J. Korea Saf. Manag. Sci. Vol. 15 No. 4 December 2013
http://dx.doi.org/10.12812/ksms.2013.15.4.161

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

기능안전의 구현을 통한 Systematic Failure의 감축에 관한 연구

정 호 전* · 박 찬 우** · 이 재 천*
*아주대학교 시스템공학과 · **한국철도기술연구원

On the Reduction of Systematic Failure by Realizing a Method for Functional Safety

Ho Jeon Jung* · Chan Woo Park** · Jae-Chon Lee*
*Dept. of Systems Engineering, Ajou University · **Korea Railroad Research Institute

Abstract

Due to the recent advances in technology, the systems are becoming more demanding in terms of functionality and implementation complexity. Therefore, when system failures are involved in such complex systems, the effects of the related safety issues can also be more serious, thereby causing in the worst case irrecoverable hazards on both human being and properties. This fact can be witnessed in the recent rail systems accidents. In general, the accidents can be attributed to the systematic failure or the random failure. The latter is due to the aging or unsatisfied quality of the parts used in implementation or some unexpected external cause that would otherwise result in accidents whereas the former is usually related to incomplete systems design. As the systems are becoming more complex, so are the systematic failures. The objective of the paper is to study an approach to solving the systematic failure. To do so, at first the system design process is augmented by the functional safety activities that are suggested in the standard IEC 61508. Analyzing the artifacts of the integrated process yields the traceability, which satisfies the requirements for reduction of systematic failure as provided in ISO 26262. In order to reduce systematic failure, the results are utilized in the conceptual design stage of systems development in which systems requirements are generated and functional architecture is developed.

Keywords : Systems Safety, Systematic Failure, Systems Engineering, Functional Safety, IEC 61508

1. 서 론

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.

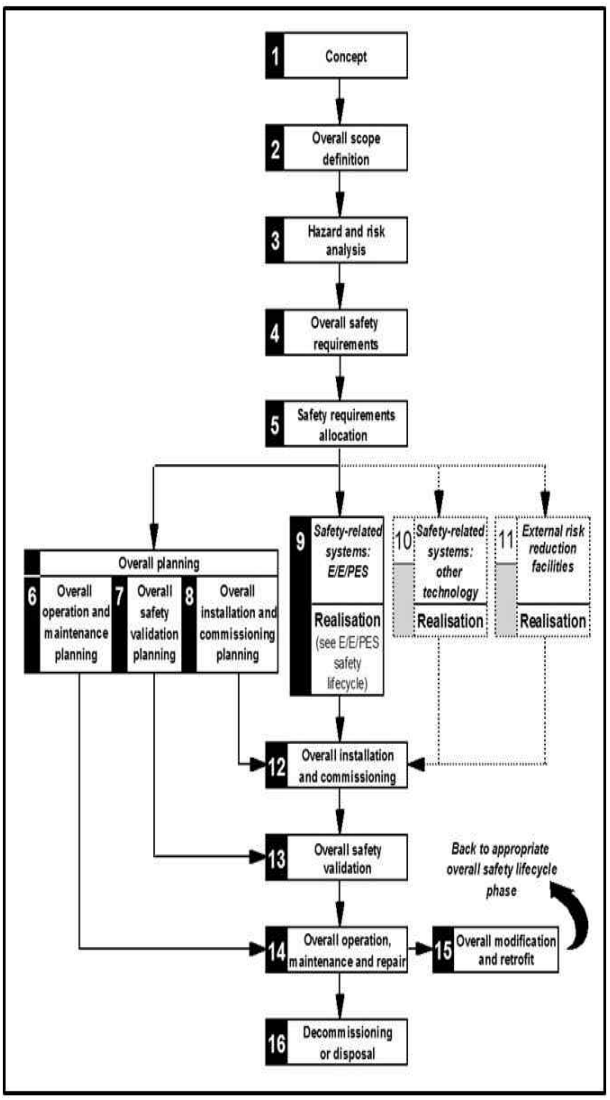
† 이 논문은 2013년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. NRF-2012R1A1A2009193)
† Corresponding Author : Prof. Jae-Chon Lee, Dept. of Systems Engineering, Ajou University, Wonchon-dong, Yeongtong-gu, Suwon, 443-749, Tel: 031-219-3941, E-mail: jaelee@ajou.ac.kr
Received October 20, 2013; Revision Received November 28, 2013; Accepted December 06, 2013

또한 현대의 시스템에서 전기전자 및 소프트웨어의 비중이 높아지면서 전기전자 기능안전성 규격(IEC 61508)이 제정되어 현대시스템의 안전에 관한 규격을 제시하고 있다. IEC61508을 바탕으로 하여 각 산업분야의 특성에 맞게 개선하여 자동차, 원자력, 의료기기 등의 산업분야에서 기능안전성에 관한 표준이 제정되어 이에 따른 시스템의 개발을 권고 하고 있다. 대표적인 안전중시 시스템중 하나인 철도분야에서는 신뢰성, 가용성, 유지보수성 및 안전성과 관련된 국제규격(IEC 62278/62279/62425)을 각종 사업제안 요청서의 요구사항에 포함시켜 이에 따른 시스템 개발 및 구축을 제시하고 있다. 이와 같이 안전은 여러 산업분야에서 시스템의 개발에 있어서 반드시 확보해야 할 필수 요소가 되었으며, 이를 위한 투자가 활발히 이뤄지고 있다.

