한국철도학회 철도저널 17권 4호, 2014년 8월, pp. 41–54

유럽철도청(ERA)의 안전관리 및 철도안전 관련 국제규격

서 사 범
㈜서현기술단 부사장
공학박사 · 철도기술사
T.010.6219.1369
suh7484@hanmail.net

Ⅰ. 머리말

철도는 토목시설물, 전기설비 등의 인프라, 차량, 운전, 보수 등의 각종 서브시스템으로 구성되는 종합시스템이다. 지금까지는 주로 철도를 구성하는 장치나 서브시스템에 대한 안전성·신뢰성 기술의 개발이나 실적평가가 이루어져 왔지만, 여기에 더해 고객에 대한 서비스품질, 즉 철도시스템으로서의 안전성·신뢰성에 초점을 맞춘 노력이 중요해지고 있다.

철도의 안전 확보방법은 현재 리스크관리를 기반으로 한 방법으로 수렴된 것으로 보아도 좋을 것이다. 철도에서는 안전관련 신호시스템, 소프트웨어, RAMS 등 몇 개의 리스크 개념을 도입한 IEC 규격이 2002년에 제정되었다. 더욱이, 유럽에서는 유럽연합(EU)지역의 철도 안전과 상호 운용성(Interoperability, EU의 철도정책과 국경을 횡단한 상호운용)을 관리·추진하는 ERA(유럽철도청, European Railway Agency)가 2005년에 설치되어 새로운 전개를 맞이하고 있다. 안전에 관해서 구체적으로는 공통 안전 목표(CSTs) 공통안전기법(CSMs) 공통안전항목(CSIs)을 도입하여 리스크 관리에 의한 안전 확보를 추진함과 동시에, 사고 데이터베이스를 구축하여 정량적 평가 등을 위한 기초 데이터를 얻는 것을 추진하고 있다.

철도차량은 질량이 크고 차륜과 레일간의 마찰계수가 작기 때문에 정지하기까지의 제동거리가 길고, 조타기능이 없기 때문에 안전하게 열차를 운전시키기 위한 열차제어시스템이 발전되어왔다. 열차의 운전에서 이상이 발생된 경우에는 열차를 정지시키는 것이 안전하기 때문에 이상이 있는 경우에는 안전한 상태로 추이하여 그 상태를 유지하는 페일세이프(Fail Safe) 기술이 열차제어시스템의 기반으로 되어 있다. 이와 같은 열차제어시스템에 대하여 유럽에서는 1985년부터 마이크로컴퓨터를 적용하고 있다. 유럽에서는 동 시기에 유럽통합의 문맥 중에 열차제어시스템을 위한 리스크 베이스(risk base)의 각종 안전규격을 작성함과 함께 2004년부터는 철도안전지령 하에 EU역내 철도의 안전관리체계 구축을 진행하고 있다. 철도의 열차제어시스템에는 SIL(Safety Integrity Level) 4에 상당하는 높은 안전레벨이 요구된다.

철도에서 최우선되어야 하는 안전성의 달성에 관하여 근년에 공식적 달성 프로세스 준거를 요구하는 안전관련 국제규격 군이 철도 비즈니스에서 영향력이 늘어나고 있다. 즉, 준거의 증명으로 되는 규격적합성 인증의 유무가 비즈니스의 중요한 요구 사항이 되고 있다. 다시 말해, 해외 철도시장에서는 안전관련 규격에 대한 인증취득의 중요성이 커지고 있다.

본고에서는 철도의 리스크 관리에 대한 적용의 검토에 이바지하는 것을 목적으로 ERA가 수행하는 유럽 철도의 안전관리에 관하여 소개함과 동시에 일반산업분야에서의 기능안전의 관점을 고려하면서 열차제어시스템에 대한 리스크 베이스의 안전 매니지먼트의 대처에 관하여 기술하며, 아울러 철도안전관련 국제규격의 역사 및 구조와 특징을 소개한다.

Ⅱ. 유럽연합(EU)의 안전관련 지령 체계와 유럽철도청(ERA)

1. 철도의 안전 및 상호 운용성에 관한 유럽연합(EU) 지령의 체계

유럽의 철도안전에 관한 유럽연합(EU; European Union) 지령으로서 EU역내 철도의 안전향상과 철도수송 서비스 시장에의 액세스(access) 개선을 목적으로 한 2004/49/EC (Railway Safety Directive)가 2004년에 제정되었다. 이에 따라 그 실시·관리 조직으로서 ERA(유럽철도청, European Railway Agency)가 프랑스 Valenciennes에 설치되었다. ERA의 설치목적과 사명은 Regulation(EC) No. 881/2004(Agency Regulation)에 규정되어 있다.

또한, EU역내의 고속철도 망과 재래선로에 대한 상호 운용성의 실현을 목적으로 하는 EU 지령이 각각 96/48/EC, 2001/16/EC로서 제정되었다(그 후에 두 지령은 2004/50/EC로 수정). 재래철도의 상호 운용성 기술사양이나 기관사 인정기준의 작성, 열차제어시스템 ERTMS (European Rail Traffic Management System) 사양의 변경·관리에 관한 업무는 ERA에서 행해지고 있다.

상호 운용성은 EU역내에서의 공통인 열차제어시스템 ERTMS의 구성 각 장치에 대해 안전 상호인증을 전제로 하고 있으며, 철도안전 지령과 상호 운용성 지령은 안전관리에 밀접하게 관련된다. ERA에서 이들 두 지령에 관한 업무가 행하여지는 이유는 여기에 있다.

또한 EU역내에서는 EU 지침이 실질적으로 법적 규제력을 갖고 있다.

2. 유럽철도청(ERA)의 임무, 조직 및 활동

유럽철도청(ERA, European Railway Agency)은 유럽연합(EU) 회원국의 기술기준과 안전기준에 관한 철도규제 법령의 평준화에 따른 각국 간의 철도 안전성의 향상과 기술적인 상호 기능성을 임무로 하는 기관이며, 2005년 6월 16일에 개청되었다.

유럽은 기본적으로 육지의 연속으로 되어 있어 철도가 국제적으로 운행(승차한 채로 월경)되고 있다(그 중에서도 1987년에 시작한 유로시티·EuroCity는 유명하다). 따라서 각국의 철도 규제법령의 평준화가 필요하게 되어 있으며, 2002년에는 속도규제에 대해 합의를 보았다.

유럽철도청(ERA)은 2004년 4월 유럽철도청규칙(공동체 규칙 2004년 제881호)에 의거하여 설립되었으며, 유럽철도청의 위치는 2003년 12월 유럽위원회의 결정에 따라, 프랑스 릴(Lille)과 발랑시엔(Valenciennes)으로 되었다. 릴에는 유럽철도청의 국제회의장이 설치되고, 발랑시엔에 사무국이 설치되어 있다.

유럽철도청은 안전(Safety) 유닛, 상호 운용성(Interoperability) 유닛, ERTMS 유닛, 경제평가(Economic Evaluation) 유닛, 자원·지원(Resources and Support) 유닛 등 5 개의 유닛(Unit)이 있으며 최근에 상호인수(Cross Acceptance) 유닛이 추가되었다. 안전유닛은 CSTs, CSMs, CSIs의 새로운 구축과 이를 적용하기 위한 가이던스(guidance)의 작성, 안전 데이터베이스의 관리 등을 행하고 있다. 상호 운용성 유닛은 재래철도의 상호 운용성 기술사양과 기관사 인정기준의 작성을 행하고, ERTMS 유닛은 ERTMS 사양의 변경·관리를 행하고 있다. 또한 경제평가 유닛은 ERA로부터의 권고에 대해 평가(assessment)를 행하고 있다.

철도안전을 위한 공통 프레임워크는 철도수송서비스에 대한 효과적인 단일시장을 설정하는 것이 필요하다. 안전유닛(Safety Unit)에서는 철도시스템 활동을 더 좋게 하기 위해 이해당사자에 걸쳐 안전관리 및 지배구조(governance)에 대한 EU의 공통 접근방식을 개발, 촉진 및 모니터링하기 위해 노력하고 있다. 안전유닛은 이 주요 목적을 달성하기 위해 다음과 같은 일을 다루는 세 가지 핵심 섹터(팀)가 있다.

