철도신호 안전성 규격의 세계화 추세와 우리의 대응

The Globalization Trend of Railway Signalling Safety Standards and its Counterplans

김종기* 조연옥** 이종우* 정의진***
Kim, Jongki Cho, Yunok Lee, Jongwoo Joung, Euijin

ABSTRACT

As the European Union has strengthened and computerized signalling systems have been widely used, the European common standards for the safety of railway signalling systems such as EN 50126, EN 50128, ENV 50129, EN 50159 began to be published from 1996 in CENELEC. At that time, a safety guideline, 'Safety Guidelines for Computerized Train Control and Protection Systems' was published in Japan. The Korean National Railroad also published a safety recommendation for the train control systems with taking into account the Korean railway conditions. Now the preparations for IEC/TC9 Standards are well underway and these standards correspond to CENELEC Standards referred above. These movements and activities are to cope with many technical and operational changes and to reflect the globalization trend of railway sectors along with the computerization of signalling devices.

In this connection, this paper studies the globalization trend in the safety standards for railway signalling systems and discusses the counterplans for the trend.

1 서론

철도기술의 발달에 따라 안전성에 관한 관심이 고조되고 전세계적인 자유화 및 개방화, 세계화 추세 속에서 철도신호보안장치의 안전성 규격이 유럽과 일본에서는 1990년대 후반, 한국은 2000년대 초부터 연구되기 시작했다. 이것은 재래식 시스템보다는 새로 개발되고 있는 전자화 및 컴퓨터화된 신호보안장치들을 주요 대상으로 하고 있다.

EU(유럽연합)가 발족되면서 유럽의 철도분야에서는 국가 간의 시스템을 공통화하여 상호간의 열차운행과 시스템의 교류를 원활하게 하는 상호운용성과, EU내의 어느 한 국가에서 안전성이 인증되면 다른 국가에서도 인증하는 제3자 상호인증 등을 주요 개념으로 하고 있는 CENELEC(유럽전기표준위원회) 규격이 속속 발표되고 있으며, 이중 철도신호장치의 안전성에 관한 규격이 EN 50126, 50128, 50129, 50159 등이다. EU내 국가들 사이에서 상호운용성을 높이고 상호인증체계를 구축하기 위해서는 강제성이 뒷받침되어야 하므로 이들 CENELEC 규격들은 법적인 규제력을 가지고 있다.

일찍이 철도선진기술을 개발해온 일본에서는 각계 전문가들의 2년여의 검토 끝에 1996년에 '열차보안제어시스템의 안전성기술지침'을 발표하였다. 이것은 IEC 61508을 토대로 일본에서 배양되어온 컴퓨터제어의 안전성 기술을 총망라한 것이며 규제가 아닌 가이드라인이다.

* 한국철도기술연구원 책임연구원, 정회원
** 한국철도기술연구원 수석연구원, 정회원
*** 한국철도기술연구원 주임연구원, 정회원

우리나라 철도청에서는 2001년에 '열차제어시스템의 안전성확보 기술 권고안'을 발표하였다. 이 권고안은 우리와 철도여건이 비슷한 일본의 안전성기술지침과 유럽의 안전성 인증체계를 참고하여 작성된 것이다.

한편, 철도신호분야의 국제표준화가 IEC에서 진행되고 있다. IEC는 동일분야 다른 기관의 규격이 있으면 그 규격을 투표용 위원회안(CDV: Committee Draft for Vote)으로 상정하여 심의하고 있다. 철도신호의 안전성에 관한 규격이 CENELEC 규격에 있으므로 CENELEC EN 50126은 IEC 62278, EN 50128은 IEC 62279, EN 50159-1과 50159-2는 IEC 62280-1과 62280-2의 CDV로 각각 지정되었다. 이들 규격이 각 국의 IEC 국가위원회에서 심의되었으며 그 결과, 이들 규격이 통과되어 IEC의 최종 국제규격안(FDIS: Final Draft Internatrional Standards) 투표를 기다리고 있다. 이를 통과하면 국제규격이 되어 정식으로 공표된다. 관련 규격중 나머지 EN 50129는 2000년 9월에 IEC의 장래업무(*PWI: Potential new Work Item*)로 지정되어 IEC 규격화 과정을 밟을 예정이다.

