Safety Case 문서를 기반한 열차제어시스템 안전성 평가방법 분석
Analysis of Safety Assessment of Railway Signalling by Safety Case Documents

황종규*, 조현정**, 윤용기**, 김용규**
Hwang, Jong-Gyu Jo, Hyun-Jeong Yoon, Yong-Ki Kim Yong-Gyu

ABSTRACT

It is demanded to produce the safety evidence documents in other to approval safety characteristic of railway signaling system which stands is included, it is demanding from IEC 62425 standards. Also it is express clearly that safety assessment if signaling system has to be verification of these safety evidence documents. This Safety Case has the results of safety activity through system life-cycle, such as hazard lists, hazard identification and analysis, risk assessment and countermeasure, verification and test results. Consequently, first of all, the analysis and verification of these Safety Case documents has to be accomplished to approval and acceptance of signaling system safety. And also if the safety assessor was want, it is able to be experimental test auditory which is, arbitrary faults injection test, to above described documents verification. In this paper, the contents and architecture of Safety Case are presented as first steps of safety assessment technology establishment for railway signaling system.

1. 서론

IEC 62425 규격[1]에서 열차제어시스템의 안전성 승인을 위해서는 시스템의 안전성을 입증할 수 있는 문서(Safety Case, 본 논문에서 '종합안전대책기술서'라는 용어를 사용)를 제시하도록 하고 있고, 이 제시된 문서들의 평가를 통해 열차제어시스템의 안전성을 평가 및 인증하도록 하고 있다. 이처럼 열차제어시스템의 안전성 평가를 위해 필수적인 종합안전대책기술서에는 시스템의 요구사항 단계부터 라이프 사이클 전 단계에 걸친 위험원 도출 및 분석, 안전대책수립 및 확인, 시험 등의 안전성 활동과정과 그 결과들을 포함하고 있다[1][2]. 따라서 열차제어시스템의 안전성 평가는 우선적으로 이러한 안전성 활동에 근거한 안전성 입증문서인 종합안전대책기술서의 적절성에 대한 평가가 기본적으로 이루어져야 하며, 시스템 안전평가자의 필요에 따라 이러한 문서적인 안전성 활동에 대한 검증과 더불어 추가적인 시스템에 대한 결함주입시험을 통한 시스템의 안전성을 검증하게 된다[4]. 본 논문에서는 열차제어시스템의 안전성 평가기술 개발 측면에서, 이처럼 열차제어시스템의 안전성 평가에 있어서 가장 기본이 되면서 중요한 부분 중의 하나인 안전성 입증의 근거가 되는 종합안전대책기술서의 구성 및 포함될 내용들을 중심으로 한 열차제어시스템의 안전성 평가방법에 대해 분석하고자 한다. 본 논문의 연구를 바탕으로

* 한국철도기술연구원 열차제어연구팀
E-mail : jghwang@krri.re.kr
TEL : (031)460-5438 FAX : (031)460-5449
** 한국철도기술연구원 열차제어연구팀

향후 국내에서 열차제어시스템의 안전성 평가를 위한 기술체계 및 가이드라인이 마련된 예정이다.

2. 열차제어시스템 안전성 평가방법 검토

열차제어시스템의 안전성 평가는 적용한 안전성 활동 절차의 적절성과 준수여부의 확인과 시스템에 관련된 리스크가 적절한 수준으로 낮아졌는지를 확인하는 두 가지 모두를 필요로 한다. 즉, 우선적으로 안전계획서의 적합성과 안전계획서와의 일치성을 확인 및 검증하는 것이 필요하다. 그러므로 열차제어시스템의 안전성 평가는 계획된 프로젝트 활동이 안전계획서에 제시된 방식과 절차에 따라 수행되고 있는지, 또 수행되었는지 확인이 되어야 한다. 이러한 안전성 평가를 위한 절차적인 내용을 확인 및 평가하는 것을 안전심사(Safety Audit)라 한다.

그리고 프로젝트 열차제어시스템에 관련해 도출된 위험원이 시스템의 설계 및 제작과정을 통해 제거되었거나, 해당 위험원의 리스크가 정한 수준 이하로 감소되었는지 여부를 확인하는 것이 필요하다. 이처럼 열차제어시스템이 실제적으로 안전성을 가지고 있는지 등에 대한 평가행위를 안전평가(Safety Assessment)라 한다. 이러한 시스템의 안전평가를 위해서는 시스템에 대한 안전요구사항을 검토하여 사양서가 위험원의 리스크를 제어하기에 충분하게 작성되었는지를 검토하고, 시스템 검토를 통해 시스템이 안전 요구사양서를 만족시켰는지를 평가한다. 즉, 기본적으로 안전성의 평가를 위해서는 프로젝트 열차제어시스템의 위험원 목록, 안전계획서, 안전 요구사양서 등의 문서들의 분석 및 확인으로부터 시작되어진다. 열차제어시스템의 안전성 평가는 이러한 안전심사와 안전평가 두 가지 측면 모두에서 수행이 필요하며, 때에 따라서는 두 가지가 중첩되어 발생되기도 한다.

