Journal of the Korea Academia-Industrial cooperation Society
Vol. 17, No. 4 pp. 382-391, 2016

http://dx.doi.org/10.5762/KAIS.2016.17.4.382
ISSN 1975-4701 / eISSN 2288-4688

경전철 역사 개념설계 단계에서 기능분석 결과를 활용한 안전요구사항의 생성방법에 관한 연구

김주욱[1], 정호전[2], 박기준[1], 김주락[1], 한석윤[1], 이재천[2*]
[1]한국철도기술연구원, [2]아주대학교 시스템공학과

On the Development of Safety Requirements Based on Functional Analysis of LRT Stations in Concept Development Stage

Joo-Uk Kim[1], Ho-Jeon Jung[2], Kee-Jun Park[1], Joorak Kim[1], Seok Youn Han[1], Jae-Chon Lee[2*]
[1]Korea Railroad Research Institute, [2]Dept. of Systems Engineering, Ajou University

요 약 철도와 같은 안전중시 시스템에 대해 체계적인 안전관리의 필요성이 점차 커지고 있어 IEC 61508, 62278, ISO 26262 등의 안전과 관련된 표준들이 제정되었고, 관련연구가 수행되고 있다. 그중 안전 프로세스의 중요한 활동인 위험원 분석에 대하여 다양한 연구가 수행되어 왔으나, 시스템설계 프로세스와의 구체적인 연계성이 부족하였다. 또한 기존의 위험원 분석 방법은 시스템 설계가 상당 수준 진행된 하드웨어 및 소프트웨어 구성품 정보에 의존하기 때문에, 설계 변경에 많은 비용과 일정이 소요된다. 이러한 문제들을 해결하기 위해서 본 논문에서는 시스템 설계초기인 개념설계 단계에서 수행한 기능분석 결과를 안전 프로세스에서 직접적으로 활용하여 위험원을 분석하고 이를 바탕으로 위험을 줄이기 위해 필요한 안전요구사항을 생성하는 방법에 대하여 연구를 수행하였다. 설계 초기에 위험원 분석 및 안전요구사항의 도출을 수행함으로써, 향후 요구사항 변경 등 여러 요인으로 시스템 설계 및 안전 설계의 변경 시에 이를 반영하는데 있어서 시간 및 비용 관점에서 상대적으로 효율적인 접근 방법이 된다. 한편, 사례연구로서 본 논문에서 제시한 방법을 경전철 역사의 안전성을 확보하기 위한 요구사항의 도출에 적용하는 연구를 수행하였다.

Abstract For safety-critical systems including railways, there has been a growing need for effective and systematic safety management processes. The outcomes of efforts in this area are international safety standards, such as IEC 61508, 62278, and ISO 26262. One of the principal activities in the safety process is hazard analysis. For this reason, considerable efforts have been directed toward methods of hazard analysis. On the other hand, the hazard analysis methods reported thus far appear to be unclear in terms of their relationship with the system design process. In addition, in some cases, the methods appear to rely heavily on information regarding the hardware and software components, the number of which is increasing. These aspects can become troublesome when design changes are necessary. To improve the situation, in this paper, hazard analysis was carried out using the result of functional analysis early in the concept development stage for a safety-critical system design. Because hazard analysis is carried out at the system level and the result is then used to develop the safety requirements, improvements can be expected in terms of the development time and cost when design changes are required due to changes in the requirements. As a case study, the generation of safety requirements for the development of light rail transit stations is presented.

Keywords : Safety-Critical Systems, Hazard Analysis, Safety Requirements, Systems Design, Functional Analysis, Model-Based Approach

본 연구는 국토교통부 철도기술연구사업의 "저심도 도시철도시스템 인터페이스 및 성능검증 연구" 연구비지원 (15RTRP-B069124-03)에 의해 수행되었음.
*Corresponding Author : Jae-Chon Lee(Ajou Univ.)
Tel: +82-31-219-3941 email: jaelee@ajou.ac.kr
Received January 27, 2016 Revised (1st March 9, 2016, 2nd March 22, 2016)
Accepted April 7, 2016 Published April 30, 2016

1. 서론

현대의 안전중시 시스템들은 고장과 이로부터 비롯된 사고가 인명피해와 재산피해로 직결되기 때문에 체계적인 안전관리가 매우 중요하다[1]. 이에 따라 철도, 국방, 항공, 원자력 등의 안전이 중시되는 분야에서는 안전에 대한 국제 표준규격을 제정하고 이를 준수하도록 권장하고 있다. 이와 같이 안전은 대형 복합 시스템 산업분야에서 시스템의 개발과정에서 반드시 수행하여야 하는 필수적인 요소가 되었으며, 이에 따른 투자와 연구가 활발히 이뤄지고 있다[2].

안전성을 확보하기 위해 제시되고 있는 많은 표준규격들은 안전을 보장하는 것을 목표로 하고 있으며, 안정보장을 위해 안전요구사항을 도출하여 설계에 반영 할 것을 권장하고 있다. 따라서 기존의 시스템 설계과정과 연계하여 시스템의 설계단계에서부터 안전이 확보 될 수 있도록 해야 한다. 이를 위해 IEC 61508, IEC 62278 등의 안전과 관련된 표준들에서는 안전수명주기에 따라 대상 시스템에 대한 안전요구사항을 도출하고 이것을 설계에 반영하는 절차를 제시하고 있다. 여러 안전 표준에서 제시하고 있는 안전수명주기를 보면 위험원 분석 및 위험 평가수행의 결과를 바탕으로 안전요구사항을 도출하도록 제시하고 있다[3][4]. 그리고 이때 위험원 분석 및 위험평가를 수행하는데 있어 시스템의 설계 과정에서 산출되는 정보들을 활용하여 수행할 것을 권장하고 있다. 이렇게 산출된 안전요구사항들은 향후 안전관련시스템을 설계하는데 반영되어 시스템의 설계과정에서부터 안전이 확보될 수 있도록 제시되어 있으므로 안전 확보를 위해 안전요구사항을 도출하는 것이 매우 중요함을 인지 할 수 있다[5].

