ISO 26262 해외 가이드라인 쉽게 이해하기

2015년 01월호 지면기사 / 글 | 채 승 엽 _ sychae@ssu.ac.kr

채승엽 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

Part5 반도체 공급받은
Supplier의 하드웨어 개발

ISO 26262는 기능안전성이 요구되는 시스템(ISO 26262, Part4)을 기준으로 하드웨어(ISO 26262, Part 5)와 소프트웨어(ISO 26262, 6)를 고려해 개발이 병렬적으로 진행된다. 그리고 ISO 26262 Part5의 하드웨어 경우는 그림 1과 같은 절차로 개발이 진행된다. 차량 반도체 회사로부터 반도체(MCU, ASIC 등)를 공급받아 Part5를 준수해 ECU 개발을 진행하게 되는데, 일반적으로 차량용 반도체를 공급하는 회사는 최종적으로 차량 반도체가 탑재될 제품이나 시스템의 요구사항을 모르는 상황에서 하드웨어를 충족시키며 개발하는 어려움이 있다.

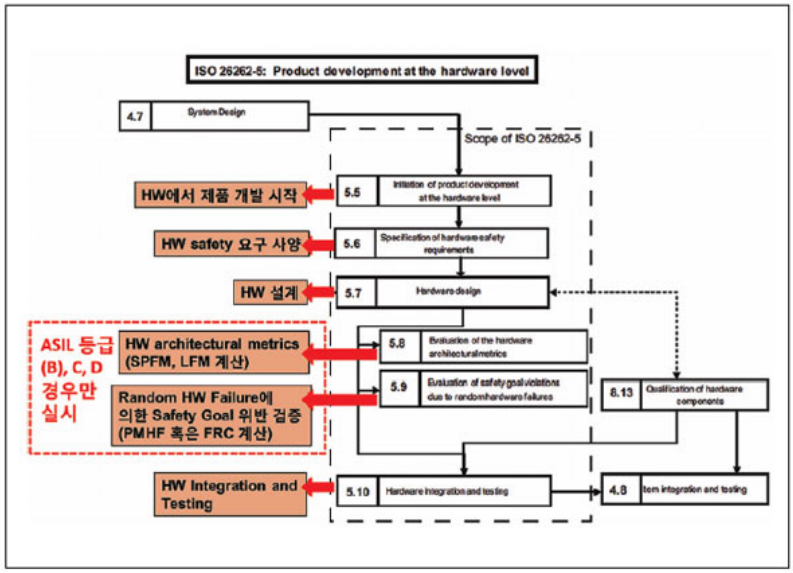


그림 1| ISO 26262 Part5의 하드웨어 양산 개발 절차(ISO 26262 Part5, Figure2)

이러한 상황을 해결하기 위해 ISO 26262에 도입된 개념이 SEooC(Safety Element out of Context)다. Out of Context는 특정 시스템에 해당하는 Context의 범위 밖에서 시스템을 모르는 상태에서 개발한다는 의미다. 즉 일반적인 차량 반도체 회사는 최종 시스템에 대해 적절한 가정을 하고 그에 따라 차량 반도체를 개발한다. 하드웨어에 대한 SEooC인 그림 2를 보면 시스템의 Part4-6~7과 Part 5-5~10에서 차량용 반도체가 고려할 산출물(Work Product)을 선정해 차량 반도체를 개발한다.

일반적으로 차량 반도체는 Part 5-6~9를 실시해 작성된 산출물을 Safety Manual이라고 지칭하는데, 이를 최종 시스템을

개발하는 고객에게 제공하고 있다. 또 차량 반도체 회사는 차량 반도체 간의 경쟁에서 앞서기 위해 고객 시스템 개발에 도움을 주고자 자사 반도체 특징과 연계돼 적용된 Safety Mechanism을 소프트웨어 라이브러리 형태로 제공하고 있다. 예를 들어 인피니언의 멀티코어 AURIX 경우는 Safety Mechanism에 대한 소프트웨어로 "SafeTlib"의 솔루션으로 34개 이상의 AURIX에 의존하는 Safety Mechanism을 유상으로 제공하고 있다.

