열차제어시스템 SIL할당 및 입증에 관한 연구

A Study on the SIL Allocation and Demonstration for Train Control System

신덕호† 백종현* 이강미** 이재호***
Shin, Ducko Baek, Jong-Hyen Lee, Kang-Mi Lee, Jae-Ho

ABSTRACT

In this paper, we introduce the estimation method by Risk or SIL(Safety Integrity Level) for the criterion of safety assurance and summarize each application method and target.

IEC 62278(EN 50126) which is international standard for the specification and verification of the railway system RAMS indicate a criterion of safety assurance. Especially, it recommend the safety verification by continuous verification as the order of requirement establishment, design, manufacture, installation, operation, and maintenance for the equipment not easy to quantify the operation environment.

In this paper, we study the SIL requirement allocation method relating to internal new system development and existing system improvement by analysing SIL recommendations which were used to understand SIL for a train control equipment in 1990s in IRSE and theoretically their allocation background.

This paper help the safety management of Korea train control system to develope the quantitative management procedure as international level by analyzing the SIL requirement allocation by operation agency and the right SIL verification procedure by manufacture and indicating the example to assure safety because it is necessary for improvement and localization for the Korea train control system having highly dependence on aboard technology.

1. 서 론

본 논문은 열차제어시스템의 안전확보의 기준으로 사용되는 위험도(Risk) 및 안전무결성레벨(SIL, Safety Integrity Level)에 의한 평가방법에 대하여 소개하고, 각각의 적용방법 및 목적을 정리한다.

철도시스템 신뢰성, 가용성, 유지보수성, 안전성의 명세 및 입증에 대한 국제규격인 IEC 62278(EN 50126)은 안전확보의 기준을 제시하였으며, 특히 운영환경에 대한 정량화가 용이하지 않은 장치의 안전확보기준인 SIL에 대하여 요구사항 수립, 설계 및 제작, 설치, 운영, 유지보수 등의 단계별 검증을 통한 안전입증을 권고한다.

SIL의 이해를 위해 국제신호협회(IRSE, Institution of Railway Signal Engineers)에서 1990년대 사용하던 열차제어시스템 장치단위 SIL권고안을 분석하고, 권고안의 SIL할당 배경을 이론적으로 분석하여, 국내 신규시스템 개발 및 기존 시스템 개량과 관련된 SIL요구사항 할당에 대한 방안을 연구한다. 또한 국외기술 의존도가 매우 높은 열차제어시스템의 개량 및 국산화를 위한 필수요인인 안전확보를 위해, 운영기관이 제시하는 SIL요구사항 할당과 제작사가 수행하는 건전한 SIL입증절차를 연구하고 사례를 제시한다.

2. 열차제어시스템안 안전관리

† 책임저자 : 정회원, 한국철도기술연구원, 열차제어통신연구실, 선임연구원
E-mail : ducko@krri.re.kr
TEL : (031)460-5442 FAX : (031)460-5449
* (정)비회원, 한국철도기술연구원,열차제어통신연구실,선임연구원
** (정)비회원, 한국철도기술연구원,열차제어통신연구실,주임연구원
*** (정)비회원, 한국철도기술연구원,열차제어통신연구실,책임연구원

역간에서는 열차의 간격을제어하고 역구내에서는 열차의 진로를 제어하는 열차제어시스템은 열차의충돌 및 탈선을 방지하는 안전필수설비이다. 따라서 열차제어시스템 내부, 인터페이스, 운영 및 유지보수와 같은 인적요인으로 인해 위험측고장이 발생하는 경우 사고로 직결되는 철도의 위험원(Hazard) 중 대부분을 포함하고 있다.

안전의 정의는 모든 위험원의 위험도(Risk)가 허용할 수 있는 수준으로 제어된 상태를 의미한다. 그러므로 열차제어를 포함한 철도전반에서는 철도응용분야의 신뢰성, 가용성, 유지보수성, 안전성에 대한 명세 및 입증에 대한 규격인 IEC 62278(EN 50126)에서 시스템의 수명주기를 개념설계부터 폐기까지 14단계로 구분하여 각 단계에서의 안전확보를 위한 요구사항 및 검증기준을 제시하고 있다[1].

