철도시스템 안전무결성레벨(SIL)의 검증방안에 대한 연구
A Study on the Verification Method for Railway System SIL

박영수*
Park, Young-Soo

ABSTRACT

This paper is about the study on the verification method for railway system SIL which is frequency of hazard, composing Risk, one of the measurement standards for railway system safety. Frequency of hazard can be identified by using FMECA, or HAZOP, and the assessment of identified dangerous failure rate should be done by systematic methods such as FTA. Therefore, this paper provides the hazard identification level for SIL verification and the requirements necessary to verify the integrity of analysis activity.

1. 서 론

본 논문은 철도시스템의 안전성확보 유무를 판단하기 위해 사용하는 위험원(Hazard)에 대한 위험도(Risk)의 구성요소인 발생빈도와 심각도 중, 위험원의 발생에 대한 안전대책 반영 후의 위험측고장률 발생빈도의 정량적인 판단기준인 안전무결성레벨(SIL, Safety Integrity Level)에 대하여 국내 철도분야에 적용되고 있는 현황을 분석하고, 제시된 SIL의 검증을 위한 방안을 제시한다.

안전의 확보유무는 ALARP(As Low As Reasonably Practicable)이론 등을 적용하여 정량적으로 평가된 위험도가 허용수준으로 제어되었거나, 기존에 사용하고 있던 환경의 위험도보다 낮음이 증명되는 것을 기준으로 판단한다. 따라서, 위험도를 구성하는 위험원의 발생빈도와 심각도를 모두 평가하기 위해서는 장치 또는 행위에 대한 인터페이스, 운영방식, 기능분석을 통해 위험도를 평가하게 되므로 신규개발되거나 RAMS(Reliability, Availability, Maintainability, Safety)활동의 범위를 장치레벨로 제한하는 경우에는 심각도의 평가가 매우 어려워지며, 심각도를 평가하더라도 평가과정이 가정에 대한 의존도가 너무 높기 때문에 평가결과가 큰 의미를 갖지 않는다.

위와 같이 RAMS활동의 범위가 장치로 제한되거나, 적용환경에 대한 인터페이스와 운영환경에 대한 정보가 정의되지 않았을 때 사용하는 안전에 대한 기준이 SIL이다. 본 논문에서는 이러한 SIL에 대한 의미를 명확히 하고, SIL4 수준의 안전필수시스템에 대한 검증을 위해 필요한 입증자료 및 검증을 위한 조직구성에 대하여 연구한다.

2. 본 문

RAMS활동은 정량적으로 제시된 시스템의 RAMS목표를 관련 규격 및 지침을 바탕으로 객관적 입증자료를 통해 관리하고 승인하는 활동이다.

* 건설교통부, 철도안전과, 회원, 공학박사
E-mail : youngsoo@moct.go.kr
TEL : (02)2110-8276 FAX : (02)503-7305

2004년 10월 22일 철도안전법(법률 제7245호) 제정에 따라, 철도운영자 및 철도시설관리자는 시스템의 도입, 구축, 개량, 유지보수시에 안전을 확인하도록 하고 있다. 따라서, 기존 최종사용자에 의한 시스템 안전확보의 판단기준이 보다 객관적인 증거를 요구하게 되었으며, 확보된 증거의 건전성과 안전확보의 유무를 판단하여 시스템을 승인해야 한다.

최근에는 국제규격을 근거로 시스템 수명주기 전반에 대한 RAMS관리 활동이 제작사를 주축으로 수행되고 있으며, 이러한 활동의 결과로 안전확보를 판단하고 사용을 승인하기 위한 활동은 최종사용자를 중심으로 확대되고 있다.

따라서, RAMS활동을 통해 활동대상에 대한 안전이 확보되었음을 최종사용자 또는 최종사용자가 권한을 위임한 독립기관에서 승인을 실시하고 있다. 승인을 위해서는 SIL과 같이 비교적 정량적인 기준이 사용되게 되었으며, 최근에는 정량화 과정에 대한 건전성을 SIL만족여부와 함께 평가하여 안전확보 유무를 승인하고 있다.