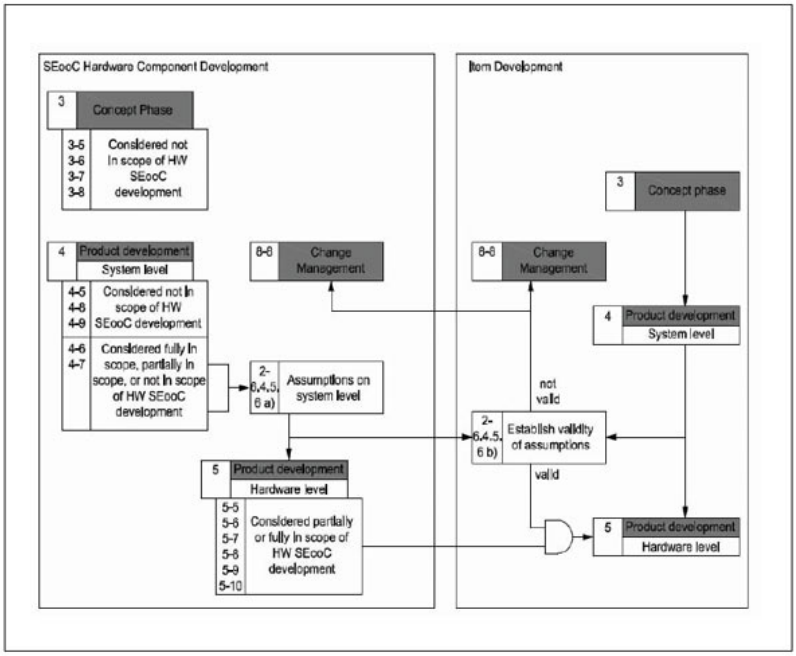


그림 2 | SEooC hardware component development(ISO 26262 Part10, Figure 20)

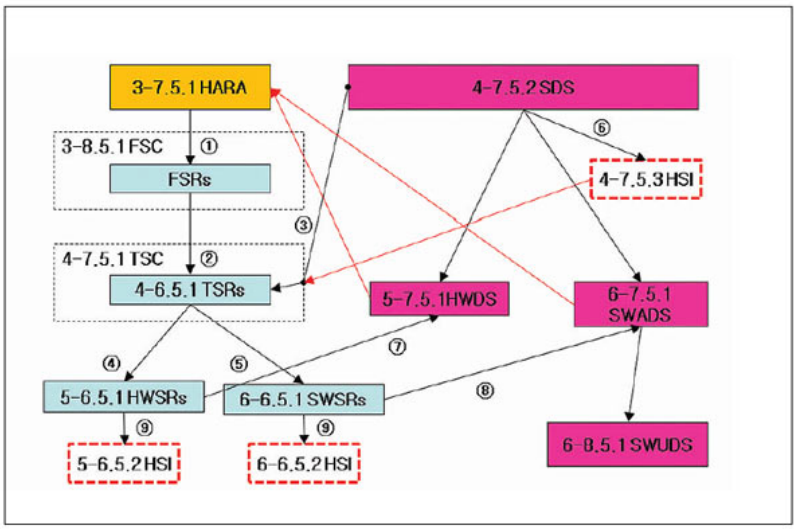
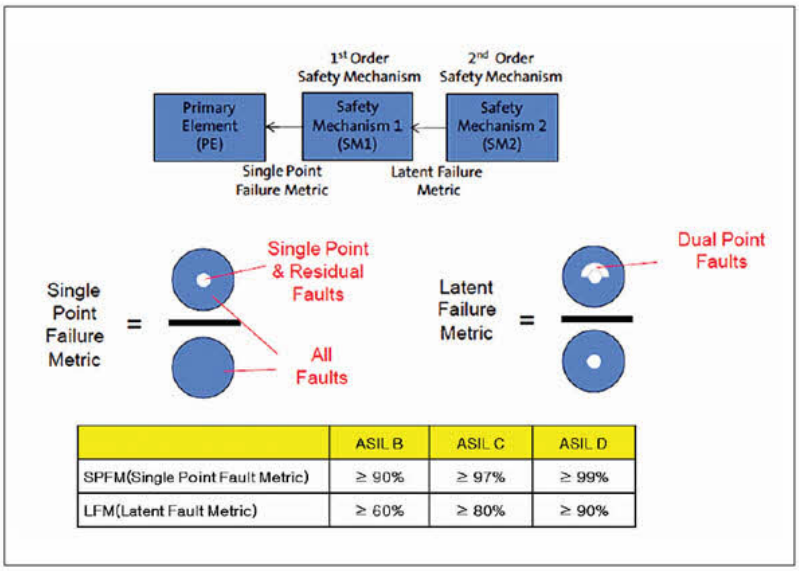