위와 같은 국제규격을 기반으로하는 안전확보는 위험도의 정량화가 핵심사항으로써 위험도의 구성요소인 위험원의 발생빈도와 심각도를 최대한 정량화 하여 허용할 수 있는 수준으로 억제되었음을 검증하도록 강제하고 있다. 위험도의 허용수준과 관련하여 IEC 62278에서는 위험도매트릭스를 제시하고 6단계 발생빈도와 4단계 심각도를 기준으로 평가된 위험원의 허용여부를 판단하도록 한다.

위험도에 의한 안전확보는 표 1과 같이 위험도허용수준을 정량적으로 구분하고, 도출된 모든 위험원의 위험도를 평가하는 방식으로써, 위험도를 평가하기 위해서는 열차의 운행빈도, 설치/운영/유지보수시 발생할 수 있는 인적오류의 발생빈도 등이 모두 정량화 되어야 한다[2].

표 1. 열차제어시스템 위험도매트릭스의 예(코레일 ATP사업적용)

위험도의 등급	치명적인 위험(Catastrophic) 3인이상 사망	중대한 위험(Critical) 1인사망-3인사망 미만	경미한 위험(Marginal) 1인중상-1인사망 미만	사소한 위험(Insignificant) 1인이하 중상
빈번한 발생(Frequent) 10^{-3}/hour 이상	허용불가	허용불가	허용불가	조건부허용
가능성 있는 발생(Probable) 10^{-4} to 10^{-3}/hour	허용불가	허용불가	조건부허용	허용가능
종종 발생 가능(Occasional) 10^{-6} to 10^{-4}/hour	허용불가	조건부허용	조건부허용	허용가능
발생가능성이 미약함(Remote) 10^{-8} to 10^{-6}/hour	조건부허용	조건부허용	허용가능	무시가능
발생가능성이 거의없음(Improbable) 10^{-9} to 10^{-8}/hour	허용가능	허용가능	무시가능	무시가능
발생가능성이 전혀없음(Incredible) 10^{-9}/hour 이하	무시가능	무시가능	무시가능	무시가능

하지만 열차운영조건 및 인적오류에 대한 발생빈도는 적용대상에 따라 큰 차이를 보인다. 예를 들어 전자연동장치의 대표적 위험원인 선로전환기 불일치를 예로 들면, 위험원의 발생이 사고인 충돌이나 탈선으로 발전하기 위해서는 열차의 운행빈도가 큰 영향을 미친다[3].

따라서 장치가 적용될 운영환경에 대한 분석이 용이하지 않은 경우에 일반적으로 사용하는 안전목표가 SIL이다. 예를 들어 전자연동장치 또는 궤도회로의 구매를 위한 요구사양서에 향후 설치될 노선의 운영정보를 함께 제시할 수 도 있으나, 운영요건이 해당 장치의 설치위치에 따라 편차가 큰 경우에 SIL로 안전목표를 할당하는 것이 잘 알려진 사례이다.

3. SIL할당 및 입증

SIL은 철도안전관련 국제규격인 IEC 62278에서도 언급되지만, 전기전자프로그래머블 제어기를 사용하는 안전필수시스템의 안전규격인 IEC 61508에서도 사용하는 개념으로써, 철도뿐 아니라 안전이 요구되는 산업전반에서 사용하는 기준이며 레벨0부터 4까지 존재한다. 레벨0은 안전과 무관한 위험원의 발생빈도이며, SIL4가 위험원의 발생빈도를 가장 많이 낮춘 수준의 시스템을 지칭하는 기준이다[4].

