열차제어시스템의 신뢰성, 가용성, 유지보수성, 안전성

김종기
한국철도기술연구원 철도신호통신연구팀

RAMS of Railway Control System

Jong-ki Kim
Korea Railroad Research Institute

Abstract - IEC 62278, a standard for Railway applications of RAMS, was established in 2002. This IEC standard is based on CENELEC EN 50126 and covered overall railway fields. Activities that had to be performed from concept to decommissioning and disposal of railway system life-cycle, were contained in this standard. On the flow of internationalization, our Railway Authorities and railway support industry need to understand and apply this standard to railway fields. In this paper Railway RAMS in IEC 62278 is introduced.

1. 서 론

열차제어시스템에 대한 대표적인 안전성 규격으로 유럽의 CENELEC 규격에는 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, 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.

현재 위의 CENELEC 규격들이 IEC 규격으로 되고 있다. 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 규격을 신속하게 제정하기 위해서 가급적 세계 각 지역의 표준화 기관과 협력, 조화를 이루어나가고 있다. 그중에서 가장 비중있는 지역기관이 유럽 전기표준위원회인 CENELEC이다. IEC 규격이 되는 과정을 보면, 먼저 IEC내의 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 상정한다. 이 CDV 투표 과정에서 규격이 실질적으로 검토되고 기술적인 논평이 제출된다. 여기서 승인조건이 충족되면 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 IEC 규격화가 진행되고 있다.

2. 본 론

IEC 62278은 철도시스템을 개발하고 운영할 때 RAMS에 관한 규격으로서 본 규격에는 IEC 61508의 안전성 수명사이클(Safety Life Cycle)과 안전성 무결성 수준(Safety Integrity Level) 개념이 반영되어 있다. 총 7개의 파트로 구성된 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 수명사이클(Life Cycle)과 안전성 요구수준에 맞는 기술요건을 정하는 안전성 무결성 수준(SIL: Safety Integrity Level) 등 두 가지의 개념을 도입하였다. 이는 수명사이클의 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.

2.1 IEC 62278의 적용대상

IEC 62278의 적용대상은 제한되어 있지 않다. 지상장치와 차상장치에 관계없이 철도의 구성요소가 되는 시스템 중, 안전성에 관련이 있고 이 규격발효 이후에 계획되거나 개발된 장치나 시스템 예를 들어, 신설노선이나 연장구간의 설비, 개량 설비, 신규개발제품 등이 적용대상이 된다. 본 규격에는 적용대상 시스템의 지정이나 범위에 관한 규정은 없다. 어떤 장치를 시스템으로 다루느냐는 하나하나 개별적으로 검토해야 한다. 즉, 적용대상은 광범위한 대규모의 시스템 전체일 수도 있고, 한 대의 장치일 수도 있다.

본 규격을 활용하는 실시 주체는 철도운영기관, 제작사가 각각 단독으로 또는 공동으로 실시 주체가 될 수 있다.

2.2 RAMS 업무

본 규격의 적용에 따른 업무는 여러 가지로 분류할 수 있으나 주요 업무는 다음과 같다.

2.2.1 안전성 무결성 수준의 설정

본 규격에서는, 허용가능한 위험 레벨을 정할 경우의 기준치는, 각 나라의 안전관련기관이 공인하거나 그 기관의 승인을 받아 철도운영기관이 정한 안전척도로 한다. 본 규격의 실시 주체는 이것을 기초로 대상시스템의 안전성 무결성 수준(SIL)을 책정할 필요가 있다. SIL 값은 0에서 4까지 5단계이다. SIL 0은 안전성과 관련이 없는 수준임을 뜻한다. 안전척도는 각국의 상황에 따라 다르므로 SIL값이 나타내는 안전성은 상대적이지만, 대체로 SIL 1, SIL 2, SIL 3은 고신뢰 시스템의 위험측 고장률에 해당되고, SIL 4는 이른바 Fail-Safe 장치의 위험측 고장률에 해당한다고 볼 수 있다.

2.2.2 RAMS 관리의 문서화

본 규격은 대상 시스템의 RAMS 특성에 관해서 목표를 달성하고 이 수준을 유지하기 위한 전체 프로세스에 대해서 문서화를 요구하고 있다. 각 수명사이클 단계별로 필요한 문서는 일반업무, RAM 업무, 안전성 업무 등으로 분류된 표 1을 참고하여 작성되어야 한다.

수명사이클이 진행됨에 따라 항상 RAMS 특성에 관한 변동상태를 감시하고 안전성에 영향을 미치는 사건이 발생하거나 시스템 개조와 수리를 할 경우에는 반드시 관련 문서를 갱신해야 한다.