2.1 RAMS활동의 조직구성

RAMS활동은 최종사용자와 공급자 사이의 관계에서 출발한다. 최종사용자는 국가에서 강제하는 사항이나 최종사용자가 원하는 만큼의 RAMS에 대한 목표를 공급자에게 제시해야 하며, 공급자가 목표달성을 입증하기 위해 제출할 문서에 대한 양식과 활동의 범위 및 건전성확보를 위한 책임에 대하여 제시하거나 승인해야 한다. 이러한 RAMS활동의 건전한 수행을 통한 과학적방법의 RAMS평가 및 승인을 위해서 전문적인 지식과 경험이 필요하며, 공급자 측면에서도 이러한 전문성이 확보된 조직을 기관에서 보유하고 있지 않은 경우에 RAMS활동에 대한 전문성의 확보를 위해 그림 1과 같이 전문기관에 제작사와 최종사용자가 각각 위임하여 RAMS활동을 수행할 수 있다.

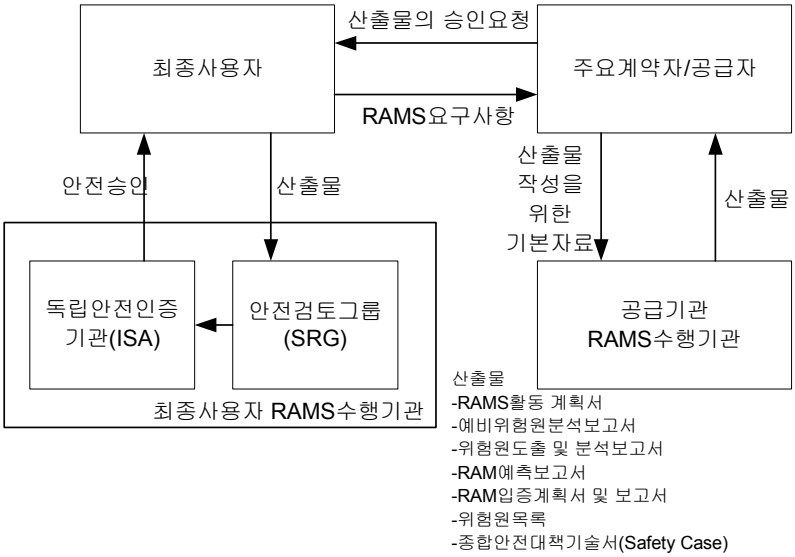

그림 1. RAMS활동의 조직 예

다시 말하면, RAMS활동의 주체는 최종사용자와 제작사이다. 하지만, 철도안전법 제정 등 국내 철도안전환경의 RAMS활동에 대한 건전성과 전문성에 대한 기대치가 높아짐에 따라, 제작사와 최종사용자가 별도로 RAMS활동 및 승인을 위한 전문기관을 지정하여 수행하고 있는 실정이다.

2.2 SIL4의 의미

SIL은 안전관련 전기전자 프로그래머블 제어기의 RAMS규격인 IEC 61508과 철도신호시스템관련 RAMS규격인 IEC 62278(EN 50126)에서 사고와 관련된 고장의 발생빈도를 완화한 수준을 평가할 때 사용되는 기준이다.

SIL은 표 1과 같이 1부터 4까지의 레벨로 표시되며, 각각의 레벨은 위험원(Hazard 또는 Dangerous Failure)의 발생빈도로 정의된다. 따라서 SIL의 대상은 위험원 또는 위험측고장이 되며, 어떤 사고를 발생시키는 위험원 또는 위험측고장인지를 정의해야만 위험측고장률에 대한 안전성측면의 SIL평가가 성립된다. 일반적으로 철도에서 언급하는 SIL4는 사고와 관련된 위험원의 발생빈도로써 표 1의 우측의 위험측고장에 대한 발생빈도를 기준으로 평가된다. 표 1의 신뢰성측면의 고장률 기준은 기대된 기능에 대한 실패의 발생빈도로써 고장발생의 영향이 사고와의 관련여부를 평가하지 않고, 단지 주어진 기능을 실패할 확률을 의미한다. 하지만 신뢰성측면의 고장률에 대한 목표는 SIL보다는 MTBF(Mean Time between Failure)나 MKBF(Mean Kilometer Between Failure)등으로 더 많이 표현된다.