열차제어시스템의 안전심사를 위해서는 기본적으로 안전계획서가, 안전평가를 위해서는 안전 요구사양서가 가장 핵심적인 문서들이다. 열차제어시스템의 안전성 평가를 위해서는 프로젝트의 안전계획서와 안전 요구사양서의 확인을 통해 안전성 평가를 위한 체크리스트를 작성 및 이 체크리스트를 통한 체계적인 안전성 평가를 하게 된다. 이 안전성 평가를 위한 체크리스트에는 안전계획서와 요구사양서를 포함한 제출되는 안전성 활동에 대한 근거가 되는 문서들의 확인뿐만 아니라 문서의 배경이 되는 프로세스와 조직 등에 대해서도 확인하여야 한다. 또한 공식적인 시험을 다시 요청할 수도 있으며, 필요에 따라서는 임의의 결함 주입 등의 추가적인 시험을 통한 시스템의 안전성이 확인 되어야 한다.

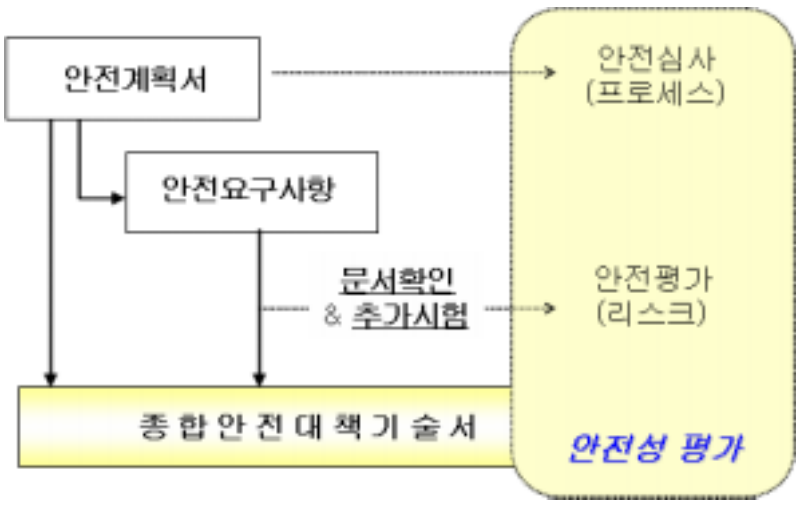

그림 1 열차제어시스템 안전성 평가 개요

그림 1은 열차제어시스템의 안전성 평가에 대한 개요를 설명한 그림으로, 앞에서 설명한 안전성 활동 프로세스 확인을 통한 안전심사와 해당 프로젝트의 도출된 위험원들의 리스크 제거 또는 저감의 확인을

하는 안전평가를 모두 포함하여 안전성 평가 활동이 이루어지게 된다. 열차제어시스템의 안전성 평가를 위해서는 우선적으로 평가자를 도와주기 위한 안전성 평가를 위한 체크리스트, 프로젝트 시스템에서 주요한 위험원이 누락 여부 확인 및 비교를 위한 일반 열차제어시스템 위험원 리스트, 그리고 추가적인 시험을 통한 확인을 위한 설비들을 필요로 한다. 이러한 시스템의 안전성 평가의 시작에서는 다음과 같은 사항들의 확인부터 시작되어진다.

- 열차제어시스템 위험원 목록
- 프로젝트 안전계획서
- 프로젝트 안전요구사양서

그림 2는 열차제어시스템의 안전성 활동 체계에 기반을 둔 안전성 평가를 위한 기술체계를 나타낸 것이다. 그림에서와 같이 열차제어시스템의 안전성 활동은 시스템의 정의 단계인 요구사항 도출부터 시스템의 위험원 도출 및 안전대책을 수립하는 예비위험원분석 단계, 예비위험원분석 단계를 통해 도출된 위험원을 대상으로 FMEA나 HAZOP, FTA 등의 기법을 통한 HIA 단계, 그리고 리스크 평가 및 안전무결성등급 할당 단계, 마지막으로 이러한 내용들이 시스템의 설계 및 제작과정에 반영시키고 그 결과를 증명하기 위한 종합안전대책기술서를 작성하게 된다. 열차제어시스템의 안전성 평가는 이러한 안전성 활동 체계에 대한 확인 및 검증의 과정이며, 이를 통해 위험원의 리스크가 제거 또는 허용수준 이하로 저감되는지 여부를 확인 하는 것이다.