2.2.3 관련 조직의 유지

대상 시스템의 RAMS 특성을 유지시키기 위해, RAMS 기술에 정통한 전문인력을 배치해야하고 전문인력이 교체될 경우에는 충분한 인수인계가 필요하다.

2.2.4 수명사이클 전체에 대한 계획

본 규격에서는 시스템의 수명사이클을 시스템 구상단계에서부터 폐기될 때까지 총14개의 단계로 분류하고 있다. 본 규격의 실시 주체는 먼저 대상시스템의 범위를 정의하고, 그 시스템의 전체 수명사이클에 따라 계획하고 예측되는 상황을 수명사이클 14단계로 각각 대응시킬 필요가 있다.

수명사이클의 각 단계와 목적을 다음에 설명한다.

(1) 개념

모든 후속 RAMS 수명사이클 업무가 만족할 정도로 충분히 수행가능하도록 하기 위하여 시스템의 이해도를 향상시키는데 있다.

(2) 시스템 정의 및 응용조건
- 시스템의 임무 프로필을 정의한다.
- 시스템의 범위를 정의한다.
- 시스템의 특성에 영향을 미칠 적용조건을 수립한다.
- 시스템의 위험상태 분석의 범위를 정의한다.
- 시스템에 대하여 RAMS 정책을 수립한다.
- 시스템에 대하여 안전계획을 수립한다.

(3) 위험도 해석
- 시스템과 관련된 위험상태를 규명한다.
- 위험상태를 유도하는 사건을 규명한다.
- 위험상태와 관련된 위험도를 결정한다.
- 위험도 관리를 진행하기 위한 공정을 세운다.

(4) 시스템 요구사항
- 시스템에 대한 전체 RAMS 요구사항을 명기한다.
- 시스템에 대해 RAMS에 대한 종합적인 입증 및 수용기준을 명기한다.
- 후속 수명사이클 단계동안 RAM업무를 통제하기 위한 RAM프로그램을 수립한다.

(5) 시스템 요구사항의 배분
- 시스템에 대한 전반적인 RAMS 요구조건을 설계된 하부시스템, 부품 및 외부설비에 배분한다.
- 설계된 하부 시스템, 부품 및 외부 설비를 위한 RAMS 수용기준을 정의한다.

(6) 설계 및 구현
- RAMS 요구조건에 맞는 하부시스템 및 부품들을 생성한다.
- 하부시스템 및 부품들이 RAMS 요구조건에 따르는 것에 대해 입증한다.
- RAMS를 포함하는 추후 수명사이클 업무에 대한 계획을 수립한다.

(7) 제작
- RAMS 검증 하부시스템과 부품을 생성하는 제작공정을 수행하기 위한 것이다.
- RAMS를 중심으로 한 공정보증체계를 수립한다.
- 하부시스템과 부품의 RAMS 지원체계를 수립한다.

(8) 설치
- 전체 시스템을 구성하기 위해 필요한 하부시스템과 부품들의 전체조합을 조립 및 설치한다.
- 시스템 지원체계를 시작한다.

(9) 시스템 검증(안전성 수용 및 시운전 포함)
- 하부시스템, 부품 및 외부적인 위험 감소수단들의 전체조합이 시스템의 RAMS 요구사항에 부합하는지 검증한다.
- 하부시스템, 부품 및 외부적인 위험 감소수단들의 전체조합을 시운전한다.
- 시스템에 대한 특정 응용 안전증명을 준비하고 적절하다면 수용한다.
- 데이터 수집 및 평가를 제공한다.

단계 10(시스템 수용)의 요구사항이, 만약 고려중인 시스템에 적절하다면, 이 단계(단계 9)의 요구사항과 통합될 수 있다는 것이 중요하다. 만약 이 경우라면, 이 단계의 산출물은 단계 10의 요구사항이 단계 9의 실현에 의해 적절하게 충족되었다는 것을 증명하여야 한다.

(10) 시스템 수용
- 하부시스템들, 부품들 및 외적 위험저감수단들의 모든 조합이 전체 시스템의 전반적인 RAMS 요구사항들에 따르는지를 평가하기 위함이다.
- 영업운전에 들어가기 위해 시스템을 수용하기 위함이다.

(11) 운영 및 유지보수

이 단계의 목적은 시스템 RAMS 요구사양이 만족되도록 하부시스템, 부품 및 외적 위험저감수단 등의 총조합이 운영되고(정해진 제약 안에서), 유지보수되고, 지원되도록 하기 위함이다.

(12) 성능 감시

이 단계의 목적은 시스템 RAMS 성능의 신뢰가 유지되도록 하기 위함이다.

