J. Korea Saf. Manag. Sci. Vol. 16 No. 4 December 2014
http://dx.doi.org/10.12812/ksms.2014.16.4.81

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

철도시스템의 안전성 확보를 위해 안전요건이 반영된 시나리오기반의 위험원 분석에 관한 연구

정 호 전* · 이 재 천*
*아주대학교 시스템공학과

On the Scenario-Based Hazard Analysis with Safety Requirements Incorporated to Assure Railway Safety

Ho Jeon Jung* · Jae-Chon Lee*
Dept. of Systems Engineering, Ajou University

Abstract

Modern systems can be characterized by ever-increasing complexity of both the functionality and system scale. Thus, due to the complexity the chances of accidents resulting from systems failure can then be growing. Even worse is that those accidents could result in disastrous damage to the human being and properties as well. Therefore, the need for the developed systems to be assured with systems safety is apparent in a variety of industries such as rail, automobiles, airplanes, ships, oil refinery, chemical production plants, and so on. To this end, in the industry an appropriate safety standard has been published for its own safety-assured products. One of the core activities included in the most safety standards is hazard analysis. A conventional approach to hazard analysis seems to depend upon the scenarios derived from the ones used previously in similar systems or based on former experience. The objective of this paper is to study an improved process for scenario-based hazard analysis. To achieve the goal, the top-level safety requirements have first been reflected in the scenarios. By analyzing and using them, the result has then lead to the development of safety-assured systems. The method of modeling and simulation has been adopted in the generation and verification of scenarios to check whether the safety requirements are reflected properly in the scenarios. Application of the study result in the case of rail safety assurance has also been discussed.

Keywords : Scenario-Based Hazard Analysis, Safety Assurance, Modeling & Simulation, Safety Requirements

†이 논문은 2014년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. NRF-2012R1A1A2009193)
†Corresponding Author : Prof. Jae-Chon Lee, Dept. of Systems Engineering, Ajou University, Wonchon-dong, Youngtong-gu, Suwon, 443-749, Tel: 031-219-3941, E-mail: jaelee@ajou.ac.kr
Received December 9, 2014; Revision Received December 11, 2014; Accepted December 22, 2014

1. 서론

오늘날 기술의 발전으로 시스템들은 점차 대형화 복잡화 되어가고 있다. 시스템들이 점차 대형화 복잡화 되어감에 따라 사고 및 고장에 대한 위험이 더욱 커지고 있다. 또한 이와 같은 대형 복합 시스템에서 발생하는 사고 및 고장은 바로 큰 재산피해나 인명피해와 직결 될 수 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. 기능안전의 확보가 중요해지면서 과거의 수동적인 안전활동에서 미리 고장 및 위험을 분석하여 예방하는 능동적인 안전활동이 중요시 되고 있다. 이를 위해 각 산업분야에서는 특성에 맞게 기능안전성 규격을 개선하여 안전활동을 수행하려 노력하고 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 위해 제시되고 있는 많은 표준규격에서는 안전을 보장하는 것을 목표로 하고 있으며, 안정보장을 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. 안전보장은 이러한 위험원 분석을 통해 위험원을 식별하여 위험을 최소화함으로써 확보할 수 있다.

기존의 위험원 분석의 개선을 통해 체계적이고 누락 없는 위험원의 분석을 수행하기 위한 연구가 수행되고 있다. 그중 대표적인 분야가 시나리오 기반의 위험원 분석방법에 대한 것이다. 특정 상황별 정상상태의 시나리오를 생성하여 시나리오 상에서 발생 가능한 위험원을 식별해 내는 방법이 시나리오 기반의 위험원 분석이다.

기존의 시나리오 기반의 위험원 분석은 Marco de Bruin 등(2008)과 같이 특정 상황에서 정상상태의 시나리오를 생성한다. 그 후 시나리오 상에서 정상상태를 벗어나게 하는 위험원이 존재하는지를 분석한다. 이러한 방법은 시나리오 기반의 위험원 분석의 가장 기본적인 수행 방법이라 할 수 있다.

이것에서 발전하여 정상상태의 시나리오를 생성하는 방법에 대한 연구가 수행되고 있다. 각종 모델링 기법을 활용하여 시나리오를 생성함으로써 좀 더 체계적인 위험원의 분석을 수행하고자 하는 것이다.

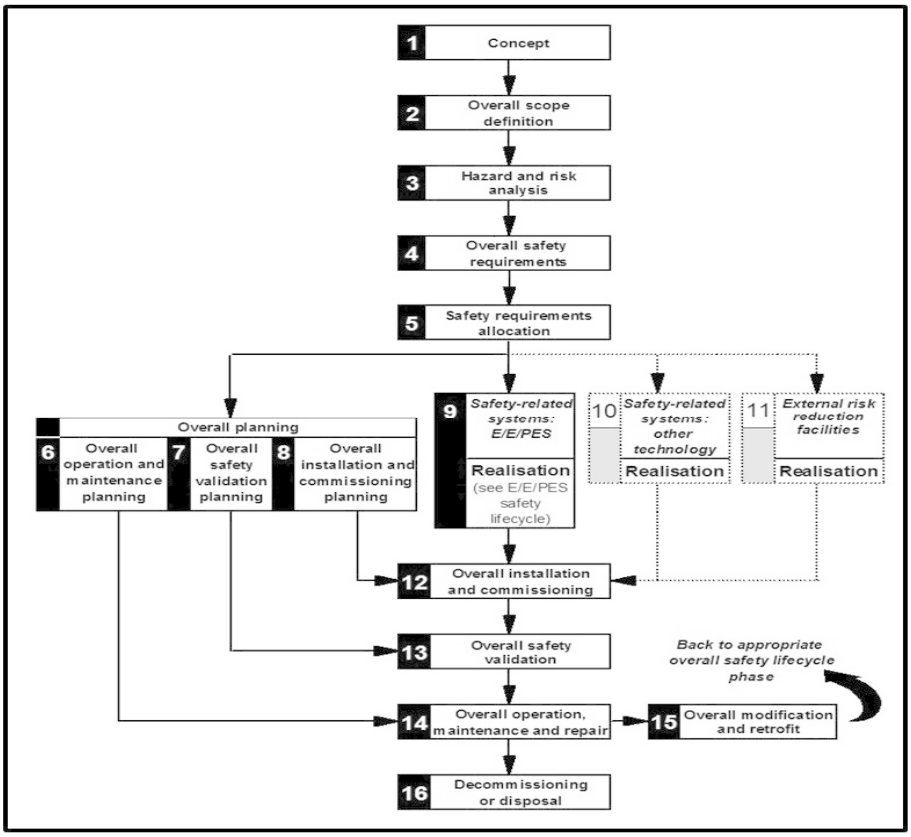
Sybert Stroeve 등(2013)에서 제시하고 있는 시나리오기반의 위험원 분석을 살펴보면 시나리오를 생성하는데 event-tree를 활용하였다. Event-tree를 활용하여 대상에 대한 시나리오를 생성하고 event-tree 상에서 발생 가능한 위험에 대한 분석 및 평가를 수행하였다.

