자동차 전자제어 장치용 소프트웨어 기술 및 표준화 동향

Technology Trends in Automotive Electronic Control Units

IT 융합 기술의 미래 전망 특집

한태만 (T.M. Han) 자동차융합플랫폼연구팀 팀장
조진희 (J.H. Cho) 자동차융합플랫폼연구팀 책임연구원

목 차

과거 단순한 이동 수단이 목적이었던 자동차는 더욱 안전하고 편리한 자동차, 서비스 지향 자동차로 거듭나고 있다. 점차 편리와 안전 서비스를 제공하기 위한 전자제어 장치의 장착이 확대되고 전자제어 장치간의 연동을 통한 서비스 개발이 늘고 있으며, 이로 인해 신뢰성 및 안전성 이슈가 최근에 많이 대두되고 있다. 본 고에서는 자동차 응용 서비스의 개발에서 IT 기술들의 집합체라고 할 수 있는 전자장치용 소프트웨어의 표준 플랫폼인 AUTOSAR의 동향과 차량 전자제어 장치의 안전성 보장을 위한 ISO 26262 표준 동향 및 이슈를 살펴본다.

Ⅰ. 서론

21세기 들어 자동차는 단순한 이동수단으로부터 섀시 프레임의 개별 제어, 통합 제어 및 자율주행 제어로 이어져 차량 탑승자의 안전을 제공하며 편리한 새로운 기능들이 추가되고 있다. 자동차 산업은 1990년대 부품 모듈의 개별 제어 수준에서 점차 통합 모듈 제어 방식으로 진화되고 있으며, 외관과 디자인 위주에서 점차 편의성이나 안전 등의 서비스 개발로 추진되고 있다. 미래 지능형 자동차는 편의와 안전 등의 서비스들이 더욱 발달할 것으로 전망되며, 향후 차량의 80% 이상의 혁신은 전기전자 시스템을 기반으로 할 것이다[1]-[4].

산업 발전에 비춰볼 때, 자동차를 생산하는 완성차 업체들은 공통 부품모듈을 다양한 차량 모델에 적용하고자 하고, 부품 개발업체 입장에서는 다양한 완성차 업체에 유사한 부품모듈 납품으로 제조원가를 낮추려고 하는 것은 지극히 자연스러운 현상이다[5].

이러한 일련의 공통 모듈 재사용성이나 차량별 부품 호환성 등의 문제를 해결하고자 전세계 완성차 업체, 부품공급회사 및 IT 기술 업체들이 협력하여 자동차 전장 소프트웨어의 재사용성과 안전성 및 응용 소프트웨어의 하드웨어 의존성 제거 등을 목표로 전장 소프트웨어 플랫폼 AUTOSAR 표준화를 진행하고 있다[6]. AUTOSAR에서는 자동차 도메인을 바디, 섀시, 파워트레인, HMI, 멀티미디어/텔레매틱스 및 안전 분야로 나누고 각 워크 패키지별로 표준화를 단계에 따라 Phase 1, 2, 3로 나누어 진행중에 있다[7].

또한 기존에 파워트레인, 섀시, 바디 등 도메인별 독립적으로 개발되고 시험되던 기능들이 향상된 기능을 위해 융합되면서(예, 자동항법장치, 차체자세 제어시스템 등) 기존의 수동 안전 기능(예, 에어백, 충돌 등) 중심의 개별적이고 단편적 기능 안전 보장 접근방식(형식승인)에서 차량의 개발 초기단계부터 폐기에 이르는 전 생명주기에 걸친 체계적이고 포괄적인 기능 안전 보장이 요구된다. 이에 기존 안전산업 분야(철도, 항공, 원자력, 화학공정 등)에 적용하던 기능 안전성(functional safety) 개념을 자동차 분야에 도입하여 ISO 26262 표준을 개발하고 있으며 2011년 중반에 정식 제정될 예정이지만, 이미 선진업체에서는 이를 적용하고 있다[8].

다음 두 장을 통해서 자동차 전장 소프트웨어의 표준 플랫폼인 AUTOSAR와 차량 기능 안전성 표준 ISO 26262에 대한 동향과 주요 이슈를 살펴본다.

Ⅱ. 자동차 전장 소프트웨어의 고도화

1. 자동차 전자제어 장치의 변화

자동차의 모습이 점차 지능형 자동차로 발전하게 됨에 따라 차량내 전자제어장치의 적용 비중이 높아졌다. 차량 안전 분야에서는 자동차의 사고방지를 위해 안전벨트나 에어백 장착 및 범퍼 등의 완충장치 장착 등 수동적인 안전을 제공하는 수준에서 점차 제동의 미끄럼 방지를 위한 ABS, 가속 미끄럼 방지용 TCS, 그리고 조향 안전을 제공하는 ESP/ESC 등의 능동적 안전 장치들이 현재 차량에 장착이 되어 탑승자의 안전성을 높여주고 있다.

또한 운전자의 편의를 높여줄 수 있는 다양한 바디 제어 제품들이 차량에 장착되고 있으며, 차내 멀티미디어 장치들을 연결하여 탑승자의 멀티미디어 정보들을 통합·제어할 수 있는 기술들, 차량 후방 안전 확보를 위한 후방 카메라 시스템, 앞 차와의 거리에 따라 속도를 자율 조절할 수 있는 SCC 및 자율주차를 제공할 수 있는 APS 등을 장착한 차량들이 출시되어 판매되고 있다.

미래 지능형 자동차를 위하여 연구되고 있는 분야로는 바디 통합제어를 위한 BCM, 종축 및 횡축의 특성을 종합할 수 있는 섀시 통합 제어 모듈, 기존 IT 분야에서 개발되었던 ad-hoc 통신기술 및 센터 통신기술 등의 다양한 통신기술들을 차량과 접목시키는 차간 통신 기술(VMC)들이 개발되고 있으며, 차선이탈을 경보하는 LKS, 사각지대 장애물 인식

시스템, 야간 장애물을 초음파 등을 통해 시각화시켜 알려주는 기술, 차량 내·외부 정보를 통합 제어할 수 있는 통합 제어 게이트웨이 시스템, 텔레매틱스 시스템과 연계된 차량 전자장치 제어 기술 등의 다양한 기술들이 연구되고 있다. 이러한 기술들에는 센서와 제어기 및 구동기로 구분되고, 제어기에는 ECU라는 핵심 제어장치가 있으며, ECU에 앞서 얘기한 서비스들이 설계되고 실제 ECU에 기록되어 지능형자동차 서비스가 실현된다.

