ISO 26262, ISO/PAS 19451을 준용한 차량용 반도체 기능안전성 평가 방안

김병철
한양대학교
미래자동차공학과

안도석
큐알티(주)

Ⅰ. 서 론

1886년 1월 29일 칼 벤츠가 세계 최초로 자동차를 가지고 특허번호 37435인 "페이턴터 모터바겐"을 발명한 지 135년째인 현재까지 자동차는 수많은 기술을 접목하며 발전해 왔지만, 지금처럼 급격하게 패러다임이 변화되는 때는 없었다. 과거의 자동차는 기계 기능 중심으로 이동 수단 중 하나였지만, 기술이 기하급수적으로 빠르게 발전하고 새로운 기술이 자동차에 접목됨에 따라 오늘날의 자동차는 인간과 자동차 사이의 상호소통을 위해 전기 전자를 중심으로 안전성, 친환경성, 편의성을 기반으로 한 인간중심의 패러다임으로 변화하고 있다. 앞으로 더 이상 인간이 운전하지 않고 자동차가 스스로 운행하고 제어하는 시대가 도래할 것이다. 이제 전 세계는 치열한 자율주행 자동차와 친환경자동차 경쟁으로 달아오를 것이다.

벤츠, BMW, GM, 토요타, 현대차 등의 기존 자동차 기업 위주의 경쟁체제에서 이제는 구글, 애플, 테슬라, 패러데이퓨처 등의 IT와 전기전자 기업들이 보다 경쟁적으로 스마트한 자동차를 개발 중에 있다. 기존 자동차 기업들도 이에 뒤질세라 자동차의 심장을 엔진에서 배터리로 바꾸고, 각종 스마트한 첨단 기술을 적용 중에 있다.

차량의 에너지원이 석탄원료, 전기, 연료전지 등 차량을 움직이기 위한 동력은 앞으로 무엇이 될지 예측 할 수 없으나, 자동차의 부품들을 작동시키기 위해서는 자동차의 동력원에 상관없이 전기로 변환하여야 한다. 전기는 차량에 장착된 전기/전자 시스템을 작동하기 위해서 반드시 필요한 에너지원이다. 더불어 전기/전자시스템의 중심에는 반도체가 있으며, 반도체의 중요성이 강조될 수밖에 없다. 그래서 차량용 반도체에 관련한 표준인 ISO/PAS 19451(ISO/PAS: the International Organization for Standardization(국제표준화기구)/Publicly

Application Specification (공개 활용 표준)이 2016년 7~8월경에 제정될 예정이며, 2018년 2차 ISO 26262를 개정판 Part 11에 반영될 예정이다.

자동차에 IT 기술이 반영되면서 자동차의 안전성 확보를 위해 기능안전과 더불어 중요한 내용이 보안(차량 내/외부 Network)이다. 기능안전과 보안은 떼놓을 수 없는 관계이며 동시에 추진하여야/되어야 한다. 따라서 기능안전의 기술 확보 없이 보안을 추진하는 것은 곧 무너질 모래성을 짓는 것과 마찬가지다. 앞으로 전기/전자시스템의 기반이 될 기술은 기능안전과 보안기술 토대위에서 진행되어야 한다. 아무리 좋은 기능과 성능을 가진 첨단 기술이라고 해도 기능안전과 보안기술이 반영되지 않으면 무용지물이 될 것이다.

ISO/PAS 19451 국제표준이 제정될 경우, 자동차뿐만 아니라 우주항공, 로봇, 원자력, 철도차량, 의료장비, 조선, 화학플랜트, 국방 등의 산업에 사용되는 반도체에 적용이 될 것이다. 앞으로 고객들은 이 표준에 맞는 반도체를 요구하게 될 것이며, 반도체 회사들은 이 국제 표준에 맞도록 개발 및 생산을 하여야 한다.

ISO/PAS 19451은 차량용 반도체 뿐만 아니라 우주항공, 원자력, 철도차량, 의료장비, 조선, 화학플랜트, 국방 등등의 모든 산업에 적용될 것이다.

Ⅱ. 관련 연구

1. ISO 26262 자동차 기능안전 표준의 개요

ISO 26262는 차량용 전기/전자시스템에 적용되는 기능안전(Functional Safety) 국제표준으로, 유럽, 미국 등 오랜 자동차 역사를 가진 완성차 및 1차 협력사(tier 1), 즉 BMW, 벤츠, 폭스바겐, 르노, 보쉬, TRW, 발레오 주도로 2011년 11일 제정되었으며, 안전과 관련한 전기/전자시스템은 ISO 26262 표준을 적용하여야 하며, ISO 26262를 적용하여 전기/전자시스템을 개발하였는데 추후 사고가 일어날 경우, PL법(Product Liability: 제조물책임법)에 의거 법원으로부터 면책이 될 수 있으나, 이를 준수하지 않고 전기/전자시스템을 개발하였는데, 추후 사고가 일어날 경우, 기업은 PL법의 면책이 되지 않고 이에 대한 피해보상 이나 징벌적 책임을 져야 한다. 징벌적 책임의 대표적인 예가 토요타 사태이다.

〈그림 1〉 차량용 전자제어 시스템의 구성

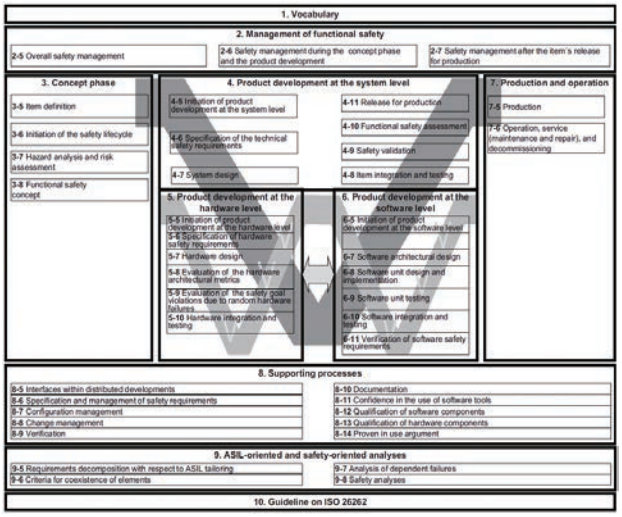
1.1. ISO 26262 적용 대상

ISO 26262의 대상은 〈그림 1〉과 같이 최소한 하나 이상의 전자 제어시스템, 즉 센서(Sensor), 제어기(ECU), 구동모터(Actuator)로 구성되어 있는 경우이며, 3,500kg 이하의 승객용 승용차에 적용된다.