곧 이들 CENELEC 규격이 IEC 규격으로 될 것으로 보이며, 유럽은 EU 통합의 맥락 속에서 신호보안장치 사양의 공통화와 법적 규제력을 갖는 규격을 계속 제정하고 이를 국제규격으로 세계에 전개함으로써 유럽에 의한 철도신호의 세계화를 추구하고 있다. 본 고에서는 이러한 철도신호 보안장치에 대한 안전성 규격의 세계화 추세를 고찰하고 우리의 대응방안에 대해 논하고자 한다.

2. 철도신호 안전성 규격의 세계화 추세

2.1 CENELEC 규격의 IEC 규격화

EU 통합의 흐름 속에서 시스템과 장치사양 및 신호보안장치의 개발·운용의 각 프로세스에 대해 안전 요건을 규정하는 CENELEC의 EN계열의 안전성 규격들이 그대로 IEC화 되고 있다. 유럽은 표준규격화를 통해서 각 나라마다 다른 안전 요건이나 사양을 공통화함으로써 이들의 목적을 실현하려고 하는 것이다.

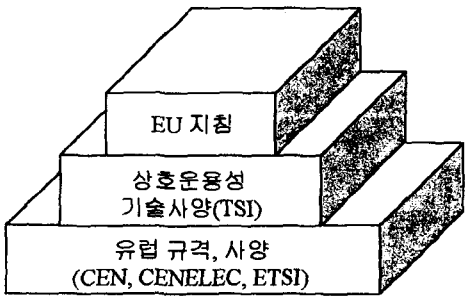

그림 1. 유럽규격의 관계

EU의 정책인 EU 지침과 CENELEC 규격과의 관계를 그림 1.에 나타냈다. 상호운용성을 위한 EU 지침이 최상위에 위치하여 이를 기술적으로 실현하기 위한 사양인 TSI(Technical Specifications of Interoperability)가 그 다음에 위치하고 이를 위한 구체적인 요건을 규정하는 CENELEC 규격이 최하위의 층에 위치한다. CENELEC 규격은 EU내의 시장개방과 상호 운용성을 확보하는데 필요한 신호보안장치 사양과 안전성 수준을 공통화하기 위해 법적 규제력을 갖는다.

신호보안장치를 대상으로 한 철도신호의 안전성 규격으로 CENELEC에는 다음 네 가지가 있다.

- EN 50126(IEC 62278) : RAMS
- EN 50128(IEC 62279) : 소프트웨어
- EN 50129 : Safety Case(문서에 의한 안전성 케이스)
- EN 50159(IEC 62280) : 안전 관련 전송

위의 규격은 일반산업분야에 있어서 컴퓨터제어기능을 대상으로 한 안전성 규격인 IEC 61508을 기초로 해서 UIC(International Union of Railways: 국제철도연합)의 기술지침과 유럽 각 국의 철도신호보안장치의 기술요건을 통합한 것이다. IEC 61508에서는 개념설계에서 폐기까지의 과정 전부를 대상으로 하는 안전성 수명주기와 안전성 요구수준에 맞는 기술요건을 정하는 안전성 무결성 수준(SIL: Safety Integrity Level) 두 가지의 개념을 도입하였다. 이는 수명주기의 각 단계를 엄밀히 구분하고 관리함으로써 불안전한 요소를 제거하는 동시에 요구되는 안전성 수준에 맞추어 다른 안전성 기준을 결정할 수 있도록 한 것이다. 이들 개념에 기초한 안전성 관리의 개념이 철도를 포

합하여 많은 분야에 있어서 향후 주류가 될 것으로 여겨진다. IEC 61508은 위의 CENELEC 규격과 일본의 열차보안제어시스템의 안전성기술지침의 토대가 되었다.

각 나라에서 실시하고 있는 신호보안장치에 대해서 EU내의 어떤 한 나라에서 인증되면 타국에서도 받아들일 수 있다고 하는 것이 상호인증이다. 이 상호인증에 관해서 철도신호를 직접 대상으로 하는 EU 지침은 없으나 유럽통합에서 상호운용성의 맥락 속에서 정해진 목표이다. 이러한 안전성 인증에 관한 방법은 철도신호만의 움직임이 아닌, EU 내에서 안전성에 대한 제3자 인증을 위한 공통의 틀로 규정되었다. 다음은 이들 규격에 대해서 간단히 소개한다.

