철도시스템의 기능안전성 확보를 위한 모델 기반 위험원 분석

On Model-Based Hazard Analysis of Railway Systems to Acquire Functional Safety

정호전*†, 이재천*

Ho-Jeon Jung*†, Jae-Chon Lee*

Abstract As today's systems are getting complex, ensuring safety in the development is becoming important issues in a variety of domains such as rail, aviation, and maritime industries. Although each industry is striving to develop their own safety solution, a common point is that most of the approaches taken so far are based on the concept of function safety, thereby resulting in the international functional safety standard and its derivatives. To meet the functional standard, several processes/tasks need to be performed. One of the core tasks is analysis of potential hazards that might be occurring in the system operation. In this paper the study of the hazard analysis is carried out for the rail systems. Particularly, in doing so, a model-based approach is taken using the models represented by SysML (systems modeling language). The analysis result shall be used to develop necessary safety measures. The model-based approach would be useful in the subsequent development of the rail systems with functional safety.

Keywords **:** Rail Systems, Functional Safety, Hazard Analysis, Model-Based Approach, SysML

초 록 철도, 항공, 해양 등의 산업에서는 각 산업에 적합한 안전관리표준을 수립하여 안전을 확보하기 위해 노력하고 있다. 기능안전 표준을 기반으로 안전을 확보하는데 있어 위험원 분석은 매우 중요하다. 위험원 분석과정을 통해 도출되는 위험원 및 위험이 시스템의 설계과정에서 반영되어야 목표로 하는 안전을 달성할 수 있기 때문이다. 본 논문에서는 안전관리를 위한 시작점이자 중요한 과정인 위험원 분석단계에서 모델링 기법을 활용하는 것에 관한 연구를 수행하였다. 위험원 분석을 위해 필요한 시스템 분석 결과를 모델기반으로 도출하여 이것을 위험원 분석단계에서 활용하는 방법을 제안하였다. 이를 통해 안전표준에서 제시하는 위험원 분석활동을 보다 효과적으로 수행할 수 있게 될 것이다.

주요어 : 위험원 분석, 모델기반 접근, SysML, 기능안전표준

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(getbackers87@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.

이처럼 중요시되고 있는 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 도달 할 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 위험원의 유형 및 위험원 분석 방법

위험원 분석을 통해 식별되는 위험원은 두 가지 유형으로 구분 할 수 있다. 개별 구성요소를 통해 도출되는 위험원과 구성요소들 간의 인터페이스 상에서 식별되는 위험원이다. 전자의 경우 대상 시스템을 구조적으로 분석하여 개별 구성요소들을 통해 발생 가능한 위험원을 분석하는 것이다.

기능안전표준들에서는 시스템에 대해 기능분석을 수행하여 기능상에서의 위험원의 식별을 수행하도록 제시하고 있다. 후자의 경우엔 복잡성이 증가하고 있는 현대의 시스템에서 중요성이 점차 커지고 있다. 현대의 시스템은 단일 구성요소로 구성된 것이 아니라 다양한 구성요소들이 서로 상호작용하고 있다. 따라서 구성요소들 간의 상호작용을 가능하게 하는 인터페이스 상에서도 위험원이 존재 할 수 있다. 따라서 인터페이스를 분석하여 이에 대한 위험원을 분석하는 것도 중요하다. 이와 같이 두 가지 유형의 위험원이 시스템에 내재하고

있으며 체계적인 시스템의 분석을 통하여 두 가지 유형 모두에 대한 위험원의 분석이 필요하다.