위와 같이 안전표준에서 제시한데로 위험분석 결과를 활용하여 안전요구사항을 도출하는 데 대한 구체적인 방법론이 아직 명확히 제시되고 있지는 않다는 것을 선행연구 분석을 통해 확인하였다. 이에 따라 본 연구에서는 설계초기 기능식별 및 분석결과를 활용한 위험분석 방법과 이결과를 활용한 안전요구사항의 도출 방법에 대하여 제안한다. 이를 통해 시스템의 설계 초기에 설계결과를 활용하여 도출된 안전요구사항을 설계초기에 반영함으로써 설계단계에서 부터 안전이 확보 될 수 있을 것이다.

본 논문의 구성은 다음과 같다. 서론에서는 사회 및 연구의 연구동향과 필요성을 제시하였고, 2장에서는 관련 선행연구 및 연구 목표를 기술하여 문제정의를 했다. 3장에서는 설계초기 개념설계 결과를 활용한 위험분석 및 안전요구사항의 도출 방법에 대해 제시한다. 4장에서는 3장에서 제시한 방법을 바탕으로 경전철 역사의 안전요구사항 도출 사례를 제시하였다. 5장에서는 본 논문의 결과를 정리 및 요약 했다.

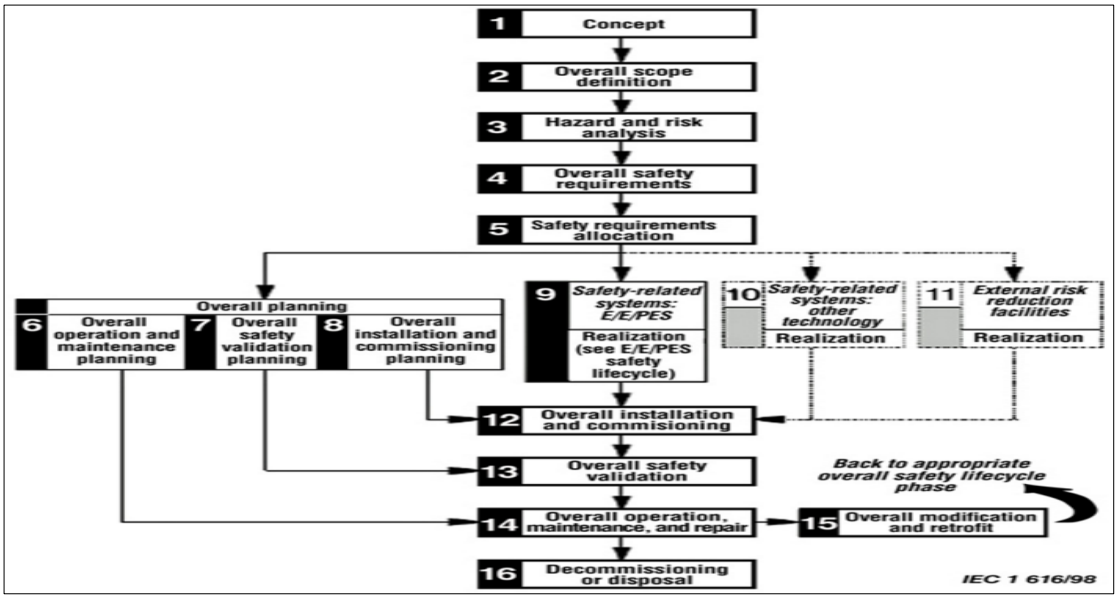

Fig. 1. Safety Life Cycle

2. 문제정의

2.1 안전표준에서 제시하고 있는 Safety Requirements 도출 방법

여러 안전표준에서는 안전수명주기를 제시하며 안전 확보를 위해 수행되어야 할 활동들에 대해서 명시하고 있다. <Fig. 1>는 대표적인 안전표준 중에 하나인 IEC 61508에서 제시하고 있는 안전수명주기 이다. 안전수명주기에 따르면 위험 분석을 수행하고 이 결과를 바탕으로 안전요구사항을 도출하도록 권장하고 있다. 그리고 이렇게 도출된 안전요구사항을 시스템에 설계에 반영하도록 제시되고 있다. 이와 같이 안전요구사항은 대상 시스템의 위험분석 결과에 따라 안전을 달성하기 위해 어느 수준의 안전목표가 필요하며, 이를 달성하기 위해 어떠한 요구사항이 필요한지에 관한 것이다. 이것을 도출하기 위해서는 설계정보를 활용한 위험분석이 필수적이다. 위험분석이 설계정보에 기반을 두어 얼마나 누락 없이 체계적으로 수행되느냐가 안전요구사항 도출의 핵심이라 할 수 있다.

