J. Soc. Korea Ind. Syst. Eng Vol. 40, No. 3 : 27-37, September 2017
https://doi.org/10.11627/jkise.2017.40.3.027
ISSN : 2005-0461(print)
ISSN : 2287-7975(online)

Developing a Quality Risk Assessment Model for Product Liability Law

Hyung Sool Oh†

Dept. of Industrial & Management Engineering, Kangwon National University

제조물 책임(PL)법 대응을 위한 품질 리스크 진단 모델 개발

오 형 술†

강원대학교 산업경영공학과

As the global uncertainty of manufacturing has increased and the quality problem has become global, the recall has become a fatal risk that determines the durability of the company. In addition, as the convergence of PSS (product-service system) product becomes common due to the development of IT convergence technology, if the function of any part of hardware or software does not operate normally, there will be a problem in the entire function of PSS product. In order to manage the quality of such PSS products in a stable manner, a new approaches is needed to analyze and manage the hardware and software parts at the same time. However, the Fishbone diagram, FTA, and FMEA, which are widely used to interpret the current quality problem, are not suitable for analyzing the quality problem by considering the hardware and software at the same time. In this paper, a quality risk assessment model combining FTA and FMEA based on defect rate to be assessed daily on site to manage quality and fishbone diagram used in group activity to solve defective problem. The proposed FTA-FMEA based risk assessment model considers the system structure characteristics of the defect factors in terms of the relationship between hardware and software, and further recognizes and manages them as risk. In order to evaluate the proposed model, we applied the functions of ITS (intelligent transportation system). It is expected that the proposed model will be more effective in assessing quality risks of PSS products because it evaluates the structural characteristics of products and causes of defects considering hardware and software together.

Keywords : Risk Management, PL Llaw, Product-Service System, FTA-FMEA based Risk Assessment Model

1. 서 론

제조 및 경영 환경이 글로벌화 되면서 제조산업 전체에서 리콜이 갈수록 증가하는 추세이다. 공정거래위원회의 발표자료에 의하면 2013년의 총 973건의 리콜건수가 2014년에 1,752건으로 80% 정도 증가한 이후로 해마다 1,600여 건의 리콜이 발생하고 있다. 특히, 최근 들어 국내외 자동차 산업 분야에서는 10% 이상씩 리콜 사례가 급격히 증가하고 있다. 이에 더해 국내 시장에서는 소비자 권한이 갈수록 커지면서 국가에서는 징벌적 손해배상제 도입과 생산자의 책임을 더욱 강화한 제조물책임법(PL법)을 2018년 3월 이후부터 시행하는 것으로 국회에서 통과되었다.

도요타의 리콜사태, 유럽 SUV 차량의 연비조작으로 인한 리콜, 삼성 갤럭시 노트7 베터리 폭발사건으로 인한 리콜, 에어백 대량 리콜 사태와 은폐 논란으로 파산한 세계적

Received 5 September 2017; Finally Revised 19 September 2017; Accepted 20 September 2017
† Corresponding Author : hsoh@kangwon.ac.kr

자동차 부품 제조업체인 일본 다카타 회사 사건. 이처럼 제조의 글로벌화로 인해 품질 불확실성이 갈수록 증가하고, 품질 문제도 글로벌화 되면서 리콜사태는 기업의 존폐를 결정하는 치명적인 리스크가 되었다. 또한 IT융합기술 발전으로 제품의 융합화(PSS : product-service system)가 일반화 되면서 하드웨어나 소프트웨어 어느 한 부분의 기능이 정상적으로 작동되지 못하면 PSS 제품 전체 기능에 문제가 생기게 된다. 이런 PSS 제품의 품질을 안정적으로 관리하기 위해서는 하드웨어와 소프트웨어 부분을 동시에 해석하고 관리할 수 있는 방법이나 도구가 필요하다. 하지만, 현재의 품질문제를 해석하는데 널리 사용되는 특성요인도(fishbone diagram), FTA(fault tree analysis), FMEA (fail model and effect analysis) 등은 각 도구들이 개별적으로 사용되며, 하드웨어와 소프트웨어를 동시에 고려하여 품질문제를 해석하기에는 적합지 않다.

최근 대다수 하드웨어 시스템에서 내장 소프트웨어(embedded software)의 사용이 확대되면서 소프트웨어 시스템이 가지고 있는 안정성과 보안성에 관련된 결함들을 분석하기 위해 FMEA와 FTA를 결합하여 고장을 해석하는 방법에 대한 연구가 발표되었다[7, 9]. 하지만 이 연구에서는 FTA를 기준으로 각 결함의 발생 가능성을 실제로 발생한 확률이 아닌 FMEA에 의해 정성적으로 평가한다. Faisal[1]은 보우타이(bow-tie) 방법을 FMEA와 연계하여 화학공장의 리스크를 평가하는 방법을 제시하였지만, 본 연구에서는 FTA와 FMEA 방법을 개별적으로 사용한다. 본 논문에서는 품질을 관리하기 위해 현장에서 매일 평가하는 불량률(% 또는 ppm) 자료와 불량문제 해결을 위한 분임조 활동 시 사용하는 특성요인도 자료를 근거로 작성하는 FTA와 FMEA를 결합한 품질 리스크 진단 모델을 제안한다.

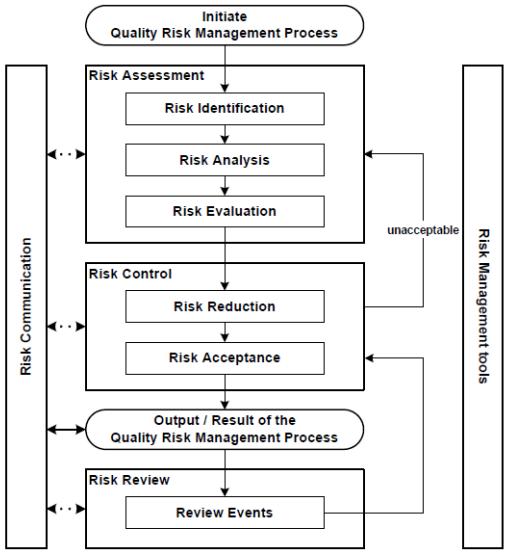
품질 리스크 진단 모델 개발을 위해 본 논문에서는 먼저 각 산업분야의 품질경영에 관한 국제적인 품질표준을 규정하는 대표적인 ISO 시리즈에서 리스크 관리를 위한 규정의 특징을 제 2장에서 살펴본다. 제 3장에서는 FTA, FMEA의 특징에 대해 살펴보고, 리스크 평가를 위해 두 가지 방법을 통합하여 적용할 필요성에 대하여 설명한다. 4절에서는 본 논문에서 제시하는 품질 리스크 진단 절차와 모델에 대하여 사례를 통해 설명한다.