가. IEC 62278(EN 50126): RAMS

새로운 시스템 개발의 관리방법으로서 개념설계부터 폐기까지 모든 단계를 수명주기로 설정하여 안전성과 신뢰성 등을 확보하기 위하여 각 단계의 과정과 절차를 정하는 일반적인 방법이 도입되고 있다. 이를 규격화한 것이 IEC 62278: 'Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety(RAMS) (EN 50126)'이다. 이 규격은 철도신호뿐 만이 아니라 차량이나 전력설비 등 철도시스템 전반을 대상으로 하여 다음과 같은 기본적인 개념을 취한다.

- 수명주기 각 단계에서 RAMS 관리를 위한 절차와 실시항목을 규정한다.
- RAMS의 요구사항과 그 요구사항이 충족되는 것을 확인하는 절차를 규정한다. 이를 위하여 필요한 분석, 작성해야할 문서를 규정한다.
- 대상 장치·시스템이 안전에 미치는 영향을 평가하는 위험(Risk) 분석을 규정한다. 단, 위험요인(Hazard) 분석, 위험 분석을 수행할 것을 요구하고 있으나 수치에 대해서는 규정하지 않는다.
- RAMS 관리를 위한 일련의 과정에 있어서 관련조직과 관계자의 역할 및 자격 등에 대해서는 유럽의 체제를 전제로 한다.

나. IEC 62279(EN 50128): 소프트웨어

IEC 62279: 'Railway Applications - Communications, Signalling and Processing Systems - Software for Railway Control and Protection Systems (EN 50128)'은 마이크로 전자화된 장치가 증가하면서 프로그램과 관련되는 신호보안장치의 개발에 관한 요구사항 및 절차를 규정한다. 이 규격은 IEC 61508의 Part 3에서 취급하고 있는 소프트웨어에 관한 규격을 토대로 하여 철도신호의 상황을 반영하고 있다. 이 규격의 기본적인 개념은 다음과 같다.

- 소프트웨어의 수명주기 각 단계에서 안전성 확보를 위한 요구사항과 그 요구사항이 충족되는지를 확인하는 과정을 규정한다. 이를 위하여 필요한 방법과 관리, 작성해야할 문서를 규정한다.
- 대상 장치·시스템에 대하여 안전성 기술을 적용하여 감소시켜야할 위험을 SIL에 대응시키고, SIL에 따라 적용해야 할 소프트웨어의 안전성 기술을 규정한다.
- SIL을 0~4의 5단계로 구분하고 안전과 관련없는 항목에 0을 할당하고 가장 높은 안전성이 요구되는 항목에 4를 할당한다. 해당 SIL에 적용이 의무화된 안전성 기술을 사용하지 않는 경우에는 이를 기록할 것을 요구하고 있다.
- 소프트웨어의 설계자, 검증자(Validator), 증명자(Verifier), 평가자(Assessor)의 독립성에 대해서 SIL에 따라 동일 조직과 동일 인물 여부를 규명한다. 가장 높은 SIL의 경우는 설계자와 증명자는 동일조직내 다른 인물이어야 하고 평가자는 다른 조직에 속해야 한다.

다. IEC PWI 9-7(ENV 50129): SAFETY CASE

CENELEC의 철도신호에 관한 안전성 규격은 IEC 61508을 토대로 지금까지 각 나라의 철도신호 안전성기술요건을 통합한 것인데, Fail-Safe를 중심으로 하는 안전성 기술·방법의 상세한 내용은 유럽 내에서도 각 나라마다 차이가 있다. 이러한 점에서 Safety Related Electronic Systems for Signalling(EN 50129)은 철도신호에서 안전 관련 전자시스템의 수용(Acceptance)과 승인(Approval)을

위한 요구사항을 규정하고 있으며, 채택된 방식에 대한 안전성 인증을 위한 문서관리에 중점을 두면서 국가 간의 교차승인(Cross Acceptance)을 목적으로 한 안전성 규격이다.