그림 3 | ISO 26262 전체 업무에서 HSI의 업무 순서 및 연계성

반도체 회사로부터 제공되는 Safety Manual과 Safety Mechanism은 이 회사의 기술 지원을 받지 않고서는 원하는 목적의 제품을 개발하기 어려워 협업이 필요하다. 뿐만 아니라, 전장부품 개발사는 내부의 하드웨어와 소프트웨어 개발 책임자가 공동작업해 ISO 26262의 HSI (Hardware Software Interface) 명세서를 작성하고 제품 개발 완료까지 검증을 진행해야 한다. HSI는 그림 3처럼 시스템(Part4), 하드웨어(Part5), 소프트웨어(Part6)에서 제품 개발 전반에 반복하며, 하드웨어와 소프트웨어 개발 책임자가 공동으로 검증을 진행해야 한다. HSI의 구체적인 검증 내용은 다음과 같다.

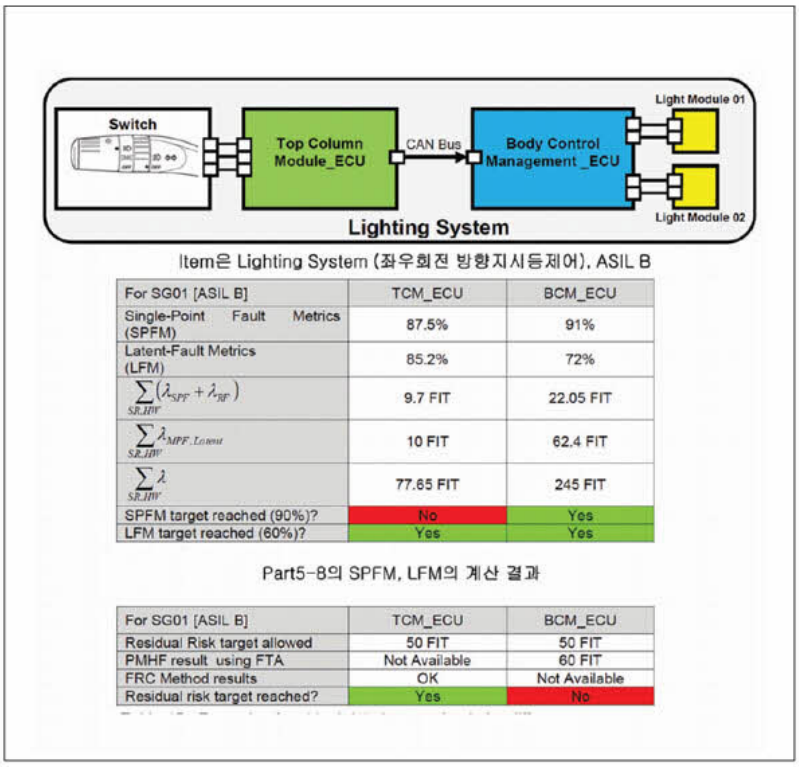
a) Part4-6.5.1 TSRs(기술 안전요구)와 Part4-7.5.2 SDS(시스템 설계)를 준수
b) Part5-6.5.1 HWSR(하드웨어 안전요구)에 대해서 일관성
c) ASIL이 올바르게 Part6-6.5.1 SWSR(소프트웨어 안전요구)와 Part5-6.5.1 HWSR(하드웨어 안전요구)에 맞게 할당. 구체적으로 작성한 Part6-6.5.1 SWSR(소프트웨어 안전요구)와 Part6-6.5.1 HWSR(하드웨어 안전요구)는 ASIL 할당이 해당 명세를 바탕으로 상위 요구(FSR, TSR)에서 잘 반영 여부.
d) Part4-6.5.1 TSRs(기술 안전요구)를 바탕으로 명확히 Part6-6.5.1 SWSR(소프트웨어 안전요구)와 Part5-6.5.1 HWSR(하드웨어 안전요구)이 구현 되었는지 여부.

