지능형 차량용 반도체의 기능안전 기술 동향

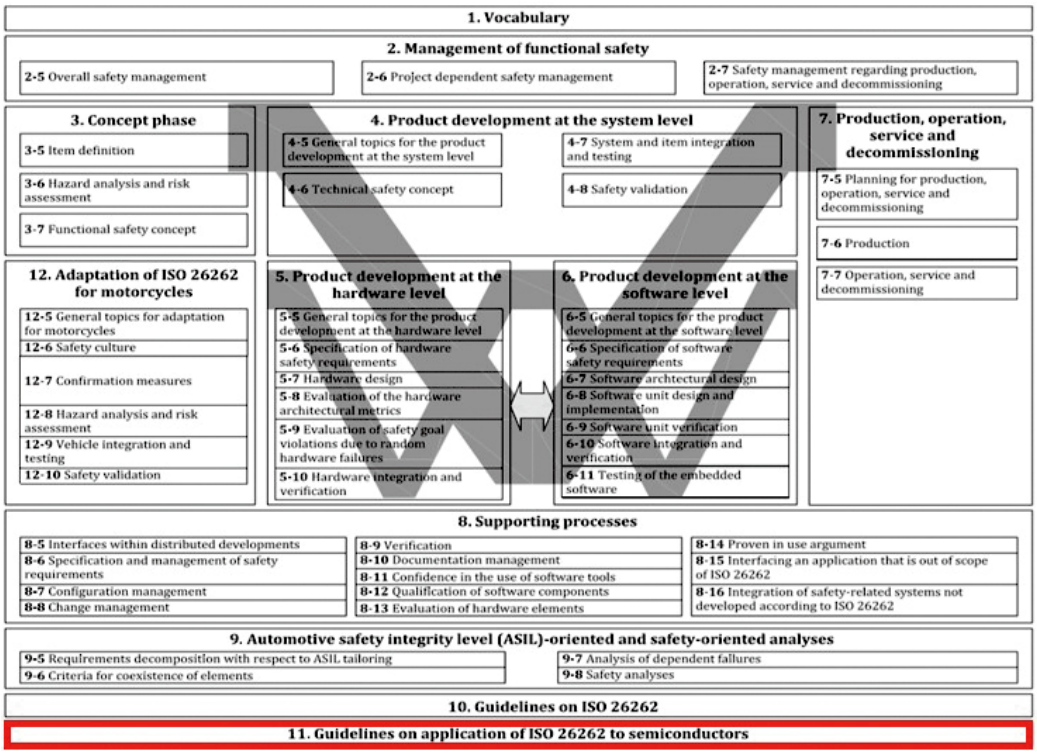
김병철 한양대학교 미래자동차공학과 교수
강성춘 ㈜에이디에스스퀘어 대표이사
김현우 생산기술연구원 서남본부 연구원

1. 머리말

4차 산업혁명이 시작됨에 따라 자동차도 패러다임의 변화가 일어나기 시작했다. 첫 번째는 자동차의 지능화를 이끌고 있는 자율주행차(Autonomous Driving Car), 커넥티드 카(Connected Car), 스마트 카(Smart Car)로 운송수단으로만 여겨졌던 자동차가 운전자, 탑승자가 편하고 안전하게 즐기며 이동하는 수단으로 변화되고 있다. 두 번째는 친환경적인 운송수단으로서 주 동력원으로 화석연료가 아닌 전기에너지를 사용하는 전기자동차, 수소전기자동차의 보급 확대이다.

친환경자동차와 자율 주행 자동차 시장의 성장에 따라 자동차에 사용되는 부품이 기계 중심에서 전기·전자 시스템 중심으로 변화하고 있으며, 자동차 부품의 소형화 및 경량화를 위해 집적 회로 반도체가 전기·전자 시스템의 주요 부품으로 활용되고 있다. 특히 자율 주행 자동차에는 많은 기능을 하나의

[그림 1] 자율주행차의 핵심기술



※ 출처: ISO 26262

[그림 2] ISO 26262:2018 2판의 전체적인 개요

반도체에서 수행하는 지능형 반도체가 필수적으로 사용된다. 이러한 지능형 반도체의 출현은 인공지능 기술과 그래픽 프로세스 유니트(GPU)가 융합한 기술 발전에 힘입어 가능해졌다. 소비자들의 편의성 향상을 위한 IT 융·복합 기술이 자동차 산업의 주요 이슈로 부상함에 따라 전기·전자 시스템의 사용이 급격하게 증가하고 있다.

