철도제어시스템의 기능안전성 확보를 위한 모델기반 기능위험원 식별

On Model-Based Functional Hazard Identification of Railway Control System to Acquire Functional Safety

정호전*, 김창원*, 이재천*†

Ho-Jeon Jung*, Chang-Won Kim*, Jae-Chon Lee*†

Abstract Achieving functional safety is becoming more important as the proportion of electronic products in the system increases. Especially, the necessity of securing safety is increasing as electronic products are widely used in the control part of the system. Therefore, it is important to identify and analyze functional hazards in order to achieve functional safety of the system. In this paper, we have studied the identification of hazard using the model in the hazard identification stage which is the starting point for securing safety. In particular, we proposed a method to identify the functional hazard based on the model for the railway control system. This will enable the identification of functional hazards in the design process of the system more effectively.

Keywords **:** Railway Safety, Functional Safety, Hazard Identification, Model-Based Approach

초 록 시스템에 전장품의 비율이 증가하면서 기능안전의 달성이 중요시되고 있다. 특히 전장품들이 시스템의 제어부에 많이 활용됨에 따라 안전확보의 필요성이 증대되고 있다. 따라서 시스템의 기능안전의 달성을 위해 기능위험원의 식별 및 분석이 중요시 되고 있다. 본 논문에서는 안전의 확보를 위한 시작점인 위험원 식별단계에서 모델을 활용한 위험원 식별에 관한 연구를 수행하였다. 특히 기능안전의 확보가 필수적인 철도제어시스템에 대하여 기능위험원을 모델기반으로 식별하는 방법을 제안하였다. 이를 통해 시스템의 설계 과정에서 기능위험원 식별을 보다 효과적으로 수행 할 수 있게 될 것이다.

주요어 : 철도안전, 기능안전, 위험원 식별, 모델기반 접근방법

1. 서 론

현대의 안전중시 시스템들은 과거와 비교해서 급격한 운영성능의 발전을 가져 왔고, 동시에 기능적으로도 매우 복잡해지게 되었다. 시스템이 점차 대형화 복잡화됨으로써, 시스템에서 발생할 수 있는 사고나 고장의 위험 또한 증가하고 있다. 특히 이런 안전중시 시스템들은 사고나 고장이 인명 및 재산피해로 직결되기 때문에 체계적인 안전관리가 필요하다[1][2]. 이에 따라 철도, 항공, 해양, 원자력 등의 산업분야에서는 안전관리체계에 대한 표준 및 매뉴얼을 제정하여 체계적인 안전관리 활동을 수행 할 수 있는 바탕을 제공하고 있다.

† 교신저자: 아주대학교 시스템공학과(jaelee@ajou.ac.kr)
* 아주대학교 시스템공학과

대표적인 대형복합 시스템인 철도분야에서도 철도 안전을 위한 표준인 EN 50128, IEC 62279등을 제정하여 안전을 달성 할 수 있도록 하고 있으며, 체계적인 안전관리를 위한 절차를 제안하고 있다.

또한 현대의 시스템에서 전장품 및 소프트웨어가 차지하는 비중이 증가함에 따라 기능안전의 중요성이 커지고 있다. 특히 전장품 및 소프트웨어들이 시스템의 제어에 대부분 활용됨에 따라 시스템의 안전과 직결되어 시스템의 기능안전을 확보하는 것이 매우 중요해졌다.

이처럼 중요시되고 있는 기능 안전의 확보를 위해 제시되고 있는 많은 표준규격에서 안전을 위한 첫걸음으로 제시하고 있는 것이 위험원 분석(Hazard Analysis)과정이다. 위험원 분석은 시스템에 내재되어 있는 위험원들을 식별하고, 향후 위험원에 의해 발현될 위험들을 미리 예상하고 평가하여, 이에 대한 대응을 수립하는 것을 포함하는 과정이다. 안전관련 표준에서는 위험원 분석을 시스템 개발의 초기에 수행함으로써 목표로 하는 안전수준에 도달할 수 있다고 제시하고 있다[3].

기능안전표준에서 제시하고 있는 안전관리절차의 목표는 위험을 식별하고 허용 가능한 범위 내에서 통제하는 것을 의미한다. 이에 따라 기능안전표준에서는 안전 수명주기에서 위험원 분석절차를 포함하고 있으며, 위험원 분석단계에서 사고 및 고장의 근본 원인인 위험원을 식별하고, 향후 발생 할 수 있는 위험에 대한 대응책을 수립하도록 제시하고 있다.

