


ISO 26262 해외 가이드라인 쉽게 이해하기

2014년 09월호 지면기사 / 글 | 채 승 업 이사, KPIT <Seungyueb.Chae@kpit.com>

rticle/articleView.asp%3Fidx=1515&t=ISO%2026262%20해외%20가이드라인%20쉽게%20이해하기)  (https://story.kakao.com/s/share?9C%EB%9D%BC%EC%9D%B8%20%EC%89%BD%EA%B2%8C%20%EC%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)

KPIT Korea가 ‘ISO 26262 해외 가이드라인 쉽게 이해하기’를 5회에 걸쳐 연재한다. KPIT의 멤버들은 KPIT Japan의 도움으로 JASPAR의 ISO 26262 W/G의 멤버 활동을 하고 있으며, 유럽 ISO 26262 가이드라인과 일본 ISO 26262 가이드라인을 비교 분석해 KPIT의 사내 규격인 영문 ISO 26262 가이드라인 작성과 AUTOSAR 4.2.1의 ISO 26262 templates 자동생성 기술을 개발하고 있다. 이번 회는 ISO 26262 Part3 가이드라인 - Concept다.

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

해외 OEM의 ISO 26262 준수와 AUTOSAR 적용 요구

국내 서플라이어가 해외 OEM에 전장부품을 납품하기 위해서는 해외 OEM으로부터 RFQ(request for quotation, 견적 요청)를 받아 입찰에 참여해야 하는데, 크게 4가지(표 1) 대응 여부에 따라 입찰의 성패가 결정된다.

그런데, 해외 OEM의 RFQ는 수 1,000페이지에 각종 ISO/IEC 표준 및 AUTOSAR 용어가 포함돼 있어 아무리 영어를 잘하더라도 사전에 국제표준 용어에 대한 이해가 없으면 해석이 어렵다. 이들은 친절하고 상세하게 설명을 해주지 않는다. 해외 OEM의 경우 국제표준에 따른 협업 업무 프로세스를 제대로 이해해 서플라이어가 대응하길 바란다. OEM은 Vehicle level(차량 레벨)의 새로운 Function(기능)을 주도, 직접 개발한 Master ECU가 서플라이어의 ECU를 Slave로 관리한다. 즉, 해외 OEM의 RFQ 핵심 요구사항으로 기존에 양산된 적이 없는 Master-Slave 형식의 새로운 개념에서 Vehicle level의 Functional Architecture가 적용되는 것이다.

표 1 | 해외 OEM RFQ에서 요구하는 4가지 사항

No	요구항목	일반적인 참고 사항
1	AUTOSAR 적용	Supplier가 개발할 ECU에 OEM이 제공하는 OEM용 SWC가 탑재됨
2	ISO26262 준수	개발할 ECU ASIL 등급과 OEM/Supplier 간 Work product가 정의됨
3	MBD 적용	Simulink/Stateflow, Targetlink 등을 사용한 OEM/Supplier 간 협업 개발(주의: UML이나 SysML을 말하는 것이 아님)
4	EMC 대응	최근 자동차 리콜 급증으로 EMC 요구사항이 높아지고 있음

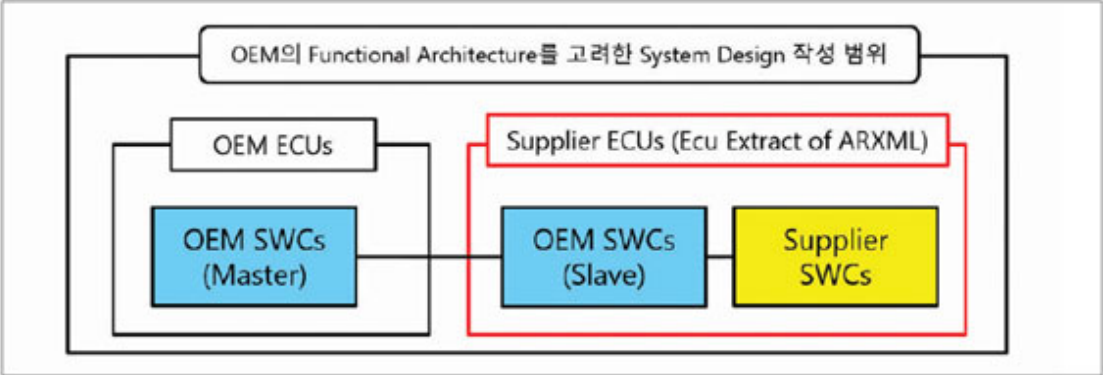


그림 1 | AUTOSAR 4.x 기반 Master-Slave 형식의 OEM SWCs 개념도

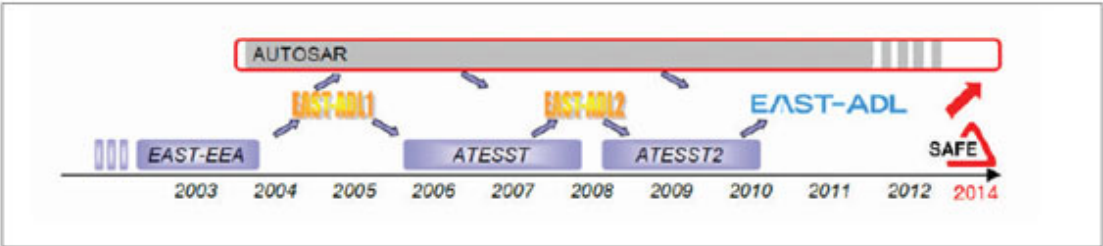




그림 2 | 유럽 중심의 Functional Architecture와 AUTOSAR 발전 출처 | http://www.east-adl.info

(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)

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)

Master-Slave 형식의 개념은 1대 차량에 탑재되는 핵심이 되는 Supplier의 ECU에 OEM이 Supplier로부터 필요한 정보를 인식/판단/제어하기 위해서 개발한 SW를 Slave 역할로 탑재를 하고, OEM이 개발한 ECU에서 Master 역할로 SW로 개발해 다른 OEM과 차별화된 Vehicle level의 기능 구현할 수 있다(그림 1). Vehicle level의 기능 구현 예를 들면 자율주행, 고안전, 고편의, 연비향상 등이 포함된다.