2.2 기존의 위험분석 결과에 기반을 둔 안전 요구사항 도출에 관한 연구 분석

안전표준을 충족하면서 안전요구사항을 도출하기 위한 연구들이 지속적으로 수행되고 있다. 참고문헌[4]는 기존의 위험분석단계에서 활용되던 기법들을 수행함으로써 안전요구사항을 어떻게 도출할 것인지에 대한 연구이다. 참고문헌[4]에서는 기존에 위험분석에서 주로 활용되어 오던 기법들을 분석하여 이것이 안전요구사항을 도출하는데 어떻게 활용 할 수 있을지에 대해 분석하였다. 위험분석 기법 각각에 대해 적용범위, 대상, 장단점 등을 분석하여 안전요구사항을 도출하는데 있어 각 기법들의 활용성에 대해 제시하였다. 참고문헌[5]에서는 자동차 분야의 안전표준인 ISO 26262를 충족시키기 위해 위험원 분석 및 위험평가 결과로 부터 안전요구사항을 도출하는 방법에 대해서 제시하고자 하였다. 참고문헌[5]에서는 이를 위해 모델기반 접근방법을 제안하고 있다.

그러나 이와 같은 기존의 연구에는 부족한 부분이 있다. 참고문헌[4]는 상당히 많은 기법들에 대해 분석이 이뤄졌으나 직접적으로 위험분석결과가 안전요구사항을 도출하는데 어떻게 활용되는지에 대해서는 부분은 부족한 점이 있다. 위험분석결과와 안전요구사항간의 연관성, 두 활동간의 상호정보교환이 어떻게 이뤄져야 할지에 대해선 구체적으로 제시되어 있지 않다. 참고문헌[5]는 안전표준을 충족시키며 안전요구사항을 도출하기 위해 모델기반 접근방법을 제안하고 있다. 그러나 모델을 통해 안전요구사항을 어떻게 도출할 것인가 보단 모델을 활용하여 안전요구사항과 위험분석 결과를 어떻게 표현할지에 관한 접근방안이다. 이것은 개별 결과를 어떻게 표현할 것인가에 관한 것이지 직접적으로 어떻게 안전요구사항을 도출할 것인가에 관한 것은 아니라고 할 수 있다.

2.3 연구 목표 및 범위

본 논문에서는 앞서 분석한 선행연구 결과들의 부족한 점을 보충하여 안전표준에 따른 안전요구사항 도출 방법에 대해 제안한다. 설계초기 기능 식별 및 분석 결과를 바탕으로 한 위험 분석 방법, 이 결과를 활용한 안전요구사항의 도출 방법에 대해 제시한다. 이를 통해 시스템 설계정보를 활용하여 어떻게 위험 분석을 수행하는지 그리고 이결과로부터 어떻게 안전요구사항을 도출 할 것인지에 대한 방법을 제안하였다. 이것은 안전표준에서 제시하고 있는 안전수명주기에 대한 구체적인 방법의 제시라 할 수 있다. 그리고 제시된 방법을 대표적인 안전중시 시스템인 철도시스템에 적용하여 사례분석을 수행하였다. 철도시스템을 구성하는 것 중 역사에 대해서 개념

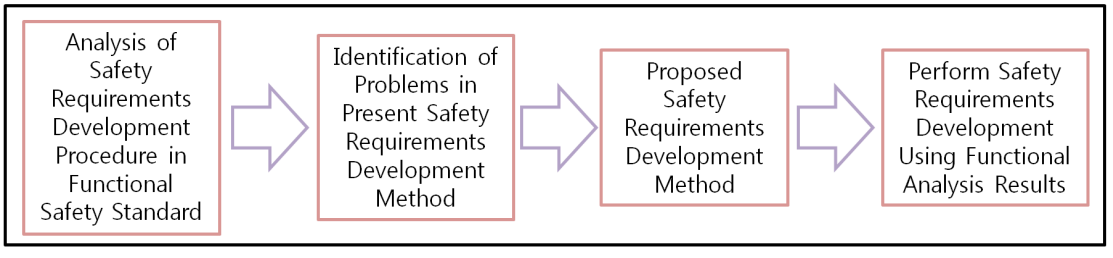

Fig. 2. Concept Model for Current Research

설계결과를 활용하여 안전요구사항의 도출을 수행하였다. 본 논문에서 제시하고 있는 연구 개념은 <Fig. 2>와 같다.

3. 기능분석 결과에 기반을 둔 위험 분석 및 안전요구사항 도출

3.1 안전요구사항 도출 절차

본 논문에서 제안하는 안전요구사항 도출 절차는 <Fig. 3>와 같다. <Fig. 3>와 같이 기능 분석, 위험원 분석, 안전요구사항의 도출의 순서로 수행하게 된다. 설계 초기 기능 분석을 수행하게 되면 식별된 기능들과 기능의 거동정보 등이 도출된다. 이것을 위험원 분석 수행의 입력으로 활용한다. 이를 통해 설계초기에 식별 가능한 시스템 수준에서의 위험원을 도출 할 수 있다. 또한 식별된 위험원 들의 위험을 평가하여 Risk Matrix상에서 분석하게 된다. 이 두 가지 결과를 기반으로 하여 안전요구사항을 도출한다. 안전요구사항은 위험원 분석 결과 위험의 감소가 필요한 위험원들에 대하여 도출하게 된다. 위험을 감소시키기 위해 필요한 추가적인 기능에 관한 것이 안전요구사항의 주요 항목이다.