EN 50129에서는 안전성 인증의 조건으로 품질경영, 안전경영, 기능 및 기술적 안전성 등의 세 가지의 사항에 대해 체계적이고 문서화된 접근을 요구하고 있다. 이 문서에 의한 안전성의 입증을 Safety Case라 하며, 본 규격의 중심개념이다.

라. IEC 62280(EN 50159): 안전 관련 전송

IEC 62280-1: 'Railway Applications - Communication, Signalling and Processing Systems Part 1: Safety-related Communication in Closed Transmission Systems(EN 50159-1)'은 폐전송 시스템에서 범용무선(회선)을, IEC 62280-2: 'Railway Applications - Communication, Signalling and Processing Systems Part 2: Safety Related Communication in Open Transmission Systems(EN 50159-2)'는 개방전송 시스템을 대상으로 하고 있다. 이 규격은 필요한 조건을 요구사항으로 규정하고 있지만 충분하게 조건이 표현되지는 않고 있다. 따라서 EN 50129를 적용하여 관련된 통신의 안전성을 보증할 필요가 있다. 양 규격 모두 특정 통신수단을 거론하고 있지는 않지만 ERTMS/ETCS의 개발로 진행된 무선에 의한 열차제어장치를 염두에 둔 것이다.

본 규격안의 기본적인 개념은 아래와 같다.

- IEC 62280-1의 전용무선(회선)에 대한 규격에는 안전측 고정(Fail-Safe) 전송을 행하기 위해 필요한 18개의 기술요건을 규정한다.
- IEC 62280-2의 범용무선(회선)에 대한 규격에는 보안상의 위험에 대해 해석할 것을 요구하며, 발신원의 특정이나 암호의 사용을 포함하여 필요한 보안대책을 실시할 것을 규정한다.

2.2 일본의 안전성기술지침

일본에서 철도신호보안장치의 마이크로 전자화에 따른 가이드라인이 1980년대부터 마련되기 시작하였으나 처음에는 미미했다. 그러나 차츰 철도신호기술의 첨단화에 대한 관심이 높아지고 이에 따른 안전성 요구사항, 정교한 기능, 비용 효율성 등에 대처하기 위해 대학, 철도회사, 산업계 등의 관련 전문가들이 참여한 전문가위원회를 1994년에 구성하여 2년 후에 '열차보안제어시스템의 안전성기술지침'을 발표하였다.

이 기술지침(가이드라인)은 전자연동장치나 자동열차제어장치 등 고도의 기능과 안전성이 요구되는 마이크로컴퓨터에 의한 신호보안장치의 개발을 지원하고 있으며 지금까지 일본에서 개발된 안전성 기술과 요건을 국제 안전성 규격인 IEC 61508의 주요 개념인 안전성 수명주기와 안전성 무결성 수준(SIL)을 접목한 것이다. 본 기술지침의 탄생 배경은 다음 그림에 잘 나타나 있다.

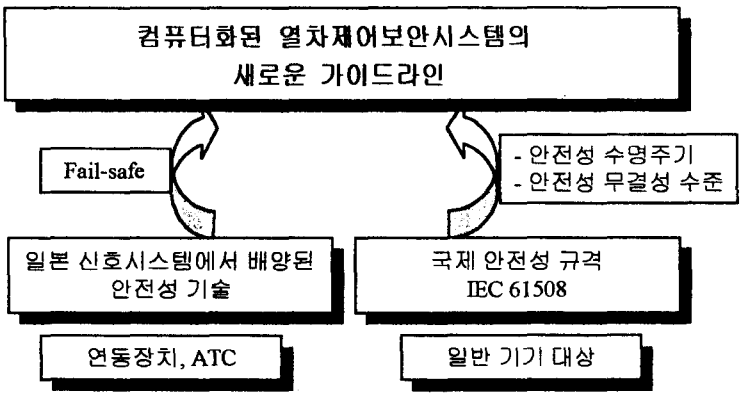

그림 2. 안전성기술지침의 배경

본 가이드라인을 형성하고 있는 기본적인 원리는 다음 세 가지이다.

1. IEC 61508의 토대 위에서 일본 신호기술의 유용한 활용을 위한 기술적인 사항을 포함한다.
2. 수명주기 내내 안전성 관리와 안전성 기술적인 활동에 대한 필요한 사항을 포함하며 규제를 목적으로 하지 않는다.
3. 가이드라인의 본문에서는

기법들이나 수치적인 목표를 규정하지 않으나 해설에서는 IEC 61508에 기초한 표를 제시하고 있다.