(13) 수정 및 갱신

이 단계의 목적은 시스템 수정 및 갱신 업무가 시스템 RAMS 요구사항을 유지하도록 하기 위함이다.

(14) 폐기처분

이 단계의 목적은 시스템 폐기처분 업무가 통제되도록 하기 위함이다.

표 1 수명사이클 단계별 업무활동과 문서화

단계	일반 업무	RAM 업무	안전성 업무
1	·철도프로젝트의 범위와 목적의 규명 ·철도프로젝트의 개념의 정의 ·재정분석 및 타당성 조사 ·관리체제의 확립	·이전에 달성된 RAM 성과 검토 ·프로젝트의 RAM 관련성 검토	·이전에 달성된 안전성 성과 검토 ·프로젝트의 안전성 관련사항 검토 ·안전성 방침과 안전성 목표 검토
2	·시스템 임무 프로필 구축 ·시스템 개요설명서의 작성 ·운용·유지보수전략 규명 ·운용조건과 유지보수조건의 규명 ·기존의 인프라스트럭처 제약사항들의 영향 규명	·RAM의 과거 경험데이터 평가 ·사전 RAM 분석 ·RAM 방침의 설정 ·장기간 운용·유지보수 조건들 규명 ·기존 인프라스트럭처 제약사항의 RAM에 대한 영향 규명	·안전성에 관한 과거 경험데이터 평가 ·사전 위험요소 분석 수행 ·전체 안전 계획 수립 ·위험기준의 허용범위 설정 ·기존 인프라스트럭처 제약사항의 안전성에 대한 영향 규명
3	·프로젝트 관련 위험도 분석 착수		·시스템 위험요소와 안전성 분석 수행 ·Hazard Log 작성, 위험도 평가 수행
4	·요구사항 분석의 착수 ·시스템 전체 요구사항 명확화 ·환경조건의 명확화 ·시스템 예증과 수용 기준 정의 ·검증 계획 수립 ·관리, 품질, 조직 요구사항의 구축 ·변경관리 절차 구현	·시스템 RAM 요구사항 상술 ·RAM 수용기준 정의 ·시스템 기능적 구조 정의 ·RAM 프로그램 작성 ·RAM 관리체제 확립	·시스템 안전성 요구사항 상술 ·안전성 수용기준 정의 ·안전 관련 기능적인 요구사항 정의 ·안전관리체제 구축
5	·시스템요구사항의 배분 - 하부시스템과 구성요소 요구사항의 상술 - 하부시스템과 구성요소 수용 기준 정의	·시스템 RAM 요구사항의 할당 - 하부시스템과 구성요소 RAM 요구사항 상술 - 하부시스템과 구성요소 RAM 수용기준 정의	·시스템 안전성 목표와 안전요구사항 할당 - 하부시스템과 구성요소 안전성 요구사항의 상술 - 하부시스템과 구성요소 안전성 수용기준 정의 ·시스템 안전 계획 갱신
6	·계획 수립 ·설계와 개발 수행 ·설계분석과 시험 수행 ·설계의 증명(Verification) 수행 ·구현과 검증 수행 ·보급지원 자원의 설계 수행	·다음에 관한 RAM 프로그램 구현 (검토, 분석, 시험, 데이터 평가) - 신뢰성과 가용성 - 유지보수와 유지보수성 - 최적 유지보수 방침 - 보급지원 ·다음을 포괄하는 프로그램 관리 - RAM 프로그램 관리 - 하부계약자와 공급자들의 관리	·다음에 관한 안전 계획 실시 (검토·분석·시험, 데이터 평가) - Hazard Log - 위험요소 분석과 위험도 평가 ·안전관련 설계 의사결정 정당화 ·다음에 관한 프로그램 관리 -안전성 관리 -하부계약자와 공급자의 관리 ·총괄 Safety Case의 작성 ·총괄 응용 Safety Case 마련
7	·생산계획 수립 및 제조 ·구성요소의 하부어셈블리 제조, 시험 ·문서화 마련 ·훈련제도의 확립	·환경 응력 적격심사 수행 ·RAM 개선 시험 수행 ·고장보고분석 및 수정활동 시스템	·안전 계획의 구현(검토, 분석, 시험 및 데이터의 평가) ·Hazard Log 이용
8	·시스템 조립 ·시스템 설치	·유지보수자의 훈련 시작 ·예비부품과 공구 공급 구축	·설치 프로그램 구축 ·설치 프로그램 구현
9	·Commission ·시험운영 수행 ·훈련 착수	·RAM 예증 수행	·Commissioning 프로그램 구축 ·Commissioning 프로그램 구현 ·특정 적용 Safety Case 마련
10	·합격기준에 따른 수용절차 실시 ·수용 증빙자료 수집 ·운행 시작 ·시범운영기간 지속	·RAM 예증 평가	·특정 적용 Safety Case 평가
11	·장기적인 시스템의 운영 ·상시 유지보수 수행 ·상시 훈련 실시	·예비품과 공구의 상시 조달 ·상시 신뢰성 중심의 유지보수 보급지원 수행	·안전성 중심의 유지보수 착수 ·상시 안전성능의 감시 및 Hazard Log 유지보수 수행
12	·운영 성능의 통계데이터 수집 ·데이터의 획득, 분석, 평가	·성능과 RAM 데이터의 수집, 분석, 평가, 사용	·성능·안전성 데이터의 수집, 분석, 평가와 사용
13	·변경요구 절차 구현 ·변경과 개조절차 구현	·변경과 개조를 위한 RAM 관련사항 고려	·개조와 개량에 대한 안전성 관련사항 고려
14	·해체와 폐기 계획 ·해체와 폐기		·안전계획 구축 ·위험요소 분석과 위험도 평가 수행 ·안전계획 구현

