Transactions of KSAE, Vol. 28, No. 10, pp.693-700 (October, 2020)

pISSN 1225-6382 / eISSN 2234-0149
DOI http://dx.doi.org/10.7467/KSAE.2020.28.10.693

하드웨어 엘리먼트 평가에 의한 하드웨어 통합의 이해와 사례 연구

박 병 규*·이 승 환

에스피아이디 엔지니어링 사업본부

Understanding and Case Study of Hardware Integration by Evaluation of Hardware Elements

Byoungkyu Park* · Seunghwan Lee

Engineering Division, SPID Co., Ltd., 145 Gasan digital1-ro, Geumcheon-gu, Seoul 08506, Korea
(Received 28 November 2019 / Revised 8 June 2020 / Accepted 25 June 2020)

Abstract : In general, the items to be developed in accordance with the ISO 26262 standard are mostly products that will be integrated by a number of companies, rather than a single product of one company. In this situation, there will be no issues if the product to be integrated is developed in compliance with the ISO 26262 standard and above the target ASIL level. If not, problems may arise with integration. The proposed solution to this is either the evaluation of the hardware elements in ISO 26262-8, clause 13, or the proven in use argument of ISO 26262-8, clause 14. This paper examines the contents and methods with regard to the evaluation of hardware elements in ISO 26262-8, clause 13, which is one of the methods used to determine the eligibility for integration when integrating hardware elements into a system or item to be developed in accordance with the ISO 26262 standard. Also, a method of integrating hardware elements in a variety of cases is proposed through an engine control system. In addition, the process of integrating a QM-level hardware component, stop lamp switch, into an ICU system to be developed in compliance with the ISO 26262 standard was explained in order to promote understanding of the method for the evaluation of hardware elements.

Key words : Functional safety(기능안전), ISO 26262(자동차 기능 안전성 국제 표준), Evaluation of hardware elements(하드웨어 엘리먼트 평가), Hardware integration(하드웨어 통합), Re-qualification(재 인정), Engine control system(엔진 제어 시스템), Stop lamp control system(스탑 램프 제어 시스템)

Nomenclature

ASIC : application specific integrated circuit
ASIL : automotive safety integrity level
BFR : base failure rate
CAN : controller area network
DFA : dependent failure analysis
ECU : engine control unit
EGR : exhaust-gas recirculation
FMEDA : failure modes effects and diagnostics analysis
FSR : functional safety requirement
FTA : fault tree analysis
HAM : hardware architecture metric
HARA : hazard and risk analysis
HSR : hardware safety requirement
IC : integrated circuit
ICU : integrated controller unit
JEDEC : joint electron device engineering council
MCU : micro controller unit
PMHF : probabilistic metric for random hardware failures
QM : quality management
SEooC : safety elements out of context
SG : safety goal

1. 서 론

기능안전 ISO 26262 표준은 2011년 11월 1판을 발간한 이래로 국내외 자동차 산업 품질 향상에 많은 영향을 끼

*Corresponding author, E-mail: pbk@espid.com

치고 있다. 하지만, 여전히 산업 현장에서는 기능안전 ISO 26262 표준에 대한 내용을 잘못 이해하는 경우가 종종 있다. 그리하다 보니, 자동차 메이커들이 하드웨어 엘리먼트를 공급하는 부품사들에게 적절하지 못한 요구사항을 전달하는 경우를 심심치 않게 목격하게 된다. 예컨대, 기능 안전 ISO 26262 표준 발행 이전에 개발되었으며, 현재까지 시장에서 아무런 문제없이 사용되고 있는 QM 수준의 하드웨어 엘리먼트 제품에 대해 할당된 하드웨어 안전 요구사항 없이 그저 "기능 안전 ISO 26262 표준을 준수하여 특정 ASIL 등급에 만족할 것"이라는 요구사항이다.

일반적으로 '기능안전 ISO 26262 표준을 준수하여 개발되었다.' 라는 의미는 차량 수준의 아이템이 정의된 상황에서 HARA 분석 수행의 결과로 ASIL 등급 및 안전 목표가 수립되고, 수립된 안전 목표에 따라 도출된 안전 요구사항들을 충족시켰다는 의미이다. 이러한 안전 요구사항들을 충족시키기 위해서는 ASIL 등급 별 기능 안전 ISO 26262 표준에서 요구된 요구사항 및 프로세스를 준수하여 관련 산출물들을 생성하고, 생성된 산출물들에 대한 검증 및 확인을 수행해야 하며, 이와 더불어 (ASIL B 이상일 경우에 해당) 하드웨어 우발 고장에 대한 정량적 목표 값인 HAM 값과 PMHF 값을 평가하여 목표 값 이내인지를 확인하여야 한다. 그럼으로, 처음부터 기능 안전 ISO 26262 표준을 준수하여 개발되지 못한 하드웨어 엘리먼트의 경우, 위의 활동을 하지 않았기 때문에, "기능 안전 ISO 26262 표준을 준수하여 특정 ASIL 등급을 만족해야 할 것" 이라는 요구사항은 다소 무리가 있다.