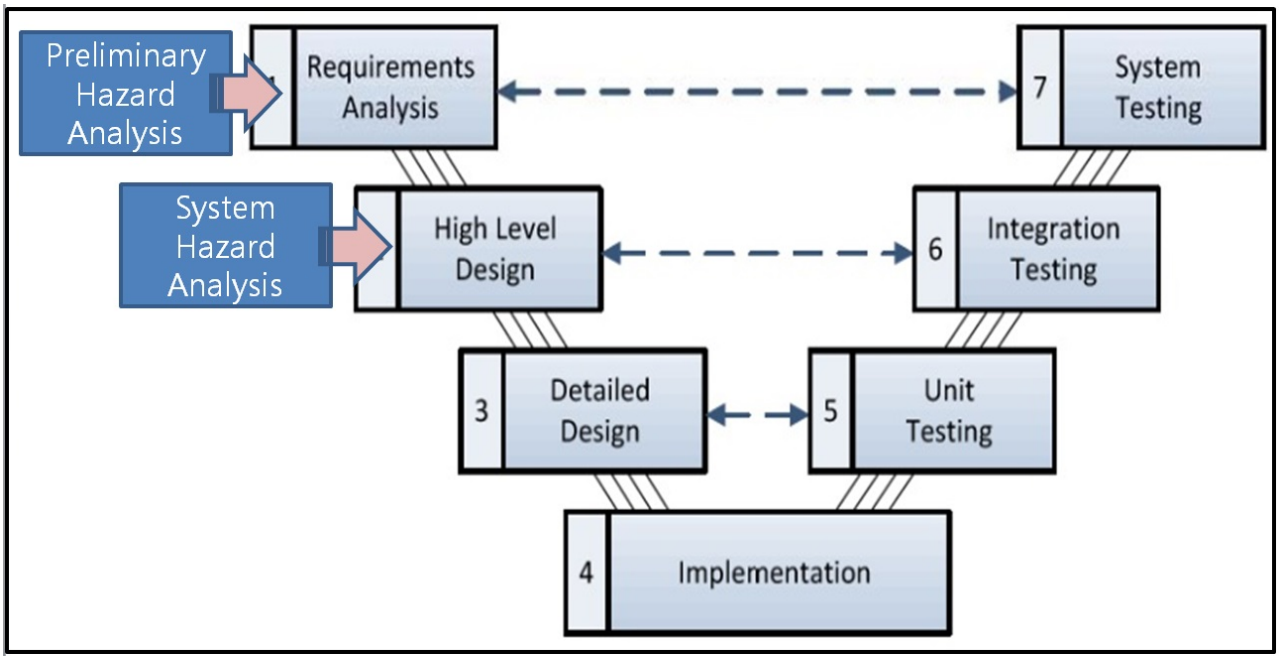

Fig.1 Hazard analysis activities on system development V-model

위험원을 분석하고자 하는 시스템의 계층, 수명주기에 따른 위험원 분석방법이 안전관련 표준에서 제시되고 있다. [Fig.1]은 시스템 개발에 대한 V-model에 PHA와 SHA의 수행시기를 매칭 하여 나타낸 그림이다. 그림과 같이 시스템 설계 초기에 가장 먼저 수행하게 되는 Preliminary Hazard Analysis(PHA)와 이후 시스템 수준에서의 요구사항 및 기능분석 과정에서 수행하게 되는 System Hazard Analysis(SHA)가 있다.

PHA의 경우 대상 시스템을 운용관점에서 분석하여 고장 시나리오 분석을 수행한다. 시나리오 분석을 통해서 대상 시스템이 운용되는 과정에서 발생 가능한 고장을 분석하여 그에 대한 위험원을 식별하는 과정을 수행하여 위험원 분석을 수행한다. PHA는 시스템 설계의 초기에 시스템의 운용개념이 정해지면 그것을 바탕으로 시나리오를 구성하여 위험원 분석에 활용한다. SHA는 시스템의 설계 중 개념설계 단계에서의 요구사항분석, 기능분석 등의 결과를 바탕으로 수행하는 위험원 분석단계이다. 대상 시스템의 대한 정의가 이뤄지면, 시스템에 대한 요구사항 분석, 기능분석이 차례대로 수행하게 된다. 이를 바탕으로 대상 시스템에 대한 구조적인 분석이 가능하여 시스템을 구성하고 있는 구성요소들의 식별이 가능하다. 또한 식별된 구성요소들이 수행하게 되는 기능 또한 식별되며 상위수준의 기능이 하위 수준의 기능으로 분해되어 구성품 수준에서의 기능식별 및 분석까지 이뤄지게 된다. SHA는 식별된 기능들이 제대로 수행되지 않을 경우 발생하게 되는 위험원들을 식별하게 된다. 여기에 덧붙여 상위수준에서 하위수준으로 기능들을 분해하면서 기능들 간의 상호작용에 대해서도 분석이 가능하다. 이를 바탕으로 하여 서로 인터페이스를 가지는 기능들 사이에서 발생 가

능한 위험원들 또한 식별이 가능하다.

이와 같이 시스템 설계 초기 단계부터 PHA, SHA를 수행함으로써 미리 위험원의 식별이 분석이 이뤄지게 되면, 향후 설계 과정 및 운용단계에서 발생 가능한 고장 및 오류에 대한 대응을 적절하게 수행할 수 있게 된다.