위와 같은 내용을 언급한 이유는 ISO 26262 Part3을 왜 OEM이 주도해 진행해야 하는지를 설명하기 위해서다.

## Functional Architecture 소개

2003년부터 유럽 중심으로 OEM-서플라이어 간 협업 관계 강화를 위해 Architecture 관점에서 해결책을 고민하기 시작해 AUTOSAR에 피드백해 반영하고 있다(그림 2). 그 결과물인 Functional Architecture는 OEM 입장에서 여러 서플라이어와의 협업에서, Vehicle level에서 System design level까지 Architecture를 고려해 Vehicle 기능을 효율화하는 것이다.

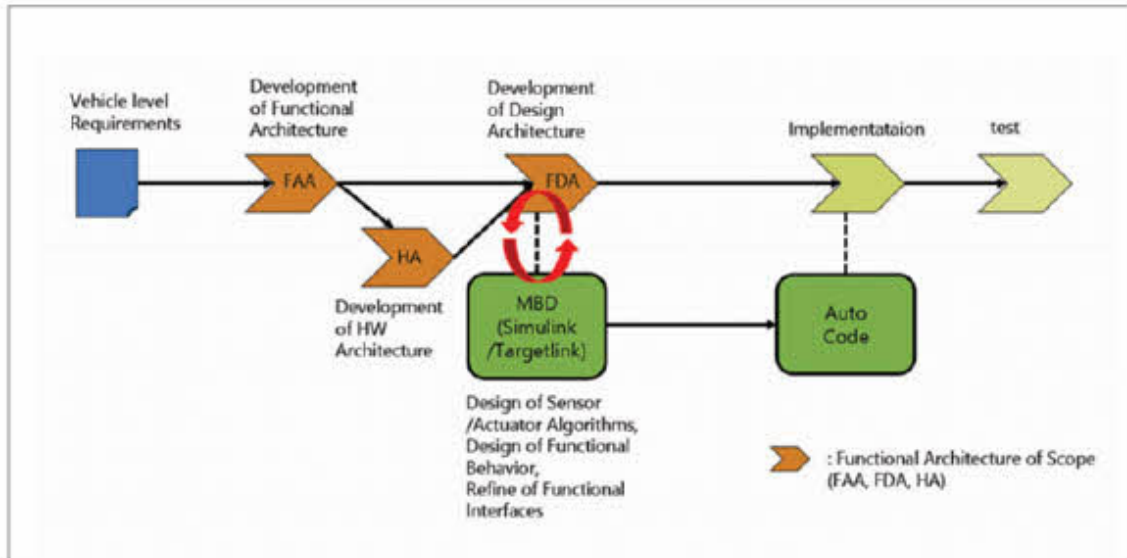


그림 3 | OEM 주도 Top-down 방식의 MBD를 고려한 EASIS Engineering Process

주 | FAA : Functional Analysis Architecture, FDA : Functional Design Architecture, HA : Hardware Architecture

