J. Korea Saf. Manag. Sci. Vol. 15 No. 3 September 2013
http://dx.doi.org/10.12812/ksms.2013.15.3.105

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

기능안전 표준들의 구현을 위한 기능 중심의 위험원 식별 방법

정 호 전* · 이 재 천* · 오 성 근**
*아주대학교 시스템공학과 · **전자공학과

On the Hazard Identification Methods for the Realization of Functional Safety Standards

Ho Jeon Jung* · Jae Chon Lee* · Seong Keun Oh**
*Dept. of Systems Engineering, Ajou University
**Dept. of Electrical & Computer Engineering, Ajou University

Abstract

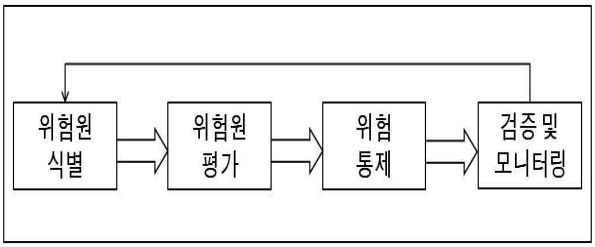
To meet the growing needs from a variety of stakeholders, the development of modern systems is getting more complex and thus, the systems failure in the actual operations can potentially become more serious. This is why several international or military standards on systems safety have been published. In spite of the importance of meeting those standards such as IEC 61508 and ISO 26262 in the systems development, the associated practical methods seem deficient since those standards do not provide them. The objective of this paper is to present a method to identify potential hazards in fulfilling the requirements of the safety standards. In particular, the approach taken here is based on applying the functional analysis that covers several levels of the system under development. Note, however, that in the most of the conventional methods for hazards identification, the analysis has been focused on the failure at or underneath the component level of the system. The hazards identification method in this paper would cover the level up to the system by utilizing the functions-oriented approach. The case study of the safety enhancement for locomotive cabs is also discussed.
Keywords : Safety, Hazard Analysis, Systems Engineering, Function Analysis, IEC 61508

1. 서론

현대의 안전중시 시스템들은 과거와 비교해서 급격한 운영성능의 발전을 가져 왔고, 동시에 기능적으로도 매우 복잡해지게 되었다. 시스템이 점차 대형화 복잡화 됨으로써, 시스템에서 발생할 수 있는 사고나 고장의 위험 또한 증가하고 있다. 특히 이런 안전중시 시스템들은 사고나 고장이 인명 및 재산피해로 직결되기 때문에 체계적인 안전관리가 필요하다. 이에 따라 국방, 철도, 항공, 해양, 원자력 등의 안전이 중시되는 산업분야에서는 안전과 관련한 표준규격을 제정하고 이를 준수하도록 권장하고 있다. 또한 현대의 시스템에서 전기전자 및 소프트웨어의 비중이 높아지면서 전기전자 기능안전성 규격(IEC 61508)이 제정되어 현대시스템의 안전에 관한 규격을 제시하고 있다.

† 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, Wonchon-dong, Yeongtong-gu, Suwon, 443-749, Tel: 031-219-3941, E-mail: jaelee@ajou.ac.kr
Received July 19, 2013; Revision Received September 5, 2013; Accepted September 16, 2013

이와 같이 안전은 여러 산업분야의 시스템 개발에 있어서 반드시 확보해야 할 필수 요소가 되었으며, 이를 위한 투자가 활발히 이뤄지고 있다.



<Figure 1> Procedure model for hazard analysis.

이처럼 중요시되고 있는 안전의 확보를 위해 제시되고 있는 많은 표준규격에서 안전을 위한 첫걸음으로 제시하고 있는 것이 잠재위험 분석(Hazard Analysis) 과정이다. 잠재위험 분석은 시스템에 내재되어 있는 잠재위험들을 식별하고, 향후 잠재위험에 의해 발현될 위험들을 미리 예상하고 평가하여, 이에 대응을 수립하는 것을 포함하는 과정이다. 안전관련 표준에서는 잠재위험 분석을 시스템 개발의 초기에 수행함으로써 목표로 하는 안전수준에 도달 할 수 있다고 제시하고 있다. 그러나 참고문헌[1][2]에서 제시하고 있는 현재의 잠재위험 분석 과정을 살펴보면, 잠재위험 분석이 부품 및 장치 수준을 중심으로 이뤄지고 있음을 알 수 있다. 이는 물리적인 부품 및 장치로 인한 잠재위험의 식별 및 위험평가가 현재 잠재위험 분석의 주요 목표라는 것을 반영하고 있는 것이다. 하지만 현대의 시스템에는 전기, 전자 장치 및 소프트웨어의 비중이 높아지고 있다. 특히 안전과 밀접한 관련이 있는 제어시스템에서 더욱 전기, 전자 장치의 비중이 커지고 있다. 그러나 현재의 부품 및 장치 중심의 잠재위험 분석은 전기, 전자 장치 및 소프트웨어에 대한 적절한 접근 방법이 아니다. IEC 61508, ISO26262등의 기능안전 표준에서 제시하고 있듯이 기능중심의 잠재위험 분석이 전기, 전자 장치에 대한 적절한 잠재위험 분석 방법이라 할 수 있다. 따라서 고장데이터 또는 전문가들의 경험을 통한 잠재위험 분석이 아닌 시스템에 대한 기능분석을 통한 잠재위험 분석이 필요하다. 이를 통해 전문가의 경험을 바탕으로 한 위험원의 식별과 더불어 체계적인 프로세스를 거친 요구사항의 분석과 기능의 식별과정을 통해 이루어지는 위험원의 식별 및 분석이 더해진다면 기존의 위험원 분석에서 발생할 수 있는 누락의 위험을 더욱 줄이고 이는 곧 더욱 견고한 위험도관리로 이어질 수 있다.