Marco de Bruin 등(2008), Sybert Stroeve 등(2013)에서 볼 수 있듯이 시스템의 위험원 분석에 대하여 시나리오기반의 접근에 대한 연구가 이뤄지고 있으며, 이때 시나리오를 어떻게 생성할 것인가에 대해 초점이 맞춰져 연구가 수행됨을 알 수 있다. 또한 위험원의 생성 과정을 보면 특정 상황에서 기존의 시스템, 유사한 시스템이 어떻게 운영되었는지, 또는 전문가의 경험에 의해 시나리오를 생성함을 확인할 수 있다.

기능 안전표준에서 제시하고 있는 안전활동에서는 먼저 안전 목표를 세우고 이를 달성하기 위한 안전요구사항을 생성하고 이것이 반영된 설계를 수행하도록 제시하고 있다. 따라서 시나리오를 생성하는 과정에서도 기존의 경험에 의한, 유사시스템 및 기존 시스템의 분석을 통한 시나리오의 생성뿐만 아니라 안전요건이 반영된 시나리오를 생성하여 안전목표를 달성하도록 하는 것이 필요하다. 안전요건이 반영된 기능이나, 제약사항들이 시나리오에 반영됨으로써 안전목표의 달성을 위한 위험원 분석을 수행할 수가 있다.

따라서 본 논문에서는 대표적인 안전중시 시스템인 철도시스템에 대하여 안전목표로부터 도출된 안전요구사항을 반영한 시나리오를 생성하고 이를 모델링과 시뮬레이션을 통해 검증한다. 그리고 검증된 시나리오 기반의 위험원 분석을 수행하여 안전성을 확보하는 것에 대해 연구하였다.

본 논문의 구성은 다음과 같다. 서론에서는 사회 및 연구의 연구동향과 필요성을 제시하였고, 2장에서는 관련 선행연구 및 연구 목표를 기술하여 문제정의를 했다. 3장에서는 안전요건이 반영된 시나리오의 생성과 모델링&시뮬레이션을 통한 검증에 대한 방법론을 제시한다. 4장에서는 3장의 활동을 바탕으로 도출된 안전요건이 반영된 시나리오 기반의 위험원 분석 방법에 따른 철도시스템에 대한 위험원 분석 사례를 제시하였다. 5장에서는 본 논문의 결과를 정리 및 요약 하였다.



[Figure 1] Safety life-cycle in functional safety standard [5]

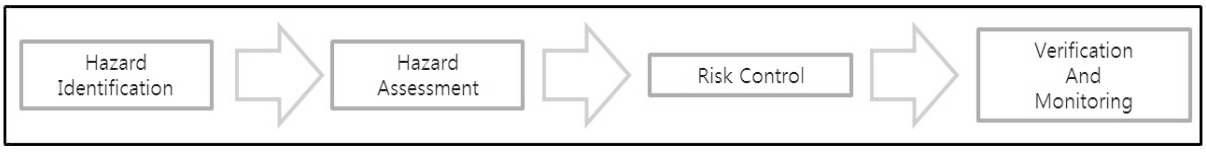
2. 문제 정의

2.1 안정보장을 위한 위험원 분석의 중요성

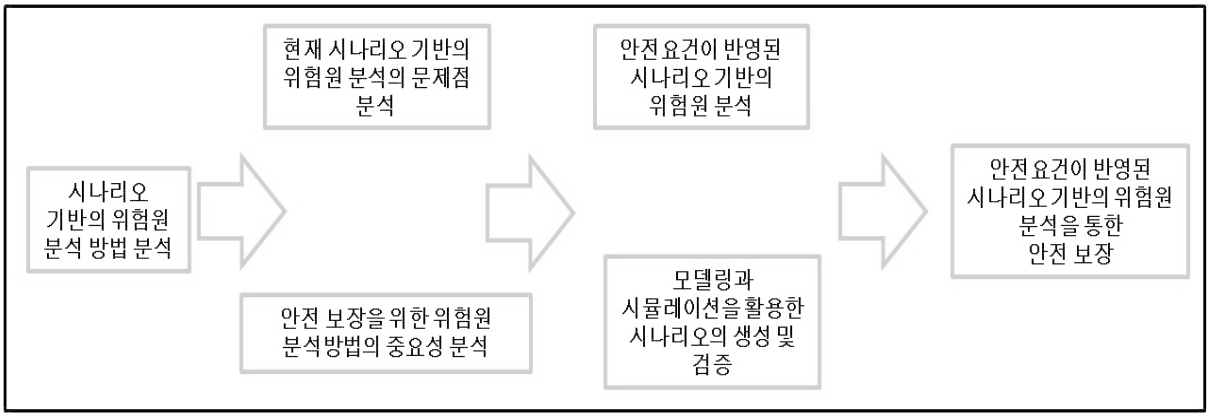
안전보장은 위험원을 식별하고 이것이 발현되었을 때의 위험을 최소화함으로써 확보될 수 있다. 따라서 위험원 분석은 안전 보장을 위해 필수적인 위험원의 식별을 수행하는 중요한 과정이라 할 수 있다. 기능안전 표준에서 제시하고 있는 안전관리절차의 목표는 위험을 식별하고 허용 가능한 범위 내에서 통제하는 것을 의미한다. 이에 따라 [Figure 1]과 같이 기능안전표준에서는 안전 수명주기에서 위험원 분석절차를 포함하고 있으며, 위험원 분석단계에서 사고 및 고장의 근본 원인인 위험원을 식별하고, 향후 발생 할 수 있는 위험에 대한 대응책을 수립하도록 제시하고 있다[3][4].