2. ISO 표준별 리스크 관리

제조 산업의 대표적 제품인 자동차 산업에서 매년 10% 이상씩 리콜이 증가하는 주요 이유가 개발과 생산비용 절감을 위해 적극 추진한 부품 공용화와 연비향상을 위해 전자부품의 비중을 높인 결과의 부작용으로 보는 진단이다[6]. 부품 공용화는 품질 특히 신뢰성 측면에서 문제가 될 수 있으며 또한, 부품 공용화는 한 부품이 잘못되면 그 부품을 채택한 여러 제품에서 품질문제가 동시에 발생할 수밖에 없게 된다. 전자부품의 경우에는 기계적 결함과 달리 사고가 나도 재현하거나 원인 입증이 어려울 수 있다는 점이다. 이 같은 제품기술의 변화로 인해 기업은 리콜이나 PL법으로 인해 감당해야하는 리스크는 점점 커질 수밖에 없을 것이다. 본 절에서는 품질 리스크 진단 모델 개발에 앞서 먼저, 기업에서의 리스크 관리에 대한 산업별 ISO의 리스크 관리에 관한 규정과 특징을 살펴본다.

2.1 ICH Q9 품질경영시스템

ICH Q9은 2002년 8월에 미국 FDA에서 제약기술의 발전과 제조의 세계화 등에 대처키 위해 개발 단계에서부터 제품 라이프사이클 전체에 대한 품질 리스크 관리(quality risk management)를 위해 고시한 규정이다[5]. ICH Q9에서는 리스크(risk)를 “위해성(harm)의 발생 확률과 심각성의 결합”으로 정의하고 있다(ISO/IEC Guide51). Q9에서 정의하는 QMS는 원료의약품과 완제의약품의 라이프 사이클 전체에 걸쳐 개발, 제조, 유통, 실사 및 허가 신청/심사 업무와 관련하여 규제기관과 업체 모두 보다 효과적이고 일관성 있는 리스크 기반 의사결정을 가능하게 하는 품질 리스크 관리 기준을 제시한다. 품질 리스크 관리의 개략도는 <Figure 1>과 같다[3].



<Figure 1> QMS Diagram in Q9

리스크 진단(risk assessment)은 위해요소들(hazards)을 파악(risk identification)하고, 이들 위해요소와 연관된 리스크를 분석(risk analysis), 평가(risk evaluation)하는 3단계

로 이루어진다. 리스크 진단 단계에서 품질 문제점이나 리스크를 정확히 규정하고, 평가하기 위해 다음의 3가지 질문을 한다.

- 무엇이 잘못될 수 있는가?
- 그 문제가 발생할 수 있는 가능성(확률)은 얼마인가?
- 그에 따른 결과는 어느 정도인가(심각성)?

2.1.1 리스크 파악(Risk Identification)

과거 데이터나 이론적 분석 또는 충분한 정보를 통하여 '무엇이 잘못될 수 있는가?'를 파악한다. 이를 통해 위해요소들을 정리하고, 그에 따라 발생할 수 있는 결과도 파악한다.

2.1.2 리스크 분석(Risk Analysis)

파악된 위해요소와 관련된 리스크를 평가하는 것이다. 발생 가능성과 위해요소의 심각성을 연계시켜 평가하는 정성적 또는 정량적 프로세스이다. 위해의 감지가능성(detection)을 고려하여 평가하기도 한다.

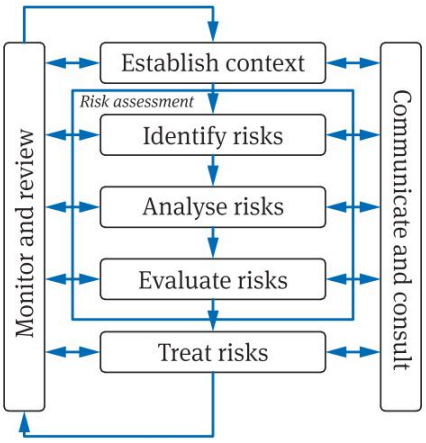
2.1.3 리스크 평가(Risk Evaluation)

분석 결과를 리스크 기준과 대비하여 위해요소의 리스크 수준을 평가하는 것이다. 데이터가 평가결과의 질적 수준을 결정하기 때문에 효과적인 리스크 평가를 위해서는 데이터의 정확성이 중요하다. 제품이나 공정에 대한 이해 부족, 공정의 변동성, 문제의 감지 확률 등으로 인한 데이터 불확실성을 고려하여 리스크 평가 결과를 정량적 추정치나 정성적 표현으로 나타낸다.

2.2 ISO 31000의 리스크 경영시스템

ISO 31000 : 2009는 리스크 관리를 구현하는 방법의 원칙 및 지침에 대한 개괄적으로 규정한 대표적인 국제표준으로서, 각 단위부문의 리스크 관리를 위한 프로세스는 <Figure 2>와 같다[5]. 이 표준은 특정 리스크를 관리하고 옵션을 선택하는 가장 적합한 방법에 대한 의사결정의 기초를 제공하여 의사결정자가 목표달성뿐만 아니라 이미 정한 의사결정의 적절성에 영향을 미칠 수 있는 리스크를 이해하는 데에도 도움이 된다[5].

ISO 31000에서는 리스크를 "목표에 대한 불확실성의 영향(effect of uncertainty on objectives)"으로 '목표', '불확실성', '영향' 3가지의 키워드로 정의하였다. 먼저, 목표는 재무, 안전 및 환경 목표 등에 대한 전략적 수준이나 제품 및 프로세스 수준 등의 다양한 수준이 대상이 될 수 있다. 불확실성은 사건(event)에 대한 지식이나 이해 부족으로 인해 그것의 결과나 가능성에 대해 정보가 부족한 상태를 의미한다. 영향은 의사결정 결과가 기대와 다르게 긍정 또는 부정적으로 나타난 결과를 의미하고 있다[5].