ISO 26262는 전기/전자 시스템에 대해 공통적으로 적용 할 수 있는 안전 기준을 요구하고 있으며, 다양한 부품 개발업체들의 안전 관련 개발 수준을 일괄적으로 관리 할 수 있는 기술 기준도 요구한다. 따라서 전기/전자 시스템의 안전 요구 수준에 따라 ASIL (Automotive Safety Integrity Level)을 정의 하고 있으며 ASIL 등급에 따라 개발, 시험 및 평가 수준이 결정되며, ASIL은 A, B, C, D 등급(D등급이 최고 엄격함)의 4등급으로 이루어지는 개별 E/E(전기/전자) 전장품의 안전무결성 평가 및 개발 기준이 된다[3-4].

1.2. ISO 26262의 구성

ISO 26262 표준은 〈그림 2〉와 같이 Part 1~10으로 구성되어 있으며, Part 1: 용어정의, Part 2: 기능안전 경영시스템, Part 3: 개념단계, Part 4: 시스템 레벨에서의 제품개발, Part 5: 하드웨어 레벨에서의 제품개발, Part 6: 소프트웨어 레벨에서의 제품개발, Part 7: 생산 및 운영, 서비스, 폐기 Part 8: 지원 프로세스, Part 9: ASIL 지향 및 안전성 분석, Part 10: ISO 26262 가이드라인이며 각 Part 별로 상호 관련성에 대하여 매트릭스 구조를 이루고 있으며 V개발 모델(V 사이클) 혹은 V&V



〈그림 2〉 ISO 26262의 구성[1]

(Verification and Validation: 검증 및 유효성확인) 모델이라 한다.

Part 1, Part 10은 ISO 26262 요구사항이 아니지만 가장 기본적으로 이해할 용어와 이해를 돕기 위한 가이드로 사례를 들어 상세하게 설명하였으며, 용어와 가이드를 이해하지 못하면 ISO 26262의 접근이 어렵다. Part 3, 4, 5, 6, 7을 핵심 프로세스(Core Process)라 하며 개발 Item의 개념 및 정의를 필두로 요구사항을 도출하여 설계에 반영하여 Item을 개발하고 양산선행, 양산이관, 양산, 차량운행, 서비스, 폐기에 이르기까지 안전 수명 주기(Safety Lifecycle)를 고려하여야 하며, Part 2, 8, 9는 핵심 프로세스를 지원하기 위해 사전에 갖추어야 할 기본적인 요구사항을 제시하고 있다[4].

2. ISO/PAS 19451 차량용 반도체 표준의 개요

ISO 26262에서 반도체의 내용을 언급한 곳은 Part 10으로 MCU에 대해서 개략적으로 이야기하고 있으나, ISO/PAS 19451은 ISO 26262를 충족하기 위한 반도체 분야에 대해서 보다 세부적으로 언급한 것이다. 완성차나 협력사 등의 자동차 산업에서는 향후의 자동차는 안전, 보안, 친환경과 편의성 방향으로 진행될 것이며, 무엇보다도 중요성한 것은 이것을 구현하기 위해서는 전기/전자시스템의 주축이 되는 반도체가 가장 중요하다는 것을 인식하여 반도체 관련한 표준 ISO/PAS 19451을 제정하게 되었다.

2.1. ISO/PAS 19451의 목적 및 범위

ISO 26262 Part 10의 부록 A에는 microcontrollers만 언급하고 있으며, 다른 종류의 반도체를 포함하지 않고 있어서 이에 대한 혼란이 우려되었다. ISO 26262 WG (Working Group: 국제표준 작업팀) 멤버들이 반도체의 중요성을 인식하여 차량용 반도체에 대한 자격인정을 논의하기 시작하였으며, ISO/PAS 19451의 적용범위는 반도체 부품에 ISO 26262를 적용할 경우, 권장 사항 및 모범 사례를 제공함으로써 사용자 모두에게 유익한 지침을 제공하는 것이며, 목적은 반도체 부품에 ISO 26262를 구현할 때 혼란을 막기 위해 전문가들의 Best practice 내용을 담은 정보의 가이드라인을 제공하는 것이다.[2]

> ISO/PAS 19451의 목적은 차량용 반도체를 ISO 26262에 충족하기 위해 전문가들의 best practice 내용을 담은 가이드라인을 제공하기 위한 것이다.

2.2. ISO/PAS 19451의 구성

ISO/PAS 19451은 Part 1과 Part 2로 구성되어 있으며, Part 1은 아날로그 반도체(Analogue/mixed signal components and ISO 26262), 지적 재산(IP: Intellectual property and ISO 26262), MC(Multi-core components and ISO 26262), PLD(Programmable logic devices and ISO 2626), 기본 고장율(BFR: Base failure rate estimation and ISO 26262), 종속고장 분석(DFA: Semiconductor dependent failure analysis and ISO 26262)을 이야기하고 있다.

Part 2는 ISO 26262에서 요구하는 하드웨어 부품의 자격인정(Qualification of hardware component)과 표준 인정(Standard Qualification)과의 차이점, 왜 자격인정이 필요한지?, 언제 인정을 받아야 하는지? 인정을 할 경우, 무엇을 해야 하는지에 대해 설명하고 있으며, 특히 부품의 자격 인정 시 고려할 사항과 향후 문제점이 발생할 경우, DIA(Development Interface Agreement: 협

력 개발)를 통하여 완성차 혹은 고객과의 해결 방안에 대해서 언급하고 있다.

2.3. ISO/PAS 19451 Part2의 개요

ISO/PAS 19451 Part2 에서는 Part 1 혹은 ISO 26262에 의거 개발된 반도체 혹은 전자부품에 대해서 자격 인정하는 방법을 설명하고 있으며, 표준인정(Standard Qualification)과 ISO 26262 Part 8의 13절에서 언급된 하드웨어의 자격인정 (Qualification of Hardware Components)에 대해서 〈표 1〉와 같이 부품별로 구분하고 있다.

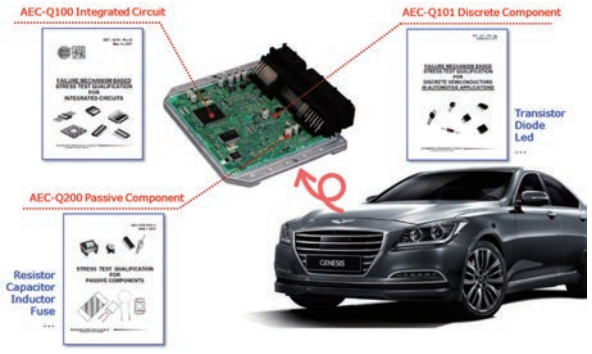
AEC-Q 100, 101, 200 은 시험 및 스트레스(가속시험) 시험을 통하여 반도체 부품 및 전자 부품에 대한 자격 인정을 하는 것이다.

