ISO 26262 해외 가이드라인 쉽게 이해하기

자율주행 위해 미국 대표로 나선 구글

2014년 07월호 지면기사 / 글 | 채 승 엽 이사, KPIT <Seungyueb.Chae@kpit.com>

일본과 유럽은 국가 차원에서 ISO 26262에 올바르게 대응하기 위해 가이드라인을 개발, 2014년 초 영문으로 전 세계에 공개함으로써 "made in Japan", "made in Europe"이라는 키워드로 자동차 제조에 대한 국가 브랜드를 보장했다. KPIT가 일본과 유럽의 ISO 26262 가이드라인은 어떻게 작성됐고, 어떠한 차이가 있는지 설명한다.

1. ISO 26262 해외 가이드라인 소개
2. ISO 26262 Part3 가이드라인 - Concept
3. ISO 26262 Part4 가이드라인 - System
4. ISO 26262 Part5 가이드라인 - HW
5. ISO 26262 Part6 가이드라인 - SW

일본과 유럽의 ISO 26262 가이드라인 소개

업계에서는 자동차 내의 E/E 시스템의 복잡성 증가로 차량 결함(Failure)에 의한 리콜이 급증하고 있어 이를 사전에 방지하기 위한 노력으로 자동차를 대상으로 하는 기능안전성 표준 ISO 26262를 2011년 11월 15일에 제정했다.

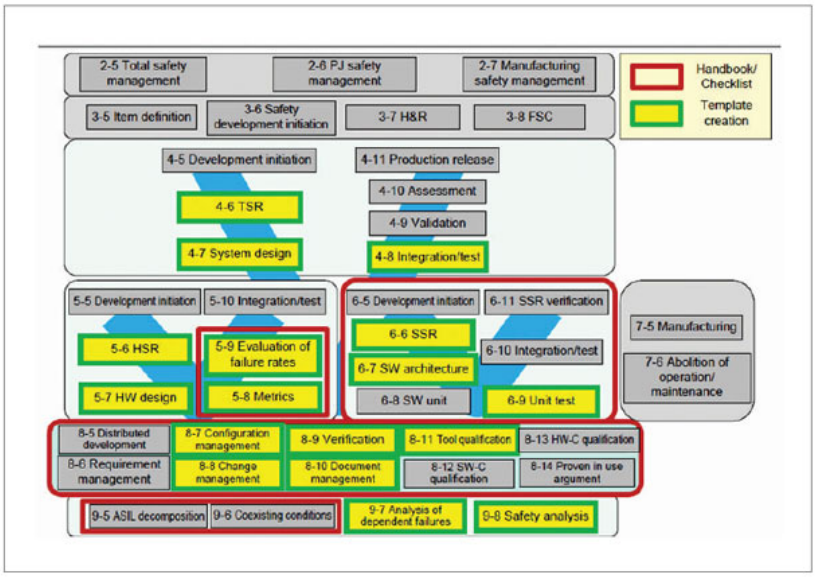


그림 1 | JASPAR의 ISO 26262 가이드라인 제공 범위

ISO 26262는 고객에 대한 제조물책임법(Product Liability Law) 대응을 위한 제조회사인 OEM과 서플라이어의 책임설명(accountability)이라고 볼 수 있다. 따라서 일본과 유럽은 국가 차원에서 ISO 26262에 올바르게 대응하기 위한 가이드라인을 개발, 2014년 초 영문으로 전 세계에 공개함으로 "made in Japan", "made in Europe"이라는 키워드로 자동차 제조에 대한 국가 브랜드를 보장했다. 그러면 일본과 유럽의 ISO 26262 가이드라인은 어떻게 작성됐고, 어떠한 차이가 있는지 설명하겠다.