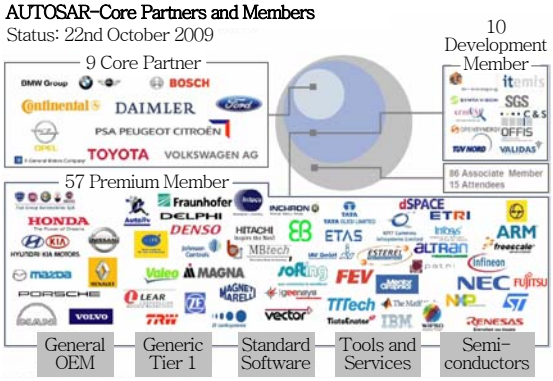
2. AUTOSAR 표준 배경 및 동향

해외 선진 자동차 업계에서는 자동차 임베디드 시스템의 기술 혁신을 위해 표준 플랫폼 및 개발 방법론의 구축을 위해 노력하고 있다. 대표적인 사례가 AUTOSAR 표준화이다. AUTOSAR는 하드웨어와 소프트웨어의 분리를 통하여 소프트웨어의 재사용성 및 확장성의 향상을 도모한다. 또한 복잡한 소프트웨어를 모델 기반으로 개발할 수 있는 도구 기반의 개발 방법론과 도구간의 인터페이스를 표준화된 XML 문서로 상호 연동할 수 있도록 하여, 신규 서비스들을 빠르고 신뢰성 있게 개발할 수 있는 방법론과 소프트웨어 플랫폼을 표준화 시켰다.

AUTOSAR는 2003년 6월 자동차의 전기/전자 아키텍처에 대한 공개 표준 제정을 목표로 유럽, 일본, 미국 등의 자동차 제조업체들과 부품 제조업체들이 공동으로 참여하는 협력체로 탄생되었다. AUTOSAR 협력체는 3단계의 회원 자격 구조로 이루어져 있으며, 2009년 10월 현재 (그림 1)에서와 같이, 9개의 코어 파트너, 57개의 프리미엄 멤버, 86개의 관련 멤버 및 10개의 개발 멤버로 구성되어 있다. 국내는 현대기아자동차, 한국전자통신연구원이 프리미엄 멤버로, 대성전기, 대우정밀, 만도, 대구경북과학기술연구원이 관련 멤버로 활동중이다.

<표 1>에서는 AUTOSAR 표준화 활동 이력을 보여준다. 2003년 AUTOSAR가 결성된 이후 지속적으로 표준을 제정·갱신하고 있다.

앞서 언급했던 바와 같이 표준화는 자동차 도메인



<자료>: Up-to-date status see: http://www.autosar.org

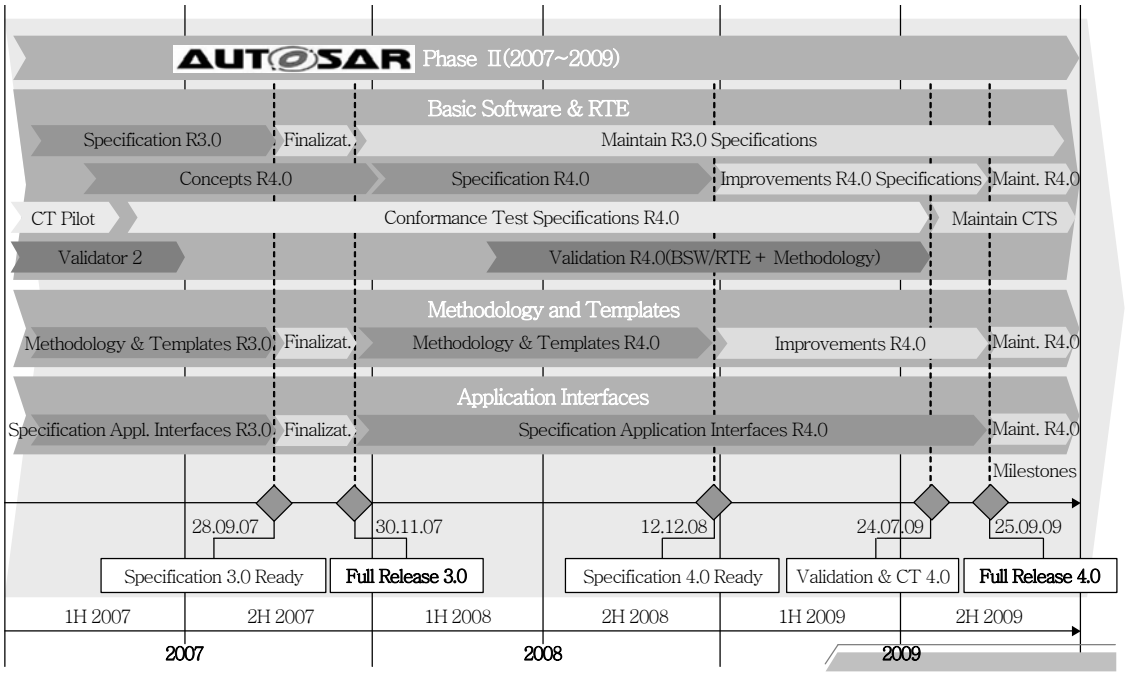
(그림 1) AUTOSAR 주요 회원사

〈표 1〉 AUTOSAR 표준 활동

연도	활동
2002. 8.	BMW, Bosch, Continental, DaimlerChrysler and Volkswagen의 Initial Discussion
2003. 7.	BMW Group, DaimlerChrysler, Bosch, Volkswagen, Continental, Siemens VDO 초기 코어 멤버 결성
2003. 11.	Ford Motor 추가 코어 멤버 참여
2003. 12.	Toyota, Peugeot 코어 멤버 참여
2004. 10.	AUTOSAR 개념 정립
2004. 11.	GM 코어 멤버 참여
2005. 6.	Release 1.0 배포(23개 소프트웨어 컴포넌트)
2006. 5.	Release 2.0 배포(42개 컴포넌트 완성)
2007. 12.	Release 3.0 배포(2008-02 Rev-002 완성)
2009 .12.	Release 4.0 배포

별로 단계적으로 진행중에 있다. (그림 2)에서와 같이 AUTOSAR는 Phase 2(2007~2009년) 규격화 작업을 완료하고 규격 4.0을 공개했다. 또한 Phase 3(2010~2012년)을 시작했는데 멀티코어 프로세서의 지원, 기능 안전성을 위한 기능 추가가 주요 이슈이다.

현재 자동차 완성차 업체에서는 규격이 적용된 자동차를 적용하고 있으며, 선두주자인 BMW가 2006년에 시험 적용한 이후, (그림 3)에서 보듯이 AUTOSAR의 9개 핵심 멤버들은 자사의 차량에 2012년까지 단계적으로 AUTOSAR 플랫폼을 적용하기로 공표했다.



(그림 2) AUTOSAR Phase 2 일정

Core Partner	2008년	2009년	2010년	2011년	2012년
BMW Group	· re 10 AUTOSAR BSW modules as part of Std Core in vehicles, tool/serial support in place			· Powertrain-, Chassis-, Safety-, Body-ECUs use AUTOSAR architecture	
BOSCH	· Body Computer with subset of AUTOSAR specs incorporated · Instrument Cluster with subset of AUTOSAR specs incorporated	· ACC ECU using AUTOSAR architecture · Powertrain EDC/ME(D) 17 ECUs using AUTOSAR architecture · Domain Control Unit using AUTOSAR BSW	· Chassis ECU using AUTOSAR architecture · Body Computer using AUTOSAR architecture		
Continental		· Body ECU using AUTOSAR architecture · Powertrain ECUs using AUTOSAR architecture	· Powertrain-, Chassis- ECU using AUTOSAR architecture		
DAIMLER		· First usage of AUTO-SAR modules in vehicles	· First AUTOSAR compatible ECUs in vehicles	· Introduction of AUTOSAR architecture and methodo-dology in vehicles	
Ford		· 1-2 AUTOSAR conformant ECUs first use of conformant tools/methodology	· Continuous roll-out of ECUs into vehicle architecture increased use of conformant tools/methodology		
GM OPEL			· First usage of AUTOSAR modules	· First usage of AUTOSAR architecture ECU	
PSA PEUGEOT CITROEN		· Powertrain ECU using AUTOSAR architecture	· Body ECU using AUTOSAR architecture		
TOYOTA			· First usage of AUTOSAR modules		· AUTOSAR architecture ECU
VOLKSWAGEN		· First AUTOSAR modules in series production		· First complete ECUs in series production	

