철도 신호보안장치 안전성 규격의 발전동향



김종기 이종우

1. 서 론

신호보안장치는 안전성을 기본 개념으로 탄생했으며, 열차를 안전하고 효율적으로 운행하기 위하여 고안된 설비이다. 안전성, 정확성, 신속성, 대량 수송, 환경친화성, 에너지 효율성 등은 다른 교통수단과 구별되는 철도의 장점이며 이의 달성에는 신호보안장치가 긴요한 역할을 담당하고 있다.

신호보안장치는 Fail-Safe 원칙을 근간으로 개발되었다. 그러나 신호보안장치가 전자화되고 복잡해지면서 철도시스템에서 차지하는 비중이 높아지고, 전세계적인 무역자유화 및 개방화, 국제화 추세 속에서 좀더 체계적이고 일관성 있는 안전성에 대한 접근이 요구되면서 철도신호보안장치의 안전성 규격이 유럽과 일본에서는 1990년대 후반, 한국은 2000년대 초부터 발표되기 시작했다. 이들 안전성 규격은 재래식 시스템보다는 새로 개발되고 있는 전자화 및 컴퓨터화된 신호보안장치들을 주요 대상으로 하고 있다.

열차가 고속, 고밀도로 운행하고 수백명의 승객을 수송하게 됨에 따라 신호보안장치가 고장나거나 오작동할 경우 대형사고로 이어질 가능성이 많아지면서 안전성에 대한 국민적인 요구와 관심이 어느 때보다 높아지고 있다. 그리고 한반도 유사이래 최고의 役事이며 우리의 발전과 번영의 상징이 될 경부고속철도 개통과 함께 한국철도의 남북 종단철도, 시베리아 횡단철도(TSR: Trans Siberia Railway), 중국 횡단철도(TCR: Trans China Railway)와의 연계와 맞물려서 신호보안장치의 안전성에 관심의 초점이 모아지고 있다.

본고에서는 유럽내 각국 철도의 상호운용성(Interoperability)를 높이기 위해 만든 신호보안장치의 안전성에 관한 유럽 규격과 일본 규격의 국제화 동향을 검토하여 한국철도의 국제화 환경에 대한 우리의 대비를 촉구하고자 한다.

2. 철도 신호보안장치 안전성 규격의 세계화 추세

2.1 CENELEC 규격의 세계화(IEC 규격화)

철도 신호보안장치에 대한 대표적인 안전성 규격으로 CENELEC의 다음의 네 가지가 있다. EN 50126, EN 50128, EN 50129, EN 50159가 있다. EN 50126은 철도시스템 전체를 대상으로 RAMS(Reliability, Availability, Maintainability, Safety)를 달성하기 위한 지침과 예증에 관한 내용을 담고 있다. EN 50128은 신호보안장치가 전자화, 컴퓨터화(프로그램화)되면서 소프트웨어 관련 제품의 성능과 품질에 관하여 설계, 구현, 검증, 인증 등에 대해 주로 안전성에 초점을 맞춰 지침을 제시하고 있다. EN 50129는 안전성 인증을 위해 작성해야 하는 문서 즉 Safety Case(안전성 증빙 문서)의 작성에 대한 것이다. EN 50159-1, 50159-2는 Closed Transmission Systems와 Open Transmission Systems의 안전관련 통신에 관한 요구사항들에 대한 것이다.

이들 CENELEC의 철도신호에 관한 안전성 규격들은 IEC 61508을 기초로 하고, 나아가 UIC(국제철도연합)의 기술지침과 각 국의 철도신호시스템의 기술요건을 통합한 것이다. 이들 규격들은 유럽통합의 정신을 철도에 반영하여 EU내 국가들간에 철도에 대한 높은 상호운용성, 상호 인증 등의 맥락을 가지고 만들어졌다.

IEC 61508은 전기, 전자, 프로그램화된 기능을 대상으로 하는 일반산업기기에 대한 포괄적인 안전성 규격으로 총 7개의 파트로 구성되어 있으며 90년대 후반부터 파트별로 공표되기 시작했다. IEC 61508에서는 개념설계에서 폐기까지의 과정 전부를 대상으로 하는 안전성 수명주기(Life Cycle)와 안전성 요구수준에 맞는 기술요건을 정하는 안전성 무결성 수준(SIL: Safety Integrity Level) 등 두 가지의 개념을 도입하였다. 이는 수명주기의 각 단계를 구분하여 관리함으로써 불안전한 요소를 제거하는 동시에 필요한 안전성 수준에 맞추어 다른 안전성 기준을 결정할 수 있도록 한 것이다. 이들 개념에 기초한 안전성 관리의 개념이 철도를 포함하여 많은 분야에서 주류가 되고 있다.

현재 위의 CENELEC 규격들이 IEC 규격으로 되고 있으며 유럽은 EU 통합의 맥락 속에서 신호보안장치 요구사양의 공통화와 법적 규제력을 갖는 규격을 계속 제정하고 이를 국제규격으로 세계에 전개함으로써 유럽에 의한 철도신호의 세계화를 추구하고 있다.

