철도신호분야의 CENELEC 규격과 다른 안전 규격들과의 관계 분석

조현정, 황종규
열차제어·통신연구실 한국철도기술연구원

Study on Relationship between the CENELEC Railway Signaling Standards and Other Safety Standards

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

Abstract - 최근의 컴퓨터화된 철도신호시스템은 증가한 복잡성으로 인해 종래의 장치들에 비해서 고장 발생의 결과가 더욱 심각해졌다. 따라서 시스템 수명주기 전반에 걸쳐서 안전성 확립을 위한 활동을 수행해야 할 것이며, 그 체계를 확립할 필요성이 커지고 있다. 이에 따라, 본 논문에서는 안전과 관련된 국제 규격들과 철도 신호관련의 안전표준들을 분석해 보았으며, 정확한 안전성 개념 파악을 위해서 이들 관계를 연구하였다.

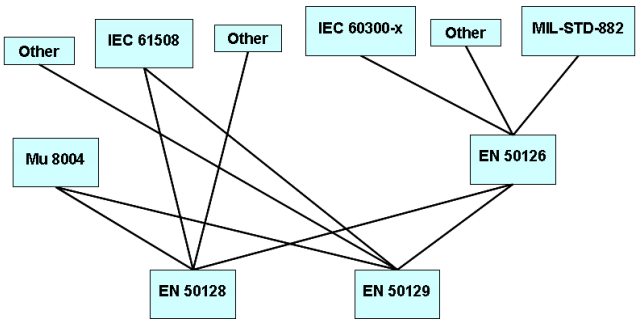
1. 서 론

철도신호시스템(railway signaling system)은 열차의 속도제어 및 진로제어 등을 담당하며, 특히 열차의 충추돌 방지의 기능을 담당하는 열차의 안전운행을 최종적으로 책임지는 바이탈 시스템이다. 최근 들어 컴퓨터화된 철도신호시스템의 사용이 증가함에 따라서 장치들의 고장이 대규모 인명피해나 경제적 손실과 직결되는 경우가 발생하고 있다. 따라서 철도신호시스템의 안전성 확보를 위한 절차를 수행하기 위해 안전성 활동 체계의 확립이 요구되고 있다. 철도신호 분야의 안전을 위해 1990년대 중반에 CENELEC의 철도 신호 체계 표준 초안이 배포되었으며, 이 중 특히 기능적 안전성과 관련된 부분이 많은 관심을 끌었다[1-4]. 이 부분은 동일분야에서는 유일한 국제 표준이였고, 철도 선진국의 수많은 전문가가 참여했기 때문이다. 따라서 철도신호 시스템의 안전성 확보를 위해 CENELEC 표준과 다른 안전 표준의 관계 분석이 선행될 필요가 있으며, 본 논문에서 이를 위한 안전성 개념 확립을 위하여 철도 신호관련 CENELEC 표준과 기타 안전 표준의 국제 규격 간의 관계를 분석하였다.

2. 본 론

2.1 주요 안전관련 규격들의 관계

각종 국제기구와 유럽, 일본, 미국 등의 안전 관련 표준이 많이 있지만, 일반적인 측면과 개념에 있어서 이들 표준은 많은 공통점이 있다. 하지만 세부적인 면에서는 차이가 있다. 예를 들어 TFM(target failure measure), THR(tolerable hazard rates), MTTHE (mean time to hazardous event) 개념은 안전 목표(safety targets) 설정과 관련하여 매우 유사하지만, 목표의 달성을 위한 확인 절차(verification process)는 다르다는 점을 들 수 있다. 이러한 차이를 구체적으로 규격 별로 조사해보면 다음과 같다.



<그림 1> 주요 안전관련 규격들의 관계도

표준도 독립적으로 만들어지는 것이 아니라 서로 영향을 주고받으며 만들어지므로, 각종 표준의 계보를 이해할 필요가 있다. 안전관련 표준들의 계보를 정리해 보면, 그림 1과 같다. 안전성 관련 문서인 IEC 61508이 가장 큰 기여를 했는데, 이 문서는 모든 적용 분야의 기능적 안전성과 관련하여 기본 개념과 접근 방식을 제시하고 있다.