이 경우에 대하여 적용할 수 있는 ISO 26262 표준은 ISO 26262-8:2018, 13절의 하드웨어 엘리먼트 평가[1] 또는 14절의 사용 입증 논거[1]이다. 이 중 ISO 26262-8:2018 14절의 사용 입증 논거의 경우 現, 국내 산업 여건상 적게는 수년에서 많게는 수십 년간 축적된 필드 데이터가 없음으로 인해, 이를 적용하기가 어렵다. 그렇기 때문에, 대개의 경우 ISO 26262-8:2018, 13절의 하드웨어 엘리먼트 평가를 적용하게 된다.

하드웨어 엘리먼트 평가는 기능 안전 ISO 26262 준수하지 못한 하드웨어 엘리먼트가 기능 안전 ISO 26262 표준을 준수하여 개발하려는 아이템, 시스템 또는 더 큰 규모를 갖는 하드웨어 엘리먼트의 일부로 사용할 때, 그 하드웨어 엘리먼트가 적합하다는 증거를 제공하기 위한 활동이다.[1] 즉, 다시 말하자면, QM 수준의 하드웨어 엘리먼트를 기능안전 ISO 26262 표준을 준수하여 개발하고자 하는 시스템, 아이템 또는 엘리먼트의 일부로 편입(통합) 하고자 할 때 편입(통합)에 대한 자격 여부를 평가하기 위한 활동으로서, 기능 안전 ISO 26262 표준 준수에 대한 대체 수단이다.[1]

본 논문은 이러한 하드웨어 엘리먼트 평가에 대한 내용을 ISO 26262-8:2018, 13절[1] 중심으로 살펴보고, QM 수준의 하드웨어 엘리먼트가 어떻게 기능 안전 ISO 26262 표준을 준수하여 개발하려는 시스템 또는 아이템에 편입(통합)이 되는지를 두 가지 사례를 통해 보여준다. 또한 하드웨어 엘리먼트 평가에 필요한 절차 및 방안을 기능 안전 ISO 26262 2nd 버전에 맞게 제시한다.

2. 하드웨어 엘리먼트 평가의 일반사항

2.1 하드웨어 엘리먼트 평가 대상

안전 관련으로 식별되고, 기능안전 ISO 26262 표준에 따라 개발되지 않았지만, 현업에서 문제없이 사용하던 하드웨어 엘리먼트들을 대상으로 하며, 재 사용 가능한 하드웨어 모듈 및 하드웨어 COTS(Commercial Off-the-Shelf) 제품들을 포함한다.[1]

2.2 하드웨어 엘리먼트 평가 수행 기반

하드웨어 엘리먼트 평가는 특정 어플리케이션 컨텍스트 내에서 수행된다.[1] 그럼으로, 컨텍스트 내(In Context)인 경우 아이템으로 부터 도출되고 할당된 안전 목표 및 안전 요구사항을 기반으로 평가를 수행하고, 컨텍스트 밖(Out of Context)인 경우에는 SEooC[2] 기반의 가정(Assumption)된 안전 목표 및 안전 요구사항을 기반으로 평가를 수행한다.

2.3 하드웨어 엘리먼트 평가의 달성 목표

하드웨어 엘리먼트 평가는 Systematic fault으로 인한 안전 목표 또는 안전 요구사항 위반 위험이 충분히 낮다는 논거를 제공하는 것을 달성 목표로 한다. 이를 위한 수단으로서 분석 또는 시험을 수행한다.[1]

- 분석을 통한 평가는 필드 데이터, 공정 데이터, 실험 데이터 및 FMEA, FTA, DFA 와 같은 안전 분석 결과를 활용하여 수행할 수 있다.
- 시험을 통한 평가는 기능 시험, 성능 시험, 신뢰성 시험(환경 시험을 포함)으로 수행 가능하다.

이를 통해 하드웨어가 적절한 기능적 성능을 가지고 있어, 기능안전 ISO 26262 표준을 준수하여 개발하려는 제품의 하드웨어 설계에서 요구하는 의도된 기능을 제공하는데 적합하다는 증거를 제공할 수 있다. 그리고 한계 시험, 가속 시험과 같은 시험 또는 분석의 수행은 알려진 고장 모드를 식별하고, 식별된 고장 모드 분포율을 정량화 하는데 유용하다. 뿐만 아니라 하드웨어 엘리먼트에 대한 알려진 사용 제한(Limits)을 확인하거나 새로이 식

별하여 시스템 통합사가 하드웨어 엘리먼트 사용을 보다 적합하게 한다.[1)]

3. 하드웨어 엘리먼트 평가 활동

3.1 하드웨어 엘리먼트의 분류

하드웨어 엘리먼트의 복잡도에 따라 평가를 달리하게 됨으로, ISO26262-8:2018, 13.4.1.1절에서 제시된 바와 같이 하드웨어 엘리먼트의 복잡도에 따라 Class I, Class II, Class III로 분류한다.[1)]

3.1.1 Class I 하드웨어 엘리먼트

1) 분류 기준

① 안전 관점에서 완전히 특성화되며, 시험되고 분석될 수 있는 몇 가지 상태를 최대로 갖는다.[1)]

② 모든 안전 관련 고장 모드가 개발 및 제품 프로세스에 대한 상세 지식 없이도 식별되고 평가될 수 있다.[1)]

③ 엘리먼트는 내부 고장을 제어하거나 검출에 관련이 있는 안전 컨셉을 위한 안전메커니즘이 전혀 없다.(여기에는 엘리먼트 외부특성을 모니터링 하는 안전 메커니즘을 포함하지 않는다.)[1)]

2) 대표적인 사례

① 수동 소자 및 이산 소자와 같은 하드웨어 기본 소자들이 이에 해당한다.[1)]

② 이러한 하드웨어 소자들은 기본 적으로 AEC-Q101 (Stress Test Qualification For Discrete Semiconductors: ex. FET, Diode, IGBT, Transistor,...),[3)] AEC-Q200 (Stress Test Qualification For Passive Components: ex. Capacitor, Inductor, Resistor,..)[4)]을 만족하는 부품이어야 한다.