IEC는 IEC 표준 규격을 효과적으로 국제화하기 위해서 가급적 세계 각 지역의 표준화 기관과 협력, 조화를 이루어나가고 있다. 그중 가장 비중있는 지역기관이 유럽전기표준위원회인 CENELEC이다. IEC의 규격이 되는 과정은 먼저 기술위원회(TC: Technical Committee)나 분과위원회(SC: Sub-Committee)에 위원회원안(CD: Committee Draft)이 회부된다. 각 국은 이 위원회원안을 검토하여 타당하면 투표용 위원회안(CDV: Committee Draft for Vote)으로 상정된다. 이 CDV 투표 과정에서 실질적으로 검토되고 기술적인 논평이 제출된다. 여기서 승인조건이 충족하면 최종국제규격안(FDIS: Final Draft International Standards) 단계로 옮겨져 최종 국제규격안으로서 마지막 각국 투표가 실시된다. 여기서 승인조건을 충족하면 국제규격으로 발행된다.

IEC는 신호보안장치의 안전성에 관한 규격으로 앞에서 언급한 CENELEC 4개 규격이 있으므로 EN 50126(RAMS)은 IEC 62278로, EN 50128(소프트웨어)은 IEC 62279로, EN 50159-1과 EN 50159-2는 IEC 62280-1과 IEC 62280-2로 FDIS를 통과하여 IEC의 정식 규격으로 약간의 수정을 거쳐 2002년 발표되었다. EN 50129는 IEC의 장래업무(PWI: Potential Work Item)으로 2000년 9월에 지정되어 IEC 규격화가 진행되고 있다.

가. IEC 62278(EN 50126): RAMS

새로운 시스템 개발의 관리방법으로서 개념설계부

터 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)이며 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 위험도(Risk) 분석을 규정한다. 단, 위험요소(Hazard) 분석, 위험도 분석을 수행할 것을 요구하고 있으나 구체적인 수치는 규정되어 있지 않다.

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 마이크로전자화된 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 충족되는 지를 확인하는 과정을 규정한다. 이를 위하여 필요한 방법과 관리, 작성해야할 문서를 규정한다.
- SIL(Safety Integrity Level: 안전 무결성 수준)을 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 반드시 기록할 것을 요구하고 있다.
- 소프트웨어의 설계자, 검증자(Validator), 증명자(Verifier), 평가자(Assessor)의 독립성에 대해서 규정한다.

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

CENELEC의 철도신호에 관한 안전성 규격은 IEC 61508을 토대로 지금까지 각 나라의 철도신호 안전성 기술요건을 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 품질관리, 안전관리, 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 Closed Transmission Systems

을 , IEC 62280-2: ' Railway Applications - Communication, Signalling and Processing Systems Part 2: Safety Related Communication in Open Transmission Systems(EN 50159-2)' 는 Open Transmission Systems을 대상으로 하고 있다. 이 규격은 ERTMS/ETCS의 개발로 진행된 무선에 의한 열차제어장치를 염두에 둔 것으로 보인다.

본 규격의 기본적인 개념은 아래와 같다.

- IEC 62280-1의 전용무선(회선)에 대한 규격에는 Fail-Safe 전송을 하기 위해 필요한 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

일본에서는 첨단기술이 철도신호보안장치에 도입되면서 이에 따른 안전성 요구사항, 정교한 기능, 비용효율성 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: Safety Integrity Level)을 접목한 것이다.

본 가이드라인을 형성하고 있는 기본적인 원리는 다음 세 가지이다.

가. IEC 61508의 토대 위에서 일본 신호기술의 유용한 활용을 위한 기술적인 사항을 포함한다.

나. 수명주기 내내 안전성 관리와 안전성 기술적인 활동에 대한 필요한 사항을 담고 있으며 규제사항이 아니라 권유사항이다.

다. 가이드라인의 본문에서는 기법들이나 구체적인 목표수치를 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.

3. 결 론

국제사회에서는 ISO/IEC 등의 각종 국제규격 준수나 국제적인 인증을 요구하고 있으므로 각종 제품의 국제표준화는 불가피한 현실이다. 또 최근 한국이 동북아시아의 물류의 허브로 떠오르면서, 철의 실크로드로 불리는 유라시아 횡단 철도의 거점으로서 장차 남북한 철도와 시베리아 횡단철도, 중국 횡단철도 등 대륙철도와 연결을 통해 한국철도가 유럽까지 진출할 것으로 예상되므로 국제물류 운송에서 철도의 역할이 크게 기대되는 지금 ISO/IEC 국제규격을 적극적으로 수용해야 할 것으로 보이며 이에 대한 대비를 해야한다.