(그림 3) 핵심멤버의 AUTOSAR 적용 계획

3. AUTOSAR 소프트웨어 개발

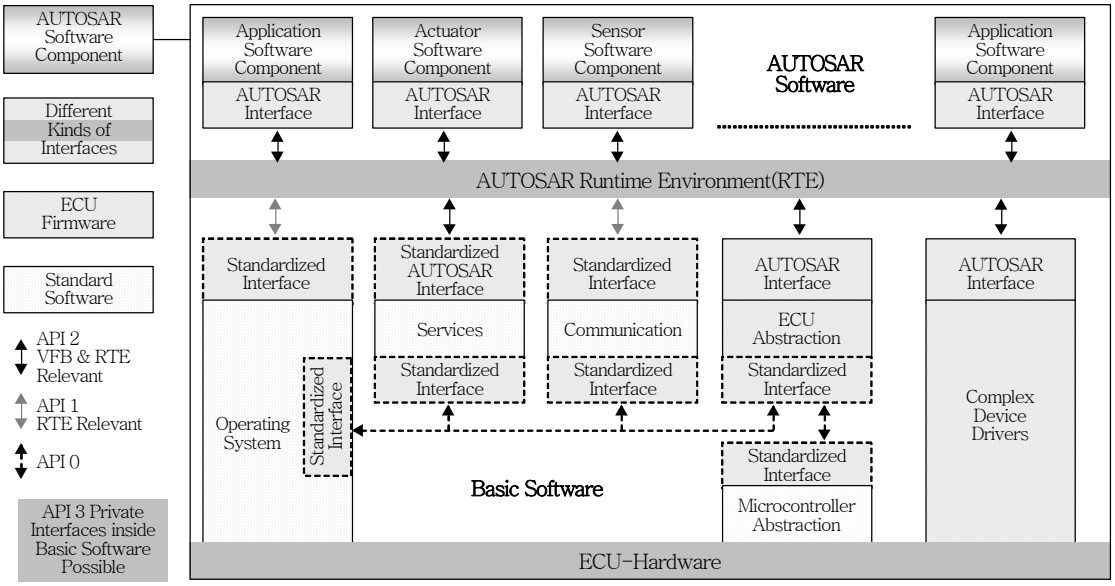
AUTOSAR 구조는 크게 AUTOSAR SW-C, RTE, BSW의 3계층으로 나누어지며, 기본 설계는 RTE 개념을 도입하여 응용 SW-C와 하드웨어 관련 소프트웨어인 BSW를 분리함으로써, 하드웨어에 독립적인 응용 서비스를 개발할 수 있도록 하는 것이다. (그림 4)에서는 AUTOSAR 소프트웨어 아키텍처를 보여주고 있다.

각 AUTOSAR SW-C는 응용 소프트웨어인 기능의 일부를 구현하고, ECU에 매핑되는 기본 단위이며, 포트와 인터페이스를 통해 상호 송수신할 신호와 데이터를 정의하고 정의된 규격에 따라 태스크들의 동작으로 메시지들을 교환한다. Sensor/Actuator SW-C는 AUTOSAR SW-C의 한 종류로써 ECU의 센서 및 액추에이터의 구현을 위한 SW-C이다. RTE는 각 SW-C 사이 및 SW-C와 BSW 사이의 정보 교환을 위한 중추적인 역할을 하며 소프트웨어와 하드웨어를 분리시키는 핵심역할을 한다. RTE는 하부 많은 서비스 계층의 컴포넌트들을 추상화하여 API들을 제공하여 향후에 ECU 보드가 바뀌더라도 상위 제작된 소프트웨어 컴포넌트 수정 변경 없이 사용할 수 있도록 가상 버스 개념을 접목하고 있다.

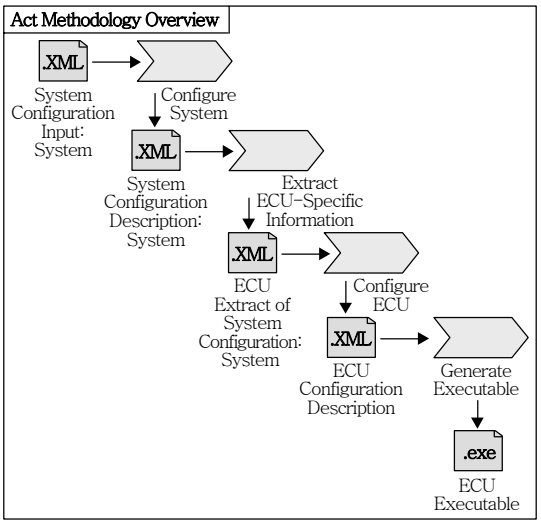
BSW의 표준 계층으로는 Service Layer, EAL, MCAL 그리고 CDD로 구성된다[9].

서비스 계층은 OS, 네트워크, 메모리, 검증, ECU 상태관리 등의 서비스 기능을 수행한다. EAL은 ECU 내부의 장치들과의 인터페이스를 제공하며, ECU에 독립적인 상위계층의 설계를 제공한다. MCAL은 상위 계층에서 마이크로 컨트롤러의 레지스터를 직접 조작하는 것을 피하게 해주며, 디지털 입출력, 아날로그 디지털 변환, 파형변환, 직·병렬 변환 등으로 구성된다.

이러한 계층화에 반하여 기존 동작중인 안정화된 장치들을 AUTOSAR 플랫폼과 호환성을 가지고 동작될 수 있도록 CDD라는 개념으로 수용하고 있다. 특히 MOST 등의 경우, 해외 MOST 칩 벤더나 소프트웨어 개발 툴킷들을 제공하는 업체들을 중심으로 안정된 장치 드라이버를 사용할 수 있도록 CDD 형태로 접목시킬 수 있으며, 또한 이더넷과 같은 장치들도 필요시 CDD를 제작하여 AUTOSAR 인터페이스를 제공한다면 RTE 하부에 동작시킬 수 있다. AUTOSAR에서는 CDD를 제공하므로 기존에 안정



(그림 4) AUTOSAR 소프트웨어 아키텍처



(그림 5) AUTOSAR 표준 개발방법론

적으로 동작되던 장치들을 최소한의 수정으로 지속적으로 서비스할 수 있도록 backward compatibility를 제공하려고 노력하고 있다.

(그림 5)에서는 AUTOSAR WP 1에서 표준화되고 있는 도구별 상호운용성을 제공할 수 있는 전장 응용서비스의 개발 방법론을 보여주고 있다. AUTOSAR 소프트웨어 개발은 시스템 설정단계와 ECU 설정단계로 나누어진다.

