판정
- Safety goal과 safety mechanism 정의
- Part 4. Product development: System**
- 시스템 수준에서의 기술적 요구사항과 시스템 설계, 테스트, 검증, 확인 심사를 정의
- Part 5. Product development: Hardware**
- 시스템 설계 명세를 기반으로 하드웨어 개발, 통합, 검증 등에 대한 요구사항을 정의
- Part 6. Product development: Software**
- 시스템 설계 명세를 기반으로 소프트웨어 개발, 통합, 검증 등에 대한 요구사항을 정의
- Part 7. Product and operation**
- 생산을 위한 계획, 샘플 생산, 양산, 서비스 등에 대한 요구사항 정의 요구사항 정의



- Part 8. Supporting process**
- 안전 요구사항에 대한 관리, 명세 방법에 대한 요구사항 정의
- 형상 관리, 변경 관리, 검증, 문서화 요구사항 정의
- 지원 도구, 재사용 SW/HW의 자격 검증 요구사항 정의
- 실제 사용을 통해 입증된 안전성(Proven in use argument)에 대한 요구사항 정의
- Part 9. ASIL-oriented and safety-oriented analysis**
- ASIL을 분해하는 방법, 안전 관련 구성요소 간의 상호 간섭 정도 및 안전 분석 방법 등을 기술

ASIL(Automotive Safety Integrity Level)의 이해

ASIL은 비합리적인 잔존 위험(unreasonable residual risk)를 방지하기 위해 적용되는 안전 수단(Safety measures)을 의미합니다. Item 혹은 element에 필요한 ISO26262 요구사항을 명시하기 위한 수단으로 사용됩니다.

Risk Classification		Risk Classification		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL A
	E4	QM	ASIL A	ASIL B
S2	E1	QM	QM	QM
	E2	QM	QM	ASIL A
	E3	QM	ASIL A	ASIL B
	E4	ASIL A	ASIL B	ASIL C
S3	E1	QM	QM	ASIL A
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D

