


⬆ (/) / Connectivity & Security (articleWebList1.asp?c\_no1=32)

## ISO 26262 해외 가이드라인 쉽게 이해하기

2014년 11월호 지면기사 / 글 | 채 승 업 <syachae@ssu.ac.kr>

rticle/articleView.asp%3Fidx=1571&t=ISO%2026262%20해외%20가이드라인%20쉽게%20이해하기) 

 (<https://story.kakao.com/s/share?>

9C%EB%9D%BC%EC%9D%B8%20EC%89%BD%EA%B2%8C%20EC%9D%B4%ED%95%B4%ED%95%98%EA%B8%B0%20-20os%2Fjavascript%20lang%2Fko-KR%20device%2FWin32%20origin%2Fhttp%253A%252F%252Fwww.autoelectronics.co.kr)



채승업 씨가 'ISO 26262 해외 가이드라인 쉽게 이해하기'를 5회에 걸쳐 연재한다. ISO 26262 대응을 위해 일본 JASPAR는 2014년 2월 24일 ISO 26262 가이드라인 영문판을 공개했다. 또 유럽은 SAFE가 ISO 26262 가이드라인을 공개하고 있다.

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

### ISO 26262 Part3과 Part4에서 OEM과 서플라이어의 역할

해외에서는, OEM의 RFQ로부터 ECU 납품에 입찰한 서플라이어는 OEM과의 DIA (DevelopmentInterface Agreement)를 시작으로 ISO 26262를 준수한 ECU를 개발하기 시작한다. 여기서 중요한 것은 OEM과 서플라이어의 협업에 대한 책임 (Responsible)이다. 일반적으로 ISO 26262의 산출물(Work Product)에 대해 Part3은 OEM이, Part4는 서플라이어가 책임을 진다(표 1).

특히 Part3-8 FSC(Functional Safety Concept)는 OEM이 주도해 작성해 서플라이어로부터 할 수 있는지, 추가 내용이 없는지를 피드백 받는다. Part4-6 TSC(Technical Safety Concept)의 경우엔 서플라이어가 주도해 작성하고 OEM으로부터 피드백을 받는다(그림 1).

([http://ssl.logger.co.kr/tracker\\_ad.tsp?u=37061&mode=C&adCode=57236](http://ssl.logger.co.kr/tracker_ad.tsp?u=37061&mode=C&adCode=57236))

([http://ssl.logger.co.kr/tracker\\_ad.tsp?u=37061&mode=C&adCode=77860](http://ssl.logger.co.kr/tracker_ad.tsp?u=37061&mode=C&adCode=77860))

### 과월호 e-Book 보기 (</ebook/list.asp>)



(</ebook/list.asp>)(</ebook/list.asp>)

### 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>)

(<https://www.drivingthenation.com>)

([http://smartn.co.kr/book/book\\_detail.asp?p\\_no=B00159](http://smartn.co.kr/book/book_detail.asp?p_no=B00159))

표 1 | Development Interface Agreement 계약서의 예제  
출처 | 2014, 06, VDA Automotive SYS 2014, Berner & Mattner Systemtechnik, Structured Safety Assessments: A Solid Foundation for the Safety Case

RASI : Responsible(책임), Approval(동의), Support(협력지침), Information(정보제공)

Activity/WorkProduct	OEM				Supplier			
	R	A	S	I	R	A	S	I
Safety Plan(OEM)	x							
Safety Plan(Supplier)		x			x			
Safety responsibilities(OEM)	x							x
Safety responsibilities(Supplier)				x	x			
Item Definition - Part3	x					x	x	
Hazard-Analysis - Part3	x					x	x	
Functional Safety Concept(OEM) - Part3	x							
Technical Safety Concept - Part4		x			x			
Component Safety Requirements	x					x		
HW Reliability analyses(FTA,FMEDA)		x			x			
Component integration and test reports		x	x		x			
ECU Test/Test Finding Report				x	x			