표준인정은 예를 들면 AEC(Automotive Electronics Council) -Q 100, 101, 200 〈그림 3 참조〉 혹은 ISO 16750(Road Vehicles – Environmental conditions and testing for electrical and electronic equipment)에서 제시한 시험 또는 스트레스(가속시험) 시험을 통하여 반도체 부품 및 전자 부품에 대한 자격 인정을 말하는 것이다.

〈표 1〉 ISO 26262 Part 8-13 Table 6 – Qualification, integration and test activities to be conducted depending on the level of hardware part or component[1]

	Safety-related basic HW part	Safety-related intermediate HW part	Safety-related intermediate HW component	Safety-related complex HW component
	(e.g. resistors, transistors…)	(e.g. gray code decoder)	(fuel pressure sensor)	(ECU)
Standard qualification	Applicable	Applicable	- (OEM 요구)	- (OEM 요구)
Qualification in accordance with Clause 13	-	Applicable	Applicable	-
Integration/test in accordance with ISO 26262-5	-	Applicable[a]	Applicable[a]	Applicable
Integration/test in accordance with ISO 26262-4	-			Applicable

[a] means that the hardware part or component will be integrated in accordance with ISO 26262-4 , or ISO 26262-5, or both ISO 26262-5 and ISO 26262-4 depending on its level.



〈그림 3〉 AEC의 주요 평가 표준 –Q 100, 101, 200[10]

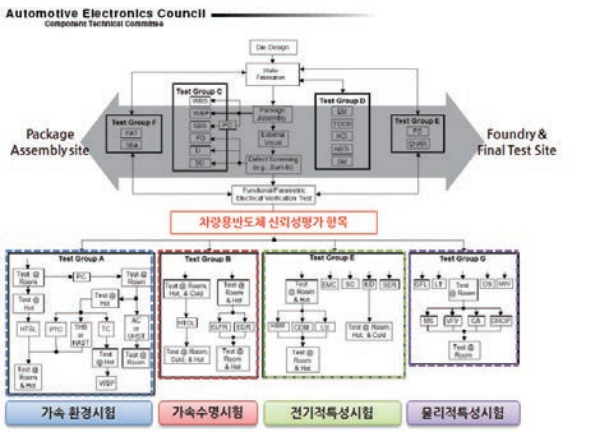
2.3.1 AEC Qualification

최근 국내외 자동차의 차량용 집적회로(IC)에 대한 신뢰성 요구사항이 강화되고 자동차 기능안전성 표준인 ISO 26262가 정식 발효됨에 따라 자동차용 전자제품의 위험 요소에 대한 사전 제거를 요구하고 있다. 이러한 과정에서 완성차 및 Sub-System은 개별적인 단위로 기능과 신뢰성 검증이 요구되며 이중 가장 작은 단위 부품인 차량용 반도체 대한 신뢰성 요구 사항은 AEC(Automotive Electronics Council : 미국 자동차 전자부품 협회) 규격에 의한 검증이 이루어진다.

AEC에서 발행한 주요 문서인 AEC-Q100 (집적회로), AEC-Q101(능동소자) 및 AEC-Q200 (수동소자)에서는 자동차에 공급되는 반도체에 대한 신뢰성 평가 절차를 규정한다. 현재 해당 문서들은 사실상 표준(de facto standard)화 되어 국, 내외 자동차 OEM으로부터 통용되

〈표 2〉 차량용 반도체 등급 분류[7]

등급	동작 온도 범위
Grade 0	-40℃ to +150℃
Grade 1	-40℃ to +125℃
Grade 2	-40℃ to +105℃
Grade 3	-40℃ to +85℃



〈그림 4〉 AEC-Q100 평가 절차 (예)[7]

고 있다.

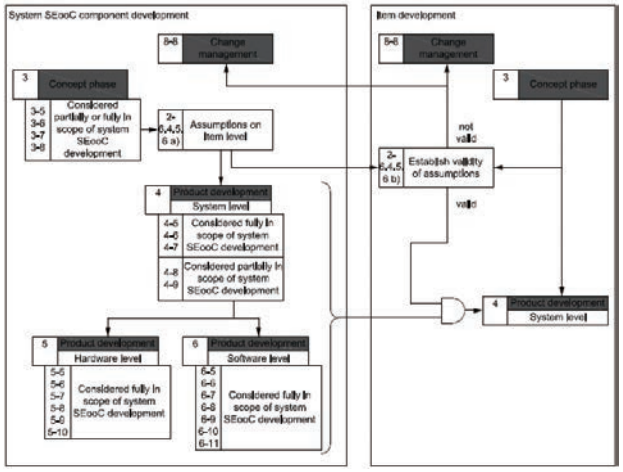
해당 문서들에서는 차량용 반도체에 대하여 사용 가능한 온도 범위별로 4가지 등급〈표 2 참조〉으로 분류하고, 설계, 제조 정보뿐만 아니라 차량용 반도체의 사용 환경을 고려한 주요 불량 메커니즘의 검증을 위해 다수의 신뢰성 평가 항목(환경, 수명, 전기적 특성 및 물리)으로 구성되었다. 이 규격을 통과한 반도체는 자동차를 비롯한 고-신뢰성을 요구하는 가혹한 사용 환경에서 사용하기에 적합한 신뢰성과 높은 품질을 갖춘 부품으로 인정된다. 〈그림 4 참조〉

AEC 규격에서 더 이상 쪼갤 수 없는 최하위 부품인 반도체에 대한 신뢰성을 검증하였다면, ISO 16750 규격 또는 자동차 OEM 규격을 통해 조립된 시스템 및 부품의 신뢰성을 확보하기 위한 전기, 물리, 기후 및 화학 환경스트레스에 대한 평가 요구사항을 규정한다.

Ⅲ. ISO 26262를 충족하는 차량용 반도체 기능 안전성 평가 방법

ISO 26262를 충족하는 차량용 반도체를 개발하고 양산하기 위해서는 ISO 26262 요구사항 뿐만 아니라 여러 가지 기존 산업계에서 활용해온 FMEDA(고장형태영향 진단분석: Failure Mode Effect Diagnostic Analysis), FTA(고장나무 분석: Fault Tree Analysis)를 통한 안전분석이 우선 실시되어야 하며, 통계 데이터를 활용하거나 산업계에서 통용되는 표준을 이용하여 기본 고장률 분석 등을 요구하고 있다. 특히 SEooC 로 개발한다고 가정할 경우, 프로세스의 활동 결과로 나오는 각종 산출물에 대해서 개발하고자 하는 차량용 반도체에 맞게 산출물을 조정하여야 하며, 이들 산출물 중에 safety manual 등의 자료는 전기/전자시스템 설계에 중요 하므로 고객에게 제공되어야 한다.