News & Analysis

2륜차 리어램프에 최적! 4ch 리니어 LED 드라이버 (/article/articleView.asp?idx=3473)

다쏘시스템, 조메트리와 파트너십 체결... (/article/articleView.asp?idx=3472)

포레스터 리서치, 산업용 IoT SW 플랫폼 리더로 마인드스피어 선정 (/article/articleView.asp?idx=3471)

[보도자료]ST, IIoT와 자동차 애플리케이션을 위한 안전한 셀룰러 연결 제공 (/article/articleView.asp?idx=3470)

뤼츠 시스템 솔루션즈, 자동차 이더넷 테스터(ATE) 발표 (/article/articleView.asp?idx=3469)

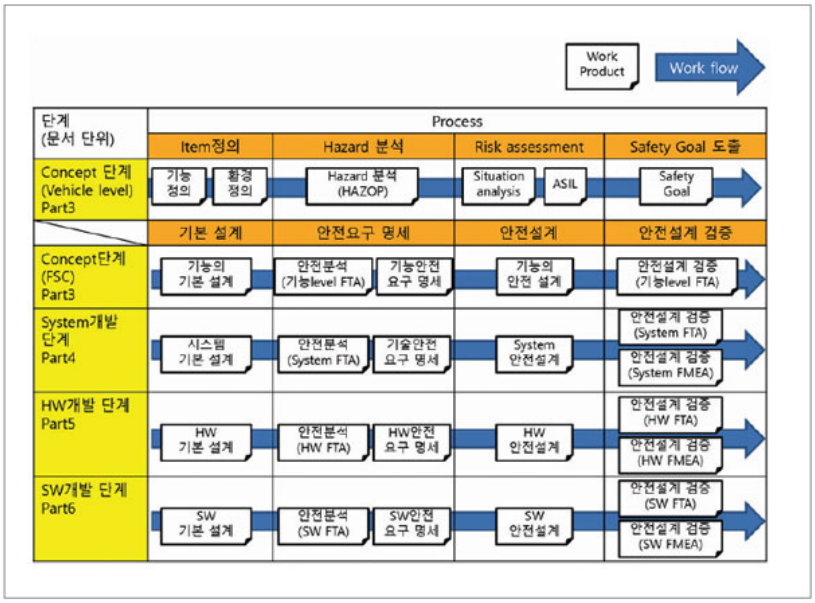


그림 2 | JASPAR의 ISO 26262 각 Part별 문서작성 시 목차 나열

일본 JASPAR의
ISO 26262 가이드라인

일본 JASPAR(Japan Automotive Software Platform And Architecture)는 자동차 관련 기술 표준인 AUTOSAR와 ISO 26262에 대응하기 위해 일본 정부와 OEM(토요타, 닛산, 혼다)이 협력해 2004년 9월 출범시킨 법인이다. 여기에는 해외기업을 포함 116개 회원사가 활동하고 있다. ISO 26262 가이드라인은 2010년 4월부터 2013년 3월까지 OEM, 티어1, 반도체 회사, 개발 툴 회사 등 27개사 총 94명의 엔지니어가 참가해 만든 1,850페이지 분량의 문서다. 검증기관으로부터 402개 항목의 지적사항을 반영했다. 2013년 7월 19일 일본어 버전을 공개했는데, 26개국 128개 회사가 다운로드했다. JASPAR는 올해 2월 24일 영문 버전도 공개했다. JASPAR의 ISO 26262 가이드라인은 JASPAR 홈페이지 (https://www.jaspar.jp (https://www.jaspar.jp))에서 누구나 다운로드할 수 있다.