참고로 Part4-7.5.3, Part5-6.5.2, Part6-6.5.2의 HSI문서는 동일한 문서이며, Part4-7.5.3에서 처음 작성돼서 Part5-6.5.2, Part6-6.5.2에서 업데이트가 되는 것이다.



	ASIL B	ASIL C	ASIL D
SPFM(Single Point Fault Metric)	≥ 90%	≥ 97%	≥ 99%
LFM(Latent Fault Metric)	≥ 60%	≥ 80%	≥ 90%

그림 4 | ISO 26262 Part5-8.5.1의 SPFM(Single Point Faults Metric)과 LFM(Latent Faults Metric)



Item은 Lighting System (좌우회전 방향지시등제어), ASIL B

For SG01 [ASIL B]	TCM_ECU	BCM_ECU
Single-Point Fault Metrics (SPFM)	87.5%	91%
Latent-Fault Metrics (LFM)	85.2%	72%
$\sum_{SR,HW}(\lambda_{SPF}+\lambda_{RF})$	9.7 FIT	22.05 FIT
$\sum_{SR,HW}\lambda_{MPF,Latent}$	10 FIT	62.4 FIT
$\sum_{SR,HW}\lambda$	77.65 FIT	245 FIT
SPFM target reached (90%)?	No	Yes
LFM target reached (60%)?	Yes	Yes

Part5-8의 SPFM, LFM의 계산 결과

For SG01 [ASIL B]	TCM_ECU	BCM_ECU
Residual Risk target allowed	50 FIT	50 FIT
PMHF result using FTA	Not Available	60 FIT
FRC Method results	OK	Not Available
Residual risk target reached?	Yes	No

그림 5 | Part5-9의 실시함에 있어서 Part5-8의 연관 관계 출처 | SAFE, D3.3.1.b, 2014.02

ISO 26262

Part5 Product development at the hardware level

ISO 26262의 Part5는 6가지 프로세스를 가지고 있으며, 다음과 같다.
특히 사항은 Part5-8과 Part5-9는 ASIL A일 경우에는 프로세스를 진행하지 않으며, ASIL C, D는 필수다. ASIL B인 경우에는 OEM이 요청한 경우만 프로세스를 수행한다.

① 5-5 Initiation of product development at the hard ware level: Part4-5에서 실시한 Project/Safety/ Item integration and testing plan의 업데이트된 내용을 고려해 하드웨어 일정을 다시 고려해서 Part5-5.5 Safety plan을 업데이트한다.

② 5-6 Specification of hard ware safety requirements: Part4-7.5.1 TSC (Technical Safety Concept), Part4-7.5.2 SDS(System Design Specification), Part4-7.5.3 HSI(Hardware Software Interface Specification)을 고려해 Part5-6.5.1 HWSR(Hard ware Safety Requirements Specification: including test and qualification criteria)을 작성하고, Part5-6.5.2 HSI(Hardware Software Interface Specification)을 업데이트 한다. 또한 Part5-6.5.3 Hardware Safety Requirements Verification Report를 작성한다.

