스마트 카 개발을 위한 기능안전 적용 방안

강현구 (현대오트론), 금득규 (유엔진솔루션즈)

목차

1. 서 론

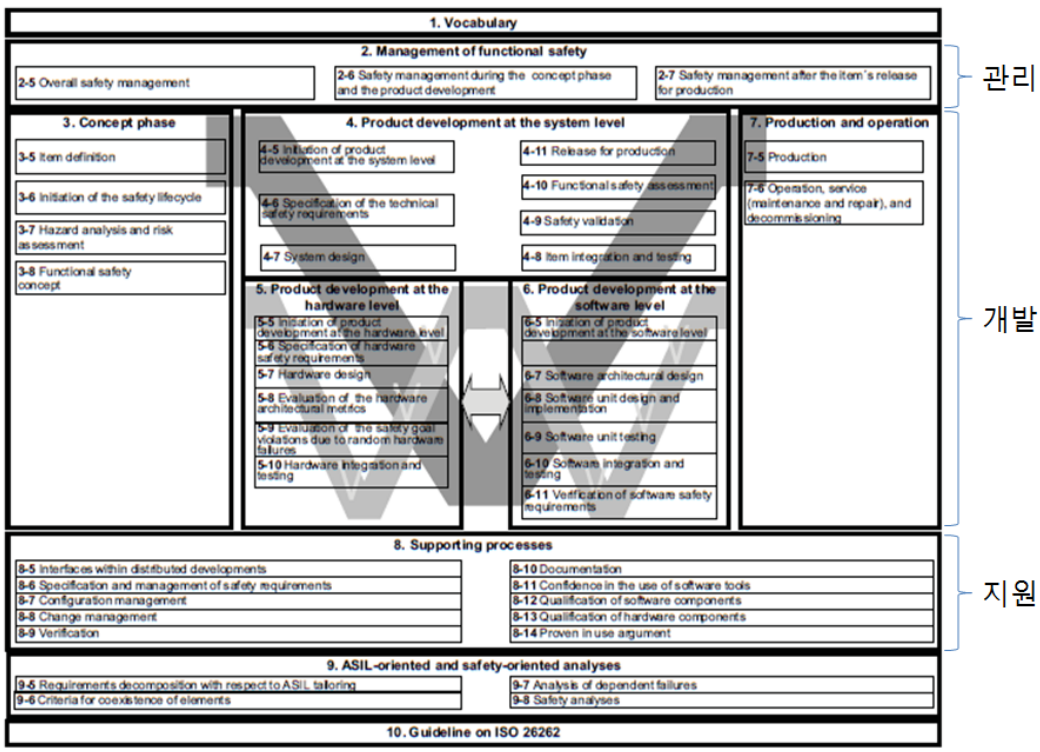
ISO 26262은 안전 표준인 IEC 61508을 차량 안전에 확장적용한 표준이다. ISO26262는 차량의 전기전자장치에 기능안전 요건을 반영하여 안전관련 활동을 진행하고 안전 메커니즘을 적용하므로 안전성을 증대시킬 수 있다. 특히 자동차 요구사항이 복잡해지며, 관련 전기전자 장치가 증가함에 따라 관련 문제들이 야기될 수 있어 자동차 분야의 특성을 반영한 차량의 전기전자의 기능안전 요건 정의 되어야 했다. 이에 2012년 ISO 산하 TC22에서 2012년 최종 공포하였다. 현재는 3.5톤 이하 승용자동차에 적용이지만 향후 상용차 및 이륜차 까지 확장 예정이다.

기능안전에서는 기능안전에 관한 컨셉부터 시작하여 컴포넌트 개발 및 검증, 통합검증까지 일련의 개발 프로세스를 제안한다. 다음 그림과 같이 크게 관리, 개발, 지원 영역으로 구분 할 수 있다.

기능안전 적용은 아이템 수준에서 기능안전 활동을 수행한다. 컨셉에서는 차량 수준에서 아이템의 정의, 위험분석, 컨셉을 정한다. 위험분석 및 평가를 통해 ASIL(Automotive Safety Integrity Level) 등급과 관련 안전목표를 정한다. 안전목표를 위배하지 않는 기능안전 요구사항(Functional Safety Requirment)을 도출한다. 공급업체는 기능안전 요구사항을 기반으로 Part4～6에 요건에 따라 개발하고 생산 및 운영은 Part7을 따른다.

