기능안전규격 ISO 26262의 효과적 구현을 위한 시스템공학 기반 요구사항 분석/검증 방법

임 관 택* · 이 재 천*
*아주대학교 시스템공학과

On a Method to Analyze and Verify the Functional Safety of ISO 26262 Based on Systems Engineering Framework

Gwan-Taik Lim* · Jae-Chon Lee*
*Dept. of Systems Engineering, Ajou University

Abstract

According to ISO 26262 (the international standard on functional safety for automotive industry), the functional safety should be considered during the whole automotive systems life cycle from the design phase throughout the production phase. In order to satisfy the standard, the automotive and related industry needs to take appropriate actions while carrying out a variety of development activities. This paper presents an approach to coping with the standard. Analyzing the standard indicates that the safety issues of the automotive systems should be handled with a system's view whereas the conventional approach to solving the issues has been practiced with focus on the component's level. The aforementioned system's view implies that the functional safety shall be incorporated in the system design from both the system's life-cycle view and the hierarchical view for the structure. In light of this, the systems engineering framework can be quite appropriate in the functional safety development and thus has been taken in this paper as a problem solving approach. Of various design issues, the analysis and verification of the safety requirements for functional safety is a key study subject of the paper. Note, in particular, that the conventional FMEA (failure mode effects analysis) and FTA (fault tree analysis) methods seem to be partly relying on the insufficient experience and knowledge of the engineers. To improve this, a systematic method is studied here and the result is applied in the design of an ABS braking system as a case study.

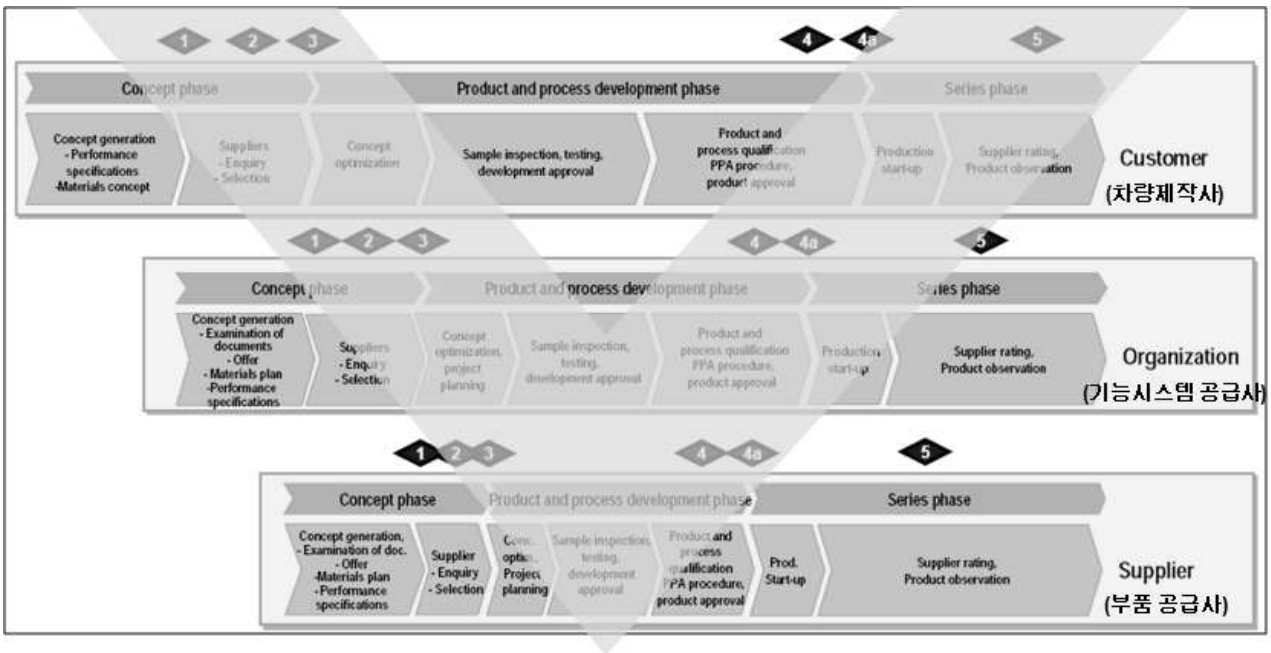
Keywords : VDA, ISO 26262, Functional Safety, System FMEA, FTA, Validation

† 이 논문은 2013년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. NRF-2012R1A1A2009193)

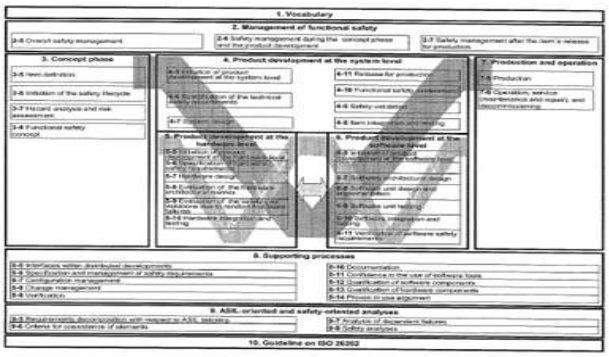
† Corresponding author: Prof. Jae-Chon Lee, Dept. of Systems Engineering, Ajou University, San 5, Woncheon, Yeongtong-Gu, Suwon, 443-749, Tel: 031-219-3941, E-mail: jaelee@ajou.ac.kr
Received July 19, 2013; Revision Received September 4, 2013; Accepted August 28, 2013.

