김 중 한 · 이 창 석
경남테크노파크 정보산업진흥본부
jhkim@gntp.or.kr

ISO 26262 기반의 자동차 산업에 대한 SW 신뢰성 이해

기계 중심으로 생산되던 자동차가 IT기술의 발전과 함께 다양한 사용자 편의 서비스를 동반하면서 급격하게 변화하고 있다. 또한 이를 제어하기 위한 자동차 내장형 시스템의 복잡도가 크게 증가되면서 기존과는 다른 SW 결함으로 인한 사고 사례 발생으로 자동차 안전에서 SW 신뢰성에 대한 이슈가 증가되었다. 따라서, 이를 대응하기 위한 국제기구의 자동차 산업 표준화 동향과 국내 표준화 동향 및 대응 전략을 살펴보고, 국제표준으로 사용되고 있는 자동차 기능 안전성 표준인 ISO 26262를 통해 SW 신뢰성을 이해하고자 한다.

1. 서론

과거 기계부품 중심의 단순 이동수단을 목적으로 생산되던 자동차가 IT기술 발전을 기반으로 다변화되고 있다. 현재의 자동차는 주행기능 이외의 기능을 포함하기 위해 다양한 전장 부품과 이를 제어할 목적으로 전자제어장치(ECU: Electronic Control Unit)를 통합한 내장형 시스템을 많이 사용하고 있다. 그 예로 자동차에 전방추돌 경고 장치(FCWS: Forward Collision Warning System), 차선이탈 경고 장치(LDWS: Lane Depart Warning System), 비상 브레이크 장치(EBS: Emergency Brake System), 자율 주행 (Automatic Driving) 등 새로운 기능이 추가되고 있으며, 새로운 개념의 커넥티드-카(Connected Car)의 등장 등 자동차 내장형 시스템의 복잡도 증가와 함께 SW 비중이 크게 향상되었다. 따라서 자동차 내장형 시스템의 SW 비중 증가로 과거와는 다르게 SW 결함으로 인한 자동차 사고 사례가 나타나고 있다. 이는 자동차의 새로운 기능을 제어하기 위해 사용되는 전자제어장치의 개수 및 복잡도가 증가함에 따라 기존 부품 수준의 신뢰성만으로는 자동차의 안전성을 보장 할 수 없음을 의미한다[1].

자동차 내장형 시스템의 SW 신뢰성은 자동차의 안전에 치명적인 영향을 주는 요소가 된다. 스마트폰의 SW 결함이 사람의 안전에 치명적인 영향을 주지는 않지만, 자동차와 같은 주행 장치에서 SW 결함을 일으키게 된다면 사용자의 안전에 치명적인 영향을 미치게 된다. 따라서 자동차의 안전과 SW 신뢰성은 땔 수 없는 관계를 가지고 있다.

본 문에서는 SW 신뢰성이 자동차 산업에서 나타난 배경과 SW 결함에 의한 자동차 안전을 연결하여 설명하고 있다. 2장에서는 SW 신뢰성을 확보하기 위한 국내 · 외 표준화 동향 대해서 우선 알아보고, 3장에서는 국제 표준화 규격인 ISO 26262관점에서의 자동차 SW 신뢰성 확보를 위한 방법, 주요 요구사항, SW 신뢰성과 자동차 안전의 상관관계를 살펴보고, 결론을 맺는다.

2. 자동차 산업의 SW 표준화 동향

자동차 산업의 SW 안전화 표준화는 국제기구인 IEC (International Electrotechnical Commission)에서 2010년 개정한 전기 · 전자 · 프로그램 가능한 전자 시스템의 기능 안전 표준인 IEC 61508을 기반으로 한다. IEC 61508은 기능 안전의 대표적인 국제 표준으로 전자기기, 원자력, 의료기기, 자동차 등으로 구분되는 다양한 기능안전 표준의 대표적인 역할을 한다.