Responsible(책임)  
OEM    Supplier



그림 1 | 해외 OEM과 서플라이어의 산출물에 대한 역할 분담 사례  
출처 | 2014, 6, VDA Automotive SYS 2014, Berner & Mattner Systemtechnik, Structured Safety Assessments: A Solid Foundation for the Safety Case

피드백은 크게 4가지로 "Accepted(받아들임), Accepted with Deviation(내용 중에 일부분을 받아들임), Not Applicable(본 ECU 개발에 적용 대상이 아님), Not Accepted(받아들일 수 없음)"다. Part3과 Part4의 Safety Requirement의 각 항목에 대해서 OEM과 서플라이어는 자기의사를 표현하는데, Accepted 이외의 항목에 대해서는 반드시 의견을 뒷받침할 수 있는 사유를 적어야 한다. 보통 OEM과 서플라이어의 의견 불일치가 발생하는 경우는 Safety Requirement를 구현하기 위한 비용 문제가 제일 크다. 또 안전과 비용에 대한 균형이 필요하다.

#### ISO 26262 Part4 시스템 레벨의 제품 개발

ISO 26262의 Part4는 7가지 프로세스를 가지고 있다. 그리고 4-8 ~ 4-11(m~p)은 Part5-8 Evaluation of the Hardware Architectural Metrics과 Part 6-9 Software Unit Testing을 시작하는 시점과 병행해서 병렬로 업무를 시작한다(그림 2).

① 4-5 Initiation of Product Development at the System Level: Part4의 업무를 계획하고 Project/ Safety Plan의 기존 계획을 업데이트한다. Part4의 프로세스에 해당하는 Item Integration and Testing/ Validation/Functional Safety Assessment Plan을 신규로 계획을 작성한다.

② 4-6 Specification of the Technical Safety Requirements: Part3-8.5.1 FSC(Functional Safety Concept)의 추상적인 Safety Requirement 결과로부터 파생해 기술적으로 하드웨어와 소프트웨어를 고려한 시스템 레벨의 Part4-6.5.1 TSRs(Technical Safety Requirements)를 서플라이어가 작성한다.

③ 4-7 System Design : 서플라이어는 OEM의 피드백을 받아 완성한 Part4-7.5.1 TSC(Technical Safety Concept)을 정리하고 이를 바탕으로 Part4-7.5.2 SDS(System Design Specification)를 작성, HW와 SW를 연계한 시스템 기능에 대해 Part4-7.5.3 HSI(Hardware Software Interface Specification) 정의를 시작, Part4-7.5.4 Specification of Requirements for Production, Operation, Service and Decommissioning에 시스템 레벨의 생산/운영/폐기에 대한 요구사항을 작성, ASIL 등급에 따라 FMEA, FTA 등을 실시 Part4-7.5.5 Safety Analysis Report 작성 등을 수행한다.