이처럼 차량 내 전기·전자 시스템의 사용 증가와 복잡화에 따라 안전주행 및 자율주행 시스템의 안전성이 차량 개발의 관건이 되고 있다. 이런 흐름에 맞춰 전기·전자 시스템에 의해 자동차의 안전이 위협받는 것을 방지하고자 자동차 기능안전 국제표준인 ISO 26262 초판이 10개의 파트로 구성되어 2011년 11월 제정되었다.

전기·전자 시스템의 작동불량(오작동)으로 인한 사고를 방지하거나 제어하기 위해 사전에 위험원을 분석하고, 분석된 위험원에 의한 리스크를 평가(HARA, Hazard Analysis and Risk Assessment)하여 리스크의 안전 등급(ASIL, Automotive Safety Integrity Level)을 결정하고, 결정된 안전 등급에 맞는 개발 활동 및 V&V(검증 및 타당성 입증)를 실시하는 것이 ISO 26262에 따른 전기·전자 시스템의 개발 절차이다.

ISO 26262 초판은 유럽, 미국 등 오랜 자동차 역사를 가진 완성차 업체 및 1차 협력사(tier 1), 즉 BMW, 벤츠, 폭스바겐, 르노, 보쉬, TRW, Valeo 주도로 제정되어 3.5톤 미만의 승용차의 안전과 관련된 차량 내 전기·전자 시스템에 적용하였다. 적용 대상으로는 [그림 1]과 같이 자율주행차의 핵심기술인 센서(Sensor), 제어기(ECU), 구동부(Actuator), 네트워크(Network)로 구성되고 소프트웨어와 융합된 최소한 하나 이상의 전자 제어 시스템이다.

[그림 3] ISO 26262:2018 2판의 확대된 적용범위

2018년 12월에는 ISO 26262:2018 2차 개정판이 [그림 2]와 같이 파트 11(반도체에 ISO 26262를 적용 가이드라인)과 파트 12(모터사이클에 대한 적용)의 2개 파트가 추가되어 총 12개 파트로 발행되었다.

[그림 3]에 나타낸 것과 같이 ISO 26262:2018 2판의 적용범위에는 기존 승용차 뿐만 아니라 버스, 트럭을 포함하여 특수 차량을 제외한 모든 차량이 해당된다. 파트 11(반도체에 대한 적용 가이드 라인)은 국제 표준화 기구(ISO)에서 차량용 반도체에 기능안전을 적용하기 위해 2016년 7월 제정한 ISO/PAS 19451을 ISO 26262에 통합한 것이다.

ISO/PAS 19451의 파트 1은 ISO 26262:2018 파트 11로 통합되며, [그림 4]의 파란 글씨 내용이 추가되었다. 파트 2(반도체에 대한 하드웨어 자격 인정의 적용)는 ISO 26262:2018 2판 파트 8의 13절 하드웨어 엘리먼트의 평가(Evaluation)에 반도체가 반영되어 내용이 대폭 변경되었다.

2. ISO 26262 Part 11 차량용 반도체에 ISO 26262 적용 가이드 (Guidelines on application ISO 26262 to semiconductors) 개요

[그림 4] ISO 26262 Part 11 구성과 ISO/PAS 19451에서 추가된 내용 비교

2.1 ISO 26262:2018 Part 11

ISO 26262 1판에서는 파트 10 부록 A에 마이크로 컨트롤러만 언급하고 있을 뿐 자율주행 기능의 핵심 역할을 수행하는 전력 반도체, 메모리 반도체, 각종 센서 등이([그림 4] 참조) 언급되지 않았다. 그러나 2015년부터 개정작업을 시작한 ISO 26262 워킹그룹(국제표준작업팀) 멤버들이 반도체의 중요성을 인식하여 차량용 반도체에 ISO 26262 적용을 논의함으로써 ISO 26262:2018 개정판에 포함되었다.