3.1.2 Class II 하드웨어 엘리먼트

1) 분류 기준

① 예를 들어 몇 가지 작동 모드, 작은 값 범위, 몇 가지 매개 변수 및 구현 세부 사항을 모르더라도 안전 관점에서 분석할 수 있는 엘리먼트[1)]

② 엘리먼트의 구현 및 개발 프로세스 상세에 대한 지식 없이 시험과 분석을 통해 시스템적 결함 평가를 지원하는 유효한 가정이 가용 가능한 문서로 문서화되어 있다. (예. 데이터시트, 사용자 매뉴얼, 어플리케이션 노트)[1)]

③ 엘리먼트는 내부 고장을 제어하거나 검출에 관련이 있는 안전 컨셉을 위한 안전메커니즘이 전혀 없다. (여기에는 엘리먼트 외부특성을 모니터링 하는 안전 메커니즘을 포함하지 않는다.)[1)]

2) 대표적인 사례

① 온도, 압력, 속도 센서 등과 같은 하드웨어 COST 제품, 중간 수준의 복잡도를 갖는 IC류가 이에 해당한다.[1)]

② 중간 수준의 복잡도를 갖는 IC류는 독립형 ADC, Regulator IC, Gate Logic IC, Driver IC, Memory IC, 마이크로 컨트롤러가 내장되어 있지 않는 단순 기능을 갖는 ASIC 등이 있다.

③ IC의 경우 기본 적으로 AEC-Q100(Stress Test Qualification For Integrated Circuit: ex. Regulator IC, Driver IC,..)[5)]를 만족하는 컴포넌트이어야 한다. 단, 어떤 ASIC의 경우, JEDEC[6)](국제 반도체 표준 협의 기구) 표준과 같은 다른 표준을 적용할 수도 있다.

3.1.3 Class III 하드웨어 엘리먼트

1) 분류 기준

① 예를 들어, 다수의 작동 모드, 광범위한 값 범위 또는 수많은 매개 변수를 가지며 알려진 구현 세부 사항 없이는 분석이 불가능한 엘리먼트[1)]

② Systematic fault에 대한 원인은 상세한 구현, 개발 프로세스 및/또는 생산 프로세스에 대한 지식으로만 이해하고 분석할 수 있음. 즉, 달리 말하자면, 설계, 제조 및 생산과 관련된 정보 없이는 Systematic fault에 대한 원인 파악이 어려운 엘리먼트[1)]

③ 내부 고장을 제어 또는 검출하기 위한 안전 컨셉과 관련된 내부 안전 메커니즘을 가진 엘리먼트[1)]

2) 대표적인 사례

① 복잡한 수준을 갖는 IC류 및 전자 제어 유닛이 이에 해당한다.

② 복잡한 구조를 갖는 IC류는 마이크로 컨트롤러가 내장된 ASIC, 마이크로 컨트롤러, 디지털 신호처리 프로세서, FPGA 등이 있다.[1)]

3.2 하드웨어 엘리먼트 평가 수행

3.2.1 Class I 하드웨어 엘리먼트

AEC-Q101,[3)] AEC-Q200[4)] 등과 같은 표준화된 인정이면 충분하다. 별도의 하드웨어 엘리먼트 평가 수행 없이 통합되어 기능안전 ISO 26262 표준에 따라 개발되어야 한다.[1)]

3.2.2 Class II 하드웨어 엘리먼트

ISO26262-8 13.4.3.1 요구사항에 따라 분석 또는 시험을 적절히 선택하여 하드웨어 엘리먼트의 기능적 성능이 안전 컨셉의 목적에 부합되는지를 보장한다. 이를 통해 평가하려는 안전 관련 하드웨어 엘리먼트에 대한 충

분한 강건성을 보장하고 엘리먼트 사용 제약 사항을 확인한다.[1)]

1) 하드웨어 엘리먼트 평가 계획

① 효과적인 평가 수행을 지원하기 위하여 하드웨어 엘리먼트 평가 수행을 계획한다. 하드웨어 엘리먼트 평가의 개별 하부 단계에서 기능안전 활동을 결정하고 계획한다. 하드웨어 엘리먼트 평가 계획서는 안전 계획서에 포함되어 갱신된다.[1)]

② 평가 계획에는 다음 사항에 대하여 기술해야 한다.[1)]

a. 하드웨어 엘리먼트 고유 식별 및 버전
b. 하드웨어 엘리먼트가 사용되도록 의도된 환경에 대한 명세
c. 평가 전략 및 근거(전략은 분석, 필요한 시험 및 단계별 설명을 포함한다.)
d. 전략에 따른 필요 도구 및 장비
e. 평가를 실행할 책임이 있는 담당자
f. 하드웨어 엘리먼트 평가에 대한 합격 및 불합격 기준