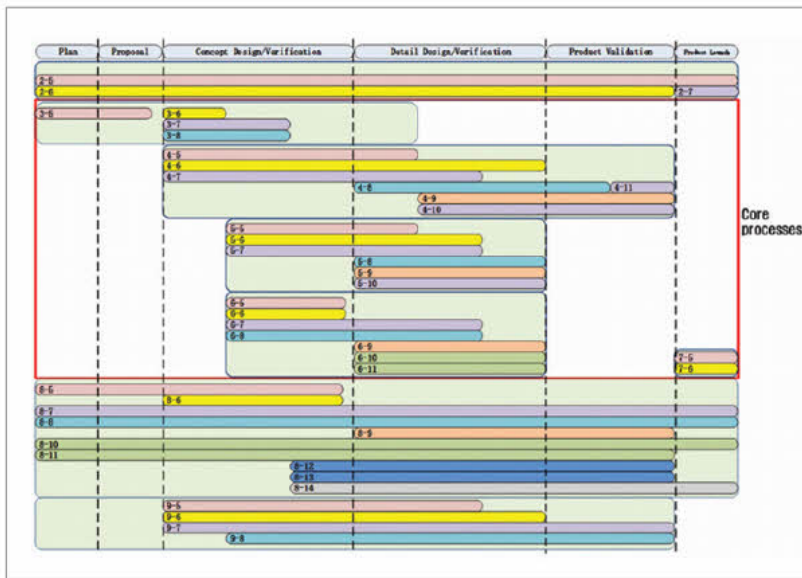


그림 2 | ISO 26262 각각의 프로세스는 병렬로 업무를 진행

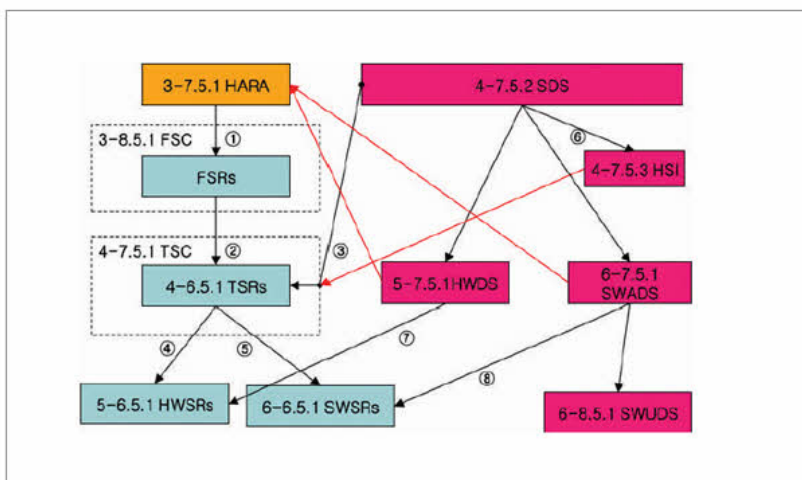


그림 3 | ISO 26262 전체 업무에서 SR(Safety Requirement)과 DS(Design Specification)의 관계도

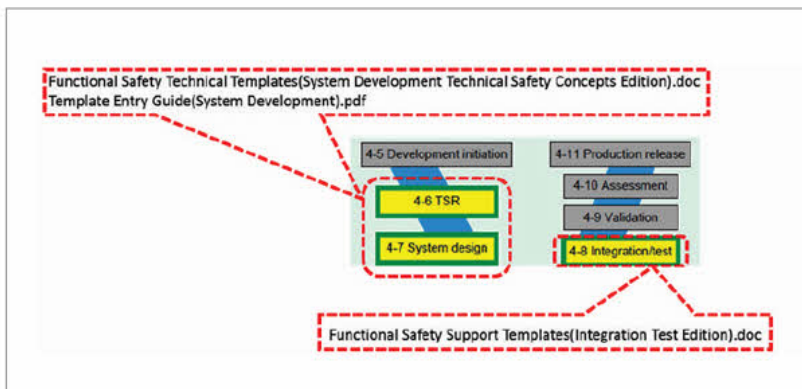


그림 4 | JASPAR의 Part4 Template와 Guide 제공 범위

Part4-7.5.3 HSI(Hardware Software Interface Specification)는 Part5 HW와 Part6 SW의 Design에서 내용이 추가되거나 수정된다. 참고로 SDS version 0.1 문서는 Part3-5 Item Definition이 완료된 내용이 들어가면서 시작되며, Part3-8 FSC(Functional Safety Concept)에서 Preliminary Architectural Assumption이 완료되면 이것 또한 SDS version 0.1 문서에 내용이 들어가 SDS version 0.2 문서가 된다.

이러한 내용은 ISO 26262 표준 명세서를 자세히 정독해보면 기술이 돼 있는 내용임을 알 수가 있다. 참고로 필자는 ISO 26262 해외 가이드라인도 좋지만, ISO 26262 표준 명세서를 수십 번씩 반복 정독해 분석하면서 공부하는 것을 권장한다.