이처럼 중요시되고 있는 안전의 확보를 위해서는 발생 가능한 고장을 설계초기에 미리 식별하고 분석하여 대응하는 것이 중요하다. 안전관련 표준규격에서는 안전 확보를 위한 절차를 제시하고 있으며 가장 핵심적인 단계로 위험원 분석 및 위험평가단계를 제시하고 있다. 또한 위험원 분석 및 위험평가를 설계의 초기 단계에 수행할 것을 권장하고 있다. 이런 분석과정을 통해 시스템에서 발생 가능한 고장을 식별하게 되는데 고장은 두 가지 유형으로 나뉜다. 첫째는 Random Failure로써 제품의 사용기한이 오래되어, 또는 외부의 충격에 의한 하드웨어 상의 고장을 일컫는다. 두 번째 유형은 Systematic Failure로써 시스템의 설계과정에서 발생 가능한 위험원에 의한 고장을 일컫는다. Random Failure의 경우 장치 및 부품 수준에서의 고장과 연관이 있고 Systematic Failure의 경우 시스템수준에서 식별해야 할 고장으로써 시스템을 구성하는 여러 구성요소들 간의 인터페이스 등의 영향을 받는 고장이다. 따라서 최신의 시스템일수록 복잡성이 증가하고 대형화되고 있으므로 Systematic Failure의 식별 및 개선이 매우 중요해지고 있다. 참고문헌 [1]에서는 Functional Safety의 Concept을 안전중시 시스템에 적용하는 방안에 대해 제시하고 있다. 본 연구에서는 기능안전 표준들을 소개하고, 설계단계에서 기능안전 활동을 수행하는 방안에 대해 제시하고 있다. 이를 통해 설계의 초기인 개념설계 단계에서 기능안전의 확보가 이뤄져야 함을 강조 하고 있다. 참고문헌[2][3]에서는 현재의 위험원 분석 과정을 살펴보면, 위험원 분석이 부품 및 장치 수준을 중심으로 이뤄지고 있음을 알 수 있다. 이는 물리적인 부품 및 장치수준에서 고려되는 Random Failure와 관련이 있다. 즉 현재의 위험원 분석은 부품 및 장치 수준에서의 Random Failure의 식별이 중점적으로 이뤄져 왔으나 복잡성이 증가하고, 전장품의 비중이 커지고 있는 현대의 시스템에는 적절하지 않다. 따라서 시스템 수준에서 Systematic Failure의 식별 및 대응 방안에 대한 제시가 필요하다. 따라서 본 논문에서는 개념설계 단계에서 요구사항 분석 및 기능분석을 수행하고 이를 바탕으로 Systematic Failure의 식별이 가능하도록 하였다.

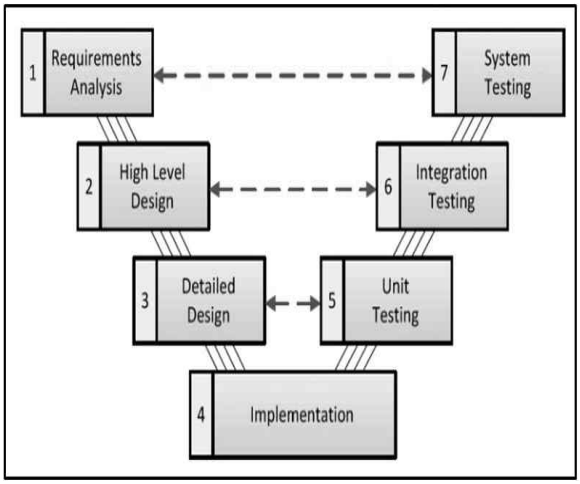
본 논문의 구성은 다음과 같다. 서론에서는 사회 및 연구의 연구동향과 필요성을 제시하였고, 2장에서는 관련 선행연구 및 연구 목표를 기술하여 문제정의를 했다. 3장에서는 개념설계 단계에서의 기능안전의 확보 방안에 대해서 제시한다. 4장에서는 3장의 활동을 바탕으로 철도차량 운전실에 대한 위험원 분석 사례를 제시하였다. 5장에서는 본 논문의 결과를 정리 및 요약하였다.

2. 문제 정의



<Figure 1> Safety life cycle.

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



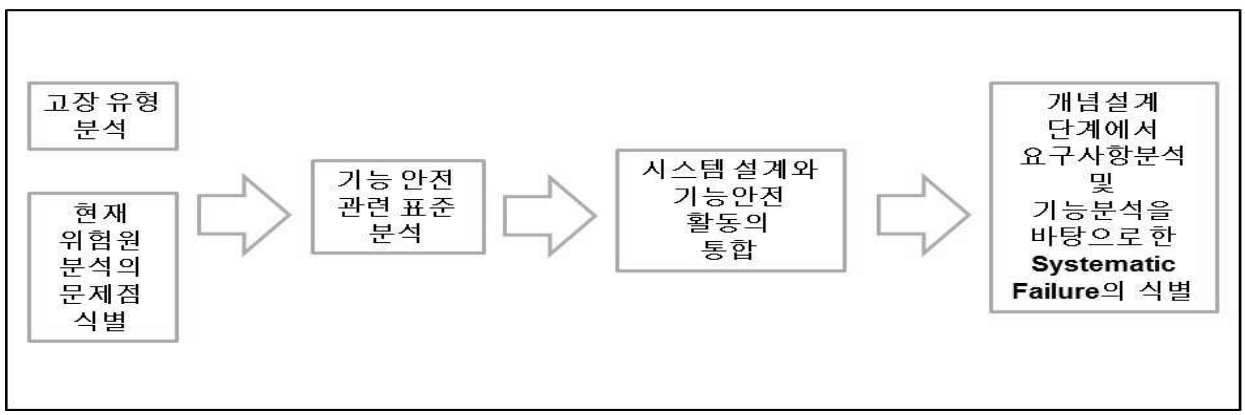
<Figure 2> V-model for systems development.