기능안전 표준에서 제시되고 있는 위험원 분석 절차를 분석해보면 대상 시스템을 분석하는 것에서 시작하여, 위험원을 식별하고, 식별된 위험원을 평가하고, 위험원에 의해 발현될 위험을 평가하고 통제하는 단계 등을 포함하고 있다. 즉 기능안전표준에서 정의하는 위험원 분석은 개발되는 시스템에 내재하고 있는 잠재적 위험원을 찾아 제거하거나 위험원으로 인해 발생하는 위험을 허용수준 이하로 줄일 수 있도록 대책을 수립하는 것이다. 또한 이를 시스템의 설계 및 개발에 반영하도록 하는 모든 일련의 활동을 의미한다[4].

이와 같이 기능안전표준들에서는 시스템의 개발에 따라 안전 활동을 수행하여 안전의 확보를 달성 할 수 있도록 제안하고 있다. 더불어 이러한 안전 활동의 핵심이자 첫 단계로써 위험원 분석단계를 제시하고 있다. 따라서 시스템의 안전의 확보를 위해서는 대상 시스템에 대한 체계적인 위험원 분석이 매우 중요하다. 이를 위해 모델링 기법을 위험원 분석에 활용하는 연구들이 수행되고 있다[5].

2. 위험원 분석 단계에서 모델링 기법의 활용

2.1 위험원 분석 절차 및 활동

위험원 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 위험원을 식별하고 분석하는 단계를 포함하며 이것이 바로 위험원 분석단계이다. 위험원 분석 단계는 대상 시스템을 정의 및 분석하는 것에서 시작한다. 이 후 위험원을 식별하고, 식별된 위험원을 평가하는 과정을 거친다. 위험원 평가 결과를 바탕으로 위험

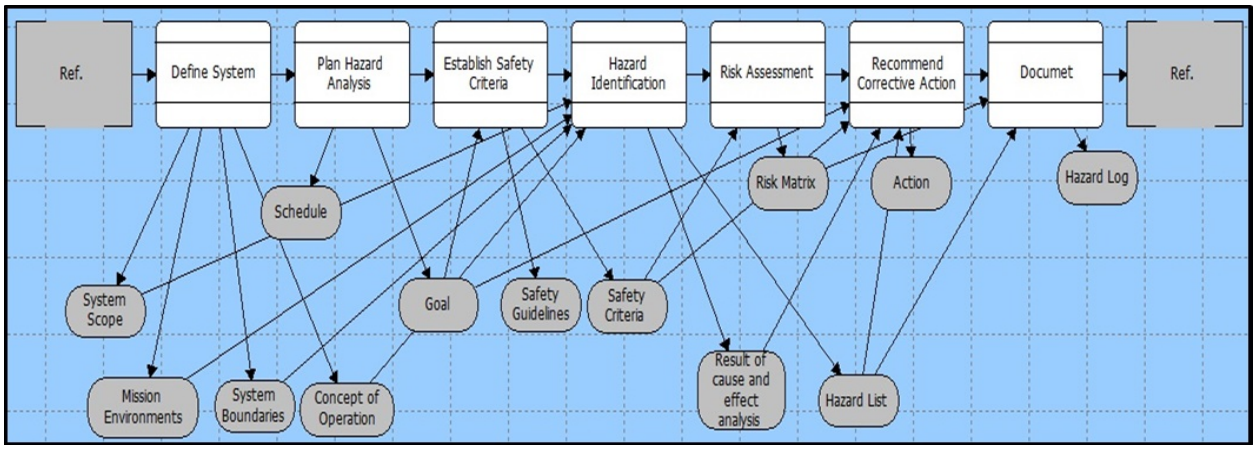

Fig.1 Hazard Analysis Process Model

원에 의해 발현될 위험을 평가하고 통제하는 단계를 거치며, 위험원 분석에 대한 검증 및 모니터링 과정을 포함한다. 위험원 분석 절차 및 활동은 [Fig.1]과 같다. 위험원 분석 프로세스 모델을 통해 세부 활동들에 필요한 데이터와 활동을 통해 도출되는 데이터들을 식별하였다.