시스템 설정 단계에서는 SW-C의 데이터 타입, 인터페이스와 연결 상태 등을 기술하는 SW-C 명세서(component description), 각 ECU의 하드웨어 구성을 기술하는 ECU 자원명세서(resource description), 그리고 버스 시그널, 토폴로지 등 시스템 제약명세서(constraint description)를 작성한다. 각 SW-C 내부에는 응용 소프트웨어 구현을 위한 태스크 동작정의 및 트리거 조건을 정의한다. 다음은 SW-C를 각 ECU에 매핑하고 네트워크 설계를 하여 시스템 설계명세서(system configuration description)를 기술한다. 작성된 파일은 XML 형식의 템플릿을 사용하며, XML을 사용함으로써 데이터의 공유 및 전달을 표준화 할 수 있다.

다음 단계는 시스템 설계명세서로부터 각 ECU 정보를 추출하여 ECU 설정을 하며, 태스크 정의 및 할당, RTE 생성, BSW 설정을 통해 ECU 설계 명세서(configuration description)를 기술한다. 응용 소프트웨어와 함께 RTE, OS, Communication 등의 AUTOSAR 소프트웨어 모듈 코드를 생성하고, 컴파일, 링크를 거쳐 실행 파일을 만들어 ECU 응용서비스를 구현한다. 구현된 동작 가능한 결과물은 설정된 ECU에 올려 시험할 수 있다.

Ⅲ. 자동차 전장 소프트웨어의 안전성

1. AUTOSAR의 안전성 확보 노력

자동차의 안전성 확보라는 관점에서 보면 AUTOSAR는 단순한 전장 소프트웨어 플랫폼 표준화 이상의 의미이다. 즉, 전장 하드웨어와 소프트웨어 분리를 통하여 소프트웨어 재사용성과 확장성을 높이고, 복잡해지는 전장 소프트웨어를 보다 빠르고 신뢰성 있게 개발하려는 AUTOSAR 소프트웨어 플랫폼은 품질 관점에서 소프트웨어 내적/외적 품질 특성인 효율성, 유지보수성, 이식성 및 신뢰성 등을 제고하기 위한 노력으로 이해할 수 있다.

또한, AUTOSAR는 규격 적합성 시험(conformance testing) 표준화를 통해 향후 AUTOSAR 플랫폼 기반으로 시장에 출시되는 전장 소프트웨어의 규격 일치 여부를 판정하는 기준이 되는 시험 명세, 시험 데이터 생성 및 시험 프로세스를 명시함으로써 보다 구체적이고 실질적인 전장 소프트웨어의 신뢰성과 안전성 확보를 위한 기능 시험 가이드라인을 제시한다.

전기전자 제어장치와 관련하여 안전성이란, 재물(property)이나 환경에 대한 피해(damage)의 결과뿐만 아니라 직접적으로 사람의 건강에 대한 피해나 물리적 상해에 대해 수용할 수 없는 수준의 위험이 없는 것이라고 정의하며, 사람에 대한 안전성을 확보하기 위해 시스템은 반드시 안전 보장 기능(functional safety)을 마련해야 한다고 명시하고 있다[10].

AUTOSAR에서 정의하는 6가지 자동차 도메인 기능—파워트레인, 바디와 편의, 섀시, HMI, MM/T

및 안전(safety)—중 안전이란, 사람의 안전을 보장하기 위한 시스템적 안전 기능을 의미하며, 그 안전의 수준은 IEC 61508 표준에 근거하여 AUTOSAR 소프트웨어 플랫폼 기반 소프트웨어 컴포넌트 개발 프로세스의 SIL-3 호환성을 명시하고 있다[7],[10],[11].

SIL이란, 기능적 안전성 보장 수준이며 안전성이 보장되어야 하는 시스템의 신뢰성 수준에 대한 통계적 기준이다. 즉, 안전성 보장이 요구되는 시스템을 운영할 때 발생한 재앙의 발생 건수가 일정 기준시간 이상 되어야 함을 의미한다. AUTOSAR 기본 요구사항으로써 요구되는 안전성 수준인 SIL-3은 AUTOSAR 기본 요구사항에서처럼 발생가능성이 "$10^{-7} < LoC < 10^{-6}$" 범위 안에 있어야 한다(AUTOSAR 기본 요구사항에서는 실패 비율이 시간 당 10^{-8} 이하여야 한다고 명시하고 있다). IEC 61508은 그러한 SIL에 대한 4가지 등급별 기준과 각 기준별 달성해야 할 요구사항을 기술하고 있다[10].

IEC 61508 안전 표준은 자동차를 비롯한 항공, 원자력발전 시스템, 기차, 의료 등 안전성 결정적 시스템에서 기본적으로 준용하는 가장 포괄적인 표준이며, 각 도메인에서는 IEC 61508 표준을 근간으로 각 도메인에 최적화된 형태의 특화된 안전성 평가 모델을 제시하고 적용하고 있다. 항공분야 시스템 안전성 평가 표준으로서 미국의 RTCA와 유럽연합의 EUROCAE가 개발하고 각각 FAA와 EASA가 채택한 DO-178B/ED-12B나 원자력 발전소 설비 제어 시스템 안전성에 관한 국제 표준인 IEC 61504-Nucreal power plants-Instrumentation and control systems Important to Safety는 IEC 61508을 프레임워크로 각 도메인에 특화된 안전성 평가 모델의 대표적인 사례이다.

AUTOSAR에서는 자동차용 전장 소프트웨어 개발 언어로서 C, C++ 및 Java를 명시하고 있지만 대부분의 전장 소프트웨어는 안전성 검증이 상대적으로 수월한 C 언어로 개발하는 것이 일반적이다. C 코드의 신뢰성 보장 방안으로 가장 널리 알려진 기준은 MISRA-C 언어 사용 규칙이고, 자동차 전장 제어용 소프트웨어의 안전성 보장을 위한 기본 규칙이다. 하지만 ECU의 기능이 복잡해지고 분산 처리가 요구되면서 소프트웨어 기능 또한 비례적으로 복잡해졌고, 수십만 라인에 이르는 전장 소프트웨어를 단순히 코드 수준에서 검증하는 것만으로 자동차의 안전성과 신뢰성을 보장하기 어려워졌다.

이러한 문제에 대응하기 위해 AUTOSAR에서는 각 기법들에 대한 FMEA 적용 가능성을 요구하고 있다[11]. FMEA는 원래 하드웨어 분야에서 기계적인 운영 실패 모드와 그 효과에 대한 정적 분석 기법(IEC 60812)으로 널리 활용되었으나, 최근 소프트웨어 분야의 모델 수준에서 FMEA 기법을 도입하여 적용하고 체계화하려는 움직임을 보이고 있다.

2. 차량 기능 안전성 표준 ISO 26262

차량 안전에 관하여서는 전통적으로 차량의 기능별로 관련 규정과 지침 및 형식승인을 통해 차량 안전 보장을 요구해 왔으나, 최근 차량이 기계장치 중심에서 전기전자장치 중심으로 발전하고 차량 기능 간 통합 및 교류가 증가하면서 선진국을 중심으로 기존의 기계장치 중심의 형식승인을 전자장치 중심으로 강화한 규정 및 지침의 필요성이 대두되고 있다[12]. 이에 글로벌 자동차 기업들을 중심으로 기존의 안전관련 시스템의 전기전자장치에 대한 기능안전 표준인 IEC 61508을 자동차 분야에 적용해 본 결과 도출된 문제점을 해소하기 위해 자동차 분야의 특성을 반영한 새로운 표준의 필요성을 인식하여 ISO 26262를 개발중이며, 늦어도 2011년이면 공포될 예정이다[13]. BMW, Daimler, GM, Bosch 등의 글로벌 자동차 메이커 및 공급업체들은 ISO 26262를 자체 개발프로젝트에 이미 도입하고 있으며, 포괄적인 적용을 위해 노력하고 있다[14],[15].