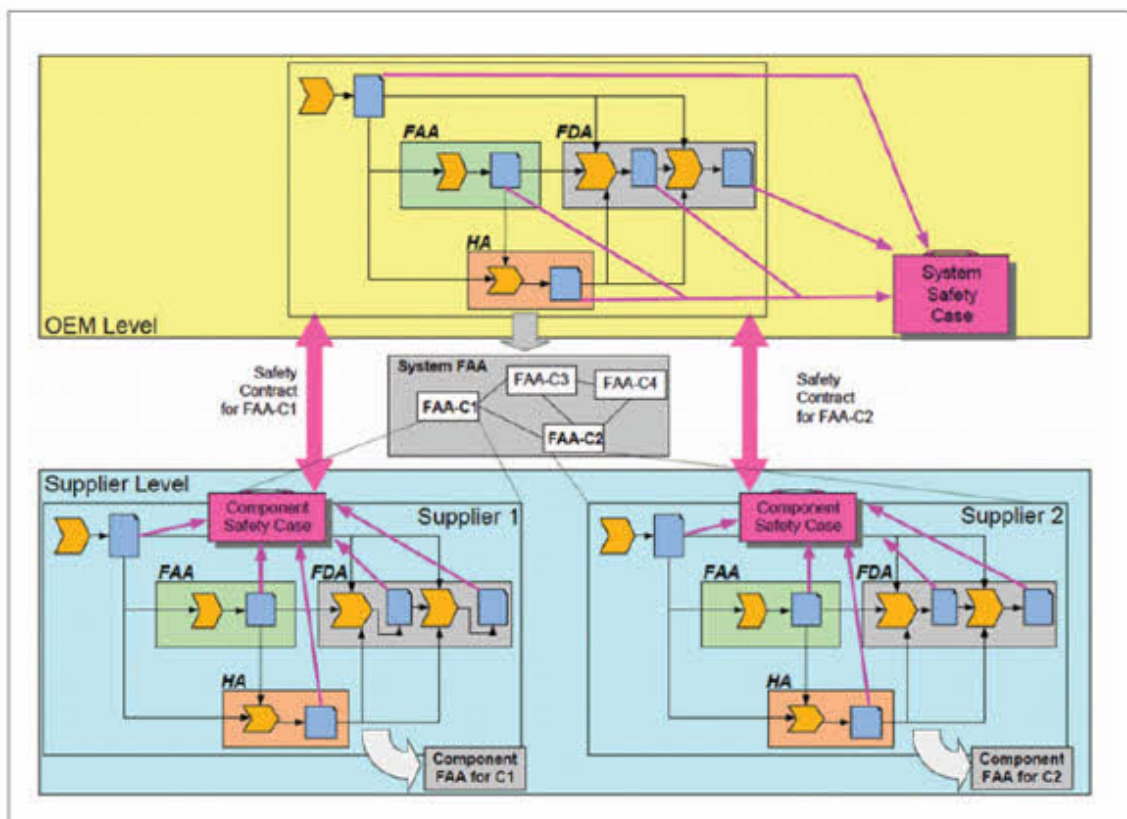


그림 4 | ISO 26262(Safety Case)를 고려한 EASIS Engineering Process

출처 | ATESS의 EASIS Deliverable D4.1, Figure A1-8

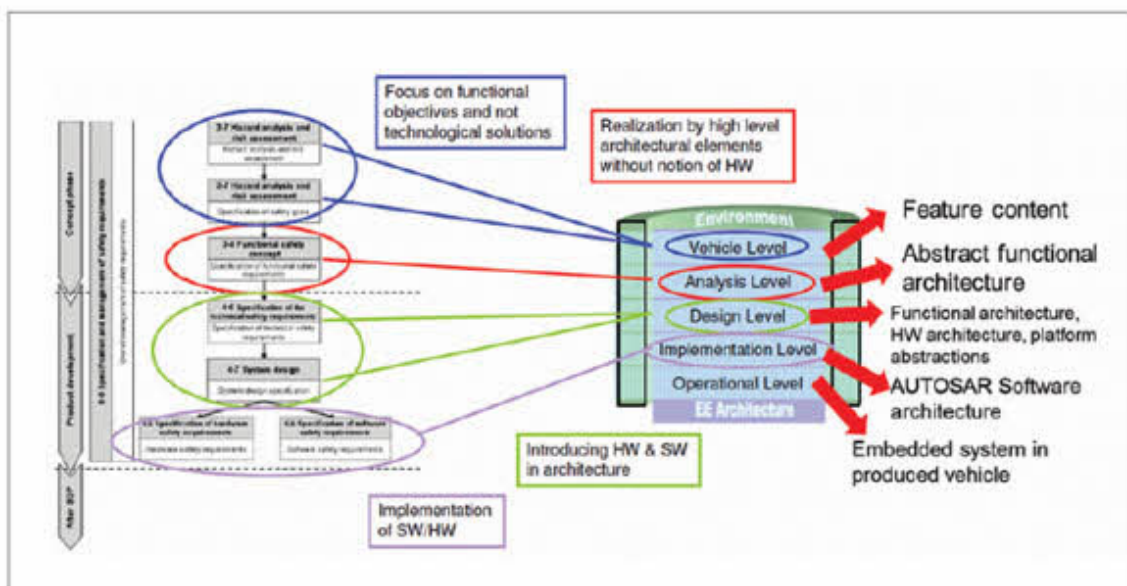


그림 5 | ISO 26262, AUTOSAR, Functional Architecture 관계도

Functional Architecture는 AUTOSAR 뿐만 아니라, ISO 26262와 MBD(Model Based Development)의 개념을 포함시켜, EASIS(Electronic Architecture and System Engineering for Integrated Safety Systems) Engineering Process를 정립했다(그림 3 ~ 6).

현재 해외 OEM은 EASIS Engineering Process를 바탕으로 OEM-서플라이어 협업 프로세스를 자체적으로 만들어 서플라이어에게 RFQ로 자사의 OEM-서플라이어의 협업 프로세스에 대한 설명과 해당 프로세스를 따라 개발 납품할 것을 요구하고 있다.

**ISO 26262 Part3 Concept Phase**

ISO 26262의 Part3은 4가지 프로세스를 가지며 다음과 같다.

- 1. 3-5 Item definition: 개발할 ECU의 ISO 26262 적용 대상 범위에 대한 Item 정의
- 2. 3-6 Initiation of the safety lifecycle: Part2의 Safety Plan(2-6.5.1)에 대한 재정립
- 3. 3-7 Hazard Analysis and risk assessment: H&R를 통한 Safety Goal과 ASIL 등급 정의
- 4. 3-8 Functional safety concept: Functional Safety Requirement(FSR)를 정리

ISO 26262의 전체 업무 프로세스는 1. 개발할 ECU의 대상 범위에 대한 Item 정의를 시작으로, 2. OEM과 서플라이어의 기존에 준비된 Internal process(내부 프로세스)인 Part2 기능안전성 관리(Management of functional safety)의 Safety Plan(2-6.5.1)을 바탕으로 쌍방 간의 Safety Plan을 재정립해, 3. OEM 주도로 서플라이어와 함께 Part3는 콘셉트 단계 (Concept Phase)의 Hazard Analysis and risk assessment(H&R)를 실시하고, 이후 OEM과 서플라이어는 Part8 지원 프로세스(Supporting processes)의 Development interface agreement(DIA, 8-5.5.2)를 체결한다. 그런 다음에 4. OEM과 서플라이어가 협력해 Functional safety concept를 피드백해 실시한다.

DIA는 OEM-서플라이어의 개발협력 계약서로 OEM과 서플라이어 쌍방이 Safety Manager를 지정해, ISO 26262의 각각 Work Product(산출물)에 대해 OEM과 서플라이어가 수행할 역할과 책임자를 결정, 공동으로 Safety life cycle과 설계 자료에 대한 합의, 쌍방의 정보교환에 대한 내용 기술, 서플라이어 컴포넌트의 ASIL 등급 지정, Supporting processes 및 Confidence in the use of software tools(Tool의 적합성 확인), 보고 경로 규정과 안전성에 관련된 사항 보고, Safety Assessment 활동의 코디네이트 등을 협의한다.