기능안전 표준에서 제시되고 있는 위험원 분석 절차를 분석해보면 [Figure 2]와 같이 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. 이런 일련의 활동을 통해 안전을 보장하게 된다[6][7].

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.



[Figure 2] Procedure model for safety management.



[Figure 3] Concept diagram for current research

2.2 안전요건이 반영된 시나리오 생성의 필요성

앞 절에서 제시한 것처럼 시스템의 개발에 있어서 안전보장을 위해서는 위험원 분석의 수행이 매우 중요하다. 따라서 기존의 위험원 분석을 개선하기 위한 많은 연구가 수행되고 있다. 그 중 한 분야가 시나리오 기반의 위험원 분석에 대한 것이다.

시나리오 기반의 위험원 분석은 위험원을 식별하기 위해 각 상황별로 시나리오를 생성하여 활용하는 방법이다. 정상상태에서의 시나리오를 생성한 후 정상상태에서 벗어나게 하는 위험원들을 식별하는 것이다.

기존의 시나리오 기반의 위험원 분석 방법들을 분석해보면 시나리오를 생성할 때 기존의 시스템이나 유사시스템을 분석하거나 전문가의 경험을 기반으로 하여 시나리오를 생성하는 경향이 있다. 물론 이와 같은 방법의 시나리오 생성을 통한 위험원 분석은 기본적으로 수행되어야 한다. 그러나 기능안전표준의 도입 이후의 안전에서는 안전목표를 정의하고 이를 충족시키기 위한 안전요구사항의 도출과 이를 설계에 반영하는 것이 매우 중요하며, 표준에서 안전 수명주기 활동을 통해 이를 달성할 수 있도록 제시하고 있다.

따라서 시나리오 기반의 위험원 분석을 수행할 경우 이런 안전 요구사항이 반영된 시나리오를 생성하는 것이 필요하다. 안전 요구사항을 충족시키기 위한 안전 기능의 수행이나 안전의 달성을 위한 제약사항들이 시나리오에 반영됨으로써 안전목표의 달성을 위한 위험원 분석의 수행이 가능하게 된다. 이를 통해 발생 가능한 고장과 위험 중심의 안전활동 뿐만 아니라 시스템의 설계초기에 목표로한 안전목표를 달성하기 위한 안전활동의 수행이 가능하다.

2.3. 연구 목표 및 범위

상위 선행연구 분석을 통해 안전 보장을 위한 위험원 분석단계의 중요성에 대해서 인지하였다. 또한 위험원 분석의 개선을 위해 시나리오 기반의 위험원 분석방법에 대한 연구가 활발히 이뤄지고 있으나 이는 초기에 안전목표를 세우고 이를 달성하기 위한 능동적인 안전활동을 수행하기에는 부족함이 있으며 이를 보완하기 위해 안전요건이 반영된 시나리오 기반의 위험원 분석방법의 필요성에 대해서 제시하였다.

안전요건이 반영된 시나리오를 생성함으로써, 안전기능이나 안전을 위한 제약사항들이 반영된 위험원 분석을 수행하여 안전을 보장하는 것이 본 논문의 연구 목표라 할 수 있다. 본 논문에서 제시하고 있는 연구 개념은 [Figure 3]와 같다.

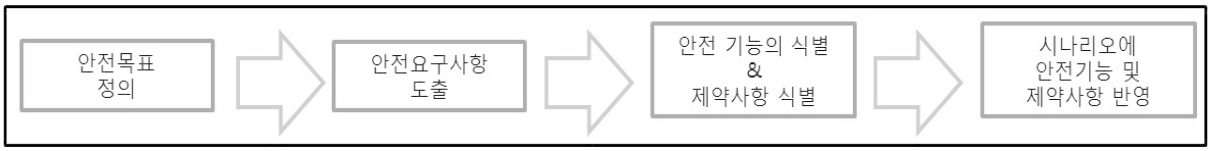
3. 안전요건이 반영된 시나리오기반의 위험원 분석 방법

3.1. 안전요건이 반영된 시나리오의 생성 방안

기능안전표준에서는 안전의 달성을 위해서는 대상 시스템에 대한 안전목표를 설정하고 이를 달성하기 위한 안전요구사항을 생성하며, 생성된 안전요구사항을 충족시키기 위한 설계를 수행해야 한다고 정의하고 있다.

안전목표라 함은 대상시스템에 대하여 요구되는 달성해야 할 안전수준이라 할 수 있다. 대표적으로 기능안전 표준인 ISO 61508에서는 SIL(안전무결성)을 대표적인 안적목표로써 제안하고 있다.

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



[Figure 4] Incorporation of safety requirements in scenarios.