2.2 모델링 기법을 활용한 위험원 분석의 수행

앞 절에서 언급했듯이 PHA와 SHA는 시스템의 개발초기부터 수행되어야 할 위험원 분석 절차이다. 또한 적절한 PHA와 SHA를 수행하기 위해서는 대상 시스템에 대한 체계적인 분석이 필요하다. 개념설계 단계에서의 요구사항 분석과 기능분석을 통하여 PHA와 SHA의 수행이 가능하다.

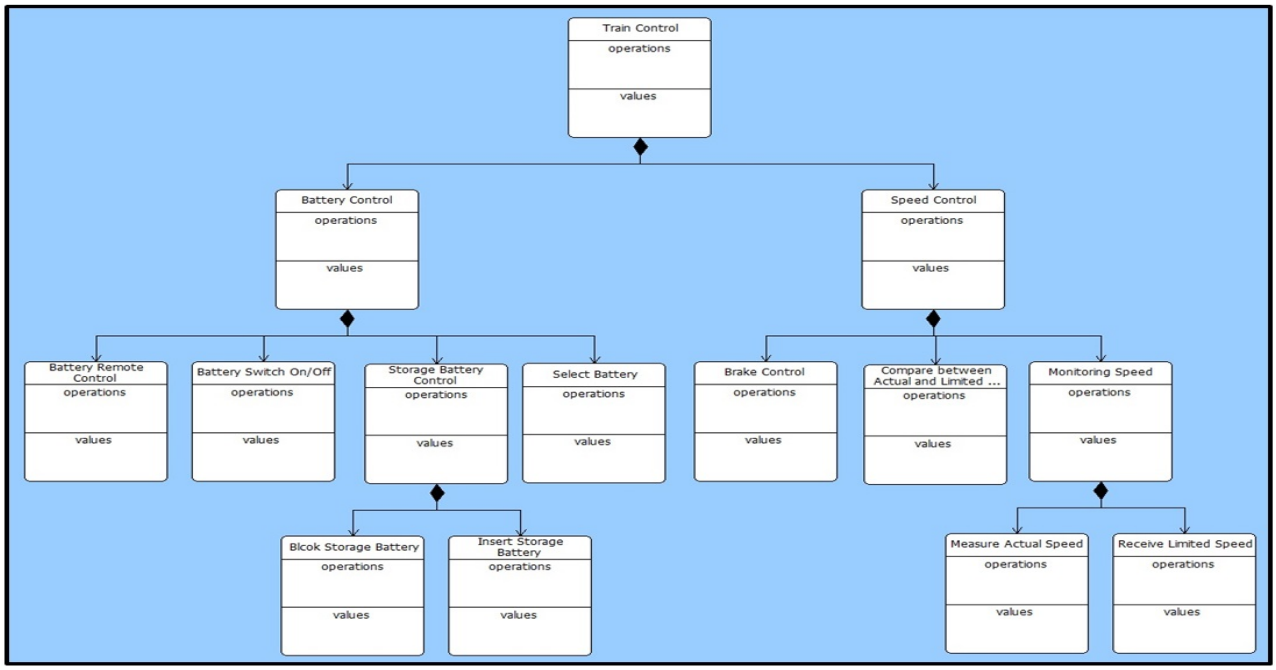

Fig.2 Block Definition Diagram of Train Control System

개념설계 단계에서의 요구사항 분석과 기능분석을 통한 위험원 분석의 첫 단계로 사용자의 needs로부터 요구사항을 도출한다. 그 후 도출된 요구사항을 구현하기 위한 기능들을 식별한다. 마지막으로 식별된 기능이 오류를 일으킴으로 발생 할 수 있는 고장들을 식별한다. 이는 단순히 장치 부품수준에서 개별 장치 및 부품에 대한 고장이 아닌 시스템 수준에서 분석된 고장이라 할 수 있다.

SysML은 여기서 효과적인 기능분석을 수행하기 위해 활용된다. 본 연구에서는 SysML의 여러 Diagram들 중 Activity Diagram과 Block Definition Diagram을 활용하여 기능분석을 수행 하였다. [Fig.2]의 Block Definition Diagram은 Block과 Block간 관계를 정의하기 위

한 Diagram이다. 이는 기능분석을 수행하기 전에 대상 시스템에 대한 정의를 명확히 하는 과정에서 활용하였다. 대상 시스템을 Block Definition Diagram으로 분석함으로써 대상 시스템의 구성요소와 구성요소간의 관계를 식별할 수 있다. 또한 Block Definition Diagram을 활용하여 기능들 간의 Interface를 분석하여 인터페이스 상에서 발생 할 수 있는 위험원에 대해서도 분석이 가능하다. 즉 Block Definition Diagram은 위험원 분석을 수행하기 위한 시스템의 정의과정과 SHA의 수행과정에서 Interface의 분석에 활용하였다.