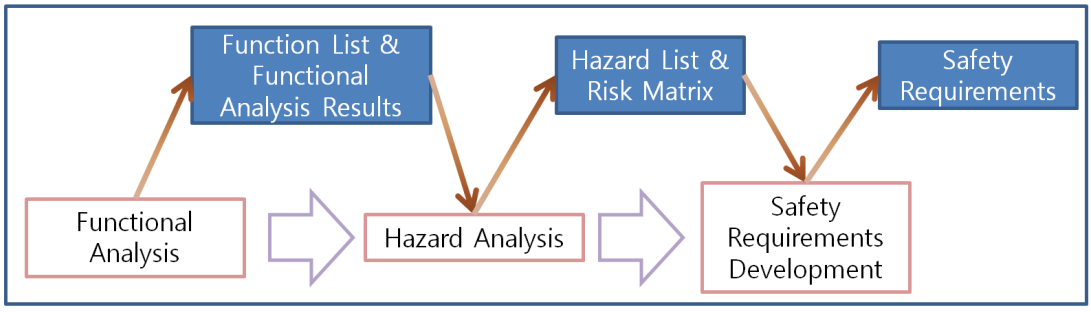

Fig. 3. Safety Requirements Development Process

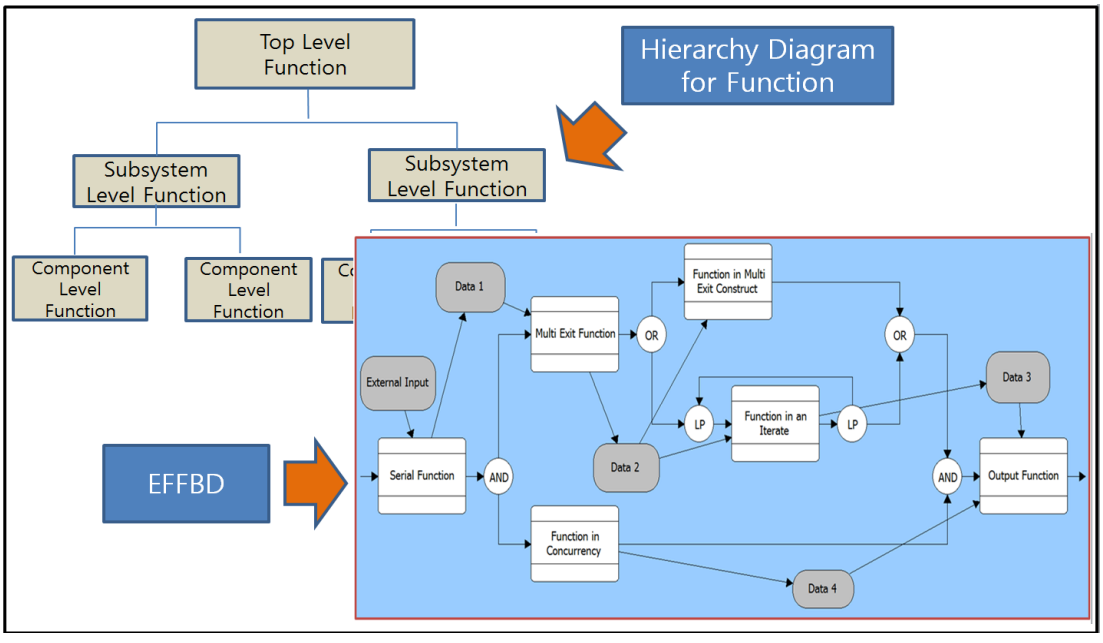

Fig. 4. Hierarchy Diagram & EFFBD Example

3.2 모델기반의 기능분석의 수행 및 이에 기반을 둔 위험원 분석의 수행

3.1절에서의 설명과 같이 기능 분석의 결과를 활용하여 요구사항을 도출하는 것을 본 논문에서는 제안한다. 이를 위해 두 가지의 모델을 기능분석에 활용하였다. 먼저 기능을 식별하고 기능구조를 분석하기 위해 <Fig. 4>의 hierarchy diagram을 활용하였다. 요구사항의 분석을 통해 식별된 최상의 수준의 기능으로부터 시작하여 기능을 분해해 나가면서 시스템 수준에 따른 기능을 식별 한다. 여기서 식별된 각각의 기능이 오류, 오작동을 행하는 경우를 위험원으로 식별한다. top-level 기능부터 component level 기능까지 식별하고 식별된 기능에 대한 위험원을 분석하는 것이다. 다음으로는 enhanced functional flow block diagram(EFFBD)를 활용하였다.

EFFBD를 활용하여 식별된 기능들이 어떤 순서로 수행이 되는지, 기능들 간에 데이터 교환은 어떻게 이뤄지는 지를 분석 할 수 있다. 이를 통해 기능의 오류가 다른 기능에 어떤 영향을 미치는지를 분석 할 수 있으며 이것은 개별 기능의 오류만이 아닌 다른 기능에 의한 오류까지 분석할 수 있게 한다. 이 두 가지 모델을 활용하여 수행한 기능분석의 결과를 활용하여 위험원 분석을 수행하게 된다.

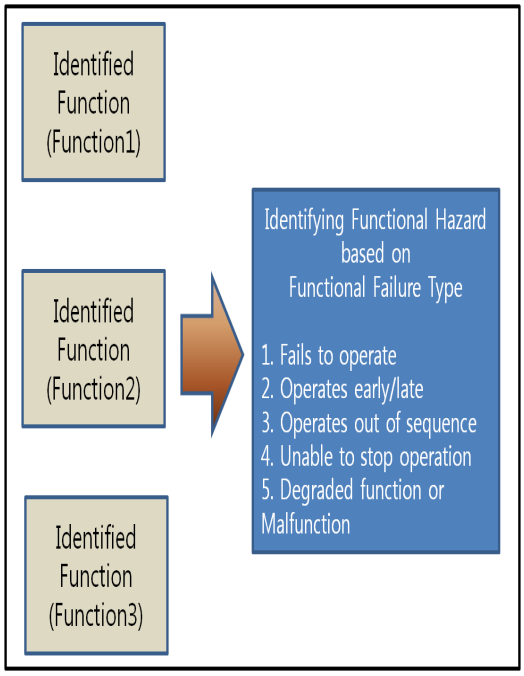

Fig. 5. Concept for Functional Hazard Identification

기능 위험원의 식별 개념은 <Fig. 5>와 같다. 식별된 개별 기능에 대해 기능 고장 유형에 기반을 두어 기능 위험원을 식별한다.