예를 들어 SIL4수준의 궤도회로장치라는 해당 궤도회로 장치로 인하여 사고를 발생시킬 수 있는 위험

원(일반적으로 열차점유시 궤도계전기 여자유지)의 발생빈도를 10-8/hour이하로 제어하였다는 의미이다. 따라서 SIL을 적용하기 위해서는 분석대상의 위험원을 예비위험원분석(PHA, Preliminary Hazard Analysis) 또는 고장모드영향 및 심각도분석(FMECA, Failure Mode, Effect and Criticality Analysis) 등의 정형화된 기법을 활용하여 모든 위험원이 도출되었음을 입증한 후 각 위험원별 발생빈도를 결함트리분석(FTA, Fault Tree Analysis) 등의 방법을 활용하여 입증해야 한다.

3.1 SIL할당

SIL의 할당은 사업단위 시스템의 안전관리에서는 표 1과 같이 목표 위험도를 만족하기 위한 장치별 위험측 고장(위험원)의 발생빈도를 할당하기 위해서 사용되며, 장치별 단품구매에서는 기존설비에 할당된 위험원 발생빈도 이하를 목표로 제시하여 신규장치로 인한 전체시스템의 위험도증가를 억제하는 것을 목적으로 한다.

2000년 이후에는 철도의 안전을 위험도기반으로 관리하게 되었으며, 특히 열차제어시스템의 분산화 및 첨단화가 빠르게 발전함에 따라 연동장치 또는 궤도회로장치와 같이 일반적인 구성에 대한 SIL목표의 할당이 응용조건에 따라 공통점을 찾기가 점점 어려워지고 있다. 하지만 열차제어시스템을 구성하는 핵심기능의 범위 및 구현방법이 일반화가 가능했던 1990년대에는 표2와 같이 국가별로 열차제어를 구성하는 각각의 기능별 SIL을 할당하여 관리하였으며, 앞에서 기술한 바와 같이 최근까지도 장치별 안전요구사항 할당을 위해서는 SIL이 많이 활용되고 있다[5].

표 2. IRSE가 조사한 유럽국가의 열차제어기능별 SIL할당사례(1992년)[5]

기능구분	독일 DB	영국 BR	벨기에 NMBS	프랑스 SNCF	스위스 SBB	이태리 FS	영국 LUL	오스트리아 OeBB	네덜란드 NS
연동	4	4	4	4	4	4	4	4	4
신호 및 선로전환	4	4	4	4	4	4	4	4	4
열차검지	4	4	4	4	4	4	4	4	4
열차제동	2	2	4	4	2	4	4	2	4
자동폐색	4	4	4	4	4	4	4	4	4
건널목제어	4	4	4	4	4	4	NA	4	4
건널목감시	4	4	2	NA	4	2/4	NA	4	NA
운영자보호	2/4	2	2	4	3	4	4	4	4
제어판넬	4	2	4	4	3	4	NA	4	2
현시장치(안전이동관련)	4	NA	4	4	3	4	NA	4	4
현시장치(운영목적)	2	2	2	2	2	2	2	2	2
원격제어(안전이동관련)	4	4	4	4	3	4	4	4	NA
원격제어(운영목적)	2	2	2	2	2	2	2	2	2
자동열차방호(안전확보주체)	4	4	4	NA	NA	4	4	NA	4
자동열차방호(기관사보조역할)	NA	NA	NA	3	2	NA	NA	2	NA
자동열차방호(자동운전방식)	NA	NA	NA	2	NA	NA	NA	2	NA
자동열차운영(자동운전방식)	NA	2	NA	NA	NA	NA	2	4	NA
열차표시	2	2	2	2	2	2	2	2	2
자동진로제어	2	2	NA	NA	2	2	2	2	2
NA = 해당 없음									

3.2 SIL입증

SIL의 입증은 시스템 또는 장치의 모든 위험원을 도출하여 해당 위험원의 위험도가 표 2와 같이 요구사항에서 할당된 SIL목표를 만족하는 것을 증명하는 절차이다.