1. 서 론

자동차 개발사를 중심으로 한 대표적인 두 영역이 북미와 유럽이며, 한국과 유럽의 자유무역협정 체결로 인해 유럽 자동차 개발사와 시장이 한국의 자동차사와 자동차 부품사에게 점점 더 중요한 고객으로 자리 매김하고 있다. 유럽 자동차 개발 주체의 중심에 독일 VDA(Verband Der Automobilindustrie; 자동차 산업 협회)가 있으며, 최근의 기능 안전성 요구사항인 ISO 26262 또한 VDA P/P(Project Plan)을 기반으로 한 계획된 표준이다[1]. VDA Band 2 Quality management in the Automotive Industry[2] 상에 <Fig. 1>과 같이 나타난 기능 시스템 및 부품 공급사를 포함한 개발 수명주기 모델은 시스템 공학의 대표적인 V-모델을 자동차 개발 프로세스 개념으로 이용하고 있으며, <Fig. 2>에서와 같이 ISO 26262 표준 Overview[3]에서도 V-모델 기반 표준 아키텍처임을 동일하게 보여준다.



<Fig. 1> Cooperation phase(in VDA Band2 Quality management in the automotive industry)[2]



<Fig. 2> ISO 26262 Overview[3]

즉, 현재 전 세계적으로 요구되는 기능 안전성 표준인 ISO 26262는 시스템 공학적 체계를 따라 구성되었으며, 세부적인 수행도 시스템 공학적 체계에 맞추면 효과적이라는 것이다.

그 중에서도 본 논문을 통해 다루고자 하는 영역은 기능 안전성의 확보를 위한 시스템 요구사항 검증/분석 방법으로 ISO 26262의 ASIL A~D 전 레벨에 "++(indicates that the method is highly recommended for the identified ASIL)"로 요구되어진 귀납적 분석 방법론인 FMEA(Failure Mode Effect and Analysis; 고장형태 및 영향분석)를 효과적으로 수행하여, 시스템 FMEA의 결과물을 도출하고 설계 검증의 명확성을 확보하기 위한 방법을 제시하는 것이다.

위험평가 기법의 정성적인 방법으로 FMEA가 있고, 정량적인 방법으로 FTA가 있다. 위험을 낮추기 위해 정성적인 방법으로 고장의 시나리오를 찾고, 정량적인 방법으로 최적의 방안을 결정한다[4]. FMEA는 ISO/TS16949 등의 표준을 통해 자동차 분야에서 필수로 요구되는 설계 검증의 항목이며, 많은 연구를 통해 수행되어 왔으나, 대부분이 부품의 설계 및 공정을 대상으로 잠재적인 고장의 형태를 도출하여 부품단위의

위험을 다뤄왔고, 또한 선행연구 들을 통해 고장형태의 예측을 너무 경험자에 의해 의존함으로써 고장형태의 누락이 많아 FMEA의 목적을 달성하기 어렵다고 하였다[5][6]. 이 문제는 실제 수행되는 고장형태 예측의 방법에 과거의 경험과 브레인스토밍을 이용하도록 유도함으로 인해 고장형태 누락의 큰 위험이 있었다.

시스템 설계 검증/분석의 방법인 FMEA는 ISO 26262 표준의 모태인 VDA P/P의 요구사항을 명확히 반영하여야 하며, 이를 위한 시스템 공학 프로세스를 이용한 자동차 시스템의 전 수명주기별 관점 그리고 동시에 계층적 관점에서 요구사항분석-기능분석-고장형태 영향분석 활동을 연계하여, ISO 26262를 만족하는 요구사항 분석/검증의 방법을 제시한다. 본 연구를 통한 결과가 ISO 26262를 만족하기 위한 수행 방법론의 핵심이 될 것이다.

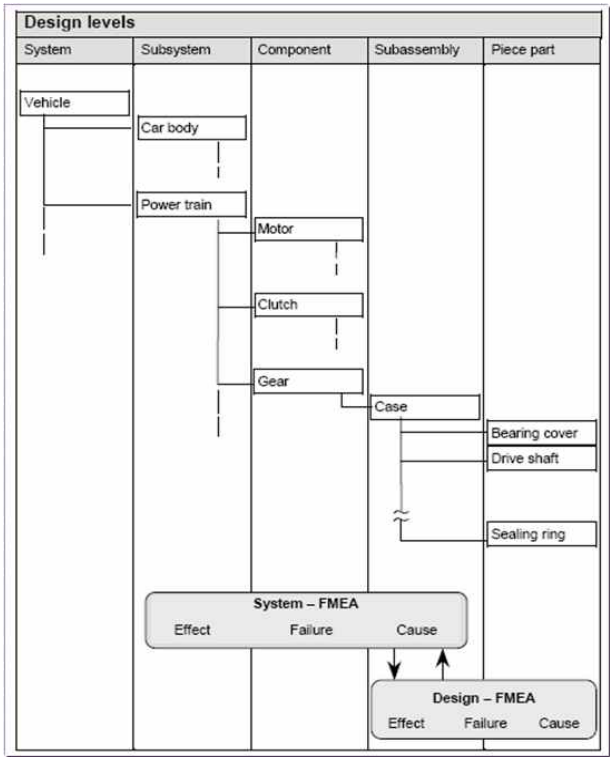
본 논문의 구성은 다음과 같다. 본 서론에 이어 제2장에서는 본 연구와 관련된 VDA P/P와 ISO 26262 관련 선행연구의 분석을 통해 문제를 정의하고 연구목표를 기술하였다. 제3장에서는 시스템 공학 프로세스에 기반하여 개발된 기능안전을 위한 안전 분석/검증 프로세스를 정의하고, 단계별 수행 활동을 설명 하였다. 제4장에서는 개발된 프로세스 모델을 자동차 ABS 시스템의 기능안전 검증 사례에 적용하여 연구결과의 검증을 수행 하였다. 마지막 제5장에서는 본 연구에서의 기여와 향후 연구수행 방향을 정리하였다.