<Figure 2> The ISO 31000 : 2009 Risk Management Process

2.3 ISO 9001 : 2015의 리스크 기반 사고(Risk-based Thinking)

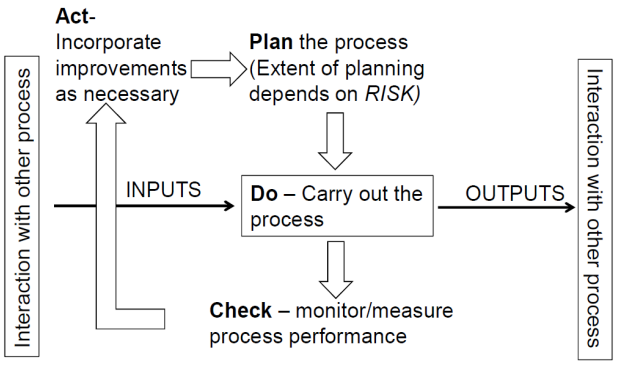
품질경영시스템(QMS)이라고도 불리는 ISO 9000은 1987년 처음으로 제정된 품질경영에 관한 국제적인 품질표준으로서, 기업이 자사의 품질경영시스템을 규정된 절차에 따라 체계적으로 이행하고 있음을 보증한다[2]. ISO 9000 시리즈는 제품 생산과정 및 품질보증 즉, 품질 시스템에 대한 기준으로 각국의 규격과 시험 및 검사 방법을 통일시키고, 시험결과를 상호 인정한다는 취지하에서 상호 간의 기술 장벽을 제거하는 중요한 수단으로 이용되고 있다[2]. ISO 9000 : 2008 시리즈는 고객의 필요를 충족하고 일관성 있는 제품 및 서비스 제공을 위해 여러 품질상의 목적과 철학에 맞추어 8가지 품질경영원칙으로 구성되었다[12, 13]. 이후로 7년 만에 개정된 ISO 9001 : 2015 품질경영시스템에서는 기존의 8대 원칙 중 '경영에 대한 시스템적 접근방법'을 프로세스 접근방법에 통합 7대 원칙으로 변경하였으며, "리스크 기반 사고(risk-based thinking)"라는 개념을 도입하였다. 새로워진 프로세스 접근방법 원칙에는 프로세스가 완전한 통합 시스템으로서 작동되도록 다음 3가지 프로세스 수립을 포함하고 있다[4].

- 경영 시스템은 목표를 달성하기 위한 프로세스와 조치를 통합한다.
- 프로세스는 상호 연관된 활동과 점검을 정의하고, 의도된 결과를 제공한다.
- 조직 상황에 따라 세부계획 및 통제를 필요에 따라 정의하고 문서화 할 수 있다.

위의 3가지 개념이 ISO 9001 : 2015 표준의 핵심 부분으로서, 목표 및 결과에 영향을 미칠 수 있는 리스크가 품질경영시스템에 의해 해결되도록 요구한다. 이를 위한 리스크 기반 사고는 프로세스 접근방법 전반에 걸쳐 다음의 것들을 규정한다[4].

- 프로세스의 결과 향상 및 바람직하지 않은 결과 방지를 위한 프로세스 수립 시, 리스크(긍정적 또는 부정적)를 어떻게 처리할 것인가?를 결정한다.
- 리스크 관점에서 필요한 프로세스의 계획 및 통제 범위를 정의한다.
- 리스크를 근원적으로 다루어 목표를 충족시키도록 시스템을 유지 관리한다.

ISO 9001 : 2015에서는 리스크 관점에서 필요한 프로세스의 계획 및 통제 범위를 정의하도록 요구는 하고 있지만, 리스크를 파악, 분석 및 평가하는 가장 적합한 도구에 대한 요구사항이 없다. 이로 인해 기업에서는 다양한 리스크 기반 접근 방식을 개발할 수 있으며, <Figure 3>처럼 일반적으로 기업별 상황(context)에 적합한 지침을 제공하는 ISO 31000을 참조한다[4].



<Figure 3> Risk-based thinking Process in ISO 9001 : 2015

2.4 리스크

새로운 기술 및 제품 개발, 사회와 환경 분야에서 일어나는 다양한 변화로 인해 각 분야에서 새롭고 다양한 유형의 리스크가 발생하고 있다. 이로 인해 리스크의 개념도 다양하게 변화되어 왔으며, 이와 관련한 중요한 몇 가지 국제표준에서의 정의를 <Table 1>에 정리하였다.

1999년 ISO/IEC GUIDE 51에서는 위험한 조건 또는 상황을 감소시키기 위해 리스크를 위해요인(hazard)과 관련된 것으로 간주하여, “위해요인의 발생 확률과 그 심각성의 결합”으로 정의하였다. 이 정의에서는 ISO 31000와는 다르게 리스크를 부정적인 개념으로 간주하였다.

<Table 1> Risk Concepts Defined in Core References

Standards	Definition
ISO/IEC GUIDE 51(1999)	Combination of the probability of occurrence of harm and the severity of that harm
ISO/IEC GUIDE 73(2002)	The combination of the probability of an event and its consequences
ISO GUIDE 73(2009) ISO 31000(2009) ISO 9001(2015)	Effect of uncertainty on objectives
ICH Q9(2005)	The combination of the probability of occurrence of harm and the severity of that harm(ISO/IEC Guide 51).

2002년 ISO/IEC GUIDE 73에서는 리스크를 잠재적인 위험한 사상과 유사한 것으로 간주하고, 리스크를 “사건의 발생 확률과 그 결과의 결합”으로 정의하였다. 이 정의에서는 리스크를 부정적인 것으로 여기지 않으며, 결과(consequence)가 부정 또는 긍정적 인지에 대해서는 언급하지 않았다. ISO 31000에서 언급된 리스크 개념은 조직의 목적(안전, 환경, 재정 등)은 불확실성에 따라 그 영향이 긍정 또는 부정적으로 나타날 수 있다고 보고 리스크를 “목적(목표)에 대한 불확실성의 영향”으로 정의하였다. 모든 사고를 예방하는 것은 불가능하기에 모든 사고의 발생을 막는 것보다 제어하기 위해 리스크를 확인 및 분석하기 위한 확률론적 접근방법을 이용하는 차원으로 접근한 것으로 이해된다. ISO 31000 리스크 개념의 접근방법을 따르는 ISO 9001 : 2015에서도 리스크를 불확실성으로부터 발생하는 목적에 대한 영향으로 이해한다. 마지막으로, 의료산업계 품질관리시스템의 국제표준인 ICH Q9에서 언급한 리스크도 ISO/IEC Guide 51에서처럼 리스크를 위해요인(hazard)과 관련된 것으로 간주하고, “위해요인(harm)의 발생 확률과 그 심각성의 결합”으로 정의하였다.