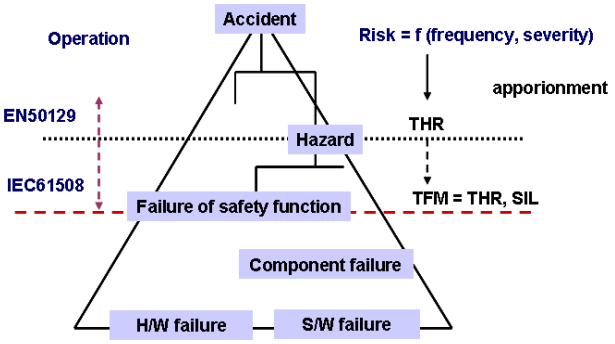
특히 EN 50129[3]의 안전성 케이스와 관련된 부분에 큰 기여를 한 것이 독일의 Mű 8004이다. EN 50129의 기술 안전성 보고서 구조 및 내용은 Mű 8004에서 온 것이다. IEC 61508과 비교하면, 이 문서는 가장 독특한 것이다. IEC 61508은 cross-acceptance의 중요 조건인 압축적 안전성 케이스 구조를 제시하고 있지 않기 때문이다.

유럽 EN 표준의 또 다른 중요한 특징은 RAMS 관리이다. 이 이슈를 다루고 있는 EN 50126[1]의 개발에 큰 기여를 한 것은 US MIL-STD-882와 IEC 60300 시리즈이다[5]. IEC는 의존성을 신뢰성, 가용성, 유지관리성을 총칭하는 용어로 보며, 이를 유럽 규격에서는 RAM이라 한다. 안전성과 의존성 이슈를 서로 다른 2개 기술 위원회가 만든 서로 다른 2개의 표준에서 다룬 점은 IEC 표준의 단점이라 할 수 있다.

2.2 CENELEC 표준과 IEC61508의 안전개념 비교

EN표준은 IEC 61508을 철도 부분에 국한하여 적용시킨 것이다. 하지만 이 둘의 공통점과 차이점을 이해할 필요가 있다. IEC 61508과 EN 50126/EN 50129는 안전성에 대하여 동일한 위험도 기반 정의를 사용하며, 위험원 및 위험도 분석에 대하여 유사한 절차를 채택한다. 모두 사례를 제시하고 있으나 특정 기법이나 위험도 허용 기준을 규정하지는 않는다. 위험 요소 제거를 목적으로 하며, 가능하지 않은 경우에는 위험도 감소를 목적으로 한다. EN 표준은 RAM과 안전성 활동을 RAMS 관리 관점에서 함께 처리한다는 장점이 있다[6].

IEC 61508은 제어 시스템의 기능에 대하여 어떤 컴포넌트가 어떤 시스템의 한 부분인지 명확히 정의하여 대상을 정해놓고 있다. 이 정의는 프로세스 자동화에서 유래한다. 하지만 다른 적용 분야에서는 프로세스 자동화보다 시스템이 훨씬 더 복잡하기 때문에 그 활용도는 제한적으로 보인다. EN 50126과 EN 50129는 시스템 레벨에서 발생할 수 있는 위험 요소에 대하여 전반적인 목표를 정해놓고 있다. safety integrity 기준이 기능적 차원에서 EN 50129에 최종적으로 정의되어 있으며, 이는 IEC가 목표를 정해놓은 레벨과 유사하다.



<그림 2> 목표 지표관련 IEC 61508과 EN 50129의 유사성

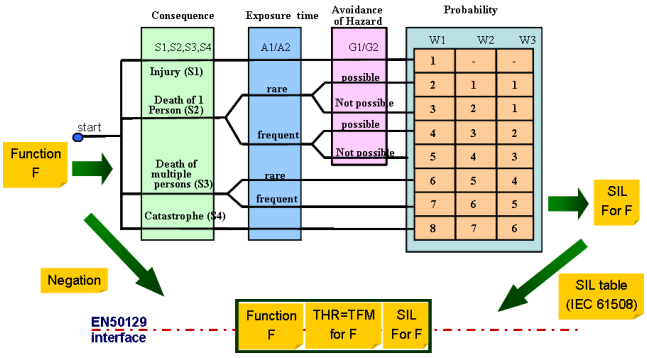
IEC 61508에 TFM이 정의되어 있는데, 이는 랜덤 실패와 시스템적 실패 모두를 대상으로 한다. TFM은 정량화되며 SIL(safety integrity level)과 동일하다. 하지만 랜덤 완전성만 정량적으로 평가할 수 있으며, 시스템적 완전성은 정성적으로 다루어야 한다

는 인식이 일반적이다. IEC 61508은 TFM의 정의가 서로 다른 저요구 운영 모드와 연속 시스템 운영 모드를 구분하고 있다. EN 50129의 THR은 IEC 61508의 TFM을 일반화한 것이다. 어떤 system indenture level에서 정의될 수 있기 때문이다. 연속 모드 기능인 경우에 TFM과 THR은 동일한 개념이고 SIL 테이블도 동일하다. 그림 2는 이를 그림으로 정리한 것이다.