그림 2 안전성 평가기술 체계

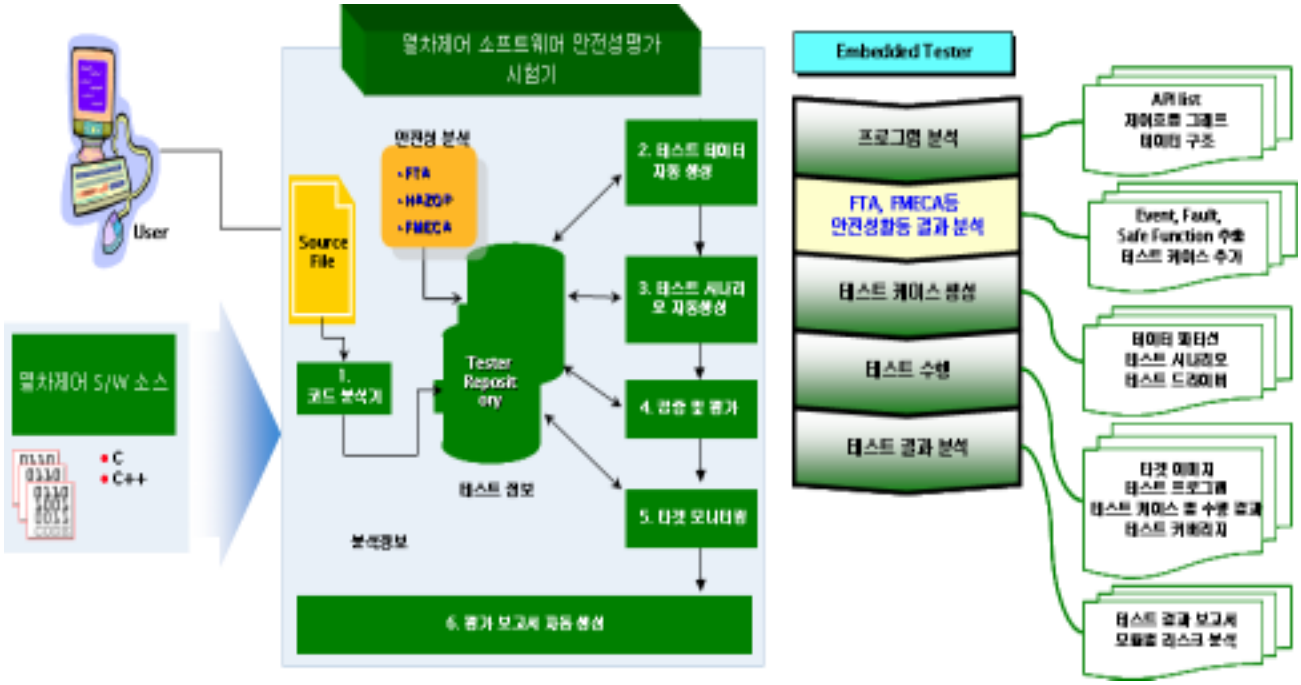

그림 3 열차제어시스템 소프트웨어 테스트기 구조

안전성 입증을 위해서는 기본적으로 종합안전대책기술서가 생성되어야 하지만, 필요에 따라 추가적인 시험이 필요로 할 수 도 있다. 이러한 추가적인 시험에는 시스템적인 측면에서 임의로 결함을 주입을 통한 시스템의 성능을 테스트 할 수도 있다. 그림 3은 열차제어시스템의 소프트웨어 안전성 테스트기의 구조로서 화이트박스 테스트를 통한 소프트웨어 품질을 테스트함과 동시에 안전성 평가를 위한 모듈의 추가를 통한 스프트웨어의 안전성 평가가 가능하도록 하는 구조를 갖는다. 현재 열차제어시스템의 안전성 평가기술 개발 측면에서 이러한 시험기에 대한 개발을 고려하고 있다[3].