ISO 31000과 ISO 9001에서 리스크 정의에 사용되는 ‘불확실성’이라는 개념이 학자들에 따라 복잡하게 나뉘기도 한다. 리스크와 불확실성을 거의 동일하게 보기도 하고, 불확실성이 리스크에 포함된다고 주장하기도 하며, 반대로 리스크가 불확실성에 포함된다고 주장하기도 한다[8]. 이에 대해서 본 논문에서는 <Table 1>에서 살펴본 정의들의 공통된 의미에서 이해하여 미래에 대한 불확실성의 영향을 자료나 경험을 근거로 계량화한 것을 리스크로 해석, 리스크(R) = 불확실성의 영향 = 발생 확률(P) ×심각성(S)의 관계로 평가한다.

3. FMEA와 FTA

3.1 FMEA와 FTA의 특징

ISO 관련 시리즈의 표준에서는 리스크 관리를 위해 FMEA나 FTA 등 여러 가지의 다양한 신뢰성 분석 방법을 권고하고 있다. 제품의 결함분석을 위해 사용되는 대표적인 방법으로는 고장유형 및 영향분석(FMEA : failure mode and effect analysis), 결함트리분석(FTA : fault tree analysis), 사건트리 분석(ETA : event tree analysis) 등이 있다.

3.1.1 FTA

FTA는 확률론을 기반으로 하며, 고장 또는 결함이라는 사건발생 확률을 최소화하고자 하는 톱다운(top-down) 방식의 정량적 신뢰성 분석 방법이다. 부울 로직(Boolean logic)을 기반으로 상위의 사건발생으로 이어지는 사건발생의 고리(failure chain)를 이해하여 시스템이나 제품의 실패 확률을 줄이기 위한 최선의 조치를 파악하는 데 사용된다[11].

3.1.2 FMEA

FMEA는 제품(하드웨어, 소프트웨어)이나 시스템 설계 단계에서 발생할 수 있는 잠재적 고장(potential failure)을 사전에 파악, 제거하여 신뢰도를 제고하기 위한 정성적 신뢰성 분석 방법으로서, 모든 잠재적 고장유형(potential failure mode)을 파악하는 것으로 시작한다. 시스템이나 제품의 고장으로 인한 영향을 심각도(Severity), 발생도(Occurrence), 검출도(Detection) 3가지의 결합으로 평가한 RPN = S×O×D을 기준으로 리스크의 우선순위(RPN : risk priority number)를 결정, 조치를 취하는 bottom-up 방식이다.

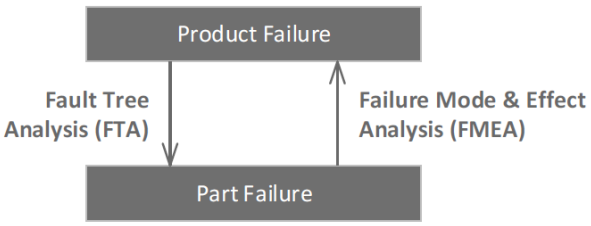
3.1.3 용어 설명

• 결함(fault) : 시스템이나 제품이 의도하지 않았거나 예기치 않은 상태로 작동되도록 하는 부품이나 시스템의 비정상적 상태를 의미한다. 이는 설계나 생산과정에서 내재된 문제점으로서 고장(failure)을 일으키는 원인이 된다. 결함은 시스템이나 제품에 표면적으로 나타나거나 잠재되어 있다가 여러 가지의 상황이 충족되면 고장을 발생시키게 된다.

• 고장(failure) : 시스템이나 제품이 지정된 요구조건 하에서 필요한 기능을 정상적으로 수행 할 수 없는 상태.

3.2 FTA와 FMEA 관계

FTA와 FMEA는 하나는 'top-down'의 정량적 분석방법이고, 다른 하나는 'bottom-up'으로 진행하는 정성적 분석방법으로서 각각이 갖고 있는 다른 절차와 특성으로 인해 개별적으로 적용되고 있지만, 두 가지의 특징을 살려서 상호 보완적으로 사용한다면 더 좋은 효과를 기대할 수 있다[10]. <Figure 4>는 FTA와 FMEA 간의 상호 보완적 관계를 보여준다[11].



<Figure 4> Relationship between FTA & FMEA

FTA 방법을 이용하여 제품에서 발생하는 고장이나 오류를 부품 단위에서의 결함(fault)으로 분석, 발생 확률을 근거하여 사건발생 고리를 확인할 수 있다. FTA에 의한 분석을 통해서 리스크의 발생 확률을 보다 구체적이고 객관적으로 평가할 수 있을 것이다. FMEA 방법은 확인된 사건발생 고리의 부품별 결함으로 인한 고장유형의 영향을 과거의 자료와 경험을 근거로 정성적으로 분석하기 위해 사용한다. FMEA 분석을 통해서는 리스크의 심각도를 체계적으로 평가할 수 있을 것이다.