③ 5-7 Hardware design: Part5-6.5.1 HWSR(Hardware Safety Requirements Specification: including test and qualification criteria) , Part5-6.5.2 HSI(Hardware Software Interface Specification), Part4-7.5.2 SDS(System Design Specification)을 고려해 Part5-7.5.1 HWDS(Hardware Design Specification), Part5-7.5.2 Hardware Safety Analysis

Report, Part5-7.5.3 Hardware Design Verification Report를 작성한다. 또한 Part5-7.5.4 Specification of requirements related to production, operation, service and decommissioning로 하드웨어 대해 생산, 운영, 서비스, 폐기에서 어떻게 할 것인지 요구사항을 작성한다.

④ 5-8 Evaluation of the hardware architectural metrics: Part5-8.5.1 Analysis of the effectiveness of the architecture of the item to cope with the random hardware failures를 실시하는데, Part8-13 Qualification of hardware components에서 각각의 반도체 및 부품회사에서 제공받은 FIT(Failure in Time, 1 FIT는 10억 시간당 1회 고장이 발생한다는 의미) 값을 참고해 SPFM(Single-Point Fault Metric)과 LFM(Latent-Fault Metric)의 수치를 계산해 작성한다(그림 4). 그리고 계산된 결과가 제대로 돼 있는지, Part5-8.5.2 Review report of evaluation of the effectiveness of the architecture of the item to cope with the random hardware failures를 작성한다.

⑤ 5-9 Evaluation of safety goal violations due to random: Part5-8에서 계산한 SPFM과 LFM이 ASIL B, C, D의 등급에서 요구하는 값을 만족하는 경우에는 Part5-9.4.2 Evaluation of Probabilistic Metric for random Hardware Failures(PMHF)의 PMHF 수치를 계산하면 되고, 만족하지 않는 경우에는 Part5- 9.4.3 Evaluation of each cause of safety goal violation에서 추가적 Safety Mechanism을 고려해 FRC(Failure Rate Class) 값을 계산하다. Part5-9.4.2 혹은 Part5-9.4.3의 결과를 바탕으로 Part5-9-1 Analysis of safety goal violations due to random hardware failures을 작성하고, 이에 대한 FIT의 상세한 근거를 Part5-9.5.2 Specification of dedicated measures for hardware, if needed, including the rationale regarding the effectiveness of the dedicated measures로 작성한다.

또 Part5-9가 제대로 수행됐었는지 Part5-9.5.3 Review report of evaluation of safety goal violations due to random hardware failures를 작성한다.

5-9에 대해서 예를 들면, 그림 5와 같이 좌우회전 방향지시등 제어 시스템에 대해서 Item으로 Lighting System을 정하고 ASIL B의 Safety Goal을 가지게 될 경우, SPFM 90% 이상, LFM 60% 이상 값을 가져야 한다. TCM ECU는 SPFM이 87.5%로 90% 이상이 되지 않으므로, Part5-9.4.3로 대응해 FRC로 계산했으며, BCM ECU의 경우는 SPFM과 LFM이 둘 다 만족됨으로 Part5-9.4.2로 대응해 PMHF로 계산했다.

⑥ 5-10 Hardware integration and testing : 하드웨어 통합 테스트를 실시하고 Part5-10.5 Hardware integration and testing report를 작성한다.