표 1 | JASPAR에서 공개한 가이드라인과 템플릿

No	ISO 26262 Part	분류	파일명	Page	내용	Word에 Checklist 엑셀 포함
1	–	Guideline	Overview of Functional safety Templates ver1.0.pdf	8	JASPAR Guideline과 Template 설명	–
2	Part 4-6	Guideline	Template Entry Guide(System Development).pdf	47	Part 4-6 TSC Template 작성 방법 설명	–
3	Part 5	Guideline	Handbook for FSI(Microcontroller Application Edition).pdf	93	MCU	–
4	Part 5	Guideline	Handbook for FSI(ASIC Edition).pdf	96	ASIC	–
5	Part 5	Guideline	Template Entry Guide(Hardware Development Edition).pdf	42	HW Template 작성 방법 설명	–
6	Part 6	Guideline	Handbook for FSI(Software Partitioning edition).pdf	186	Non OS, AUTOSAR OS, MultiCore OS 등 SW partitioning 관점 기술	–
7	Part 6	Guideline	Template Entry Guide(Software Development Edition).pdf	47	SW Template 작성 방법 설명	–
8	Part 8	Guideline	Template Entry Guide (Supporting Process and Verification).pdf	95	Part 8 Template 작성 방법 설명	–
9	Part 2	Template	Functional Safety Support Templates (Confirmation Review Edition).doc	8	Confirmation measures	O
10	Part 4-6	Template	Functional Safety Technical Templates (System Development Technical Safety Concepts Edition).doc	15	TSC	–
11	Part 4-8	Template	Functional Safety Support Templates (Integration Test Edition).doc	12	통합테스트	O
12	Part 5	Template	Functional Safety Technical Templates (Hardware Development Edition).doc	14	HW	–
13	Part 6	Template	Functional Safety Technical Templates (Software Development Edition).doc	15	SW	–
14	Part 6-9	Template	Functional Safety Support Templates(Test Edition).doc	10	유닛 테스트	O
15	Part 8-10	Template	Functional Safety Support Templates (Document Management Plan).doc	7	문서관리	–
16	Part 8-7	Template	Functional Safety Support Templates (Configuration Management Plan Edition).doc	6	형상관리	O
17	Part 8-8	Template	Functional Safety Support Templates (Change Management Plan Edition).doc	9	변경관리	O
18	Part 8-9	Template	Functional Safety Support Templates (Verification Review Edition).doc	8	Verification	O

JASPAR의 ISO 26262 가이드라인 제공범위는 Part 4, 5, 6, 8, 9이며, ISO 26262의 산출물(Work Products)을 작성하기 위한 문서양식(Templates)과 체크리스트(Checklists)를 포함한다(그림 1~2, 표 1). 특히 ISO 26262 Part (HW Level)에서 설명이 부족한 반도체 분야의 MCU 가이드라인, ASIC 가이드라인을 제공하고, ISO 26262 Part 6(SW Level)의 최신 기술인 Multicore OS와 AUTOSAR에 대한 내용을 보강해 SW Partition 가이드라인으로 제공한다. 그러나 전반적인 내용인 Part 6, Part 8 가이드라인은 유상으로, 일본 JSA(일본규격협회, http://www.webstore.jsa.or.jp/webstore/top/index.jsp (http://www.webstore.jsa.or.jp/webstore/top/index.jsp))에서 각각 약 7만 원에 책으로만 받을 수 있다.

JASPAR의 ISO 26262 가이드라인에서 주의할 사항은 일본 OEM(토요타, 혼다, 닛산)에 납품하기 위한 티어1 관점에서 작성돼 있기 때문에 Part 3 가이드라인이 없고, OEM과 서플라이어가 어떻게 협력해 진행할 것인가에 대해 기술하지 않은 점이다.