안전 요구사항을 충족시키기 위해 안전기능을 도출하여 수행되도록 할 수도 있으며, 안전 요구사항이 안전을 위한 제약사항으로 제시되고 있다면, 시스템의 설계에 이를 반영할 수 있도록 해야 한다.

따라서 시나리오 기반의 위험원 분석을 수행하는데 있어서 안전요건이 반영된 시나리오의 생성이 필요하다.

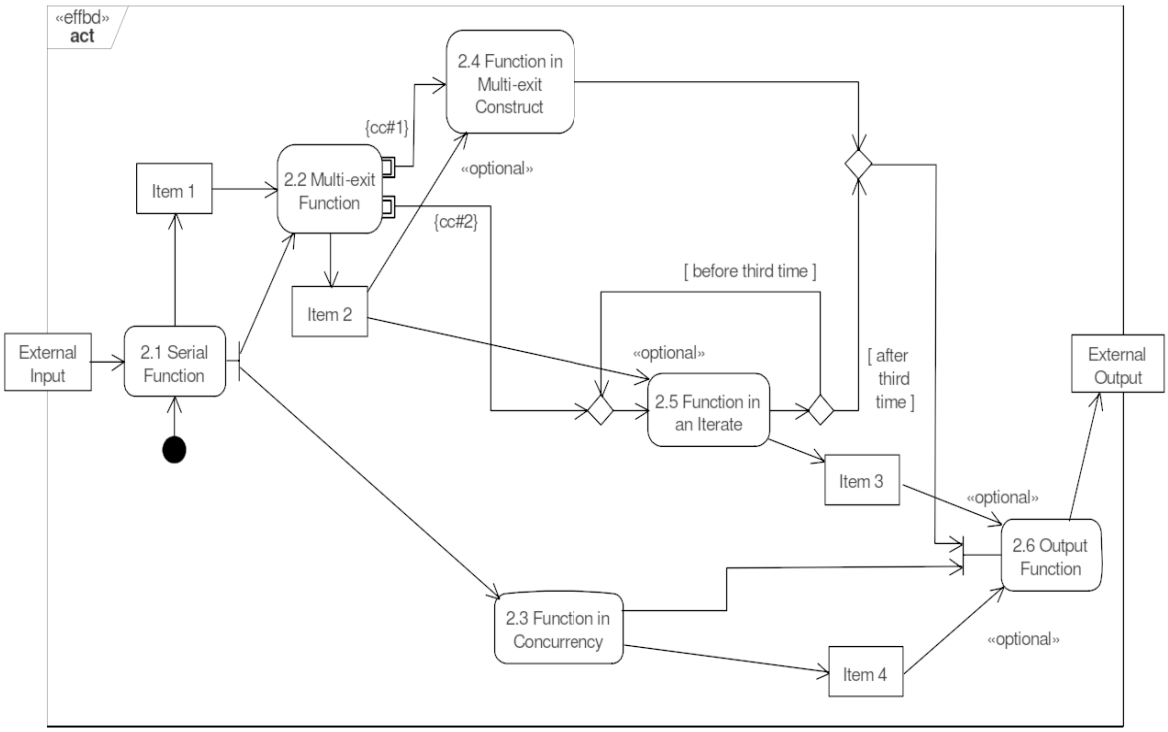
안전요건을 시나리오에 반영하는 방안은 [Figure 4]와 같다. [Figure 4]에서 알 수 있듯이 안전요건을 시나리오에 반영하는 방법은 두 가지가 있다.

안전 요건을 충족시키기 위한 안전 기능을 식별하여 이를 시나리오에 반영하는 방법과 안전요건으로 제시되는 안전을 위한 제약사항들을 시나리오에 반영하는 방법이 있다.