이러한 기능 중심의 잠재위험 분석을 위한 연구가 진행되고 있다. 참고문헌[3]을 통해서 위험 분석을 위한 시스템공학적 접근 방법을 제시하고 있다. 시스템 공학 프로세스인 요구사항 분석, 기능분석을 통한 잠재위험의 식별을 참고문헌[3]에서 제시하고 있다. 참고문헌[3]에서제시하고 있는 방법은 시스템에 대한 요구사항을 분석하고, 각 요구사항을 구현하기 위한 모든 기능을 식별한다. 식별된 모든 기능들에 대해서 각 기능들이 오류를 일으킬 경우를 위험으로 정의하고 있다. 그러나 참고문헌[3]의 연구내용은 요구사항의 분류, 각 요구사항을 통해 도출할 수 있는 기능의 형태에 대해서만 제시하고 있으며, 이를 바탕으로 단순히 식별된 기능들을 나열한 수준에 그치고 있다. 따라서 단순히 기능을 식별하여 나열하는 것이 아니라 기능을 구조적으로 분석하여 잠재위험을 식별함으로써 하나의 기능이 다른 기능에도 영향을 미칠 수 있다는 것을 파악할 수 있을 것이다. 또한 상위수준인 시스템 수준에서부터 체계적으로 기능을 식별함으로써 단순히 부품, 장치수준에서의 위험이 아닌 시스템 수준에서의 위험의 대응이 가능 하다. 따라서 본 논문에서는 상위수준에서부터 Top-down 접근을 통한 기능분석을 수행하고 이를 바탕으로 잠재위험의 식별을 수행하여 시스템 수준에서의 잠재위험 분석이 가능하도록 노력하였다.

본 논문의 구성은 다음과 같다. 서론에서는 사회 및 연구의 연구동향과 필요성을 제시하였고, 2장에서는 관련 선행연구 및 연구 목표를 기술하여 문제정의를 했다. 3장에서는 기능중심의 잠재위험 분석을 위한 절차를 제시한다. 4장에서는 3장의 활동을 바탕으로 도출된 잠재위험 분석절차에 따른 철도차량 운전실에 대한 잠재위험 분석 사례를 제시하였다. 5장에서는 본 논문의 결과를 정리 및 요약 하였다.

2. 문제 정의

<Table 1> Safety activity according to the system life-cycle [4].

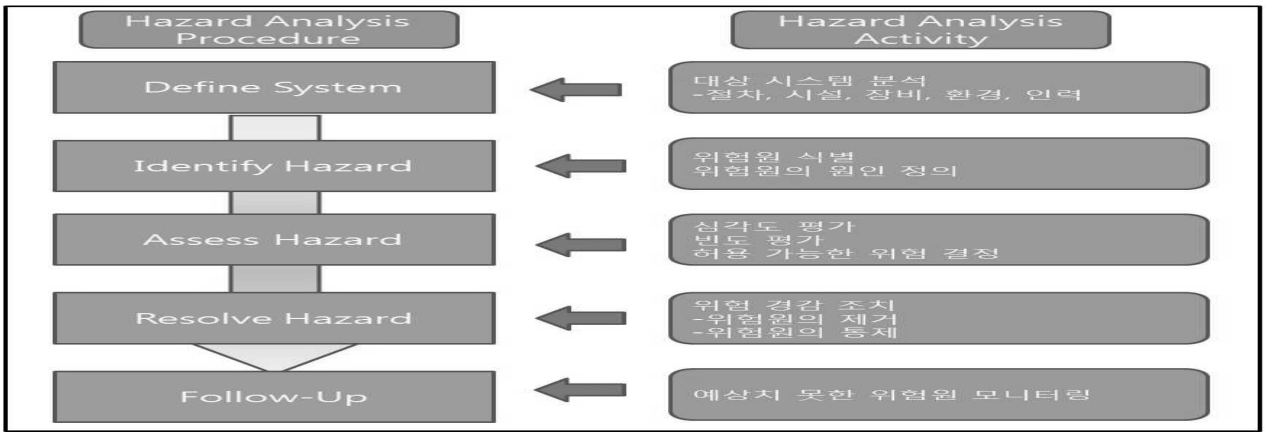
시스템 수명주기	안전성 활동
개념 시스템 정의	시스템 정의
	잠재위험 도출
리스크 분석 시스템 요구사항 도출	리스크 분석
시스템 요구사항 할당	잠재위험 원인 분석 및 추가 잠재위험 확인
	하부시스템 안전성 요구사항 할당
설계 및 구현 제작	설계&제작
시스템 검증 시스템 인수	안전성 입증