2) 하드웨어 엘리먼트 평가 논거

① 하드웨어 엘리먼트의 기능적 성능이 명세에 부합하고 하드웨어 설계에 따라 의도된 용도에 적합하다는 포괄적인 논거가 이용 가능해야 한다.[1)]

② 요구되는 성능은 정의된 정상 환경 조건과 이벤트의 발생으로 인해 가정된 고장 환경에서의 동작을 포함한다.[1)]

③ 포괄적인 논거는 다음 유형의 정보 조합을 기반으로 하여야 한다.[1)]

a. 사용된 분석 방법 및 가정
b. 운영 경험으로 부터 데이터
c. 기존 시험 결과

④ 추정을 포함하여, 모든 가정에 대한 근거가 제공되어야 한다.[1)]

3) 분석에 의한 하드웨어 엘리먼트 평가

① 분석은 안전관련 하드웨어 엘리먼트의 성능이 요구되는 성능을 달성하거나 넘어섰다는 충분한 증빙자료가 존재해야 한다.[1)]

② 충분한 증빙자료는 분석된 분석적 기법이나 가정, 수행 경험으로 부터 수집된 데이터 또는 기존의 시험 결과의 조합을 바탕으로 존재해야 한다.[1)]

③ 사용될 수 있는 분석 방법은 ISO 26262-9:2018, 8. Safety analysis[7)]와 같은 검증 방법을 포함하며, 보간법, 외삽법, 수학적 모델, 손상 분석 또는 이와 유사한 방법, 공정 갭 분석을 통해 체계적인 고장 방지에 대한 충분한 증거를 제시할 수 있어야 한다.[1)]

④ 분석은 안전관련 하드웨어 엘리먼트가 노출되는 모든 환경 조건, 이러한 한계 및 작동과 관련된 기타 추가 스트레스(예, 예상 스위치 사이클, 충전 및 방전, 장시간 전원 차단)을 고려해야 한다.[1)]

⑤ 분석의 결과는 포괄적이며 관련 공학 또는 과학 분야의 자격을 갖춘 사람이 확인할 수 있는 형태로 제공되어야 한다.[1)]

4) 시험에 의한 하드웨어 엘리먼트 평가

① 다음과 같은 내용을 포함하는 시험 계획서가 작성되어야 한다.[1)]

a. 하드웨어 엘리먼트의 기능에 대한 설명
b. 할당된 안전 요구 사항
c. 실시할 시험 순서 및 명세
d. 시험과 안전 요구 사항 간의 추적 성
e. 조립 및 연결에 대한 요구 사항
f. 모의 실험되는 운전 및 환경 조건
g. 시험된 엘리먼트의 개수
h. 합격 및 불합격 기준
i. 측정되어야 하는 환경 파라메터
j. 정확도를 포함하는 시험 장비에 대한 요구 사항

② 하드웨어 엘리먼트의 강건성 검증을 위한 외부 스트레스 시험은 ISO 26262-5:2018, 10.4.6[8)]에 따라 수행되어야 한다.[1)]

③ 시험은 시험 계획에 따라 실시되어야 하고 시험 결과 데이터는 이용될 수 있어야 한다.[1)]

④ ISO 26262:2018에 적합한 엘리먼트로 통합은 ISO 26262-5:2018, 10절 '하드웨어 통합 및 검증[8)]과 ISO 26262-4:2018, 7절 '시스템과 아이템 통합 및 시험[9)]을 준수하여야 한다.[1)]

⑤ 시험에 의한 하드웨어 엘리먼트 평가 보고서에는 작동 범위 및 상태를 포함하며, 하드웨어 엘리먼트에 할당된 안전 요구 사항에 관한 분석 및 시험 수행에 근거한 평가를 합격했는지 또는 불합격했는지에 대한 여부가 명시되어야 한다.[1)]

⑥ 평가 보고서는 결과에 대한 보고와 해석에 대한 메모가 포함된 일련의 문서로 구성될 수 있어야 하며, ISO 26262-8:2018, 9절 '검증(Verification)'에 따라서 검증되어야 한다.[1)]

3.2.3 Class III 하드웨어 엘리먼트

Class III 하드웨어 엘리먼트는 그 복잡성으로 인해 되도록 기능 안전 ISO 26262 표준에 따라 개발된 제품을 사용할 것을 권장한다. 그럼에도 불구하고 Class III 하드웨어 엘리먼트에 대한 평가를 수행할 경우, 아래의 요구사항들을 만족하여야 한다.[1)]