참고로 해외 OEM의 RFQ에는 ASIL 등급의 목표가 명시돼 있다.



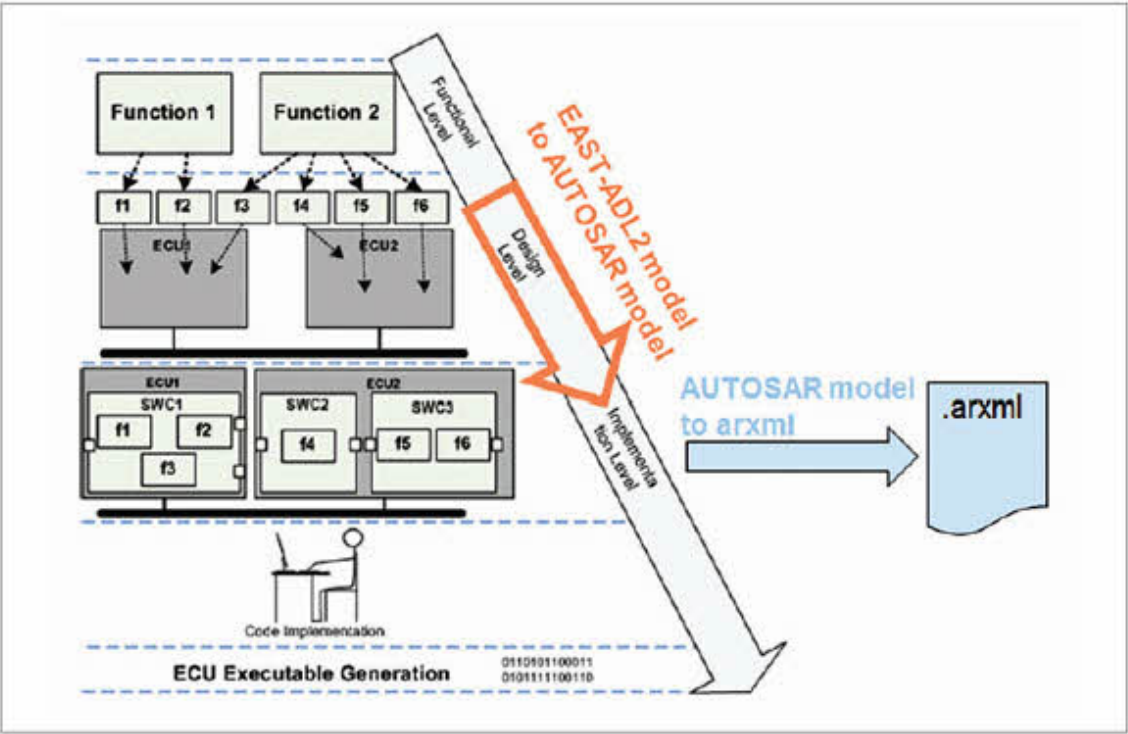


그림 6 | OEM의 Functional Architecture에서 서플라이어에게 AUTOSAR Ecu Extract of ARXML 전달 과정 출처 | MAENAD Deliverable D6.1.3 Figure 5-13

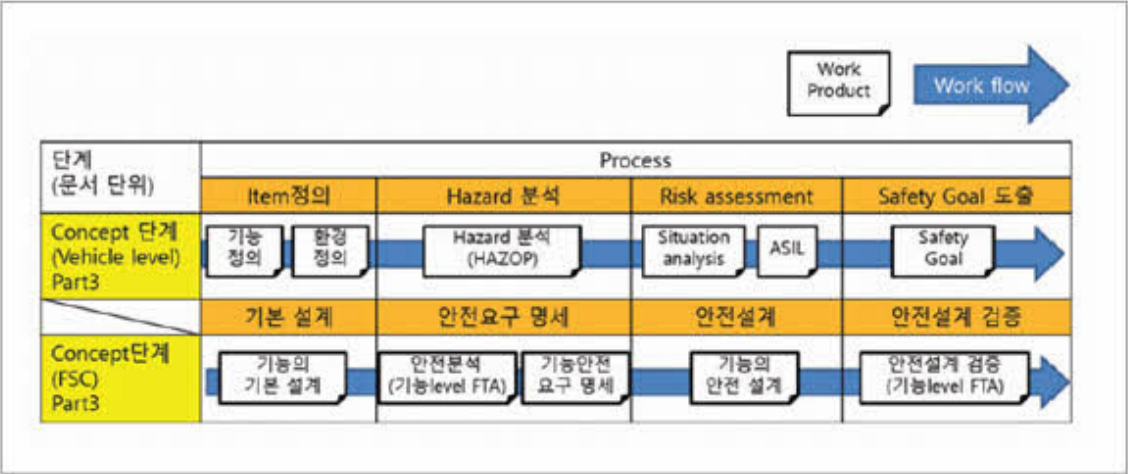


그림 7 | JASPAR의 ISO 26262 Part 3 업무 프로세스 출처 | Functional Safety Technical Templates(System Development Technical Safety Concepts Edition).doc의 Figure 11

표 2 | JASPAR의 EPB에 대한 Safety Goal 예

Safety Goal ID	EPB-SG-001
Hazard ID	HAZ_01
Hazard	의도하지 않는 급제동
ASIL	B
Safe State	Lock 해제
최상의 안전요구 사항	의도하지 않는 주차 브레이크 록이 발생한 경우, 운전자가 제어 가능한 시간 내에 록을 해제

### JASPAR의 ISO 26262 가이드라인 Part3 Concept Phase

일본 JASPAR에서 Part3은 OEM 주도하에 실시한 내용이라고 판단해, ISO 26262 가이드라인에서 제외시켰다. 그렇지만, 올해 4월 1차 기능안전성 정기회의를 통해 Part3의 업무 내용에 대해 간단하게 설명했는데, 이때 EPB(Electronic Parking Brake)에 대해 Part3의 적용사례를 설명했다.