그림 2와 같은 각 단계별 생성문서들과 최종적으로 생성될 프로젝트 열차제어시스템의 안전성 입증 문서인 종합안전대책기술서의 문서확인을 기본으로 하여 안전 프로세스의 확인 및 리스크가 제거 또는 저감되었는지 확인하게 된다. 따라서 안전성 평가를 위해서는 기본적으로 안전계획서, 안전요구사양서, 그리고 종합안전대책기술서라는 세 가지의 문서들에 대한 확인 및 평가를 필요로 한다. 본 논문에서는 이 중 열차제어시스템의 안전성 평가에서 가장 중요한 부분 중의 하나인 종합안전대책기술서의 구성 및 포함될 내용을 분석하였다.

3. 종합안전대책기술서

종합안전대책기술서는 앞 절에서 설명하였듯이 프로젝트 시스템의 안전성 평가를 위해 평가기관에 제출되어지는 종합적인 문서로서, 시스템이 안전 요구사항을 따르고 있으며 위험원이 제거 되었거나, 허용 수준 이하로 리스크가 제어되었는지를 증명하는 시스템의 안전성 평가를 위해 매우 중요한 문서이다. 본 절에서는 이러한 열차제어시스템 안전성 평가를 위해 가장 핵심적인 문서인 종합안전대책기술서에 포함되어야 할 내용을 분석하고, 이를 통한 열차제어시스템의 안전성 평가를 위한 이 문서의 목차와 구성 등을 제시한다.

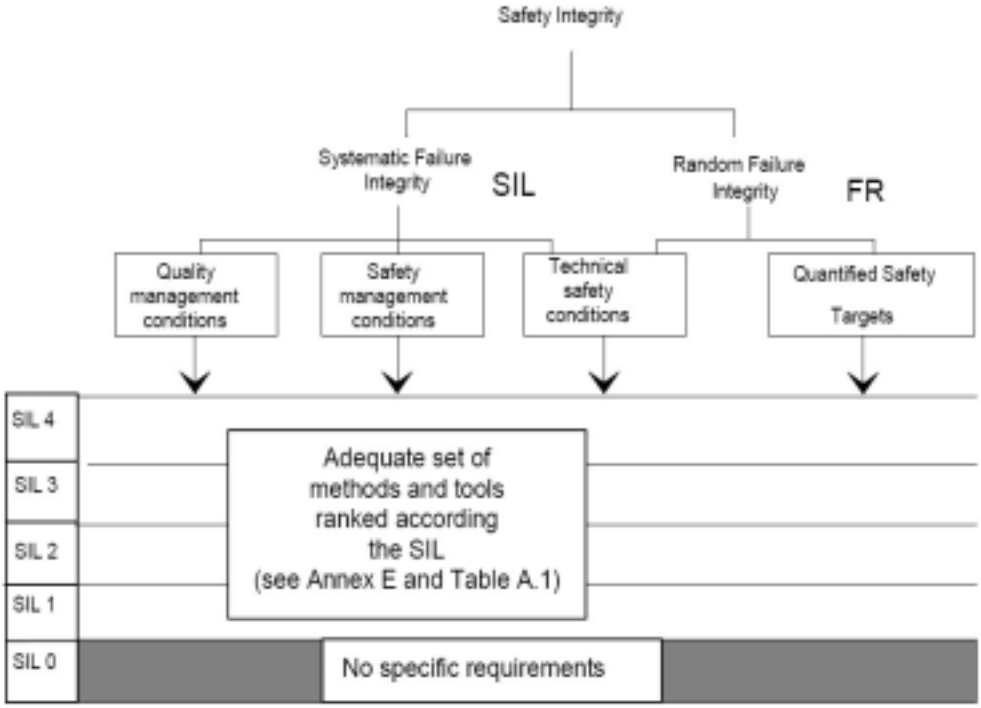

그림 4 SIL 등급과 안전도와의 관계

그림 5 종합안전대책기술서 구성

그림 6 기술안전보고서의 구성

시스템의 안전성 인증을 위해서는 그림4와 같이 안전무결성등급(SIL)과 고장률(FR) 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, 그림 4에 나타난 시스템에서 요구되는 안전도 및 SIL 등급의 만족을 증빙하기 위한 종합안전대책기술서를 그림 5와 같이 구성할 수 있다. 그림에서와 같이 1장은 프로젝트 시스템에 대한 정의, 2~4장은 앞에서 언급한 품질관리, 안전관리 및 기술안

전 보고서이고, 그리고 5장은 해당 프로젝트에 적용되는 다른 관련된 종합안전대책기술서 그리고 6장 결론으로 구성할 수 있다.