- 관리시스템 섹터(Management Systems Sector)는 철도 섹터 조직에 걸쳐 리스크를 컨트롤하기 위한 새로운 또는 기존의 조화된 접근방법(approaches)을 촉진하고 모니터링 한다.
- 감독·조사섹터(Supervision and Investigation Sector)는 규제기관(National Safety Authorities·국가안전기관 및 National Investigation Bodies·국가조사기관)에 걸쳐 리스크를 컨트롤하기 위한 새로운 또는 기존의 조화된 접근방법을 촉진하고 모니터링 한다.
- 규제·안전모니터링 섹터(Regulation and Safety Monitoring Sector)는 EU레벨에서 리스크를 컨트롤하기 위한 새로운 또는 기존의 조화된 접근방법을 촉진하고 모니터링 한다.

Ⅲ. 철도의 리스크 허용 수준

1. 유럽에서 안전의 원칙

유럽에서는 안전에 관한 원칙으로서 리스크의 허용한도를 수치로서 규정하고 있다. 영국에서는 ALARP(As Low As Reasonably Practicable), 프랑스에서는 GAMAB (Globalement Au Moins Aussi Bon), 독일에서는 MEM (Minimum Endogenous Mortality)로서 판단기준이 나타내어져 있다.

2. 리스크 허용수준에 관한 사고방식

철도에서 신규 시스템의 도입이나 대규모의 개량 시에 리스크가 어느 정도의 수준이라면 수용할 수 있는가 등은 지금까지 명시된 것이 없었다. 최근에 유럽 각국에서 의논되고 있는 리스크 허용수준의 사고방식을 이하에 소개한다.

[영국의 예]

- ALARP(As Low As Reasonably Practicable) : 리스크가 실제의 면에서 타당한 레벨 이하로 저감될 수 있으면 좋다고 한다. 역으로 리스크 저감이 실제상 불가능 또는 안전성 향상/코스트 비율이 어울리지 않고 저대한 리스크가 예측되는 경우에 그 시스템은 수용되지 않는다.

[프랑스의 예]

- GAME(Globalement Au Moin Equivalent principle) : 시스템 전체로서 기존 시스템의 안전성과 동등하다면 허용된다.

[독일의 예]

- MEM(Minimum Endogenous Mortality principle) : 5～15세 어린이의 내재적 사망률(선천적인 신체적 결함에 기인하는 사망률로 이 연대가 최소)의 5 % 이하에 상당하는 리스크 수준 이라면 허용된다. 또한, 당해 어린이의 사망률은 2×10^{-4}(연간 5천 명에 1명)라고 하고 허용수준은 10^{-5}/년으로 된다.

이들 이외에 리스크 허용수준으로서 T. A. Kletz는 자발행위(예를 들어, 자동차를 운전)에 따른 치사 확률과 피재(예를 들어, 교통기관의 승객이나 홍수 피재 등)로 인한 치사 확률을 나누어 전자에 10^{-5}/년을, 후자에 10^{-7}/년을 제안하고 있다. 또한, 사고 시의 치사율과는 약간 다르지만 J. H. Bownen은 화학 플랜트의 치사사고 발생확률의 허용수준으로서 10^{-5}[건/년·시스템]을 제안하고 있다. 이와 같이 10^{-5}/년이 비교적 많이 제안되어 있으며 철도의 운전사고 사망확률의 허용수준에 관하여도 10^{-5}/년을 하나의 안으로 하는 사고방식이 그 간의 실적 치로부터도 타당하다고 생각된다. 철도는 토목구조물, 차량, 신호시스템 등 각종 서브시스템으로 구성되어 있어 서브시스템마다 사명에 따른 리스크 허용수준의 검토도 필요하다고 생각된다.

리스크 허용수준에 과한 상기 이외의 제안 예로서 항공기 분야에서는 ICAO(국제민간항공기관)가 치사사고율 6.5×10^{-7}[건/비행시간]을, 공중충돌 사고율 6×10^{-8}[건/비행시간]을 각각 설정하고 있다. IEC 61508 규격에서는 전기/전자/컴퓨터 시스템에 안전기능을 부가한 경우의 위험側 오동작 확률에 관하여 대상물의 사명에 따라 4단계의 요구수준 SIL(Safety Integrity Level)을 설정하고 있고 가장 안전이 요구되는 시스템(예를 들어, ATC)에서는 10^{-8}～10^{-9}/h(≒ 10^{-4}～10^{-5}/년)가 적용된다.

3. 철도의 리스크 허용 수준

2009년에 철도안전 지령의 실시기관인 ERA(European Railway Agency)가 EU역내 철도의 안전수준 목표치인 CSTs(Common Safety Targets)로서 연간當 0.25×10^{-6}[FWSI/여객열차주행 킬로미터]을 권고하였다. 여기서, FWSI(Fatalities and Weighted Serious Injures)는 중상자를 0.1로 환산한 사망자수이다(FWSI = 1 Fatality + Serious injuries/10). 이 CSTs는 최초의 것이기 때문에 EU 멤버국가의 2004～2007년 철도사고 실적데이터의 평균치에 적당한 하한 허용치를 부가하여 설정하고 있다. 사고실적에는 EU 멤버국가 간에서도 최대 50배 정도의 차이가 있으므로 향후에 더욱 데이터를 축적하여 EU역내의 바람직한 철도의 안전수준에 상당하는 CSTs의 설정을 지향하고 있다.

철도의 안전에 대하여는 사고실적에 의거하여 사고분석은 하고 있기는 하나 리스크(risk) 허용수준에 대하여는 각국 독자적으로 검토가 이루어지고 있는 실정이다. 상기처럼 영국에서는 ALARP(As Low As Reasonably Practicable) 안전원칙에 따라 허용 불가능한 리스크 수준으로서 연간당의 개인사망 확률 10^{-4}, 널리 수용 가능한 리스크 수준으로서 동 10^{-6} 등을 각각 기본적인 상한치로서 정하고 있다. 또한 독일의 MEM(Minimum Endogenous Mortality) 안전원칙에서는 외부요인을 받기 어려운 15세 남자의 개인사망 확률의 5 % 이하의 리스크수준이라면 허

표 1. 치사사고에 대한 허용 리스크 (사망확률/년)

		환산 사망자수 (명)		
		1	10	100
운전사고	허용 수준 R_{A1}	10^{-5}	10^{-6}	10^{-7}
	널리 수용 가능한 수준 R_{A2}	10^{-6}	10^{-7}	10^{-8}
열차사고	허용 수준 R_{B1}	10^{-7}	10^{-8}	10^{-9}
	널리 수용 가능한 수준 R_{B2}	10^{-8}	10^{-9}	10^{-10}

용한다. 그러나 철도의 사고실적과 사회에서 허용되는 리스크 수준의 관계에 대하여는 반드시 명확하게 되어 있지 않다.

이와 같은 상황 외에 철도의 사고실적에 의거하여 허용 리스크수준의 지표 값과 그 타당성에 대하여 검토와 제안이 이루어지고 있다. 그 제안에서는 모든 국민이 철도를 이용할 기회가 있다고 하는 가정을 기초로 하여 철도의 열차사고에 기인하는 사고사망 리스크의 허용수준과 널리 수용 가능한 수준을 제시하고 있다. 구체적으로는 사고사망 리스크(사고의 발생빈도와 사고 1 건당의 평균 사망자수의 곱)를 사고의 규모에 의거하지 않고 일정하게 하여 국민 1인이 1년간에 조우하는 사고사망 리스크의 허용수준 R_{B1}을 $R_{B1}=10^{-7}$, 널리 수용 가능한 수준 R_{B2}를 $R_{B2}=10^{-8}$로 정하며, 후자는 전자보다도 한자리수 엄한 값으로 하고 있다(표 1). 더욱이, 표 1의 R_{A1}와 R_{A2}는 각각 운전 사고에 관한 허용 리스크수준과 널리 수용 가능한 리스크수준이다. 운전 사고에는 중대사고로 이어지기 쉬운 충돌·탈선·화재를 대상으로 하는 열차사고에 더하여 건널목 사고나 선로연변 공사 등의 사고를 포함한다.

이들을 구하기 위해 과거 50년간의 치사사고 데이터베이스를 기초로 하여 열차의 중·대사고의 각 5년간 발생빈도 평균치의 추이를 최소 제곱법을 이용한 회귀식으로 근사하여 최근의 열차사고 발생빈도로 치사 열차사고 발생빈도를 보정하고 있다. 이와 같이 보정된 중·대사고의 열차사고 리스크는 실적치보다도 한 자리수 낮게 된다.