2. VDA P/P과 ISO 26262의 분석

2.1 VDA P/P에서의 시스템 FMEA

체계적인 설계가 필요한 자동차 개발 프로세스는, 시스템 FMEA와 설계 FMEA는 수행하지 않으면 안 되는 항목이다. 두 FMEA를 통해 잠재적인 시스템 고장의 체계적 평가를 수행해야 한다.

라이프 사이클 개념의 개발 프로세스인 VDA P/P <Fig. 1>에서 “Customer” 레벨 상의 Concept phase에서부터 시스템 FMEA가 작성되어, “Organization” 레벨의 Concept phase에 입력되어야하며, 이하의 ”Supplier” 레벨에도 동일하게 입력된다. 이후 각 레벨에서 제품 및 공정 개발 단계(Product and process development phase) 활동이 수행된 후, 이 단계의 끝부분에서 제품 및 공정 승인의 활동이 상위 레벨로 연계된다. 즉, VDA P/P 기반 자동차 개발 프로세스는 <Fig. 1>에 표시한 V 형태의 의미와 같이 V-모델을 기반으로 한다.

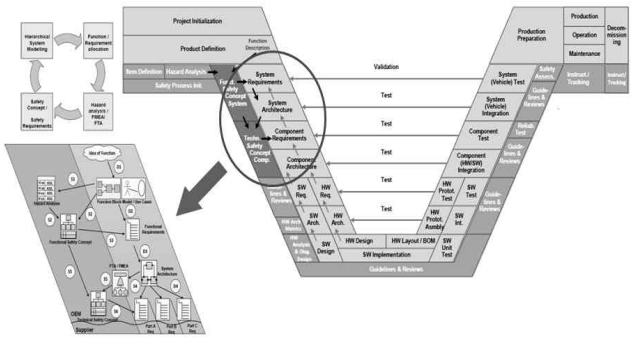


<Fig. 3> Example for design levels(in VDA Band3 Part1)[2]

위 라이프 사이클 개발 개념이 제품기준의 레벨로 표현하면 <Fig. 3>의 사례와 같다. 자동차 시스템을 구성하는 서브 시스템인 구동장치의 하위 수준 컴포넌트 단위에 모터, 클러치, 기어 등이 시스템 FMEA의 대상이 되며, 컴포넌트 하위 수준 들이 설계 FMEA의 대상 영역이 된다. 상위 수준의 시스템 FMEA가 하위 수준의 설계 FMEA로 전환되기 쉽다는 것은 설계 FMEA를 수행하는데 있어서 시스템 FMEA의 중요성을 강조하는 것이며, 본 연구의 중요한 배경인, FMEA의 고장형태는 경험자의 예측이나 브레인스토밍의 영역이 아닌, 상위 레벨의 고장 데이터가 입력되어야 한다는 것으로 시스템 FMEA의 수행이 필요하다.

2.2 ISO 26262에서의 귀납적 고장 분석 방법

ISO 26262와 IEC61508의 차이는 적용 대상의 차이에 있으며, 기본적으로 이동성을 전제로 하는 시스템으로서 제어 시스템과 안전 메커니즘이 통합되어야[7] 하는 차량은 차량 개발 프로세스와 연계되어야 한다. 시스템 공학 V-모델과 연계된 ISO 26262가 중점적으로 연구된 B. Kaiser(2012)는 <Fig. 4>와 같이 V-모델을 기반의 시스템 공학과 기능 안전의 통합을 다루었다[8].



<Fig. 4> Integration System Engineering & Functional Safety[6]

그리고, H. Aboutaleb, M. Bouali, M. Adedjouma, and E. Suomalainen(2012)는 시스템 공학 프로세스와 안전 공학 프로세스의 단계를 정의하고 두 프로세스의 연관관계와 출력물을 정의하였다[9]. 이 출력물의 두 가지가 FMEA와 FTA로 시스템 개발 프로세스와 연계된 안전 활동의 개별적 두 출력물로 존재한다.

이러한 시스템 공학적 V-모델로부터 연계되는 안전 활동까지, 전 세계 자동차 업체의 기능 안전 ISO 26262 요구사항에서 FMEA는 핵심적인 방법론이다. ISO 26262에 지정된 시스템 설계 검증을 위한 분석의 방법으로 <Fig. 5>와 같이 연역적/귀납적 수행 요구사항으로 명시되어 있다.

ISO 26262의 핵심 항목인 FMEA에 대해 이상과 같은 선행연구들을 통해, 시스템 공학 모델인 V-모델을 기반으로 하였음을 강조하는 이유는, 기능 안전 측면에서 다루어져야 하는 고장의 데이터 들이 경험에 의존한 사항이 아닌, 체계적인 분석을 통해 도출되는 산출물이며, ISO 26262의 필수항목이기 때문이다.

	Methods	ASIL			
		A	B	C	D
1	Deductive analysis[a]	o	+	++	++
2	Inductive analysis[b]	++	++	++	++
[a] Deductive analysis methods include FTA, reliability block diagrams, Ishikawa diagram.					
[b] Inductive analysis methods include FMEA, ETA, Markov modelling.					

<Fig. 5> System design analysis[3]

2.3 고장형태 도출의 선행 연구 분석

하지만 고장형태의 도출에 있어 선행 연구된 내용을 보면, 그 자체의 수준에서 더 효과적인 방법이 있는가를 연구한 것으로, 장준순(1997)[5]는 효과적인 FMEA 실시를 위해, 실시목적에 맞는 개별 FMEA 양식의 사용을 제안하였지만 난점으로 언급한 “고장모드의 예측을 너무 경험자에 의존함으로써 고장모드의 누락이 발생할 수 있다.”는 문제를 해결하지 못했고, 김상연(2007)[6]도 동일한 문제점을 지적했지만 RPN (Risk Priority Number; 위험 우선수)에 세부 항목인 심각도, 발생도, 검출도의 기준 설정의 내용을 통한 우회적 문제해결의 방안 밖에는 제시하지 못했다.