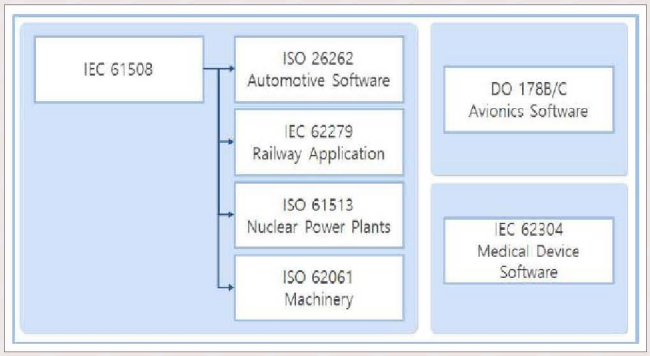

그림 1 국제 표준 현황 관계도

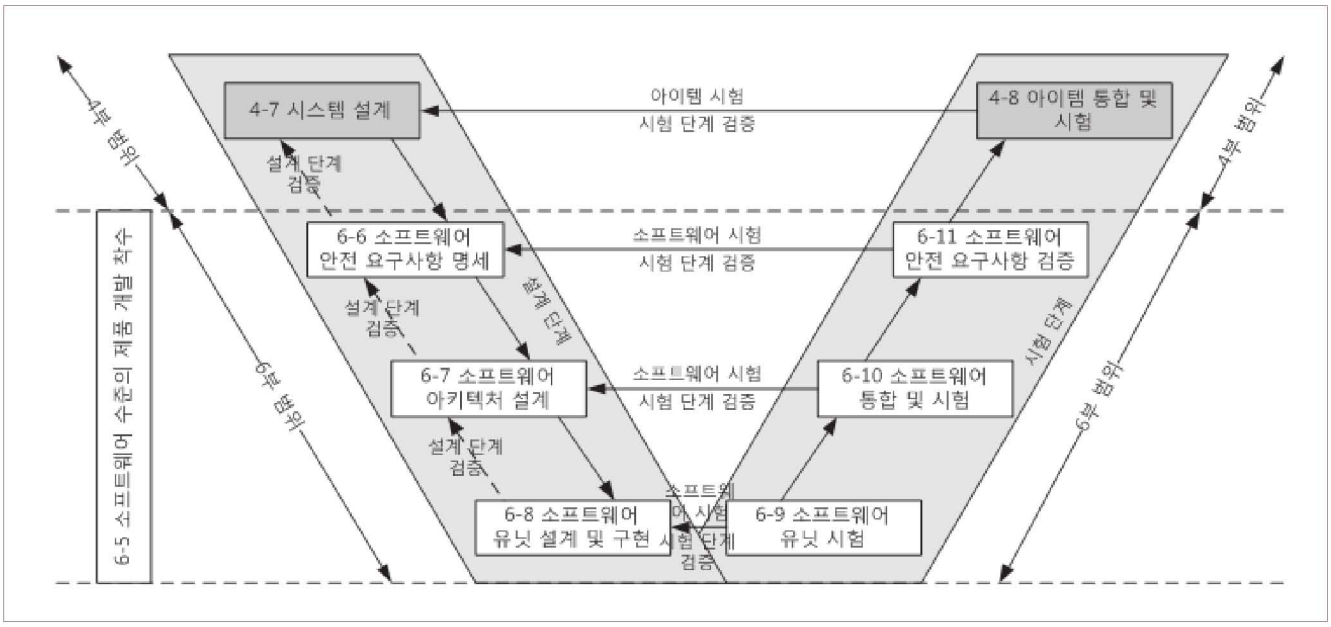

그림 2 ISO 26262 기능안전 V 모델

2.1 국제 표준화 동향

국제 표준은 독일, 미국 등 선진국에서 주도하여 관련 사업에 따라 지속적인 수정 보완이 진행되고 있다. 기술적 우위를 바탕으로 SW 안전에 대해 많은 연구가 진행되고 있으며, IEC 61508을 근간으로 각 산업 군별로 산업 특성을 고려한 소프트웨어 안전 표준을 제정하는 등 관련 산업의 지속적인 발전과 많은 보완을 통해 개선이 진행되고 있다.

과거에는 영국 자동차 산업 소프트웨어 신뢰성 협회(MISRA: Motor Industry Software Reliability Association)에서 2014년에 발표한 자동차 산업용 임베디드 시스템 소프트웨어 개발 가이드라인(MISRA C)을 사용했지만, 현재는 자동차 기능 안전성 국제표준인 ISO 26262가 사용되고 있다. ISO 26262는 국제표준기구(ISO: International Organization for Standardization)에서 제정한 표준화 규격으로 검사, 명세, 설계, 구현, 통합, 운영 등 600개 정도의 주요 요구 사항으로 자동차에서 사용되는 SW에 대한 대부분의 사항을 다룬다.