1) ISO26262-8:2018, 13.4.3 'Class II 하드웨어 엘리먼트 평가'에 규정된 요구사항을 만족해야 한다.[1)]
2) Systematic fault으로 인한 안전 목표 또는 안전 요구사항 위배 위험이 충분히 낮다는 논거를 위해 추가적인 수단이 제공되어야 한다. 추가적인 수단은 아래 사항을 포함하지만, 이것 만으로 제한하지는 않는다.[1)]
   ① 안전 관련 기능의 검증 가능성: ISO 26262-8:2018, 13.4.3 'Class II 시험에 의한 안전 관련 기능 검증 수행[1)]
   ② 현장 경험/신뢰할 만한 컴포넌트(Well-trusted component): 현장 경험은 하드웨어 평가를 위해 논거를 지원하는 일부로 사용될 수 있으며, ISO 26262-8:2018 14절 '사용 입증 논거'에 명시된 사용으로 입증된 논거가 이 절을 대신한다.[1)]
   ③ 안전과 관련된 고장 모드를 탐지할 수 있는 능력을 가진 독립적인 다양한 엘리먼트에 의한 통제(Supervision): ISO 26262-9:2018, 7절[7)]에 따른 의존 고장 분석은 독립성을 보여준다.[1)]
   ④ 비견할 만한 무결성 수준을 가진 다른 안전 표준을 준수하는 개발[1)]
   ⑤ (필요한 경우) FMEA/FTA/DFA 안전 분석 결과서 및 FMEDA 결과서

3.3 하드웨어 엘리먼트 평가 검증 (Verification)

1) 하드웨어 엘리먼트 평가 보고서는 ISO 26262-8:2018, 9절 에 따라 검증되어야 한다.[1)]
2) 검증의 목적은 하드웨어 엘리먼트 평가 보고서가 요구사항을 준수하는지 확인하는 것이다. (ISO 26262-8:2018, 9.1)[1)] 이를 통해 평가된 하드웨어 엘리먼트가 기술 안전 개념에 부합하는지를 확인하고, 하드웨어 엘리먼트에 대한 사용 적합성, 인정 결과가 유효한지를 확인한다.
3) 검증 계획에는 다음을 사항을 기술해야 한다. (ISO 26262-8:2018, 9.4.1.1)[1)]
   ① 검증하는 산출물의 내용
   ② 검증에 사용된 방법
   ③ 검증에 사용되는 합격/불합격 기준
   ④ 검증 환경(시험 또는 시뮬레이션 환경)
   ⑤ 안전 이상(Safety anomalies) 발견 시 대응 활동
   ⑥ 회귀 전략
4) 검증 계획을 수행할 때 고려사항은 다음과 같다. (ISO 26262-8:2018, 9.4.1.2)[1)]
   ① 검증 방법의 적절성
   ② 검증할 산출물의 복잡성
   ③ 특정 컴포넌트, 부품에 관련된, 선 경험 지식
   ④ 해당 관련 기술의 성숙도 또는 해당 기술 적용의 리스크
5) 검증 방법으로는 Walk-through, Inspection, Simulation, Safety analyses, Demonstration and testing 등이 있으며, 일반적으로 한 가지 이상의 방법을 적절히 조합하여 수행한다.

4. 하드웨어 엘리먼트 평가와 통합

4.1 사례 1 : 엔진 제어 시스템에서의 하드웨어 엘리먼트 통합

Fig. 1은 기능 안전 ISO 26262 표준을 준수하는 엔진 제어 시스템을 개발 때, 통합 하려는 개별 하드웨어 엘리먼트들에 대한 통합 사례를 보여준다.

먼저 Fig. 1의 내용을 설명하기에 앞서, Fig. 1에서 표기된 안전 관련 대상 여부 및 평가 여부에 대한 표기들은 하드웨어 통합에 대한 이해를 도모하기 위하여 가정하였음을 밝힌다. 즉, 단지 예시일 뿐이다.

통합하려는 개별 하드웨어 엘리먼트들에는 다음과 같이 두 가지 부류로 구분할 수 있다.

1) 시스템 제어기인 엔진 컨트롤 유닛의 외부 인터페이스로 연결되는 완제품 형태의 하드웨어 엘리먼트와
2) 엔진 컨트롤 유닛 내 하드웨어 부품으로서 존재하는 하드웨어 엘리먼트이다.

첫 번째인[1)]의 경우는 서로 다른 업체로 부터 제공되는 완제품 형태의 하드웨어 엘리먼트로서 컴포넌트 수준 이상의 하드웨어 제품들이다. 편의상 'A社~ I社'로 표기하였다.

'A社', 'F社', 'I社'의 경우는 안전과 관련이 없는 비안전측 하드웨어 엘리먼트로 식별되었기 때문에, 기능안전 ISO 26262 표준을 준수하여 개발되지 않아도 통합하는데 문제가 없다. 즉, 이들 제품은 하드웨어 엘리먼트 평가 대상이 아니며, QM 수준으로 개발된 제품이면 충분하다.

나머지 'B社', 'C社', 'D社', 'E社', 'G社', 'H社'의 제품들은 안전 관련으로 식별되어 통합에 대한 자격 여부를 확인하여야 한다.

