열차제어시스템 안전성 평가 업무 분석

황종규, 조현정, 윤용기
한국철도기술연구원 열차제어연구팀

Analysis of Safety Assessment Activities for Railway Signalling System

Jong-Gyu Hwang, Hyun-Jeong Jo, Yong-Ki Yoon
Korea Railroad Research Institute

Abstract - According to the computerization of railway signalling systems, the safety demonstration and assessment of railway signalling system is very important. For this reason, railway signalling systems reflect the needs of methodology to assessment the safety. Then many studies of safety assessment methodology for railway signalling systems centering on the Europe, have been made continuously, and the requirements for safety acceptance are currently standardized by IEC. To develop and establish the safety assessment technology for railway signalling system in Korea, we are reviews the safety assessment activities for signalling system through the reviews of related std., case study and consulting by experts.

1. 서 론

전자 및 컴퓨터 기술을 이용한 열차제어시스템들에 의해 기존의 전기 및 기계적인 열차제어시스템을 대체되어 감에 따라 시스템이 지능화 및 자동화되는 등 성능이 향상되어가고 있다. 열차제어시스템은 그 특성상 대규모 인명피해나 경제적 손실과 직결되는 바이탈 시스템으로 엄격한 안전성 활동 및 평가기술이 요구되고 있다. 기존의 열차제어시스템은 경험적, 물리적으로 안전성을 확보해 왔으나, 컴퓨터화된 시스템은 고장모드 예측의 어려움 등의 문제로 안전성의 입증 및 이의 평가에 어려움이 있다.

열차제어시스템의 안전성 활동에 대한 요구사항을 IEC에 의해 국제규격화 되어 있으며[1], 또한 이러한 안전성 활동을 입증하기 위해 필요한 문서의 요구사항도 규격화되고 있다[2].

본 논문에서는 열차제어시스템의 안전성 평가를 위해 우선적으로, 안전성 활동 절차를 분석하였으며, 이를 토대로 안전성 평가를 위한 업무를 분석하였다. 그리고 이러한 안전성 평가업무 분석을 토대호 안전성 평가를 위해 필요한 기술 및 항목들을 제시한다.

2. 열차제어시스템 안전성 평가기술 분석

2.1 안전성 평가기술 개요

기존의 유럽규격으로 있던 철도시스템의 안전성 관련 규격들이 IEC에 의해 국제규격화됨에 따라 열차제어시스템의 안전성 활동 및 이에 따른 안전성 평가가 필수적으로 요구되고 있다. 외국의 경우는 열차제어시스템 제작사도 국제규격에 따른 안전성 활동을 수행하고 있고[1]-[3], 또한 각 나라별 독립된 안전성 평가기관이 있어 관련된 많은 프로젝트를 수행하고 있다. 국내의 경우 몇 년 전부터 관련 규격들이 소개되면서 이에 따른 안전성 활동 및 평가에 대한 필요성을 인식하고 있고 관련된 연구가 시작되고 있는 단계이다[4].

열차제어시스템의 안전성 평가는 적용한 안전성 활동에 대한 적절성과 준수여부의 확인 그리고 시스템에 관련된 위험원의 리스크가 제거되었거나 허용수준으로 제어되었음을 객관적인 자료를 통해 확인 및 평가하는 것이 필요하다. 이러한 안전성 평가업무에는 우선적으로 안전성 활동을 분석하는 업무와 결함주입 시험 등 추가적인 테스트 평가로 구분할 수 있다. 즉, 안전성 평가를 위해서는 우선적으로 안전성 활동에 따른 안전계획서와 안전 요구사양서를 토대로 안전성 평가를 위한 체크리스트를 작성 및 이 체크리스트를 통한 안전성 평가계획을 도출하게 된다. 그리고 이 도출된 평가계획에 따라, 안전성 활동의 최종적인 문서로 작성되는 안전성 입증 문서 종합안전대책기술서의 분석을 통해 해당 시스템에 대한 모든 위험원들이 도출 및 제어되었는지는 평가하게 된다. 이 후 기능확인 시험이나, 결함 주입 시험 등 추가적인 테스트 평가를 통해 최종적으로 모든 위험원이 종결되었음(Hazard Closure Verification)의 확인을 통해 최종적인 안전성 승인이 이루어지게 된다. 이러한 과정이 그림 1에 나타내어져 있다.