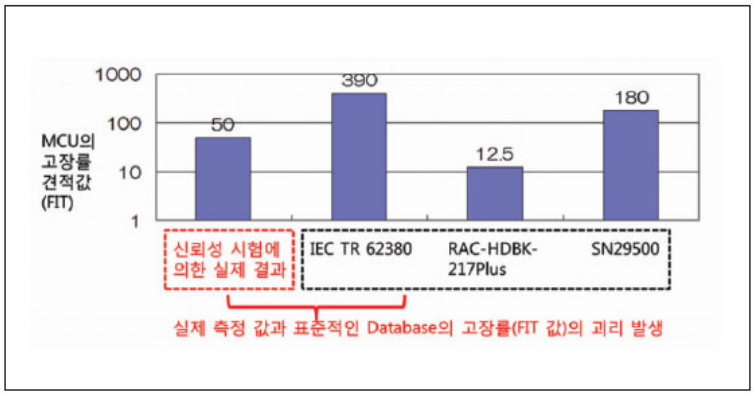


그림 6 | 실제 측정 값과 표준적인 Database의 고장률(FIT값)의 괴리

표 1 | ISO 26262 Part3에 대한 일본과 유럽의 Block 개념 비교

국가	일본 JASPAR	유럽 SAFE
Part5	ISO 26262 Part5에서 부족한 MCU와 ASIC에 내용을 자세히 설명	ISO 26262 Part5의 업무 절차를 자세히 설명
	Part5-9.4.2의 PMHF만 대응함	Part5-9.4.2의 PMHF와 Part5-9.4.3의 FRC로 나누어서 대응함
	JASPAR는 일본 OEM에 납품하기 위한 Tier1의 입장에서의 ISO 26262 대응 방법이 기술되어 있어, OEM 노하우 부분인 Safety Mechanism이 작성되지 않아 Part5-9.4.3의 FRC가 빠져 있음	SAFE에서는 OEM인 BMW가 Safety Mechanism을 구체적으로 정리해서 Part5-9.4.3의 FRC가 설명되어 있음

JASPAR ISO 26262 가이드라인 Part5
MCU와 ASIC의 고장률 추정 방법

JASPAR ISO 26262 가이드라인에는 ISO 26262 Part5 하드웨어 표준에서 자세히 다루지 않는 MCU와 ASIC에 대해 "Handbook for FS(Microcontroller Application Edition).pdf"와 "Handbook for FS(ASIC Edition).pdf"를 제공한다. 전장부품사가 기능안전성을 준수한 ECU를 개발하기 위해 MCU와 ASIC을 어떻게 고려해야 하는지, 또 Part5-8~9에서 고장률 추정(FIT값 계산)을 어떻게 해야 하는지를 설명한다.

ISO 26262의 Part 5-8.4.3에서는 고장률(Failure rates)을 추정하기 위해 다음과 같이 3가지 방법을 제시하고 있다. 그러나 MCU와 ASIC의 고장률을 계산하기 위해서는 주의가 필요하다.

① 업계에서 널리 인정되고 있는 공개 표준 데이터베이스를 사용하는 방법
- 고장율(Failure rates)과 고장 모드(Failure mode)가 인지된 데이터베이스 10개 종류: IEC TR 62380, IEC 61709, MIL-HDBK-217F notice 2, RAC-HDBK-217Plus, UTE C80-811, NPRD-95, EN 50129 Annex C, EN 62061 Annex D, RAC FMD-97, MIL-HDBK-338
a) JASPAR에서는 MCU에 대해 IEC TR 62380, MIL-HDBK-217F, RAC-HDBK-217Plus, UTEC80-811, SN 29500의 5개의 사용하기를 권장한다. 5개 이외의 내용은 고장 모드만을 다룬 것이거나, 기초 고장률이 없어서 그것만으로는 고장률을 추정할 수 없다. 그러나 표준적인 Data Base를 사용하는 경우, 입력 조건으로 MCU 고유의 설계 조건(트랜지스터 수, 활성화 에네르기 등), 운용 조건(Mission Profile)이 필요하다. 이것들은 MCU 및 MCU의 사용 사례에 의존하는 것이기 때문이기도 해, 일률적으로는 결정할 수 없다. 또 Parameter 값에 대해서도 반드시 최신 차량 MCU의 설계가 반영된 것이 아니기 때문에 실제 FIT 값과 괴리될 수 있다(그림 6).
b) JASPAR에서는 ASIC에 대해 IEC TR 62380 혹은 UTE C80-811(FIDES 2009)를 이용하기를 권장한다. 이 2가지 Data Base를 선택한 이유는 비교적 신규 Data Base가 있어 ASIC 고장률 계산 방법이 규정되어진 반도체의 고장률 계산에 용이하기 때문이다.