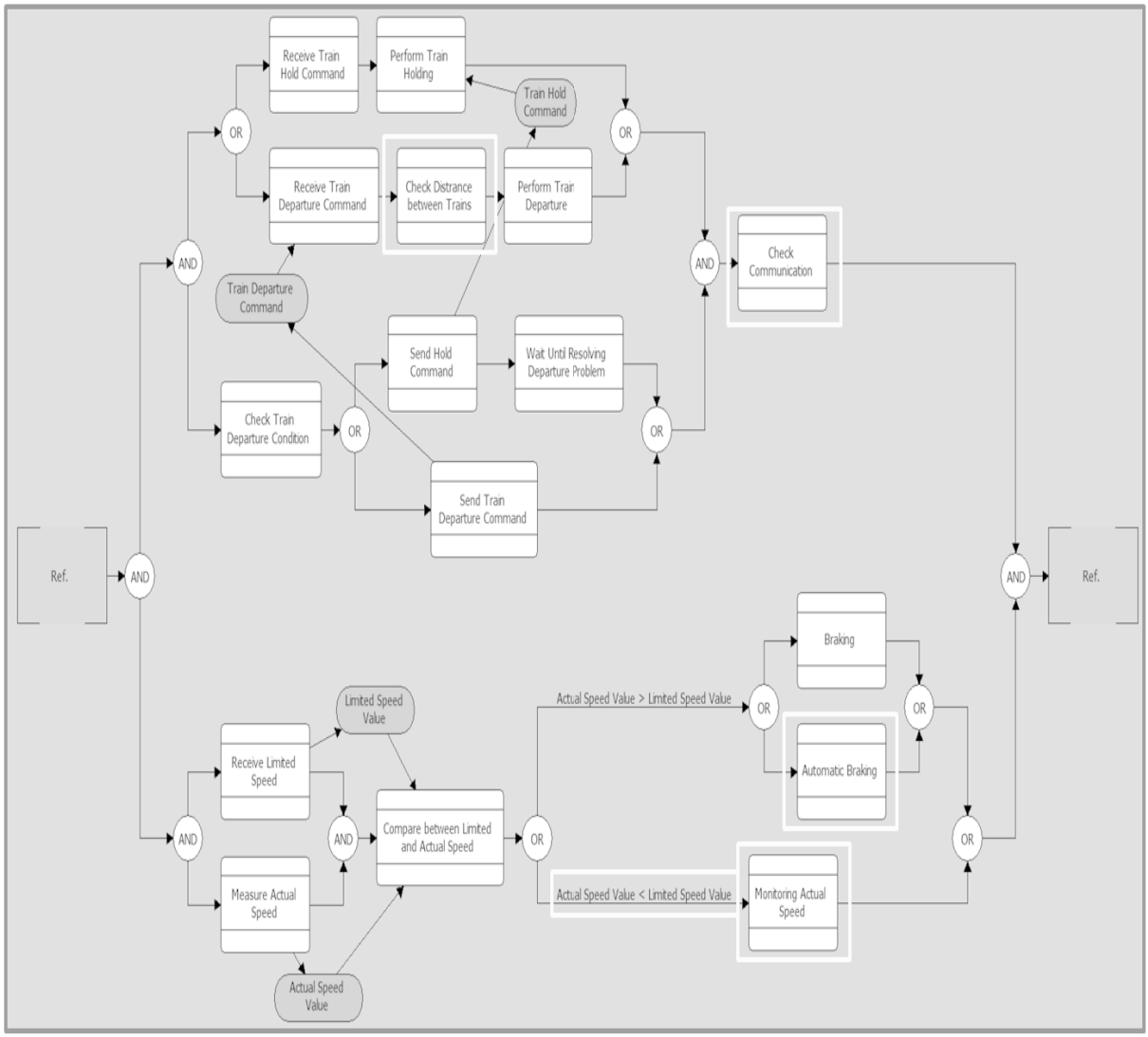
기능안전표준에서는 안전을 확보하기 위한 핵심으로써 안전기능을 설계에 반영할 것을 제시하고 있다. 안전기능의 작동을 통해 고장 및 위험이 발생했을 시 피해를 최소하거나, 이전에 능동적으로 위험원의 발현을 막을 수 있다. 따라서 안전기능의 수행이 시나리오에 반드시 반영되어야 안전요건이 반영되었다 할 수 있다. 그리고 안전요건의 형태로 제시되는 제약사항들이 있다. 고장 및 위험이 발생되는 상태까지 가지 않도록 미리 제약사항을 둬서 미연에 방지하고자 하는 것이다. 이러한 제약사항들 또한 시나리오에 반영되어야 한다.

이처럼 안전요건을 시나리오에 반영하기 위해서는 안전기능의 동작 및 제약사항들을 시나리오에 반영해야 한다.

이와 같이 시나리오에 안전요건이 반영됨으로써 안전목표를 달성하기 위한 요소들이 시나리오 상에 반영되고 여기서 발생 가능한 위험원들을 분석하여 위험을 통제함으로써 안전 목표를 달성할 수 있다.



[Figure 5] An example model using EFFBD [8]



[Figure 6>] EFFBD model of "Train Start Case"

3.2. 모델링과 시뮬레이션을 활용한 시나리오의 생성 및 검증 방법

서론에서 언급했듯이 시나리오 기반의 위험원 분석의 개선 방안 중에 하나로써 시나리오 생성방법에 대한 연구가 이뤄지고 있다. 본 연구에서는 텍스트 기반으로 작성되던 시나리오를 EFFBD(Enhanced Functional Flow Block Diagram)를 활용하여 모델링하고 이를 시뮬레이션을 통해 검증하였다.

EFFBD는 시스템의 거동을 표현하는 다이어그램 중의 하나이다. [Figure 5]와 같이 EFFBD는 기능의 흐름과 기능간의 데이터의 교환 모두가 표현되는 다이어그램이다. EFFBD를 활용하여 모델링함으로써 시나리오 상에 표현된 개별 활동이나 기능들이 어떤 순서를 가지고 수행되는지를 파악할 수 있으며, 또한 활동이나 기능들 간의 데이터의 흐름까지 분석이 가능하다. 즉 시나리오에 텍스트로 표현된 활동 및 기능들의 순서, 활동 및 기능들 간의 상호관계 등의 파악이 가능하다. 또한 EFFBD를 활용하여 시나리오를 모델링함으로써 이를 시뮬레이션을 통해 검증을 수행할 수 있다. 시뮬레이션을 통해 안전요건의 반영을 위해 시나리오 상에 제시된 안전기능이 필요한 시점에서 제대로 수행이 되는지, 시나리오 상에서 설정된 제약사항들이 모델에 제대로 반영되어 시나리오가 수행되는데 반영이 되고 있는지를 시뮬레이션을 통해 분석할 수 있다.

본 논문에서는 시나리오의 모델링 및 시뮬레이션을 수행하는데 전산지원도구인 Core를 활용하였으며, 이를 통해 시나리오의 생성 및 검증을 수행하였다.

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

3.3. 안전요건이 반영된 시나리오 기반의 위험원 분석방안

앞 절에서 언급했듯이 안전기능의 수행과 제약사항들을 시나리오에 반영함으로써 대상시스템에 대한 안전요건을 반영할 수 있음을 확인하였다.

또한 생성한 시나리오를 EFFBD를 활용하여 모델링하고 시뮬레이션을 수행함으로써 시나리오에 안전요건이 제대로 반영되었는지를 검증하였다.

검증된 시나리오를 바탕으로 위험원 분석을 수행함으로써 안전목표를 달성하는 위험원 분석을 수행하게 된다.