ISO 26262는 차량의 전기전자장치의 기능 안전성에 관한 요건을 정의한 표준으로서 ISO 산하 기술위원회 TC22의 SC3(Road Vehicle Subcommittee), WG16(Electrical and Electronic Equipment)에서 작업중인 문서이다. 2004년 말부터 표준 제정

움직임이 시작되어 2009년 7월 현재 DIS로서 ISO 회원국에 배포된 상태이고 2011년 중순 전후하여 최종안이 제공될 것으로 예상하고 있다.

전기전자 장치 안전에 관한 포괄적 규격으로는 IEC 61508이 있는데 2000년대 초반 FAKRA를 중심으로 독일 자동차 업계에서 IEC 61508을 자동차 분야에 적용한 결과 여러 가지 문제점이 제기되었다. 일반 전기전자 장치 안전에 관한 포괄적 규격인 IEC 61508은 제어 시스템과 안전 메커니즘(예, 1, 2, 3차 보호 시스템 등)을 별개로 고려하는데 반해 차량은 기본적으로 이동성을 전제로 하는 시스템으로서 제어 시스템과 안전 메커니즘은 통합되어야 한다. IEC 61508은 또한 자동차 개발 생명주기와도 맞지 않으며, 자동차 산업의 특성상 완성차 업체(OEM)와 부품공급업체 간의 전문화, 분업화된 생산 방식에 적합하지 않았다. 특히, IEC 61508은 최종 제품(자동차)을 사용하는 소비자 관점의 '안전'이 아니라, 안전이 보장된 제품을 제공해야 하는 공급자 중심의 제품 '안전'에 초점을 맞추고 있는 점이 가장 큰 문제점으로 지적되었다.

이러한 문제점을 해결하기 위해 ISO 26262에서는 IEC 61508의 핵심 개념인 안전성보전등급(SIL)과 하드웨어 중심의 안전생명주기(safety lifecycle)를 개선하여 ASIL과 시스템 중심의 안전생명주기를 도입하고 있다.

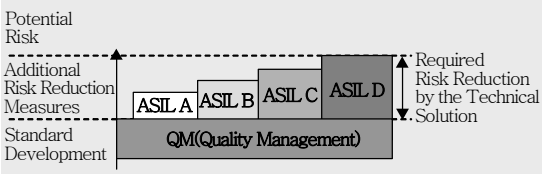
3. ASIL 개념

ISO 26262의 차량안전성보전등급(ASIL)이란 IEC 61508의 안전성보전등급(SIL) 개념을 자동차 제품 특성에 맞게 개선한 차량의 안전성보전등급을 말한다. IEC 61508의 안전성보전등급(최저 SIL 0부터 최고 SIL 4)을 결정하는 2가지 핵심 요소는 재난을 야기하는 위험 발생확률(probability of occurrence)과 발생 가능한 재난(hazard) 결과로써 안전에 미칠 영향의 심각도(severity of its effects)이다[10]. 이에 반해, ISO 26262에서는 안전성보전등급을 재난 상황에 노출가능성(probability of exposure), 위험의 잠재적 심각도(potential severity) 그리고 통제가능성(controllability)에 따라 차량 안전성보전등급을 결정한다. 이것은 자동차 제품의 특성을 반영한 것으로 ASIL은 최저 등급인 ASIL A부터 최고 등급인 ASIL D까지 총 4개 등급이다[13].

<표 2>는 ISO DIS 26262에 제시된 재난의 심각성(S: 최저 S0, 최고 S3), 노출확률(E: 최저 E0, 최고 E4) 및 통제가능성(C: 최저 C0, 최고 C3) 요소에 따라 ASIL을 결정하는 데 참조하는 ASIL 결정기준표를 보여준다(표에는 ASIL 판정 제외 요건이 되는 S0, E0, C0는 표시되어 있지 않다).

〈표 2〉 ASIL 결정

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D



(그림 6) ASILs 비교

ASIL이 높다는 것은 그 개발 대상의 오류로 인해 사고가 날 경우 상대적으로 피해가 클 수 있으며, 그 위험을 줄이기 위해 높은 수준의 안전메커니즘이 필요하므로 안전에 대한 요구사항이 강력해지는 것이다. (그림 6)은 각 ASIL별 상대적인 비교를 보여주고 있다.

SIL과 ASIL을 결정하는 구성요소를 통해 짐작할 수 있듯이, IEC 61508에서 제시하는 SIL 결정 방식이 일반적인 재난분석과 위험심사를 통한 포괄적인

기준이라면, ISO 26262의 ASIL은 자동차의 특성을 반영한 것이다. 즉, 재난분석을 통해 식별된 위험이 안전에 미치는 심각성이 높다 하더라도 실제 그 위험에 노출될 확률이 낮거나, 설사 심각한 위험에 대한 노출 확률이 높다 하더라도 자동차 운전자나 보행자 등 자동차 안전과 관련된 이해관계자가 충분히 그 위험 상황을 통제할 수 있다면 굳이 안전 메커니즘을 고려하지 않아도 되지만, 그러려면 부품공급사 혹은 제조사는 그에 상응하는 충분히 문서화된 증거자료를 제조사 혹은 권한을 지닌 기관에 제출할 것을 명시하고 있다[13],[15].

품목(item) 개발 프로젝트의 수행자 관점에서는 ASIL이 높아짐에 따라 개발과정에서 수행하는 활동의 엄격한 정도가 달라진다. 가령, 소프트웨어 개발 단계에서 요구사항을 검증하기 위한 기법을 적용함에 있어서 개발 대상 품목이 ASIL A등급이라면 워크스루(walkthrough)를 통한 비공식적 검증방법을 강력히 권고(highly recommended)하며 인스펙션은 단순 권고(recommended)하는 수준이다. 반면에 그보다 높은 ASIL C등급인 경우는 준 정형(semi-formal) 검증 방법을 강력히 권고하며, ASIL D등급의 경우 정형검증 방법을 권고하면서 ASIL A등급에서 권고하던 워크스루는 오히려 사용하지 말아야 할 검증방법으로 정의하고 있다. <표 3>은 ISO 26262에서 ASIL 등급별 적용 기법에 대한 예이다.

〈표 3〉 요구사항 검증 기법

Methods		ASIL			
		A	B	C	D
1a	Informal verification by walkthrough	++	+	o	o
1b	Informal verification by inspection	+	++	++	++
1c	Semi-formal verification[a]	+	+	++	++
1d	Formal verification	o	+	+	+

* [a] : Method 1c can be supported by executable models.