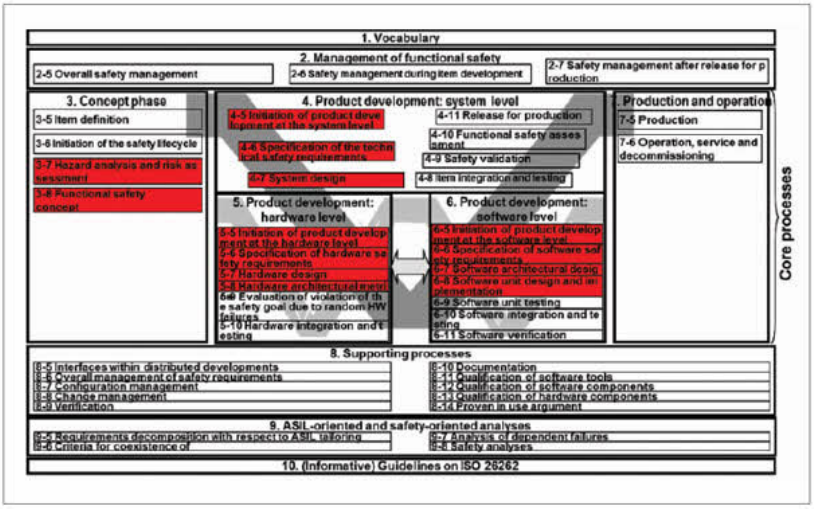


그림 3 | SAFE의 ISO 26262 가이드라인 제공 범위

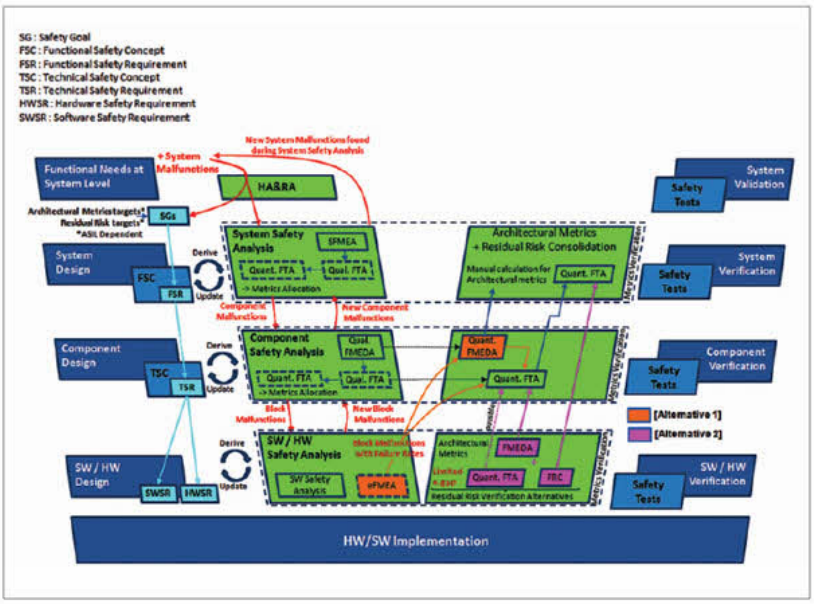


그림 4 | SAFE의 Safety Analyses 절차

JASPAR에서는 ISO 26262 가이드라인이 현업에서 실제로 적용할 때 문제가 없는지, 다른 해외 가이드라인과 비교해 잘못된 내용이 없는지를 검토하기 위해 2014년 3월부터 12월까지 매월 정기회의를 통해 산출물(Work Products)을 실제로 작성 검증하고 있다. 첫 회 모임에서는 오프라인으로 70명이 참석했고, Webex로 실시간으로 병행해 진행했다.