환산 사망자수가 10 명 미만의 소규모인 운전 사고에 대하여는 최근 5년간의 발생빈도와 환산 사고사망자수의 평균치를 취하면, 열차사고의 집합 리스크는 4.6 명/년으로 된다. 또한, 열차사고의 리스크는 운전사고의 리스크보다도 2자리수 정도 작은 것이 구해진다. 이들의 결과를 기초로 100 명 정도의 환산 사망자수인 大사고는 100 년에 1 회의 발생은 수용된다고 하여 $R_{B2}=10^{-8}$로 설정하고 있다. 허용수준에 대하여는 T. A. Kletz의 제안에 의거한 자발적 행위에 기인하는 리스크와 동일하다고 한 운전사고의 허용리스크수준 $R_{A1}=10^{-5}$보다 2자리수 작은 $R_{B1}=10^{-7}$로 하고 있다. 또한, 이들의 리스크수준의 타당성에 대하여는 열차사고의 집합 리스크가 4.6 명/년으로 10^{-8}의 차수이며, $R_{B1}=10^{-7}$을 만족하는 것 등으로 나타내어진다.

Ⅳ. 리스크 허용 수준과 설계지표—SIL의 결정방법

1. 국제규격에 의거한 철도 안전성의 평가

근년에 유럽을 중심으로 하여 국제규격을 정하고 이에 따른 통합적인 철도시스템을 목표로 하는 움직임이 강해져 있고 철도 안전성 평가의 분야에서도 예외가 아니다.

일반적으로 시스템의 안전성에 관하여는 IEC(국제전기표준회의) 규격에 정해져 있으며 이에 따라서 국내 규격을 구축하도록 요구되고 있다. 이하에서는 철도의 안전성에 관한 IEC 규격을 소개한다.

(1) IEC 62278에 의거한 평가

이것은 철도시스템의 신뢰성, 가용성, 보수성, 안전성에 관하여 정량적으로 평가, 관리하기 위한 규격이다. 여기서 정량적인 것은 철도관련 설비의 안전에 관하여 요구되는 레벨(SIL; Safety Integrity Level)을 정하여 사업자의 책임으로 설계, 제조, 관리를 행한다고 하는 생각이다. 표 2에 SIL 레벨과 그 경우에 요구되는 위험側 고장발생 확률의 관계를 나타낸다.

또한, 이 구격에는 시스템의 계획으로부터 폐기까지의

표 2. SIL레벨과 요구되는 위험側 고장발생 확률

SIL 레벨	1시간에 1회 위험側 고장이 발생할 확률(10^{-*}/h)
4	10^{-8}~10^{-9}
3	10^{-7}~10^{-8}
2	10^{-6}~10^{-7}
1	10^{-5}~10^{-6}

일련의 과정(라이프사이클)에서 각각에 요구되는 작업을 실시하여 평가, 관리하여야 한다고 되어 있다.

(2) IEC 62279에 의거한 평가

이것은 철도의 신호보안用 소프트웨어에 관한 규격이지만, 기본적인 요구사항은 IEC 62278의 사고방식을 답습하고 있다.

2. 안전수준의 지표 값 SIL

IEC 61508 등의 기능안전에 관한 규격에서는 주어진 안전수준의 지표 값 SIL(Safety Integrity Level, 안전성 레벨)에 대하여 안전관련 계통이 실현하기 위한 요건만을 규정하고 있으며, 전 장에서 기술한 것과 같은 사회에서 허용되는 리스크 레벨과의 관련에 대하여는 기술하고 있지 않다. 이와 같은 기능안전규격의 SIL은 안전관련 계통 설계를 위한 지표 값으로 해석해야 하며, 본래는 대상으로 하는 설계 시스템의 외부환경인 사회에서 허용되는 리스크 지표 값을 반영하여 설계를 위한 지표 값을 결정해야 하지만, 그를 위한 방법은 반드시 명확하게는 되어 있지 않다.

기계안전에서 기능안전규격인 ISO 13849-1에서는 특정의 위험 원(源)에 대하여 장해의 정도, 위험 원에의 접근빈도, 회피가능성의 3 개를 파라미터로 하는 리스크 그래프에 따라 4단계의 퍼포먼스 레벨을 결정한다. 기계안전의 분야에서는 공장 내 등 설계대상 시스템의 외부환경이 복잡하지 않으므로 리스크 그래프의 적용이 가능하지만, 보다 넓은 외부환경 하에서의 컴퓨터 제어에서는 사회에서 허용되는 리스크지표 값과 설계계통 시스템을 위한 리스크지표 값을 관계지우는 방법이 필요하게 된다.

3. 사회 리스크지표 값과 설계 리스크지표 값의 관련 짓기

제2절과 같은 두 가지 리스크지표 값을 관계붙이는 방법의 하나로서 식 (1)로 나타내는 건널목 제어시스템의 검토예가 나타내어지고 있다.

$$IRF_i = N_i\left\{HR_j \times (D_j + E_{ij}) \sum_{accident\,Ak} C_j^k \times F_i^k\right\} \quad (1)$$

여기서,

IRF_i : 개인의 사망 확률

N_i : 사용회수

HR_i : 해저드(hazard)발생 확률

D_i : 해저드 계속시간

E_{ij} : 폭로시간

C_j^k : 리스크 감소계수

F_j^k : 사망확률

이 검토 예에서의 기본적인 고려방식은 건널목 제어시스템의 해저드 발생확률 HR_i와 건널목의 이용조건 N_i~F_I^k를 관계지우어서 식 (1)과 같이 건널목을 이용하는 개인의 리스크 IRF_i를 도출한다. 여기서 IRF_i를 사회적인 허용리스크로 하여 N_i~F_I^k의 각 파라미터를 대상으로 하는 건널목의 상황을 반영하여 주어지면 식 (1)의 값을 실현하기 위한 HR_j가 구해진다. 이 HR_j가 설계상의 평가지표 값이며, SIL의 지표 값에 대응하는 THR(Tolerable Hazard Rate)에 상당한다.

이 예에서는 10만 명의 자동차 운전자가 건널목을 연간 1,000회 이용하여 사망사고가 생긴다고 하고, 더욱이 1자리수의 여유를 가진 $IRF_i=10^{-6}$으로 하고 있다. 더욱이, $D_i+E_{ij}=10h$ $C_j^k+F_j^k=1.4\times10^{-2}$로 하여 $HRj=7\times10^{-8}h^{-1}$을 유도하고 있다. THR를 $7\times10^{-8}h^{-1}$로 하여 SIL 3의 건널목 제어를 필요로 하고 있다.

이와 같이 함으로써 사회 리스크지표 값과 설계 리스크지표 값을 관계지우는 것이 가능하게 된다. 이 방식에서는 보다 넓은 외부환경의 것에서의 컴퓨터 제어의 기능안전에 대하여도 확장하여 적용할 수 있다.

4. 철도의 수송조건에 따른 설계 리스크지표 값의 결정

한편, 사회 리스크지표 값과 설계 리스크지표 값을 관련지우는 방법으로서 사회적인 조건을 직접 가미하지 않고, 시스템 측만의 조건에서 간접적으로 사회리스크 평가지표 값을 고려해두어 설계 리스크지표 값을 결정한다고 하는 대처도 행해지고 있다. 2009년에 발행된 철도신호시스템에 대한 리스크베이스 평가의 잠정규격 VDE(Verband Deutscher Elektrotechnicker) V 0831-100에서는 정성적인 구분에 따라 새로 할당한 정수치를 정량적으로 다루어 설계지표 값 SIL을 결정하는 방법을 나타내고 있다.

리스크 어세스먼트(risk assessment) 방법으로는 사고발생 확률이나 전자기기의 고장률 등의 데이터에 의거하여 상세한 분석을 하는 정량적인 것과 사고나 고장의 발생 빈도나 사고 손해의 크기를 몇몇의 대략적인 단계로 나누어

분석하는 정성적인 것이 있다. 그러나 실제의 적용에서 정량적인 리스크 어세스먼트에서는 적용하는 데이터의 확실함을 보증하기 위해서도, 코스트를 위해서도 과제가 있고, 정성적인 리스크 어세스먼트에서는 기능안전으로서 철도신호에서 요구되는 보다 정량적인 SIL(SIL 4, $10^{-9} \leqq THR < 10^{-8}$)과의 정합성 확보에 어려움이 있었다.

구체적으로 VDE V 0831-100에서는 사고 손해의 크기에 관하여

T : 사고의 유형(충돌;3, 탈선;2, 소규모충돌;1)
A : 사상자(대다수;4, 다수;3, 소수;2, 극소수;1)
V : 열차속도(고속;8, 160 km/h 이하;7, 80 km/h 이하;5, 40 km/h 이하;3, 25 km/h 이하;2)

을 제시하여 각각의 정도를 정성적인 기술(記述)로 분류하고 있다. 정성적으로 분류한 각 정도에는 0～8의 수치를 할당하고, *T*～*V* 에 대하여 정도에 따른 평가량을 정한다.