2.1 Systematic Failure와 기능안전의 연관성

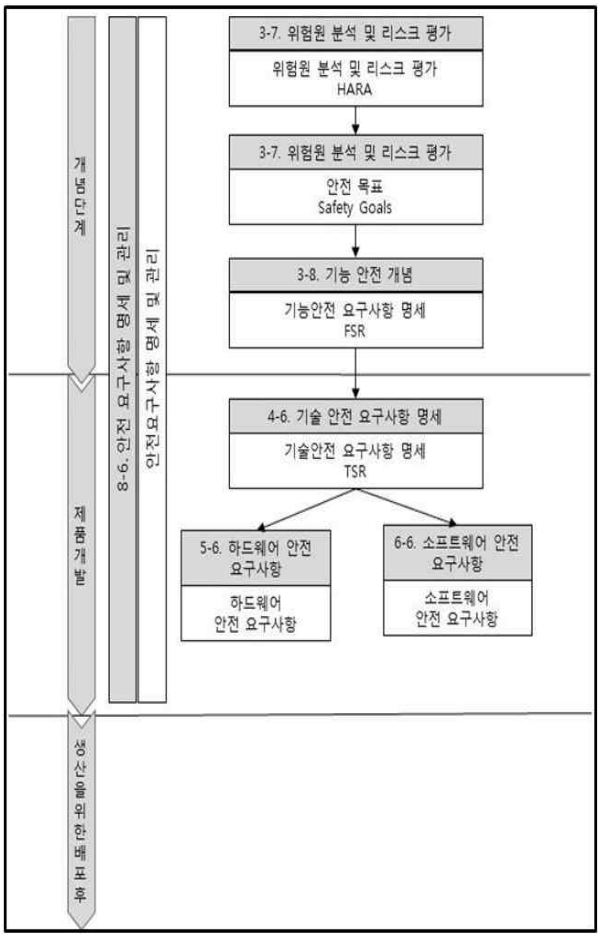
앞서 서론에서 밝혔듯이 고장의 유형엔 Systematic Failure와 Random Failure가 있다. Random Failure는 부품 장치 수준에서 부품의 수명에 따른 고장이나 외부 충격에 의한 고장으로써 기존의 위험원 분석이나 고장 식별에서는 부품 장치 수준에서의 Random Failure가 고려되었다. 그러나 현대의 시스템은 더욱 복잡성이 증가하고 있고 구성 요소들 간의 인터페이스도 더욱 많이 이뤄지고 있다. 따라서 단일 부품 장치에 대한 고장만이 아닌 부품들이 모여서 이뤄진 컴포넌트, 또는 더 상위수준인 시스템 수준에서의 위험분석이 필요하다. 이는 두 가지 고장 유형 중 Systematic Failure와 연관이 있다. Systematic Failure는 시스템의 설계 및 개발 단계에서 발생 가능한 고장이다. Systematic Failure를 줄이기 위해서는 개발 프로세스에 따른 시스템의 개발이 필요하다. 기능안전 관련 표준인 ISO 26262에서는 V-Model에 따른 시스템의 개발이 Systematic Failure의 감소를 도출할 수 있다고 제시하고 있다. 따라서 <Figure 1>, <Figure 2>와 같이 기능안전 표준에서 제시하고 있는 안전 수명주기 및 V-Model을 바탕으로 하여 기능안전을 시스템의 설계단계에서 확보함으로써 시스템의 Systematic Failure의 감소를 이룰 수 있다. 또한 Systematic Failure의 감소를 위해서 안전 활동의 각 단계별로 체계화된 문서 및 산출물의 관리가 필요하다고 참고문헌[4] 에서는 제시하고 있다. 따라서 시스템의 개발에 따른 산출물의 식별 및 관리 또한 Systematic Failure를 감소시키기 위한 기능안전 확보 프로세스에 포함되어야 한다. 즉 기능안전 표준에서 제시하고 있는 안전 관리 프로세스, 산출물 등을 시스템의 개발프로세스에 접목하여 기능안전을 시스템의 설계단계에서 달성함으로써 Systematic Failure의 감소가 이뤄질 수 있다.

2.2 Systematic Failure의 개선을 위한 개념설계단계에서 기능안전 확보의 필요성

앞 절에서 제시한 것처럼 Systematic Failure의 감소는 복잡성과 구성요소간의 인터페이스가 증가하고 있는 현대의 시스템의 개발에 있어서 매우 중요하다[5]. 본 논문에서는 기능안전의 달성을 위해서 개념설계단계에서의 안전 활동을 제시하고자 한다. 그 이유는 안전과 관련한 많은 표준에서 공통점으로 제시하고 있는 점이 시스템의 안전과 관련한 활동은 시스템의 개발초기 단계에서 수행 할 것을 권장하고 있다[6]. 시스템의 상세설계단계나 제작단계 이후에 고장 및 위험이 발생하여 대응하기에는 많은 시간과 비용이 소모되기 때문이다[7]. 따라서 본 논문에서도 시스템의 개발 단계 중 개념설계 단계에서의 기능 안전 확보를 위한 활동을 수행하고 이를 바탕으로 Systematic Failure의 식별 및



<Figure 3> Concept model for current research.



<Figure 4> An architecture for safety requirements.

대응을 할 수 있도록 한다. 또한 기능안전 확보를 위해 필요한 기능분석이 바로 시스템의 개념설계단계에서 이뤄진다. 따라서 개념설계단계서 이뤄지는 요구사항 분석, 도출된 요구사항을 바탕으로 한 기능분석을 기반으로 프로세스에 따른 기능안전 활동이 이뤄질 수 있도록 한다. 이를 통해 개발프로세스에 따른 기능안전 활동이 수행되고, 그 결과 식별된 기능기반의 Systematic Failure를 통해 차후 상세 설계 및 제작단계, 운용단계 등에서 발생 할 수 있는 고장에 대한 대응을 수행할 수 있도록 해준다.