④ 4-8 Item Integration and Testing: Part4-8.5.2 Integration Testing Specification을 정의하고 실제 HW와 SW 기반으로 통합시험(Integration Testing)을 수행해 Part4-8.5.3 Integration Testing Report를 작성한다.

⑤ 4-9 Safety validation: Safety Requirement가 누락되거나, 잘못된 사항이 없는지 등을 확인해 Part4-9.5.2 Validation Report를 작성한다.

⑥ 4-10 Functional Safety Assessment: OEM에서 중간보고, 완료보고 형태로 해당 제품의 기술적인 지식과 경험이 있는 Functional Safety Manager가 Assessment를 실시해 Part4-10.5.1 Functional Safety Assessment Report를 작성한다.

⑦ 4-11 Release for Production: 양산 위한 준비를 완료하기 위해 Part4-11.5.1 Release for Production Report를 작성한다.

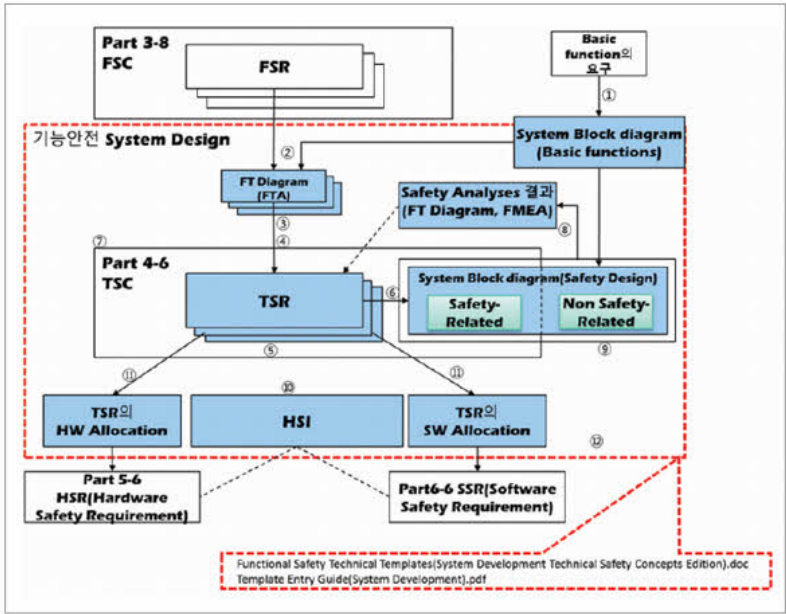


그림 5 | JASPAR에서 제시한 ISO 26262 Part4 업무 순서

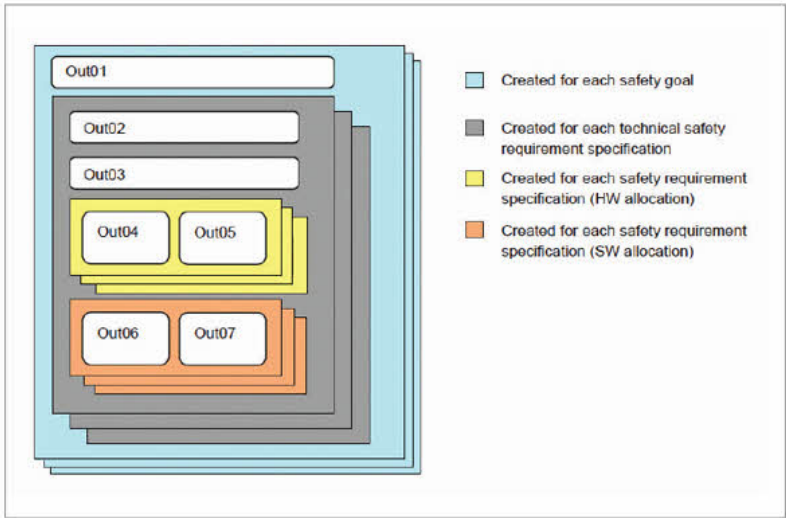


그림 6 | Composition of Output – Technical Safety Requirement Specifications(HW Allocation/SW Allocation)