2.2 위험원 식별 단계에서 모델링 기법을 활용한 기능위험원의 식별

위험원의 식별을 위해 다양한 방법 및 기법들이 활용되고 있다. 이 중 시나리오 기반의 위험원 식별 방법은 정상상태에서의 시나리오를 생성한 후 정상상태에서 벗어나게 하는 위험원들을 식별하는 방법이다. 이는 부품 및 장치수준이 아닌 상위수준에서의 위험원 식별과정에 유용하게 활용 할 수 있다. 상위수준에 시스템의 운영에 관한 시나리오를 생성하여 위험원을 분석함으로써 시스템을 정상상태에서 벗어나게 하는 위험원들의 식별이 이뤄진다.

운영시나리오를 생성하는데 다양한 모델링 기법들이 활용된다. 대표적인 기법중 하나가 SysML이다. SysML은 시스템 모델링 언어로써 시스템을 구현할 때 효과를 발휘하는 모델링 언어이다. SysML은 시스템의 분석, 설계, 확인/검증을 위해 사용 할 수 있다. SysML에서 지원하는 다양한 다이어그램을 활용하여 시스템의 운영 시나리오를 생성 할 수 있다. 시스템의 운영을 표현하는데 적절한 다이어그램은 Activity Diagram이다. [Fig.2]와 같이 Activity Diagram은 시스템이 운용되는 과정을 순차적으로 표현 할 수 있다. 따라서 Activity Diagram을 활용하여 시스템의 정상상태에서의 운영과정을 모델링하여 시나리오를 작성 할 수 있다. 이를 기반으로 운용과정에서 정상상태를 벗어나게 하는 위험원들의 식별이 가능하다.

[Fig.2]와 같이 정상상태에서의 운영시나리오가 작성되면 이를 기반으로 위험원의 식별을 수행한다. 먼저 시나리오상에 표기된 Activity들이 정상적으로 수행될 수 없는 상황들을 가정한다. 이런 것을 HAZOP과 같은 Hazard Analysis Technique에서는 Deviation이라 표현한다. 즉 정상상태에서 벗어난 상태라는 의미이다. 이 때 정상상태를 벗어난 상태로 식별된