2.3. 연구 목표 및 범위

상위 선행연구 분석을 통해 Systematic Failure의 감소를 위한 기능안전 활동의 필요성에 대해서 인지하였다. 또한 현재의 고장 및 위험분석 활동이 부품 및 장치 수준에서 Random Failure측면의 집중에 되어 있다는 것을 인식했다. 이러한 관점은 복잡성 및 구성요소간의 인터페이스가 증가하고 있는 현대의 시스템에는 부적절함을 알 수 있었다. 따라서 시스템의 개발단계에서 시스템 수준에서의 고장 및 위험분석의 결과라 할 수 있는 Systematic Failure의 식별 및 대응을 위해 개념설계단계에서의 기능안전달성을 본 논문의 연구 목표로 한다. 즉 <Figure 3>과 같이 기존의 고장유형을 분석하고 현재 위험원분석의 문제점을 식별하고, 이의 해결을 위해 기능안전 관련표준을 분석하여 시스템 설계단계에서의 기능안전 활동의 수행을 가능하게 하는 것이 목표이다. 이를 통해 최종적으로 개념설계단계에서 요구사항 분석 및 기능분석을 바탕으로 한 Systematic Failure의 식별이 최종 결과물이라 할 수 있다.

<Table 1> System Life-cycle에 따른 Safety Life-cycle

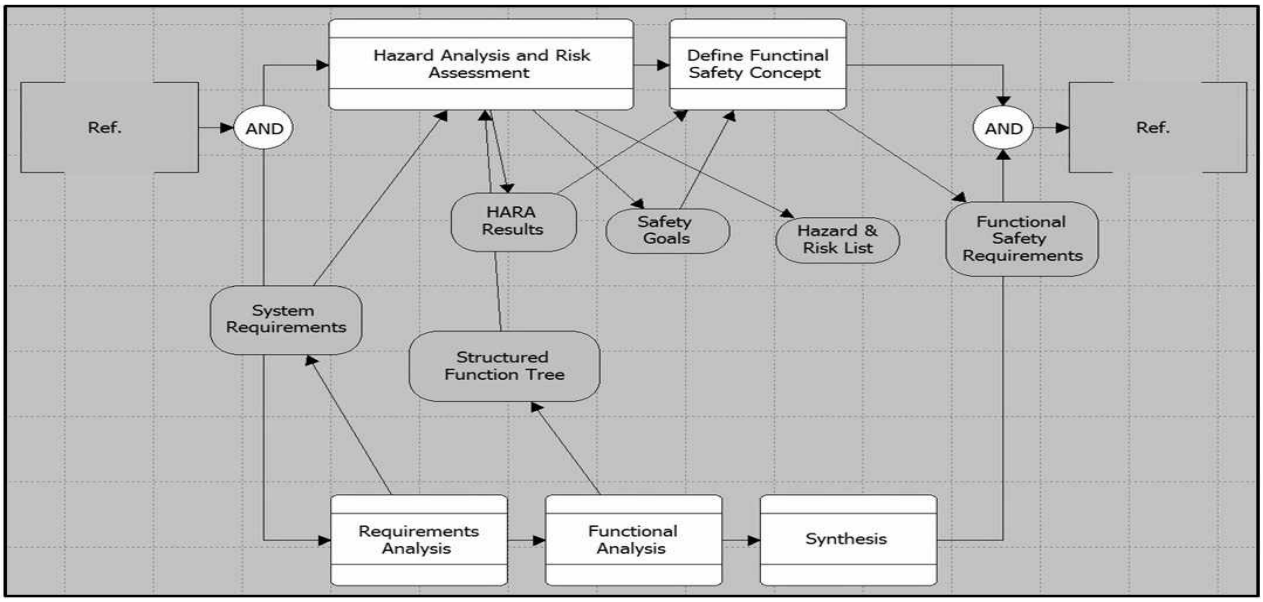
시스템 수명주기	안전 수명주기
개념 시스템 정의	시스템 정의
	위험원 및 위험 분석
리스크 분석 시스템 요구사항 도출	안전요구사항 도출
시스템 요구사항 할당	안전요구사항 할당
	위험원 원인 분석 및 추가 위험원 확인
	하부시스템 안전성 요구사항 할당
설계 및 구현 제작	Safety-related systems 설계 및 구현
시스템 검증 시스템 인수	안전성 입증
	안전 모니터링

3. 개념설계 단계에서의 기능안전 활동

3.1. 시스템의 개발 수명주기와 기능안전 수명주기의 통합

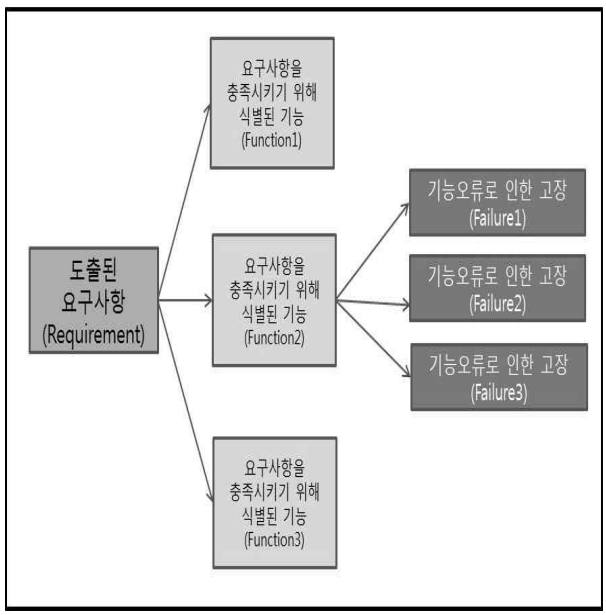
개념설계 단계에서 안전 활동의 통합을 위해서 먼저 개념설계 단계에서의 설계활동을 분석했다. “Systems

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



<Figure 5> An integrated process model for system development with safety activity and product.