② Filed에서 수집된 Data 또는 Test에 기반한 통계치 이용

③ 정성적, 정량적 논거에 기본을 둔 공학적 방법에 의한 전문가의 판단(export Judgment): JASPAR는 기존에 없는 새로운 기능은 MCU와 ASIC에 대해 ②과 ③에 따른 고장률 계산을 추천한다. 이를 위해서는 오랫동안 시장에서 판매된 노하우의 Filed data와 경험이 있는 전문가가 필요한데, 이는 우리나라 차량 반도체의 국산화가 어려운 가장 큰 이유가 되고 있다.

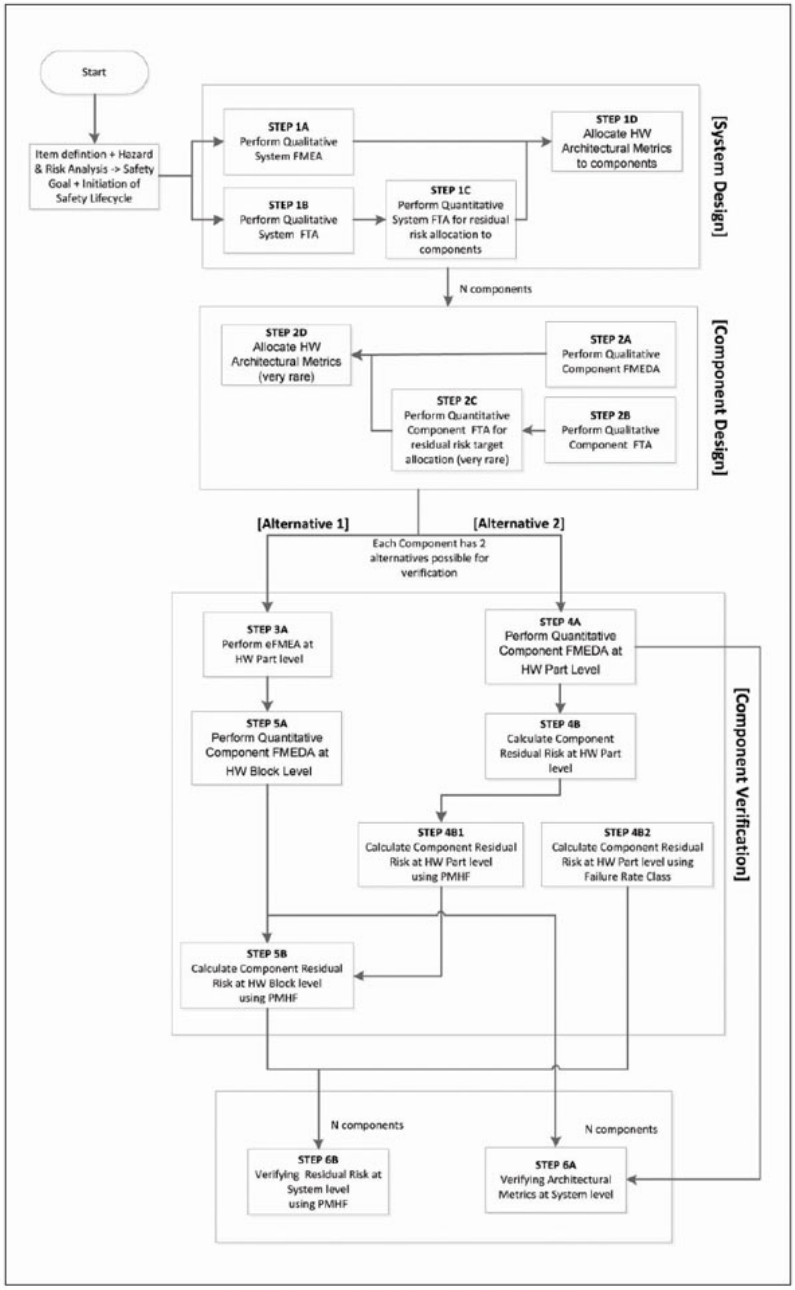


그림 7 | SAFE의 Part5 하드웨어 고장률 추정 절차 및 방법

유럽 SAFE의 ISO 26262 가이드라인

Part5의 고장률 추정 방법

유럽 SAFE의 ISO 26262 가이드라인은 "SAFE_D3.3.1.b.pdf"의 "Deliverable D331b: Methodology and Tool specification for analysis of qualitative and quantitative cut-sets issued from error failure propagation analyses"에 Part5의 하드웨어 고장률 추정 절차 및 방법이 자세히 기술돼 있다(그림 7). 자세한 내용은 "http://www.safe-project.eu/SAFE-Publications/SAFE_ D3.3.2.pdf"를 참고하시기 바란다.

일본과 유럽의 ISO 26262의 Part5 가이드라인 비교

일본과 유럽의 ISO 26262 가이드라인은 서로 보완하는 관계임으로 비교보다는 둘 다 깊게 읽어 봐야 한다. 일본의 ISO 26262 Part5는 표준에 내용이 부족한 MCU와 ASIC에 대한 내용이 자세히 다뤄져 있고, 유럽의 ISO 26262 Part5는 업무 절차와 방법에 대해서 자세히 다루고 있다.

ISO 26262 Part5에서 하드웨어의 EMC 이슈

최근에 해외 자동차의 리콜 사유 중에 EMC 문제로 발생되는 경우가 증가하고 있다. 일본 혼다에서 출시한 하이브리드 자동차 리콜 사건(Fit Hybrid 2014년 10월, Vezel Hybrid 2014년 9월)을 보면은 EMC에 대해서 다음과 같은 2가지 문제가 발생했다.