분석대상의 범위 및 기능을 그림 1과 같이 요약한 후 분석대상의 기능에 대한 FMECA를 표 3과 같이 실시하여 위험원을 도출하고 각 위험원별 발생빈도를 부품고장률로써 산출한다. 이때 부품의 고장률은 MIL-HDBK-217이나 최근 미국신뢰성센터(RAC)에서 통합한 217Plus등의 기준을 사용하여 예측하고, 신뢰성시험 또는 운영 및 시운전기간 중 발생된 고장분석내용을 근거로 입증된 고장률을 사용한다. FMECA를 통해 도출된 각 기능별 위험원은 사고의 원인이 되는 대표위험원의 세부원인이 된다. 따라서 각 세부위험원별 발생조건의 관계를 그림 2와 같이 FTA를 통해 정량적으로 평가할 수 있다.

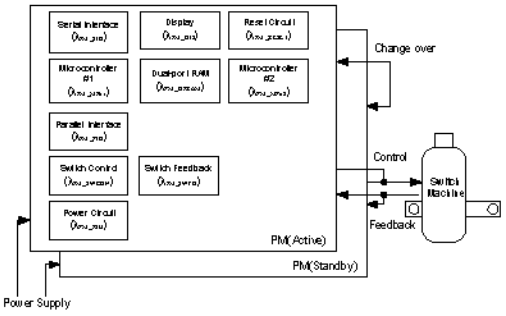

그림 1. 한국형고속철도 IXL의 선로전환기모듈

표 3. FMECA의 예(한국형고속철도 IXL PM)

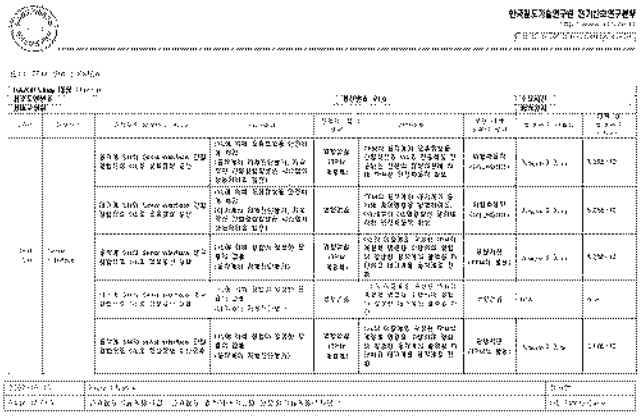

그림 2의 결과는 한국형고속철도 열차제어시스템 전자연동장치의 선로전환기 불일치위험원에 대한 FTA로써 전자연동장치의 대표위험원인 선로전환기불일치의 발생확률이 1.2×10−11/hour로써 SIL4의 기