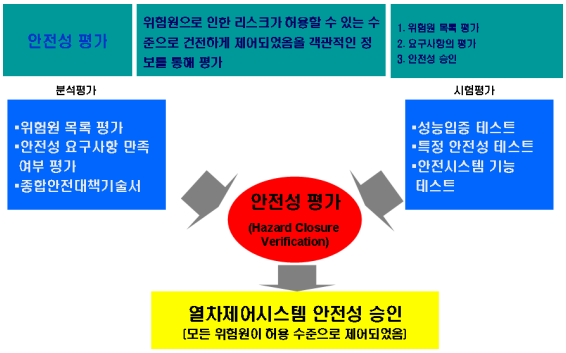

그림 1 안전성 평가기술 개요

2.2 안전성 평가 업무 분석

열차제어시스템의 안전성 평가업무는 기본적으로 안전성 활동에 대한 분석 및 평가를 바탕으로 수행되게 된다. 따라서 안전성 평가 업무의 분석을 위해 우선 그림 2와 같이 열차제어시스템의 안전성 활동을 분석하였다.

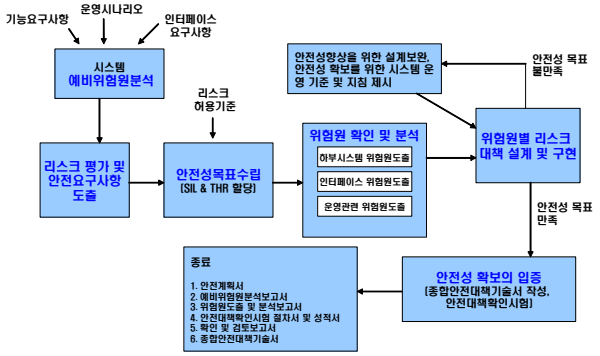

그림 2 안전성 활동 절차

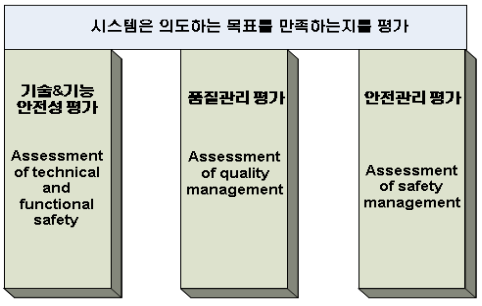

그림 3 안전성 평가의 구성

안전성 활동은 먼저 시스템 기능 요구사항, 운영시나리오 등을 바탕으로 예비 위험원 분석을 수행하고, 이를 통해 관리하여야 할 위험원 리스트와 이에 대한 대책기술을 반영한 안전 요구사항 도출 단계, 그리고 하부시스템 분석을 통한 안전성 목표수립 및 할당단계, 그리고 각 하부시스템별 상세 위험원 확인 분석 단계, 그리고 위험원별 대책기술 설계 및 구현단계, 마지막으로 일련의 과정을 통한 안전성 확보 입증의 단계로 구성되어 진다. 최종적으로 안전성 평가는 이러한 안전성 활동의 절차, 각 단계별 생성 문서의 적절성 확인을 통해 최종적으로 모든 도출된 위험원이 종결되었음을 확인하는 업무가 된다.