2. 기능안전 프로세스 적용

컨셉 수준은 OEM에서 진행하며, 공급업체는 Part4 시스템 레벨부터 진행한다. 공급업체는 OEM의 컨셉을 검토하고 공급업체 기능안전 개발 프로세스를 기반으로 시스템을 개발해야 한다. 기능안



(그림 1) ISO 26262 기능안전 프로세스 구조

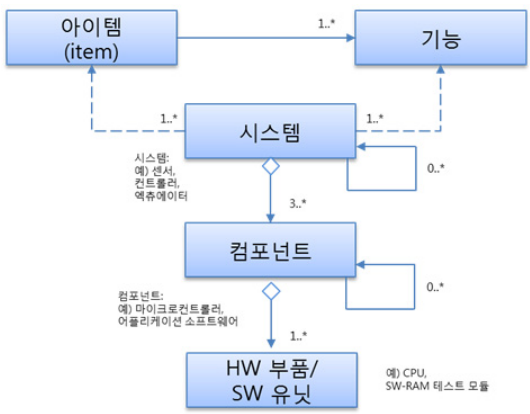
전에서 시스템의 범위는 센서, ECU, 엑츄에이터로 구성된다. 특히 시스템의 고장은 궁극적으로 차량 수준에서 관찰 될 수 있어 컨셉은 차량 수준에서 진행한다.

개발 프로세스는 요구사항, 설계, 시험과 같이 진행된다. 기능안전도 이와 같은 흐름으로 진행이 된다. 그림 3과 같이 요구사항 단계는 안전목표, 기능안전요구사항, 기술안전요구사항, 하드웨어/소프트웨어 요구사항이 도출 되고, 설계 단계에서는 컨셉개발에서 도출된 예비아키텍처, 시스템 아키텍처, 소프트웨어 아키텍처의 흐름으로 진행한다. 시험단계에서는 차량통합시험, 시스템 통합시험, HW-SW 통합시험, 소프트웨어통합시험, 하드웨어 통합시험의 흐름으로 진행된다.

이와 같은 기능안전 프로세스를 적용하기 위해 개발프로세스와 갭분석을 진행한다. 비교시 차이점은 컨셉단계에서 산출물이 입력이 되어 안전목표 중심의 요구사항과 ASIL 중심의 활동이 전개된다. 그리고 각 개발단계에서 안전분석이 강화 되어 연역적/귀납적 안전분석을 통한 설계와 검증이 이루어져야 한다. 검증과정에서 ASIL 등급별 테스트 스펙이 강화 된다. 또한 이 모든 단계별 산출물이 추적관리 되도록 지원 관리 프로세스를 이행하고 도구를 적용하여 Tool chain을 구축해야 한다.

다음은 기능안전 프로세스 적용시 고려해야 할 항목이다.

- ASIL등급별 기능안전 절차 테일러링 적용 기준
- 안전분석 절차 수립 및 활동 입력과 출력 산출물 정의
- 하드웨어 설계 및 정량적 안전분석 적용 기준