2.3 CENELEC 표준과 독일 안전규격과의 비교

주 선로의 신호 체계에 관한 독일 가이드라인인 Mű 8004는 안전성에 규칙 기반 접근 방식(rule-based approach)을 적용한다. 안전성 애플리케이션 유형별로 디자인 규칙을 정해 놓았으며, 이 규칙을 충족하는 제품은 안전한 것으로 간주한다. 이런 방식은 CENELEC 접근 방식보다 더 건설적이지만, 새로운 기술의 도입과 경쟁 측면에서는 단점을 갖고 있다. Mű 8004는 특정 안전성 아키텍처만을 대상으로 하며, 다른 것은 배제하기 때문이다. Mű 8004와 CENELEC 표준 사이의 또 다른 중요한 차이점은 Mű 8004의 안전성에 관한 정의가 위험도를 기반으로 하지 않는다는 것이다. 그러므로 Mű 8004를 국제 표준으로 정할 가능성은 없다. Mű 8004의 기본 철학은 경험에 근거한 상향식 전략이며, 안전성 시스템은 안전한 컴포넌트의 컬렉션으로 구축된다. 이러한 Mű 8004 접근 방식은 장점이 많은데, 그 장점이 부각되는 안전성 케이스의 구조와 내용, 항목의 독립성에 관한 정성적 규칙과 같은 부분을 CENELEC 표준에 통합시켰다.

지역 또는 매트로 노선의 신호 체계에 관한 또 다른 가이드라인인 VDV 331은 이미 위험도 기반 안전성 접근 방식을 채택하고 있는데, 이는 주로 정성적 위험도 분석 방법인 위험도 그래프를 바탕으로 한다. 이 위험도 그래프는 IEC 61508에서 하나의 예로 언급한 방법이다. 위험도 허용도 기준(risk tolerability criterion)은 직접적으로 표현되어 있지 않으나, 위험도 그래프에 통합되어 있다. 위험도 그래프가 일부 매력적인 특징을 가짐에도 불구하고 EN 50129에서 표준 방법으로 할 수 없었던 이유가 여기에 있다. 또한 GAMAB(globalement au moins aussi bon) 또는 ALARP(as low as reasonably practicable)과 같이 위험도 그래프와 다른 위험도 허용도 기준 사이의 관계도 명확하지 않다. VDV 331이 IEC 61508에 부합하듯이 CENELEC에도 부합하는데, 이는 그림 3에서 VDV 331가 위험도 그래프를 활용하여 기능에 SIL을 부여하는 것을 통해 확인할 수 있다. 이 기능이 제대로 발휘되지 않으면 위험 요소가 되며, IEC 61508 또는 EN 50129의 SIL 표를 활용해 그에 해당되는 THR = TFM을 도출할 수 있다. VDV 331이 지역 노선과 매트로 노선에 대하여 만족스러운 정의와 가이드라인을 제시하고 있지만, 아직까지는 이 접근 방식이 주요 노선 상황에 유의미하게 적용될 수 있음은 증명되지 않았다.



<그림 3> 위험도 그래프를 활용한 안전성 목표 정의 절차

2.4 일본 안전성 가이드라인과의 관계

일본의 경우에 최초의 컴퓨터화된 연동장치 개발 이후, 1980년대에 철도 신호 체계에 마이크로 전자 장치를 도입하는 것과 관련한 안전성 가이드라인을 개발했지만, 아직까지는 부처 내부 문서 수준이다. 보다 정교한 기능과 보다 높은 수준의 시스템 안전성 기준에 대응하여, 1996년에 RTRI사무국과 함께 전문가 위원회가 새로운 안전성 가이드라인을 만들었다. 현재까지는 안전성 가이드라인이 전체적으로 또는 부분적으로 시스템 변형을 포함하여 일부 신규 신호 체계 시스템에 적용되어 왔다. 안전성 가이드라인의 기본 특성은 다음과 같다. IEC 61508에 근거하여 일본에서 철도 신호 체계와 관련해 몇 년 동안 개발된 필수적인 기술 조건을 포함하고 있다. 또한, 라이프사이클 전체에 걸친 안전성 관리 및 기술 활동에 관한 필수 조건을 제시하며, 규정으로써 강제되는 것은 아니다.