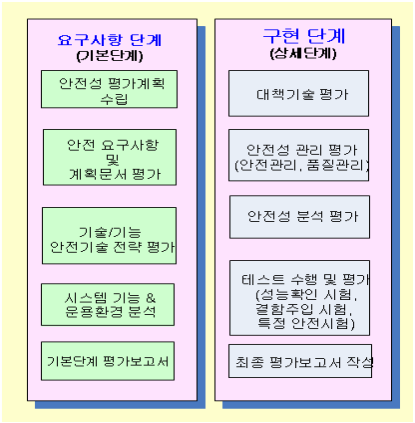

그림 4 안전성 평가 업무의 구분

[1][2] 국제규격의 분석을 통해 열차제어시스템의 안전성 평가는 그림 3과 같이 구성할 수 있다. 즉, 시스템이 기술 및 기능적으로 안전성을 갖는지에 대한 평가가 기본적으로 수행되어야 하며, 그다음 안전성 활동의 절차가 정상적으로 수행되지 등을 확인하는 안전관리의 평가, 그리고 지속적으로 해당 시스템의 설계, 제작되는 지를 보증하기 위한 절차 등의 확인을 위한 품질관리의 평가로 구성되어진다. 그림 4는 그림3과 같은 안전성 평가를 위해 실제로 수행하여야 할 업무를 나타낸 것으로 기본단계와 상세단계의 두 단계로 나눌 수 있다. 기본단계에서는 안전요구사항과 안전계획 등의 기본문서 분석을 토대로 안전성 평가를 위한 계획을 수립하는 단계를 말하며, 상세단계에서는 위험원의 리스크 제어를 위해 설계된 대책기술의 적정성과 결과의 평가, 안전성 관리의 평가, 테스트 평가 등의 실제적인 평가활동이 수행되게 된다.

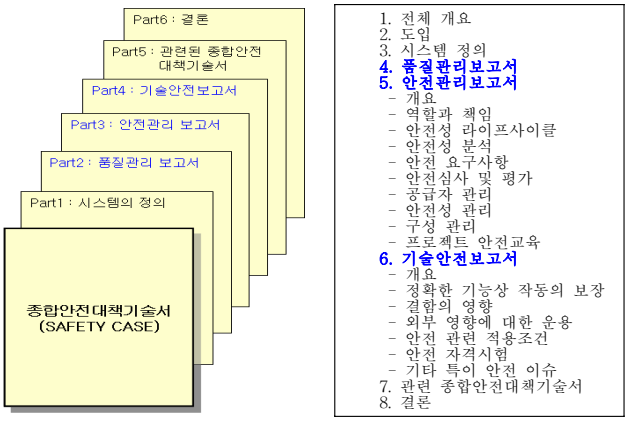

그림 5 종합안전대책기술서의 구성

안전성 활동의 마지막 단계에서는 안전성 입증을 위한 근거들을 포함하는 종합안전대책기술서를 작성하게 된다. 안전성평가는 기본적으로 이 종합안전대책기술서를 토대로 수행되게 되며, 이 문서에는 그림 3의 내용을 포함하여야 하므로 이 세부분에 대한 입증자료들을 중심으로 구성되게 된다. 종합안전대책기술서는 시스템의 안전성 평가를 위해 평가기관에 제출되어지는 시스템의 안전을 증명하는 근거들이 포함된 문서로서, 시스템이 안전 요구사항을 따르고 있으며 위험원이 제거 되었거나, 허용수준 이하로 리스크가 제어되었는지를 증명하는 시스템의 안전성 평가를 위해 매우 중요한 문서이다. 본 논문에서는 이러한 열차제어시스템 안전성 평가를 위해 가장 핵심적인 문서인 종합안전대책기술서에 포함되어야 할 내용을 분석하고, 이를 통한 열차제어시스템의 안전성 평가를 위한 이 문서의 목차와 구성 등을 제시하였다. 열차제어시스템의 안전성 인증을 위해서는 안전무결성등급(SIL : Safety Integrity Level)과 고장률(FR : Failure Rate) 모두를 만족하는지를 입증하여야 한다. 즉, 품질관리 근거, 안전관리 근거, 기술적인 안전관련 근거 그리고 정량적인 안전성 근거가 종합안전대책기술서에 모두 포함되어야 한다. 이중 품질관리와 안전관리 근거는 프로젝트 수행 관련된 프로세스 측면의 근거에 대한 문서들이다. 즉, 시스템에서 요구되는 안전도 및 SIL 등급의 만족을 증빙하기 위한 종합안전대책기술서를 그림 1과 같이 구성할 수 있다. 그림에서와 같이 1장은 프로젝트 시스템에 대한 정의, 2~4장은 앞에서 언급한 품질관리, 안전관리 및 기술안전 보고서이고, 그리고 5장은 해당 프로젝트에 적용되는 다른 관련된 종합안전대책기술서 그리고 6장 결론으로 구성할 수 있다.