① 점화 시 통전에 의한 아크방전에 의해 방어 저항의 끝단 부분이 단선됨으로, 점화 코일의 출력이 부족해 엔진이 동작되지 않아 엔진 경고등이 점등되고, 점화 시에 발생하는 소음은 연료 분사 장치가 제대로 통제가 안되어 엔진이 정지될 수 있음.
② 전기 노이즈에 대한 보호가 불충분하기 때문에 차량의 전장부품에 발생하는 노이즈의 영향으로 전원제어 장치가 오동작해, 엔진 제어 ECU에 전원 공급 릴레이가 작동하지 않고 주행 중에 계기판이 꺼지고 엔진이 정지될 수 있음.

또한 미국의 리콜 요청을 하는 기관인 도로교통안전청(NHTSA)은 2014년 10월 7일에 미국 의회에 "Request for Comment on Automotive Electronic Control Systems Safety and Security"로 법제화 요청을 했다.

여기서 3가지 항목이 핵심인데 이는 ISO 26262, Security, EMC 등이다. 자동차에 탑재되는 ECU의 수가 많아지고, 복잡화되면서 EMC 문제 발생이 높아지고 있으며, 특히 자율주행 자동차의 경우는 V2X 등 외부 통신이 급증함으로 EMC에 대한 법적 규제가 높아질 것으로 예상된다.

이번 연재에도 지면의 제약으로 Part5에 대해서 시원하게 설명을 못한 것이 아쉽다. 이러한 아쉬움을 해소할 수 있도록 "ISO 26262 해외 가이드라인 쉽게 이해하기"의 연재를 마치면, "일본 JASPAR의 ISO 26262 가이드라인 쉽게 이해하기"와 "유럽 SAFE의 ISO 26262 가이드라인 쉽게 이해하기"로 나눠 오프라인 세미나를 준비해, 현업에서 일본과 유럽 OEM에 대응하는데 도움이 될 수 있는 자리를 마련하도록 하겠다.

[참고문헌]

1. "ISO 26262에 따른 차량용 ECU 소프트웨어와 SoC 대응 방안", 김원종 박사(ETRI), 채승엽, 한국정보처리학회, 2012년 3월
2. "기능안전성을 준수한 차량용 반도체 개발을 위한 기술적 고려 사항",위재경 교수(숭실대), 채승엽, 대한전자공학회, 2014년 1월

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