Engineering Management, Department of Defense Standard, MIL STD 499B, 1994."은 미 국방 분야에서 제시한 시스템 공학표준으로서 개념 설계단계에서의 Systems Engineering Process를 제시하고 있다. 시스템의 개념설계는 요구사항의 분석, 기능분석, 통합 세 가지 단계로 이루어져 있다. 첫 번째 요구사항 분석 단계에서는 사용자의 needs로부터 시스템의 구현에 필요한 요구사항을 도출한다. 이때 도출된 요구사항들은 기능분석의 근거가 되며, 향후 시스템의 통합단계에서 시험요구사항으로도 이용된다. 따라서 개발의 시작점으로써 요구사항의 분석은 매우 중요하다. 요구사항 분석결과 도출된 요구사항을 바탕으로 요구사항을 시스템에 구현하기 위해 필요한 기능을 식별하는 기능분석단계가 수행된다. 도출된 요구사항을 할당받아 필요한 기능을 식별한다. 기능도 최상의 수준의 기능으로부터 하위 수준의 기능까지 구조적으로 식별한다. 이 두 가지 단계가 개념설계 단계에서의 핵심 활동이라 할 수 있으며, 이 두 단계의 결과는 안전 활동 수행을 위한 데이터로 이용된다. 가장 대표적인 기능안전표준인 ISO61508[9]에서는 <Figure1>과 같이 기능안전을 달성하기 위한 안전 수명주기를 제시하고 있다. 또한 기능안전의 달성을 위해 도출되어야 할 안전요구사항의 구조를 <Figure 4>와 같이 제시하고 있다. 이를 통해 개념설계 단계에서 위험원 분석 및 리스크 평가가 이뤄져야 하고 이를 통해 안전요구사항의 중요 요소인 안전 목표와 기능안전요구사항이 도출됨을 알 수 있다. 따라서 개념설계 단계에서의 Systems Engineering Process에 기능안전 활동을 통합하여 수행함으로써 개념설계단계에서 기능안전의 달성을 이룰 수 있다. 이를 위해 먼저 시스템의 개발 수명주기와 ISO61508에서 제시하고 있는 안전수명주기를 서로 매칭 하였다. 이를 통해 시스템 수명주기의 각 단계에서 어떠한 안전수명주기 활동이 수행되어야 하는지를 식별 할 수 있다. 그 결과는 <Table 1>과 같다. 이를 바탕으로 통합된 시스템 개발 프로세스는 <Figure 5>와 같다. 기본의 개념설계에서 수행되는 요구사항 분석 및 기능분석 단계의 산출물인 시스템의 요구사항과 식별된 기능들이 안전 활동의 핵심단계인 위험원 및 위험 분석(Hazard Analysis and Risk assessment)단계에 입력으로 이용된다.



<Figure 6> On how to identify systematic failure.

이를 바탕으로 수행된 위험원 및 위험분석 단계의 결과로 안전요구사항 및 식별된 고장 및 위험 리스트 등이 도출된다. 즉 앞서 설명했듯이 본 논문의 연구 목표라 할 수 있는 개념설계 단계에서의 기능안전의 확보를 통한 Systematic Failure의 식별 및 감소를 달성 할 수 있다.

기능안전표준인 ISO26262에서 제시하고 있듯이 Systematic Failure를 감소하기 위해서는 시스템의 개발과 안전 활동을 수행하기 위한 프로세스가 명확히 제시되어야 하며, 프로세스를 수행하며 도출되어야 하는 산출물들 또한 명확히 제시되어야 한다. 따라서 <Figure 5>에서 제시하고 있는 시스템의 개발 및 안전 활동의 수행과 이에 따른 산출물이 명시된 프로세스를 제시함으로써 Systematic Failure의 감소를 달성 할 수 있다.

3.2 요구사항 분석과 기능분석을 통한 Systematic Failure의 도출

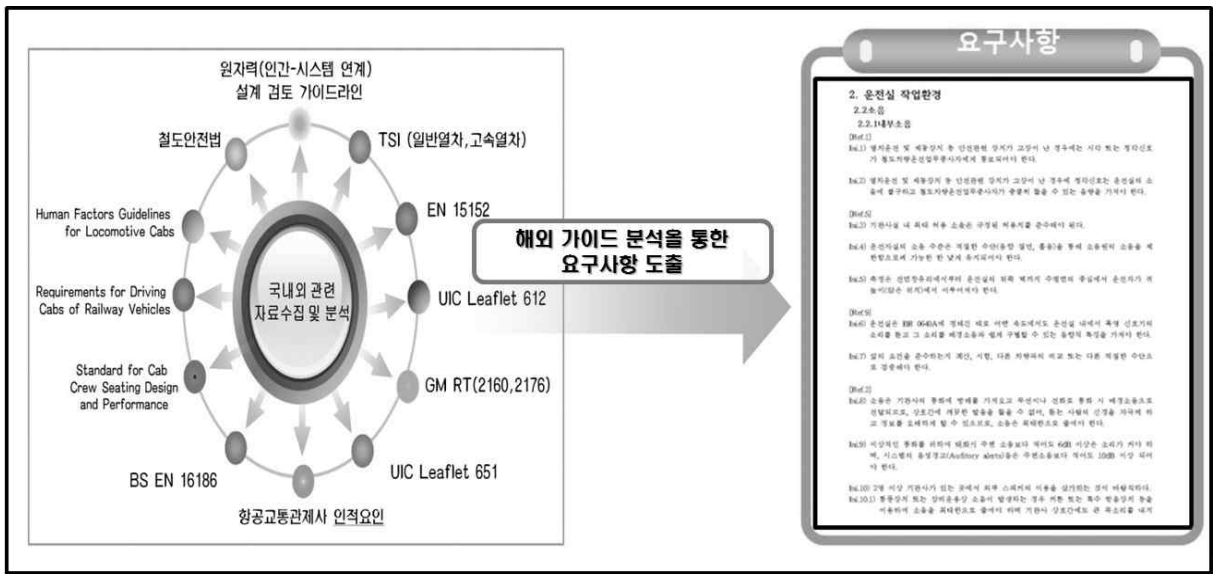
개념설계 단계에서의 요구사항 분석과 기능분석을 통한 Systematic Failure의 도출의 개념은 <Figure 6>와 같다. 첫 단계인 요구사항 분석을 통해 사용자의 needs로부터 요구사항을 도출한다. 그 후 도출된 요구사항을 구현하기 위해 식별한 기능들을 요구사항별로 식별한다. 마지막으로 식별된 기능이 오류를 일으킴으로 발생할 수 있는 고장들을 식별한다. 최종적으로 식별된 고장은 시스템의 개발과정에서 식별할 수 있는 Systematic Failure이다. 이는 단순히 장치 부품수준에서 개별 장치 및 부품에 대한 고장이 아닌 시스템 수준에서 식별된 고장으로써 기존의 하드웨어 상에서 발생 가능한 Random Failure의 측면이 아닌 설계 단계에서 식별 가능한 Systematic Failure임을 확인 할 수 있다.