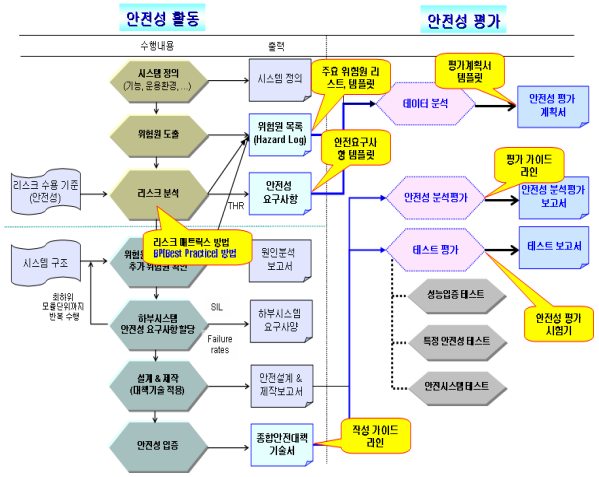

그림 6 안전성 활동을 통한 안전성 평가 업무 분석

그림 6은 열차제어시스템을 위한 안전성 활동절차와 이에 따른 안전성 평가 업무를 나타낸 것으로, 안전성 활동에 따른 안전성 분석 평가와 테스트 평가로 구성되어짐을 설명하고 있다. 또한 안전성 평가기술 확보를 위해 현재까지 연구한 각 단계별 항목들을 그림에 별도로 색인하여 표시하였다. 즉, 안전성 평가는 위험원별 리스크가 제어되었는지를 분석 및 평가하는 업무를 수행하는 것으로, 기본적으로 안전성 평가를 위해서는 열차제어시스템에 대한 주요한 위험원 리스트가 확보되어 있어야 한다. 그리고 안전요구사항 템플릿, 평가계획서 템플릿을 분석하였다. 그리고 안전성 입증 문서인 종합안전대책기술서의 작성 가이드라인과 소프트웨어 안전성 평가 가이드라인에 대한 연구도 진행 중에 있다. 그리고 리스트 분석 및 평가를 위한 방법 중 보다 정량화된 방법인 BP(Best Practice) 방법을 국내 열차제어시스템에 적용을 위한 연구가 수행되고 있다.

3. 결 론

국제규격에 의해 열차제어시스템의 안전성 활동의 필요성이 증가되고 있고, 또한 이의 검증을 통한 평가기술의 개발 필요성이 증대되고 있다. 이에 따라 본 연구에서는 안전성 활동 절차를 우선적으로 분석하였으며, 이 안전성 활동에 따른 안전성 평가업무를 도출하였다. 이 안전성 활동절차에 따른 안전성 평가 업무의 분석을 토대로 안전성 평가기술의 확보를 위해 필요한 항목 및 내용을 도출하였으며, 종합안전대책기술서의 목차 등 일부 안전성 평가를 위해 수행한 연구결과를 설명하였다. 본 논문의 안전성 평가업무 분석을 바탕으로 안전성 평가를 위한 보다 구체적이고 심도 있는 연구가 필요하다.

[참 고 문 헌]

[1] IEC 62278, "Railway Applications - The specification and demonstration of RAMS", 2002.
[2] IEC 62425 Ed. 1, "Railway Application : Communications, signalling and processing systems - Safety related electronic system for signaling", 2005.10.
[3] NASA Dryden Flight Research Center, "Dryden Handbook Code S - System Safety Handbook", March 1999.
[4] 한국철도기술연구원, "철도종합안전기술개발 연구성과발표회 자료집", 2006. 10.