#### 일본 JASPAR의 ISO 26262 가이드라인에서 Part4

일본 JASPAR의 ISO 26262 가이드라인의 “Functional Safety Technical Templates (System Development Technical Safety Concepts Edition). doc”는 Part4의 2가지 프로세스의 4-6 Specification of the Technical Safety Requirements, 4-7 System Design의 모든 Work Product가 포함된다(그림 4).

“Functional Safety Technical Templates (System Development Technical Safety Concepts Edition). doc”를 작성하기 위한 업무 순서는 다음과 같다(그림 5). 주의할 사항으로는, JASPAR의 가이드라인 Part4에서 사용하는 System Block이라는 용어는 일본에서만 쓰는 신규 용어로, Part4 System Level에서 기능 단위로 Block Diagram을 표현하는 것이다.

- ① Basic Function의 System Design
- ② Non Safety Related System에 대한 FTA
- ③ 취약 요소의 규정
- ④ TSR 도출
- ⑤ TSR의 Verification
- ⑥ System Design
- ⑦ TSC로 최종 정리
- ⑧ System Design에 대한 Safety Analyses
- ⑨ RHF(Random Hardware Failure) Metrics의 Target Values 규정: ASIL (B), C, D 대상



- ⑩ HSI 설계
- ⑪ TSR의 HW/SW 분배
- ⑫ System Design의 Verification

그리고 JASPAR의 Technical Safety Require Ment의 문서 구성은 그림 6, 표 2와 같이 1개의 Safety Goal(Part3-7.5.2)에 각  
 각의 FSR (Functional Safety Requirement, Part3-8.5.1)에 대해서 1개의 FSR에 여러 개의 TSR(Part4-6.5.1)을 도출해 작성  
 할 것을 요구한다.

표 2 | Output – Technical Safety Requirement Specifications

No.	Item	Creation unit
Out01	Target safety goal ID	Safety goal
Out02	Related functional safety requirement specifications	Functional safety requirement specification related to the safety goal
Out03	Explanation of the technical safety requirement specification	Functional safety requirement specification related to the safety goal
Out04	Technical safety requirement specifications	Technical safety requirement specification related to the safety goal
Out05	Technical safety requirement specifications: Latent fault avoidance	Technical safety requirement specification related to the safety goal (specification for latent fault avoidance only)
Out06	System block diagram (including safety functions which reflect the technical safety requirement specifications)	Safety goal
Out07	Summary of the system blocks	Safety goal
Out08	Operating mode	Safety goal
Out09	Operating mode state transition diagram	Safety goal

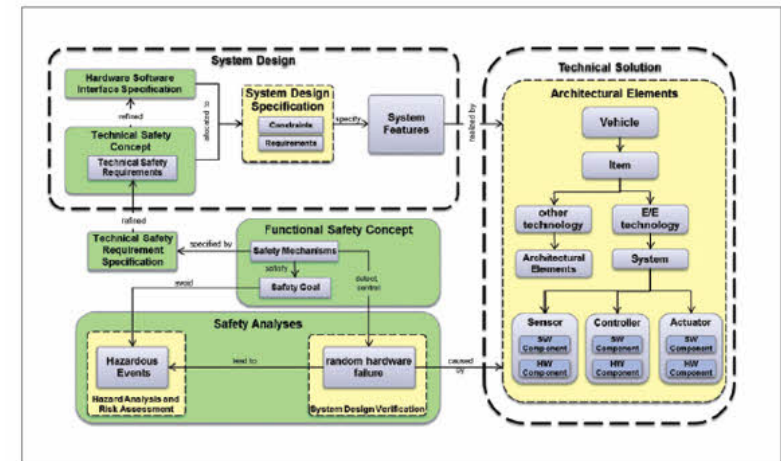


그림 7 | SAFE의 ISO 26262 Part4 도식화 출처 | SAFE\_D3.2.1.c

표 3 | SAFE의 ISO 26262 블록 다이어그램의 신규 용어

Part3-8 FSC	Function Block	System Function Block	기능위주의 Block
Part4-6 TSC	Architecture Block	System component architecture Block	System위주의Block (Sensor, Controller, Actuator)
		SW architecture Block	SW 위주의Block
		HW architecture Block	HW 위주의 Block