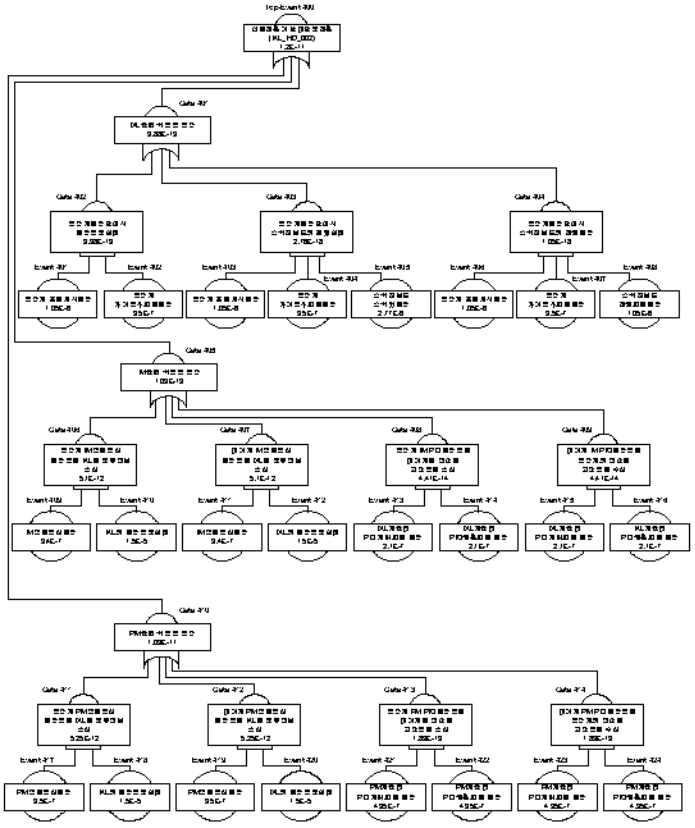

그림 2. 한국형고속철도 IXL 위험원(선로전환기불일치)의 FTA

할당된 SIL목표의 입증과정에서 일반적으로 발생될 수 있는 오류로써 Salami Slicing을 주의해야 한다. Salami Slicing은 그림 2와 같이 대표위험원인 선로전환기 불일치(Top Event)의 발생확률이 SIL4를 만족하지 못하는 경우에 Top Event의 원인이 되는 IXL관련 위험측동작(Gate 401), IM의 위험측동작(Gate 405), PM의 위험측작(Gate 410)으로 SIL목표의 기준이 되는 위험원을 3분할 한 뒤 각각의 위험원에 대하여 SIL4가 만족하는 것으로 SIL4를 입증하는 방법이다. 따라서 고의 또는 부주의에 의해서 발생할 수 있는 Salami Slicing에 의한 안전미확보장치의 안전승인을 방지하기 위해 안전계획서 및 예비위험원 분석보고서에 의한 대표위험원의 선정에는 고도의 전문성과 경험이 요구되고 있다. 또한 그림 2와 표 3에서 사용된 부품 및 기능단위 고장률(λ)은 할당된 SIL목표의 입증에 핵심사항이므로, 고장률의 예측과

입증에 사용된 근거자료는 반드시 검증되어야 할 항목이다.

4. 결 론

본 논문은 열차제어시스템을 포함한 철도의 안전확보의 정의를 확인하고, 국제수준의 안전확보를 위한 기준으로써 위험도평가방식과 SIL에 의한 안전평가방식을 소개하였으며, 특히 순수 장치의 위험원발생 빈도에 대한 안전기준인 SIL의 할당과 입증방안에 대하여 실제 활용된 사례를 들어 현업에 적용할 수 있는 절차를 제시하였다.

한국철도는 과거의 수송능력증대 및 고속화에 올인하는 개발도상국 수준의 기술단계에서, 이미 성숙단계에 접어든 선진국과의 경쟁을 준비하는 단계로 발전되어야 한다. 이를 위해서는 안전성향상 및 안전과 비용의 과학적 분석에 의한 최적화에 대한 연구도 수행되어야 한다.

한국철도의 건전한 안전문화 조성을 위해서는 과거 국산화를 위해 선진국 기술을 모사하던 방식을 탈피하여, 안전에 대한 충실한 기본이론 및 관련 전문가들의 철학이 충실히 반영된 안전관리체계 구축에 대한 투자가 지속되어야 한다.

본 논문은 국토해양부 "한국형 틸팅열차 신뢰성 평가 및 운용기술개발" 연구과제로 수행되었음.

참고문헌

1. IEC 62278(2002.09), "Railway applications -Specification and demonstration of RAMS", pp.13
2. 한국철도기술연구원(2008.01), "코레일 차상신호(ATP)시스템 구축사업의 RAMS활동, 전기기관차 인터페이스 위험원도출 및 분석보고서", pp.16-17.
3. 신덕호외6(2006), "열차제어시스템의 안전입증에 관한 연구", 한국철도학회논문집, 제9권 제4호, pp412-418.
4. IEC 61508(1998.12), "Functional safety of electrical/electronic/programmable electronic safety-related systems"
5. IRSE(1992), "Safety system validation with regard to cross acceptance of signalling systems by the railways", pp. A-18.
6. 한국철도기술연구원(2007), "고속철도기술개발사업, 고속철도 열차제어시스템 안정화기술개발(5차년)", pp22-34.