# 바이탈 열차제어시스템의 리스크 분석 및 헤저드 제어방법

*황종규, 조현정, 윤용기
한국철도기술연구원 열차제어연구팀
e-mail : {jghwang, hjjo, ykyoon}@krri.re.kr

# Risk Analysis and Hazard Control Process for Vital Train Control Systems

*Jong-Gyu Hwang, Hyun-Jeong Jo, Yong-Ki Yoon
Train Control Systems Research Team, Korea Railroad Research Institute

## Abstract

Railway signaling systems are so vital to ensure the safe operation of railroad and the assurance and demonstration of the safety is so important. The safety management process shall consist of a number of phases and activities, which are linked to form the safety life-cycle. The basic processes of safety management and safety activity throughout the lifecycle are 'risk analysis' and 'hazard control'. The safety managements and activities for the two kinds of aspects are implemented throughout the whole steps of system lifecycle. The risk analyses and hazard controls like those are needed, these activities have to be carried out through the whole of system lifecycle.

## I. 서론

열차제어시스템은 철도의 안전운행을 보장하기 위한 바이탈한 장비로서, 안전의 확보 및 입증이 매우 중요하다. 이에 따라 열차제어시스템에는 안전성 확보를 위한 많은 기술들이 반영되어 있다. 이러한 바이탈 열차제어시스템의 안전성 확보를 위해서 유럽을 중심으로 바이탈 제어시스템의 라이프사이클 각 단계별 안전성 확보를 위한 요구사항 및 주요한 활동에 대해 규격화하고 있으며 최근 들어 IEC에 의해 국제규격화 되고 있다. 이러한 규격들에 의하면 안전성 활동을 위해서는 사고를 유발할 수 있는 위험원(Hazard)을 도출하고 이 도출된 위험원에 대한 리스크 평가 및 허용 가능한 수준 이하로 시스템 라이프사이클 전 단계에서 헤저드를 제어하도록 하고 있다.

본 논문에서는 국내의 열차제어시스템에 적용을 위한 헤저드의 분석을 통해 리스크를 평가하고 라이프사이클 전주기에 걸친 헤저드를 제어하는 방법에 대해 고찰하였다. 이러한 헤저드 관리를 위해서는 우선적으로 국내의 열차제어시스템을 위한 헤저드의 도출이 필요하다. 이러한 도출된 헤저드들이 열차제어시스템의 개발 라이프사이클을 통해 어떻게 제어되고, 또한 어느 정도 수준 이하로 제어되는지를 관리하는 헤저드를 관리 프로세스가 안전성 활동의 근간이 된다.

## II. 본론

유럽을 중심으로 열차제어시스템을 위한 안전성 활동 체계 및 안전성 평가기술에 대한 많은 연구가 진행되어 왔으며, 최근 들어 열차제어시스템을 위한 RAMS 체계 및 요구사항 그리고 안전성 수용(safety acceptance)을 위한 요구사항들이 규격화되고 있다. 열차제어시스템 RAMS 관련 규격을 보면 유럽의 EN 규격화 되었다가, 현재 IEC에 의해 국제 규격화되어가고 있다. 이러한 규격들을 분석하여 보면 열차제어시스템을 위한 안전성 확보를 위해서는 기본적으로 시스템의 리스크 분석 및 헤저드 관리가 시스템 라이프사이클 전 단계에 걸쳐 수행하도록 요구하고 있다.

그림 1은 사고를 유발할 수 있는 헤저드의 근간이 되는 요소들을 크게 세 단계로 구분한 그림이고, 또한 헤저즈의 확인에서 제어 및 평가까지의 일련의 헤저드 관리 프로세스를 나타낸 그림이다.

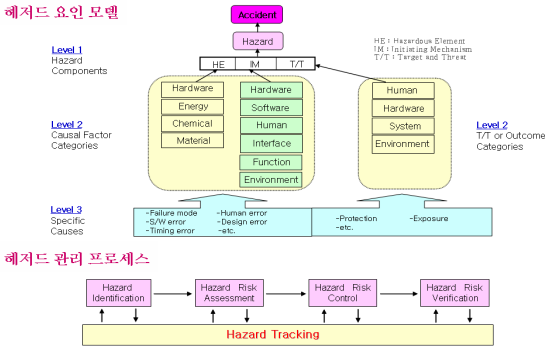


그림 1. 해저드 요인 관리 프로세스 일반

해저드의 분석 및 확인은 열차제어시스템의 리스크를 결정하고, 이에 의해 안전설계 수단이 해저드를 제거하거나 완화하도록 설계될 수 있게 하여 해저드들이 관리되도록 하는데 사용되며, 분석은 시스템, 서브시스템, 설비, 구성성분, 소프트웨어, 사람들, 그들 사이의 상호관계를 체계적으로 검사하기 위해 수행된다. 이러한 위험원의 분석 방법에는 그림 2와 같이 다양한 방법들이 적용되어질 수 있다.