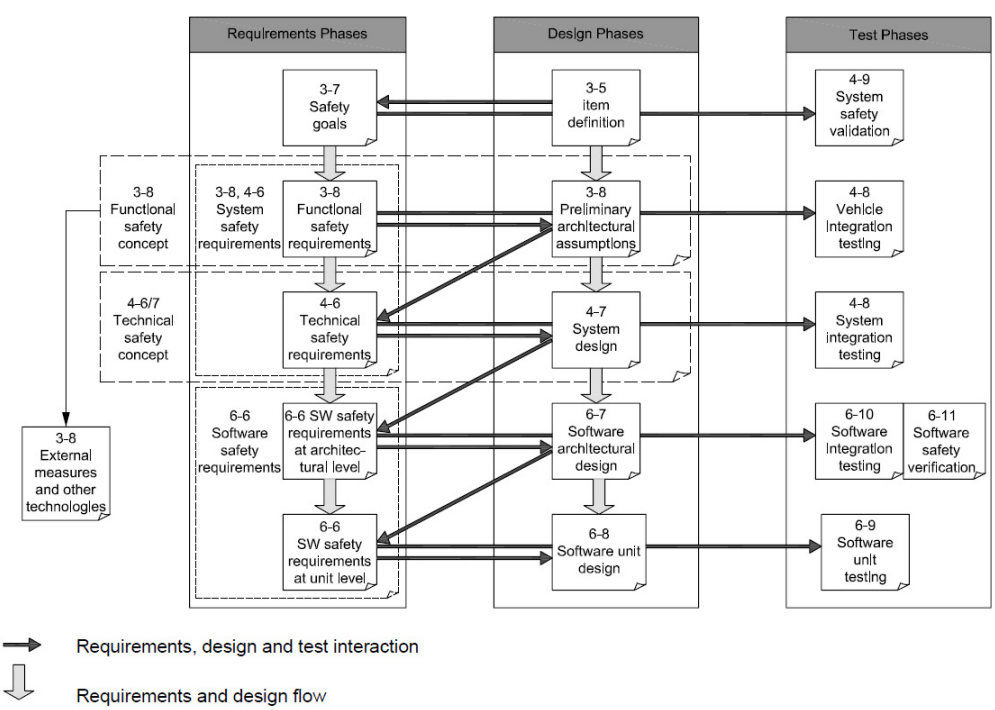


(그림 2) 아이템, 시스템, 컴포넌트, HW/SW 단위 관계

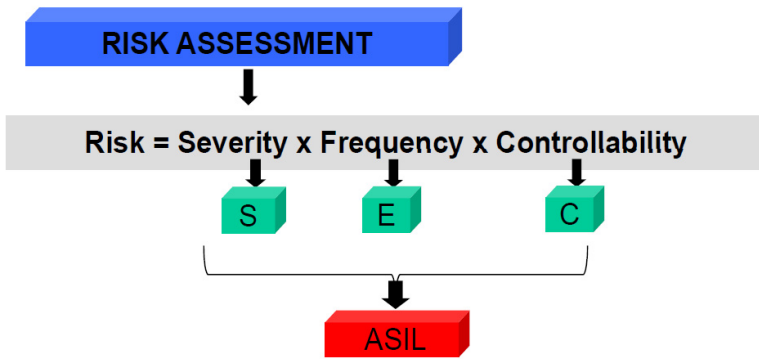
- 소프트웨어 검증(Verification) 단계 및 테스트 검증 강화

ASIL이 높을수록 요건이 강화되어 진행해야 하는 활동이 증가하게 되며, 시스템/하드웨어/소프트웨어 개발 단계에서 안전분석(FMEA/FTA)를 작성이 되어야 한다. 시스템 고장모드를 분석하여 영향을 분석하기 위해 FMEA를 수행하고 원인고장 분석 및 의존고장을 분석하기 위해 FTA를 사용할 수 있다. 하드웨어는 ASIL등급별 목표값을 만족하도록 하드웨어 아키텍처 메트릭을 작성하여 우발적 고장으로 인해 안전목표에 위반하지 않음을 정량적으로 증명해야 한다. FMEDA 양식을 통해 정량적 분석이 가능하다. 소프트웨어는 ASIL 등급별 시험 항목에 따라 테스트케이스 작성 방법과 테스트 활동을 요구한다. 특히 검증활동을 강화하고 있어 요구사항, 설계, 구현 단계마다 검증활동을 요구하며, 단위 및 통합 시험을 통한 검증을 진행해야 한다.