유럽 SAFE의
ISO 26262 가이드라인

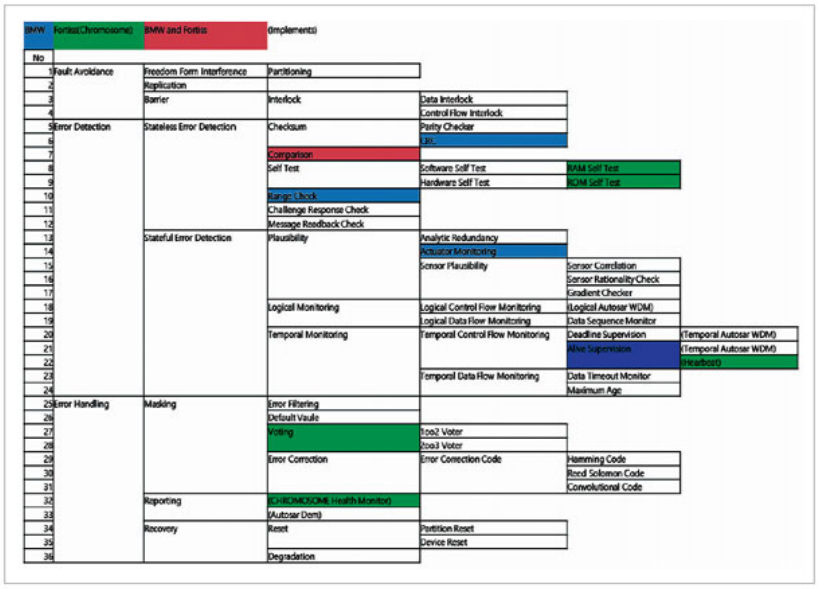
유럽에서는 BMW를 중심으로 ISO 26262의 산출물(Work Products)을 AUTOSAR ARXML로 변환하기 위해 SAFE(Safe Automotive soFtware architEcture)란 프로젝트를 만들었다. 2011년 7월부터 2014년 12월(3년 6개월)까지 진행하는데 ISO 26262 가이드라인과 템플릿(Templates)을 제공한다. SAFE의 ISO 26262 가이드라인은 SAFE 홈페이지 (http://www.safe-project.eu/ (http://www.safe-project.eu/) SAFE-Download.html)에서 누구나 다운로드할 수 있다.

표 2 | SAFE의 Safety Measure의 정의

BMW define	ISO 26262 guidelines(SAFE) in EU	Semiconductor		Safety Measure	
		SPFM(Fault detectionand mitigation)	LFM(Self-testcapability)	Safety Activity (systematic failure)	Safety Mechanism (random HW failure)
Fault Avoidance	avoid			O	
Error Detection	detect	O	O		O
Error Handling	mitigate	O		O (control)	O (control)

2014년 10월 15일에 공개 예정인 AUTOSAR 4.2.1에 SAFE의 결과물들이 Safety Extension으로 반영된다.
SAFE의 ISO 26262 가이드라인 제공범위는 Part 3에서 6까지이며, 추가적으로 Part 8의 Traceability와 Part 9의 Safety Analyses도 제공한다(그림 3, 4). SAFE는 유럽 OEM 관점에서 서플라이어와 어떻게 협력해 진행할 것인가를 중점으로 다룬다. OEM과 서플라이어는 ISO 26262 산출물(Work Products)을 AUTOSAR ARXML기반으로 데이터베이스를 구축해 개발 협력을 진행한다.

특히 SAFE에서는 ISO 26262의 핵심 기술 Safety Measure(Safety Activity와 Safety Mechanism)를 BMW가 OEM 입장에서 구체화했다. Safety Measure는 BMW와 독일 국가 연구소인 포티스(Fortiss)가 공동으로 기술 확보를 위한 연구를 진행하고 있으며, 크게 3가지(Fault Avoid, Error Detection, Error Handling)로 분류해 소분류까지 36가지로 규정한다. 현재 BMW가 확보한 Safety Measure는 CRC, Range Check, Actuator Monitoring, Alive Supervision 등이 있으며, 앞으로 더 많은 기술을 확보할 방침이다(그림 5, 표 3). 또 Safety Analyses에서는 OEM과 서플라이어가 서로 협력하는 방법을 정확한 가이드라인으로 제공하고 있다.