2.2 국내 표준화 동향 및 정책

국제적으로는 자동차 산업의 표준화에 대한 연구가 활발히 진행되고 있는 반면에 국내에서는 표준화에 대한 및 국제 표준 준수 등 대응이 미비한 상태로 일부 산업 분야에서만 국제 표준에 대한 대응을 강화하고 있는 상태이다[2]. 그 예로 2017년 정부와 관련업계가 자동차 전자제어장치 200 분야의 SW 안전성 확보를 위한 가이드라인을 마련하기 위한 사업을 추진하며, SW와 시스템 안전성 확보를 위한 활동 등 세부 방안과 현장 적용 사례 등을 포함하고 있다[3].

하지만 국내 자동차 SW 신뢰성 확보를 위해서는 SW의 품질(Quality), 보안(Security), 안전(Safety)간의 개념을 명확하게 하고, 자동차 SW 안전과 관련된 국제 표준을 국내에 적용하기 위해 그대로 수용하는 것이 아니라 국내 환경에 반영할 수 있는 연구가 선행될 필요가 있다. 또한 해외 선진국에서 소프트웨어 안전 표준이 준수 될 수 있도록, 직간접적으로 법·규정을 제정하고, 관리감독 기관에서 감독을 수행하는 것처럼 국내에서도 일관된 소프트웨어 안전 관련 정책을 시행하기 위해 소프트웨어 안전에 대한 기본법을 제정하거나, 산업별 특성을 고려하여, 소관 부처 및 전문기관과의 협력을 통해 기존의 관련 규정 및 지침에 소프트웨어 안전 내용을 반영해야 한다[2],[6].

3. ISO 26262에서의 자동차 SW 신뢰성 확보

안전은 위험이 생기거나 사고가 날 염려로부터의 자유를 말한다. 시스템에 대한 안전의 개념을 Storey(1996년)는 1차적 안전(Primary safety), 기능안전(Functional safety), 간접안전(Indirect safety)으로 분리하였다. 1차적 안전은 직접적 사고로부터의 안전으로 정의하고, 기능안전은 리스크 평가 측정결과에 따라서 설계과정을 통해 위험이 제거되는 장비의 안전을 뜻하며, 간접안전은 잘못된 정보 제공으로 일어날 수 있는 원인으로부터의 안전을 정의한다[4],[7]. ISO 26262에서는 리스크를 반영하여 위험요소를 제거하거나 낮추는 기능안전에 대해서 다루고 있다.

3.1 ISO 26262 내용(구성 및 특성)

ISO 26262 파트 1~파트 4 까지는 공통 내용으로 표준 적용에 대한 범위, 참조, 용어, 표 해석방법, 요구사항에 따른 적합성 만족에 대한 설명이 있으나, SW에 대한 범위는 그림 2 V 모델과 같이 파트 6에서 SW 신뢰성 평가에 대한 내용을 담고 있다. 6-5절은 SW레벨 제품개발의 착수, 6-6절은 SW 안전요구사항의 명세, 6-7절은 SW 아키텍처 설계, 6-8절은 SW 유닛 설계 및 구현, 6-9절은 SW 유닛 시험, 6-10절은 SW통합 및 시험, 마지막으로 6-11절은 SW 안전 요구사항의 검증에 대한 요구사항을 명시하고 있다.

3.2 ASIL(Automotive Safety Integrity Level)

ASIL은 ISO 26262 준수를 위한 핵심 사항으로 개발 프로세스가 시작될 때 각 기능들은 일어날 수 있는 위험에 따라 분석된다. 위험도 분석은 노출 등급(E: 분석 대상 고장 모드와 동시에 발생할 경우 위험할 수 있는 작동 상황이 되는 상태로), 심각도 등급(S: 위험할 수 있는 상황에서 위해 범위의 예상치로 정의), 제어 가능성 등급(C: 당사자가 시기적절한 대응을 통해 지정된 위해 또는 피해를 방지할 수 있는 역량)의 3가지의 등급을 조합한다.