파트 11은 반도체 부품을 ISO 26262에 따라 개발할 때 적용할 수 있는 권장 사항 및 모범 사례를 제공하여 개발자에게 유익한 지침을 제공한다. 반도체 부품 개발에 ISO 26262를 적용할 때 발생할 수 있는 혼란을 막는 것이 목적이다. 특히 전문가들이 최적 사례 내용을 담아 개발 절차 정보에 대한 가이드라인을 제공한다

[그림 4] 와 같이 ISO 26262 파트 11의 4절과 5절에 주요 적용 항목이 기술되어 있으며, 부록 A~E는 진단 커버리지 평가를 위한 디지털 고장 모드 사용 방법의 예제, 종속결함 분석과 디지털·아날로그·PLD (Programmable Logic device) 컴포넌트에 대한 정량적 사례를 제시한다.

ISO 26262 파트 11의 5절은 반도체 기술 분류에 따라 디지털 컴포넌트와 메모리, 아날로그와 혼합신호 컴포넌트, 프로그램 로직 소자, 멀티코어 컴포넌트, 센서와 트랜스듀서에 대해 4절의 4-1 ~ 4-12를 적용하는 가이드를 제시하고 있다. 4절의 각 항목에 대한 설명은 다음과 같다.

4-1. 반도체 개발 시 기능안전의 적용범위와 고려할 사항에 대한 가이드 제시.

4-2. 반도체 부품을 계층인 파트, 서브파트, 엘리멘터리 서브파트(Elementary subpart)로 나누는 방법에 대한 가이드 제시.

4-3. 반도체에서 발생하는 결함 모델, 에러, 고장 모드의 분류와 고장 모드별 고장률 분포에 대한 가이드 제시 및 반도체 내부의 결함이 에러를 야기해서 반도체의 고장으로 발전하는, 차량수준의 결함-에러-고장으로 전개되는 과정을 통해 반도체에서 고려할 가이드 제시.

4-4. 반도체의 안전 분석 결과를 시스템에 적용하는 가이드 제시. 안전 분석을 강조하면서 시스템, 하드웨어, 소프트웨어 설계 시 귀납적, 연역적 안전분석 방법을 활용하여 요구사항 및 고장형태, 고장에 대한 영향을 검토하거나 검증하도록 요구. 귀납적 방법의 대표적인 예는 FMEA이며, 연역적 방법의 대표적인 예는 FTA, RBD로, 차량용 반도체는 FMEDA(Failure Mode Effects Diagnostic Analysis, 고장형태 영향 진단분석)을 작성하여 고장률에 대한 분석 및 하드웨어 아키텍처 메트릭과 PMHF 평가를 동시에 실시(3장 참조).

4-5. 반도체 IP(Intellectual Property)의 개발 방법 및 IP 개발자와 IP를 사용하는 사용자 측면에서는 무엇을 고려해야 하는지에 대한 가이드 제시. 완성차 OEM은 개발 목표인 차량의 요구사항을 정의하고 공급자에게 개발을 의뢰. 일반적으로 공급업체에서 개발하는 부품들은 요구 사항을 기반으로 개발이 진행되나, 반도체의 경우는 반도체가 사용될 환경을 고려한 요구 사항을 가정하여 개발을 진행하고, 개발시 적용된 요구 사항을 부품 개발업체에 제시하여 차량용으로 사용되도록 하는 경우가 많은데, 이러한 경우를 위하여 ISO 26262에서는 선행 개발 또는 특정 고객을 타깃으로 하지 않는 제품의 개발에도 적용하기 위해 SEooC(Safety Element out of Context)의 개념을 정의하고 가이드.

4-6. 기본 고장률을 추정하는 방법으로 ① 시험을 통한 고장률 산출, ② field에서 수집된 데이터 관찰 및 분석에 의한 고장률 산출, ③ 산업에서 사용하고 있는 신뢰성 데이터 북(IEC/TR 62380, SN 29500, FIDES)을 이용하여 고장률을 산출하는 방법 설명.

4-7. 하나의 원인으로 2개 이상의 부품이 동시에 고장이 발생하거나, 순차적으로 고장이 일어나는 고장을 분석하는 방법인 종속고장 분석(Dependent Failure Analysis) 방법 제시.