이 가이드라인은 열차보안제어시스템의 수명주기 전반에 걸친 안전성 관리와 기술적 활동에 대한 요건을 정했으며 새로 개발되고 있는 마이크로 전자연동장치에 적용되고 있다. 과거의 안전성에 대한 접근방식은 초기 설계, 테스트 등에 초점이 맞춰져 있으나 새로운 접근방식은 수명주기 내내 초기부터 엄격한 관리를 요구하고 있다. 따라서 많은 문서화에 따른 부담이 증가하나 시스템의 변경이나 구형장치의 개량에는 용이하게 안전성을 보증할 것으로 보인다. 기존의 관행을 탈피하여 가이드라인을 적용하기는 어려움이 많으나 가이드라인에 따르는 열차제어보안시스템의 안전성 수준이 향상될 것이다.

일본에서는 1987년 JNR의 민영화 이후로 안전성에 관한 업무를 국토교통성에서 관리하고 있다. 국토교통성은 기반시설 지침에 기초하여 문서 검토, 현장 조사, 테스트를 통해 신호보안장치 설치의 안전성 인증을 수행하고 있다. JR 철도회사는 운영개시 전에 국토교통성으로부터 안전성 인증을 받아야 한다. JR 철도회사는 모든 안전성에 책임이 있으며 JR 철도회사와 공급자들은 국토교통성의 조사 이전에 모든 안전성을 체크한다. 철도회사와 제작사가 새로운 기술들을 장치와 장비에 적용할 경우에는 제삼자에 의해 평가된 안전성 평가 보고서를 첨부한다. RTRI는 안전성 평가를 수행하고 있다. 이 평가는 철도회사나 제작사, 국토교통성의 의뢰로 이루어진다. RTRI의 안전성 평가는 가이드라인에 의거하여 문서에 기초하여 수행되며 대부분의 경우에 공급자 측이 제공하는 일반적인 설계자료와 테스트 결과를 검토하여 수행된다. RTRI는 안전성평가보고서를 작성하며 여기에는 추천사항이 포함되어 있다. 이 보고서는 인증이 아니고 단지 정보일 뿐이다.

3. 우리의 대응

IEC는 국제표준화작업을 효율적으로 진행하기 위하여 세계 각 지역의 표준화 기관과 협력하고 있으며, 가장 중요한 지역인 유럽의 전기분야 표준화 기구인 CENELEC 규격을 적극 수용하고 있다. 유럽 철도신호의 안전성 규격의 경우 그대로 IEC화되고 있는 중이다.

일본의 국토교통성은 철도시스템 중 전기, 차량에 관한 국제규격에 대하여 효과적으로 대응하기 위해 2000년 가을 철도전기기술협회에 국제규격조사검토회를 설치하였다(현재는 철도총합기술연구소에 설치). 이 검토회 산하에는 전기, 차량 시스템에 관한 분과회가 있어 각각 관련 분야의 규격에 대한 검토가 이루어진다. 여기서 심의된 규격안에 대한 답변은 IEC/TC9 국내위원회에서 일본공업표준조사회를 거쳐 IEC에 제출된다.

유럽은 국가 간의 상이한 안전성 규격과 시스템의 차이점, 주변환경, EU 지침, 시장의 개방화, 상호운용성 등을 고려하여 법적인 구속력이 있는 공통 규격을 마련했다. 유럽과의 상황이 다른 일본은 IEC 61508에 기초하여 구속력이 없는 안전성 가이드라인을 제정했으며 이는 일본의 상황에서는 적절한 것이다.

유럽 규격인 CENELEC 규격이 그대로 IEC규격으로 되면 우리에게 많은 영향을 미칠 것으로 예상된다. 그러나 이런 국제표준화는 철도신호에 한정된 것이 아니어서 안전에 관한 분야의 세계적인 동향으로 보았을 때 불가피하다. 그러므로 앞으로 철도신호의 전개 양상과 함께 규격을 검토하고 대응할 필요가 있다. 우리의 현 실정에서 IEC 규격화에 따라 예상되는 점은 다음과 같다.