위험원 분석 과정에서 시나리오 상에서 정상상태에서 벗어나게 하는 위험원들을 식별하게 된다. 본 연구에서 활용한 안전요건이 반영된 시나리오를 활용하게 되면 기존의 위험원에 더하여 안전기능의 작동과정에서 발생가능 한 위험원과 제약사항이 지켜지지 못해 발생가능 한 위험원들을 식별할 수 있다.

이렇게 식별된 위험원들을 분석하여 위험을 통제하는 과정을 거치게 되면 안전목표를 달성하게 되며 이는 안전 보장으로 이어지게 될 것이다.

4. 안전요건이 반영된 시나리오 기반의 철도 시스템 위험원 분석

3장에서 제시한 안전요건이 반영된 시나리오기반의 위험원 분석방법에 따라 철도시스템에 대한 위험원 분석을 수행했다. 철도가 출발할 때와 출발 후의 속도 통제과정에 대한 시나리오를 생성하였다. 시나리오는 EFFBD를 활용하여 모델로 표현하였으며, 모델링 결과를 시뮬레이션 하여 안전기능의 수행이 시나리오에 반영되어 수행되고 있음을 확인하였다. 마지막으로 검증된 시나리오를 바탕으로 철도시스템에 대한 위험원을 식별하였다.

4.1. 안전요건이 반영된 철도시스템 출발 시나리오의 생성 및 검증

철도 차량이 출발할 때의 시나리오를 생성하기 위한 출발 전 준비 상황과, 출발 직후 주행을 시작할 때의 철도시스템의 기능을 식별 하였다. 기능이 어떠한 순서를 가지고 수행되는지와 기능들 간의 상호작용을 분석하기 위해 [Figure 6]과 같이 철도시스템의 출발 상황에 대한 EFFBD 모델링을 수행하여 시나리오를 생성했다.

EFFBD 상에 사각표시가 되어 있는 기능 및 제약사항들은 철도가 출발할 때의 철도시스템에 대한 안전요건이 반영된 부분이다. 이 때 반영된 안전요건 및 안전요건으로부터 도출된 안전기능 또는 제약사항은 <Table 1>과 같다.

안전을 위해 철도가 출발할 때의 안전요건으로써 철도차량의 속도, 관제팀과의 통신연결에 관한 안전요건을 도출하였다. 도출된 안전요건을 충족시키기 위해 자동브레이킹, 속도 모니터링과 같은 안전기능을 도출하였고, 실제 차량 속도에 대한 제약사항 또한 식별하였다.

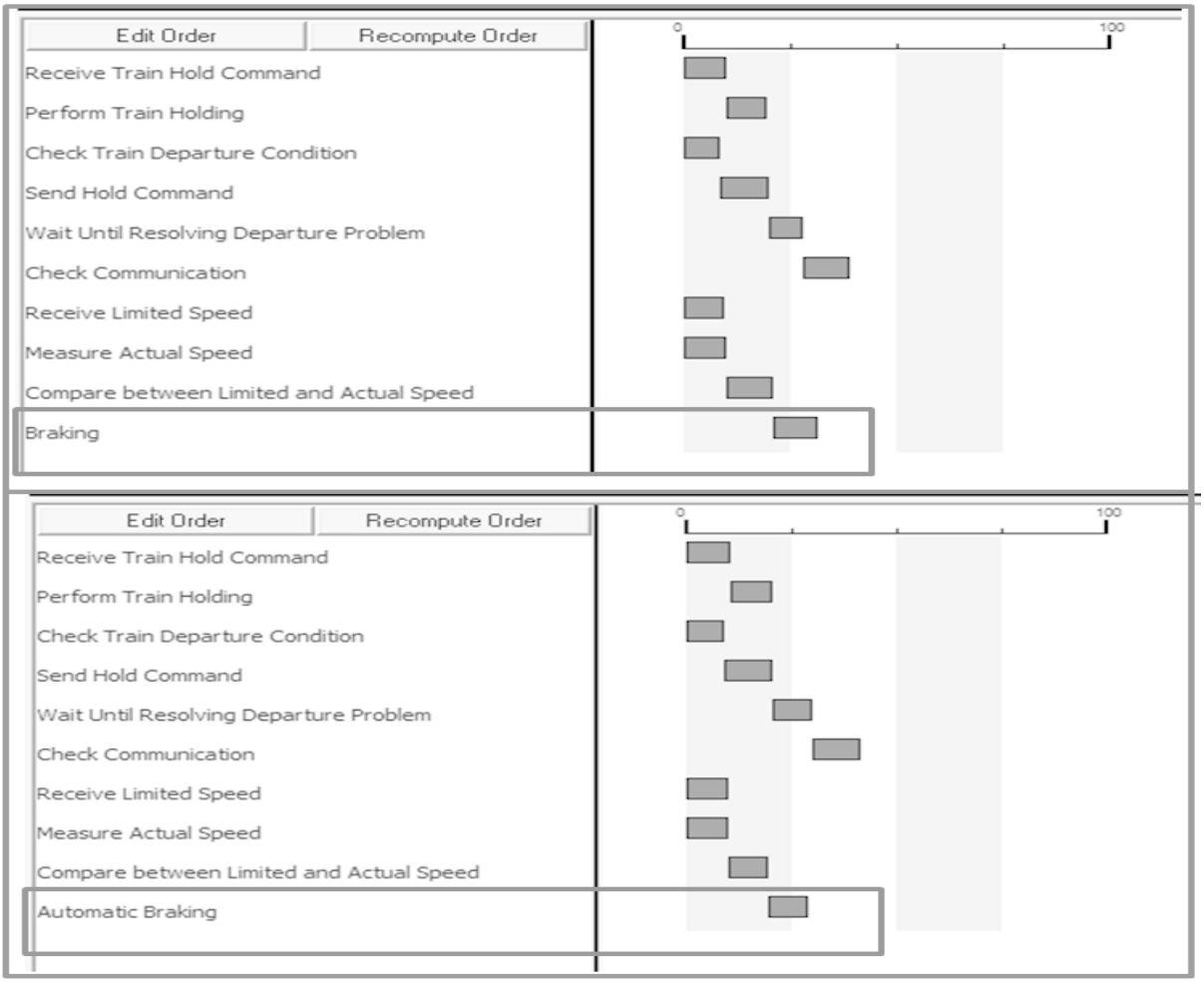
위와 같은 안전요건이 시나리오에 반영됨으로써 철도시스템의 출발 시에 안전을 확보하는 시나리오의 생성이 가능하다.