1. 전체 개요
2. 도입
3. 시스템 정의
4. 품질관리보고서
5. 안전관리보고서
 - 개요
 - 역할과 책임
 - 안전성 라이프사이클
 - 안전성 분석
 - 안전 요구사항
 - 안전심사 및 평가
 - 공급자 관리
 - 안전성 관리
 - 구성 관리
 - 프로젝트 안전교육
6. 기술안전보고서
 - 개요
 - 정확한 기능상 작동의 보장
 - 결함의 영향
 - 외부 영향에 대한 운용
 - 안전 관련 적용조건
 - 안전 자격시험
 - 기타 특이 안전 이슈
7. 관련 종합안전대책기술서
8. 결론

표 1 종합안전대책기술서 목차(안)

1장의 시스템 정의는 해당 시스템, 하부시스템 또는 장치를 정확하게 정의하거나 언급하도록 하며, 버전넘버와 모든 필요사항, 설계 및 응용문서의 수정 상태 등을 포함하도록 한다. 즉, 이 부분은 시스템 설명, 시스템에 대한 가정을 포함한 시스템 경계와 인터페이스에 대한 정의 그리고 하부시스템 구성요소 등이 설명되어지도록 한다. 2장의 품질관리에 대한 근거는 시스템의 수명주기 동안 효과적인 품질관리 시스템에 의해 통제되어 왔는지를 입증하는 내용을 품질관리 시스템은 수명주기 동안 각 단계에서 인위적인 오류발생을 최소화하고자 하는데 있다. ISO 9001에 의한 품질관리 등이 그 예가 될 수 있다.

3장의 안전관리 근거는 프로젝트에서 안전성 활동 측면이 어떻게 진행되었는지를 설명하여야 한다. 또한 안전계획서에 따라 안전성 활동이 진행되었음을 입증해야하고, 이런 활동이 적절했음을 증명해 보여야 한다. 4장의 기술안전보고서는 앞의 품질관리 및 안전관리 시스템에 의해 프로젝트 시스템이 충분히 안전함을 입증하기 위한 설계의 안전에 대한 기술적인 입증내용들이 여기에 포함된다. 이 부분에서는 적용된 모든 근거(예, 설계원리와 계산, 시험사양과 결과, 안전무결성 분석)를 포함하여 설계의 안전성을 보증하는 기술원리들이 설계되어야 하며, 그림 6은 이 기술안전보고서의 세부 구성안을 나타낸 것이다. 표 1은 열차제어시스템 안전성 평가를 위해 필요한 종합안전대책기술서의 목차(안)를 나타낸 것으로, 앞에서 설명한 내용들을 모두 반영한 문서를 필요로 한다.

4. 결론

본 논문에서는 종합안전대책기술서를 기반으로 한 문서확인을 중심으로 한 열차제어시스템의 안전성 평가방법에 대해 고찰하였다. 열차제어시스템의 안전성 평가를 위해서는 기본적으로 시스템의 안전성 입

증을 위한 근거들을 정리한 종합안전대책기술서, 안전계획서 및 요구사항 등 문서의 확인 및 검증에 중점을 두고 수행되어진다. 이때 기본적으로 해당하는 문서가 모두 준비되었는지와 안전관리 및 품질관리 프로세스를 준수하면서 안전성 활동이 수행되었는지에 대한 절차의 확인이 필요하다. 그리고 시스템의 설계 및 제작과정에서 위험원의 제거 또는 저감이 되었는지에 대한 확인을 하고, 필요시 추가적인 시험을 수행하게 된다. 본 논문에서는 이러한 열차제어시스템의 안전성 평가기술의 개발의 일환으로 그림 5와 같은 종합안전대책기술서에 대해 분석하여 그 구성과 목차안을 제시하였다. 향후 본 논문의 연구를 바탕으로 종합안전대책기술서를 중심으로 한 국내 열차제어시스템 안전성 평가 가이드라인을 마련하고자한다. 이 안전성 평가 가이드라인에는 종합안전대책기술서의 상세한 목차 및 내용, 작성지침 및 작성예 등이 포함될 예정이며, 안전성 평가를 위한 체크리스트의 도출, 문서확인 및 검증과 더불어 그림 3과 같은 추가적인 시험기를 제작하여 보다 효율적이고 충분한 안전성 평가기술이 확립되고 평가체계가 구축되도록 할 예정이다.

참고문헌

[1] IEC 62425 Ed. 1, “Railway Application : Communications, signalling and processing systems - Safety related electronic system for signaling", 2005.10.

[2] RAILTRACK, "Engineering Safety management Issue 3 Yellow 3, 4", 2005.

[3] 한국철도기술연구원, “철도종합안전기술개발 연구성과발표회 자료집”, 2006. 10.

[4] NASA Dryden Flight Research Center, 'Dryden Handbook Code S - System Safety Handbook', March 1999.