Controllability	Exposure	Severity			
		S0	S1	S2	S3
C1	E1	QM	QM	QM	QM
	E2	QM	QM	QM	QM
	E3	QM	QM	QM	A
	E4	QM	QM	A	B
C2	E1	QM	QM	QM	QM
	E2	QM	QM	QM	A
	E3	QM	QM	A	B
	E4	QM	A	B	C
C3	E1	QM	QM	QM	A
	E2	QM	QM	A	B
	E3	QM	A	B	C
	E4	QM	B	C	D

그림 3 ASIL 등급표

ASIL에서는 안전에 확보가 실패할 경우, 운전자와 다른 운전자에게 일어날 수 있는 위험도를 기준으로 나뉜다. 각 안전요구사항은 A, B, C, D 등급으로 나뉘는데, 여기서 D등급이 안전이 중요한 프로세스와 엄격한 테스트 규제를 가지는 등급이다. ISO 26262 는 컴포넌트의 ASIL의 구성요소를 기반으로 하여 최소한의 테스트 요구사항을 상세히 파악하고, 테스트에 반드시 사용되어야 하는 방식을 판단하는 데 사용된다. ASIL에 대한 분석이 완료된 후 시스템에 대한 안전 목표 결정됨으로 안전을 보장하기 위해 필요한 시스템 동작을 결정한다.

3.3 자동차의 안전과 SW 신뢰성

위의 절에서 언급된 ISO 26262의 구성 및 ASIL은 기능안전을 달성하기 위해 SW관점에서의 리스크 요소를 분석하여 위험도에 따른 제제를 통해 SW 신뢰성을 검증함으로써 안전을 확보한다. 비록 모든 사고가 SW 결함으로 인해 발생하는 것은 아니지만, 설계, 구현, 시험 등의 과정을 통해 사전에 결함을 예방하거나 개선 할 수 있다는 측면에서 SW 신뢰성과 자동차 안전은 상호관련이 되어 있다.

4. 결론

본 논문에서는 자동차 산업의 SW 신뢰성을 접근하기 위해 SW 신뢰성이 등장한 배경과 SW 표준화 동향을 살펴보았다. 또한 자동차 기능안전 표준화 규격인 ISO 26262 설명하고, 안전을 기반으로 SW 신뢰성과의 상관관계를 설명하였다. 한국은 세계적인 자동차 수출국의 위상에 비해서는 SW 신뢰성을 확보를 위한 대응이 미비하다.

자동차 산업이 안정적인 발전을 지속하기 위해서는 자동차 안전에 대한 심각성을 이해하고 SW 신뢰성을 확보하기 위한 다양한 활동을 지원하고, 국내 환경에 적합한 표준화 대응 노력과 지속적인 연구가 필요하다.

참/고/문/헌

[1] 김병철, "차량용 기능안전 ISO 26262 표준과 자동차 산업의 대응," 전자공학회지, 40권, 5호, pp. 20-33. 2013.

[2] 4차 산업혁명에서의 SW 안전성 표준화

[3] 김지선, "자동차 SW 안전성 확보, 한국이 이끈다," CIOBIZ, 전자신문, 2017.

[4] "IT융합 산업의 H/W 및 S/W의 안전표준화 기술 동향," 방송통신기술 이슈&전망 19호, 2013.

[5] 박태형, 김태호, 진회승, "소프트웨어 안전성 확보 체계에 관한 연구 - 시험, 평가, 인증을 중심으로," SPRI, 2015.

[6] "소프트웨어 안전(Safety) 산업 동향 조사," SPRI, 2015.

[7] D. J. Smith and K. G. L. Simpson, "Functional safety(A straightforward guide to applying IEC61508 and related standards)," Hutterwirth-Heinemann, 2004.

[8] 고요한, 이경우, "자동차 내장형 시스템을 위한 소프트웨어 신뢰성," 정보처리학회지, 21권, 4호, 2014.

김중한(金中韓) 경남테크노파크 정보산업진흥본부 ICT진흥팀 연구원

1986년 8월 23일생. 2013년 창원대 공과대학 컴퓨터공학과 졸업. 2015년 동 대학원 컴퓨터공학과 졸업(석사).
2016년~현재 (재)경남테크노파크 정보산업진흥본부 ICT진흥팀 연구원.

이창석(李昌錫) 경남테크노파크 정보산업진흥본부 ICT진흥팀장

1971년 2월 10일생. 1990년 창원대 공과대학 전자계산학과 졸업. 2012년 동 대학원 컴퓨터공학과 졸업(공박).
2012년~현재 (재)경남테크노파크 정보산업진흥본부 ICT진흥팀장.