이외에도 기능안전 프로세스 이행을 통해 작성된 산출물의 추적관리가 필요하며, 도구활용을 권장한다. 개발 활동 중에 잦은 변경관리로 인해 추적



(그림 3) 기능안전 컨셉부터 소프트웨어 개발 단계의 흐름[1]



(그림 4) ASIL 도출 요건

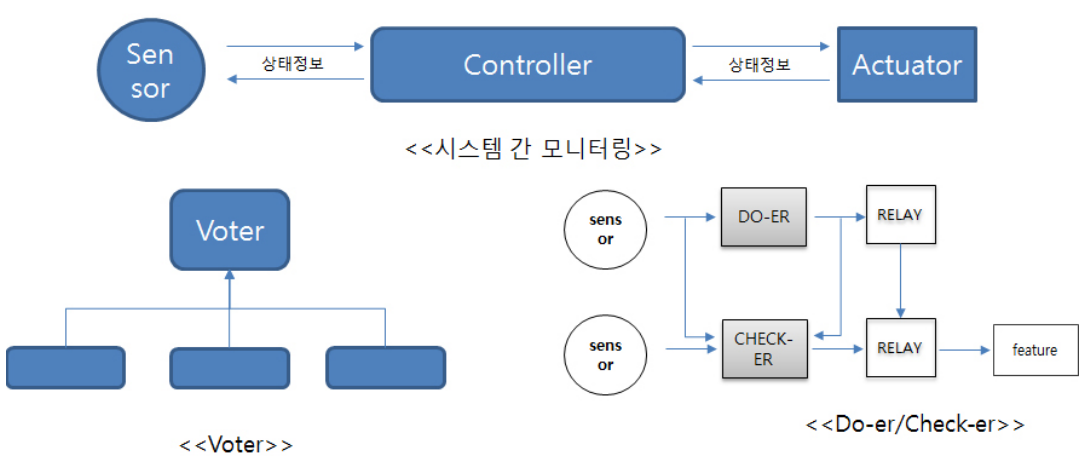
성이 혼동 될 수 있어 도구가 필요하다. 컨셉부터 시작하여 생산관리까지 각 단계별 추적성을 관리를 위한 도구는 많으나 기능안전이 적용되어야 하는 조직의 상황과 기존 도구의 활용성을 고려하여 추적관리 시스템을 구축해야 한다.

3. 강건성 설계를 위한 안전 메커니즘 도출 방안

안전목표를 위배하지 않고 고장을 방지하거나 제어하고, 하드웨어 우발고장을 감지/제어할 수 있는 활동이나 기술적인 해결책이다. 시스템 내에서 고장을 야기하는 결함을 방지하거나 결함이 잠재화 되는 것을 방지해야 한다. 안전 메커니즘은 다음 두 가지로 분류 할 수 있다. 시스템을 안전 상태로 전이하거나 유지 할 수 있어야 한다. 또는 운전자가 고장의 영향을 제어 할 수 있도록 운전자에게 정보를 제공해야 한다.

진단 모니터링을 통해 안전목표를 위배할 수 있는 엘리먼트를 감시하고 고장 발생 시 조치 및 경감할 수 있도록 기술적 지원이 가능해야한다.

그림 5과 같이 차제 모니터링 보다는 외부진단/비교진단/이중진단을 적용해야 한다. 기능안전 표



(그림 5) 보편적인 진단컨셉

〈표 1〉 센서의 진단 커버리지 종류[1]

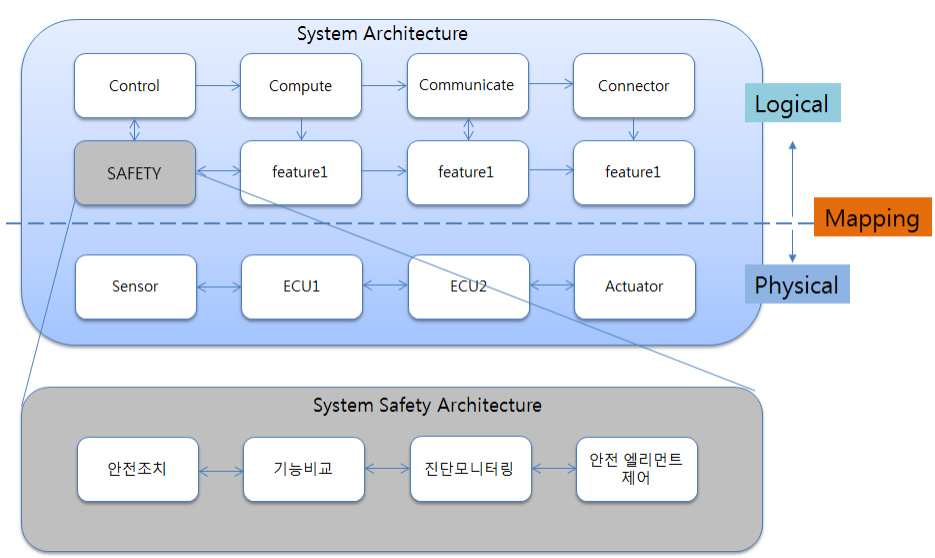
안전 메커니즘	기법 검토 참조	진단 커버리지	비고
온라인 모니터링에 의한 고장 검출	D.2.1.1	저	고장 검출의 진단 커버리지에 따름
시험 패턴	D.2.6.1	고	-
입력 비교/선택(voting) (1oo2,2oo3 또는 더 나은 중복구현)	D 2.6.5	고	진단 시험 간격 내에서 데이터흐름이 변경되는 경우에만
센서 유효 범위	D 2.10.1	저	접지나 전원 단락 및 여러 개방회로 검출
센서 상관관계	D 2.10.2	고	범위 내 고장 검출
센서 합리성(rationality) 검사	D 2.10.3	중	-