또한, 사고의 회피에 관하여

G : 사고의 회피(불가능;4, 불리조건 하에서 스킬 요;3, 좋은 조건 하에서 스킬 요;2, 불리조건 하에서 규칙 행동 요;1)

을 제시하여 마찬가지로 정성적인 기술(記述)에 따라 분류한 정도에 0～4의 수치를 할당하고 있다. 더욱이, 고장의 빈도에 관하여도 마찬가지로 *H* ;고장빈도(매일;17, ～10년에 1회;10, ～30만 년에 1회;1)로 하고 있으며, 고장빈도에 따른 평가량이 결정된다.

최종적으로는 리스크 어세스먼트의 대상으로 되는 신호시스템에 대하여 상기의 고장빈도 *H* 의 평가량, 사고 손해의 *T*～*V* 의 각 평가량의 합, 사고의 회피 *G* 의 평가량의 합계

$$R = H + T + A + V + G$$

을 구하여 합계수량에서 신호시스템에 구해지는 SIL(THR)을 리스크 어세스먼트 결과로서 표에서 얻을 수가 있다.

이들의 기법에서는 사회 리스크 지표 값과의 관계를 정성적으로 분류한 파라미터에 적절하게 반영되어 있는 것이 극히 중요하다. 그 때문에 케이스 스터디에 따른 파라미터 정밀도의 향상이 필요하다. 더욱이, 이와 같은 대처를 리스크 그래프의 파라미터에도 적용하여 리스크 그래프 파라미터의 가감산에서 SIL을 직접 구하는 제안도 이루어지고 있다.

Ⅴ. 유럽철도청(ERA)에서 공통안전기법(CSMs)에 의거한 안전관리

1. 유럽철도청(ERA)에서의 철도안전관리에 관한 검토

유럽철도의 안전관리에서 Railway Safety Directive는 가장 중요한 document이다. ERA이 document에 규정되어 있는 각 조항을 실현·달성하기 위하여 기한을 정하여 ERA를 중심으로 하여 철도의 안전관리를 확립하기 위한 각종 활동이 이루어지고 있다. 또한, Agency Regulation에 의거해 ERA의 구체적인 활동내용이 정해져 있다.

이와 같은 ERA에서의 철도안전관리에 관한 활동으로서 안전관리시스템(SMSs, Safety Management Systems), CSTs(Common Safety Targets, 공통 안전 목표)이나 CSMs (Common Safety Methods, 공통안전기법)가 Safety Unit 내의 두 Sector에서 검토되고 있다. SMSs는 우리나라처럼 상하분리(上下分離) 방식으로 되어 있는 유럽의 철도사업자와 인프라(infrastructure) 관리자에 대하여 각국의 안전관리 당국(우리나라의 국토교통부에 상당)이 인가(Safety Certification and Authorization)하기 위한 것이며, CSTs나 CSMs는 철도의 수송과 설비에 관한 리스크 어세스먼트 방법이다.

2. SMSs(Safety Management Systems, 안전관리시스템)

전 절에서 기술한 것처럼 SMSs는 상하분리(上下分離) 방식으로 되어 있는 유럽의 철도사업자와 인프라 관리자에 대하여 각국의 안전관리 당국을 위한 안전관리시스템이다. Railway Safety Directive의 제9조에는 SMSs의 요건으로서 다음의 4 항목이 규정되어 있다.

① 인프라 관리자와 철도사업자가 CSTs(공통 안전 목표)를 달성하기 위한 SMSs의 제정
② Annex Ⅲ에 따른 SMSs의 요구사항
③ 철도사업자에 대한 인프라 관리자의 열차운전 보증
④ 매년마다 안전 리포트의 제출

실제로는 이들 요건이 대략적이며, 상세한 기술로는 되어있지 않다.

이와 같은 SMSs에 의거한 철도의 안전관리를 실현하기 위하여 대상으로 하는 SMSs가 Railway Safety Directive의 제9조에 적합한가를 판단하는 Assessment Criteria를 ERA가 작성하고 있다. 이 Assessment Criteria에 대하여도 세부

사항까지 기술한 것은 아니고, 각국의 철도사업자와 인프라 관리자에게는 큰 부담으로는 되어있지 않다고 생각된다.

SMSs는 2012년부터 EU 역내에서의 실시를 의무화하도록 되어 있다.

3. CSTs(Common Safety Targets, 공통 안전 목표)

CSTs는 유럽에서 철도의 공동 안전 목표치이며, 철도의 안전레벨을 유지·향상시키는 것을 목적으로 한다. 그 리스크 수용 평가기준으로서 철도에서 개인 리스크(여객, 철도종사원, 건널목. 기타)와 사회 리스크가 이용된다. CSTs는 넓게는 SMSs(안전관리시스템)의 범주에 들어간다고 보아도 좋다.

CSTs는 SMSs에서 철도사업자와 인프라 관리자에 직접 관계되는 목표치이며, ERA가 2008년에 그 산출방법을 권고로서 나타내고 있다. 그 산출방법에 대하여는 2008년도의 보고서에도 기술되어 있는 것처럼 Eurostat(EU의 공적 통계데이터 기관)의 데이터에 가중 이동 평균 등의 처리를 가하며, CSTs는 각 EU 멤버국가(25 국가)의 철도 안전레벨(NRVs, National Reference Values)을 현시점에서 모두 만족시킴과 함께 각국에서는 각각의 현행 안전레벨을 하회하는 것은 허용되지 않는다. 이와 같은 CSTs는 EU 멤버국가 중에 가장 안전레벨이 낮은 국가의 값으로 결정되어 그 의미가 의문으로 되지만, 안전관리를 위한 공통의 틀을 구축하기 위한 하나의 과정으로 보아야 할 것이다.

더욱이 CSTs의 구체적인 단위는 환산 사망자수/여객열차·km 등 사고 데이터에 의거한 것이다. 더욱이 철도전체에서의 안전레벨과 개개의 선구 종별 (고속선로, 재래선로 등) 마다로 정의되는 것으로 되어있다

4. CSMs(Common Safety Methods, 공통안전기법)

CSMs는 안전레벨, CSTs(공통 안전 목표)의 달성, 관계 안전요건 등을 어떻게 평가하는지를 나타내기 위한 것이다. 이러한 CSMs 내용은 다음과 같이 두 가지로 나눠 검토되고 있다.

① CSIs(공통안전항목)를 이용한 CSTs(공통 안전 목표)의 달성에 대한 안전 퍼포먼스(performance)의 평가를 위한 통계적 방법

② 안전레벨과 안전요건에 대한 적합성 평가를 위한 예측的 리스크 어세스먼트(risk assessment) 방법

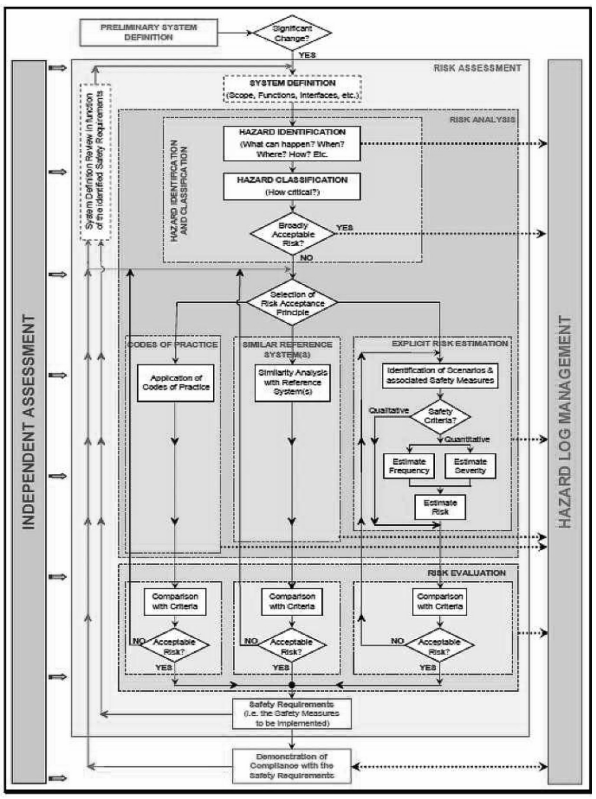

그림 1. CSMs의 리스크 어세스먼트 프레임 워크

CSMs는 철도의 수송과 설비에 관한 리스크 어세스먼트 방법(그림 1)이며, 제2절의 SMSs(안전관리시스템)가 조직적인 관리에 중점이 있음에 대하여 보다 기술적으로 운전과 설비를 대상으로 하고 있다고 볼 수가 있다.