표 1. SIL레벨에 따른 고장률 범위

SIL	신뢰성측면의 고장률(/Hour)	안전성측면의 위험측고장률(/Hour)
4	≧1E-5 to 1E-4	≧1E-9 to 1E-8
3	≧1E-4 to 1E-3	≧1E-8 to 1E-7
2	≧1E-3 to 1E-2	≧1E-7 to 1E-6
1	≧1E-2 to 1E-1	≧1E-6 to 1E-5

따라서, SIL4의 의미는 사고(국내의 경우 철도안전법상의 중대사고인 '열차충돌', '열차탈선', '화재', '건널목')를 먼저 정의하고, 대상시스템의 고장으로 인해 사고를 발생시킬 수 있는 위험원을 분석하여 해당 위험원의 발생빈도가 SIL4의 범위인 단위시간당 10^{-8}미만임을 입증해야한다.

현재 국내 철도환경에서는 안전성의 높고 낮음을 판단하기 위해 SIL을 많이 사용하고 있으며, 특히 본 논문의 모두에서 제시한 바와 같이 적용대상이 결정되지 않은 장치레벨에 대한 안전성의 수준을 이야기 할 때 SIL을 많이 사용한다.

SIL에 대한 관심과 적용이 빈번해 지면서 일부에서는 위와 같은 SIL에 대한 정의를 안전확보와 혼동하여 적용하는 경우가 있다. 예를 들어 "전자연동장치는 SIL4를 만족해야 한다."는 어떤 의미일까? 전자연동장치의 모든 기능이 SIL4, 즉, FMEA(Failure Mode and Effect Analysis)를 통해 도출된 고장모드의 발생빈도가 10^{-8}/hour 미만을 만족해야 함을 의미하는 것일까? 만약 SIL4를 전자연동장치의 모든 기능에 대하여 적용하였다고 하면, 역구내 제어모드에서 진로를 취급하기 위해 사용되는 현장제어판넬의 조작을 위한 마우스와 키보드의 고장발생빈도도 SIL4여야 한다. 이는 전자장비의 평균고장률을 고려할 때 마우스나 키보드를 다중화하지 않고는 불가능한 값이다. 따라서, 전자연동장치가 SIL4를 만족한다는 의미는 모든 고장에 대한 발생빈도가 아닌, 사고와 직결되는 전자연동장치관련 위험측고장, 예를 들어 선로전환기의 도중전환, 불일치, 쇄정의 위험측 해정 등의 위험원에 대한 발생빈도가 10^{-8}/hour 미만으로 완화되었을 때 각 위험원에 대하여 SIL4가 확보되었다고 이야기 할 수 있다.

또한, 위에서 언급한 전자연동장치의 대표적 위험원인 선로전환기 도중전환, 불일치, 쇄정의 위험측 해정 등에 대해서도 위험도를 평가하여 위험도의 허용수준에 대한 사고심각도를 고려하면 전자연동장치가 설치될 역의 규모나 열차의 통행량에 따라 SIL3수준만 확보되어도 안전이 확보될 가능성도 있다.

따라서, 일반적으로 RAMS활동에서 언급하는 위험원도출 및 분석(HIA, Hazard Identification and Analysis)을 위한 FMECA(Failure Mode Effect and Criticality Analysis)나 HAZOP(Hazard and Operability)보고서와 정량적인 위험도 평가를 위한 FTA(Fault Tree Analysis) 및 ETA(Event Tree Analysis) 등의 정량화 보고서가 첨부되지 않은 SIL4 확보의 주장은 아무 의미가 없다.

장치수준으로 RAMS활동이 제한되는 경우에는 위와 같이 HIA보고서가 첨부된 SIL4의 확보를 제사용이 가능하지만 프로젝트 단위 RAMS활동에서는 동일한 시스템이 다른 응용분야에 사용되어 안전하게 운영된 실적이 있다고 하더라도, 철도시스템의 특성상 소프트웨어 또는 인터페이스, 그리고 운영인력에 대한 위험도를 다시 평가해야 한다.

2.3 SIL4의 검증을 위해 필요한 문서 및 행위

RAMS활동관련 규격에서는 수명주기 단계별 최소사항만을 제시하며, 구체적인 활동의 문서화는 영국의 Yellow Book과 같은 문서화 기준이 사용되기도 하지만 국내외 제작사들은 자체 양식을 사용하고 있다.

따라서, RAMS활동을 입증하는 체계 및 구분에 대한 분류는 서로 상이하더라도 표 2와 같이 규격에서 요구하는 핵심사항에 대한 문서화 및 검증활동은 수행되어야 안전이 확보되었음을 확인할 수 있다.