준에서 진단 커버리지 기준에서도 권장하고 있다. 이와 같은 기준을 안전컨셉을 정하고 안전설계를 진행해야 한다.

강건설계는 유효하지 않는 입력 또는 스트레스 환경 조건에서도 올바르게 작동할 수 있도록 설계되어야 한다. 강건한 소프트웨어는 비정상적인 입력과 조건에 올바르게 작동되어야 하며, 하드웨어 경우는 설계 한계 내에서 환경 스트레스를 견디고, 작동 수명 내내 안정적으로 동작할 수 있는 설계를 해야 한다. 대표적인 강건 설계는 E-GAS 모니터링 컨셉[2]이다. 3 단계 모니터링을 통해 안전목표를 위배하지 않는다.

안전 컨셉에 따른 안전설계 시 진단 모니터링 속성은 다음과 같다

- 하드웨어 엘리먼트 제어 및 모니터링
- 커뮤니케이션 프로토콜 정보 모니터링
- 완화(Mitigation) 조치



(그림 6) 시스템 안전컨셉 아키텍처

- 경고(Warning) 과 경감(Degradation) 조치

위와 같은 요소를 고려하여 시스템/하드웨어/소프트웨어 설계시 적용해야 한다. 특히 시스템 아키텍처에서 기능안전이 표시되어야 하며 이는 다시 기능안전 아키텍처로 구체화 될 수 있다. 시스템 개발에서 설계는 아키텍처를 작성해야 하며, 논리적 아키텍처와 물리적 아키텍처를 작성하여 안전컨셉이 적용 되어야 한다. 그림7은 논리적 아키텍처에 안전 관련 엘리먼트를 정의하였다. 이와 같은 방법으로 시스템 수준에서 아키텍처를 설계하면 하드웨어/소프트웨어 레벨에서 구현 되어야 한다.

4. 안전분석(FMEA) 적용방안 및 사례

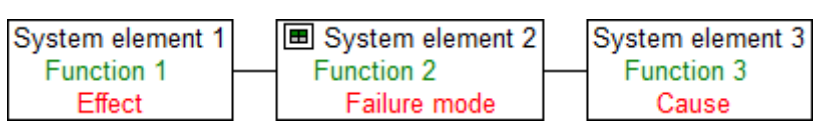
기능안전 표준에서 각 개발 단계별 안전분석을 요구한다. 안전분석에서 대표적인 방법으로 FMEA(Failure Mode Effect Analysis), FTA(Fault Tree Analysis)를 사용한다. FMEA는 아이템의 개발동안 고장을 감지하고 이를 회피하거나 고장으로 인한 영향성을 감소시키기 위해 수행되는 활동이다. FMEA는 고장(Failures)과 그 영향(Effect) 및 원인(Faults)의 분석 할 수 있다.