++ : highly recommended, + : recommended, o : no recommendation

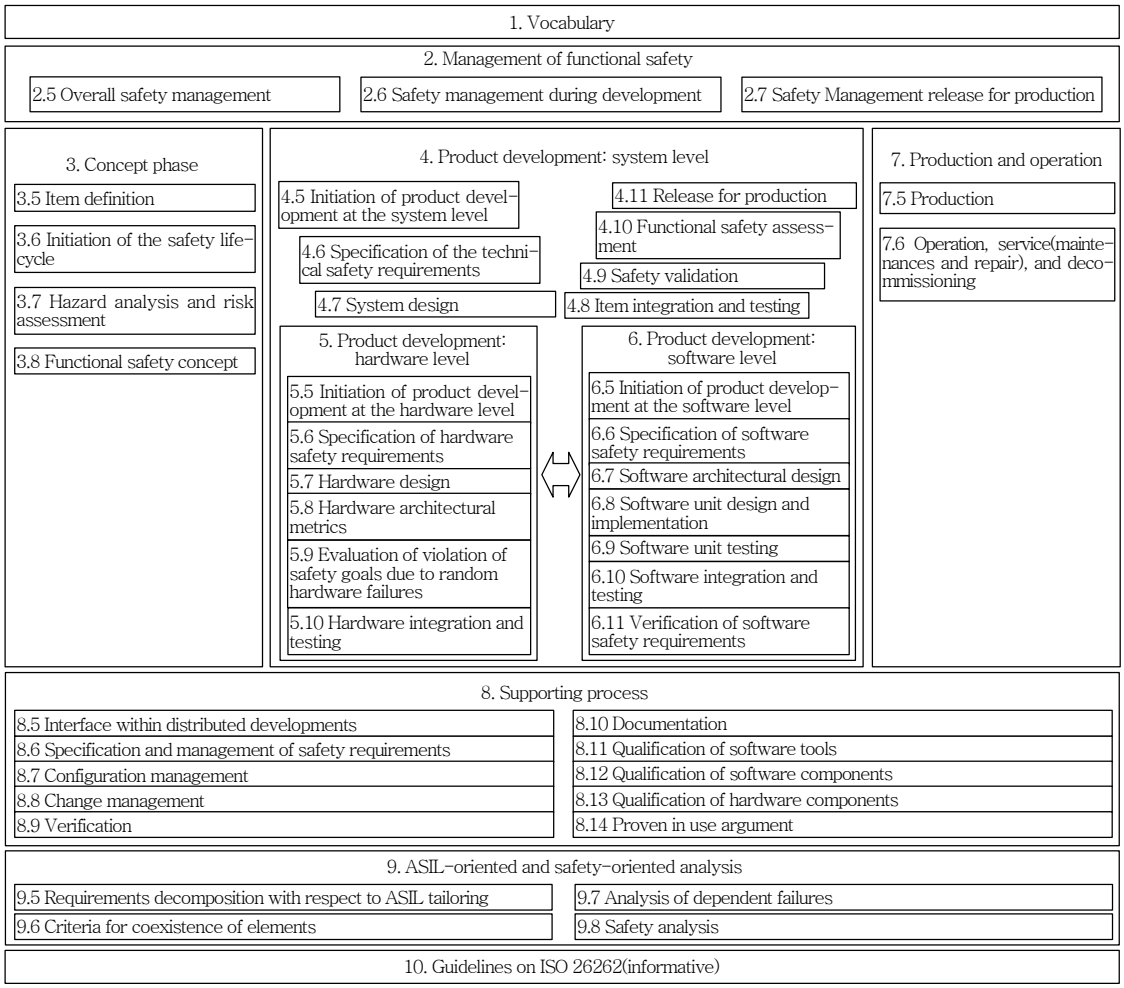
4. ISO 26262 구성

IEC 61508에서 참조하는 생명주기 모형은 'V' 주기모형을 기반으로 하며, 하드웨어의 안전 요구사항이 결정된 후 소프트웨어(전장 소프트웨어)의 안전 요구사항을 추출하여 접근하는 전형적인 하드웨어 중심의 시스템 개발 생명주기 특성을 띤다[10].

이에 반해 ISO 26262는 기본적으로 IEC 61508과 동일한 'V' 주기모형을 따르고는 있지만 하드웨어와 소프트웨어 구성요소를 모두 고려한 시스템 수준에서 독립적인 제품개발 단계((그림 7)의 4. Product development: system level)를 통해 시스템을 설계한 후((그림 7)의 4.8 System design) 하드웨어와 소프트웨어 개발이 독립적으로 병행될 수 있는 구조로 구성되어 있다.

ISO 26262의 파트별 구성을 간략히 기술하면 다음과 같다.

1) Vocabulary – 관련 용어를 정의함
2) Management of functional safety – 기능 안전성에 관련된 개발활동을 계획, 조정, 추적하는 요건을 정의하며 안전문화와 같이 조직차원에서 갖추어야 할 것에서부터 품목개발, 생산 이후에 걸친 전반적인 안전성 관리 요구사항을 정의함
3) Concept phase – 개발 품목 정의를 기반으로 해저드 분석 및 위험심사를 통해 ASIL을 판정하며, 안전 목표와 안전 메커니즘을 정의함
4) Product development: system level – 시스템 수준에서의 개발은 기본적으로 V모델을 따르며 기술적 요구사항과 시스템 디자인, 그리고 테스트 프로세스가 통합의 왼쪽부분에 오고, 검증, 확인과 심사가 오른쪽 부분에 위치함. 전기전자 시스템 외의 타 기술로 구현된 안전 메커니즘을 확인(validation), 외부 수단으로 구현된 안전 개념의 효과 확인, 사람의 통제성 및 작동작업에 대한 전제 등을 검증하는 것을 포함함
5) Product development: hardware level – 시스템 설계명세를 기반으로 하여 아이템의 하드웨어 개발이 이루어지는데, V모델의 개념에 따른 하드웨어의 개발, 통합, 검증 등에 대한 요구사항을 정의함



(그림 7) ISO 26262 구조

6) Product development: Software level – 소프트웨어 수준의 개발에 대해 V모델의 개념에 따라 개발, 통합, 검증 등에 대한 요구사항을 정의함

7) Production and operation – 품목 생산을 위한 계획, 샘플 생산, 양산, 서비스 등에 관한 요구사항을 정의함

8) Supporting process – 안전 요구사항의 관리와 명세 방법, 형상관리, 변경관리, 검증, 문서화, 지원도구의 자격검증(qualification), 재사용 소프트웨어의 자격검증, 하드웨어의 자격검증, 실제 사용을 통해서 입증된 안전성(proven in use argument) 등에 대한 요구사항을 정의함

9) ASIL-oriented and safety-oriented analysis – 안전 요구사항 ASIL을 분해하는 방법, 안전 관련 구성요소 사이의 공존의 조건인 상호간섭의 정도, 위험분석 방법 등을 기술함

10) Guidelines on ISO 26262 – 주요 개념, 안전 케이스, ASIL 분해 등 ISO 26262의 이해에 도움이 되는 정보를 기술함

ISO 26262 적합성을 인정받기 위해서는 위에서 정의하는 각 요구사항에 따라 개발이 되어야 하며, 반드시 문서화된 증거자료로 입증해야 한다. 다음 절에서는 ISO 26262를 개발에 적용할 경우 개발 조직 차원에서 미치는 영향을 기술한다.