EFFBD를 활용하여 시나리오 모델링을 수행한 이유 중 하나가 앞서 언급했듯이 시뮬레이션이 가능하기 때문이다. 따라서 생성된 EFFBD 모델에 대하여 시뮬레이션을 수행하여 검증하였다. 시뮬레이션은 전산지원도구인 Core의 시뮬레이션 기능을 활용하였다.

철도차량 출발시 시나리오에 대한 시뮬레이션 결과는 [Figure 7]과 같다.

안전요건	안전기능 또는 제약사항
1. 앞차와의 배차간격을 일정히 유지해야 한다.	열차 간에 거리 모니터링 기능
2. 출발 후 속도는 관제팀에서 전송하는 제한속도를 일정시간 이상 넘어서는 안 된다.	측정되는 스피드는 제한속도를 일정시간 이상 초과해서는 안 된다.
3. 출발 후 속도는 지속적으로 모니터링 되어야 한다.	주행속도 모니터링 기능
4. 출발 후 관제팀과의 통신연결은 지속되어야 한다.	주행 중에는 관제팀과의 통신연결이 끊겨선 안 된다.
5. 실제속도가 일정시간 이상 제한속도를 상회하면 자동적으로 브레이킹이 작동하게 해야 한다.	자동 브레이크 기능

<Table 1> Safety requirements, safety functions and constraints for “Train Start”



[Figure 7] Simulation results for the EFFBD model of "Train Start".

EFFBD를 통해 확인할 수 있듯이 철도시스템 출발 시에는 다양한 기능이 병렬의 형태로 수행된다. 따라서 다양한 형태의 시뮬레이션 결과가 도출된다. [Figure 7]의 상단 부분과 하단 부분의 결과의 차이점은 안전기능중의 하나인 자동 브레이킹 기능의 작동여부이다. 상단부분은 실제 차량속도와 제한속도를 비교했을 때 실제 차량속도가 높아서 브레이킹 기능을 수행한 시나리오이다. 반면 하단부분은 실제 차량속도가 제한속도를 넘겨 브레이킹 기능이 수행되어야 하지만 일정기간 동안 브레이킹 기능이 수행되지 않아 안전기능인 자동 브레이킹이 작동하여 차량속도를 제어한 시나리오 결과이다.

즉 위험이 발생 가능한 상황을 방지하기 위해 안전요건을 통해 반영한 자동브레이킹 기능이 시나리오상에 반영되어 수행이 필요한 순간에 적절히 수행되고 있음을 시뮬레이션 결과를 통해 파악할 수 있다. 이와 같이 시나리오의 생성에 모델링을 활용하면 시뮬레이션을 통한 검증의 수행이 가능하다.

본 논문에서는 철도차량의 출발 시에 철도시스템의 운영에 관한 시나리오를 분석하여 EFFBD 모델링 통해 구현하였고, 안전요건을 반영하기 위한 안전기능 및 제약사항들을 모델링에 반영하였다. 모델링 결과를 시뮬레이션을 수행하여 안전기능 이 시나리오에 반영되어 적절히 수행되고 있음을 확인할 수 있었다. 이와 같이 모델링과 시뮬레이션을 통해 생성 및 검증된 안전요건이 반영된 시나리오는 위험원 분석을 수행하는데 활용된다.

4.2. 안전요건이 반영된 시나리오 기반의 위험원 식별

4.1절에서 생성 및 검증된 안전요건이 반영된 시나리오를 활용하여 위험원 식별을 수행하였다.

기존의 시나리오와의 차이점인 안전요건의 반영은 안전목표를 달성하기 위한 안전기능 및 제약사항들이 시나리오에 반영되었다는 것을 의미한다.

<Table 2> Result of identifying hazards on "Train Start"

철도 차량 출발시의 기능	Hazard	Deviation
1. 차량 출발/정지 신호 전송	신호 전송 불가	관제부에서의 신호전송 불가로 인한 차량 출발 불가
	잘못된 신호 전송	출발조건에 맞지 않은 출발/정지 신호 전송으로 이한 잘못된 운행
2. 차량 출발 조건 확인	차량 모니터링 불가	출발 전 차량 상태 모니터링 불가로 인한 출발 금지
	차량-관제부간 통신 불가	차량-관제 간 통신 불가로 인한 차량 출발 조건 확인 불가
3. 차량 제어 명령 수신	제어 명령 수신 오류	출발 불가 상황에서의 출발로 인한 사고 위험
	관제부와의 통신 불가	차량 출발 제어 명령 수신 불가로 인한 차량 출발 지연
4. 실제 차량 운행속도 측정	속도 측정 불가	현재 운행속도 측정 불가로 인한 속도 제어 불가
	속도 측정 오류	잘못된 측정값으로 인한 제한속도 초과 및 지연 발생
5. 차량 운행속도와 제한속도 비교	속도 비교 오류	잘못된 속도비교로 인한 제한속도 초과 및 지연 발생
	속도 비교 불가	속도 비교기능의 수행 불가로 인해 차량 제어를 위한 속도비교 불가 및 이로 인한 속도 제어 불가
6. 관제부와 속도 값 송수신	관제부와 통신 불가	제한속도 값 수신 불가로 인한 속도 제어 불가
	잘못된 제한속도 값 수신	잘못된 제한속도 값으로 인한 제한속도 초과 및 지연 발생
7. 차량간의 거리 확인	차량 간의 거리 확인 불가	차량 간의 거리확인이 불가능 할 시에 차량의 출발이 금지되어 차량의 출발 지연 발생
	차량 간의 거리 수치 오류	잘못된 차량 간의 거리 확인으로 인해 차량 간의 거리가 제한된 수치 이내로 접근
8. 자동 브레이킹	자동 브레이킹 기능 불가	선로의 제한속도 이상으로 주행하게 되어 사고위험 발생
	잘못된 속도에서 기능 수행	제한속도 아래에서도 속도가 제한되어 지연이 발생가능
9. 통신연결 모니터링	통신연결 확인 불가	관제팀과의 통신연결이 확인되지 않은 상황에서 차량 출발 불가로 인해 지연 발생