유럽 규격인 CENELEC 규격이 그대로 IEC 규격이 됨

에 따라 우리에게 많은 영향을 미칠 것이다. 이런 국제화의 흐름은 이미 철도이외의 많은 분야에서 이루어졌으며 동북아 물류의 중심에 있는 우리에게는 거스를 수 없는 대세이다. 그러므로 앞으로 철도신호의 전개양상과 함께 규격을 검토하고 대응할 필요가 있다. 우리의 현 실정에서 유럽의 규격이 IEC 규격화로 진전됨에 따라 예상되는 점은 다음과 같다.

- 시스템 개발에서 종래에는 제작사가 실시했던 시스템의 기능, 안전성 · 신뢰성 수준을 제시해야 하므로 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, 평가, 인증 등에 관한 조직, 인원, 체계 등에 대한 정비가 필요하다.
- IEC 규격을 적용할 때 재량의 범위가 명확하게 설정되어야 하며 안전성 규격의 적용 경험을 축적해야 한다.
- 제작사나 운영기관에는 안전성과 신뢰성을 위한 별도의 인원과 조직을 구성할 필요가 있다.

우리나라 철도청은 2001년 7월 열차제어시스템의 안전성 확보 기술 권고안을 발표하였다. 본 권고안은 전자화된 신호보안장치의 안전성 확보를 위한 것이다. 우리나라는 아직 안전성 기술, 관리체계 등이 미미하며 이제 철도선진국과 비교할 때 시작단계에 불과하다. 그러므로 범국민적인 차원으로 산 · 학 · 연 · 관이 함께 연구하고 적용하는 분위기와 조직을 형성하여 지속적으로 우리의 권고안을 연구하고 발전시켜 우리의 철도신호 실정에 맞는 세부지침도 마련할 필요가 있다.

우리는 먼저 안전성은 결코 방임해서는 안되는 개인의 생존과 국가의 안위가 걸려있고 기업의 경쟁력, 국가적인 신인도와 직결되는 가장 기본적이고 중요한 요소라는 사실을 이제 철저하게 인식해야 한다. 둘째, 각 철도용품 제작사, 철도운영기관, 안전성 평가기관과 인증기관 등 관련 기관은 안전성을 전담하는 조직과 인력을 강화해야 한다. 셋째, 산학연관 각계의 전문가들로 구성된 위원회를 조직하여 철도신호 안전성 전반에 관하여 검토되어져야 하겠다. 아래는 그 예이다.

- 국내외 신호보안장치 제작사, 운영기관의 안전성 기술 실태 파악
- 제작사, 운영기관, 인증기관 등 각 기관에게 국제 안전성지침을 만족하는 바람직한 역할 제시
- 신호보안장치 및 철도시스템에 대한 안전성 기술의 연구개발
- 국내외 타 분야, 각 기업, 기관의 안전관리(Safety Management) 방식의 벤치마킹
- 안전성 규격의 국제화 움직임을 예의주시하고 각종 국제적인 의사결정에 적극 참여
- TSR, TCR, 북한철도와의 연계, 국제인증 등의 흐름에 대비한 신호보안장치의 발전방향 모색
- 한국의 열차제어시스템의 안전성 확보 기술 권고안의 성력화
- 철도신호보안장치에 대한 인증기관으로서 국제적인 수준의 검증, 평가, 인증 기술력 확보
- IEC 62279의 '6절 인원과 책임'에 규정되어 있는 수준의 충분한 훈련, 경험, 자격을 갖춘 유능한 요원으로 구성된 안전성 전담조직 구성
- 철도 RAMS(Reliability, Availability, Maintainability, Safety)의 필요성에 대한 국민적인 홍보우리는 지금 철도 신호보안장치 세계화의 새로운 시대에 있다. 철도신호에 마이크로전자화가 도입되면서 우리의 기존 접근방식을 크게 전환한 것처럼, 지금은 국제화의 물결 속에서 세계적인 경쟁력이 있고 책임 있는 철도신호 안전성을 위해 다시 한번 전환하고 도약을 해야할 때이다.

참고문헌

1. 철도청 (2001년), "열차제어시스템 안전성확보 기술 권고안," http://www.korail.go.kr.
2. 국제전기기술위원회(IEC) 조직 및 현황, 산업자원부 기술표준원, 1999.
3. IEC 62278, IEC 62279, IEC 62280-1, IEC 62280-2
4. CENELEC EN 50126, EN 50128, ENV 50129, EN 50159.
5. http://www.iec.ch
6. 이종우 외 4명(2001년), "철도신호제품에 대한 신뢰성과 안전성 검증기준 제정 연구," 한국철도기술연구원 철도청 수탁과제 최종보고서.
7. Yuji, Hirao(2001), "New European Norms from a Japanese Viewpoint," Signal+Draht, No. 93, pp. 34-37.
8. Yuji, Hirao and Ikuo, Watanabe, "Safety Technologies and Management of Railway Signalling in Japan," Signal+Draht(92), 5/2000, pp. 33-37.