5. ISO 26262 제정이 국내 업계에 미칠 영향

ISO 26262를 도입한다는 것은 자동차 산업계에 큰 도전이라고 한다[14]. 왜냐하면 ISO 26262는 차량의 개발 초기에서부터 생산, 폐기에 이르는 전체 생명주기에 걸친 방대한 안전 관련 요구사항을 제시하는데, 개발 조직의 내부 상황을 고려하여 이 요구사항들을 효율적으로 구현해야 하며, 이것은 성숙된(matured) 개발프로세스 역량이 요구되기 때문이다. 비근한 예로, 유럽의 안전성에 관한 선행 연구 개발(EASIS) 보고서에 의하면 CMMI 레벨 4 정도의 조직이 ASIL C 정도를 만족할 수 있다고 한다.

가. 개발 체계(프로세스)에 미칠 영향

기존에는 품목 개발 생명주기와 안전 생명주기를 별개로 하는 이중구조로 구성되어 각 담당자별로 나뉘어 수행되었다. 또한 차량 개발시 다양한 개발 품목이 병행 개발되며, 개발 품목별로 CMMI, Automotive SPICE, 기타 품질 시스템을 충족해야 하는데 여기에 추가로 ISO 26262를 도입하면 개발 체계 및 품질 체계는 그 복잡도가 훨씬 증가하게 된다. 또한 자동차 생산에 있어서 글로벌 기업들과의 협력은 필수인 상황에서 이해당사자 모두가 받아들일 수 있는 표준이 요구된다. 따라서 이러한 프로세스 복잡도 증가를 해소하고 표준 프로세스를 제공하기 위해 ISO 26262 기능 안전성 표준, 기존 개발 프로세스, Automotive SPICE, CMMI, 기타 사내 표준 등을 모두 포괄하는 참조 프로세스의 개발이 필요하다[15].

나. 새로운 지원도구의 필요성

ISO 26262의 요구사항을 충족하기 위해서는 차량의 개발초기부터 체계적인 재난 분석, 개발 품목에 적절한 ASIL 결정, 전체 생명주기에 걸쳐서 다양한 기법이 적용되는 안전 관리 활동이 요구되고 이 활동의 성공적인 수행을 문서화된 증거로서 입증할 수 있어야 한다. 이것은 개발자에게 많은 추가 부담이 될 것이며 이를 경감시킬 수 있는 다음과 같은 새로운 개념의 지원도구가 필요하다.

다. ASIL 분석도구

개발 품목의 안전성 보장을 위해서는 차량에 대한 체계적인 재난분석을 통해 합당한 ASIL을 결정하여야 한다. 재난분석을 위해서는 기존의 HAZOP, FMEA, FTA, Markov chain 등의 분석기법을 적용할 수 있는데, 현재는 각 기법들과 관련된 단편적인 도구들과 함께 DOORS나 MS 엑셀 등을 이용하여 관련정보를 관리하고 있다. 그러나 이러한 단편적인 도구들을 연계하여 사용하는 것으로는 개발초기의 상위수준의 재난분석에서부터 개발 후반부의 상세한 수준에서 서로 다른 분석기법을 통한 재난분석을 반복적으로 수행하고 그에 따라 ASIL을 결정해서 관련 정보를 체계적으로 관리하기가 어렵다. 그리고 ISO 26262의 적합성을 입증하기 위해 재난분석 활동의 성공적인 수행 결과를 쉽게 입증하기 위해서는 새로운 ASIL 분석을 지원하는 도구가 필요하다.

라. ASIL와 통합된 프로젝트 관리 지원도구

앞서 언급한 바와 같이 ASIL은 개발 품목의 개발 활동의 엄격함 정도에 영향을 미친다. 개발 품목은 내부에 여러 개의 서브시스템 혹은 구성요소로 구성될 수 있으며, 이것들은 다시 여러 구성요소로 분해되고 개발되는 것이 일반적이다. 이때 분해된 각 구성요소들은 ISO 26262의 ASIL 분해 원칙에 따라 초기의 ASIL이 여러 개의 하위 ASIL로 분해될 수 있고, 이것은 하나의 품목 아래 다양한 ASIL이 존재할 수 있다. 이 ASIL의 등급에 따라 개발과정에서 적용해야 하는 안전 메커니즘, 검증기법, 시험기법이 달라지게 된다. 이것은 전통적으로 미리 정해진 사내 표준 프로세스 및 방법론에 의거 일괄적으로 단순히 적용하던 방식을 더 이상 적용하기 어렵다는 것을 의미한다.

이러한 복잡한 프로세스(개발 활동)를 관리하는

방법을 단순하게 나눈다면 두 가지 방법이 있을 수 있다. 첫번째는 높은 ASIL 등급에 적용 가능한 고수준의 기법을 일괄적으로 적용하도록 단순화시키는 방법이고, 두번째는 효율적인 도구를 활용하는 것이다. 전자의 경우의 예는 ASIL A등급에 워크스루를 사용하고 ASIL B등급에는 인스펙션을 하도록 되어 있는 것을, 사내에서 ASIL A, B 모두에 인스펙션을 적용하도록 단순화 하는 방법이다. 그러나 이러한 방법은 일부의 개발 활동에는 적용할 수 있으나 개발 품목이 많은 수의 구성요소로 이루어질 때에는 복잡도가 크게 달라지지 않을 수 있다.

결국 이렇게 개발 품목의 많은 구성요소들과 다양한 ASIL로 인한 실행 프로세스의 복잡도를 관리해 줄 수 있는 프로세스 지원도구가 필요하다.

Ⅳ. 결론

차량 탑승자의 편의와 안전을 제공하기 위한 다각도의 노력으로 국내에서 생산되는 차량들의 편의성과 안전성은 해외 유수 자동차 업체와 비교하여도 뒤지지 않는 수준에 이르렀다. 또한 정부 주도로 이루어지는 미래 자동차의 로드맵과 연구 추진으로 미래 무인자동차와 자동화는 점차 현실로 다가오는 듯하다. 편의/안전 서비스의 증가는 전자장치의 모듈화를 가속화시키고 전자 장치별 상호 연동을 통한 네트워킹이 증가시켰다. 복잡성의 증가와 소프트웨어 적용 빈도가 높아지면서 모델기반 개발 방법 등 소프트웨어의 공학적 접근법이 조심스럽게 추진되고 있으며, 이러한 조류와 더불어 사용빈도가 높아지는 자동차용 운영체제와 AUTOSAR 소프트웨어 플랫폼의 표준화는 가시적인 성과를 거두고 있다.

미래는 AUTOSAR와 같은 통일된 소프트웨어 플랫폼을 적용하는 부품 모듈들의 조립에 의한 자동차 모델 개발이 가능하게 되며, 재사용성의 증가로 신차 모델의 개발기간 단축과 안전성이 보장되는 부품모델의 제공으로 서비스 신뢰성 향상이 기대된다. 또한 신뢰성을 제공하는 소프트웨어 플랫폼은 자유로운 부가서비스 개발로 이어져 항상 변화하는 지능형 자동차 모습을 앞당길 것으로 예측된다.