일반적으로 차량용 반도체를 개발하는 제조사들은 차량의 요구사항을 알지 못한체 역으로 자동차 회사에 요구사항을 제안하는 경우를 SEooC 개발이라고 한다.



〈그림 5〉 ISO 26262 Part 10 – SEooC에 의한 Hardware Component 개발 절차[1]

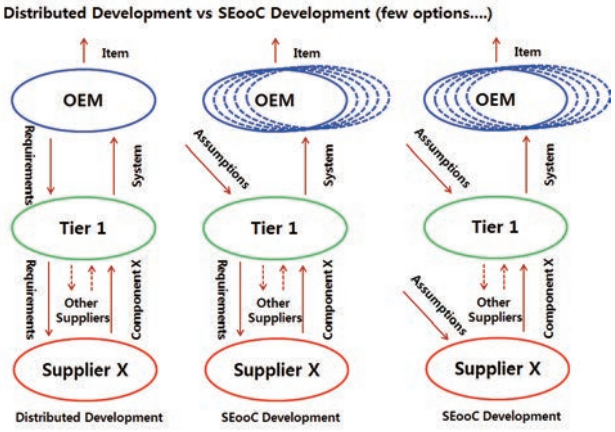
1. 반도체 개발절차

차량용 반도체의 경우는 일반적으로 〈그림 5〉[1]와 같이 개발이 진행된다. ISO 26262에서 요구하는 122개 산출물 중에서도 차량용 반도체에 해당하는 산출물로 tailoring(조정) 선정하여 개발하여야 한다. 차량용 반도체는 Part 5에 따라서 작성된 산출물을 일반적으로 Safety Manual 이라고 지칭하며, 대부분의 반도체 회사들은 Safety Manual을 1차 협력사 혹은 최종시스템을 개발하는 고객에게 제공되고 있다.

AEC에서는 차량용 반도체 개발의 전체 주기에 대한 관리 도구 및 프로세스에 대한 내용을 AEC-Q004 "Zero Defect Guideline"라는 문서로 제공하고 있다. 해당 문서에서 ISO 26262의 요구사항을 다수 고려하고 있으므로 참조하는 것이 효과적이다.[8]

2. SEooC 개발

일반적으로 차량용 반도체를 개발하고 공급하는 대부분의 반도체 제조사들은 차량의 요구사항이나 차량에 장착되는 시스템 요구사항을 모르는 상황에서 하드웨어 요구사항을 충족하도록 개발하거나, 역으로 반도체 회사에서 요구사항을 제안하여 개발하는 경우가 대다수이다.[4] 그래서 ISO 26262에서는 이러한 상황을 고려하여 〈그림



〈그림 6〉 SEooC의 개념

6〉와 같이 SEooC(Safety Element out of Context)의 개념으로 부품이 개발되며, 완성차(OEM)로 부터 요구사항 없이 1차 협력사 (Tier 1) 혹은 반도체 회사에서 요구사항을 만들어 완성차(OEM)에 제안하는 것이다. 만약 완성차로부터 요구사항이 1차 협력사를 통해 반도체 회사로 내려오는 경우에는 SEooC의 개념은 아니고, 고객 요구사항에 의한 개발로 정의된다.

고장율을 추정하는 방법론은 시험에 의한 방법, 데이타의 관찰과 수집에 의한 방법, 신뢰성이 확보된 데이타북을 이용하여 고장율을 산출한다.

3. 고장 형태 및 고장률

ISO/PAS 19451 Part 1에서 고장률을 추정하는 방법으로 3가지를 이야기하고 있다.[2] 1) 시험을 통한 고장률 산출, 2) field에서 수집된 데이터 관찰 및 분석에 의한 고장률 산출, 3) 산업에서 사용하고 있는 신뢰성이 확보된 데이터북(IEC/TR 62380, SN 29500, FIDES)을 이용하여 고장률을 산출하는 방법을 이야기 하고 있으며, 2) 번 방법은 차량용 반도체를 개발하는 회사에서 가장 효과적으로 데이터를 수집하고 분석하는 절차를 정하고 실시하여야 하는 방법이므로 여기에서는 1), 3)번의 방법에 대해서 이야기하고자 한다.

〈표 3〉 반도체의 주요 고장 모드 및 관련 시험을 고려한 가속 모델[7]

구분	관련 시험 항목	가속 모델
Operation	고온동작수명시험 (HTOL)	Arrhenius $A_f = \exp\left[\frac{E_a}{k_B}\cdot\left(\frac{1}{T_u}-\frac{1}{T_t}\right)\right]$
Thermo-mechanical	온도사이클시험 (TC, PTC 등)	Coffin Manson $A_f = \left(\frac{\Delta T_t}{\Delta T_u}\right)^m$
Humidity	고온고습시험 (THB, HAST 등)	Hallberg-Peck $A_f = \left(\frac{RH_t}{RH_u}\right)^p \cdot \exp\left[\frac{E_a}{k_B}\cdot\left(\frac{1}{T_u}-\frac{1}{T_t}\right)\right]$

1) 번의 가장 대표적인 예는 반도체에 대한 가속 스트레스 시험을 실시(e.g. AEC-Q100)하여 고장률을 추정하는 것이다. 반도체의 주요 고장 메커니즘을 고려한 가속 모델은 아래 〈표 3〉과 같이 분류할 수 있다.

일반적인 고장률 추정은 고온동작수명시험을 통한 반도체의 wear-out (장기 열화) 메커니즘을 고려한다. AEC-Q100에서는 차량용 반도체의 동작 환경에 따라 구분된 등급 온도에 231개의 시료를 1,000시간동안 고온동작 환경에 노출시키며, 이를 〈표 3〉의 아레니우스(Arrhenius) 공식에 대입하면 해당 값을 추정할 수 있다.

$$Acceleration\ Factor(AF) = e^{\frac{E_{aa}}{k}\left(\frac{1}{T_{use}}-\frac{1}{T_{stress}}\right)}$$

where:

E_{aa} = apparent activation energy in eV/atom

k = Boltzmann's constant (8.62×10^{-5} eV/K)

T_{use} = use temperature in kelvins

T_{stress} = Test temperature in kelvins

Assumption :

사용온도는 55 °C, 스트레스 온도 125 °C

고장모드 – 게이트 단락*

* Failure Mechanism: Intrinsic breakdown; for gate oxide thickness 〉 4 nm

* Eaa = 0.7 (activation energy reference " JEP122D")