- 시스템 개발에서 종래에는 제작사가 실시했던 시스템의 기능, 안전성·신뢰성 수준을 제시해야 하는 등 사용자(철도사업자, 고객)의 역할이 중시된다.
- 각 단계에서 문서화를 요구하고 있다. 문서화 부담이 사용자와 제작사에게 모두 증가한다.
- 안전성과 신뢰성에 관한 각종 데이터를 취급해야 한다.
- 검증, 증명, 평가 등에 관한 조직, 인원, 체계 등에 대한 정비가 필요하다.
- 담당기관의 재량권으로 해석될 수 있는 IEC 규격의 구현 깊이에 따라 업무량이 크게 증감될 수 있으므로 재량의 범위가 명확하게 설정되어야 하며 안전성 규격의 적용 경험을 축적해야 한다.

· 제작사나 운영기관에는 안전성과 신뢰성을 위한 별도의 인원과 조직을 구성할 필요가 있다.

각종 국제기관은 ISO/IEC 등의 국제규격을 가맹국에 요구하고 있으므로 각종 제품의 국제표준화는 불가피한 현실이다. 또 최근 국제무역의 개방화, 공통화가 가속되고 있으며 한국이 동북아시아의 물류의 허브로 떠오르면서, 철의 실크로드로 불리는 유라시아 횡단 철도의 거점으로서 장차 남북한 철도와 시베리아 횡단철도(TSR: Trans Siberia Railway), 중국 횡단철도(TCR: Trans China Railway) 등 대륙철도와 연결을 통해 유럽까지 한국철도의 진출이 예상되므로 국제물류 운송에서 철도의 역할이 크게 기대되는 지금 IEC/ISO 국제규격을 적극적으로 수용해야 할 것으로 보이며 이에 대한 대비를 해야한다.

철도신호분야의 경우에는 안전성은 항상 절대적으로 기본적인 것이었고 이미 지난 15년 동안 유럽과 일본은 철도신호분야에 대한 마이크로전자화의 적용에 관한 노하우를 쌓았다. 따라서 폭넓은 안전성 시대로 진입하고 있다는 것은 의심할 바가 없다. 안전성, 비용과 규격의 구현 깊이 등이 세 가지는 삼각관계를 형성한다. 여기에 대한 경험이 축적되면 이 관련성에 대한 구체적인 값을 얻게 될 것이다. 또 복잡한 안전성 관리 접근방식은 필연적이다. 다른 분야의 진보된 안전성 시스템(예를 들어 핵발전, 항공교통제어)에도 유사한 패턴이 이어지고 있다.

우리는 지금 철도신호 세계화의 새로운 시대에 있다. 안전성 관리는 더 이상 전적으로 지역적인 것이 아니다. 15년 전에 철도신호에 대한 마이크로전자화의 소개로 인해 우리의 관점이 크게 변화되었고 오늘날에는 세계적이고 책임있는 안전성 관리가 영향력을 가지고 있다.

우리나라 철도청은 2001년 7월 열차제어시스템의 안전성 확보 기술 권고안을 발표하였다. 본 권고안은 전자화된 신호장치의 안전성 확보를 위한 것으로, 일본의 안전성기술지침과 유럽의 안전성 인증체계를 참조하여 작성되었다. 앞으로 우리의 철도신호 실정에 맞는 세부지침도 마련할 필요가 있다. 우리나라는 아직 안전성 기술, 관리체계 등이 미미하며 이제 철도선진국과 비교할 때 시작 단계에 불과하다. 그러므로 범국민적인 차원으로 산·학·연·관이 함께 연구하고 적용하는 분위기와 조직을 형성하여 지속적으로 우리의 권고안을 연구하고 발전시켜야 할 것이다.

참고문헌

1. 철도청 (2001년), "열차제어시스템 안전성확보 기술 권고안," http://www.korail.go.kr.
2. CENELEC EN 50126, EN 50128, ENV 50129, EN 50159.
3. 이종우 외 4명(2001년), "철도신호제품에 대한 신뢰성과 안전성 검증기준 제정 연구," 한국철도기술연구원 철도청 수탁과제 최종보고서.
4. Yuji Hirao(2001), "New European Norms from a Japanese Viewpoint," Signal+Draht, No. 93, pp. 34-37.