그림 7의 Part3 업무 프로세스와 같이 개발할 ECU Item의 대상 범위를 정의하고, Part3-7 H&R에서 HAZOP(HAZard Analysis and OPerability study)을 실시해 여러 개의 Hazard를 식별하고 Safety Goal과 ASIL 등급을 정의했다(표 2). 그리고 Safety Goal과 ASIL 등급을 바탕으로 FTA(Fault Tree Analysis)를 실시해 FSR(Functional Safety Requirement)을 도출하고 Part3-8 FSC(Functional Safety Concept)를 완성했다. 참고로 FSC는 여러 개의 FSR의 총 묶음을 의미한다.

마지막으로 안전설계를 검증하기 위해서 FTA(Fault Tree Analysis)를 실시해 누락되거나 잘못 지정된 Basic Event가 없는 지 재확인한다. 참고로 Basic Event는 TopEvent를 결함(failure)으로 이르게 하는 하나의 사상(Event)이다(그림 8). JASPAR의 ISO 26262 가이드라인 Part3의 FSC에서는 기능(function) level FTA를 수행하며 구체적인 HW Component를 고려하지 않은 Vehicle level 기능을 중심으로 FTA를 실시하는 것이 특징이다. 또 Quantitative(정량적) FTA처럼 FIT(고장률을 나타내는 단위로 10억 시간에 1회 고장)를 계산하지 않는다.

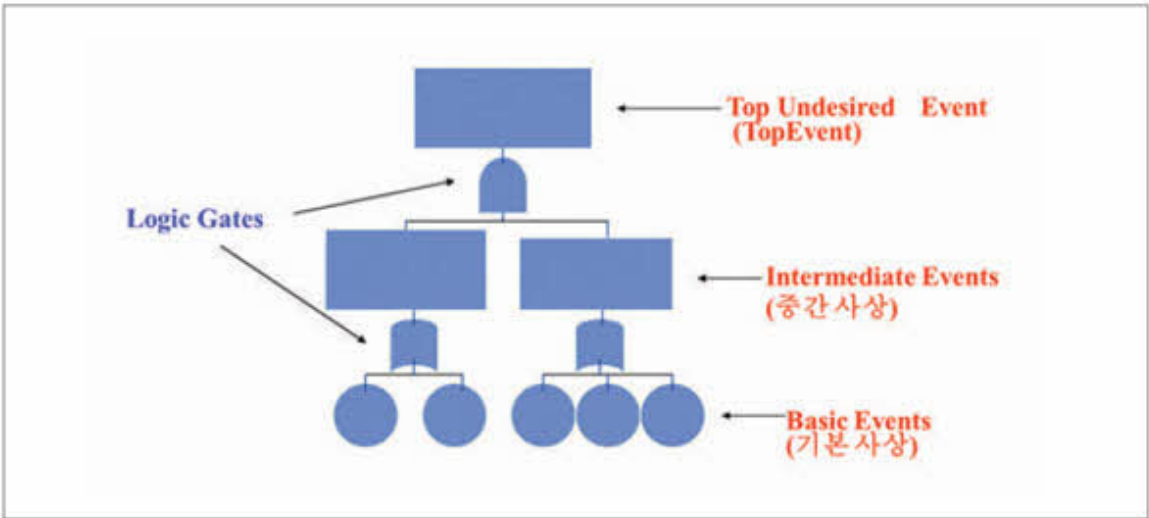


그림 8 | FTA의 구조와 도형에 관한 용어  
 주 | ISO 26262 Safety Analysis에 주로 사용하는 표준, IEC 61882:2001 Hazard and operability studies(HAZOP studies) – Application guide, IEC 61025:2006 Fault tree Analysis(FTA), IEC 60812:2006 Analysis techniques for system reliability – Procedure for failure mode and effects Analysis(FMEA)