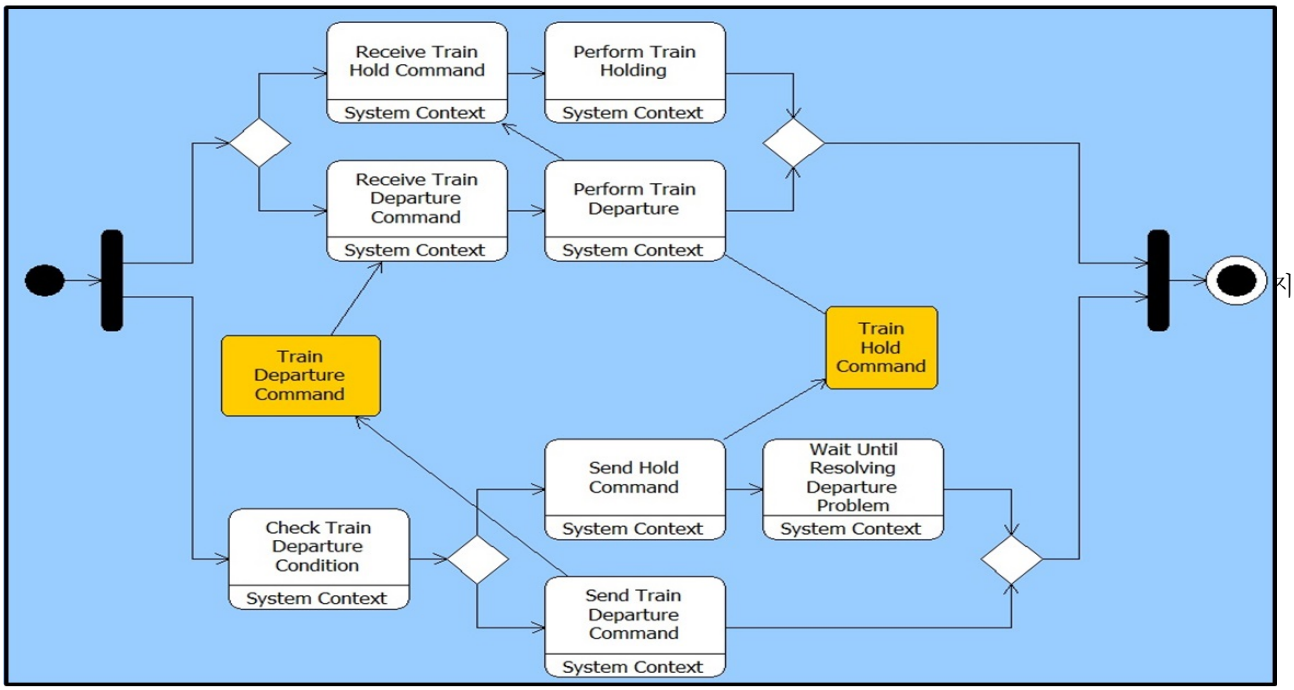

Fig.3 Activity Diagram of Train Start

초기에 PHA를 수행하기 위함으로써 Activity Diagram을 활용한 시나리오 분석을 통해 시스템의 운용상에서 발생 가능한 위험원의 분석이 가능하다. 즉 Activity Diagram은 PHA를 수행하기 위한 시나리오 분석과 SHA를 수행하기 위한 거동분석에 활용하였다.

이와 같이 SysML에서 지원하는 여러 Diagram을 시스템의 분석에 활용함으로써 그 결과를 바탕으로 PHA와 SHA를 수행할 수 있다.

3. 결론

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 소프트웨어의 비중이 높아짐에 따라 기능안전의 중요성이 높아지고 있다. 이에 따라 IEC 61508, ISO 26262, IEC62279 등의 기능안전 표준들

이 제정되어 산업에 적용되고 있다.

본 논문에서는 대상 시스템에 대한 안전을 확보하기 위해 기능안전표준에서 명시하고 있는 위험원 분석을 모델기반으로 수행하는 방법에 관한 연구를 수행하였다. 기능 분석과정에서 SysML을 활용함으로써 개별 기능에 대한 위험원뿐만이 아니라 기능간의 인터페이스 상에서 발생 가능한 위험원들 또한 식별이 가능하였다. 이를 통해 기능안전표준에서 제시하고 있는 시스템 수준에서의 기능안전의 달성이 가능하다.

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.