2.1 시스템 개발에서 잠재위험 분석의 중요성

국제규격에서 정의하는 안전성 활동은 개발되는 시스템에 내재하고 있는 잠재적 잠재위험을 찾아 제거하거나 잠재위험으로 발생하는 위험을 허용수준 이하로 줄일 수 있도록 대책을 수립하는 것이다. 또한 이를 시스템의설계 및 개발에 반영하도록 하는 모든 일련의 활동을 의미한다. 이러한 잠재위험 관리 측면에서의 안전성 활동 과정은 <Figure 1>과 같다. 즉, 시스템의 안전성 활동은 위험원 도출, 잠재위험 평가, 잠재위험으로 인한 위험을 허용 가능한 수준으로 관리하기 위한 위험통제, 모니터링 및 확인 과정이 필요하다. 이러한 절차는 각 단계가 항상 피드백 되어 잠재위험이 도출, 위험이 허용 가능한 수준이 되도록 제어하고 검증 될 때까지 반복적으로 수행되도록 표준에서는 제시되고 있다.

<Table 1>은 안전관련 표준인 IEC 62278에서 제시된 시스템 수명주기에 따른 안전 활동을 나타낸 것이다.

이와 같이 안전관련 표준들에서는 시스템의 개발에 따라 안전 활동을 수행하여 안전의 확보를 달성 할 수 있도록 제안하고 있다. 더불어 이러한 안전 활동의 핵심이자 첫 단계로써 잠재위험 분석단계를 제시하고 있다. 따라서 시스템의 안전의 확보를 위해서는 대상 시스템에 대한 체계적인 잠재위험 분석이 매우 중요하다.



<Figure 2> Model for hazard analysis procedure with corresponding hazard analysis activity.

2.2 기능 중심의 잠재위험 분석의 필요성 및 접근 방법

앞 절에서 제시한 것처럼 시스템의 개발에 있어서 안전의 확보를 위해서는 잠재위험 분석의 수행이 매우 중요하다. 현재의 잠재위험 분석 절차는 <Figure 2>와 같다. 그러나 현재의 잠재위험 식별 기법들은 시스템의 하부수준인 부품 및 장치수준에서의 잠재위험 식별에 치중되고 있다. 하지만 ISO26262와 같은 안전표준에서는 시스템 수준에서의 잠재위험의 식별을 수행하도록 명시하고 있다. 부품 및 장치수준에서는 FMEA와 같은 잠재위험 식별 기법의 적용에 대한 많은 연구와 사례들이 존재하여 이전의 유사시스템 등의 사례에 따라 쉽게 수행 할 수 있다. 그러나 현재의 위험원 분석 기법들은 새로운 시스템의 개발 또는 유사시스템의 개발이 이뤄질 때 설계 및 개발에 있어서 이전 시스템과의 차이점을 반영한 위험원 식별 및 분석이 이뤄지지 못하고 위험원의 누락이 발생할 위험이 있다. 이를 보완하기 위해 사용자의 필요에서 시작하여 요구사항의 분석 및 검증, 도출된 요구사항을 구현하기 위한 기능의 식별 및 검증과 같은 체계적인 프로세스를 거쳐 이뤄지는 기능 중심의 위험원 분석을 이전의 위험원 분석 기법의 단점을 보완하기 위해 제시하고자 한다.

또한 이제까지 실제 산업분야에서는 장치 및 부품 수준에서의 잠재위험 식별만을 수행해 왔고, 그것을 종합 한 것을 시스템수준에서의 잠재위험 식별이라고 제시하고 있는 수준이다. 즉 시스템 수준에서의 잠재위험 식별은 아직 어떻게 수행해야 할지에 대한 연구가 부족하며 실제 사례 또한 거의 존재하지 않는다. 따라서 이러한 시스템 수준에서의 잠재위험 식별을 위한 시스템 공학적 접근 방법이 필요하다. 시스템에 대해 체계적인 분석을 통하여 상위수준부터 하위수준까지의 잠재위험 식별이 가능하도록 한다. 시스템 공학 프로세스인 요구사항 분석과 기능분석을 수행함으로써 대상 시스템에 대한 체계적인 분석이 가능하다. 이를 바탕으로 상위수준에서부터 Top-down 접근을 통한 잠재위험 식별이 가능 하다.