유럽 SAFE의 ISO 26262 가이드라인에서 Part4

유럽 SAFE의 ISO 26262 가이드라인은 각각 ISO Part 내용들이 흩어져 있으므로, 국제 표준 ISO 26262 명세서를 읽어 보지  
 않은 상태에서는 이해하기 어려운 내용이 많다. Part3-8.5.1 FSC(Functional Safety Concept)의 Safety Mechanism으로  
 부터 Part4-6.5.1 TSRs(Technical Safety Requirements)를 도출, OEM과 피드백해 Part4-7.5.1 TSC(Technical Safety  
 Concept)를 정리하고, Part4-7.5.3 HSI(Hardware Software Interface Specification)를 작성, Part4-7.5.2 SDS(System  
 Design Specification)을 완성하는 순서로 업무가 이뤄진다(그림 7). SAFE에서 Part3과 Part4에서 사용하는 각 Block에 대  
 한 신규 용어 및 도식화 방법은 표 3, 그림 8과 같다.

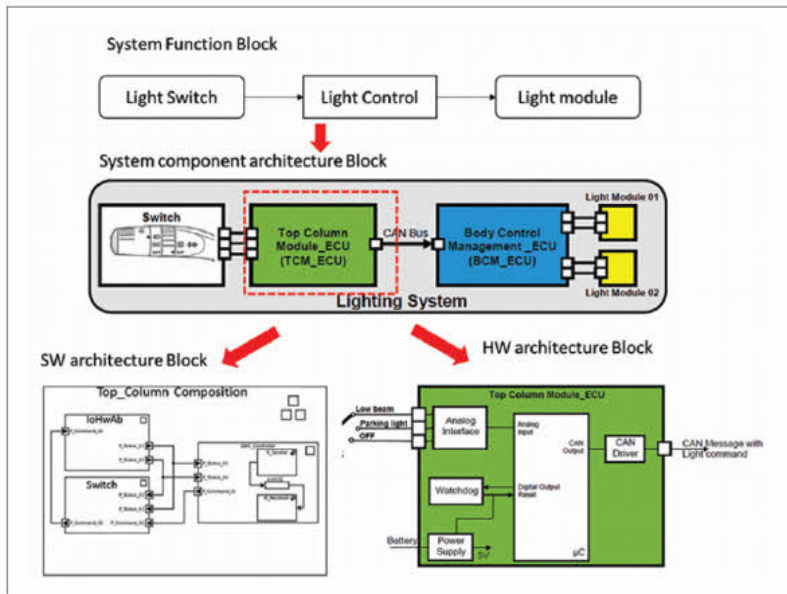


그림 8 | SAFE의 각각 Block 개념에 대한 도식화 사례

표 4 | ISO 26262 Part3에 대한 일본과 유럽의 Block 개념비교

국가	일본 JASPAR	유럽 SAFE
Part3-8 FSC	Function block	
Part4-6 TSC	System block	Architectural Block (System component architecture Block, SW architecture Block, HW architecture Block)

#### 일본과 유럽의 ISO 26262 Part4 비교

일본과 유럽의 ISO 26262 가이드라인에는 국제표준 ISO 26262 명세서에서 정의하지 않는 신규 용어가 추가돼 있다. 그 이유는 ISO 26262 Part1의 용어 정의만으로는 설명하기 부족한 내용들이 존재하기 때문이다. 그리고 일본과 유럽이 Part3 ~ 6에서 실시하는 Safety Analyses에 대해 서로 다른 절차 및 신규 용어를 사용하고 있다. 이렇게 기존에 없는 신규 용어나 절차에 관한 문제는 향후 2015년부터 시작하는 ISO 26262 Second Edition에서 풀어야 할 숙제가 될 것이다.