이러한 고장에 대한 부족한 분석은 기능 안전 영역의 ISO 26262 대상 시스템에는 더욱 치명적인데, 이 영역의 양승익(2012)[10]은 Use Case를 이용하여 FSR (Functional Safety Requirements; 안전 목표를 달성하기위한 안전조치를 포함한 기능적 관점의 요구사항), 시스템 요구사항을 이용하여 TSR(Technical Safety Requirements; 시스템이 FSR을 구현하기 위해 어떻게 구성되고 어떤 특성을 가져야 하는지 기술해야 하며, 잠재적 고장을 검출, 알림, 제어를 통해 안전 상태로 도달할 수 있도록 하는 구체적인 안전 메커니즘을 포함)을 바로 도출할 수 있는 것으로 주장하였고, 김연호(2011)[11]는 OEM에 의해 도출된 기능안전 요소를 포함한 요구사항을 DIA(Development Interface Agreement) 문서의 하부 항목으로 Tier(Organization or Supplier)에게 전달하고, Tier는 OEM에 의해 제공받은 시스템 요구사항을 상세화하며, 상호간의 실질적인 요구사항 교환/추적은 별도의 방법이 요구된다고 하였다. 이 DIA와 관련하여 좀 더 자세한 사례를 포함한 것이 E. Armengaud(2012)[12]의 주장인데, “프로젝트의 첫 번째 단계는 ISO 26262 작업 산출물을 전달해야 하고, 어떤 파트너에 의해서 수행되는지를 결정하는 것이다. 이러한 활동을 위해 개발 인터페이스 계약(DIA) 템플릿이 생성되며, 다음과 같은 정보를 포함한다.”고 사례를 밝히고 있지만 Tier의 수행내용을 포함하지 않은 사례로 구체적 수행 방법에 대해서는 밝히지 못하고 있다.

이는 분석 대상의 상위 레벨인 시스템을 고려하지 않거나, 구체적 수행 방법을 제시하지 못한 이유로, 시스템과 서브 시스템 또는 Customer와 Organization 간의 DIA를 명확히 정의/전달하지 않은 상태에서 분석의 결과물 만을 고객이 감사하기 때문이다. 따라서 시스템 레벨 간의 명확한 구분과 요구사항의 체계를 가지고 분석이 수행되어야 하며, V-모델 앞쪽 단계인 고객 요구사항 분석과 기능분석을 통한 고장분석을 통해 달성될 수 있다.

2.4 연구 목표 및 범위

시스템 공학의 CDR(Critical Design Review; 제시된 도면에 따라 제품이 제작되고 위험이 검토됨을 증명하

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)

는 생산보증 게이트[13])에 해당하고, V-모델 기반 ISO 26262 Part4(Product development at the system level)의 안전 분석/검증 방법인, 시스템 FMEA의 작성 프로세스를 도출한다. 이는 선행연구 들을 통해 접근하였던 단일 레벨에서의 방법론과는 다르게 시스템 공학의 프로세스를 활용하여 요구분석과 기능분석이 고장과 연계될 수 있도록 유도하는 방법론을 제시하고자 한다. FSR을 브레인스토밍을 통한 체계적으로 구성되지 못하는 문제점[14]이나 과거 경험에 의존한 데이터 확보를 주장하는 기존 연구에 대해, 본 연구가 꼭 필요한 방법론을 제시할 것이며, ISO 26262를 만족하기 위한 수행 방법론의 핵심이다.

3. 기능안전을 위한 시스템 공학 기반 안전 분석/검증 프로세스의 개발

3.1 안전 분석/검증 프로세스 개념

시스템 공학적 방법론 상위 수준 흐름도[15]의 기본 개념 중, 기능분석 부터의 항목을 이용하여,

1) 기능분석 단계의 개념이 연계될 FSC와 FSR을 도출하고, TSR의 초기 개념을 도출한다.

2) 물리적 정의 단계의 개념이 적용될 기능/부품 분석도를 이용한 기능이 적용될 부품 체계를 구축한다. 여기서 TSR의 세부 항목이 결정될 수 있으며, TSC 또한 명확해질 수 있다.

3) 기능 분석도의 세부 기능을 고장으로 변환하여 FTA(Fault Tree Analysis)의 세 레벨(고장영향/고장형태/고장원인)을 구축한다.

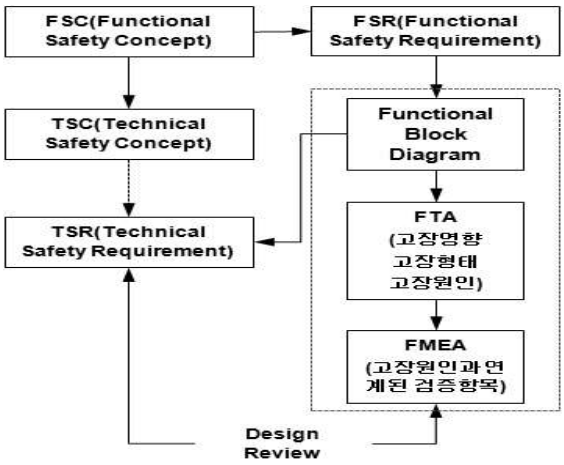
4) FTA 결과물과 연계된 검증항목을 추가한 FMEA를 완성한다.

5) 도출된 FMEA의 검증항목과 TSR의 항목이 비교되면 안전 분석/검증의 단계가 마무리된다.