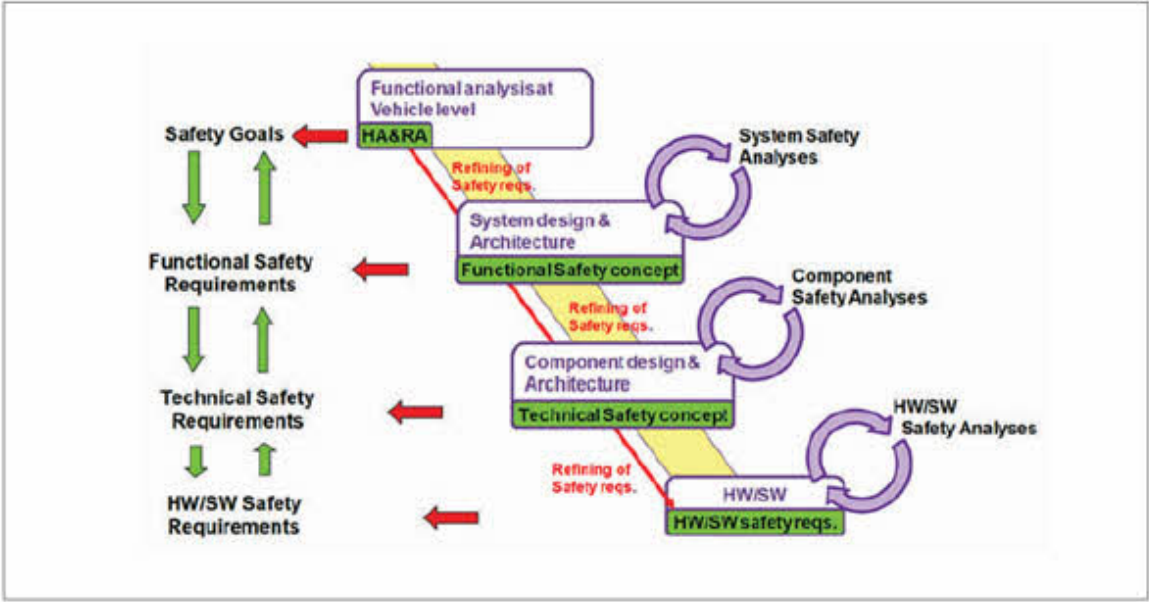


그림 9 | SAFE의 Safety Analyses 업무 프로세스  
 출처 | SAFE D3.3.1.a.2의 Figure 2

표 3 | JASPAR의 EPB에 대한 FSR(Functional Safety Requirement) 예

ID	EPB-SG-001
Function Block	HAZ_01
Basic Event	시스템 이상은 의도하지 않은 주차 브레이크 록이 발생할 가능성
안전요구 시험	시속 10Km/h 이상에서 핸드 브레이크 케이블에 OON 이상의 장력이 100ms 이상 출력되지 않도록 장력을 약하게 주차 브레이크 록을 해제
ASIL	B
Fault Tolerant Time Interval	100ms
operating modes	-
Emergency Operation Interval	-

유럽 SAFE의 ISO 26262 가이드라인에서 Part3 Concept Phase

유럽 SAFE의 ISO 26262 가이드라인은 OEM-서플라이어가 협력해 ISO 26262 Work Product를 데이터베이스로 XML을 도입 정형화를 목표로 하고 있다. 따라서 구체적인 데이터 정보가 언급돼 있다. 또 지난 연재에서도 언급했듯이 SAFE의 ISO 26262 가이드라인은 ISO 26262의 Part별로 나눠지지 않고 여기저기 분리돼 있어, ISO 26262 표준문서 Part1 ~ 10까지 정독해 이해한 후에 SAFE의 ISO 26262 가이드라인을 보지 않으면 전체 구성을 알아보기 힘들게 돼 있다.