3.3 FTA와 FMEA 통합 필요성

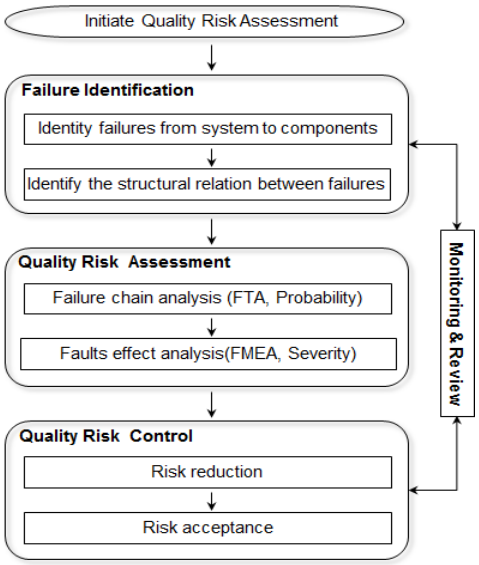
최근의 IT 네트워킹 기술 발달로 대부분의 제품들이 소프트웨어 기술과 융합되어 다양한 서비스를 사용하도록 하는 융합화가 빠르게 진행되는 추세이다. 소프트웨어 기술과 하드웨어 기술이 하나의 제품에 융합된 PSS 제품의 품질은 이전처럼 단순히 하드웨어 부분의 품질보증만으로는 달성하기가 어렵다. 이런 제품기술의 변화와 함께 제조물 공급자의 책임을 더욱 강화한 PL법의 지난 7월의 국회 통과로 인해 기업은 지속성장을 위해선 제품의 라이프 사이클 전체 기간 동안 품질을 보증할 수 있어야 한다. 이를 위해선 현재의 불량률 중심으로 이루어지는 품질관리와 함께 제품의 설계 단계 및 생산 과정에서 하드웨어와 소프트웨어 및 이들의 융합으로 인한 기능의 결함으로 인해 발생 가능한 품질 리스크를 체계적으로 진단할 수 있는 프로세스가 필요할 것이다.

FTA 방법에 의해 하드웨어의 고장이나 소프트웨어의 오류를 유발하는 결함이나 위해요인을 부품 단위에서의 사건발생 고리 파악을 통해서 찾아내고, 부품의 결함이나 위해요인들로 발생 가능한 고장 유형과 영향들을 과거

의 자료를 근거로 개발단계에서 통합적으로 평가할 수 있는 FTA- FMEA 통합 리스크 진단 프로세스가 융합제품의 품질경영시스템을 위해 필요하다고 판단된다.

4. 품질 리스크 진단 모델

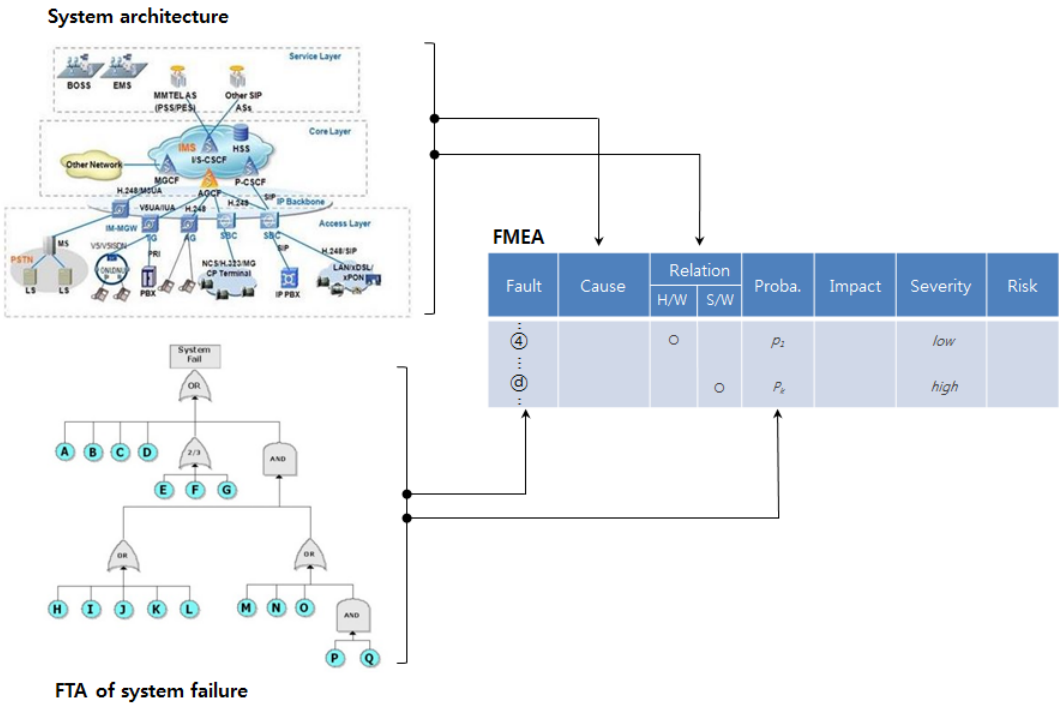
앞에서 살펴본 것처럼 리스크란 심각도와 발생확률 두 가지 핵심요소에 의해 평가한다. 고장(failure)이란 결함요인들이 발생할 수 있는 여건이 충족되는 사건이 발생하는 상황에서 일어난다. 따라서, 고장의 발생확률은 결함에 의해 고장원인을 분석하는 FTA 방법으로 평가하는 것이 적합하다. 심각도는 그 실패나 고장이 시스템의 목적에 미치는 영향과 다른 부분에 미치는 파급효과 등을 종합적으로 고려하여 평가해야 한다. 본 논문에서 제안하는 품질 리스크 진단을 위한 절차와 모델은 <Figure 5>, <Figure 6>과 같다.



<Figure 5> Risk Assessment Process

문제가 되는 고장으로 인한 품질 리스크의 진단은 <Figure 6>처럼 FMEA를 기준으로 진행한다. 리스크의 두 가지 요소 중 하나인 발생확률을 기존의 FMEA 방법에서는 1~10까지의 범주형 값으로 평가한다. 본 논문에서는 부울대수 규칙(Boolean algebra rule)을 적용하여 결정되는 최소절단집합(minimal cut sets) FTA의 고장결함(fault) 각각에 대하여 품질관리를 통해 파악된 불량률 자료로 평가한다.

심각도는 원인(cause)으로 인한 영향(impact)의 정도에 대한 평가다. 결함의 원인이 다른 부분의 기능에 미치는 파급효과 등을 종합적으로 고려하기 위해서는 결함이 시스템의 어느 부분에서 발생하는지, 하드웨어와 소프트웨어 어느 부분과 관련된 결함인지를 고려해야한다. 이를 위해 본 논문의 리스크 진단 모델에서는 FMEA에 의한 리스크 평가 시, 원인이 시스템 구조의 어느 부분에 위치하는지를 알 수 있도록 하였으며, 하드웨어와 소프트웨어 중 어느 부분의 결함인지가 고려되도록 하였다.