안전 검증 프로세스 개념을 <Fig. 6>과 같이 도시하였다.

3.2 안전 분석/검증 프로세스 모델의 상세 수행활동 정의

1) FSC와 FSR은 ISO 26262 Part3 Concept phase의 활동이며, 이는 시스템 수준의 제품개발 이전에 해당된다. 따라서 차량 기준의 안전목표가 FSC로 표현될 것이며, 시스템을 구성하는 서브 시스템의 기능으로 할당되는 FSR이 도출될 것이다. 이 단계에서의 활동은 자동차 전체 영역을 범위로 분석될 대상에 대한 다른 시스템의 상호관계를 고려하여 분석되어야 하나, 사실상은 Organization 수준의 전문 업체 들이 자동차를 대행하여 분석/제출하고 승인받는 형태를 취하므로, 자동차 전체를 고려한 결과물이 아닌 경우들이 많아 출발 단계에서부터 분석 데이터의 리스크를 가진다고 볼 수 있다.



<Fig. 6> System Safety Analysis Process Concept

따라서 기능안전을 위해 수행해야 할 일 중에는 OEM의 역할이 더 크다고 볼 수 있고, 이를 위해 고객 요구사항을 명확히 전달해야 한다.

2) ISO 26262에서 DIA를 통해, FSC를 기반으로 도출된 TSC가 협력사에 전달된다고 하나, 실제 TSC는 개념적인 사항으로 구체적인 TSR이 도출되어야 의미가 있는 개념이 된다. 여기서 본 연구의 핵심적 내용인 기능분석도(Functional Block Diagram; FBD), FTA, FMEA가 수행되어야 TSR이 명확하게 도출될 수 있다. 특히 본 연구의 핵심적인 항목은 FBD-FTA-FMEA의 연계성을 통한 TSR의 명확한 도출의 방법론을 제시하는 것이다.

3) 기능분석도가 만들어지면, 고장을 도출하기 위한 전환을 수행하는데, 고장은 기능이 안 되는 것을 의미하는 것이다. 따라서 기능분석도의 입/출력 및 분석 대상의 기능을 FTA의 형태로 정리하는데, 고장의 레벨을 맞추는 것이 필수이다. 왜냐하면 <Fig. 3>에서 보이듯이 고장의 데이터는 동일한 표현이라도 시스템 FMEA에서는 고장의 원인인 것이 설계 FMEA에서는 고장의 영향이 되기 때문에, 목표로 하는 분석의 대상이 설계 레벨의 어디인지를 명확히 해야 한다. 마지막 레벨은 고장의 원인을 추가하는데, 검증과 연계되는 가장 중요한 시스템 FMEA의 목적 항목이 고장원인이다.

4) FMEA 형태로 고장의 세 수준(고장영향, 고장형태,

고장원인)을 정리(양식에 기입)한 후, 현 설계관리 항목을 추가하는데 고장의 원인과 연계된 시스템 설계 검증 항목이 기입된다.

5) 이 검증 항목의 전체는 도면과 고객요구사항에 있어야하며 이것이 설계검증 결과인데, 기능안전 측면에서는 TSR과 일치되어야 함을 의미한다.

1)~5)항을 통해 언급되는 고객요구사항을 사례로 <Fig. 7>과 같이 구축해 보았다. 이는 항목별로 명확히 구분되어야하며, FSR을 별도로 구분하는 것이 필요하다.

<Fig. 7> Customer Requirement Description Example

이상과 같이 설명한 본 논문에서 제시하는 ISO 26262 만족을 위한 안전 분석/검증 프로세스와 구체적인 방법론들은 다음의 실제 자동차 개발 시 적용된 사례를 통해 검증했다.

4. 개발된 안전 분석 프로세스의 적용 사례 - ABS 제동 시스템

개발된 안전 분석 프로세스가 적용된 ABS 제동시스템의 사례를 제시한다.

차량 제작사로부터 “마른노면에서 직진 주행 중 100kph에서 0kph로 제동 시 제동거리 70m이하이고, 차선 폭 3.5m를 이탈하지 않을 것”으로 FSR이 제시되면, 이를 만족하기 위한 TSR을 도출하고 검증하기 위해, 안전 분석 프로세스를 적용한다.

1) <Fig. 8>을 통해 시스템 및 서브 시스템의 사례인 ABS와 ABS Module을 표현하고, 기능분석을 위한 부품 구성도를 연계된 입/출력 부품과 구분하여 추가하였다. ABS 시스템의 기능분석의 수행은 자체 수준의 기능 분석은 물론, 서브 시스템인 Valve Block, Motor, ECU 등의 Organization 수준의 하부 단계에 입력될 요구사항으로서의 ABS 시스템 기능분석을 수행하는 것이 또 하나의 목적이 될 수 있다.

2) ABS의 부품 구성도를 기준으로 기능분석도를 작성한 것이 <Fig. 9>과 같다.

3) 기능 분석한 각 항목을 레벨 구분하여 FTA 형태로 정리하면 <Fig. 10>와 같은 결과를 얻을 수 있다.