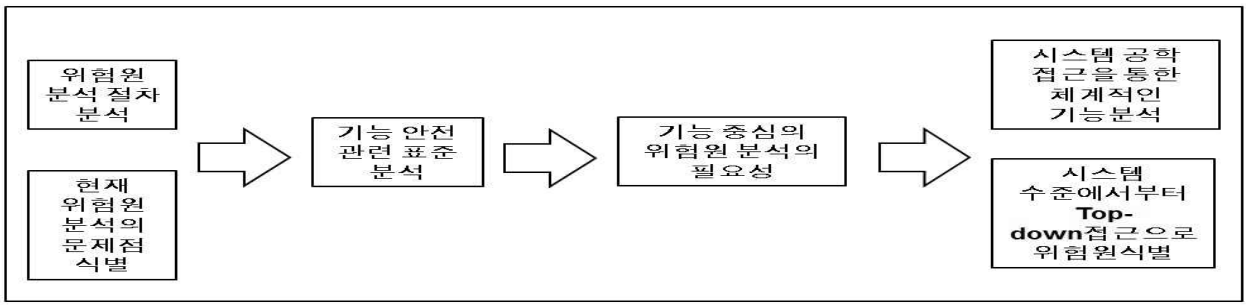
2.3. 연구 목표 및 범위

상위 선행연구 분석을 통해 안전 확보를 위한 잠재위험 분석단계의 중요성에 대해서 인지하였다. 또한 현재의 잠재위험 분석의 문제점을 분석하여 기능중심의 잠재위험 분석의 필요성에 대해서 제시하였다. 이를 위해 시스템 공학 기반의 잠재위험 분석의 필요성을 제시하 였다. 이에 따라 시스템의 상위수준에서부터 체계적인 잠재위험 식별을 수행하는 것이 본 논문의 연구 목표라 할 수 있다. 즉 본 논문에서는 철도차량의 운전실에 대해 현재 중요성이 점차 강조되고 있는 기능안전의 달성을 위해 기능중심의 잠재위험 분석을 수행하고자하며 이를 위해 시스템 공학적 접근을 통한 체계적인 기능 분석을 수행한다. 이를 바탕으로 구조화된 기능 식별을 통해 개별 기능의 오류로 인한 위험뿐만 아니라 기능간의 상호작용에 의한 위험 또한 식별하여 대응 할 수 있도록 한다. 본 논문에서 제시하고 있는 연구 개념은 <Figure 3>과 같다.

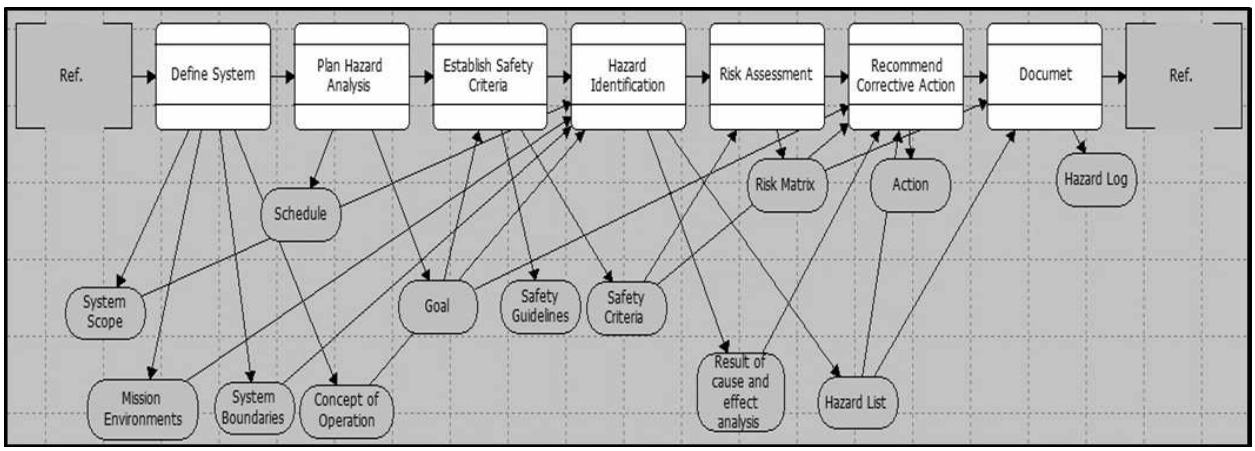
3. 시스템공학 기반의 잠재위험 분석 방법

3.1. 잠재위험 분석 절차 및 활동

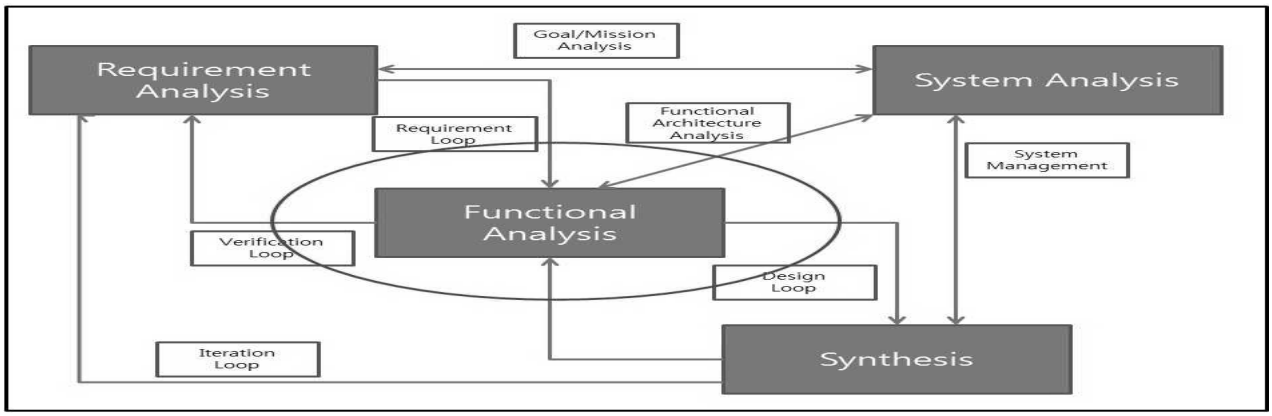
잠재위험 분석 단계는 안전관리에서 위험관리 단계에서 수행된다. 안전관리의 목적은 안전을 확보하는 것이고, 이는 위험을 허용 가능한 범위 내에서 통제하는 것을 의미한다. 따라서 안전관리에서는 위험관리단계를 포함하고 있다. 그리고 위험관리 단계에서 사고 및 고장의 근본 원인인 잠재위험을 식별하고 분석하는 단계를 포함하며 이것이 바로 잠재위험 분석단계이다. 잠재위험 분석 단계는 대상 시스템을 정의 및 분석하는 것에서 시작한다. 이 후 잠재위험을 식별하고, 식별된 잠재위험을 평가하는 과정을 거친다. 잠재위험 평가 결과를 바탕으로 잠재위험에 의해 발현될 위험을 평가하고 통제하는 단계를 거치며, 잠재위험 분석에 대한 검증 및 모니터링 과정을 포함한다[6][7]. 잠재위험 분석 절차 및 활동은 <Figure 2>와 같다. 제시된 잠재위험 분석절차와 더불어 잠재위험 분석과정을 통해 만들어지는 산출물들을 식별하여 잠재위험 분석에 프로세스 모델을 <Figure 4>와 같이 제시했다. 잠재위험 분석 프로세스 모델을 통해 세부 활동들에 필요한 데이터와 활동을 통해 도출되는 데이터들을 식별 하였다.