엘리먼트의 고장원인으로 인해 고장모드가 발생하여 시스템의 영향을 끼치게 된다. 이를 FMEA를 통해 분석이 가능하다. 특히 고장모드와 고장원인이 분석이 된 후 고장을 회피하거나 영향을 최소화 할 수 있는 발견조치와 예방조치를 도출 할 수 있다. 고장에 따른 위험을 평가하기 위해 RPN(Risk Priority Number)를 산정한다. RPN은 심각도(Severity), 결함의 발생(Occurrence), 발견(Detection)가능성의 요소를 S * O * D를 통해 계산한다. RPN의 기준은 각 조직에 따른 기준값이 필요하다. 조직의 기준치를 만족하기 위한 예방과 발견조치를 추가하여 RPN을 기준값에 만족 시킬 수 있다.

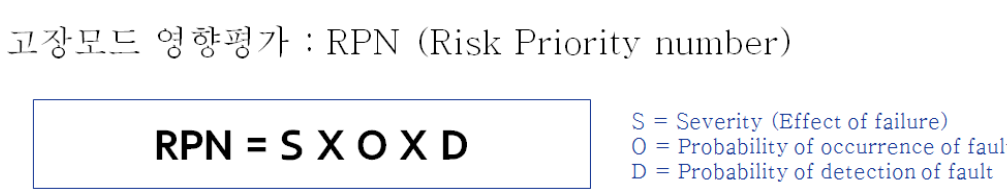
예방조치를 통해 고장발생도를 경감시킬 수 있으며, 발견조치를 통해 발생가능성을 증가 시킬 수 있다.

VDA-FMEA 방법을 사용하여 변속기 FMEA 예제를 진행한다. VDA-FMEA는 다음과 같은 순서로 진행한다.

1. 시스템 구조 작성
2. 시스템 기능 및 기능네트워크작성
3. 오류모드 및 오류네트워크 작성
4. 오류모드에 관한 예방 및 발견 조치작성



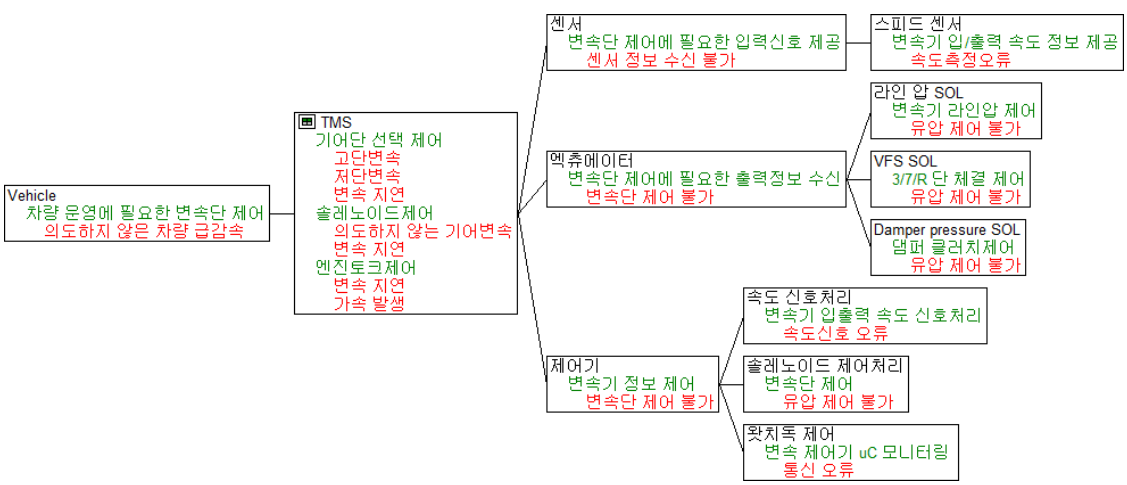
(그림 7) FMEA 기본 구조



5. RPN 입력을 통한 최적화

변속기 시스템 FMEA를 진행하기 위해 시스템 구조를 작성하고 구조를 기반으로 기능을 정의하였다. 각 기능별 네트워크를 작성하여 기능의 연관성을 분석할 수 있다. 기능에 대한 오류 모드를 작성하고 오류의 연관성을 확인하기 위해 오류네트워크를 작성 한다. 그림 10과 같이 변속기 구조, 기능, 오류를 표현 할 수 있다.