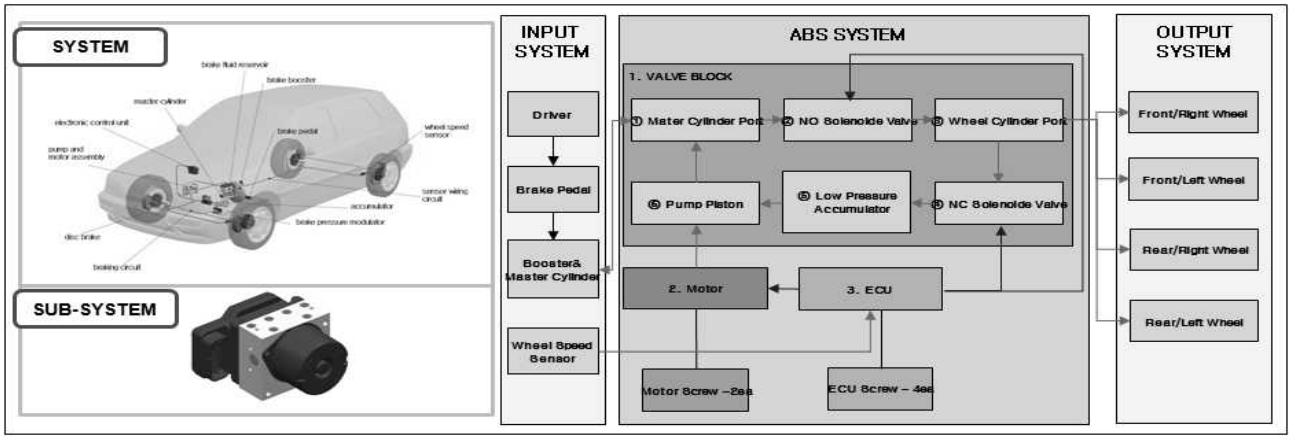
4) FTA 각 레벨은 그대로 고장영향, 고장형태, 고장원인이므로 FMEA 양식에 기입하고, 설계검증의 항목을 기입하면 <Fig. 11>의 결과를 얻는다.

5) FMEA의 현 설계관리(검증) 항목이 TSR 항목과 일치하면 요구사항 검증이 되며, TSR이 제대로 도출되었는지를 확인할 수 있거나 역으로 TSR을 도출하여 FSR과 연계성을 확인함으로서 ISO 26262의 요건을 만족할 수 있다. 이 TSR이 실제 부품 협력업체에서 수행하는 설계구상서 안에 포함되어 있고, 이 과정을 시스템 공학에서는 CDR이라 한다.

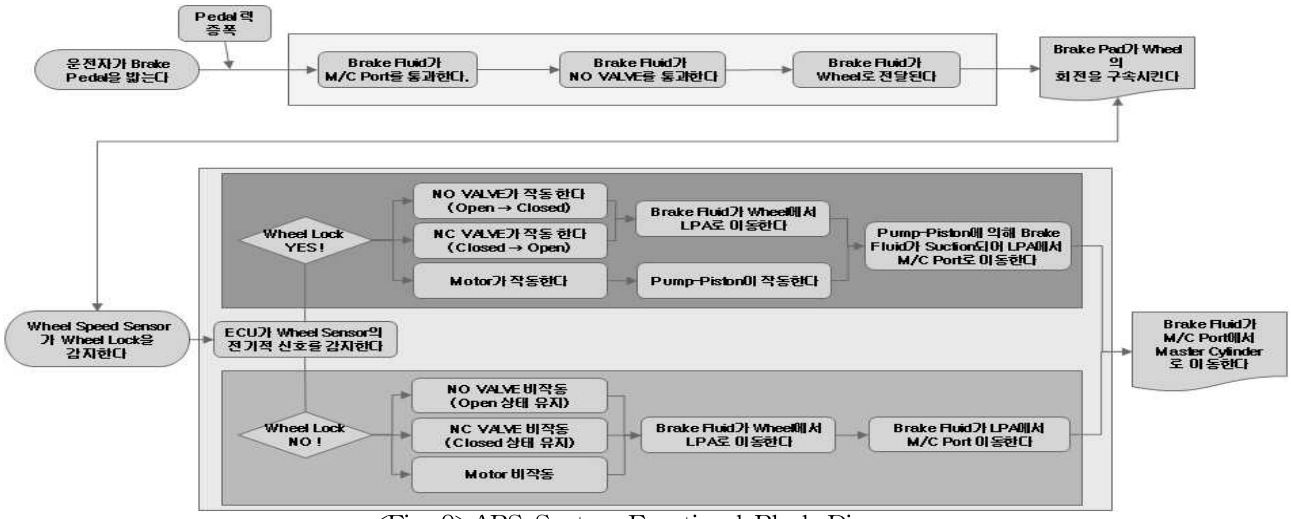
이상의 사례 분석을 통해 표준의 내용에 포함되지 않은 수행 방법론의 모호성으로 인해 공학적으로 필요치 않은 활동들이 수행될 가능성을 줄이기 위해 사례 분석을 추가하여 명확히 방법론의 효과를 설명하였다.

5. 결 론

VDA P/P를 기반으로 한 ISO 26262 표준에는 제품 개발 과정에서 제품의 안전을 확보하기 위해 반드시 필요한 안전 활동들과 그에 대한 수행방법에 대한 요구사항 만을 기술하고 있다. 구체적인 설계 방법이나 하드웨어와 소프트웨어 개발 방식에 대해서는 명확하게 표현되어 있지 않으며, 제품 개발 조직 내에서 개발 가이드라인이 반드시 필요한 조건이라고 기술되어 있다[16]. 또한 핵심 내용인 고장을 누락 없이 정의하는 것이 명확해야 함을 인지하여, 시스템 공학 이론을 이용한 개발 가이드라인을 제시하기 위해 <Fig. 6>과 같은 실행 프로세스를 제시하고, 그 방법론을 연구하여, 세부 실행 방법을 설명하고, 사례를 제시하였다.