$A_F = \exp[(0.7/k) \times (1/328 - 1/398)] = 77.94$

∴ Accelerated Test time = $A_F \times$ Test Time

= $77.94 \times 1000 = 8.89$ years

AEC-Q100 요건(0 Fail)을 고려, 시험 간 불량 이 없고 지수함수를 따르는 것으로 가정(자유도 = 2, $\chi^2 = 4.61$ @

〈표 4〉 IEC/TR 62380 에서의 부품 고장률 예측 모형[9]

부품 유형	부품 유형
Integrated circuits	Low dissipation wirewound resistors
Power diodes	High dissipation wirewound resistors
Power transistors	Fixed, low dissipation surface mounting resistors
Optocouplers	Inductors and transformers
Optoelectronics	Microwave passive componentspiezo electric components sur face acoustic wave filters
Fixed plastic, paper, dielectric capacitors	Mercury wetted reed relays, low power
Fixed ceramic dielectric capacitors – Class I	Dry reed relays
Fixed ceramic dielectric capacitors – Class II	Electromechanical relays
Tantalum capacitors, solid electrolyte	Industrial relays
Aluminum, non-solid electrolyte capacitors	Switches and keyboards
Aluminum electrolytic capacitor, solid electrolyte	Connectors
Dielectric ceramic	Displays
Thermistors with negative temperature coefficient (NTC)	Solid state lamps
Fixed, low dissipation film resistors	Protection devices
Hot molded carbon composition fixed resistors	Energy devices, thermal management devices, disk drive
Fixed, high dissipation film resistors	Converters

신뢰도 90%)하면, 관련 수식에 따라 다음과 같이 고장율을 구할 수 있다.

$$Failure\ rate\ (\lambda) = \frac{10^9 \times \chi^2}{2 \times AF \times ss \times t}$$

$= 10^9 \times 4.61 / (2 \times 77.94 \times 231 \times 1000) =$
128 FIT(10E−9)

3) 방법중에서도 IEC/TR 62380의 방법론을 이용하여 고장률을 추정하는 것을 소개하면, 2000년에 Union Technique de l'Electricit'e 과 France telecom 에 의하여 전자부품의 신뢰성 예측을 위하여 RDF 2000을 발표하였고, 2004년에 RDF 2000을 내용의 변경 및 갱신없이 그대로 IEC Technical Report 62380으로 이관되었다. IEC/TR 62380에서의 신뢰성 예측 모형〈표 4 참조〉의 특징은 먼저 임무 프로파일(mission profile)을 고려하여 분석하는 것이며, 크게 3부분으로 구성되어 있다. 1) 전자부품 자체의 고장률과 PCB에 마운트 되었을 때의 온도 및 전기적 스트레스 수준을 고려하는 부분 2) 패키지에서 스트레스 환경요소를 고려하는 부분 3) 해당 부품이 다른 시스템(컴퓨터, 통신제품, 철도, 항공전자제품 등등)과 인터페이스 되었을 때의 과부하(overstress)를 고려하는 부분

직접회로(IC)에 대해서 사례를 들어 고장률 산출을 아래와 같은 공식을 적용하며, 기본 고장률을 구하기 위해서 몇 가지 프로파일 및 가정을 통하여 구할 수 있다. 자동차 승객 객실(automotive passenger compartment)용 마이크로 프로세스에 대한 고장률을 예측한다고 가정

〈표 5〉 예) 마이크로 프로세스의 제품정보와 임무 프로파일 정보

$$\blacktriangleright \lambda = \left[(\lambda_1 \times N \times e^{-0.35 \times \alpha} + \lambda_2) \times \frac{\sum_{i=1}^{n}(\pi_T)_i \times t_i}{t_{on} + t_{off}}\right]_{\lambda_{die}} + \underbrace{(2.75 \times 10^{-3} \times \pi_\alpha \times (\sum_{i=1}^{n}(\pi_Q)_i \times (\Delta T_j)^{0.68}) \times \lambda_3)}_{\lambda_{package}} + \underbrace{(\pi_S \times \lambda_{EOS})}_{\lambda_{overstress}} \times 10^{-9}/h$$

공식의 기호에 대한 내용을 정리하면 다음과 같다.
- $(t_{on})_i$: 임무 프로파일의 i 번째 단계 동안 장비 주위의 평균 외기 온도
- $(t_{on})_i$: 해당 부품 근처의 PCB 주위의 평균 온도
- λ_1 : IC를 구성하고 있는 트랜지스터의 기본 고장률
- N : IC를 구성하고 있는 트랜지스터의 개수
- λ_2 : IC의 마스터링 기술과 관련된 고장률
- α : 제조년도 – 1998, 신뢰도 성장의 인자
- $(\pi_T)_i$: 임무 프로파일의 i 번째 단계에서 IC와 연결부위 온도와 관련된 온도 인자로서 연결부위 온도를 사용하여 Arrhenius 법칙에 의하여 구함
- τ_i : 임무 프로파일의 i 번째 단계에서 IC와 연결부위 온도와 관련된 동작시간의 비율
- τ_{on} : IC의 총 동작기간 비율 $(\tau_{on} = \sum_{i=1}^{n} \tau_i)$
- τ_{off} : IC의 비동작 기간의 비율 $(\tau_{on} + \tau_{off} = 1)$
- π_Q : 회로기판과 패키지 사이의 온도 차에 따른 열팽창 영향 인자로서 회로기판의 재질과 패키지의 재질에 따른 열팽창 계수를 표에서 구하여 Coffin-Manson 법칙에 의하여 구함
- ΔT_j : 임무 프로파일의 i 번째 단계에서 열변동(온도변화)의 크기
- $(\pi_N)_i$: 임무 프로파일의 i 번째 단계에 대한 연간 사이클 횟수에 비례하는 영향 인자
- π_α : 다른 시스템과 인터페이스 유무를 나타내는 인자, $\pi_\alpha = 1$(인터페이스 됨) 혹은 $\pi_\alpha = 0$(인터페이스 안됨)
- λ_{EOS} : 다른 시스템과 인터페이스 되었을때의 과부하(overstress)에 따른 고장률