국내 자동차 산업에서는 기능 안전성 개념이 아직은 생소하다. 소수 업체에서 기능 안전성 표준 ISO 26262에 관심을 가지고 있으나, 아직은 많은 개발자와 전문가들이 도메인별로 단편적인 안전 기능 개발에만 관심을 두고 있고, 기능 테스트를 열심히 하는 것으로 안전성이 보장되는 것으로 여긴다. 그러나 자동차 분야에서 이미 30~40%의 개발은 소프트웨어로 그 기능이 개발되고 소프트웨어는 그 엄청난 복잡성으로 인해 충분히 테스트한다는 것은 불가능하다는 것이 알려져 있다. 미국 NASA의 경우 소스코드 1라인 당 850달러의 비용을 들여 개발한 소프트웨어의 KLOC(1,000 lines of codes) 당 오류는 0.004개로 알려져 있다. 최근의 자료에 따르면 고성능 자동차의 경우 1억 라인의 소프트웨어가 들어갈 예정이라고 하는데 NASA 만큼 개발 비용을 들인다 하더라도 확률적으로 400개의 오류가 들어 있다는 결론이 나온다[4],[16].

향후 자동차에 있어서 혁신의 대부분(80% 이상)은 전기전자 시스템을 통해 이루어지는데 그 중심에는 최근에 부각되고 있는 “X-by-wire”라는 개념이 있다[4]. 이것은 차량내 기존의 기계적인 장치를 네트워크 통신으로 연결된 구동기, 휴먼인터페이스 및 전기전자 제어 시스템으로 대체함으로써 무게를 줄이고 기능을 고도화 한다는 개념이다. 이들 전기전자 시스템에서 제어 소프트웨어의 사용은 날로 증가할 것이다. 따라서 이러한 상황을 고려했을 때 “제품이 서비스되는 시점에서 최신의 과학과 기술을 적용해야 한다”라고 하는 유럽의 85/374/EEC 규정은 미래 자동차 산업을 준비하는 업체에 있어 현실적인 대안이라고 할 수 있다. 이 규정에는 최신의 기술을 적용하였고 그것을 증빙할 수 있을 경우, 비록 결함으로 인해 사고가 났더라도 면책한다는 내용이 포함되어 있으며 만약 최신 기술을 적용하지 않았을 경우, “태만”으로 여긴다는 것이다. 이 규정은 제조업체나 소비자 모두에게 win-win이다. 소비자 입장에서는 보다 안전한 자동차를 구입하기 위해 자동차 업체들로 하여금 최신의 기술을 적용하도록 강제할

수 있으며, 자동차 업체는 최신의 기술을 적용함으로써 피할 수 없는 오류로 인해 발생할 수 있는 책임을 면할 수 있기 때문이다. 현재까지는 IEC 61508이 공식적인 최신 기술이며, 향후 2011년 중순 이후 자동차 분야에서는 ISO 26262가 정식 배포되면서 이것을 대체할 것이다.

다만 국내현실에서 우려되는 것은 기존의 차량 배기가스의 규제가 후발 업체에게는 비관세(non-tariff) 무역 장벽화 되었다는 것을 고려하면 차량의 안전성이란 명목으로 ISO 26262가 향후 더 높은 비관세 무역 장벽이 될 수 있다는 우려가 일본에서도 제기되었다[17]. 그러한 전망은 MISRA의 Guidelines of Safety Analysis 자료에서도 곧 현실화 될 수 있음을 알 수 있는데, ISO 26262가 향후 전통적인 형식승인을 대체하는 새로운 차량 안전 관리 규정으로 공식 대두될 것으로 전망하고 있다[12].

● 용 어 해 설 ●

ESP/ESC: 고속 주행중 발생하는 긴급상황에서 조향의 안전을 제공할 수 있도록 각 회전 바퀴별로 따로 제어가 가능하도록 하는 기술

약어 정리

ABS	Anti-lock Brake System
APS	Auto Parking System
AUTOSAR	AUTomotive Open System Architecture
BCM	Body Control Module
BSW	Basic Software
CDD	Complex Device Driver
EAL	ECU Abstraction Layer
EASA	European Aviation Safety Agency
ECU	Electronic Control Unit
ESC	Electronic Stability Control
ESP	Electronic Stability Program
EUROCAE	European Organization for Civil Aviation Equipment
FAA	Federal Advisory Committee
FMEA	Failure Mode & Effects Analysis
HMI	Human-Machine Interface
LKS	Lane Keeping System
LoC	Likelihood of Occurrence per operational hour
MCAL	Microcontroller Abstraction Layer
MISRA	Motor Industry Software Reliability Association
MM/T	Multi-Media & Telematics
MOST	Media Oriented System Transport
RTCA	Radio Technical Commission for Aeronautics
RTE	Run-Time Environment
SCC	Smart Cruise Control
SIL	Safety Integrity Level
SW-C	Software Component
TCS	Traction Control System
VMC	Vehicle Multihop Communication
WP	Work Package

참 고 문 헌

[1] 유우석, 박지용, 홍성수, “분산형 실시간 차량제어 시스템을 위한 RTOS, 미들웨어 및 결함 허용성 요소기술 연구,” 2006.

[2] 장승주, “자동차용 임베디드 SW 기술동향,” 주간기술동향, 2006. 12.

[3] 장승주, 권오훈, “자동차용 임베디드 운영체제 기술 동향,” 주간기술동향, 2007. 8.

[4] Robert N. Charette, “This Car Runs on Code,” http://www.spectrum.ieee.org/greentech/advanced-cars/this-car-runs-on-code, Feb. 2009.

[5] 최상원, 선원웅, “자동차 전장기술의 동향과 전망,” 한국자동차산업연구소 연구보고서, 2005-19, 2005. 12.

[6] Frost & Sullivan, “Strategic Analysis of the European Market for Software in Passenger Cars,” M03B-26, 2007.

[7] AUTOSAR Technical Overview 3.0, AUTOSAR, Dec. 2007.

[8] 나지하, 권기선, “비 IT 분야 임베디드 SW 기술 융합 동향,” 2007. 6.

[9] AUTOSAR Layered Software Architecture, AUTOSAR, Dec. 2007.

[10] IEC 61508: Functional safety of E/E/PE safety-related systems.

[11] AUTOSAR Main Requirements 3.0, AUTOSAR, Dec. 2007.

[12] MISRA Guidelines for Safety analysis of vehicle based programmable systems, Nov. 2007.
[13] ISO DIS 26262 Road Vehicles - Functional safety, July 2009.
[14] Axel Dold and Daimler AG, "Implementation of Requirements from ISO 26262 in the Development of E/E Components and Systems," http://www.eacxpo.com/forum_2008/pdf/day_1/axeldold.pdf, Automotive Electronics and Electrical Systems Forum 2008, May 6, 2008, Stuttgart, Germany.
[15] SAE World Congress & Exhibition, Reinhold Hamann - Robert Bosch GmbH, "Application of ISO 26262 in Distributed Development ISO 26262 in Reality," Apr. 2009.
[16] Balachander Swaminathan, "Agile Overview," http://agileindia.org/agilecoimbatore07/presentations/AgileOverview.pdf
[17] Daichi Mizuguchi, "A Report of the Current Situation on Software Certification in Japan," http://www.jaist.ac.jp/joint-workshop/verite/06JaistAist_mizuguchi.pdf