2.3 IEC 62278의 영향

본 규격에 따라 예상되는 철도운영기관과 제작사의 업무로 다음이 있다.

2.3.1 규격의 달성에 따른 비용 발생

방대한 문서작업, 관련 조직의 유지, 외부기관에 의한 인증 등을 수행해야 하므로 이에 따른 비용이 발생된다.

2.3.2 개념단계에서 전체 수명사이클 계획 작성

대상 시스템의 개념설정 시점부터 수명사이클 전체에 대한 계획을 작성하여 표 1에 따라 문서화할 필요가 있다.

2.3.3 철도운영기관이 규격 달성 활동에 참여

철도운영기관은 대상 시스템의 SIL 목표값을 제시할 필요가 있다. 그리고 수명사이클 전체에 걸쳐 예상되는 추가 비용이나 운용 중 안전성에 관련된 인적 요소를 고려한 RAMS 사양의 검토도 운영기관의 역할이다.

2.3.4 경제성 분석

본 규격은 목표 SIL의 달성을 절대적인 목표로 상정하고 있으며 동시에 경제성도 달성할 수 있는 활동이 수명사이클 각 단계에서 요구된다. 따라서 이를 위해서는 관련 비용에 관해서 정확한 내역과 분석이 필요하다.

2.3.5 규격의 달성을 위한 관련 기술의 확립

본 규격 및 관련 규격의 올바른 이해, 가용성과 유지보수성에 대한 정량평가가 가능한 데이터베이스의 구축, 인간오류의 발생확률 정보 수집, RAMS 요인들간 정량적인 관계파악, 복합요인을 분리하는 노하우의 취득 및 고장영향의 상세한 분석기술의 확립 등이 필요하다.

3. 결 론

열차제어시스템 관련 유럽의 규격들이 IEC 정식규격으로 발표되고 있다. 이제는 이런 규격을 우리 철도현장에 어떻게 적용해야하며 적용에 따라 수반되는 문제점이나 효과, 주변 국제적인 철도정세에 미치는 영향들에 대해 면밀하게 분석하여 대처해야한다. 이들 안전관련 규격은 장치나 기기의 사양, 시험 등에 관한 제품 규격과는 성질이 다른 시스템 전반이나 관리에 대한 규격이므로 철도운영기관, 제작사, 연구기관 등등 관련 종사자들이 서로 협력하여 공동으로 연구하고 검토하고 현장에 적용하고 그 결과를 다시 반영하는 체제구축이 시급하다.

또 한국을 기점으로 하는 철도의 국제화를 눈앞에 둔 우리에게 유럽통합 맥락 속에서 흘러가고 있는 유럽철도의 통합 움직임은 우리에게 좋은 참고가 될 것이다. 여기서 탄생한 IEC 62278은 우리의 철도가 유럽까지 뻗어나가기 위해서는 반드시 거쳐야할 통과의례이며 앞으로 많은 연구가 필요하다.

[참 고 문 헌]

[1] IEC 62278: Railway applications - Specification and demonstration of reliability, availability, maintainability and safety(RAMS), 2002.

[2] IEC 62279: Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems, 2002

[3] 田代維史, "RAMS(信頼性, 可用性, 保守性, 安全性)," 鐵道と電氣技術, Vol. 14, No. 1, pp. 39-42, 2003.

[4] 平尾裕司, "信號システムの安全性規格," 鐵道と電氣技術, Vol. 14, No.1, pp.51-53, 2003.

[5] 김종기, 이종우, "철도신호보안장치 안전성 규격의 발전동향," 한국철도학회지, 제5권, 제4호, pp. 25-30, 2002.