제품 정보	임무 프로파일 정보
-. 제조년도: 1999년 -. 마이크로 프로세스 종류: Silicon MOS Standard circuit; Digital circuit, Micros, DSP -. 트랜지스터 개수: 1,500,000 개 -. 공급전력: 0.5 W -. 패키지 종류: QRP (Epoxy: Plastic package). 핀수: 80 pins -. 서브스트레이트 종류: FR4(Epoxy Glass) -. 대류방식: 자연 대류 (natural convection) -. 외부 시스템과 인터페이스: 없음	-. 차량 연간 운행 시간: 500 시간/년 → 운행시간의 2/3는 낮시간에 운행(333시간), 운행시간의 1/3은 밤시간에 운행(167시간) -. 1년중 30일은 운행하지 않음 -. 운행기간(500 시간) 중 온도 변화에 따른 임무 프로파일 • Temp 1 : 이 부품 근처의 PCB 주위 온도 = 27 ℃, 기간=50시간/년 • Temp 2 : 이 부품 근처의 PCB 주위 온도 = 30 ℃, 기간=400시간/년 • Temp 3 : 이 부품 근처의 PCB 주위 온도 = 85 ℃, 기간=50시간/년 -. 연간 사이클 횟수(운행 중 시간당 4회 on-off 함, 운행하지 않을 때에는 하루 1번) • 낮시간 운행의 연간 사이클 횟수 : 1340회/년 • 밤시간 운행의 연간 사이클 횟수 : 670회/년 • 운행하지 않을 때의 연간 사이클 횟수 : 30회/년 -. 장비 근처 평균 외기 주위온도 • 낮시간 운행시 장비 근처 평균 외기 주위 온도 : 15℃ • 밤시간 운행시 장비 근처 평균 외기 주위 온도 : 5℃ • 운행하지 않을 때의 장비 근처 외기 주위 온도의 최대, 최소 차이에 대한 사이클링 평균온도 : 10℃

〈표 6〉 ISO 26262 안전 분석 방법[1]

Methods	ASIL A	ASIL B	ASIL C	ASIL D
1 연역법 Deductive analysis [a]	0	+	++	++
2 귀납법 Inductive analysis [b]	++	++	++	++

[a] Deductive analysis methods include FTA, reliability block diagrams(RBD), ishikawa diagram.
[b] Inductive analysis methods include FMEA, ETA, Markov modeling.

할 경우, 마이크로 프로세스의 제품정보와 임무 프로파일 정보는 〈표 5〉와 같다.

$$\lambda = ((3.4 \times 10^{-6} \times 1500000 \times e^{-0.35 \times 1} + 3.4) \times (1.21 \times 0.0057 + 1.33 \times 0.0457 + 5.5 \times 0.0057) + (2.75 \times 10^{-3} \times 1 \times ((1340)^{0.76} \times (31)^{0.68} + (670)^{0.76} \times (41)^{0.68} + (30)^{0.76} \times (10)^{0.68}) \times 10.2) + (0 \times \lambda_{eos})) \times 10^{-9} = 121.679 \times 10^{-9}$$

4. 안전 분석 (Safety Analysis)

ISO 26262에서는 안전 분석을 강조하고 있으며 시스템, 하드웨어, 소프트웨어 설계 시, 안전 분석 시에 귀납적, 연역적 방법을 활용하여 요구사항 및 고장형태, 고장에 대한 영향을 재검토하거나 검증하도록 요구하고 있다. 귀납적 방법의 대표적인 예는 FMEA이며, 연역적 방법의 대표적인 예는 FTA, RBD 이다〈표 6〉. 특히 차량용 반도체는 FMEDA(Failure Mode Effects Diagnostic Analysis: 고장형태 영향 진단분석)[3, 5]을 작성하여 고장율에 대한 분석 및 하드웨어 아키텍처 메트릭과 PMHF

〈표 7〉 반도체의 FMEDA 보고서 사례

function	failure mode	effect	distribution failure mode	failure rate (128 FIT)
CAN Transmitter	Does not transmit CAN	No CAN messages are transmitted	12.99%	16.62566
	Permanent dominant not detected	CAN Bus not relased	0.13%	0.16794
CAN Receiver	Does not wake from sleep on CAN message	Device does not start up, CAN message not received	6.13%	7.84384
	Does not receive CAN message	CAN message not received	9.04%	11.5697
	Permanent dominant not detected	Rxd Pin not released	0.15%	0.19609
Thermal Shutdown	Device stuck in shutdown	No Transmitter output, No CAN communication	3.95%	5.0496
	Device enters thermal shutdown	Transmitter shuts down, CAN communication interrupted	3.95%	5.0496
Pins	Vdd internally open or shorted to Vss	Device will not start up	15.77%	20.1843
	CANH internally open or shorted to Vdd or Vss	No CAN communication	15.16%	19.408
	CANL internally open or shorted to Vdd or Vss	No CAN communication	12.13%	15.5264
	Split internally open or shorted to Vdd to Vss	No CAN communication	12.74%	16.3027
	TXD is internally open or shorted to Vdd or Vss	No CAN message transmitted	1.21%	15.526
	RXD is internally open or shorted to Vdd or Vss	No CAN message received	1.21%	15.526
	STBY shorted to Vdd	Device will not wake up	1.21%	15.526
	STBY shorted to Vss	Device will not enter Standby Mode	1.21%	15.526
Mode Control	Device does not exit POR	No CAN communication	0.44%	0.5683
	Device does not exit standby mode	No CAN communication	0.89%	11.366
	Device does not go from normal to standby mode	Higher current consumption	0.89%	11.366

평가를 동시에 실시하고 있으며, FMEDA 보고서 사례를 〈표 7〉에서 참조할 수 있다.

〈표 8〉 ISO 26262 Part 5의 표 D.6 – 휘발성 메모리(Volatile memory) 진단 커버리지[1]

안전 메커니즘	구현 가능한 기본 진단 커버리지	비고
RAM 패턴 시험	중 (90%)	끼임 고장에 대한 높은 커버리지. 연결된(linked) 고장을 위한 커버리지 없음. 인터럽트 보호(interrupt protection)하에서 동작시키기에 적합
RAM March 시험	고 (99%)	연결된 셀 커버리지에 대한 쓰기 읽기 순서에 따름. 일반적으로 동작중에는 적합하지 않은 시험.
패러티 비트	저 (60%)	–
오류 검출 정정 코드 (EDC)를 사용한 메모리 모니터링	고 (99%)	유효성은 부가된 비트 수에 따름. 오류 정정을 위해 사용가능
블록 복제	고 (99%)	공통 고장형태는 진단 커버리지를 감소시킬 수 있음.
동작(running) 체크섬/CRC	고 (99%)	서명의 유효성은 보호될 정보의 블록 길이와 관련한 다항식에 따른다. 체크섬 계산 동안 체크섬 결정에 사용되는 값들이 변경되지 않도록 주의해야 함.

반도체의 주요 고장 모드 및 관련 시험을 고려한 가속 모델을 이용하여 기본 고장율이 128 FIT(128×10^{-9}) 일 경우, FMEDA 분석을 통하여 고장모드별 고장분포를 알아냄으로 고장모드별 고장율을 구할 수 있다.