No	BMW	Fortiss(Chromosome)	BMW and Fortiss	(Implements)		
1	Fault Avoidance		Freedom Form Interference	Partitioning		
2			Replication			
3			Barrier	Interlock	Data Interlock	
4					Control Flow Interlock	
5	Error Detection		Stateless Error Detection	Checksum	Parity Checker	
6					CRC	
7				Comparison		
8				Self Test	Software Self Test	RAM Self Test
9					Hardware Self Test	ROM Self Test
10				Range Check		
11				Challenge Response Check		
12				Message Readback Check		
13			Stateful Error Detection	Plausibility	Analytic Redundancy	
14					Actuator Monitoring	
15					Sensor Plausibility	Sensor Correlation
16						Sensor Rationality Check
17						Gradient Checker
18				Logical Monitoring	Logical Control Flow Monitoring	(Logical Autosar WDM)
19					Logical Data Flow Monitoring	Data Sequence Monitor
20				Temporal Monitoring	Temporal Control Flow Monitoring	Deadline Supervision (Temporal Autosar WDM)
21						Alive Supervision (Temporal Autosar WDM)
22						Heartbeat
23					Temporal Data Flow Monitoring	Data Timeout Monitor
24						Maximum Age
25	Error Handling		Masking	Error Filtering		
26				Default Vaule		
27				Voting	2oo2 Voter	
28					2oo3 Voter	
29				Error Correction	Error Correction Code	Hamming Code
30						Reed Solomon Code
31						Convolutional Code
32			Reporting	(C+)ROMOS/OME Health Monitor)		
33				(Autosar Dem)		
34			Recovery	Reset	Partition Reset	
35					Device Reset	
36				Degradation		

그림 5 | SAFE의 ISO 26262에 필요한 Safety Measure 분류

일본과 유럽의 ISO 26262
가이드라인 비교

일본과 유럽의 ISO 26262 가이드라인은 표 3과 같이 간단히 비교를 할 수 있다. 일본과 유럽의 ISO 26262 가이드라인 세부 내용을 비교하면 ISO 26262 Part 1에서 언급하지 않는 새로운 용어 정의가 서로 다른 것을 알 수 있다. 다음과 같은 2가지 사례(이음동의어와 동음이의어)가 대표적이다.

첫 번째로 이음동의어(단어는 다르나 뜻이 같은 경우)의 예로 Part 4-6 TSC(Technical Safety Concept)에서 System Design을 도식화하기 위해 Block 단위로 TSR (Technical Safety Requirement)을 도출하게 되는데, 이때의 Block을 JASPAR에서는 "System block" 이라고 하는데, SAFE에서는 "Architectural Block"이라고 서로 다른 단어를 사용한다.

두 번째로 동음이의어(단어는 같으나 뜻이 다른 경우)의 예는, Safety Analyses로 FMEA을 수행을 하게 되는데, JASPAR에서는 Part 4-6 TSC(Technical Safety Concept)에서 System FMEA를 실시해 Verification을 수행하고 있는데 반해 SAFE에서는 Part 3-8 FSC(Functional Safety Concept)에서 System FMEA를 FSR(Functional Safety Requirement)를 도출하기 위해 실시하고 있다. 단어는 같으나 뜻이 다르게 사용되고 있어 각 나라별 ISO 26262 가이드라인의 해석에 주의할 필요가 있다.

표 3 | 일본과 유럽의 ISO 26262 가이드라인 비교

국가	일본 JASPAR	유럽 SAFE
목표	일본 OEM에 납품하기 위한 Tier 1 입장에서의 ISO 26262 대응 방법	유럽 OEM과 서플라이어 협력 관계에서의 ISO 26262 대응 방법.
제공 범위	Part 4, 5, 6, 8, 9 (Tier 1 입장이므로 Part 3 제외)	Part 3~6 (Part 8, 9는 부분적으로 Traceability와 Safety Analyses 방법 제공)
장점	ISO 26262에서 내용이 부족한 Part 5의 MCU와 ASIC 대응과 Part 6의 SW Partitioning 보강	ISO 26262 산출물(Work Products)을 AUTOSAR ARXML 변환 방법을 사용한 OEM과 서플라이어의 협력 관계 구축 ISO 26262에서 이해하기 어려운 용어에 대해 사례를 들어서 잘 정리
단점	OEM과 서플라이어 협력 관계 방안이 없으며, 일본 OEM에 납품을 목적으로 기술됨	ISO 26262 가이드라인 문서의 구성이 ISO 26262의 Part 별로 나눠지지 않고 여기저기 분리돼 있어, 모든 문서를 읽어 보면서 스스로 정리하지 않으면 전체 구성을 알아보기 힘듬