위험원을 식별하고 난 후 식별한 기능 위험원들에 대해 위험평가를 수행하게 된다. <Fig. 6>는 본 연구에서 활용한 risk matrix이다. Risk matrix의 빈도와 심각도는 대표적인 철도안적규격인 EN 50128 및 철도사고 통계 자료를 기반으로 작성하였다. 위험은 빈도와 심각도로 평가를 하게 되며 risk matrix의 우상방면에 위치하는 위험원일수록 높은 위험을 가진 위험원이라 할 수 있다. 이와 같이 위험원에 대한 위험평가를 수행해야 안전요구사항의 도출이 필요한 위험원들이 분류된다. 모든 위험원에 대하여 안전 요구사항을 도출할 필요는 없다. 위험평가 결과 위험이 허용 가능한 수준 이상인 위험원들에 대해서만 위험을 낮추기 위한 안전요구사항을 도출하게 된다.

3.3 위험분석 결과를 활용한 안전요구사항 도출

3.1, 3.2절을 통해 기능분석 결과를 활용한 위험원 분석 방법에 대해 제시하였다. <Figure 3>에서 제시하였듯이 위험분석 이후 최종적으로 안전요구사항을 도출하게 된다. 위험분석을 수행하게 되면 산출물로 Hazard List와 Risk Matrix가 도출된다. 이 두 가지를 활용하여 안전요구사항을 도출한다. Hazard List에 명시된 모든 위험원에 대하여 빈도와 심각도에 기반을 둔 위험평가를 수행한다. 위험평가 수행결과 허용 가능한 위험이상의 위험을 가지는 위험원에 대하여 안전요구사항을 도출한다. 안전요구사항은 허용 가능한 범위를 넘어선 위험을 허용 가능한 수준으로 내리기 위한 기능에 관한 것이 핵심이다. 도출된 안전요구사항들은 향후 시스템의 설계에 반영하여 물리적으로 구현되어 시스템의 위험을 허용 가능한 수준으로 내릴 수 있게 된다.

4. 경전철 역사의 안전요구사항 도출사례

4.1 경전철 역사의 기능 분석

3장에서 모델을 활용한 기능분석 방법에 대해서 제시하였다. 경전철 역사의 사례에 적용하기 위해 hierarchy diagram과 EFFBD를 활용하여경전철 역사의 기능을 분석하였다. 경전철 역사는 크게 신호실, 통신실, 기계실,

전기실로 이뤄져 있다. 각각의 실에서 수행되어야 할 기능들을 분석하며 기능구조를 식별하였다. <Figure 7>은 식별된 기능구조를 나타내고 있다. 이를 통해 경전철 역사에서 수행되어야 할 기능들을 최상위 수준부터 식별하였다. 다음으로는 식별된 기능들의 수행순서와 기능간의 관계를 분석하였다. <Figure 8>은 경전철 역사의 기능들에 대한 EFFBD 이다. 이를 통해 기능들의 수행순서와 기능들 간의 정보교환을 분석하였다. 이와 같이 경전철 역사의 기능분석의 결과로써 기능구조와 기능간의 관계를 식별하였다. 이것을 바탕으로 기능에 대한 위험원을 식별함으로써 최종적으로Hazard List를 도출 할 수 있다.

4.2 경전철 역사의 위험원 분석

경전철 역사의 기능분석 결과를 바탕으로 경전철 역사의 위험원 분석을 수행하였다. <Fig. 7>, <Fig. 8>은 경전철 역사에 대한 기능분석을 수행한 결과이다. 역사에서 수행되어야 할 기능을 식별하였고, 기능들 간의 순서 및 상호관계에 대해서 분석하였다. <Table 1>은 경전철 역사의 기능에 대한 hazard list이다. 식별된 위험원들은 기능분석 결과와 3.2절에서 제시한 것과 같이 기능에 대한 failure type을 근거로 하여 경전철 역사에서 수행되어야 할 기능에 대한 위험원을 식별하였다. 이것은 역사의 물리적 구성품의 고장을 기반으로 식별하던 위험원과는 다른 것이다. 기존의 경우 경전철 역사의 위험원

	Negligible	Minor	Moderate	Significant	Severe
Very Likely (81~100%)	Low Medium	Medium	Medium High	High	High
Likely (61~80%)	Low	Low Medium	Medium	Medium High	High
Possible (41~60%)	Low	Low Medium	Medium	Medium High	Medium High
Unlikely (21~40%)	Low	Low Medium	Low Medium	Medium	Medium High
Very Unlikely (~20%)	Low	Low	Low Medium	Medium	Medium