IEC 61508 개념이 일본 안전성 가이드라인에 적용되었고 EN 표준도 원칙적으로는 IEC 61508을 토대로 하지만, 이들 사이에는 약간의 차이가 있다. EN 표준은 법적 규정이지만 일본의 안전성 가이드라인은 조언이라는 점이 가장 큰 차이점이다. 또한 가이드라인은 3개 구조로 구성되어 있다는 점도 차이라 할 수 있다. 즉 소프트웨어, 트랜스미션, 시스템을 통합하여 본문, 설명과 정보로 구성된다. 본문은 가이드라인의 기본 사항을 설명하며, 상세하고 구체적인 아이디어와 개념은 설명 부분에서 제시한다. 정보는 설명을 보완한다. 상기 사항 이외에도 EN 50129에 주로 기술된 정량적 분석도 더 논의가 필요한 주제이다. SIL 개념을 설명하고 있는 부록 A에는 정량적 수치별로 SIL을 정의한 표가 있다. 일본의 경우에는 가장 핵심적인 부분을 파악하고 연속적인 안전성 접근법 결과를 확인할 목적에서만 정량적 분석을 적용해야 한다는 인식이 있다.

2.5 미국 표준과의 관계

현재 미국은 유럽의 EN 50126, EN 50128, EN 50129 문서와 같은 프로세서 기반 시스템의 안전성 보증 표준이나 규정이 없다. 미국의 경우에는 공급업체가 자체 기준과 각종 단체가 만든 다양한 표준을 바탕으로 안전성 보증 절차를 채택하는 것이 일반적이다. 현재의 각종 표준이 안전성 핵심 철도 제품/시스템의 안전성 보증과 관련한 모든 주요 부분을 다루고 있지 않거나 동일한 수준으로 엄격하게 다루고 있지 않기 때문이다. 이 분야의 규정이 충분하지 않기 때문에 공급업체는 AREMA(American Railway Engineering and Maintenance-of-Way Association)의 “Communication and Signals Manual of Recommended Practices”, MIL-STD-882C, IEEE 1483-2000, IEEE 1012-1998, 그리고 다른 산업 분야의 기타 표준 등을 활용하고 있다. 안전성 핵심 철도 적용에 프로세서 기반 시스템을 활용하는 문제와 기술 진보에 따른 안전성 문제를 다루기 위해, FRA(Federal Railroad Administration)은 몇 년 전에 기존 규정의 개정 작업을 시작했다. 그에 따라 RSAC(Railroad Safety Advisory Committee)가 설치되었고, NPRM(Notice of Proposed Rulemaking)가 개발되어 CFR(Code of Federal Regulation)을 통해 공표되었다[7].

3. 결 론

이와 같이 철도 신호관련 CENELEC 규격과 IEC 61508이 위험도 기반 접근 방식, 안전성 라이프사이클 개념, 안전성 목표 설정 관련 접근 방식과 같은 부분에서 유사점을 갖는다는 것을 알았다. 이에 반해, system indenture level, 운영 모드의 활용, RAM과 안전성의 통합, 안전성 케이스 개념 부분에서는 서로 차이를 나타낸다는 것을 알았다. 또한, 일본은 CENELEC 규격과 달리 정량적 분석과 절대 목표보다는 안전성 평가 시에 정성적 분석을 강조하며, 정량적 분석은 확인 역할을 한다는 것도 알 수 있었으며, SIL 개념이 미국 철도 산업의 경우에 일반적이 아니라는 것도 확인했다. 이와 같은 각국의 안전관련 규격들과 CENELEC 규격과의 관계 분석 결론이 안전성 개념의 확립과, 앞으로의 안전성 활동 체계 구축에 효율적으로 활용될 것을 기대할 수 있다.

[참 고 문 헌]

[1] EN 50126, Railway applications - The specification and demonstration of RAMS, 1998.
[2] EN 50128, Railway applications - Communications, signalling, and processing systems - Software for railway control and protection systems. 2000.
[3] EN 50129, Railway applications - Safety-related electronic systems for signalling, 2002.
[4] EN 50159-1/-2, Railway applications - Communications, signalling, and processing systems - Safety-related communication in open/closed communication systems. 2001.
[5] IEC 60300, Dependability Management, 1997
[6] Braband, J., RAMS-Management nach CENELEC, SIGNAL+DRAHT, 1998, issue 11.
[7] Standards for the Development and Use of Processor -based Signal and Train Control Systems, Proposed Rule, Federal Register, August 10, 2001.