〈표 9〉 ISO 26262 Part 5의 표 D.7 – 아날로그와 디지털 I/O 진단 커버리지[1]

안전 메커니즘	구현 가능한 기본 진단 커버리지	비고
온라인 모니터링에 의한 고장 검출 (디지털 I/O)a	저 (60%)	고장 검출 진단 커버리지에 따름
시험 패턴	고 (99%)	패턴 타입에 따름
디지털 I/O를 위한 코드 보호	중 (90%)	코딩 타입에 따름
멀티 채널 병렬 출력	고 (99%)	–
모니터링된 출력	고 (99%)	진단 시험 간격 내 데이터흐름이 변하는 경우에 한 함.
입력 비교/선택 (voting) (1oo2, 2oo3 또는 더 나은 리던던시)	고 (99%)	진단 시험 간격 내 데이터흐름이 변하는 경우에 한 함.

5. 안전 메카니즘(Safety Mechanism)과 진단범위 (Diagnosis Coverage)

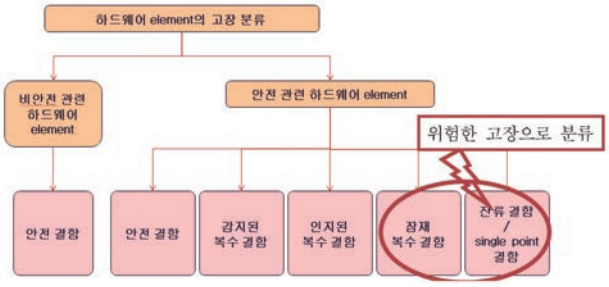
안전 메커니즘의 진단범위를 산출하는 근거를 제공하는 ISO 26262-5, 부속서 D의 표 D.1 ~ D.14가 이를 산정하는 출발점으로 유용하게 사용될 수 있다. 반도체에 해당되는 ISO 26262-5, 부속서표 D.6, D.7 일부를 〈표 8〉 〈표 9〉 에 명기하여, 안전 메카니즘의 진단범위의 이해를 돕기위해서 진단 커버리지를 저, 중, 고로 표시하여 저는 60%, 중은 90%, 고는 99%의 진단범위를 가진다. 해당되는 것을 기술이나 방법론을 명기하고 있다.

6. 하드웨어 아키텍처 메트릭 및 PMHF 평가[3-6]

차량용 반도체를 설계한 후에 ISO 26262 Part 5에 의거하여 반도체 설계가 잘 되었는지의 여부를 정량적으로 평가하여야 한다. 하드웨어의 우발고장(Random Hardware Failure)에 대처하기 위해 ISO 26262 에서는 하드웨어 아키텍처 메트릭(단일결함, 복수 잠재결함) 평가, 이를 보완하기 위하여 안전 목표를 위반하는 평가 PMHF (Probability Metric of Random Hardware Failure), FRC(Failure Rate Class) 방법이 있다. 하드웨어 아키텍처 메트릭 평가 방법은 필히 수행되어야 하며, PMHF와 FRC 평가 중 최소한 하나 이상을 선택하여 평가하여야 한다. 여기에서는 하드웨어 아키텍처 메트릭과 PMHF 평가에 대해서 설명하고자 한다.

ISO 26262와 ISO/PAS 19451에서는 귀납적, 연역적 방법론인 FTA, RBD, FMEA 등의 안전 분석 기법을 사용하여 기능 및 안전 요구사항, 고장형태, 고장의 영향을 파악하고, 재 검토 및 검증을 요구하고 있다.

하드웨어를 평가하기 위해서는 ISO 26262표준에서는 정해진 방법 및 순서는 언급하지 않으나 보다 체계적이며 효율적인 방법의 하나로 아래의 하드웨어 평가 5 단계 절차 및 방법을 제시하고자 한다.



〈그림 7〉 하드웨어 element의 고장 분류

1단계 : 설계 엔지니어와 인터뷰 및 하드웨어 엘리먼트 및 부품(소자)에 대한 BOM(Bill Of Material), 회로도, 기능블럭도 등을 통하여 부품(소자) 제조업자로부터의 수명시험 데이터(life test data) 또는 고장모드 핸드북(MIL HDBK 217F, IEC/TR 62380, SN 29500, IEC 61709 등등)을 기반으로 하여 기본 고장률 추정.

2단계 : 고장형태별(Open, Short, Drift 등등) 통계적 고장 비율결정.

3단계 : ISO 26262에서는 하드웨어의 고장을 〈그림 7〉과 같이 분류하고 있으며, 안전측으로 분류되는 결함과 위험으로 분류되는 단일결함(Single point fault), 잔류(Residual fault)결함, 잠재 복수결함(Latent multiple point fault)으로 나눈다. 안전관련 부품여부를 확인 및 고장을 분류(안전한 고장, 단일결함, 잔류결함, 잠재복수결함) 〈그림 7〉 하드웨어 element의 고장 분류 참조.

4단계 : 하드웨어 소자(부품) 및 엘리먼트에 대한 안전메카니즘의 진단범위를 결정하여 잔류결함, 잠재복수결함 계산.

5단계 : 고장률을 합계하여 단일(잔류)결함은 계산공식 ①에 따라 계산하여 결과값을 〈표 10〉 ASIL 등급에 따른 single point fault metric 평가 기준과 비교하여 ASIL 만족 여부 결정.

잠재복수결함은 공식 ②에 따라 계산하여 결과값을 〈표 11〉 ASIL 등급에 따른 latent faults metric 평가 기준 기준과 비교하여 ASIL 만족 여부 결정.

PMHF는 안전관련 부품 및 엘리먼트의 위험으로 분류되는 고장의 총 고장률을 합산하여 공식 ③에 따라 계산하여 결과값을 〈표 12〉 ASIL 등급에 따른 PMHF 평가 기준 기준과 비교하여 ASIL 만족 여부 결정.

$$\text{Single Point Fault metric} = 1 - \frac{\sum_{\text{safety-related HW elements}} (\lambda_{SPF} + \lambda_{RF})}{\sum_{\text{safety-related HW elements}} \lambda} = \frac{\sum_{\text{safety-related HW elements}} (\lambda_{MPF} + \lambda_{S})}{\sum_{\text{safety-related HW elements}} \lambda}$$

계산공식 ①

〈표 10〉 ASIL 등급에 따른 single point fault metric 평가 기준[1]

	ASIL B	ASIL C	ASIL D
single point fault metric	≥ 90 %	≥ 97 %	≥ 99 %

$$\text{Latent Fault metric} = 1 - \frac{\sum_{\text{safety-related HW elements}} (\lambda_{MPF\_L})}{\sum_{\text{safety-related HW elements}} (\lambda - \lambda_{SPF} - \lambda_{RF})} = \frac{\sum_{\text{safety-related HW elements}} (\lambda_{MPF\_DP} + \lambda_S)}{\sum_{\text{safety-related HW elements}} (\lambda - \lambda_{SPF} - \lambda_{RF})}$$