<Figure 3> Concept model for current research.



<Figure 4> Hazard analysis process model.



<Figure 5> Systems Engineering Process[5].

3.2. 시스템공학적 접근을 통한 체계적인 기능분석의 수행방법

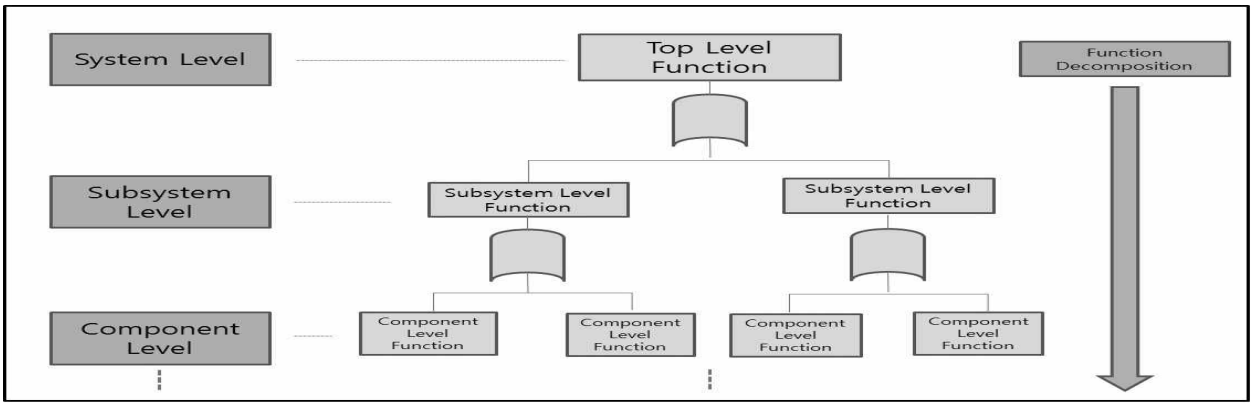
참고문헌[3]과 같이 기능분석을 통한 잠재위험 분석의 시도는 있었다. 참고문헌[3]는 시스템공학적 접근을 통해 대상 시스템에 대한 요구사항 분석 및 기능분석을 수행했다고 주장했다. 그러나 요구사항 분석은 요구사항 분석을 통해 도출될 수 있는 요구사항들에 대한 분류 수준을 제시하였다. 또한 기능분석의 경우에도 분류한 요구사항을 통해 식별되는 기능의 분류를 정의하고 있는 수준이다.

이는 부품 및 장치 수준에서 개별 부품 및 장치에 대해서만 잠재위험 분석을 수행하는 기존의 방법에 대한 개선을 제시하지 못하고 있다고 볼 수 있다. 기능의 식별을 통한 잠재위험 분석의 접근은 기능안전을 위한 잠재위험 분석의 수행이라 할 수 있지만 결과적으로 하위수준의 개별 기능의 분류 및 식별만을 수행하여 기능들 간의 상호작용으로 이한 잠재위험은 식별하지 못하고 있다. 따라서 시스템공학적 접근을 통해 시스템 수준에서부터 Top-down 측면의 기능분석이 필요하다. 이를 통해 구조화된 기능식별이 이뤄지며 하위수준의 개별 기능의 오류로 인한 잠재위험의 식별뿐만 아니라 하나의 기능이 다른 기능에 미치는 영향을 분석하여 결과적으로 시스템 수준에서의 잠재위험 분석이 가능하다.

<Figure 5>는 시스템공학 표준들에서 제시하고 있는 시스템 공학 프로세스이다. 본 논문에서는 시스템공학 프로세스 중 기능분석 단계에 초점을 맞춘다. 기능분석을 상위수준인 시스템수준에서부터 수행함으로써 시스템 수준부터 장치 및 부품 수준까지의 수준에 따라 구조화된 기능식별이 가능하다. 이를 바탕으로 식별된 기능의 오류로 인한 잠재위험을 식별함으로써 개별 기능뿐만이 아닌 기능간의 관계분석을 통한 시스템 수준에서의 기능오류로 인한 잠재위험 또한 식별 할 수 있다.