4. 철도차량 운전실 설계에서의 Syste matic Failure 분석 사례

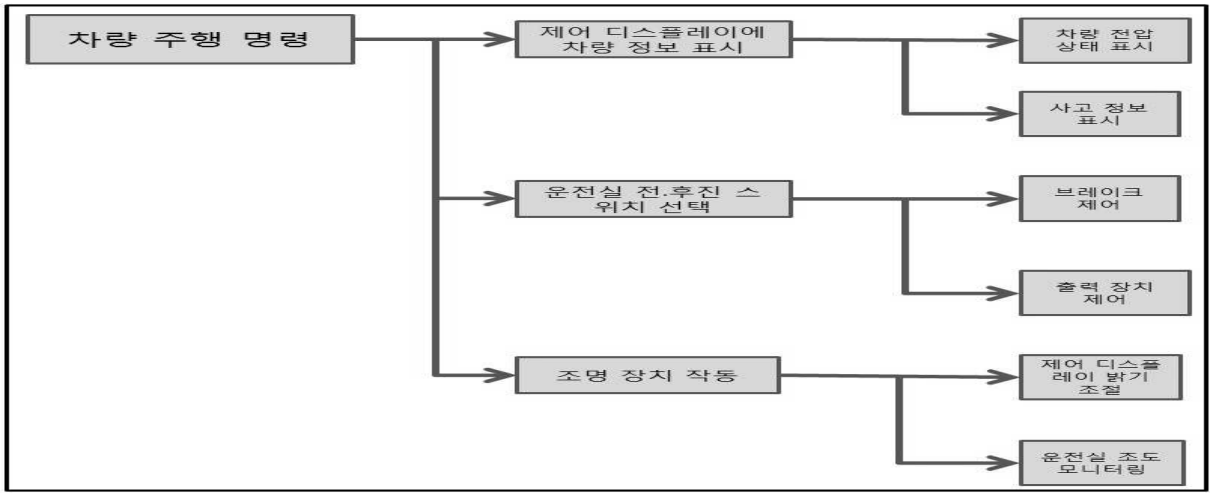
3장에서 제시한 통합프로세스에 따라 철도차량 운전실의 설계에 대한 Systematic Failure의 분석을 수행했다. 먼저 철도차량 운전실에 대한 요구사항을 도출했다. 다음으로는 식별된 요구사항을 충족시키기 위한 기능을 식별하였고, 위의 두 결과를 바탕으로 기능오류로 인한 철도차량 운전실의 설계에서의 Systematic Failure를 식별 했다.

4.1. 철도차량 운전실 설계에 대한 요구사항 도출

철도차량 운전설의 설계를 위한 요구사항을 도출하기 위해 국, 내외 철도 관련 법률, 표준, 운전실관련 원자력 및 항공분야 표준 등을 분석하였다. <Figure 7>과 같이 요구사항 분석의 대표적인 방법인 문헌분석을 통해 철도차량 운전실의 설계를 위한 요구사항을 도출하였다. 총12가지의 표준 및 법률을 분석하였으며 크게 철도차량 운전실의 구조 및 장치와 관련한 요구사항과 운전실의 작업환경과 관련된 요구사항 두 가지로 나누어 요구사항을 도출하였다.



<Figure 7> Requirement development for locomotive cabs.



<Figure 8> Results of functional analysis of railroad vehicle driving.

운전실 구조와 관련해서는 제어대, 좌석 등 5개 분야에 대해 31개의 세부분야에 대해 요구사항을 도출하였다. 작업환경과 관련해서는 조명, 색상 등 8개 분야 14개 세부 분야에 대해 요구사항을 도출하여 총 693개의 요구사항을 도출하였다.