<Fig. 8> ABS(System level), ABS module assembly(Sub-system level)의 Hardware Block Diagram



<Fig. 9>ABS System Functional Block Diagram

P1	Brake Pad가 Wheel의 회전을 구속시키지 못한다	P11	Brake Fluid가 M/C Port를 통과하지 못한다	P111	이물질로 인해 M/C Port 유로가 차단된다
				P112	M/C Port에서 Brake Oil Leak 발생한다
		P12	Brake Fluid가 NO VALVE를 통과하지 못한다	P121	이물질이 Orifice의 유로를 차단한다
				P122	Armature가 Orifice의 유로를 차단한다
				P123	Filter에 이물질이 끼어 유로를 차단한다
				P124	Filter가 손상되어 내부 Leak가 발생한다
		P13	Brake Fluid가 W/C Port를 통과하지 못한다	P131	이물질로 인해 W/C Port 유로가 차단된다
				P132	W/C Port에서 Brake Oil Leak 발생한다
		P14	Brake Fluid가 Wheel로 전달되지 못한다	P141	W/C Port에서 Brake Oil Leak 발생한다
P2	Brake Fluid가 M/C Port에서 Master Cylinder로 이동하지 못한다.	P21	ECU가 Wheel Sensor의 전기적 신호를 감지하지 못한다	P211	통신 Cable 사양이 차량 요구 사항과 맞지 않다
				P212	ECU S/W에 이상이 있다
		P22	NO VALVE가 작동 하지 않는다(Open → Closed)	P221	Sleeve에 Armature가 끼인다
				P222	NO VLAVE에 인가되어지는 전류량이 충분하지 않다
				P223	Orifice에 이물질이 끼어 Plunger가 유로를 차단하지 못한다
				P224	Plunger를 밀어주는 Spring의 탄성력이 충분하지 않다
				P225	Magnet Core와 Armature사이의 자속량이 충분하지 않다
		P23	NC VALVE가 작동 하지 않는다(Closed → Open)	P231	Magnet Core와 Armature사이의 자속량이 충분하지 않다
				P232	Magnet Core와 Armature사이에Spring의 탄성력이 과도하게 크다
				P233	Magnet Core와 Armature사이의 Air Gap이 충분하지 않다
				P234	Orifice에 이물질이 끼어 Armature가 뒤로 밀려도 유로가 형성되지 않는다
				P235	Armature가 Seat-Housing에 낀다
		P24	Motor가 작동하지 않는다	P241	Bearing이 Motor Shaft에서 이탈된다
				P242	Motor 작동 전류가 충분하지 않다
		P25	Brake Fluid가 LPA로 이동/임시저장되지 않는다	P243	LPA 외부 Leak 가 발생한다
				P244	LPA Piston이 Block에 낀다
				P245	LPA Spring의 탄성력이 과도하다
		P26	Pump-Piston이 작동하지 않는다	P261	Piston이 Block에 끼인다
				P262	Piston이 Motor Bearing과 접촉되어 있지 않다
				P263	Sealing-Ring이 파손되어 Leak 발생한다
				P264	Piston Return Spring의 탄성력이 과도하다
		P27	Pump-Piston에 의해 Brake Fluid가 Suction되어 LPA에서 NO VALVE로 이동하지 못한다	P271	연결 유로에 이물질이 끼어 유로를 차단한다
		P28	Motor가 비작동 상태를 유지하지 못한다	P281	ECU에서 전류를 차단하지 못한다
		P29	Brake Fluid가 Wheel에서 M/C Port로 이동하지 못한다	P291	연결 유로에 이물질이 끼어 유로를 차단한다

<Fig. 10> Using the concept of FTA, derived Failure effects, failure modes and failure causes

잠재적 고장 형태 및 영향분석 (시스템 FMEA)

시스템: 설계책임:
서브시스템: 핵심팀:
모델연도/모델명:

기능	고장 형태	고장 영향	심각도	분류	고장 원인/발생과정	발생도	현 설계관리 항목
Brake Pad가 Wheel의 회전을 구속시키지 못한다	Brake Fluid가 M/C Port를 통과하지 못한다	Brake Pad가 Wheel의 회전을 구속시키지 못한다 차량을 제동시키지 못한다			이물질로 인해 M/C Port 유로가 차단된다		조립 gap, Rod 길이 치수, 실린더 스트로크
					M/C Port에서 Brake Oil Leak 발생한다		gap, 누적공차분석
	Brake Fluid가 NO VALVE를 통과하지 못한다				이물질이 Orifice의 유로를 차단한다		내마모/시일 type, 작동유와 match, 작동온도, 경도
					Armature가 Orifice의 유로를 차단한다		내마모성, 재질, 패턴
					Filter에 이물질이 끼어 유로를 차단한다		재질/oil, 작동시 온도
					Filter가 손상되어 내부 Leak가 발생한다		내열성
	Brake Fluid가 W/C Port를 통과하지 못한다				이물질로 인해 W/C Port 유로가 차단된다		gap 및 R.spring
					W/C Port에서 Brake Oil Leak 발생한다		단면적/스트로크
	Brake Fluid가 Wheel로 전달되지 못한다				W/C Port에서 Brake Oil Leak 발생한다		밀폐
Brake Fluid가 M/C Port에서 Master Cylinder로 이동하지 못한다.	ECU가 Wheel Sensor의 전기적 신호를 감지하지 못한다	Brake Fluid가 M/C Port에서 Master Cylinder로 이동하지 못한다.			통신 Cable 사양이 차량 요구사항과 맞지 않다		oil type/유로 선정
					ECU S/W에 이상이 있다		seal 내구성/내마모/내열성

<Fig. 11> ABS System FMEA

ISO 26262의 프로세스 중 잠재적인 고장에 대해 기능안전을 위해 수행해야할 핵심인 고장의 도출 및 검증 방법을 요구사항과 연계한 방법으로 제시한 것에 있어서, ISO 26262를 만족해야만 수출이 가능한 자동차사 및 부품사에 꼭 필요한 실무적 방법론이다.