표 2. SIL의 검증을 위한 문서목록

수명주기	관련문서	문서의 요건(제작사 제공)	검증사항(최종사용자 행위)
개념설계 (RFP작성 및 제안단계)	·안전계획서 ·예비위험원분석보고서	**·RAMS활동을 위한 계획** (일정, 투입자원, 관련근거, 예측방법, 입증방법, 위험원의 도출 및 분석방법, 검증을 위한 조직구성 등) **·예비위험원분석** (프로젝트에 적용할 대표 위험원의 선정)	·계획의 승인 (계획에 포함된 방법론에 대한 면밀한 검토가 필요) ·예비위험원분석보고서의 승인 (안전확보의 범위를 승인하는 행위)
설계 및 제작	·RAM예측보고서 ·위험원도출 및 분석 보고서 (기능, 인터페이스, 운영시나리오)	**·구성요소단위 고장률예측** (FMEA와 FTA를 통한 정량적 예측) **·유지보수도 예측** **·위험원도출 및 분석** (FMECA 또는 HAZOP방법등과 같은 정형화된 기법을 사용한 위험원의 도출과 각각의 발생빈도 산출)	·고장모드 및 위험원별 정량적 평가의 건전성 승인 ·누락된 위험원의 확인 및 사용된 안전대책의 적정성과 위험도평가의 건전성 평가
시운전	·RAM입증보고서 ·안전대책확인보고서 ·위험원목록 ·최종보고서	**·RAM예측치의 입증** (시운전시 발생된 고장정보를 바탕으로 입증) **·안전대책확인보고서** (SIL4로 위험원의 발생빈도를 완화시키기 위해 사용된 안전대책의 확인결과) **·위험원목록** (대상에 대한 핵심 위험원을 지속적으로 관리할 수 있는 데이터 시트)	·시운전시 발생된 고장정보의 분석결과 승인 ·적용된 안전대책의 확인 ·위험원목록의 실용성 승인
운영	·위험원목록 갱신	-	·운영시 발생된 고장을 바탕으로 지속적으로 관리 (대상을 포함하여 인터페이스 되는 장치 등의 갱신시 기존 위험원목록도 갱신)

결론적으로 장치의 SIL4를 검증하기 위해서는 제작사가 다음의 문서를 제출해야 한다.

a. SIL4가 확보된 위험원(위험측 동작)과 사고의 목록

b. 위험원분석 증빙자료(FME(C)A 또는 HAZOP보고서)

c. 위험원의 발생빈도 증빙자료(FTA보고서 및 RAM예측/입증보고서)

d. 위험원목록(Hazard Log)

e. 위 사항이 정리된 최종보고서(Safety Case)

3. 결론

본 논문에서는 정량적인 RAMS활동을 위한 위험원의 발생빈도에 대한 안전수준인 SIL의 정의를 명확히 하고, 현재 국내에서 SIL과 관련하여 잘못 알려진 사항에 대하여, SIL의 올바른 적용을 위한 방안을 제시하였으며, 최종사용자의 목표수립에 대하여 제작사에서 제출하는 SIL의 만족여부를 입증하는 문서에 대한 요건, 검토조직, 수명주기별 검증요건을 제시하였다. 이러한 SIL에 대한 정량적인 목표달성 및 활동의 건전성에 대한 검증은 안전성확보의 승인을 발행하기 이전에 필수적으로 구비해야할 사항으로써, RAMS활동의 건전성은 제작사 뿐만 아니라 최종사용자도 단계별 승인과 시스템 인수, 그리고 유지보수와 운영에 대하여 객관화해에 하므로 앞으로도 지속적으로 정량적 판단기준을 포함하여 체계화가 연구되어야 할 것이다.

참고문헌

1. IEC62278(2002), "Railway applications-Specification and demonstration of RAMS", pp.59-65
2. Railtrack(2000), "Engineering safety Management Issue 3, Yellow Book 3", Chapter 8.
3. 한국철도기술연구원(2005), “차상신호(ATP)시스템 구축사업의 RAMS활동계획서”
4. 한국철도기술연구원(2006), “차상신호(ATP)시스템 구축사업의 위험원도출 및 분석보고서(지상장치 인터페이스)”