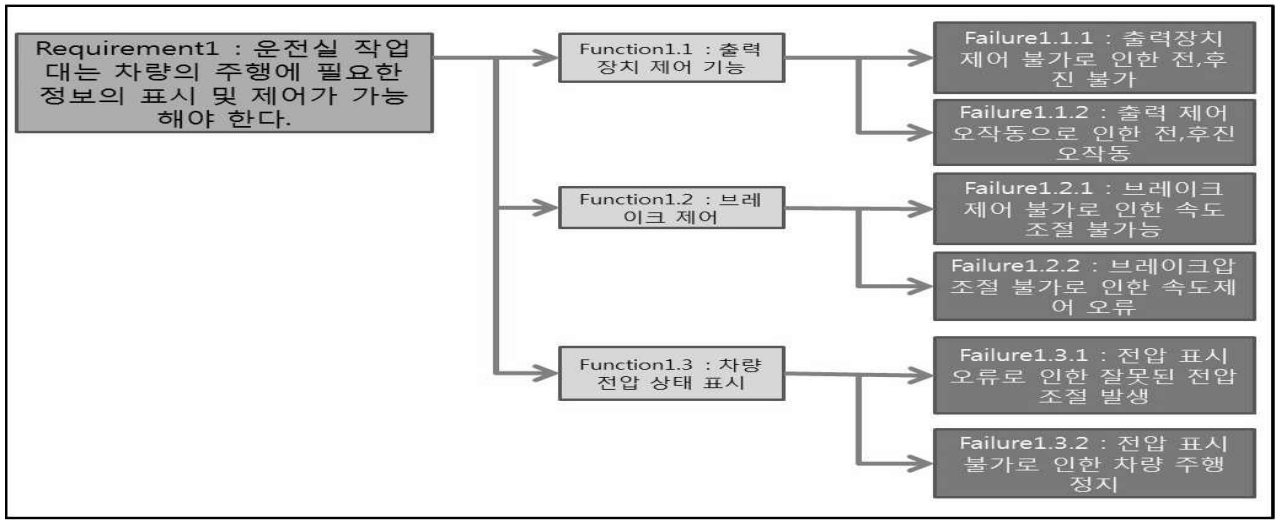
도출된 요구사항은 기능분석에 이용되며 향후 시스템의 통합과정에서 시험평가를 수행하는데 검증 요구사항으로도 이용된다.

4.2. 철도차량 운전실 기능 분석

4.1절에서 도출한 요구사항을 바탕으로 철도차량 운전실의 기능을 식별한다. 도출한 결과는 <Figure 8>과 같다. 4.1절에서 도출하는 요구사항을 시스템에서 충족시키기 위해서 시스템에 필요한 기능을 식별하는 단계이다. 예시로 포함한 <Figure 8>은 시스템의 주행을 위해 필요한 기능을 식별한 결과의 일부이다. 요구사항을 식별하고 그것을 바탕으로 기능을 식별 및 분석하고 이를 바탕으로 Systematic Failure를 식별하는 프로세스에 따른 결과라 할 수 있다. 차량의 주행을 위해서는 운전실의 작업대에 차량정보를 표시하는 기능이 필요하며, 전, 후진 명령을 위한 전, 후진 스위치 선택 기능이 필요하며 운전실의 조명을 제어하는 장치 또한 필요하다. 기능분석의 경우에도 단일 기능의 식별로 끝나는 것이 아니라 상위 수준의 기능을 1차적으로 분석하고 각각의 기능에 대해 필요할 경우 하위 수준의 기능 또한 식별 및 분석한다. <Figure 8>의 경우엔 차량주행이라는 기능 아래에 2 level의 하위 기능들이 식별된 것을 확인 할 수 있다. 이를 통해 체계적으로 시스템이 요구사항을 충족시키기 위한 기능들을 누락 없이 식별 할 수 있다. 이는 향후 Systematic Failure를 식별하는데 있어서도 최대한 누락을 줄인 고장의 분석이 가능함을 의미한다. 철도 차량 운전실에 대하여 4.1,2절을 통해 요구사항 분석과 기능분석을 수행하였고 그 결과 도출된 구조화된 요구사항 및 기능들을 가지고 최종적으로 Systematic Failure의 식별을 수행 4.3절에서 수행한다.

4.3. 철도차량 운전실의 Systematic Failure 분석

4.1절과 4.2절을 통해 수행한 개념설계 단계에서의 요구사항 분석과 기능분석 결과를 바탕으로 최종적으로 철도차량 운전실에 대한 Systematic Failure를 식별하였다. Systematic Failure의 식별의 결과의 일부는 <Figure 9>와 같다. 먼저 요구사항 분석결과를 통해 도출된 운전실 작업대는 차량의 주행에 필요한 정보의 표시 및 제어가 가능해야 한다는 요구사항을 도출 하였다. 앞의 요구사항을 시스템이 충족시키기 위해서 기능분석을 수행한 결과 필요한 기능이 식별되었고, 그중 일부가 출력장치 제어기능, 브레이크 제어기능, 차량 전압상태 표시 기능이다. 이는 4.2절에서 수행한 기능분석 결과에서 도출된 기능 중에 일부임을 확인할 수 있다. 최종적으로 Systematic Failure는 식별된 기능이 오작동 또는 오류를 발생한 경우로 정의된다. <Figure 9>의 결과와 같이 출력 장치 제어기능이 오작동하거나 기능이 수행이 불가한 경우 2가지의 Failure가 식별되었다. 다음으로 브레이크 제어기능에서 브레이크의 제어가 불가능한 경우와 브레이크 압의 제어가 불가능한 두 가지 경우에 대한 Failure가 식별되었다. 세 번째로



<Figure 9> Results of identifying systematic failure.