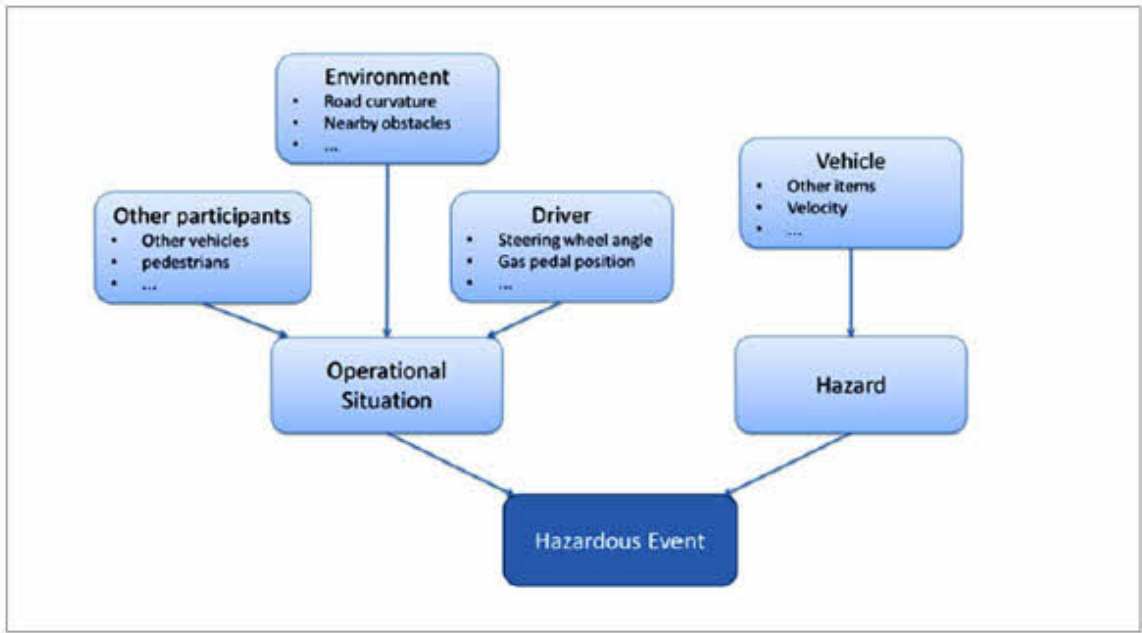


그림 10 | SAFE의 Hazardous Event에 대한 구체적인 시나리오 요구  
출처 | SAFE D3.1.1.b의 Figure 3

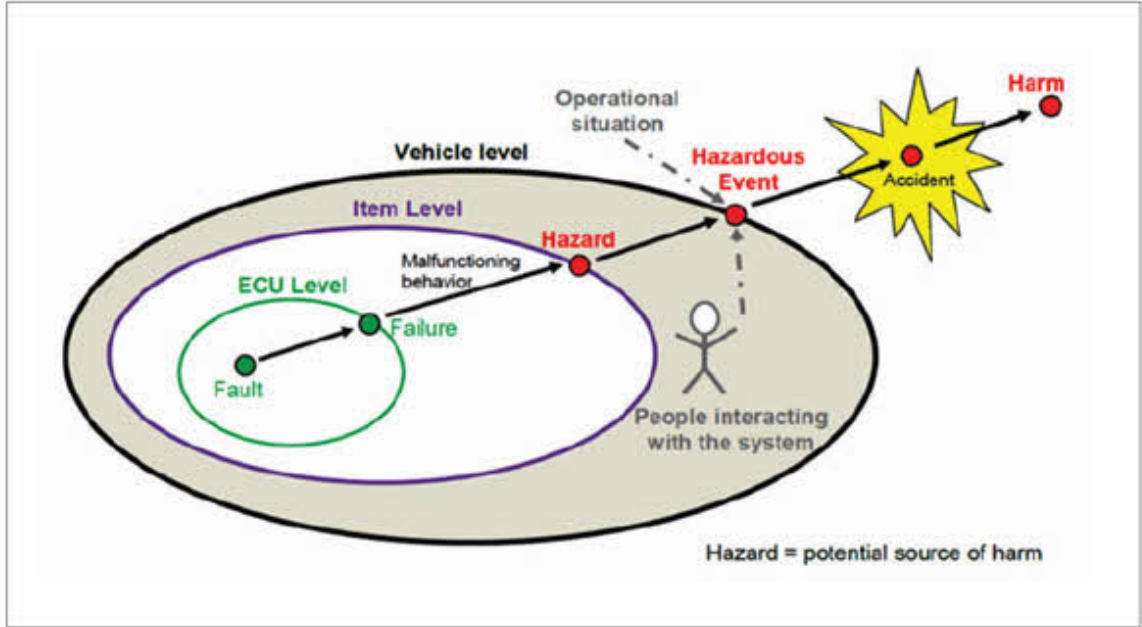


그림 11 | Hazardous Event 개념도  
출처 | SAFE D3.3.1.a.2의 Figure 4

	ASIL A	ASIL B	ASIL C	ASIL D
Residual risk Metric	Nothing required or recommended	$< 10^{-7} / h$ Recommended	$< 10^{-7} / h$ Required	$< 10^{-8} / h$ Required

그림 12 | Metrics allocation by ISO 26262  
출처 | SAFE D3.3.1.b의 Table 4)

표 4 | ISO 26262 Part3에 대한 일본과 유럽의 비교

국가	일본 JASPAR	유럽 SAFE
Part3-7 H&R	H&R을 위해 HAZOP이라는 Safety Analysis 기법 사용	Hazardous Event를 바탕으로 구체적인 차량 시나리오 내용이 기술되기를 요구
Part3-8 FSC	기능(Function) Level FTA들 실시 Basic Event를 바탕으로 FSRs를 도출하며, FTA에서는 FIT 값을 계산 요구하지 않음	SFMEA(System FMEA) → Qual.(정성적) FTA → Quant.(정량적) FTA를 실시하는데, SFMEA에서는 Safety Mechanism을 고려하지 않은 것과 고려한 것의 효과가 기술이 되어 하며, Quant.(정량적) FTA에서는 FIT 값 계산을 요구하며, FSRs를 도출

참고로 ISO 26262 Part3에 관련된 SAFE의 문서로는 아래와 같은 3가지 문서를 집중적으로 읽어보면 된다.

1. D3.1.1.b Update of final proposal for extension of SAFE meta model for safety requirement expression modeling
2. D3.1.2.c Update of final proposal for extension of SAFE meta model for safety requirement expression modeling
3. D3.3.1b Methodology and Tool specification for analysis of qualitative and quantitative cut-sets issued from error failure propagation analyses

SAFE는 Part 3-7 H&R에 대해 JASPAR처럼 HAZOP 등과 같은 Safety Analysis를 요구하지 않으며, Safety Requirement를 도출하기 위해서만 Safety Analyses를 실시한다(그림 9). 또한 SAFE의 설명에 따르면, 3-7 H&R에서 Hazardous Event(1개의 Operational Situation과 1개 Hazard의 조합을 의미하며, Hazardous Event 발생하면 Safety Goal을 위배함)를 도출해 Safety Goal과 ASIL 등급을 결정해야 하며, JASPAR의 HAZOP과는 다르게, 구체적인 차량 시나리오 내용이 기술되기를 요구한다(그림 10 ~ 11).

SAFE에서는 Part3-8 FSC(Functional Safety Concept)을 도출하기 위해 Safety Analyses를 다음과 같이 SFMEA(System FMEA) → Qual.(정성적) FTA → Quant.(정량적) FTA를 실시하는데, SFMEA에서는 Safety Mechanism을 고려하지 않은 것

과 고려한 것의 효과가 기술이 돼야 하며, Quant.(정량적) FTA에서는 FIT 값을 계산해 Part5-9.4.2.1의 Table6의 ASIL 등급에 따른 Residual Risk Metric을 만족해야 하도록 해야 한다(그림 12).