3.3. 기능분석을 통한 잠재위험 식별

존의 잠재위험 분석기법인 FMEA, FTA, HAZOP, PHA등을 분석해보면 잠재위험 분석이 앞서 제시했듯이 부품 및 장치수준에서 이뤄진다[8][9]. 이에 더하여 잠재위험 분석이 기존의 고장 및 사고 데이터, 전문가 집단의 브레인스토밍, 경험 등에 의존하여 이뤄지기 때문에 잠재위험의 누락의 위험도 존재하였다. 이제까지의 FMEA나 FTA는 이전의 고장 데이터, 전문가의 경험과 같은 정보를 바탕으로 잠재위험의 식별이 이뤄지지만 이에 의존할 경우 유사시스템 또는 새로운 시스템을 개발하는데 있어서 변경사항에 적절히 대응하지 못하여 잠재위험의 누락의 위험이 있다. 이를 보완하기 위해 기능분석 및 그 결과인 Function Tree를 활용한 잠재위험의 분석을 수행한다. 대상 시스템의 요구사항 분석 및 검증, 이를 바탕으로 한 기능의 식별 및 검증 과정을 통해 식별된 기능을 바탕으로 한 잠재위험의 식별 방법을 본 논문에서 제시한다. 즉 현재 부품 및 장치 중심으로 이뤄지고 있고 잠재위험의 누락의 가능성이 존재하는 기존의 잠재위험 분석기법을 보완하기 위해 기능분석을 통한 잠재위험 식별 방법을 본 논문에서는 제시한다. 요구사항의 분석을 통해 식별된 최상의 수준의 기능으로부터 시작하여 기능을 분해해 나가면서 시스템 수준에 따른 기능을 식별 한다. 이것을 일종의 Function Tree구조로 표현한다. Function Tree의 각각의 대상이 기능이 되는 것이다. 여기서 식별된 각각의 기능이 오류, 오작동을 행하는 경우를 잠재위험으로 식별한다. 이를 통해 먼저 하위수준에서 개별 기능의 오류로 인한 잠재위험을 식별 할 수 있다.



<Figure 6> Function tree along with system level.

다음으로 Function Tree 구조로 표현된 기능 Tree를 바탕으로 기능간의 상호관계를 분석한다. 이를 통해 하나의 기능이 다른 기능에 미치는 영향을 분석할 수 있게 되며 이를 통해 상위수준의 기능이 하위수준의 어떤 기능의 오류에 영향을 받는지를 파악할 수 있다. 이를 통해 시스템 수준에서의 기능오류로 인한 잠재위험의 식별이 가능하다. <Figure 6>과 같이 시스템 수준에 따른 기능 분석을 통한 기능트리를 만들어 잠재위험 식별에 이용한다. 시스템 수준에서 부품수준까지의 기능을 최상위 시스템 수준에서의 기능으로부터 기능분해를 통해 식별해 나간다. 이를 통해 부품 수준에서의 개별 기능뿐만 아니라 시스템 수준에서의 기능이 하위 수준의 어떠한 기능과 연관이 있는지를 식별하여 시스템 수준의 잠재위험 식별에 이용 할 수 있다.

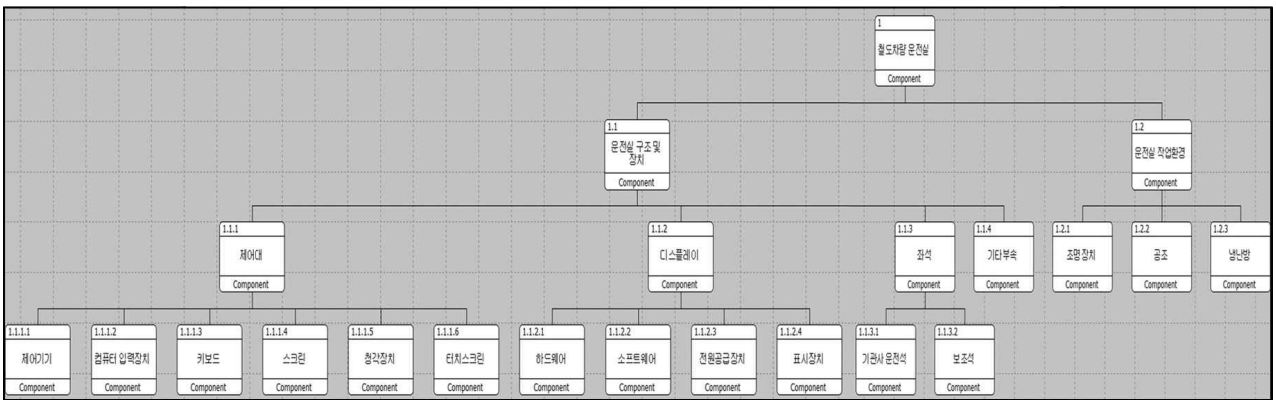
4. 철도차량 운전실의 잠재위험 분석 사례

3장에서 제시한 잠재위험 분석 방법에 따라 철도차량 운전실에 대한 잠재위험 분석을 수행했다. 먼저 시스템 정의를 통해 대상시스템의 요소를 식별하였다. 다음으로 기능분석을 통한 철도차량 운전실의 잠재위험 식별을 수행한 결과를 1,2절에 제시하였다.