Fig. 6. Risk Matrix

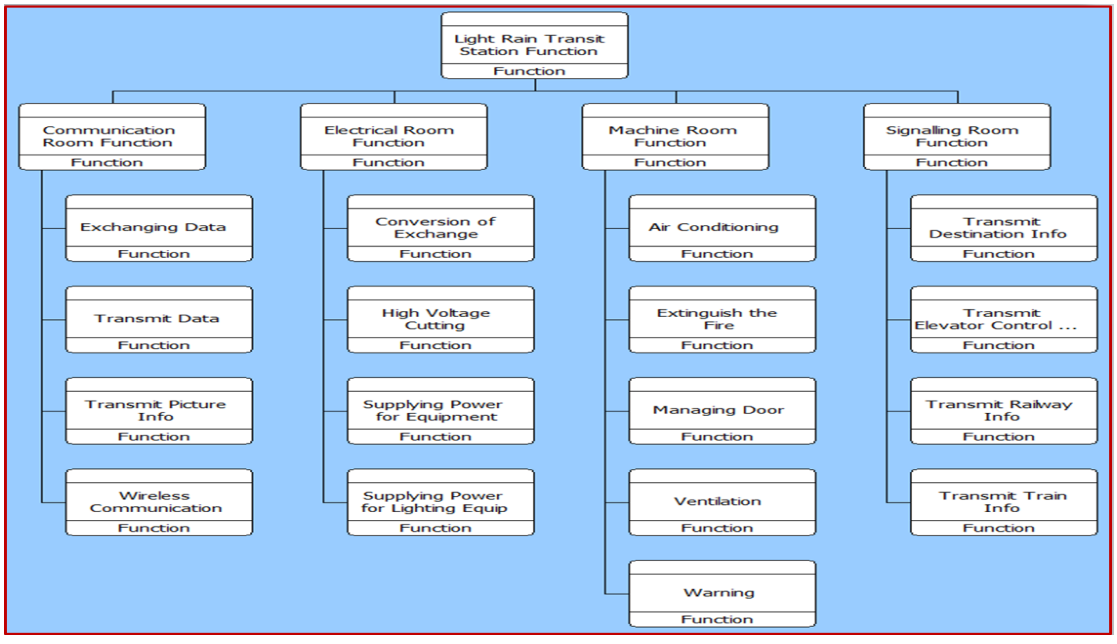

Fig. 7. Hierarchy Diagram for LRT Station

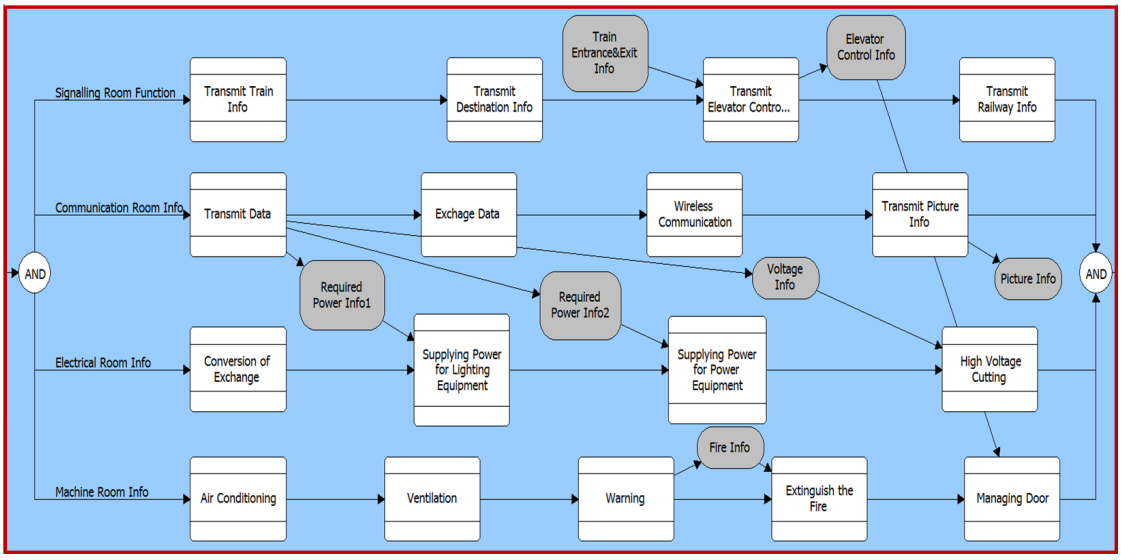

Fig. 8. EFFBD for LRT Station

은 신호실 랙의 구성품의 고장, 기계실 공조기의 고장, 스크린도어의 오작동 등과 같이 물리적인 구성품의 고장에 의한 것이었다. 이러한 것들은 기존의 구성품에 대한 고장데이터가 확보되거나 설계가 물리아키텍처의 도출까지 수행되어야 식별할 수 있다. 그러나 본 논문에서 제시한 온전히 기능분석 결과를 활용하여 식별한 위험원들은 개념설계 초기 설계 결과를 활용하여 식별되는 것이므로 설계초기부터 안전성을 고려한 설계를 수행 할 수 있게된다. 이와 같이 설계초기에 기능 기반으로 위험원이 분석되면 이것을 실제 물리적 구성품으로 구현할 때 식별된 위험원을 방지하기 위한 설계를 수행하여 안전을 확보 할 수 있다.

<Table 1>과 같이 식별된 위험원들에 대한 위험평가를 수행하였다. 개별 위험원들에 대해 빈도와 심각도를 바탕으로 위험평가를 수행했다. 이때 빈도 및 심각도는 철도사고 통계에 기반을두어 평가되었다. <Fig. 9>은 경전철 역사 위험원에 대하여 위험평가를 수행한 결과이다. 평가결과 식별된 위험원들은 Medium High, Medium, Low Medium 세 분류에 속한 것으로평가되었다. Risk Matrix의 심각도는 정량적인 기준을 도출하기 힘들지만 빈도의 경우 철도사고 통계자료에 따르면 risk matrix의 very unlikely는 사고발생확률이10^{-8} ~10^{-9},

Table 1. Hazard List for LRT Station

Function of LRT Station	Hazard List
Transmit Data	1. Data transfer disabled
	2. Incorrect data transfer
	3. Speed control disabled due to incorrect speed information
	4. Not maintain the distance between the train
Exchanginmg Data	5. Incorrect information exchange
	6. Control room can not communicate with train
Wireless Communication	7. Wireless communication disabled with headquarters
	8. Incorrect data transfer
High Voltage Cutting	9. Excessive voltage supply
	10. Supply voltage of less than required
Managing Door	11. Open door at the wrong time
	12. Can not close the door after the boarding
Transmit Railway Info	13. Can not be aware of the exact location of the train
	14. Can not pass through block section
Transmit Train Info	15. Not check the distance between the train
	16. Numerical errors of the distance between the train