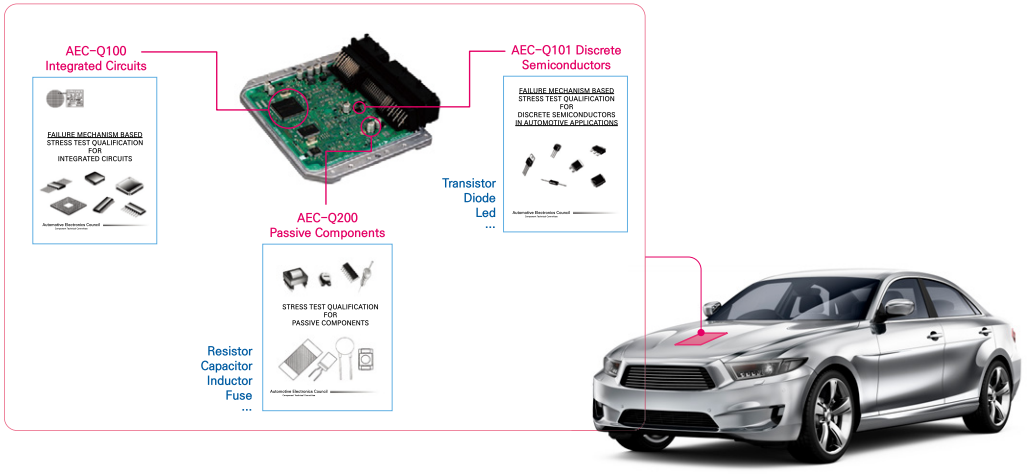
4-8. 결함주입(Fault Injection, FI) 방법을 통해 반도체의 설계에 오류가 없는지를 확인하기 위하여 인위적으로 결함을 유발하여 반도체의 오동작 여부를 검증 및 실증하기 위한 방법과 가이드 제시.

4-9. 생산, 운영에 대한 것으로 반도체가 개발되어 반도체 공정(라인)에서 생산할 때 공정의 관리 방법 제시. 반도체 생산 공정은 안전과 관련이 있으므로 특별 관리에 대한 가이드 제시.

4-10. 협력개발 시 적용할 사항을 제시. 예를 들면 삼성전자, SK 하이닉스와 같이 종합 시스템반도체 회사는 독자적으로 설계 및 생산을 같은 회사내에서 진행할 수 있지만, 팹리스 회사들은 설계는 회사 내에서 진행하고 생산은 공정을 갖춘 반도체 회사에 외주 처리하므로 협력하는 반도체 공정을 제공하는 회사에도 ISO 26262 준수 가이드 제시.

4-11. 확인 대책으로 ISO 26262에서는 반도체 개발 시에 확인 검토, 기능안전 평가 및 기능안전 심사를 하는데 이때 적용해야 할 방법 제시. ASIL 등급에 따른 산출물, 프로세스, 반도체에 대해서 자격을 보유한 독립된 인원에 의해 개발 각 단계마다 확인 검토.

4-12. 하드웨어 통합 및 검증의 명확으로 통합 단계마다 test case, 시험항목, 방법에 대한 기준 도출과 검증, 실증 가이드 제시.



※ 출처: QRT

[그림5] AEC의 주요 평가 표준 –Q 100, 101, 200

2.2 AEC-Q 100

차량용으로 사용되는 반도체 및 전자소자들은 기본적으로 [그림 5]와 같이 신뢰성 요구 사항인 AEC (Automotive Electronics Council) 규격에 의해 검증이 이루어져야 한다. AEC-Q100(집적회로), AEC-Q101(능동소자) 및 AEC-Q200(수동소자)는 자동차에 공급되는 반도체에 대한 신뢰성 평가 절차를 규정한다. 현재 해당 문서들은 사실상 표준(de facto stand-ard)으로 국·내외 자동차 OEM들이 통용하고 있다. 해당 문서들은 차량용 반도체에 대하여 사용 가능한 온도 범위별로 4가지 등급으로 분류하고, 설계, 제조 정보뿐만 아니라 차량용 반도체의 사용 환경을 고려한 주요 불량