전술한 것처럼 EU역내 철도의 안전향상을 목적으로 한 철도안전지령이 2004년에 제정되었다. 구체적인 EU 내 철도의 안전관리 CSMs 기법으로서 안전 레벨과 안전요건에의 적합 어세스먼트를 위한 기법이 EU 규정으로서 2009년에 발행되었다.

설비의 갱신이나 새로운 시스템의 개발 등에서는 리스크 어세스먼트가 필요하며, 그런 의미에서 CSMs는 중요한 것이다. ERA가 2007년에 구체적으로 어떻게 리스크 어세스먼트를 수행하여야 하는가에 대하여 CSMs에 관한 권고를 제시했다. 이 권고의 특징은 최초로 해저드(hazard)의 확인과 분류를 행하여 철도시스템에 대한 변경이나 신규성 영향의 크기에 따라서 안전에의 영향을 평가하기 위한

리스크 수용원칙을 선택하는 것이며, 코스트 등도 고려하여 현실적으로 타당한 것이라고 생각된다.

이와 같은 CSMs에 대한 ERA의 권고를 기본으로 하여 Railway Safety Directive의 제6조 제3항 (a) CSMs의 리스크 평가·어세스먼트를 대상으로 한 Regulation안이 검토되어 공개되었다. 또한, Regulation으로서 정식으로 제정되어 리스크 평가·어세스먼트의 방법으로서 규제력을 갖고 있다.

리스크 평가와 어세스먼트 기법은 열차제어시스템의 인증에도 관계되며, 최초로 해저드(hazard)의 확인과 분류가 이루어져 열차제어시스템에 큰 변경이 있다고 판단되었을 때만 CSMs가 적용된다. 그때

① 기존의 규격類(code of practice)
② 동양(同様)의 참조시스템(similar reference system)
③ 명시적인 리스크 평가(explicit risk estimation)

등 3개의 리스크 허용원칙이 취해진다. 이것은 이미 사용되고 있는 규격類나 동양(同様)의 참조시스템이 있다면, 그들의 종래부터의 안전 확보방법의 적용을 인정하며, 해당되는 종래부터의 방법이 적당하지 않을 때만 명시적인 리스크 평가를 하는 것이다,

컴퓨터 제어를 이용한 열차제어에서도 페일 세이프 기술이 도입되고, 그 기술적 요건은 안전규격에도 규정되어 있다. CSMs의 적용에서도 그 중요성은 변하지 않는다.

또한, 안전과 시스템기능 양쪽을 향상시키기 위한 방법으로서 RAMS(Reliability, Availability, Maintainability and Safety)가 열차제어시스템, 차량 등의 철도시스템을 대상으로 하여 도입되고 있다. RAMS에서는 안전과 열차운행 정시성의 두 가지가 중요하게 되며, 시스템의 안전성과 신뢰성을 실현하는 기능안전을 포함하는 프로세스 관리로 되어 있다.

5. CSIs(공통안전항목)

CSIs는 CSTs(공통 안전 목표)의 결정과 안전레벨을 파악·관리하기 위해 각국의 안전관리 당국에서 ERA로 제공되는 사고나 안전설비에 대한 데이터이며, 철도안전 지령에 구체적인 내용을 나타내고 있다. 또한 SMSs(안전관리시스템)에 대하여는 철도운행 조직 또는 인프라관리 조직이 그 업무의 안전관리를 위한 것이며, CSTs와 CSMs가 이를 위한 기초가 된다.

6. 안전 데이터베이스의 구축

CSTs(공통 안전 목표)의 결정, EU역내 철도안전레벨의 파악·관리, 더욱이 CSMs(공통안전기법)의 검토에 유효하게 활용할 수 있는 충분한 철도 안전 데이터베이스를 구축하기 위해 유럽 내의 전 분야를 대상으로 한, Eurostat(통계 데이터 취급조직)의 비교적 거친 데이터를 이용하여 CSTs이 검토되었다. 2007년 이후부터는 ERA에 각국의 안전관리 당국에서 CSIs(공통안전항목)가 제공되어 데이터가 축적되었다. 다만, 이 데이터는 설비의 고장에 관한 자세한 내용을 포함하는 것이 아니므로 구체적으로 CSMs의 리스크 평가와 어세스먼트에 직접 사용할 수 있는 것은 아니라고 하며, 이러한 상세한 평가·어세스먼트를 위한 데이터는 각국의 관계 조직 내에 있고 EU역내에서 공통인 안전 데이터베이스 구축까지에는 이르지 못한 것으로 보인다.

7. 정리 및 고찰

이상으로 유럽철도청(ERA)에서의 철도안전관리에 관하여 기술하였다. 이를 정리하여 고찰하면 다음과 같다.

① 유럽의 철도는 정량적인 안전레벨을 정하는 CSTs(공통 안전 목표)와 CSTs의 달성 및 관계 안전요건을 어떻게 평가하는지를 나타내는 CSMs(공통안전기법)에 따라 리스크 관리를 기반으로 한 안전관리의 실현을 목표로 하고 있다. 이러한 배경에는 EU역내 수송기관으로서의 철도의 지위 확보와 철도산업 시장의 개방(open)化가 있다.

② CSTs(공통 안전 목표)와 CSMs(공통안전기법)의 검토에서는 EU역내의 관계 조직(안전관리 조직, 철도운행 조직, 인프라관리 조직, 산업계 등)에서 널리 의견을 구하고 이를 반영하는 방법(approach)이 취해지고 있다. 그 결과, 검토·권고 내용은 현상(現狀)을 고려한 것으로 되어있다.

③ CSTs(공통 안전 목표)에 대하여는 수치에 의거한 정량적 목표 안전레벨을 결정하는 것이며, 철도에서의 개인 리스크(환산 사망자 수 / 여객열차 · km)를 이용하여 EU 회원국 모두가 현시점에서 클리어(clear)할 수 있는 ALARP(As Low As Reasonably Practicable)의 허용가능 영역의 상한치를 검토하고 있다.

④ 또한, 철도신호시스템의 리스크 평가는 SIL(Safety Integrity Level) {예를 들어, SIL 4로 허용 해저드 율

THR(h^{-1}), $10^{-9} \leqq THR < 10^{-8}$}이 이용되지만, 이것과 CSTs(공통 안전 목표)의 개인 리스크와의 관계를 붙이기 위해서는 별도의 검토가 필요하다.

⑤ CSMs(공통안전기법)에 대하여는 리스크 평가와 어세스먼트 기법으로서 이미 사용되고 있는 규격類와 같은 참조 시스템이 있다면, 그들 기존의 안전 확보 방법의 적용을 인정하고 해당되는 기존의 방법이 적당하지 않을 경우에만 명시적인 리스크 평가를 행한다. 이것은 타당한 내용이지만, 인증 등의 비용 증가를 우려하는 철도신호 산업계에서의 의견이 반영된 결과라고 생각된다.

⑥ 철도시스템 (특히 철도신호시스템)의 안전인증은 EU 역내에서는 철도산업시장의 개방(open)化와 철도조직의 상하 분리에서 보다 중요한 과제로 되어 있다. 이미 일부에서 상호 인증 등도 행하여지고 있다.

⑦ 철도안전 지령에서는 CSTs(공통 안전 목표), CSMs(공통안전기법)와 CSIs(공통안전항목) 등을 체계화하여 적절하게 기술하고 있으며 빠른 시기부터 리스크 관리를 베이스로 한 유럽의 철도 안전관리의 검토가 이루어져 왔다.

⑧ 이상과 같은 유럽에서의 철도 안전관리는 체제와 제도는 다르지만 우리나라에서도 철도에 대한 리스크관리 적용의 검토에 참고로 되는 점이 많다고 생각된다.

⑨ CSTs(공통 안전 목표)와 CSMs(공통안전기법)를 중심 개념으로 하는 유럽의 철도 안전관리는 철도 이외의 산업분야에 비해서도 선진적인 노력이며, 안전관리 기법으로서 검토 대상으로 되는 것이다. 철도에서는 이미 재빨리 RAMS(Reliability, Availability, Maintainability and Safety) 규격을 제정하였고, 유럽 철도의 안전관리는 RAMS 규격을 전개한 것으로도 자리 매김을 할 수 있다.

Ⅵ. 철도의 안전관련 국제규격

1. 국제규격의 종류

(1) 국제규격이란?

표준(standard)이란 룰(rule)이나 규칙·규제 등을 약정하는 일(① 판단의 근거, ② 본연의 모습. 본보기, ③ 가장 보통의 본연의 자세)이며 표준화(standardization)란 표준을 만들어 이용하는 활동의 일(① 표준에 맞추는 것. ② 공업제품 등의 품질·형상·치수를 표준에 따라 통일하는 것. 이에 따라 호환성을 높인다)을 말한다.