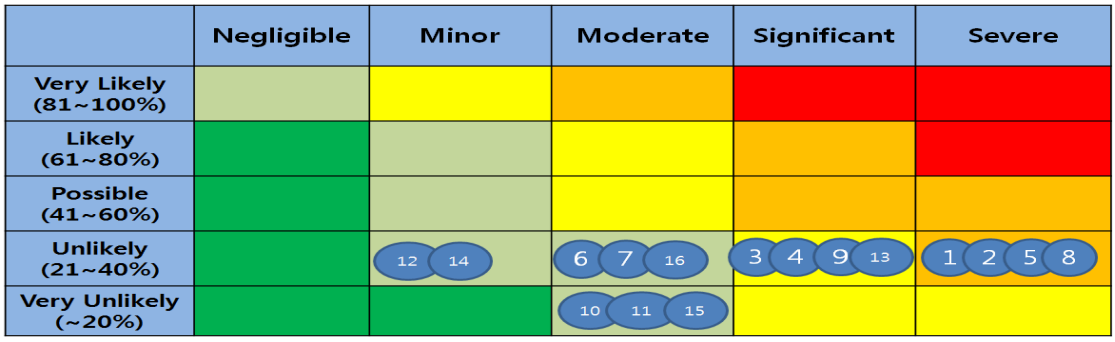

Fig. 9. Risk Matrix for LRT Station

unlikely는 10^{-6} ~10^{-7}로 정의가 된다. 이러한 사고 발생확률을 기반으로 위험원을 평가하였을 때, High 수준의 위험을 가지는 위험원은 없었지만 철도와 같은 안전중시 시스템들은 Medium High 이상의 위험에 대해서는 위험을 낮추기 위한 노력을 수행해야 한다.

4.3 경전철 역사에 대한 안전요구사항 도출

<Figure 9>의 위험평가 결과를 바탕으로 안전요구사항을 도출하였다. 철도와 같은 안전중시 시스템들은 Medium High이상의 위험에 대해서는 위험을 낮추기 위한 노력을 수행해야 한다. 따라서 Medium High 영역에 있는 4가지 위험원들에 대하여 안전요구사항을 도출하였다. <Table 2>는 안전요구사항을 도출하여 Hazard List에 반영한 결과이다. 데이터 전송과정에서 통신연결이 끊기는 경우, 잘못된 데이터가 전송된 경우, 데이터 교환에 오류가 발생한 경우 등이 이에 속한다. 이러한 위험원들은 실제 발현되었을 때 철도 역사에서 입출입 관리를 수행하게 되는 열차의 사고를 유발할 확률이 높다. 따라서 이러한 위험원이 발현되었을 때 이것을 다시 안전한 상태로 되돌리기 위한 기능에 관해 안전요구사항을 도출하였다. 이러한 안전요구사항은 식별된 위험원이 발현되지 않도록 하는 안전목표를 결정하고 안전목표를 달성할 수 있도록 하는 기능 요구사항을 식별한 결과이다. 즉 위험원이 발현되지 않도록 하는 기능이 설계에 반영될 수 있도록 이러한 기능에 관한 요구사항을 식별한 것이다.

Table 2. Adding Safety Requirements to Hazard List for LRT Station

Function of LRT Station	Hazard List	Risk	Safety Requirements
Transmit Data	1. Data transfer disabled	Med Hi	Communication automatically need to reconnect when it is disconnected.
	2. Incorrect data transfer	Med Hi	Perform data inspection when receiving the information
	3. Speed control disabled due to incorrect speed information	Medium	
	4. Not maintain the distance between the train	Medium	
Exchanginmg Data	5. Incorrect information exchange	Med Hi	When exchanging the data, it is necessary to inspect the information to each other
	6. Control room can not communicate with train	Low Med	
Wireless Communication	7. Wireless communication disabled with headquarters	Low Med	
	8. Incorrect data transfer	Med Hi	Perform data inspection when receiving the information
High Voltage Cutting	9. Excessive voltage supply	Medium	
	10. Supply voltage of less than required	Low Med	
Managing Door	11. Open door at the wrong time	Low Med	
	12. Can not close the door after the boarding	Low Med	
Transmit Railway Info	13. Can not be aware of the exact location of the train	Medium	
	14. Can not pass through block section	Low Med	
Transmit Train Info	15. Not check the distance between the train	Low Med	
	16. Numerical errors of the distance between the train	Low Med	

5. 결론

본 논문의 목표는 설계초기 기능분석결과를 활용하여 안전요구사항을 도출하는 방법을 제시하는 것이다. 이를 달성하기 위해 다음과 같은 연구수행결과를 도출하였다.

첫째, 기능분석 결과를 활용하여 위험원 분석을 수행하는 방법을 제시하였다. 개념설계의 결과 중 하나인 기능분석 결과를 활용하여 시스템 수준에서 위험원을 식별하였다.

둘째, 식별된 위험원들에 대하여 위험평가를 수행하여 안전요구사항의 도출이 필요한 위험원을 식별하였다.

셋째, 위험원 분석 결과를 활용하여 위험의 감소가 필요한 위험원들에 대하여 위험을 줄이기 위한 안전요구사항을 도출하였다.