'D社'와 'E社'는 기능안전 ISO 26262 표준을 준수한 제품은 아니지만, 유사 프로젝트에서 이미 하드웨어 엘리먼트 평가가 수행된 제품들로써 하드웨어 통합에 대한 자격이 충분하다. 그리고 'G社'와 'H社' 역시, 통합될 시스템에 목표 ASIL 수준을 만족하여 개발된 제품들임으

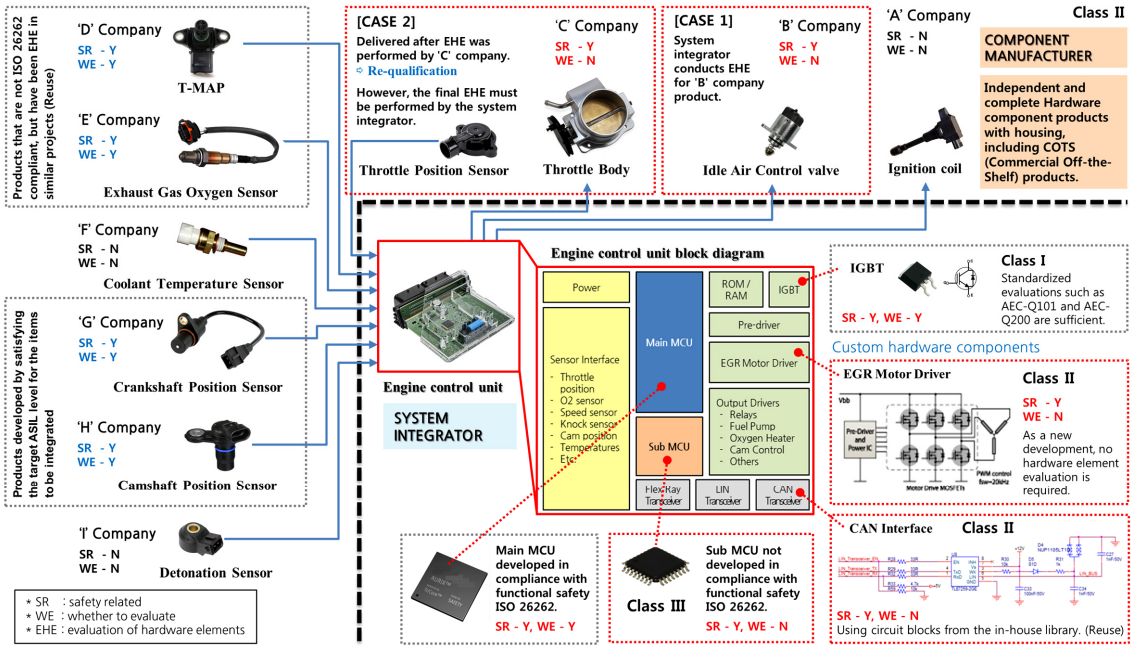

Fig. 1 Hardware integration case and hardware element evaluation in engine control system

로 통합에 대한 자격이 충분하다.

하지만 이와는 달리 'B社', 'C社'는 안전 관련이긴 하나 통합에 대한 자격이 없는 제품들로써 ISO26262-8: 2018, 13절의 하드웨어 엘리먼트 평가[1] 또는 14절의 사용 입증 논거[1]를 통해 통합에 대한 자격을 획득하여야 한다.

기능안전 ISO 26262 표준에서는 하드웨어 엘리먼트 평가 수행의 주체를 특별히 지정하지 않았음으로, 할 수 있는 곳에서 수행하면 된다. 즉, 시스템 통합 업체이든 공급 업체이든 상관없다. 허나 하드웨어 엘리먼트 평가에 대한 최종 평가는 아이템 수준에서 이뤄져야 함으로, 이것은 적어도 시스템 통합 업체 수준에서 이루어져야 한다.[1]

제시된 사례에서 'B社'의 경우는 시스템 통합 업체에서 하드웨어 엘리먼트 평가를 수행하는 경우이고, 'C社'의 경우는 자신들의 제품에 대한 하드웨어 엘리먼트 평가를 수행하는 경우이다. 이 경우를 다른 말로 재 인정(Re-qualification) 이라고도 말한다. 왜냐하면, 이미 QM 수준의 품질 인정을 받은 제품을 다시 평가하는 것이기 때문이다.

두 번째인 2)의 경우는 엔진 컨트롤 유닛 내에서 부품으로 존재하는 하드웨어 엘리먼트들로서, Class I, Class II, Class III 하드웨어 엘리먼트들이 동일 공간 내에 서로 공존하는 경우이다.

Class I의 경우, 부품의 데이터 시트에 표기 되어있는 AEC-Q101,[3] AEC-Q200[4]과 같은 표준화된 인정이면 충분함으로 별도의 하드웨어 엘리먼트 평가는 필요치 않다.

Class II의 경우, 딸 보드(Daughter board)와 같은 별도의 하드웨어 엘리먼트 모듈로서 존재하거나, EGR motor drive circuit, CAN Interface circuit 등과 같은 하드웨어 컴포넌트로 분류 될 수 있는 회로 블록으로 존재하는 경우이다. 하드웨어 컴포넌트 회로 블록 경우, 일반적으로 신규 개발에 해당되어 기능 안전 ISO 26262 표준 개발 프로세스에 처음부터 편입된다. 그럼으로 굳이 별도의 하드웨어 엘리먼트 평가 수행을 요구하지 않는다. 그러나 사내 라이브러리에 있는 회로 블록을 적용하는 재사용 이거나 독립적으로 구성된 딸 보드(Daughter board)를 사용하는 경우는 ISO 26262를 준수한 유사 프로젝트에서 적용되어 그 자격을 입증한 경우를 제외 하고서는 안전 목표 위배 가능성 및 안전 요구사항을 충족시킬 수 있는지에 대한 기능 및 성능 시험 후에 제어기 개발에 포함시켜야 한다. 단, 신뢰성 시험의 경우, 단독으로 수행하기 어렵기 때문에 엔진 컨트롤 유닛 내 다른 하드웨어 부품과 함께 ISO 26262-5:2018, 10절 하드웨어 통합 및 검증[8]에 따라 수행한다.