이것을 국제적으로 이용할 수 있는 형으로 하는 것이 국제표준화이며, 국제표준으로서 국제규격이 정해져 있다. 최근의 예로는 크레디트(신용) 카드(credit card)나 건전지 등도 국제규격에 의거하여 만들고 있으며, 외국에 가더라도 같은 카드를 사용하기도 하고, 현지에서 구입한 건전지를 그대로 이용할 수 있다.

규격을 그 성립의 성격이나 기능으로부터 분류하면 다음의 제(2)(3)항과 같이 된다.

(2) 규격의 성격에 따른 분류

(가) 디 쥴 스탠더드(de jure standard)

일반적으로 인정되고 있는 표준화단체가 작성한, 또는 작성하고 있는 표준이다(de jure란 '법에 맞는', '법률상으로 정식의' 뜻). 공적(公的) 표준이라고도 한다. 예; SI단위, ISO규격, IEC규격, 각종 KS규격 등.

(나) 디 팩토 스탠더드(de facto standard)

법적 강제력은 없지만, 시장에서 널리 이용되고 있는 표준이다(de facto는 '사실상의'의 뜻). 사실상의 표준, 실질표준, 이른바 '세계표준'이다. 예; Microsoft社의 기본 소프트웨어 Windows, 바코드 등.

(3) 규격의 기능에 따른 분류

규격에는 하기에 나타낸 것처럼 기능에 따른 분류가 있다. 최근에는 시스템의 기능요건을 규정하기도 하고 신뢰성이나 안전성을 확보하기 위한 규격이 늘어나고 있다. 이들의 규격은 물건의 치수 등 물리적 요건을 규정하는 것이 아니라 일의 달성을 위한 요건, 조건, 프로세스 등을 규정하는 것이며, 적용하는 대상에 따라 사고방식을 정리할 필요가 있고 적용 시에는 넓은 견지에서의 종합적인 대처를 필요로 하여 왔다.

- 시스템 규격(시스템 전체를 규정하는 규격)
- 하드웨어 규격(개개의 기기 · 부품에 대한 규격)
- 소프트웨어 규격(소프트웨어의 작성순서 등의 규격)

- ●신뢰성·안전성의 규격
- ●제조방법에 관한 규격
- ●시험방법에 관한 규격
- ●제조 자격인정에 관한 규격(소프트웨어 작성이나 기량 등에 관한 규격)
- ●제3자 인증에 관한 규격

2. 철도안전관련 국제규격의 역사적 경위

유럽에서는 18세기부터 민간주체로 인증사업이 시작되어 20세기 후반의 유럽통합에 따라 역내규격의 통일을 도모했다. 한편, 미국은 제2차 세계대전 후 군사·우주분야에서 신뢰성 매니지먼트 기술이 진전되어 아폴로계획 등의 성과를 얻을 수 있었다. 이 기술과 유럽에서 태어난 설계안전 개념이 융합한 결과, 철도분야에서는 1990년대에 R:신뢰성, A:가용성, M:유지보수성, S:안전성으로 이루어진 RAMS 성능과 그 달성프로세스의 매니지먼트를 요구하는 통칭 RAMS 규격이라고 부르는 유럽규격 EN 50126이 개발되어 세계표준의 IEC 62278로 되었다.

그림 2에 안전 매니지먼트 규격과 관계하는 기관군의 구도를 나타낸다. 안전매니지먼트 규격은 제품개발 착수의 시작 시에 목표로 하는 SIL(Safety Integrity Level, 안전성 레벨)을 선언하고 그 다음에 SIL을 달성할 수 있었던 매니지먼트의 증거(문서와 입회 감사)를 요구하며 그 증거의 타당성 판단을 중립·공정한 제삼자에게 위임할 것을 요구한다. 게다가, 제3자性은 SIL에 따라 높아지게 되도록 규정되어 있다. 이 장치에 의하여 이른바 이중안전이 요구되는 철도신호와 같은 시설의 경우에 외부의 인증기관으로

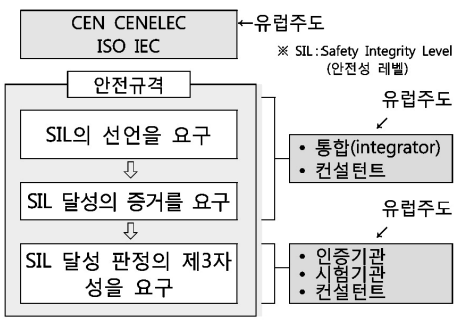

그림 2. 안전관련 국제규격과 관련기관의 구도

부터의 인증을 획득하여야만 하는 상황이 만들어져 있다. 안전 매니지먼트 규격에는 철도와 같은 특정 산업분야를 대상으로 하는 것과 분야 횡단적인 것이 있지만, 어느 것도 지금까지 유럽의 표준화단체 CEN(유럽표준화위원회)와 CENELEC(유럽전기표준화위원회)가 개발과 관리를 행하여 왔다. 게다가, 규격이 적용되는 제품의 계획·설계·제조 등의 각 단계에서 관련된 시스템 통합(integrator)과 컨설팅, 인증기관과 시험기관도 유럽세력이 주도권을 쥐고 있다.

이상의 결과, 안전관련 규격의 개발, 규격대응 컨설턴트로부터 규격 적합성 인증까지 일관되게 유럽세력이 주도권을 가지는 구도가 생겨났다.

3. 철도의 안전성·신뢰성에 관한 국제규격의 동향

근년에 ISO(국제표준화기구)나 IEC(국제전기표준회의)의 장에서 국제규격의 제정이 유럽 주도로 진행되고 있으며, 특히 1995년에 발족된 WTO(세계무역기구)에서의 정부조달협정이나 TBT 협정(무역의 기술적 장해에 관한 협정)의 발효에 따라 ISO 규격이나 IEC 규격의 사실상의 준수가 국제적으로 요구되게 되었다.

철도에 관하여는 최근에 국제규격화가 진행되고 있으며 종래의 장치나 부품 레벨보다도 시스템적인 규격이 주류로 되어 있다. 일례로서 제2절에서 언급한 IEC 62278 철도용 RAMS(Reliability, Availability, Maintainability and Safety)가 열거된다. 이것은 다음과 같은 4 가지 성능과 경제성에 비추어 시스템을 종합적으로 밸런스 좋게 유지하는 매니지먼트 시스템 규격으로서 제정된 것으로 RAM 부분은 일반산업계를 대상으로 한 ISO 9000 규격(품질 매니지먼트 시스템)을, S 부분은 마찬가지로 IEC 61508 규격(전기/전자/컴퓨터시스템의 기능안전)을 각각 준용하고 있다.

- ●R(신뢰성) : 기능·성능이 유지될 수 있다.
  - • 대상의 예; 수송 장해에 직결되는 장치고장률, 중요기기/시스템 전체의 평균 고장간격 등
- ●A(가용성) : 사용하고 싶은 때에 사용한다.
  - • 대상의 예; 차량주행거리에 따른 열차지연 시간과 빈도, 선구의 열차킬로미터 당의 수송 장해 발생확률 등
- ●M(보전성) : 보수하기 쉽다.
  - • 대상의 예; 고장발생 시의 복구시간(logistics를 포함), 검사/보수 코스트 등

● S(안전성) : 안전의 허용수준을 충족시킨다.

• 대상의 예; 대상 선구의 운전사고 확률의 허용수준 등

RAMS 규격제정의 배경에는 EU통합에서 철도망의 상호직통운전 계획(Interoperability)과 유럽 철도산업의 세계시장 제패전략이 있다고 한다. 공적 기관, 철도회사, 벤더(vendor)의 역할을 명확하게 하여 삼위일체로 협조와 책임을 분담하는 구조로 추진하고 있다.

철도용 RAMS 규격의 컨셉트는 대상 시스템의 구성단계부터 폐기에 이르는 라이프사이클을 통하여 다음 사항을 요구하고 있는 것이다.

① 안전성과 신뢰성을 저해하는 요인의 추출과 리스크의 허용수준 등 안전성과 신뢰성의 목표 설정

② 목표를 충족시키는 것의 논거, 사전평가·검증, 문서기록의 실행

③ 제3자에 의한 인증 등

그러나 이들을 실현하기 위한 기법이나 목표수준 등은 규정되어 있지 않고 유럽의 철도에서 RAMS 규격을 실제로 적용한 사례에서는 현시점에서는 각각 독자의 방법으로 실시하고 있는듯하다. 또한, 제3자 인증에 대하여는 영국, 프랑스, 독일 등에서 몇 개인가의 기업과 단체가 인증기관의 인정을 받아 활동하고 있다.