〈표 1〉 하드웨어 엘리먼트 평가 구분

	Class I	Class II	Class III
Evaluation	• ISO 26226-5, Clause 10 Hardware integration and testing	• Combination of tests and analysis	• Argument showing that the risk of a safety goal violation or the risk of a safety requirement violation is sufficiently low.
Classifi-cation	• The element has no or only a few states • Failure modes can be evaluated without detailed knowledge, and • No internal safety mechanism	• The element has a manageable state space • Documentation allows assumptions about systematic faults, testing and analyzing freedom from them without detailed knowledge, and • No internal safety mechanism	• The element has a state space • Systematic faults can only be understood and analyzed by knowledge about detailed implementation/development process/production process, or • Has internal safety mechanism
Example	• Resister • Capacitor • Diode • Quartz • Resonator	• Fuel pressure sensor • Temperature sensor • Stand-alone ADC	• Microprocessor • Microcontroller • DSP • Accelerator
ISO 26262-8 Clause 13	• Integrated shall be developed in compliance with ISO 26262	• According 13.4.3 (13.4.3.1 methods for evaluation ~ 13.4.3.6 evaluation report)	• Developed in compliance with ISO 26262 • According 13.4.4

※ 출처: ISO 26262

메커니즘의 검증을 위해 다수의 신뢰성 평가 항목(환경, 수명, 전기적 특성 및 물리)으로 구성되어 있다. 이 규격을 통과한 반도체는 자동차를 비롯한 고 신뢰성을 요구하는 가혹한 사용 환경에서 사용하기에 적합한 신뢰성과 높은 품질을 갖춘 부품으로 인정된다.

3. 차량용 지능형 반도체의 하드웨어 엘리먼트 평가(Evaluation)

ISO 26262 파트 11의 가이드를 참조하여 차량용 반도체를 개발하더라도 결국에는 ISO 26262에 적합하다는 것을 증명하려면 ISO 26262 파트 8의 13절에 따라서 하드웨어 엘리먼트 평가가 실시되어야 한다. 해당하는 전자소자, 센서, 반도체가 〈표 1〉과 같이 Class I, II, III 로 구분되며, ISO 26262를 준수하여 개발, 평가되어야 한다.

하드웨어를 평가하기 위해서는 ISO 26262 표준 준수에 좀 더 체계적이며 효율적인 방법의 하나로 다음의 하드웨어 평가 5단계 절차 및 방법을 제시한다.

- **1단계**: 하드웨어 엘리먼트 및 부품(소자)에 대한 부품목록(Bill Of Material), 회로도, 기능 블록도 등을 통하여 부품(소자) 제조업자로부터의 수명시험 데이터(life test data) 또는 신뢰도 데이터 핸드북(MIL HDBK 217F, IEC/TR 62380, SN 29500, IEC 61709 등)을 기반으로 하여 기본 고장률 추정.
- **2단계**: 고장 형태별(Open, Short, Drift 등) 통계적 고장 비율 결정.
- **3단계**: ISO 26262에서는 하드웨어의 고장에 대해 결함과 위험으로 분류되는 단일점 결함(Single point fault), 잔류결함(Residual fault), 잠재 복수결함(Latent multiple point fault)으로 분류.
- **4단계**: 하드웨어 소자(부품) 및 엘리먼트에 대한 안전 메커니즘의 진단범위를 결정하여 잔류결함, 잠재 복수결함 고장률 계산.
- **5단계**: 안전한 고장의 비율에 대하여 단일점 결함 메트릭(Single Point Fault Metric), 잠재 결함 메트릭(Latent Fault Metric), 랜덤 하드웨어 고장 확률 메트릭(PMHF, Probability Metric of random Hardware Failure)을 계산공식에 따라 계산하여 결과값을 ASIL 등급에 따른 평가 기준과 비교하여 ASIL 만족 여부 결정.
  (사례로 〈표 2〉 PMHF의 평가 기준 참조.)

〈표 2〉 ASIL 등급에 따른 PMHF 평가 기준

ASIL Level	Random hardware failure target values
D	$< 10^{-8}\,h^{-1}$
C	$< 10^{-7}\,h^{-1}$
B	$< 10^{-7}\,h^{-1}$

※ 출처: ISO 26262

4. 맺음말

최근 테슬라 오토파일럿 모드 주행 중 발생한 운전자 사망 사고와 우버 자율택시 시험운행 중 발생한 보행자 사망 사고는 실제 자동차 주행 환경과 상황 분석을 인공지능으로 완벽하게 한다는 것이 불가능하다는 사실을 보여준다.