그리고 Safety Requirements(3-8 FSC, 4-6 TSC, 5-6 HWSR, 6-6 SWSR)를 도출하거나 Verification을 하기 위해서 Safety Analyses(FMEA, FTA)를 실시하는데 있어 일본과 유럽은 절차나 방법이 크게 다르다. 따라서 국내 서플라이어는 일본과 유럽 OEM을 구별해서 Safety Analyses를 실시해야 하는 상황이다.

이러한 문제는 ISO 26262 Second Edition(2018년 제정 예정)에서 해결될 전망이다. AUTOSAR를 기반으로 제품을 개발한다면 SAFE에서 Safety Analyses의 산출물(Work Products)이 ARXML로 변환됨으로 유럽 방식을 따를 수밖에 없는 상황이다. 따라서 국가 입장에서 표준 활동이 중요하다. 이러한 정보를 JASPAR의 ISO 26262 W/G에 필자가 열심히 요청해 개선 활동을 하고 있다. 국내에서도 필자가 우리나라를 위해 공식적으로 ISO 26262 활동을 하고 싶지만 기회가 없어 본 매거진 연재를 통해 관련 정보를 공유하고자 한다.

ISO 26262
Second Edition의 요구 사항

ISO 26262가 2011년 제정된 이후 2012년 말부터 2015년 중순까지 ISO PAS(Publicly Available Specification)로 3가지 SWG(Sub Working Group)인 ISO PAS 19451(반도체, 텍사스 인스트루먼트가 리더), ISO PAS 19695(모터사이클, MSIL, 혼다가 리더), 트럭과 버스(볼보가 리더)를 제정하고 있다.

또 ISO 26262 Second Edition(다임러가 리더)은 2015년 중순부터 2018년까지 제정을 완료하는 것을 목표로, 자율주행/무인/ 전기차를 중심으로 진행되고 있다.

놀라운 사실은 구글이 자율주행차를 양산하기 위해 미국 대표로 2012년부터 ISO 26262 W/G에 적극 참여하고 있으며, 활동하고 있는 분야는 ISO PAS 19451 (Semiconductor)과 ISO 26262 Second Edition의 표준화 작업이다. 구글은 애플이 스마트폰 시장에서 아이폰에 자체 반도체를 탑재한 것처럼, 자율주행차의 핵심 반도체를 연구개발하고 있는 것으로 보인다. 또 구글이 무인 로봇 관련 집중적인 M&A를 하고 있어, 자동차의 반도체가 로봇 반도체에서도 활용될 가능성이 커보인다. 구글은 애플이 스마트폰 시장에서 강자가 된 것처럼, 2017년 상용화를 목표로 올 여름까지 최소 100대의 프로토타입을 생산 시운전해 자율주행차 시장에 도전할 것으로 보인다.

국내에서는 해외 ISO 26262에 대한 분석 및 대응이 이뤄지고 있지 않다. 일본과 유럽에 수출하는 서플라이어는 해외 ISO 26262 가이드라인에 대한 준비가 돼 있지 않아 수출에 많은 어려움을 겪을 것으로 예상된다. 따라서 필자는 조금이나마 도움이 될 수 있도록 "ISO 26262 해외 가이드라인 쉽게 이해하기"의 연재를 기획했다. 다음 연재에는 "ISO 26262 Part 3 가이드라인 "Concept"를 설명하겠다.

등록

스마트앤컴퍼니(주) 대표이사 : 박성규 사업자등록번호 : 108-81-64739 통신판매업신고 : 2019-서울구로-2138호

서울특별시 구로구 디지털로34길 43, 607호(구로동, 코오롱싸이언스밸리1차) P: (Phone) 02-841-0017 F: (Fax) 02-841-0584 webmaster@smartn.co.kr