철도용 RAMS 규격은 상기의 성능 중에 철도이용자에게 직결되는 서비스성능, 즉 가용성과 안전성의 두 가지를 중시하고 있다. 가용성에 대하여는 예를 들어 신규로 차량을 조달 시에 그 차량 주행거리에 따라 어느 정도의 보수빈도와 보수량을 허용하는가, 어느 정도의 열차지연 빈도와 지연시간을 허용하는가, 등, 벤더(vendor)의 요건을 철도회사 자신이 결정할 수 있다. 그러나 안전성에 관하여는 철도회사의 방침만이 아니라 사회적인 컨센서스(consensus)라고 하는 몇 개인가의 객관성을 나타낼 필요가 있다. 이 때문에 EU에서는 SAMNET(SAfety Management and interoperability thematic NETwork in Railway systems)라고 칭하는 프로젝트를 시작하여 공통으로 이용할 수 있는 구체적인 기법이나 실시 룰 등을 수 년에 걸쳐 개발하는 활동을 개시하였다.

4. RAMS 규격의 특징

일반적으로 규격에는 특정 제품의 기술사양을 정하여 그 달성을 요구하는 것과 목표달성의 업무프로세스 매니지먼트를 요구하는 것이 있다. RAMS 규격의 특징은 이러한 요구를 일체화한 점과 철도제품의 종별을 한정하지 않는 점이다. 즉, 이 규격은 임의로 선정된 철도제품에 관하여 기술적 RAMS 사양을 정하여 달성할 것과 달성 프로세스 매니지먼트의 타당성 증명문서의 작성을 요구한다(그림 3). 또한, 달성프로세스는 그림 4와 같이 제품의 구상단계로부터 설계, 제조, 사용, 폐기까지의 전 라이프 사이클 단계를 커버해야 하고, 메이커는 제품의 RAMS 성능 달성을 위한 활동(RAMS Activity)을 각 단계에서 규정하고 실행의 증거를 문서로 설명하여야 한다. 각 단계에서의 활동은 먼저 그 단계에서 달성되어야 할 요구사항을 규정하고 이전 단계로부터의 인풋(해석결과, 시험검증의 결과, 참고정보 등)이 구비되어 있는지를 확인하여 요구사항을 실현하는 업무를 실행하며 그 결과가 타당하다는 것의 '검증'을 행하고 다음 단계에의 아웃풋(다음 단계에의 인풋)을 행하는 것이다.

여기서 말하는 '검증'을 일반적 통념으로서 보면 다음 단계에 대한 문제의 유무를 확인하는 것이지만, RAMS 규격은 더욱 정성을 들인 검증을 요구한다. 마치 데이터통신 프로토콜의 계층 구조와 같이 14개의 RAMS 라이프사이클 단계를 상위계층, 중간계층, 하위계층으로 분류한다. 통신 프로토콜로 말하면, 예를 들어 데이터통신을 하는 두 대의 컴퓨터에 내장된 프로토콜의 각 계층은 상대방의 동위계층과는 상호로 통신이 완전히 가능해야 하지만. 이에 유사하게 RAMS 규격에서는 라이프사이클 중 제2단계 (적용범위의 정의)와 제10단계(수용)를 상위계층의 조(組)라고 생각하고 제2단계에서 정의한 사양이 만족되고 있는지의 여부를 제10단계에서 검증할 것을 요구한다. 중간계층에서는 제5단계(안전요구의 배분)와 제9단계(기능과 안전성

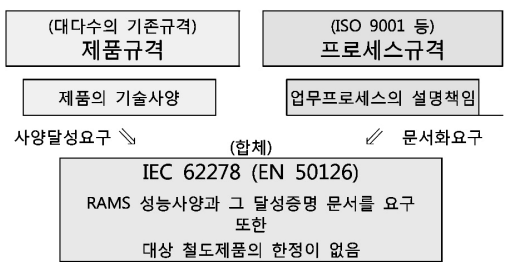

그림 3. RAMS 규격의 요구a

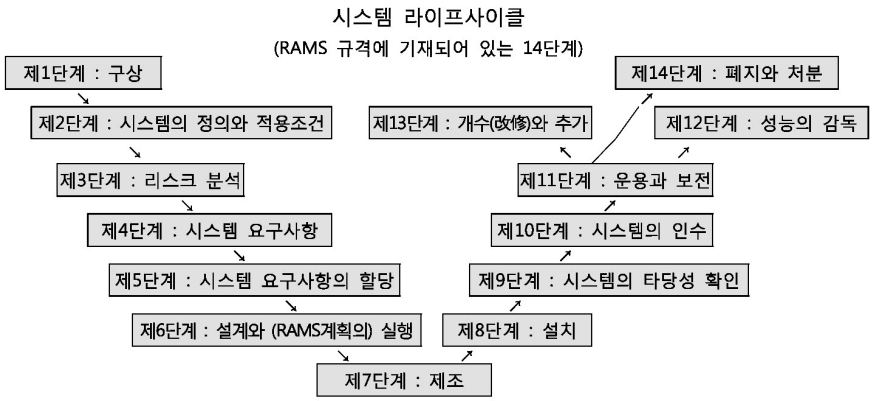

그림 4. 시스템 라이프사이클

의 검증), 하위계층에서는 제6단계(설계)와 제7단계(제조) 중의 출하검사가 각각 검증하여야 할 조(組)이다. RAMS 규격에서는 다음 단계로의 아웃풋의 검증을 Verification, 같은 계층 내의 조(組)끼리의 검증을 Validation이라고 불러 구별하고 또한 양쪽의 검증을 합하여 V & V(Verification and Validation)라는 호칭을 이용하는 것이며, 검증 누설은 허용하지 않는다는 자세를 강조하고 있다.

5. RAMS 문서

일반적으로 매니지먼트 규격은 제품의 기능·성능의 규정, 제품화 과정의 상황 기록, 수정 관리 및 요구 사항과의 정합의 검증을 기술적 및 관리상의 각 측면에서 문서화하고 관리하는 것을 Configuration management라고 부른다. RAMS 규격의 운용에서 Configuration management에 대응하는 문서는 RAMS 문서라고 통칭된다. 규격 원문 중의 RAMS support documentation이나 System support documentation이 이것에 상당하지만, 어떠한 체계의 문서를 작성하면 좋은 것인가를 RAMS 규격 자체는 기술하지 않고 있다. RAMS 규격에는 단지 적절한 Configuration management가 달성되어야 한다고 하는 기재밖에 없다.

그래서 참고로 되는 것은 IEC 61508과 EN 50129(IEC 62425의 원안)이다. 전자는 산업 분야를 불문하고 E/E/PES(Electric/Electronic/Programmable Electronic System; 전기 · 전자 · 프로그래머블 전자시스템) 제품 안전성 매니지먼트 규격이며, 후자는 철도에서 보안레벨(이른바 이중안전)의 안전에 관계되는 전자장치의 안전성 매니지먼트 규격이다. 이 두 표준은 모두 RAMS 성능 중의 S=안전에 중점을 두고 있지만, RAMS 규격 대응의 문서체계에 관한 실용적인 예를 제공하고 있다.

전자는 그 참고 부속문서에 안전성 라이프 사이클의 전체를 커버하는 문서구조와 E/E/PES 및 소프트웨어의 안전성에 관하여 기술하는 것이 바람직한 정보의 사례를 상세히 나열하고 있다. 또한 문서의 실체에 대해서는 여러 종류의 문서 세트이며, 개개의 문서 타이틀의 예를 들고 있다. 문서 세트에는 대상 제품의 라이프 사이클의 모든 국면을 커버하는 완전한 세트 외에 규격을 운용하는 사용자(user)의 입장(설계, 제조, 검증, 보수·보전 운용)에 따른 세트가 있을 수 있는 점과 문서분류의 방법은 대상 제품의 시스템 규모의 대소에 따라 선택하면 좋다는 것을 기재하고 있다. 후자는 더 나아가서 강제력이 있는 규격본문 중에 보다 구체적으로 문서의 구성을 제시하고 있다.

상기의 두 가지 기준은 RAM 성능에 대한 요구사항을 명시적으로 내걸고 있지는 않지만, 예를 들어 S=안전성을 마르코프(Markov) 상태 천이도(遷移圖)를 이용한 위험 측고장률 계산으로 수치적으로 평가하는 경우에 R=신뢰성과 M=보수성의 수치가 안전성과 상관을 갖는 것을 나타낸다. 그 때, A=가용성도 동시에 산출된다. 이와 같이 이들의 두 가지 규격의 대상인 안전성은 원래 RAM 성능과도 밀접하게 결부되어 있다. 그 때문에 RAMS 문서의 체계로서 이러한 규격의 예를 참조하는 것은 합리성이 있다고 한다.