<Figure 6> FTA-FMEA based Quality Risk Assessment Model

4.1 잠재적 고장유형 확인(Failure Identification)

FTA와 FMEA 분석은 결함이나 고장이 부품과 이들의 기능과 밀접하게 관련되기 때문에 제품이나 시스템 설계 후에 진행되어야 한다. 이는 FTA와 FMEA 방법에 의한 품질 리스크 분석이 설계나 요구사항 분석 과정에서 작성되는 잠재적 고장유형(failure identification) 목록을 기초하여 이루어지기 때문이다. 파악된 고장유형들 중 제품 또는 시스템의 품질에 특별하게 위해한 핵심적인 위해요인과 치명적 고장유형을 파악해야 한다. 본 논문에서는 단계별 설명을 위해 지능형정보시스템(ITS : intelligent transportation system)의 기능 중 하나인 신호등 상황에 따른 적정 운행속도를 제시하는 기능(ODSA : optimized driving speed advisory)을 사례로 택하여 설명하며, ODSA 시스템의 구조와 각각의 기능은 <Figure 7>과 같다[11].

4.2 품질 리스크 진단(Quality Risk Assessment)

4.2.1 FTA에 의한 사건발생 고리 확인

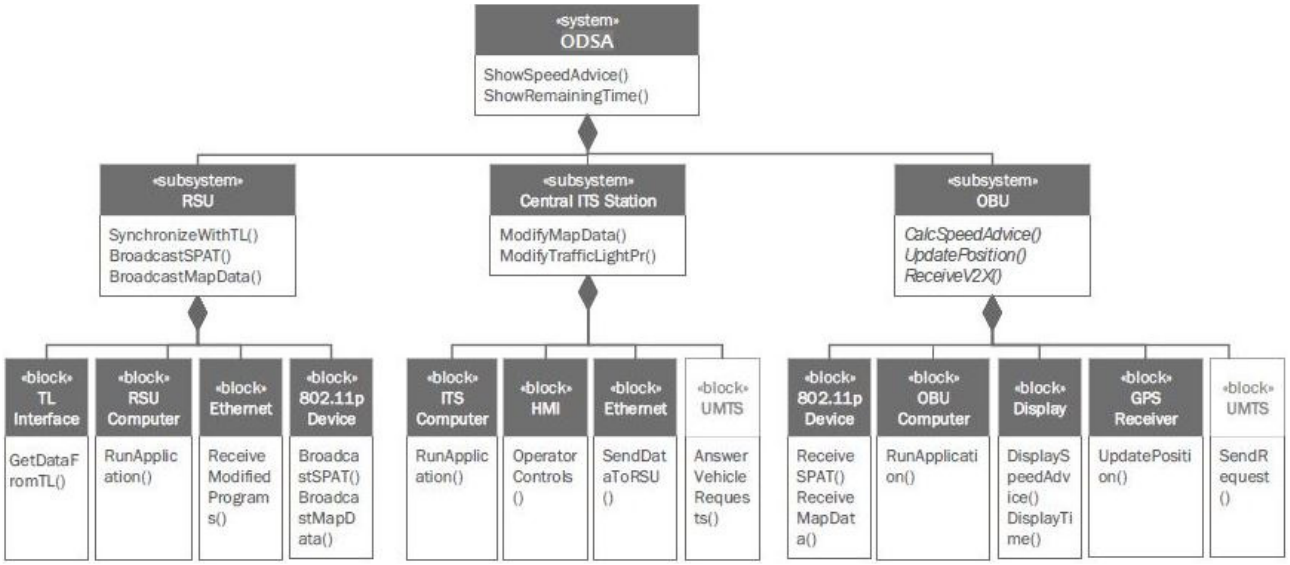
FTA 분석에 의해 상위사건(top event)을 일으키는 결함들의 결합정보와 메카니즘 즉 사건발생의 고리를 확인하고, 부울대수 규칙을 적용하여 상위사건에 해당되는 고장을 일으키는 유일한 사건집합인 절단집합을 확인하게 된다. 실패유형 중 영향이 큰 속도정보오류(wrong speed advice display)를 상위사건으로 선정하였다.

FTA 분석을 위해서는 다음 사항들을 사전에 결정해야 한다.

① 고장유형 가운데 FTA에 의해 분석해야 할 사건(top event)을 정한다 : FTA의 대상 결정
② 분석할 시스템의 범위를 정한다 : FTA의 범위 결정
③ 분석에서 고려해야 하는 인과관계 사건(causal events)을 정의한다. FTA의 분석 수준 결정
④ 분석 시스템의 초기상태를 정의한다.

ITS는 하드웨어와 소프트웨어가 밀접하게 결합된 시스템이기 때문에 FTA 분석을 통해 파악된 결함들도 그것이 하드웨어나 소프트웨어와 어떻게 관련되어 있는지를 구분하여 해석한다. 이를 위해 각 결함들이 시스템 구조의 어느 부분과 관련된 결함인지 나타내는 'Related ID'를 표기한다. 이는 하나의 고장이나 오류가 다른 오류나 고장과 연관되어질 수 있으며, 모든 결함은 다른 결함을 유발할 수 있거나 자체적으로 유발 될 수 있기 때문이다. 이를 통해 각 결함의 발생확률을 보다 정확하게 평가할 수 있을 것이며, 발생확률을 정량적으로 평가하기 위해서는 불량률이나 오류율이 결함단위 수준까지 관리되어야 한다.

