열차제어시스템 안전성 개념 확립을 위한 국제 표준들의 관계분석

*조현정, 황종규
한국철도기술연구원 신호제어연구실
e-mail : *hjjo@krri.re.kr, jghwang@krri.re.kr*

The Analysis of Relationship between Railway Signaling Standards and Other Safety Standards for Safety Meaning Establishment

*Hyun-Jeong Jo, Jong-Gyu Hwang
Train Control System Research Team
Korea Railroad Research Institute (KRRI)

Abstract

Failures of equipments are linked directly to extensive damages of human lives or financial losses from the increasing uses of railway signaling equipments utilizing computers. Then safety organizations have to establish for guaranteeing safety during the system life-cycle. In this paper, we examine the relationship between railway signaling standards and other safety standards for safety meaning establishment.

I. 서론

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. 따라서 본 논문에서 이를 위한 안전성 개념 확립을 위하여 철도 신호관련 표준과 기타 안전 표준의 국제 규격 간의 관계를 분석하였다.

II. 본론

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.

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 적용분야의 기능적 안전성과 관련하여 기본 개념과 접근방식을 제시하고 있다.

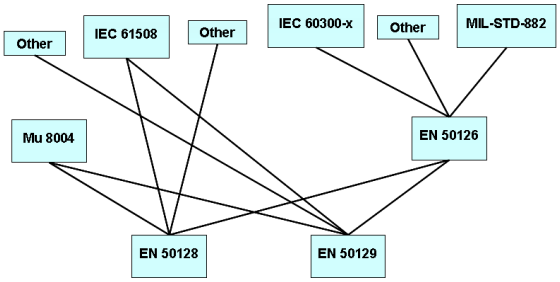

그림 1. 주요 안전관련 규격들의 관계도

특히 EN 50129[1]의 안전성 케이스와 관련된 부분에 큰 기여를 한 것이 독일의 Mu 8004이다. EN 50129의 기술 안전성 보고서 구조 및 내용은 Mu 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[2]의 개발에 큰 기여를 한 것은 US MIL-STD-882와 IEC 60300 시리즈[3](dependability management 기법을 다룬 문서)이다. 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.

Ⅲ. 분석

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 위해 감소를 목적으로 한다. EN 표준은 RAM과 안전성 활동을 RAMS 관리 관점에서 함께 처리한다는 장점이 있다[4].

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.

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 한다는 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.

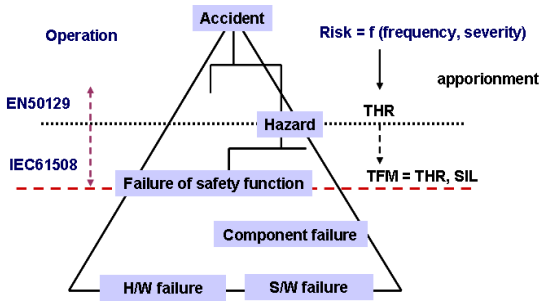

그림 2. 목표 지표관련 IEC 61508과 EN 50129의 유사성

Ⅳ. 결론 및 향후 연구 방향

이와 같이 분석을 통해 철도신호규격 EN 50126/EN 50129와 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. 이러한 결론을 통해 안전성 개념을 확립할 수 있으며, 앞으로 안전성 활동 체계 구축에 효율적으로 활용될 것이다.

참고문헌

[1] EN 50129, Railway applications - Safety-related electronic systems for signalling, 2002.

[2] EN 50126, Railway applications - The specification and demonstration of RAMS, 1998.

[3] IEC 60300, Dependability Management, 1997

[4] Braband, J., RAMS-Management nach CENELEC, SIGNAL+DRAHT, 1998, issue 11.