Class III의 경우, MCU 또는 특수 목적의 복잡한 ASIC이 해당될 수 있다. 이들은 기본적으로 기능 안전 ISO 26262 표준을 준수하여 개발된 제품을 선택할 것을 권한다. 물론 기능 안전 ISO 26262 표준을 준수하지 못한 MCU 제품을 사용할 수 있겠으나, 통합에 대한 자격을 평가하기 위한 노력과 비용을 고려한다면 기능 안전 ISO

26262 표준을 준수한 제품을 선택하는 것이 훨씬 좋다. 만약 부득이하게 기능안전 ISO 26262 표준을 준수하지 못한 Class III 수준의 하드웨어 엘리먼트를 사용할 경우, ISO 26262-8:2018, 13절의 하드웨어 엘리먼트 평가[1]에서는 Class II 수준의 평가뿐만 아니라, 정성적 및/또는 정량적 안전 분석을 포함하는 추가적인 조치를 요구한다.

4.2 사례 2 : QM 수준의 하드웨어 엘리먼트를 ISO 26262를 준수하는 시스템에 통합하는 과정

Fig. 2는 QM 수준의 하드웨어 엘리먼트인 Stop lamp switch를 하드웨어 엘리먼트 평가를 통해 기능 안전 ISO 26262 표준을 준수하는 시스템에 통합되는 과정을 설명하기 위해 준비된 예시이다. 통합되는 과정을 설명하기에 앞서 시스템의 이해가 선행되어야 함으로, Fig. 2에 표현된 아키텍처를 설명한다.

Stop lamp switch는 Inductive 방식의 비 접촉 스위치로서 운전자가 브레이크 페달을 밟으면 상호 반전된 이중 신호를 출력한다. 출력된 신호는 ICU로 입력되고, ICU는 Stop lamp switch로부터 입력된 신호를 판단하여 Stop Lamp를 점등시킨다.

Stop lamp의 점등 트리거로 사용된 Stop lamp switch는 기능안전 표준을 준수하여 개발되지 않았으나, 시장에서 오랫동안 문제없이 쓰던 제품으로서 내부 고장 진단을 위한 안전메커니즘이 없다. 따라서 이 하드웨어 엘리먼트는 ISO 26262-8:2018 13절[1]에 의해 Class II로 분류된다. 그리고 자동차 메이커로부터 주어진 안전 목표와 안전 요구사항은 다음과 같다.

- SG-01: 주행 중 의도하지 않은 Stop lamp 미점등은 방지되어야 한다. (ASIL B 등급)
- FSR: [Brake_SW]에서 [ICU]로 입력되는 하드와이어 신호 [L_BrakeLpSW]는 [SG-01] 위배를 방지하기 위해 [ASIL B]에 맞게 개발되어야 한다.

다음의 1)~7)번은 하드웨어 엘리먼트 평가에 의한 Stop lamp switch의 통합 과정을 설명한다.

1) ICU 개발 업체인 시스템 통합사는 Stop lamp switch에 대한 하드웨어 안전 요구사항을 도출하여 Stop lamp switch 제조사에게 전달한다. 이 하드웨어 안전 요구사항에는 안전 메커니즘을 포함하는 안전 관련 기능 및 비 기능 요소가 고려되어야 한다. 아래는 하드웨어 안전 요구사항 예시이다.
   ① HSR-01: 감지 방식은 비 접촉 이어야 한다.
   ② HSR-02: 상호 반전된 이중 신호를 출력해야 한다.
   ③ HSR-03: ...
2) Stop lamp switch 제조사는 주어진 하드웨어 요구사항을 만족시킨다는 증거를 제공하기 위해서 기능 및 비 기능적 관점에서의 평가를 수행한다. 이를 위해 ISO 26262-8:2018, 13절의 하드웨어 엘리먼트 평가[1]를 통한 분석 또는 시험을 수행한다. 평가에 따른 산출물 목록은 다음과 같다. 산출물 목록 중 하드웨어 엘리먼트 평가 결과서는 ICU 제조사인 시스템 통합사에게 제공되어야 한다.
   ① 하드웨어 엘리먼트 평가 계획서
   ② 하드웨어 엘리먼트 시험 계획서 (평가 계획서에 포함 가능)
   ③ 하드웨어 엘리먼트 평가 결과서
   참고로, 하드웨어 엘리먼트 평가 결과서에는 다음 내용이 포함되어야 한다.
   a. Systematic fault에 대한
      • 평가 기준 및 평가 결과
      • 고장 모드 및 고장 모드 분포율
   b. Random Hardware fault에 대한
      • Stop lamp switch에 대한 BFR 값
3) ICU 개발 업체는 Stop lamp switch의 고장모드를 방어 또는 억제하기 위한 안전 메커니즘을 구현하고, 안전메커니즘의 진단 커버리지 값을 산정한다.
4) ICU 개발 업체는 안전 목표를 위배하려는 Stop lamp switch의 고장 모드를 충분히 방어할 수 있는 설계가 되었는지에 대한 평가를 위해 안전 분석 수행을 수행한다.
5) ICU 개발 업체는 정량적 분석 방안인 FMEDA를 수행하여 통합된 Stop lamp switch가 하드웨어 아키텍처 메트릭 및 하드웨어 우발 고장으로 인한 안전 목