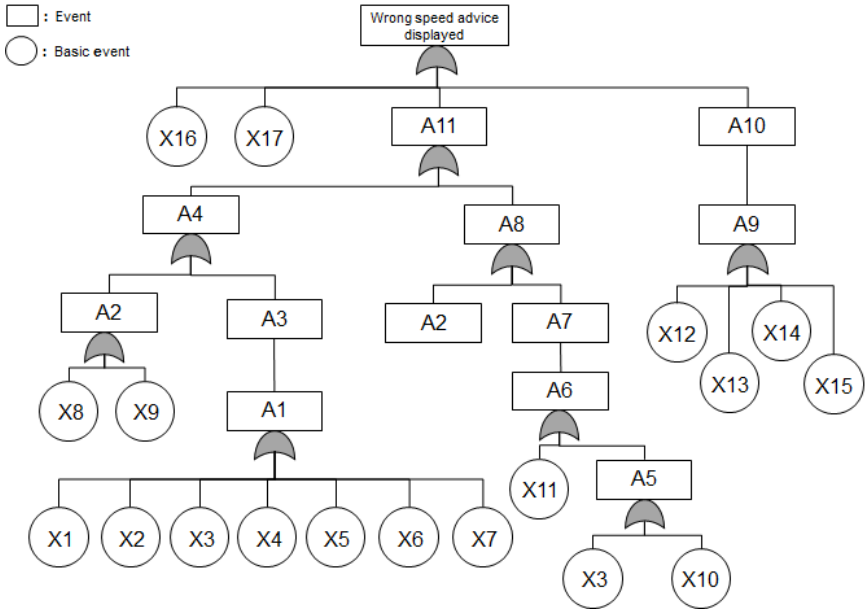
<Table 2>는 ODSA의 구성요소별 발생 가능한 실패유형을 정리한 것이며, 실패유형 중 속도정보 오류의 결과가 매우 치명적이어서 상위사건으로 선정하였다. 속도정보 오류에 대한 부울대수 규칙을 적용한 최종 FTA는 <Figure 8>과 같으며, FTA의 기본사건(basic event)과 기본사건들의 'AND' 또는 'OR' 관계로 결합되는 사건(event) 들에 대한 설명은 <Table 3>에 정리하였다. 이 결과를 근거로 상위사건의 고장을 해결하기 위해 반드시 해결되어야 하는 근원적 결함들의 발생 가능성과 이를 통한 상위사건의 발생 가능성을 확률로서 평가한다.



<Figure 7> Architecture and Functions of ODSA

<Table 2> Failure Modes in the System Elements of ODSA

System Element			Function	Failures
Name		ID		
System		OD	ShowSpeedAdvice() ShowRemainingTime()	• System does not work properly
Subsystem *means the subsystem in <Figure 7>	RSU(Road Side Unit)	R	SynchronizeWithTL() BroadcastSPAT() BroadcastMapData()	• SPAT/MapData wrong (SPAT : Signal Phase and Timing) • Broadcast failure
	Central ITS(Intelligent Transportation Systems) Station	C	ModifyMapData() ModifyTrafficLightPr()	• Modification error
	OBU(On-Board Unit)	O	CalcSpeedAdvice() UpdatePosition() ReceiveV2X()	**• No SpeedAdvice displayed**
Block *means the block in <Figure 7>	TLI(Traffic Light Interface)	R1	GetDataFromTL()	• Fail to connect • Wrong data • Emergency not detected
	RSU computer	R2	RunApplication()	• System frozen • Unit broken • Time not synchronized
	Ethernet(at RSU)	R3	ReceiModifiedPro()	• Fail to connect • Packet error/loss/delayed
	802.11p device(at RSU)	R4	BroadcastSPAT() BroadcastMapData()	• Fail to send data
	ITS computer	C1	RunApplication()	• Unit broken • System frozen
	HMI(Human-Machine Interface)	C2	OperatorControls()	• System frozen • Unit broken • Wrong operator input
	Ethernet(at ITS)	C3	SendDataToRSU()	• Fail to connect • Packet error/loss/delayed
	802.11p device(at OBU)	C4	ReceiveSPAT() ReceiveMapData()	• Fail to connect • Packet error/loss/delayed
	OBU computer	O1	RunApplication()	• System frozen • Unit broken • Time not synchronized
	Display	O2	DisplaySpeedAdvice() DisplayTime()	• Fail to connect • Driver does not see/watch/react
	GPS Receiver	O3	UpdatePosition()	• No reception • Unit broken • Wrong or unsteady position



<Figure 8> Fault Tree Analysis of wrong Speed Advice Display

4.2.2 FMEA에 의한 리스크 평가

상위사건에 대한 FTA 분석 결과를 정리한 <Table 3>의 내용을 토대로 <Table 4>와 같이 FMEA 평가를 실시한다. FMEA 평가 시, 각각의 결함에 대한 리스크를 평가할 때 'Related ID'를 고려함으로서 결함의 원인(cause)이 시스템 구조의 어느 부분과 관련되어 있는지를 고려하여 평가할 수 있으며, 결함의 원인이 하드웨어와 소프트웨어 요인 중 어느 부분과 관련되는지를 고려함으로 인해서 PSS 제품의 특징을 고려한 리스크 분석이 가능할 것이다. 기존의 FMEA 분석에서는 발생확률을 범주형 값으로 평가하였으나, 본 논문에서는 품질관리 과정에서 파악된 실제의 불량률로서 발생확률을 평가한다. 이것이 실제로 이루어지기 위해서는 불량의 원인들이 FTA의 기본단위가 되어서 품질관리가 이루어져야 할 것이며, 소프트웨어의 불량률도 관리되어져야 할 것이다. 본 논문에서는 앞에서 살펴본 정의들의 공통된 의미를 근거로 상위사건인 고장유형의 리스크를 발생확률×심각도로 평가하며, 심각도는 정량평가의 한계로 인해 기존처럼 범주형 값을 이용한 정성평가를 한다. 심각도에 대한 범주값은 다양한 기준을 사용하나, 본 논문에서는 5등급(Very High = 5, High = 4, Medium = 3, Low = 2, Very Low = 1) 척도로 심각도를 평가한다. 즉, 심각도는 발생확률에 반영되는 가중치로서의 의미를 갖는다.

<Table 3> Events and Basic Events in wrong Speed Advice Display

Event	Fault mode	Related ID	Component fault	Basic event	Source	
					H/W	S/W
A1	Traffic light interface failure	R1	Remaining time(s) wrong	X1		○
			State(s) wrong	X2		○
			Lane no.(s) wrong	X3		○
			Time stamp wrong	X4		○
			Phase time(s) wrong	X5	○	
			IntersectionID wrong	X6	○	
			Intersect. status wrong	X7		○
A2	Communication channel problem	C	Delayed packet	X8	○	
			Bit error	X9	○	
A3	RSU problem	R	Traffic light data failure	A1		
A4	SPAT message problem	R	Communication channel problem	A2		
			RSU problem	A3		
A5	Approach(es) wrong	R4/O1	Lane no. wrong	X3	○	
			Position offset wrong	X10	○	
A6	MapData problem	R4/O1	Reference point wrong	X11	○	
			Approach(es) wrong	A5		
A7	RSU problem	R	MapData problem	A6		
A8	MapData message problem	R	Communication channel problem	A2		
			RSU problem	A7		
A9	GPS-Receiver problem	O4	Delayed	X12	○	
			Heading wrong	X13	○	
			Speed wrong	X14	○	
			Position wrong	X15	○	
A10	Position failure	O4	GPS-Receiver problem	A9		
A11	Traffic light data failure	C	SPAT message problem	A4		
			MapData message problem	A8		
			Calculation error	X16	○	
			Time/Clock failure	X17	○	

<Table 4> Risk assessment for the failure

Fault		Cause	Relation		Probability	Impact	Severity	Risk
Mode	Related ID		H/W	S/W				
X1	R1	TL does not change timing		○	*p1*	wrong speed advice	5	*p1 × 5*
		TL has no emergency info.	○	○	*p2*	wrong speed advice	4	*p2 × 4*
.....	.....	.....	.....	.....	.....	.....	.....	.....
A10	O4	Unit broken	○		*pk*	no speed advice	4	*pk × 4*
		Internal part failure	○		*pk+1*	no speed advice	4	*pk+1 × 4*
.....	.....	.....	.....	.....	.....	.....	.....	.....