#### 일본 업계 현황

이번 연재에도 마찬가지로 지면의 제약으로 Part4에 대해 좀 더 자세한 내용을 기술할 수 없었던 것이 아쉽다. 2014년 9월 18일에 열린 JASPAR 상반기 활동 결과 발표회를 다녀왔는데, ISO 26262 관련 2가지 재미있는 사실이 있었다. 첫 번째는 JASPAR에서 회원사를 대상으로 매달 ISO 26262 스터디 세미나를 진행하고 있는데, 54개사에서 161명이 참석하고 있다.

청강자들이 강사 중심의 강의 형태로 진행돼 ISO 26262 공부에 도움이 안 된다고 의견을 주니, JASPAR는 스터디 시작 전에 모든 참여자의 ISO 26262 능력 수준을 조사한 결과를 바탕으로 5~7명으로 팀을 만들고 좌석을 소규모 원탁 형태로 변경했으며, 강의 진행 후 팀 토론을 병행하는 구조로 바꿨다.

두 번째는 이 능력 조사 결과인데, 참가자 중에 ISO 26262를 전혀 모르는 사람이 39%, ISO 26262를 조금 알고 있으나 전문가의 도움 없이는 대응할 수 없는 초보가 41%, 가이드라인과 템플릿이 있으면 ISO 26262 문서를 혼자서 작성할 있는 중급자가 17%, Safety Manager로서 팀을 리더할 수 있는 사람이 3%, 다른 회사에 ISO 26262 컨설팅을 할 수 있는 수준이 0%로 나왔다. 즉, 80%가 스스로의 힘으로 ISO 26262를 준수하며 ECU 개발을 할 수 없는 것으로 나타났다.

이에 따라 JASPAR는 스터디 멤버 전원을 내년 3월까지 중급자 이상으로 만들겠다고 했다. 이는 내년 4월부터 일본 OEM이 C언어가 들어가는 ECU를 개발하는 모든 일본 서플라이어에게 ISO 26262 준수를 요청했기 때문이다. JASPAR는 ISO 26262 스터디 진행을 위한 장소와 강사료에 대해서만 정부와 OEM 지원을 받고 있다. ISO 26262가 필요한 회사들이 적극적으로 참여하고 있는 것이다.

참여 회사들은 스터디가 요구하는 수준을 따라가기 위해서는 참여자들이 이를 100% 자기 업무로 하지 않으면 할 수 없다고 판단해 사내 ISO 26262 대표 전문가 육성을 위해 100% 자기 업무화 하고 자체 비용을 들여 참여자를 지원하고 있다.

100자평 쓰기 [로그인](#)

로그인후 입력하세요

등록

[Advertising / Media Partnership / Sponsoring \(/member/inquiry.asp?sel\\_type=ad\)](#)

[회사소개 \(http://www.smartn.co.kr\)](http://www.smartn.co.kr) [개인정보취급방침 \(/member/protect.asp\)](/member/protect.asp) [이메일주소 무단수집 거부 \(/member/noemailcollect.asp\)](/member/noemailcollect.asp)

[온라인 문의 \(/member/inquiry.asp\)](/member/inquiry.asp) [정기구독 신청 \(http://www.smartn.co.kr/book/book\\_detail.asp?p\\_no=B00033\)](http://www.smartn.co.kr/book/book_detail.asp?p_no=B00033)

[정기구독 주소변경 \(/member/subs\\_edit.asp\)](/member/subs_edit.asp)

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](mailto:webmaster@smartn.co.kr)

© Smart & Company