4.1. 시스템 정의 및 요구사항 도출

철도차량 운전설의 시스템을 정의하기 위하여 유럽의 철도차량 표준인 UIC(Union Internationale Des Chemins De Fer)와 TSI(Technical Specification for Interoperability)를 바탕으로 철도차량 시스템 범위를 비교/분석을 통해서 설정 하였다. 철도차량 운전실의 구조 및 환경에 대해 TSI 표준 분석을 통해 고속열차와 일반열차에서 철도차량 운전실에 관련한 시스템 요소 분석을 수행하였다.

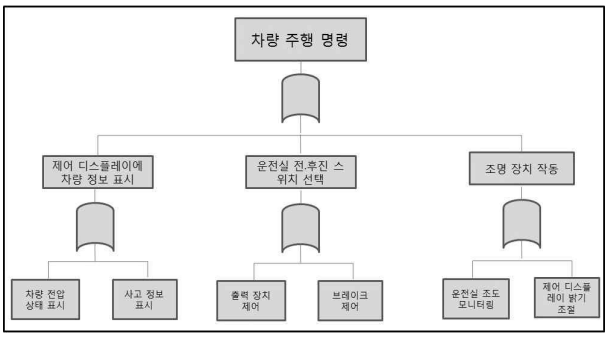
이를 바탕으로 철도차량 운전실의 서브시스템 및 하위 수준에 대해 Hierarchy Diagram을 <Figure 7>과 같이 제시하여 대상시스템인 철도차량 운전실의 요소를 파악하였다. 이를 바탕으로 개별 요소에 대한 요구사항을 도출하여 철도차량 운전실에서 충족해야 할 요구사항을 도출 하였다. 도출된 요구사항은 4.2절에서 수행할 기능분석의 입력 정보가 된다. 요구사항을 바탕으로 요구사항을 구현할 수 있는 기능을 식별한다.



<Figure 7> Hierarchy diagram of a locomotive cab.

4.2. 철도차량 운전실 기능 분석

4.1절에서 도출한 요구사항을 바탕으로 철도차량 운전실의 기능을 식별한다. 도출한 결과는 <Figure 8> 과 같다. 차량 운전실에서 차량 주행 명령 기능이 수행되면 디스플레이 장치에서는 제어 디스플레이에 차량 정보를 표시하는 기능이 수행된다. 운전실 제어대에서는 운전실의 전. 후진 스위치를 선택하는 기능을 수행한다. 또한 주행 명령과 함께 조명 장치의 작동이 수행된다.



<Figure 8> Function tree for a locomotive cab.

제어 디스플레이에 차량 정보를 표시하는 기능은 다시 차량의 전압상태를 표시하는 기능과 사고 정보가 수신 되었을 때 정보를 표시하는 기능으로 분해된다. 운전실 제어대의 운전실 전. 후진 스위치 선택 기능은 출력장치 제어 기능과 브레이크 제어 기능으로 나뉜다. 그리고 조명 장치의 작동은 운전실의 조도 모니터링 기능과 조도 정보를 바탕으로 제어 디스플레이의 밝기를 조절하는 기능으로 나눠진다. 이처럼 상위 수준에서의 기능은 하위 수준으로 내려오면서 분해되며, 각각의 개별 기능은 상, 하위 기능과 연관성을 가진다. 식별된 기능을 <Figure 8>과 같이 Function Tree 형태로 나타내어 상 하위 기능간의 관계를 파악 할 수 있다. 이를 바탕으로 개별 기능의 오류로 인한 잠재위험을 식별한 결과는 <Table 2>와 같다. 하위 수준에서의 개별 기능의 오류로 인한 잠재위험을 식별하고 이것들이 영향을 미치는 상위 기능에서의 오류를 식별하고 이것을 상위 수준에서의 잠재위험으로 정의 하였다. 기존의 잠재위험 식별 기법인 FMEA나 HAZOP등과는 달리 계층적으로 잠재위험을 식별하여 시스템 수준에서의 잠재위험 식별이 가능하도록 하였다. Component수준에서 식별된 기능의 오류로 인한 잠재위험을 1차적으로 식별 하였다. 그 다음으로 Component수준에서 기능의 오류 인해 발생되는 Subsystem의 기능오류를 식별하여 잠재위험으로 정의 하였다. 최종적으로 System 수준에서의 잠재위험을 하위 수준에서의 식별한 기능을 바탕으로 식별하여 정의 하였다. 단순한 개별 기능의 오류만을 식별하는 장치 및 부품수준에서 잠재위험을 식별하는 것이 아니라 계층적으로 기능을 분석하여 시스템 수준에서 잠재위험의 식별이 가능했다.

5. 결 론

오늘날 점차 대형화 복잡화 되어가고 있는 시스템들은 더욱 커진 사고 및 고장에 대한 위험을 내재하게 된다. 또한 철도와 같은 대형 복합 시스템에서 발생하는 사고 및 고장은 바로 큰 재산피해나 인명피해와 직결 될 수 있다. 따라서 체계적인 안전관리의 필요성이 점차 커지고 있다. 더불어 시스템에서 전기, 전자 장치 및 소프트웨어의비중이 높아짐에 따라 기능안전의 중요성이 높아지고 있다. 이에 따라 IEC 61508, ISO 26262등의 기능안전 표준들이 제정되어 산업에 적용되고 있다. 본 논문에서는 안전관리를 위한 시작점이자 중요한 과정인 잠재위험 분석단계에서 기능안전을 달성하기 위해 기능중심의 잠재위험 식별에 관한 연구를 수행했다. 기능 분석을 통해 시스템 수준에서 컴포넌트 수준까지의 기능을 식별했다.