차량용 지능형 반도체에 자동차 기능안전 ISO 26262를 적용한다는 것은 자율주행시스템의 안전성을 보완하고 높인다는 점에서 의미가 있다. 자율주행 차량 외에도 철도차량, 드론, 농기계, 우주항공, 로봇, 원자력, 화학플랜트, 국방산업 등에서도 고신뢰, 고안전 지능형 반도체 공급을 요구할 것으로 예상된다.

이런 측면에서 ISO 26262를 적용한 하드웨어 평가나 지능형 반도체의 수요가 증가할 것으로 전망되기에 반도체 산업의 패러다임이 바뀌어야 한다. 기능안전 기술이 반영된 지능형 반도체가 부가가치가 높은 반도체로 거듭날 수 있도록 연구를 체계화하고 자동검사 장비들을 상용화하는 것이 바람직하다.

또한 통신에 의해 모든 사물이 연결되므로 사이버 보안도 같이 고려하여 설계되어야 한다. 자동차 보안 관련한 국제표준은 이미 제시돼 있으며, 빠르게 표준화가 진행되고 있다. 기능안전과 사이버 보안은 분리해 이야기할 수 없으며, 자율주행자동차의 안전을 확보하기 위해서는 더 그렇다.

2020년에는 ISO 21434(지상차량-사이버보안 엔지니어링)이 정식으로 국제 표준이 될 것이고, 산업계에서는 기능안전과 사이버보안이 동시에 적용된 반도체를 요구할 것이다.

지능형 반도체는 IoT, 로봇, 인공지능(AI), 4차 산업혁명에 지대한 영향을 줄 것이다. 지능형 반도체에서 중요한 원천기술을 확보하고, 지능형 반도체의 부가가치를 높이기 위해 기능안전과 사이버 보안을 지능형 반도체 기술에 적용하는 것이 필수적이다.

마지막으로 지능형 반도체 평가 기준 및 체계 확립이 중요하다. 여기에 지능형 반도체 제품의 소형화, 통합화, 고속화, 지능화가 추가된다면 새로운 장이 열릴 수 있다.

※ 본 연구는 산업통상자원부 및 한국산업기술진흥원의 시스템산업 기술개발 기반 구축 사업(친환경자동차 부품 클러스터 조성사업)에 의하여 개발중인 "EMS 기능을 갖는 반자율주행 전기차 공용샤시플랫폼"에 관한 기술개발의 연구 결과로 수행되었음(P0000752)

참고문헌

[1] ISO, 'ISO 26262-11:2018, Road Vehicles - Functional Safety - Part 11: Guidelines on application of ISO 26262 to semiconductors', International Organization for Standardization, 2018

[2] 김병철, 강성춘, 차량용 반도체의 ISO 26262 기능안전 기술, 오토저널 (학회지), 42권 2호, pp. 26-32, 2020. 02.

[3] 김병철, 안도석, ISO 26262, ISO/PAS 19451을 준용한 차량용 반도체 기능안전성 평가 방안, 전자공학회지, Vol. 43 No.7, pp. 450-460, 2016. 7.

주요 용어 풀이

- ISO: International Standard Organization 국제 표준 협회
- 기능안전: 전기·전자 시스템의 오동작으로 인한 위험원에 의한 비합리적인 위험이 없음
- 엘리먼트: 시스템, 컴포넌트, 하드웨어 파트들 또는 소프트웨어 유니트들
- 단일점 결함: 하나의 결함으로 인해 안전을 해치는 결과를 초래하는 결함
- 잔류 결함: 결함에 대한 안전 대책을 수립 후에도 제거되지 않는 랜덤 하드웨어 결함
- 잠재 결함: 여러 개의 결함 중에서 안전 대책으로 감지되지 않는 결함
- 안전 메커니즘: 안전을 해치지 않도록 결함 발생을 감지, 억제하거나, 고장을 제어 또는 회피하기 위한 전기/전자 시스템으로 구현된 기술적 해결책
- 랜덤 하드웨어 고장: 하드웨어 사용에 의해 발생하는 통계적 분포를 가진 하드웨어 고장