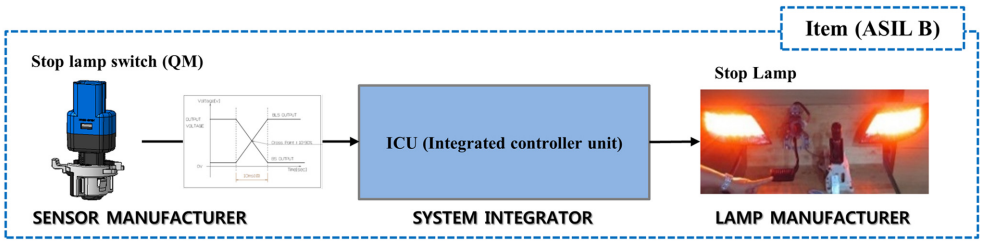

Fig. 2 Stop lamp control system

표 위배 확률에 대하여 얼마만큼 기여하는지를 평가한다. 평가 결과에 따라 설계 개선이 요구될 수 있다.

6) ICU 개발 업체는 ISO 26262-5:2018, 10절[8]에 따라 하드웨어 통합 및 검증을 수행하여 Stop lamp switch에 할당된 하드웨어 안전 요구사항이 ICU 입장에서 충족하였음을 검증한다.
7) ICU 개발 업체로부터 평가된 Stop lamp switch에 대하여 하드웨어 우발 고장에 대한 정량적 목표 값이 충족되고, ISO26262-5:2018 하드웨어 개발 단계에서의 통합 및 시험[8]에서 요구된 안전 요구사항이 충족하였음을 검증되었다면, Stop lamp switch에 부여된 목표 ASIL 등급은 만족 하다고 평가될 수 있다.

4. 결 론

본 논문은 기능안전 ISO 26262-8:2018, 13절 하드웨어 엘리먼트 평가[1]에 대한 내용과 더불어 수행 방안을 살펴보았으며, 엔진 제어 시스템에 대한 개별 하드웨어 엘리먼트의 통합 사례를 제시하여 하드웨어 엘리먼트 통합에 대한 이해를 도모하였다. 뿐만 아니라, QM 수준의 Stop lamp switch를 기능안전 ISO 26262 표준을 준수하는 ICU 시스템에 통합하는 과정을 설명함으로서 자동차 메이커, 시스템 통합사, 부품사들 간의 역할과 책임을 제시하였다.

이를 통해 하드웨어 엘리먼트 평가 및 하드웨어 엘리먼트 통합을 수행할 때 자동차 메이커, 시스템 통합사, 부품사들 간에 올바른 이해와 더불어 합당한 적용을 기대해 본다.

후 기

‘4.2 QM 수준의 하드웨어 엘리먼트를 기능 안전 ISO 26262 표준을 준수하는 시스템에 통합하는 과정’에 대한 설명은 컨텍스트 내(In Context)를 기반으로 하였음으로 하드웨어 엘리먼트 평가를 수행할 업체는 상위 업체인 고객사로부터 명확한 요구사항을 할당 받는 것으로 상정하였다. 그러나 현장에서는 종종 명확한 요구사항을 할당 받을 수 없는 상황이 발생하게 된다. 이러한 상황에 대처할 수 있는 적절한 수단은 ISO 26262-10: 2018에서 제시된 SEooC[2]이다.

향후 과제로서 이러한 SEooC 기반의 가정(Assumption)에 따른 하드웨어 엘리먼트 평가 방안 및 하드웨어 통합에 대한 연구가 필요해 보인다.

References

1) ISO 26262-8:2018, Road Vehicles Functional Safety Part 8: Supporting processes, 2nd Edn., 2018.
2) ISO 26262-10:2018, Road Vehicles Functional Safety Part 10: Guidelines on ISO 26262, 2nd Edn., 2018.
3) AEC-Q101-Rev-D1, Failure Mechanism Based Stress Test Qualification for Discrete Semiconductors in Automotive Applications, AEC(Automotive Electronics Council) September 6, 2013.
4) AEC-Q200-Rev-D, Stress Test Qualification for Passive Electrical Devices, AEC(Automotive Electronics Council), June 1, 2010.
5) AEC-Q100-Rev-H, Failure Mechanism Based Stress Test Qualification for Integrated Circuits, AEC (Automotive Electronics Council), September 11, 2014.
6) JEDEC JEP122H, Failure Mechanisms and Models for Semiconductor Devices, 2016.
7) ISO 26262-9:2018, Road Vehicles Functional Safety Part 9: Automotive Safety Integrity Level (ASIL)-Oriented and Safety-oriented Analyses, 2nd Edn., 2018.
8) ISO 26262-5:2018, Road Vehicles Functional Safety Part 5: Product Development at the Hardware, 2nd Edn., 2018.
9) ISO 26262-4:2018, Road Vehicles Functional Safety Part 4: Product Development at the System Level, 2nd Edn., 2018.