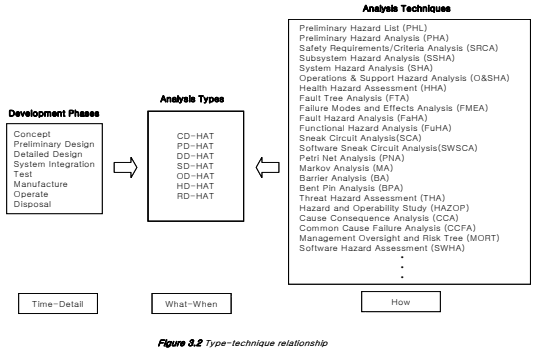


*Figure 3.2* Type-technique relationship

그림 2. 해저드 분석 방법

도출된 헤저드들은 각각 발생빈도와 심각도의 분석을 통해 리스크를 평가가 이루어져야 한다. 그리고 도출된 헤저드들이 시스템 내에서 허용수준 이하로 제어되도록 하여야 한다. 이러한 일련의 과정이 안전성 관리 및 활동 절차이가. 리스크는 보통 다음과 같이 정의되어진다.

*리스크(Risk)=발생빈도(Probability)×심각도(Severity)*

이러한 안전성 관리 및 활동절차는 기본적으로 Risk analysis와 Hazard control에 있다. 이러한 두 가지 측면의 관리 및 활동은 시스템의 Lifecycle 전체 단계를 통해 이루어지게 되며, 이러한 과정과 그 결과물들이 safety management를 위한 문서로 정리되어야 하며, 이것이 Safety Case의 가장 중요한 부분 중의 하나가 된다.

그림 3은 이러한 리스크 분석 및 헤저드 제어를 통한 안전성 활동체계를 간략하게 나타낸 것이다. 그림 4는 이 중에서 리스크 분석을 위한 절차는 나타낸 것으로 시스템의 헤저드 분석을 통해 헤저드 로그를 도출하고 리스크 별 THR(Tolerable Hazard Rate)를 할당하는 과정을 나나낸 것이다.

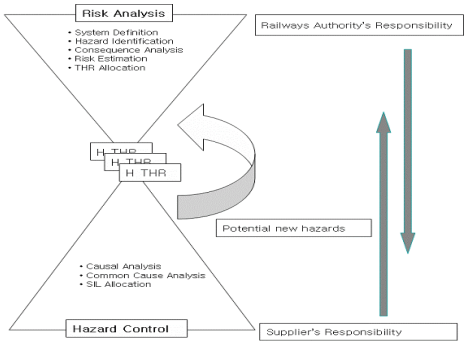


그림 3. 안전성 활동 체계

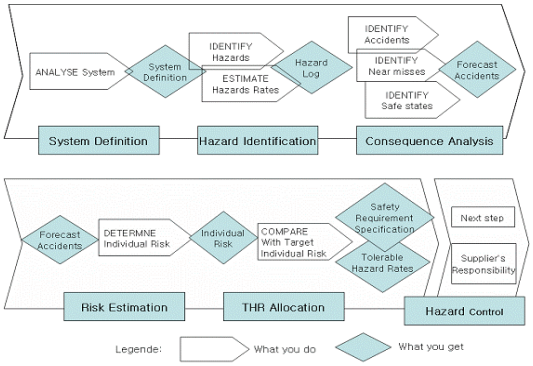


그림 4. 리스크 분석 절차

## II. 결론 및 향후 계획

철도의 열차제어시스템은 다른 어느 장치들보다 더욱 시스템의 안전성 확보가 중요하다. 이러한 이유로 열차제어시스템을 위한 RAMS 요구사항들이 국제 규격화되고 있으나, 아직 국내에서는 이러한 RAMS 체계에 맞추어 어떠한 안전성 관리 및 활동을 수행하여야 하는지에 대한 연구가 부족하다. 본 논문에서는 국내의 열차제어시스템을 위한 리스크 분석을 통한 헤저드 관리 방법 및 절차에 대해 분석하였다. 향후 이러한 제시된 방법 및 절차들의 적용성 연구를 통해 최종적으로 국내 환경에 맞는 안전성 활동방법 및 절차에 대한 연구가 필요하다.

## 참고문헌

[1]C.A.Ericson, "Hazard Analysis Techniques for System Safety", 2005.

[2]IEC 62278, "Railway Applications - The specification and demonstration of RAMS", 2002.

[3]IEC 62279, "Railway Applications - Software for railway control and protection systems", 2002.

[4]EN 50129, "Railway Applications - Safety related electronic systems for signaling", 2003.