운전실 작업대의 차량 전압상태 표시기능의 경우 잘못된 전압이 표시된 경우와 전압표시가 불가능한 경우에 대한 Failure가 식별되었다. Systematic Failure의 분석결과를 통해 개념설계 단계에서의 요구사항 분석, 기능분석, 이를 바탕으로 한 고장 분석은 체계적으로 절차에 따라 수행이 되어야 하며, 각각의 단계에서 도출되는 산출물들은 다음단계의 수행을 위한 입력으로 필요함을 알 수 있다. 즉 ISO 26262표준에서 제시한바와 같이 Systematic Failure를 식별하기 위한 절차 즉 프로세스가 3절에서와 같이 제시되었고, 이때 각 단계별로 도출되는 산출물들의 연계성도 식별하여 ISO 26262 표준에서 제시하는 Systematic Failure의 감소 조건을 충족시킬 수 있음을 사례를 통해 확인 할 수 있다. 이러한 분석 결과는 기존의 고장분석이 부품 및 장치 수준에서 수행되어 온 것과는 달리 시스템수준에서의 고장 분석임을 알 수 있다. 즉 시스템 수준에서의 요구사항과 기능분석을 통해 식별된 고장으로써 Top-down 개념의 시스템에 대한 분석의 결과이다. 이는 하위 수준에서의 개별 부품 및 장치 수준의 고장 분석결과와는 달리 상위 수준에서 부터의 고장 분석 결과이며, 이는 향후 개별 파트에서의 고장뿐만 아니라 상호간의 인터페이스를 가지는 수준에서의 고장 또한 식별 가능 하다.

5. 결 론

오늘날 점차 대형화 복잡화 되어가고 있는 시스템들은 더욱 커진 사고 및 고장에 대한 위험을 내재하게 된다. 특히 대표적인 안전중시 시스템인 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 전장품 및 소프트웨어의 비중이 높아짐에 따라 기능안전의 중요성이 높아지고 있다. 이에 따라 IEC 61508, ISO 26262등의 기능안전 표준들이 제정되어 산업에 적용되고 있다. 본 논문에서는 개념설계단계에서 기능안전의 달성을 통해 두 가지 고장유형 중 Systematic Failure의 감소를 목표로 하여 연구를 수행하였다. Systematic Failure는 부품 및 장치 수준에서의 하드웨어상의 고장과 관련이 있는 Random Failure와는 달리 시스템의 설계 및 개발과 관련이 있다. 따라서 본 논문에서는 시스템의 개발 단계 중 개념설계 단계에서의 기능안전의 달성을 통해 Systematic Failure의 감소를 달 성 하고자 했다. 이를 위해 시스템의 개념설계 단계에서의 시스템공학 프로세스와 ISO61508표준에서 제시하고 있는 안전수명주기 활동 및 산출물이 통합된 프로세스를 제시하였다. 이는 대표적인 기능안전 표준인 ISO 26262에서 제시하고 있는 Systematic Failure의 감소 조건을 충족시키기 위함이다. ISO 26262에서는 Systematic Failure의 감소를 위한 조건으로 체계적인 시스템 개발 및 안전 관리 프로세스가 필요하며, 이 때 도출되는 산출물의 정의가 필요하다고 제시하고 있다. 이를 개념설계에서 달성하기 위해 개념설계 단계에서의 통합 프로세스를 제시하였고 이를 대표적인 안전중시 시스템인 철도분야의 운전실 설계에 적용함으로써 검증하였다.

본 논문에서의 고장분석을 통해 기존의 부품 및 장치 수준에서의 고장 분석에 더하여 상위 수준에서부터 Top-down측면의 고장 분석을 수행하여 누락을 최소화한 고장의 식별과 이를 통해 실제 개발과정에서의 Systematic Failure의 발생을 감소시킬 수 있다. 이는 기존의 고장분석의 단점 중 하나인 하위 수준 즉 부품

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

및 장치수준에서의 개별 부품 및 장치중심의 고장분석의 단점을 개선시킬 수 있다. 상위수준에서부터의 시스템의 분석을 통해 고장을 분석함으로써 하위 기능수준에서의 개별 고장분석 뿐만 아니라 서로 영향을 미치는 기능들에 의한 고장 또한 분석 할 수 있으며, 이는 더 많은 Systematic Failure의 식별이 가능함을 의미하며 이를 통해 개발과정에서의 고장 발생의 위험을 줄일 수 있다. 향후 시스템수준에서의 기능중심의 위험평가 방법에 대한 연구가 필요하며 이를 바탕으로 개념설계 단계에서 기능안전 표준에서 제시하고 있는 기능안전 활동이 완전히 통합된 프로세스의 개발이 가능할 것이다.

6. References

[1] Kazimierz Kosmowski, "Functional safety concept for hazardous systems and new challenges," Journal of Loss Prevention in the Process Industries, vol. 19, pp. 298-308, Jun. 5, 2006.

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

[5] M. Bellotti and R. Mariani, "How future automotive functional safety requirements will impact microprocessors design," Microelectronic Reliability, vol. 50, no. 9-11, pp. 1320-1326, Sep 2010.

[6] P. J. Wilkinson and T. P. Kelly, "Functional hazard analysis for highly integrated aerospace systems," in Proc. IEE Certification of Ground/Air Systems Seminar, London, UK, Feb 17, 1999.

[7] C. A. Ericson, Hazard Analysis Techniques for System Safety. Hoboken, NJ: WILEY, 2005.

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

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

저 자 소 개

정 호 전

현 아주대학교 시스템공학과 박사과정. 관심분야는 시스템 안전관리체계, 위험원 분석 및 식별, 모델기반 시스템공학, Modeling & Simulation 등.

주소: 경기도 수원시 영통구 원천동 산5번지 아주대학교 성호관 244호

박 찬 우

현 한국철도기술연구원 선임연구원. 시험인증센터의 시스템안전실 근무 중, 경희대학교 산공학과에서 공학사, 공학석사 및 박사 학위를 취득, 현재 관심분야는 철도시스템 위험도 평가, 확률 모형, 시스템 모델링, 시뮬레이션, 경영과학 등.

주소: 경기도 의왕시 철도박물관로 176 한국철도기술연구원

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