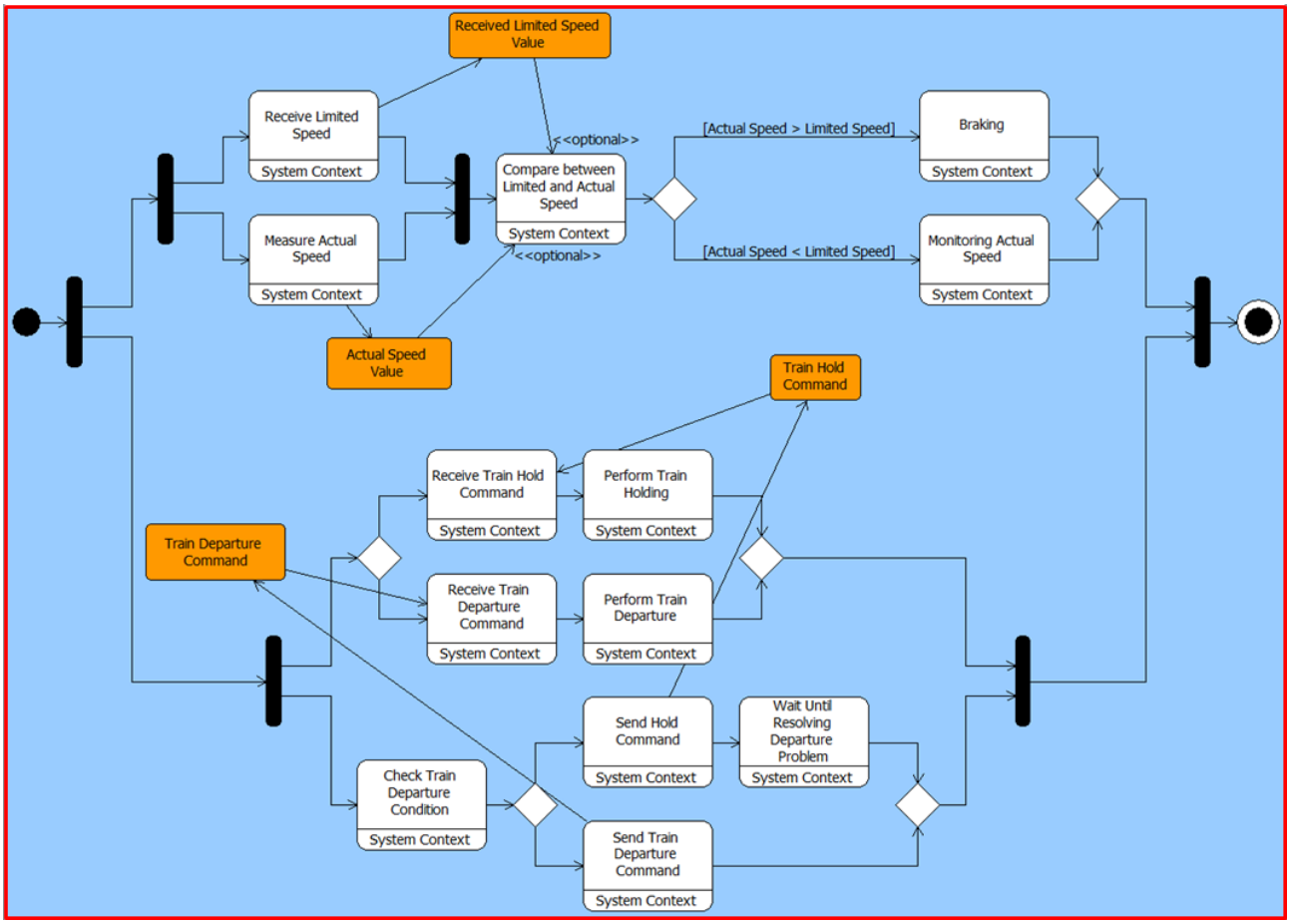

Fig. 2 Normal Operation Scenario Model

상황들이 시스템의 운영과정에서의 위험원이라 할 수 있다. 이와 같이 위험원을 식별한 후에는 이것의 원인과 영향을 분석한다. 이를 통해 위험원을 발현하여 리스크를 발생시키게 하는 원인과, 리스크가 발생했을 때의 영향에 대해 파악 할 수 있다. 이와 같은 과정이 운영시나리오로부터 위험원을 식별하는 과정이라 할 수 있다.

시나리오 분석을 통해 식별할 수 있는 위험원들은 기능의 failure이다. 기능의 failure를 식별하는 것은 단순히 기능이 수행되지 않았을 때 만을 의미하는 것은 아니다. 다음과 같이 6가지의 failure type을 활용하여 누락없이 functional failure를 식별 할 수 있도록 한다.

1) Fails to operate
2) Operates early/late
3) Operates out of sequenece
4) Unable to stop operation
5) Degraded function or Malfunction

앞서 생성한 정상상태의 운영시나리오 모델과 functional failure type을 활용하여 기능 위험원을 식별할 수 있다.

3. 결론

시스템에 전장품의 비율이 증가하면서 기능안전의 달성이 중요시되고 있다. 특히 전장품들이 시스템의 제어부에 많이 활용됨에 따라 안전확보의 필요성이 증대되고 있다. 따라서 시스템의 기능안전의 달성을 위해 기능위험원의 식별 및 분석이 중요시 되고 있다. 본 논문에서는 안전의 확보를 위한 시작점인 위험원 식별단계에서 모델을 활용한 위험원 식별에 관한 연구를 수행하였다. 특히 기능안전의 확보가 필수적인 철도제어시스템에 대하여 기능위험원을 모델기반으로 식별하는 방법을 제안하였다.

기능위험원을 식별하기 위한 정상상태 시나리오모델의 생성방법, Functional Failure Type의 식별을 수행하였다.

향후에는 기능안전표준에서 제시하고 있는 전체 안전수명주기에 따른 안전활동을 모델기반으로 수행하는 방안에 대한 연구가 필요할 것이다. 이를 통해 전수명주기에 따른 안전활동을 보다 효과적으로 수행할 수 있을 것이다.

참고문헌

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

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

[3] A. Berrado, E. El-Koursi, A. Cherkaoui, and M. Khaddour (2011) A framework for risk management in railway sector: application to road-rail level crossings, The Open Transportation Journal, pp. 34-44.

[4] Rob Alexander and Tim Kelly (2013) Supporting systems of systems hazard analysis using multi-agent simulation, Safety Science, 51(1), pp. 302-318.

[5] J. Langheim, B. Guegan, L. Maillet-Contoz, K. Maaziz, (2010) System architecture, tools and modelling for safety critical automotive applications - the R&D project SASHA , in Proc. ERTS 2010, Toulouse, France,pp.19-21.