계산공식 ②

〈표 11〉 ASIL 등급에 따른 latent faults metric 평가 기준[1]

	ASIL B	ASIL C	ASIL D
latent fault metric	≥ 60 %	≥ 80 %	≥ 90 %

$$PMHF = \sum \lambda_{SPF} + \sum \lambda_{RF} + \sum \lambda_{MPF}$$

계산공식 ③

〈표 12〉 ASIL 등급에 따른 PMHF 평가 기준[1]

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

Ⅵ. 향후 연구 및 결론

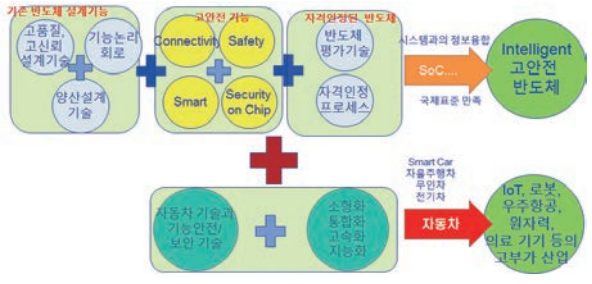
지금까지 ISO 26262 및 ISO/PAS 19451에 준용하여 차량용 반도체의 기능안전성을 평가하는 과정을 살펴보았다. 향후 2018년 ISO 26262 개정판에는 ISO/PAS 19451이 ISO 26262 Part 11 에 반영될 예정이며, 철도차량, 우주항공, 로봇, 국방 산업 등에서도 고신뢰, 고안전용 반도체 공급을 요구할 것으로 예상된다. 따라서 ISO/PAS 19451에 맞춰 하드웨어 평가 및 자격 인정된 반도체의 수요가 증가되므로, 반도체 산업의 패러다임이 바뀌어야 한다. 일반 산업용 반도체도 고신뢰, 고안전 부품을 요구할 것으로 보이며, 산업계 전반적으로 통용될 것으로 보인다. 반도체 평가 및 자격인정 방법론이 체계적으로 연구되어 부가가치가 높은 반도체로 거듭날 수 있도록 평가의 체계화와 자동으로 검증 가능한 장비들을 상용화하는 것이 바람직하다.

한국의 반도체 산업이 나아가야 할 방향성은 Intelligent한 고안전 반도체에 자동차 기술, 기능안전 기술, 보안기술과 더불어 소형화, 통합화, 고속화, 지능화된 제품을 접목하여야 한다.

더불어 보안도 고려하여 같이 설계되어야 한다. 올해 자동차 보안 관련하여 국제표준으로 제안되었으며, 빠르게 표준화가 진행될 예정이다. 기능안전과 보안 2가지 분야를 떼놓고 이야기 할 수가 없으며, 아버지와 자식 같은 하나의 가족을 구성한다. 보안은 ISO new proposal ISO/TC 22 N 3556 (new proposal) Automotive Security Engineering 으로 제안되었으며, 2020년 경 국제 표준으로 정식 발행될 예정이다.

향후 산업계에서는 반도체의 기능안전이나 보안을 동시에 요구할 것으로 예상되며, 반도체를 평가할 경우 가장 기본적으로 ISO 26262를 준용하는 하드웨어 평가 방법이 요구될 것이다. 반도체로 보안을 구현하는 경우에도 마찬가지로 반도체의 평가 및 자격인정 방법은 ISO/PAS 19451와 동일하거나 유사할 것으로 보인다.

반도체는 IT를 결합한 IoT, 로봇 산업, AI(인공지능), 4차 산업혁명에 지대한 영향을 줄 것으로 판단된다. Intelligent한 고안전 반도체로 나아가는 중요한 원천 기술을 다시 말하면, 반도체 기술의 경쟁력 확보와 부가가치가 높은 산업으로 거듭나기 위해서는 기능안전과 보안을 같이 접목한 반도체 평가 기준 및 체계 확립과 기술의 확보가 중요하다. Intelligent한 고안전 반도체에 자동차 기술, 기능안전 기술, 보안기술과 더불어 소형화, 통합화, 고속화, 지능화된 제품의 개발 및 접목을 통하여 한국의 반도체 산업이 앞으로 나아가야 할 방향성에 대해서 〈그림 8〉로 제시하고자 한다.



〈그림 8〉 고신뢰 고안전을 기본으로 미래의 반도체 방향

참 고 문 헌

[1] ISO 26262: 2011–2012 Road vehicle – Functional safety, Part 1~10, ISO(International Organization for Standardization)

[2] ISO/PDPAS 19451:2016 – Application of ISO 26262:2011–2012 to semiconductors, Part 1~2, ISO(International Organization for Standardization)

[3] 김병철, "ISO 26262를 충족하는 차량용 반도체 표준 ISO/PAS 19451", 2016, 한국반도체 산업협회(KSIA)

[4] 김병철, 박화세, "자동차 반도체용 ISO 26262 추진 매뉴얼", 2013, (사)한국반도체연구조합.

[5] 김병철, "FMEDA를 통한 ISO 26262–5 하드웨어 아키텍처 메트릭 및 PMHF 평가 방법", 2014, 오토저널

[6] 김병철, "ISO 26262 차량용 시스템 반도체(SOC) 엔지니어 과정", 2013, 대한전자공학회(KIEE)

[7] AEC–Q 100, "Qualification of Hardware Components for ISO 26262", QRT 반도체, 2012.

[8] AEC–Q 004, "Zero defect guide line", 2007, AEC(Automotive Electronics Council).

[9] IEC/TR 62380: 2004 – Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment, IEC(The International Electrotechnical Commission).

김 병 철

- 1989년 2월 동아대학교 산업공학과
- 1993년 8월 부산대학원 산업공학과
- 1990년 3월~1998년 6월 한국표준협회 선임심사원
- 1998년 6월~2001년 5월 TUV SUD Korea 부장
- 2001년 6월~2007년 9월 TUV Nord 한국지사장
- 2007년 10월~2011년 2월 BV(Bureau Veritas) 부사장
- 2012년 8월~현재 한양대학교 미래자동차공학과 산학협력중점교수

〈관심분야〉
자동차 기능안전, 자동차 전장시스템, 차량용 반도체

안 도 석

- 1986년 2월 경북대학교 전자공학과 졸업
- 1986년 6월~1998년 2월 현대전자
- 1998년 3월~2003년 2월 성우전자
- 2003년 3월~현재 큐알티(주) 근무

〈관심분야〉
반도체 신뢰성