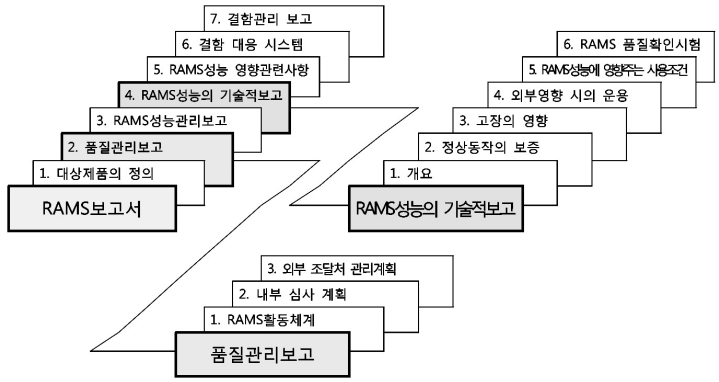

그림 5. RAMS 문서체계 예

그림 5에 RAMS 문서의 구성 예를 나타낸다. 이 예에서는 문서전체의 명칭을 RAMS Report로 하고, 그 아래에 7종류의 문서를 배열하고 있다. 이 중에 주요한 두 가지 문서, Quality Management Report와 Technical RAMS Report에 대하여 그들의 내부 문서의 구성 예를 도시하였다.

RAMS 문서 규격의 사용자(super)에게 최대의 문제는 각 문서 내용의 기재 방법이 이해하기 어려운 점이다. 이것의 주요한 원인의 하나는 라이프사이클 단계마다 요구되는 여러 가지 RAMS Activity와 그림 5와 같은 실체 문서 개개의 내용을 결부시키는 기술방법에 관한 가이던스(guidance)가 명시되어 있지 않은 점이다. 이것에 관해서는 문서마다 모든 RAMS 라이프사이클 단계가 포함되어 있다고 생각하여야 한다. 즉, 그림 5에 나타낸 각 문서는 개개의 라이프 사이클 단계에서 사용자가 문서의 타이틀에 따라 행한 활동(계획, 설계, 리뷰·revue, 제조, 검사, 품질매니지먼트 등)을 기재한다는 것이다.

또 하나의 주요 원인은 지금까지 작성하여 온 기술문서(설계도서, 검사보고서 등)와 RAMS 문서의 구성이 다르고, 동일 사항이라도 각 문서에 기재하여야 하며, 게다가 그림 5의 RAMS Report 중의 Traceability report 작성에 대한 대응을 하여야 한다는 점이다. RAMS 규격이 요구하는 Traceability(추적성)의 기본은 라이프사이클의 제1단계 내지 제5단계 사이에서 발생된 요구사항이 뒤쪽의 라이프사이클 단계에서의 검증사항과 완전히 링크되어 있는 것을 기술하는 것이다. 상기와 같이 RAMS 문서체계는 같은 주제를 복수의 문서에 기재하는 것이 생기기 때문에 하나의 사항에 관하여 추적(trace)하여야 하는 링크가 복수로 필요하게 된다.

또한, RAMS 규격은 라이프사이클의 어느 단계에서 RAMS 성능 달성상의 결함이 발견된 경우에 그 원인을 최초로 만든 단계로 되돌아가 대책하는 것(피드백) 및 그 전말을 모두 기록할 것을 요구한다. 일반적으로 라이프사이클 제7 단계(제조)에서 사양항목 수가 최대에 도달하고 그 후의 단계에서는 검증사항으로서 정리되기 때문에 링크 수가 줄어져 간다. 복잡한 시스템 제품의 경우에 이 링크를 관리하는 Traceability report 문서는 거대한 것으로 된다. 또한, 라이프사이클의 n + 1 번째 단계로 후단으로부터의 피드백, 즉 결함 대책을 위한 사양 변경이 요구되었다고 한다. 이 변경이 복수의 문서에서 새로운 사항이 생기거나 기존의 사항에 대한 변경이 생겨 라이프사이클의 후단으로도 파급되어 간다. 그 때문에 특히 복수의 팀이 개발에 참가하는 규모의 제품인 경우에 Traceability의 관리는 어려움을 겪는다. 따라서 Traceability에 관하여는 유효하고 관리가 가능한 기록 방법의 궁리가 필요하다.

Ⅶ. 맺음말

유럽에서 철도의 안전관리체계 구축 움직임의 근원은 유럽통합이다. 이 통합의 문맥 중에서 철도의 본연의 자세에 관하여는 2001년에 EU에서 발행된 Transport White

Paper "A Time to Decide"에 그 기본방침이 나타내어져 있다. 장기적인 관점에서 본 철도의 본연의 자세의 논의가 극히 중요하다.

철도에는 열차제어시스템과 같이 안전을 정의할 수 있는 시스템이 많고 리스크 베이스의 안전관리에서도 시스템의 설계에서는 과도하게 정량적인 안전성평가에 중점을 두지 않아야 한다. 안전 관련계통에 구조로서의 안전을 도입하는 것이 유효하며, 그를 위해서도 범용적으로 저비용의 안전기술이 필요하게 된다.

철도의 안전성·신뢰성과 관련하여 철도시스템, 또는 구성 서브시스템의 안전성과 신뢰성의 목표설정, 리스크 저감 등에 적용되는 기술의 타당선 논거와 사전평가, 사고나 장해가 발생된 경우에도 활용할 수 있는 각종 도큐먼트(document) 등 정량적 또는 확률논적인 어프로치를 가미한 목표관리방식으로 바꿀 필요가 있다. 그러한 실시내용과 결과의 객관성을 나타내기 위해서는 제3자에 의한 평가/인증도 필요할 것이다.

한편, 해외 철도시장의 안전관련 규격에 대한 적합성 설명문서 작성에 상당한 노력을 필요로 하며, 인증취득에 대한 곤란한 조건이 있기 때문에 이들의 해결이 강하게 요구되고 있다.

♣ 참고문헌

[1] ERA, Recommendation on the first set of Common Safety Targets as referred to in Article 7 of Directive 2004/49/EC (ERA/REC/03-20009/SAF). 2009.

[2] Evaluation of Regulation 881/2004, Final Report, European Commission, 2011.4

[3] New Regulation EC No. 352/2009 Common Safety Method (CSM). 2009.

[4] Benoit Debusschere, Railway Safety activities at the European Railway Agency, Coordinator NSA Network – Safety Unit, 2009.5.

[5] ERA, Railway Safety Performance in the European Union, 2012.

[6] Safety Integrity Level – Magnetrol International, Special Application Series

[7] ERA, European Railway Agency Recommendation on the 1st set of Common Safety Methods (ERA-REC-02-2007-SAF)

[8] DIRECTIVE 2004/49/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 April 2004.

[9] European Railway Agency Recommendation on the revision of the common safety method on risk evaluation and assessment and repealing Commission Regulation(EC) No 352/20091 (ERA/REC/02-2012/SAF)

[10] Commission Regulation(EC) No.352/2009 of 24 April 2009 on the adoption of a common safety method on risk evaluation and assessment as referred to in Article 6(3)(a) of Directive 2004/49/EC of the European Parliament and of the Council(2009)

[11] INTERNATIONAL STANDARD, Railway applications – Specification and demonstration of reliability, availability, maintainability and safety(RAMS), IEC 62278,

[12] European Commission, White Paper "European Transport policy for 2010: Time to Decide, 2001.

[13] European Railway Agency Safety Unit, Intermediate report on the development of railway safety in the European Union, 2013.5

[14] Angelo Pira, Roberto Piazza and Torben Holvad, A SUSTAINABLE SAFETY PERFORMANCE FOR RAILWAYS, ERA, 2008.2.

[15] 서사범, "유럽에서의 철도시스템의 리스크 베이스 안전관리", 대한토목학회지 제62권 제4호, 2014.4.

[16] 서사범, 철도공학의 이해(Railway Engineering), 도서출판(주) 얼과 알, 2000. 4. (ISBN 89-88900-82-0 93550)

[17] 서사범 철도공학(Railway Engineering), 도서출판 BG 북 갤러리, 2006. 9. (ISBN 89-91177- 23-9 93530)

[18] 서사범, 철도공학 입문(Fundamentals of Railway Engineering), 도서출판 BG 북 갤러리, 2010. 4. 7. (ISBN 89-91177-97-0 93530)