4.3 품질 리스크 관리(Quality Risk Control)

FMEA에 의해 리스크를 평가해서 우선순위만을 정하는 것이 목적이 아니라 사전에 결함을 발견할 수 있는 방법을 강구하는 것이 품질 리스크 진단 모델의 목적이다. 이 단계에서는 리스크 분석을 통해 제품이나 시스템의 결함을 예방(prevent)하거나 제거(remove)할 수 있어야 하고, 그렇지 못한 경우에는 이런 결함을 발견할 수 있는 방법을 강구해야만 한다.

5. 결 론

개발과 생산비용 절감을 위해 적극 추진한 부품 공용화는 dimension이 다른 제품들에 동일한 부품을 채용하는 상황으로 인해 품질의 신뢰성 문제를 야기할 수도 있다. 또한, 부품 공용화는 한 부품이 잘못되면 그 부품을 채택한 여러 제품에서 품질문제가 동시에 발생할 수밖에 없는 상황을 초래하게 된다. 이와 더불어 전자부품의 비중이 35% 정도인 현재의 자동차가 무인자동차가 되면 정보통신 기술의 비중이 82%까지 차지한다고 한다. 전자부품의 경우에는 기계적 결함과 달리 사고가 나도 재현하거나 원인 입증이 어렵다.

제품기술의 패러다임 변화로 제품 리콜은 계속 증가할 수밖에 없는 상황이며 더하여 강화된 PL법 시행으로 인해 제품을 생산 판매하는 제조 기업이 갖는 리스크도 갈수록 커지고 있다. 따라서, 기업은 단순히 품질을 불량률 관점에서 관리하는 수준을 넘어서 리스크 관점에서 접근, 평가하고 관리해야 할 것이다. 이러한 상황에 대처하기 위한 방안으로 본 논문에서는 품질 리스크 진단 모델을 제안하였다. 제안한 FTA-FMEA 통합 리스크 진단 모델은 결함요인들에 대해 시스템 구조 특성을 하드웨어와 소프트웨어와의 관련성 차원에서 고려하며, 품질 문제를 단순히 불량률로 평가하고 관리하는 차원에서 더 나아가 리스크로 인식, 관리하는 진단 모델이다. 제안한 리스크 진단 모델을 통해 융합제품의 리스크를 제품의 구조적 특성과 결함의 원인을 하드웨어와 소프트웨어를 같이 고려하여 평가하기 때문에 PSS 제품의 품질 리스크 진단에 보다 효과적일 것으로 기대된다.

Acknowledgement

This study was supported by 2015 Research Grant from Kangwon National University(No. 201510023).

References

[1] Aqlan, F. and Ali, E.M., Integrating lean principles and fuzzy bow-tie analysis for risk assessment in chemical industry, *Journal of Loss Prevention in the Process Industries*, 2014, Vol. 29, pp. 39-48.

[2] Byun, S.N. and Dong, H.L., Implementation of Quality Management Policy and ISO 9000 Series under Product Liability Law, *Journal of The Korean Society for Quality Management*, 1998, Vol. 26, No. 1, pp. 27-47.

[3] ICH Expert Working Group, Quality Risk Management Q9, 2005, https://www.ich.org/fileadmin/Public Web Site/ICHProducts/Guide lines/Quality/Q9/Step4/Q9Guide line.pdf.

[4] International Organization for Standardization, Implementation Guidance for ISO 9001 : 2015, 2015, https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/iso-2015-how to use it.pdf.

[5] International Organization for Standardization, ISO 31000 Risk management, 2015, https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/iso 31000 for smes.pdf.

[6] Jang, J.S., Toyota recalls and industrial engineering lessons, *IE Magazine*, 2010, Vol. 17, No. 1, pp. 28-33.

[7] Jin, E.J., Kim, M.H., and Park, M.G., An Integrative Method of Fault Tree Analysis and Fault Modes and Effect Analysis for Security Evaluation of e-Teaching and Learning System, *Korea Information Processing Society Review*, 2013, Vol. 2, No. 1, pp. 7-18.

[8] Kim, J.H. and Park, D.J., A Study on the Review of Risk Concepts, *Journal of the Korean Society of Safety*, 2013, Vol. 28, No. 6, pp. 90-96.

[9] Kim, M.H., Jin, E.J., and Park, M.G., Fault Tree Analysis and Fault Modes and Effect Analysis for Security Evaluation of IC Card Payment Systems, *Journal of Korea Multimedia Society*, 2013, Vol. 16, No. 1, pp. 87-99.

[10] Lee, S.K., Kim, J.U., and Koo, J.S., Risk Assessment for Pneumatic Braking of EMU, *Journal of the Korean Society of Safety*, 2015, Vol. 30, No. 5, pp. 114-122.

[11] Nagel, C.E., Design and Failure Mode and Effects Analysis of a Vehicular Speed Advisory System, [Master's Thesis], Hamburg University of Technology, 2015.

[12] Park, D.J., Empirical Analysis for Evaluation Index of Quality Competitiveness Excellent Companies, *Journal of Society of Korea Industrial and Systems Engineering*,

2016, Vol. 39, No. 1, pp. 37-46.

[13] Park, D.J., Kim, H.G., and Yun, W.Y., Research Trend and Futher of ISO 9000 Quality Management System : Literature Review, *Journal of The Korean Society for Quality Management*, 2007, Vol. 35, No. 3, pp. 1-16.

ORCID

Hyung Sool Oh | http://orcid.org/0000-0001-6341-8007