이와 같이 본 논문에서 제시한 방법은 물리적 고장이 아닌 시스템이 수행해야 할 기능의 오류, 오작동등으로 인한 위험을 설계 초기에 미리 식별하고 이를 허용 가능한 위험내에 존재 할 수 있도록 안전요구사항을 도출하는 방법에 대하여 제시하였다. 이를 기반으로 위험에 대응하기 위한 설계를 설계초기부터 반영해 나갈 수 있다. 이것은 향후 설계과정에서 재설계의 가능성을 줄여 시간 및 비용의 초과를 방지 할 수 있게 한다. 이것은 안전요구사항을 설계초기에 도출해야 하는 중요 이유였으며 본 논문에서 제시한 방법을 통해 달성 할 수 있다. 이것은 안전 표준을 충족시키는 안전요구사항 도출 방법이며 기존에 안전측면에서 단독적으로 수행되는 안전요구사항의 도출이 아닌 시스템의 설계와 연계하여 안전요구사항을 도출하는 방법이라 할 수 있다.

References

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

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

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

[4] K. G. Lough, "The risk in early design method," Journal of Engineering Design, vol. 20, no. 2, pp. 155-173, Mar. 2009.
DOI: http://dx.doi.org/10.1080/09544820701684271

[5] M. H. Ordouei, A. Elkamel, and G. Al-Sharrah, "New simple indices for risk assessment and hazard reduction at the conceptual deisgn stage of a chemical process," Chemical Engineering Science, vol. 119, pp. 218-229, Nov. 8, 2014.
DOI: http://dx.doi.org/10.1016/j.ces.2014.07.063

[6] C. Raspotnig and A. Opdahl, "Comparing risk identification techniques for safety and security requirements," Journal of Systems and Software, vol. 86, no. 4, pp. 1124-1151, Apr. 2013.
DOI: http://dx.doi.org/10.1016/j.jss.2012.12.002

[7] K. Beckers, I. Cote, T. Frese, D. Hatebur, and M. Heisel, "Systematic derivation of functional safety requirements for automotive systems," in Proc. 33rd International Conference, SAFECOMP 2014, Florence, Italy, Sep. 10-12, 2014, pp. 65-80.
DOI: http://dx.doi.org/10.1007/978-3-319-10506-2_5

[8] Safety Management Manual(SMM), ICAO(International Civil Aviation Organization), 3rd ed., 2013.

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

김 주 욱(Joo-Uk Kim) **[정회원]**

- 2000년 2월 : 고려대학교 전기공학과 (공학사)
- 2011년 2월 : 아주대학교 시스템공학과 (공학석사)
- 2014년 8월 : 아주대학교 시스템공학과 (박사수료)
- 2004년 3월 ~ 현재 : 한국철도기술연구원 광역도시교통연구본부 선임연구원 재직

<관심분야>
철도 시스템엔지니어링, 철도 안전 및 신뢰성

정 호 전(Ho-Jeon Jung) **[정회원]**

- 2010년 8월 : 경북대학교 전자공학과 (공학사)
- 2013년 2월 : 아주대학교 시스템공학과 (공학석사)
- 2013년 3월 ~ 현재 : 아주대학교 시스템공학과 (박사과정)

<관심분야>
시스템공학, 모델기반 시스템공학, 시스템 안전(SystemSafety), 기능안전(Functional Safety), 시스템안전관리체계, Modeling & Simulation 등.

박 기 준(Kee-Jun Park) **[정회원]**

- 1987년 2월 : 아주대학교 기계공학과 (공학사)
- 1989년 2월 : 아주대학교 기계공학과 (공학석사)
- 2011년 8월 : 성균관대학교 기계공학과 (공학박사)
- 1997년 1월 ~ 현재 : 한국철도기술연구원 광역도시교통연구본부 책임연구원 재직

<관심분야>
철도 시스템엔지니어링, 철도 차량 인터페이스, 신뢰성 분석

김 주 락(Joorak Kim) **[정회원]**

- 1997년 8월 : 홍익대학교 전자전기공학과 (공학사)
- 1999년 8월 : 홍익대학교 전기제어공학과 (공학석사)
- 2010년 8월 : 홍익대학교 전기정보제어공학과 (공학박사)
- 2000년 8월 ~ 현재 : 한국철도기술연구원 광역도시교통연구본부 선임연구원 재직

<관심분야>
철도 급전시스템 해석 및 전력품질 평가

한 석 윤(Seok Youn Han) **[정회원]**

- 1983년 2월 : 부산대학교 기계공학과(공학사)
- 2006년 2월 : 성균관대학교 산업공학과(공학박사)
- 1996년 7월 ~ 현재 : 한국철도기술연구원 광역도시교통연구본부 수석연구원 재직

<관심분야>
철도 시스템엔지니어링, 철도 신뢰성 분석, 도시철도시스템 설계

이 재 천(Jae-Chon Lee) **[정회원]**

- 1977년 2월 : 서울대학교 공과대학 전자공학과 (공학사)
- 1979년 2월 / 1983년 8월 : KAIST 통신시스템 (석/박사)
- 1984년 9월 ~ 1985년 9월 : 미국 MIT Post Doc 연구원
- 1985년 10월 ~ 1986년 10월 : 미국 Univ. of California 방문연구원
- 1990년 2월 ~ 1991년 2월 : 캐나다 Univ. of Victoria (Victoria, BC) 방문교수
- 2002년 3월 ~ 2003년 2월 : 미국 Stanford Univ. 방문교수
- 1994년 9월 ~ 현재 : 아주대학교 시스템공학과 정교수

<관심분야>
시스템공학 (SE), Model-Based SE (MBSE), Systems Safety, Systems T&E, Modeling & Simulation