이는 위험원 식별 시에 기존 시나리오에 더하여 안전목표와 직결되는 위험원의 식별이 추가적으로 수행된다는 것을 의미한다.

이를 통해 안전에 대한 최상위 요구사항이라 할 수 있는 안전목표의 달성을 가로막는 위험원들을 추가적으로 식별하여 향후 위험관리에 활용하여 안전 보장을 달성할 수 있다.

검증된 시나리오 기반으로 위험원 식별을 수행한 결과는 <Table 2>와 같다.

<Table 2>는 모델링된 시나리오에서 확인 가능한 차량 출발 시에 수행되는 기능들에 대해서 위험원 식별을 수행한 것이다.

차량의 출발 시에 철도시스템은 차량의 출발제어와 속도제어에 관한 기능들이 수행된다. <Table 2>의 1-6번의 기능들은 차량의 출발제어와 속도제어에 대한 기능들이다. 이러한 기능들은 시나리오 상에서 기능들의 수행순서, 기능들 간의 상호작용 등이 포함되어 반영되어 있음을 [Figure 6]를 통해 확인할 수 있다. 이러한 기능들에 대하여 위험원과 위험원이 발현되었을 때 발생 가능한 Deviation을 식별함으로써 기능들에 대한 위험원 식별이 수행되었다.

7-9의 기능들은 안전요건이 시나리오에 반영됨으로써 식별된 기능들이다. <Table 1>의 안전요건을 충족시키기 위해 도출된 안전기능들이 7-9번의 기능들이다. 시나리오에 안전요건이 반영됨으로써 이러한 기능들 또한 모델에 반영이 되었으며, 이에 대한 위험원이 식별이 수행되었다. 안전기능들은 특히 안전과 직결된 기능들이기 때문에 반드시 이에 대한 위험원의 식별이 이뤄져야 한다.

이처럼 안전요건이 반영된 시나리오를 기반으로 위험원을 수행함으로써 안전기능에 대한 위험원 식별이 추가적으로 더해짐을 확인할 수 있다.

이는 안전확보와 직결되는 위험원들에 대한 분석 및 위험관리과 수행됨을 의미하며 이를 통해 안전 보장이 가능해진다.

5. 결론

오늘날 점차 대형화 복잡화 되어가고 있는 시스템들은 더욱 커진 사고 및 고장에 대한 위험을 내재하게 된다. 또한 철도와 같은 대형 복합 시스템에서 발

생하는 사고 및 고장은 바로 큰 재산피해나 인명피해와 직결 될 수 있다. 따라서 체계적인 안전관리의 필요성이 점차 커지고 있다.

본 논문에서는 대상 시스템에 대한 안전을 확보하기 위해 기능안전표준에서 명시하고 있는 기능중심의 위험원 분석방법 중 시나리오 기반의 위험원 분석방법의 개선에 대한 연구를 수행하였다. 안전요건을 반영한 시나리오 기반의 위험원 분석을 수행하기 위해 안전요건의 시나리오 반영 방안과, 시나리오 모델의 생성 및 시뮬레이션을 통한 검증 방안, 검증된 시나리오 기반의 위험원 분석의 수행 등에 대해 연구 하였다.

시나리오에 안전요건을 반영함으로써 안전의 확보와 직결되는 안전기능과 제약사항들이 시나리오에 추가적으로 반영되었다. 또한 시나리오를 모델링 하여 시뮬레이션을 수행함으로써 안전기능이 필요한 상황에서 적절히 수행되도록 시나리오가 작성되었음을 검증할 수 있었다.

안전요건을 충족하는 것은 안전에 대한 최상의 요구사항인 안전목표를 충족시키는 것이다. 따라서 안전요건이 반영된 시나리오의 생성과 이를 기반으로 한 위험원분석은 안전 보장으로 이어진다.

향후에는 시나리오 기반의 위험평가 까지를 고려하여 시스템 수준에서 위험원 분석 전체 활동을 수행하는 것에 대한 연구를 수행 할 필요가 있다.

6. References

[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] Sybert Stroeve and Henk Blom, "Contrasting safety assessments of a runway incursion scenario," Reliability Engineering & System Safety, vol. 109, pp. 133–149, Jan. 30, 2013.

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

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

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

[6] 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.

[7] 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.

[8] OMG Systems Modeling Language (OMG SysML), Object Management Group, Jun. 1, 2012.

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

이 재 천

현 아주대학교 시스템공학과 정교수. 서울대학교 전자공학과에서 공학사, KAIST 전기 및 전자공학과에서 공학석사 및 박사학위를 취득. 미국 MIT에서 Post–Doc을 수행하였으며, 미국 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, 모델기반 시스템공학 (MBSE), Systems Safety, Systems T&E 및 다양한 산업 분야에서의 응용 등.
주소: 경기도 수원시 영통구 원천동 산5번지 아주대학교 서관 309호