오류모드가 작성되었다면, 오류대한 발견조치와 예방 조치를 작성한다. 이는 안전 메커니즘과 연관성을 가지고 작성해야 한다. 요구사항에서 작성된 안전 요구사항은 안전 메커니즘을 명세화 하며, 안전 분석을 통해 안전 메커니즘의 적절성을 확인 할 수 있다. 이후 조치에 따른 RPN을 산정할 수 있으며, 심각도(S), 발생도(O), 발견가능성(D)을 수치화 하여 RPN을 작성한다. 그림11은 저단변속의 오류모드에 관한 RPN 값을 표현한 FMEA 시트이다.



(그림 8) 변속기 시스템 구조

Effects	S	C	Failure mode	Cause	Preventive action	O	Detection action	D	RPN	R/D
System element: TMS										
Function: 기어단 선택 제어										
[Vehicle] 의도하지 않은 차량 급감속	10		저단변속	[라인 압 SOL] >> 유압 제어 불가	Initial state:					
					Limphome	5	Electrical Error Check	3	150	
				[VFS SOL] >> 유압 제어 불가	Initial state: 2013-09-09					
					특정 단 고정	5	Electrical Error Check 운전자에게 MIL등으로 표현	3	150	
				[솔레노이드 제어처리] >> 유압 제어 불가	Initial state:					
					특정 단 고정	6	Electrical Error Check(Feed Back 전류와 전압 수준으로 비교) 운전자에게 MIL등으로 표현	3	180	

(그림 9) 변속기 시스템 FMEA sheet

6. 결 론

스마트 카 개발을 위해 요구사항은 복잡하고 고도화 되고 있다. 특히 연비/성능/품질/편의성 등 고객요구사항과 스마트 카 개발요구사항이 증가와 접목을 통해 더욱 복잡해진 개발환경에서 안전을 고려한 ISO26262 표준이 등장하였다. 제조업체 및 부품업체는 기능안전 프로세스를 적용하여 개발된 스마트 카 시스템이 안전을 고려하여 개발되었음을 증명 할 수 있어야 한다. 특히 안전분석을 적용하여 차량 수준의 오작동과 시스템 오류에 효과적인 대응이 스마트 카 개발에 중요한 역량으로 작용할 것이다. 스마트 카 전기/전자 시스템의 최적화를 위해 다양한 연구가 이루어지고 있으며 특히 전자/전기 시스템 간 연계성을 고려하여 개발 초기 단계부터 최적화된 개발 프로세스를 적용하는 개발 전략이 필요하다. 향후 ISO26262 표준의 발전된 개정과 향상된 개발 프로세스 모델 간 결합을 통해 스마트 카 특화된 개발 프로세스가 필요하다.

참 고 문 헌

[1] International Standard ISO 26262 “Road Vehicles - Functional Safety,” ISO/FDIS 26262:2011

[2] Standard “Standardized E-Gas monitoring concept” version 5.5, E-Gas work group, 2013

[3] Brewerton, S., Schneider, R., and Eberhard, D., “Implementation of a Basic Single-Microcontroller Monitoring Concept for Safety Critical Systems on a Dual-Core Microcontroller,” SAE Technical Paper 2007-01-1486, 2007

[4] Schäffele, J. and Zurawka, T., “Automotive Software Engineering: Principles, Processes, Methods and Tools,” Society of Automotive Engineers, Inc., Warrendale, PA,

저 자 약 력

강 현 구

이메일: Hyunkoo.Kang@hyundai-autron.com

- 2012년~현재 ㈜현대오트론 기능안전 담당
- 2007년 숭실대학교 컴퓨터공(석사)
- 현대오트론 기능안전 담당,

금 득 규

이메일: dkkum@uengine.org

- 2015년~현재 (주)유엔진솔루션즈 CTO
- 2009년~현재 동서울대학교 컴퓨터소프트웨어과 겸임교수
- 2014년 건강보험심사평가원 자문위원
- 2013년 국립국어원 자문위원
- 2012년 숭실대학교 전산학과(박사)
- 2007년 한국 BPM 표준화분과위원회 위원
- 관심분야 : 서비스지향 아키텍처, 스마트 자동차, 빅데이터 분석기술 등