이를 바탕으로 컴포넌트 수준에서 개별 기능의 오류로 발생 할 수 있는 잠재위험을 먼저 식별하였다. 다음으로 기존의 부품 및 장치 중심으로 이뤄지던 잠재위험 분석의 단점을 개선하기 위해 시스템 수준에서의 잠재위험 분석을 수행했다. 시스템 수준에서 컴포넌트 수준까지 식별된 기능을 바탕으로 하여 상하위 수준의 기능들 간의 연계성을 구조화를 통해 분석했다. 이에 따라 하위 수준에서의 기능오류가 시스템 수준에서의 기능오류에 영향을 미치며 이때의 시스템 수준에서의 기능오류로 인한 잠재위험을 시스템 수준에서의 잠재위험으로 식별했다. 이와 같은 방법을 통한 기능 중심의 잠재위험 분석은 IEC 61508등의 기능안전규격에서 상세히 제시하지 않고 있는 기능안전의 달성을 위한 잠재위험 분석에 대한 방법론으로 제시 될 수 있다. 또한 기능중심의 위험원식별은 사용자의 필요에서 시작하여 이를 충족시키기 위한 요구사항의 분석. 도출된 요구사항을 구현하기 위한 기능의 식별 및 검증 과정을 포함하는 프로세스를 거치게 된다. 따라서 시스템의 개념 설계 단계에서 기능의 오류로 이한 위험원들을 피하기 위해 요구사항의 변경 및 보완 과정이 다시 수행하게 된다. 이를 통해 개념설계과정에서 위험원을 피하기 위한 요구사항의 수정 및 보완, 수정 및 보완된 요구사항을 구현하기 위한 기능의 분석과정이 반복해서 이뤄져 설계단계에서의 위험원 분석의 결과가 반영

될 수 있다. 기능안전규격들은 기능안전의 달성을 위해 잠재위험 분석을 수행하라고 제시하고 있지만 상세한 방법론은 제시하지 않고 있다. 따라서 본 논문에서 제시하고 있는 기능 중심의 잠재위험의 분석을 통해 기능 안전 규격에서의 기능안전을 달성 할 수 있다. 향후 기능 중심의 위험평가 까지를 고려하여 시스템 수준에서의 기능 중심의 잠재위험 분석 전체 활동을 수행 하는 것에 대한 연구를 수행 할 필요가 있다.

5. 참고문헌

[1] Marco de Bruin and Paul Swuste, "Analysis of hazard scenarios for a research environment in an oil and gas exploration and production company," Safety Science, vol. 46, no. 2, pp. 261-271, Feb. 2008.

[2] Maddalena Casamirra, Francesco Castiglia, Mariarosa Giardina, and C Lombardo, "Safety studies of a hydrogen refuelling station: Determination of the occurrence frequency of the accidental scenarios," International Journal of Hydrogen Energy, vol. 34, no. 14, pp. 5846-5854, Jul. 2009.

[3] Y.M. Chen, K. S. Fan, and L. C. Chen, "Requirements and Functional Analysis of a Multi-Hazard Disaster-Risk Analysis," Human and Ecological Risk Assessment : An International Journal, vol. 16, no. 2, pp. 413-428, Apr. 9, 2010.

[4] Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS), International Electrotechnical Commission Standard, IEC 62278, 2002.

[5] Systems Engineering Management, Department of Defense Standard, MIL STD 499B, 1994.

[6] Road vehicles -- Functional safety --, International Organization for Standardization Standard, ISO 26262, 2011.

[7] Functional safety of electrical/electronic/programmable electronic safety-related systems, International Electrotechnical Commission Standard, IEC 61508, 2010.

[8] Jordi Dunjo, Vasilis Fthenakis, Juan Vilchez, and Josep Arnaldos, "Hazard and Operability (HAZOP) analysis. A literature review," Journal of Hazardous Materials, vol. 173, no. 1-3, pp. 19-32, Jan. 30, 2010.

[9] Rob Alexander and Tim Kelly, "Supporting systems of systems hazard analysis using multi-agent simulation," Safety Science, vol. 51, no. 1, pp. 302-318, Jan. 2013.

저 자 소 개

정 호 전

현 아주대학교 시스템공학과 박사과정. 관심분야는 시스템 안전 관리체계, 잠재위험 분석 및 식별, 모델기반 시스템공학, Modeling & Simulation 등.
주소: 경기도 수원시 영통구 원천동 산5번지 아주대학교 성호관 244호

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

오 성 근

현 아주대학교 전자공학과 정교수. 경북대학교 전자공학과 공학사, KAIST 전기 및 전자공학과 공학석사 및 공학박사 학위 취득. 캐나다 Simon Fraser 대 방문교수, 삼성전자(주) 책임연구원 역임. 연구 및 관심 분야는 통신 시스템 (이동통신) 이론 및 응용 등.
주소: 경기도 수원시 영통구 원천동 산5번지 아주대학교 원천관 402호