특히 기능안전을 필요로 하는 대상의 한 부분은 전자부품이며 이 경우 FMEDA(Failure Modes Effects and Diagnostic Analysis)를 사용할 수 있는 것은 부품의 데이터베이스가 구축되어 있기 때문이다. 하지만 이 방법의 근본적 문제는 기계적 구성요소에 대한 데이터베이스가 부족하다는 것이다[17]. 따라서 본 연구의 유용성은 기계와 전자부품이 함께 사용되는 기능안전 대상부품에 있다.

실무적으로 필요한 부분에 더 많은 연구의 노력을 들이고자 하였다. 향후에는 ISO 26262 기능안전의 배경 지식인 운영환경에 내재하는 기존의 위험과 시스템 오류로 인해 생성된 위험[18]에 대해 더 세부적으로 연구를 수행하여, 세계 자동차사 들이 추진하는 ISO 26262 기능안전을 위한 효과적 수행을 위해 기여토록 하겠다.

6. 참 고 문 헌

[1] P. Robert and H. Ibrahim, "Assurance of Automotive Safety - A Safety Case Approach," in Proc. 29th International Conference, SAFECOMP 2010, Vienna, Austria, Sep. 14-17, 2010, pp. 82-96.

[2] VDA(Verband Der Automobilindustrie), "Band 2, 3, 4 Quality management in the Automotive Industry," German Automotive Industry Association, 4. edition 2004

[3] ISO 26262-4, Road vehicles－Functional safety－Part 4: Product development at the system level, First edition, 2011-11-15

[4] B. William, "Selection of Hazard Evaluation Techniques," Retrieved October, Knoxville, USA, 2004, p. 2009.

[5] Jang, J.S., and An, D.J., "How to perform FMEA effectively", KSQM, KISTI, v. 25 no. 1, pp. 156-172, Mar. 1997.

[6] Kim, S.Y., Kim, H.G., and Yun, W.Y., "Reestablishment of RPN Evaluation Method in FMEA Procedure for Motors in Household Appliances ", KSQM, KISTI, v.35 no.1, pp. 1-9, Jan. 2007.

[7] Cho, J.H., Jung, Y.J., Jeon, S.H., Han, T.M., and Kim, H.S., "An implementation of automotive development methodology based on ISO26262," KASE Conference, KASE, Nov. 2010, pp. 2052-2059.

[8] B. Kaiser, "Approaches towards reusable safety concepts," in Proc. VDA Automotive SYS Conference, May 15, 2012.

[9] A. Hycham, B. Mohamed, A. Morayo, and S. Emilia, "An integrated approach to implement system engineering and safety engineering processes: SASHA Project," ERTS2012, pp. 1-6, 2012.

[10] Yang, S.I., and Lee, N.H., "The case study of

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)

ISO26262 product requirements analysis applying requirements engineering," KASE Conference, KASE, Nov. 2012, pp. 2609-2615.

[11] Kim, Y.H., Cho, S.Y., and Kim, H.W., "A method of system requirements specification corresponding to ISO26262 functional safety," KASE Conference, KASE, Nov. 2011, pp. 1548-1553.

[12] E. Armengaud, Q. Bourrouilh, G. Griessnig, H. Martin, and P. Reichenpfader, "Using the CESAR Safety Framework for Functional Safety Management in the context of ISO 26262," ERTS²- EMBEDDED REAL TIME SOFTWARE AND SYSTEMS, 2012.

[13] F. Kevin, M. Hal, and C. Howard, Ed(s). Visualizing project management: Models and frameworks for mastering complex systems. New Jersey: Wiley. com, 2005, Chapter 9.

[14] M. Ellims, H. Monkhouse, and A. Lyon, "ISO 26262: Experience applying Part 3 to an in-wheel electric motor," in Proc. 2011 6th IET International Conference on System Safety, 2011, pp. 1-8.

[15] A. Kossiakoff and W. N. Sweet, Ed(s). Systems Engineering Principles and Practice. New Jersey: Wiley, 2011.

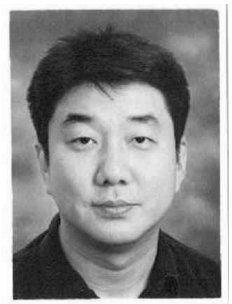
[16] Jung, Y.J., Cho, J.H., Jeon, S.H., and Han, T.M., "Solution for complexity of HW-SW integration for automotive platform," KASE Conference, KASE, Nov. 2009, pp. 2051-2055.

[17] G. John C and G. William M, "FMEDA - Accurate Product Failure Metrics," exida, Sellersville, USA, Feb. 19, 2007.

[18] B. Cogan, Ed(s). SYSTEMS ENGINEERING - PRACTICE AND THEORY. Rijeka Croatia: InTech, Mar. 2012, 4. A Safety Engineering Perspective, pp. 97-126.

저 자 소 개

임 관 택



현 아주대학교 시스템공학과 박사과정. 관심분야는 시스템 안전 설계, 요구사항 관리, 모델기반 시스템공학, 설계 검증, 설계 추적성 등.

주소: 경기도 수원시 영통구 원천동 산5번지 아주대학교 성호관 242호

이 재 천

현 아주대학교 시스템공학과 정교수. 서울대학교 전자공학과에서 공학사, KAIST 전기 및 전자공학과에서 공학석사 및 박사 학위를 취득. 미국 MIT에서 Post-Doc을 수행하였으며, Univ. of California (Santa Barbara)에서 초빙연구원, 캐나다 Univ. of Victoria (BC)에서 방문교수, KIST에서 책임연구원 재직. 이 후 미국 Stanford Univ. 방문교수 역임. 현재 연구 및 교육 관심분야는 시스템공학 및 Systems Safety에의 응용 등.

주소: 경기도 수원시 영통구 원천동 산5번지 아주대학교 서관 309호