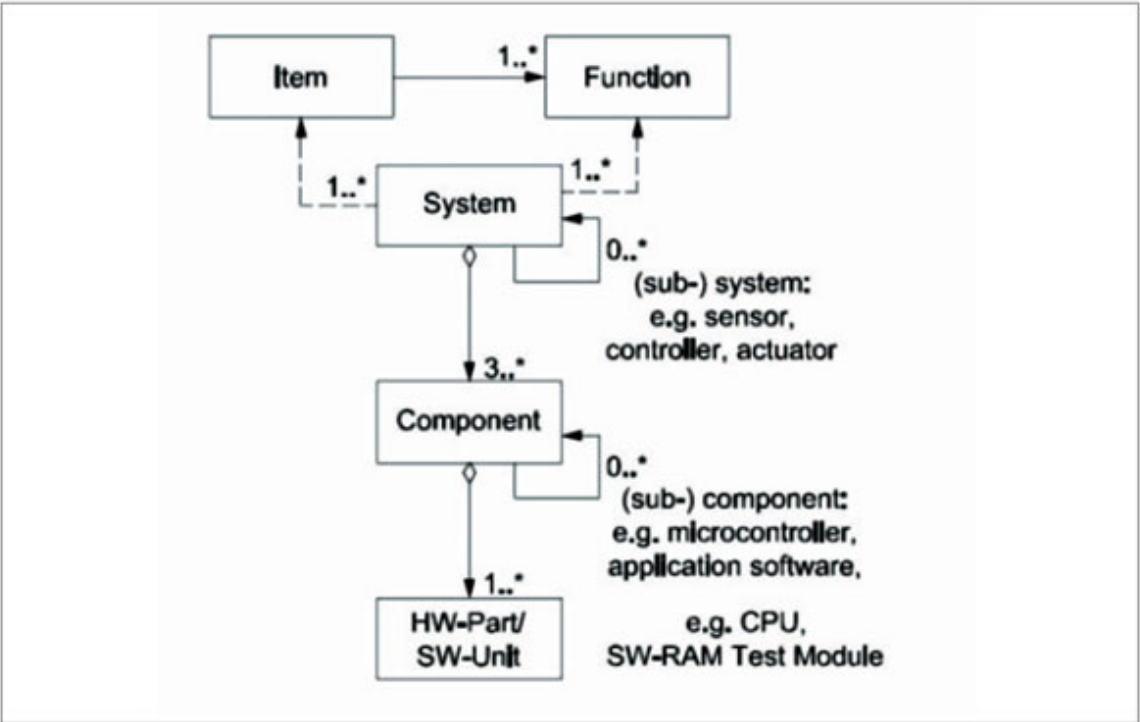


그림 13 | ISO 26262의 Item, Function, System, Component, HW-Part/SW-Unit 관계도  
출처 | ISO 26262 Part10의 Figure 3

일본과 유럽의 ISO 26262 Part3 가이드라인 비교

일본 JASPAR의 ISO 26262 가이드라인은 서플라이어가 최소한의 범위로 작성해야 하는 내용을 중심으로 작성됐으나, 유럽 SAFE는 OEM-서플라이어가 협력해 최대한의 범위로 작성해야 하는 내용을 중심으로 구체적으로 기술돼 있다. 그림 10의 ISO 26262 Part10의 Figure3을 바탕으로 ISO 26262 level에 대해서 그림 13과 같이 정의했다. 유럽 SAFE에서는 OEM이 Functional Architecture를 고려해 Item의 Function(기능)을 정의하는 것을 시작으로 ISO 26262 대응이 필요하다.

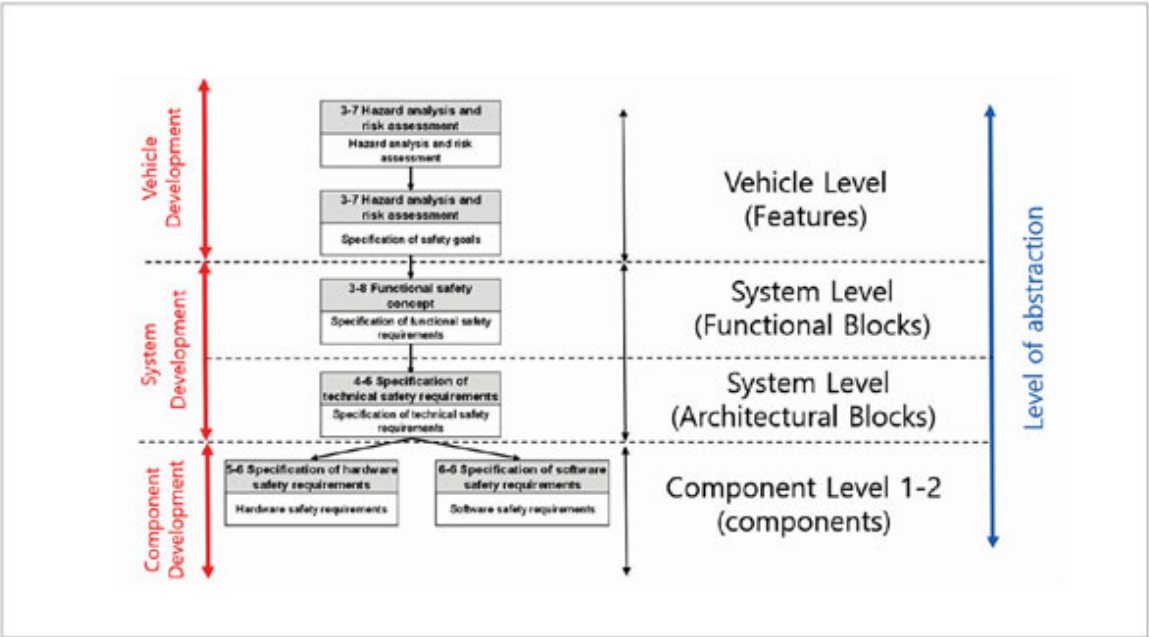


그림 14 | SAFE에서 정의한 ISO 26262 level 계층도

마치며

필자는 Part3에 대해 좀 더 자세한 내용을 기술하고 싶었으나, 페이지 제한으로 많은 정보를 독자들에게 전달하지 못한 것이 아쉽다. 국내에서도 OEM이 주도해 Functional Architecture를 고려, ISO 26262 Part3을 정의하고, 서플라이어가 ISO 26262에 잘 대응할 수 있도록 협력하는 것이 중요하다.

유럽 SAFE에서는 올 11월 30일까지 새로운 ISO 26262 가이드라인 문서를 지속적으로 공개하고 있기 때문에 정보를 모니터링하면서 공부할 필요가 있다. 다음 연재에서는 “3. ISO 26262 Part4 가이드라인 - System”을 설명하면서 역시 일본과 유럽 가이드라인의 차이를 다룰 예정이다.

<저작권자(c)스마트앤컴퍼니. 무단전재-재배포금지>

100자평 쓰기 로그인

로그인후 입력하세요

등록

회사소개 (<http://www.smartn.co.kr>)   개인정보취급방침 (</member/protect.asp>)   이메일주소 무단수집 거부 (</member/noemailcollect.asp>)

온라인 문의 (</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, 코오롱사이언스밸리1차)   P: (Phone) 02-841-0017   F: (Fax) 02-841-0584   ✉ [webmaster@smartn.co.kr](mailto:webmaster@smartn.co.kr)

© Smart & Company