철도 RAMS의 적용에 관한 고찰
A Study of Railway RAMS Application

김종기* 이종우* 임훈**
Kim, Jong-Ki Lee, Jong-Woo Lim, Hoon

ABSTRACT

The interests about railway safety have been highly increased. Early railway safety was widely studied in Europe and Japan, and safety standards were established in 1990s. EN 50126 of CENELEC, Railway applications - Specification and demonstration of RAMS, became IEC 62278 in 2002. This standard provides Railway Authorities and railway support industry with a process which will enable the implementation of a consistent approach to the management of RAMS. IEC 62278 will be often referred to in the field of railway system. This paper examined the application of railway RAMS on basis of IEC 62278.

1 서론

IEC 62278 Railway applications - Specification and demonstration of reliability, availability, maintainability and safety(RAMS)는 2002년 10월에 발표되었다. 이 규격은 유럽의 IEC(국제전기기술위원회)에 해당하는 CENELEC(유럽전자기술표준화위원회)의 EN 50126이 IEC 규격으로 된 것이다.

유럽의 철도산업에서는 상호운용성(interoperability)와 상호인증제도에 의한 유럽 내 철도기술개발의 효율성을 높이려는 움직임이 활발해지면서 유럽 공통규격이 잇따라 제정되고 있다. 유럽은 드레스덴(1996년) 협정에 따라 IEC와 CENELEC의 규격을 일치시키려고 노력하고 있으며, EN 규격을 원안으로 하는 IEC 규격이 계속 제정되고 있다. 또 IEC는 전기, 전자 이외의 분야의 표준화를 담당하고 있는 ISO(국제표준화기구)와도 밀접한 관계를 맺고 표준화 절차를 동일하게 적용하고 있다.

과거에는 장치나 기기의 사양, 시험에 관한 규격인 제품규격이 많았지만 최근에는 시스템 전반이나 관리에 관한 시스템 규격이 증가하고 있다. 또 최근의 제품은 하드웨어와 소프트웨어의 밀접한 결합에 의한 시스템화 경향이 많아지면서 IEC와 ISO의 공동작업을 필요로 하는 분야가 많아지고 있다. 특히 철도시스템의 안전은 시스템 개념 설정 단계부터 안전에 대한 위해요인을 차단하는 것이 중요하므로 시스템적인 접근과 관리가 필요하다.

IEC 62278은 시스템 수명사이클 전체에 대해서 시스템적인 접근을 취하고 있으며 ISO 9000시리즈의 품질관리 요구사항과 일치시켜 적용할 것을 명시하고 있다.

최근 철도의 전기분야에 관한 규격은 심의되고 있는 규격의 수가 증가하고 있으며 제품규격에서 시스템 규격으로 질적인 변화가 일어나고 있다. 또 국제화가 가속되면서 국제규격을 충족하도록 국내규격을 검토해야 할 필요도 있으며, 우리나라의 지정학적인 위치나 국제화 추세로 볼 때 국제규격에 무관심할 수는 없다.

* 한국철도기술연구원 책임연구원, 정회원
** 한국철도기술연구원

따라서 본고에서는 철도시스템에 대한 RAMS를 다룬 포괄적인 규격인 IEC 62278을 중심으로 철도 RAMS의 적용에 관해 고찰하고자 한다.

2. 철도 RAMS

철도시스템의 목표는 주어진 시간 내에 정해진 철도수송을 안전하게 달성하는 것이다. 철도 RAMS는 철도시스템이 목표를 달성할 수 있다는 확신을 나타내고 있다. 이 확신을 얻기 위해서는 시스템의 수명사이클동안 확립된 공학적 개념, 기법, 도구 등을 적용함으로써 가능하다. 따라서 어느 한 시스템의 RAMS는 시스템, 하부시스템, 구성요소가 안전하게 규정된 대로 잘 작동할 수 있는가에 대한 정성적이고 정량적인 지표라고 볼 수 있으며, IEC 62278에서 시스템 RAMS는 신뢰성, 가용성, 유지보수성, 안전성의 적당한 조합이다.

2.1 철도 RAMS의 요소

철도 RAMS의 요소인 신뢰성, 가용성, 유지보수성, 안전성 사이의 상호작용을 고려하는 것이 중요하다. 안전성과 가용성은 경우에 따라서 서로 상충될 수 있는 요소이다. 즉, 상황에 따라서 안전성을 높이면 가용성이 낮아지고, 가용성을 높이면 안전성이 낮아질 수 있다. 그러므로 이들 두 요소간의 대립을 잘 관리해야 한다. 이들 두 요소의 목표를 달성하기 위해서는 모든 신뢰성과 유지보수성 요구사항을 만족하면서 장기간, 상시 유지보수 활동과 운영 활동, 시스템 환경을 제어해야 한다.

가용성에 대한 기술적인 개념은 다음의 신뢰성, 유지보수성, 작동 및 유지보수를 근거로 설정할 수 있다.

가) 신뢰성
- 지정된 어플리케이션과 환경에서 모든 가능한 시스템 고장 모드
- 각 고장의 발생확률 또는 각 고장의 발생빈도
- 고장이 시스템 기능에 미치는 영향

나) 유지보수성
- 계획된 유지보수를 수행하는데 걸리는 시간
- 결함의 검지, 식별, 위치파악에 걸리는 시간
- 고장난 시스템의 복구에 걸리는 시간(비계획 유지보수)

다) 작동 및 유지보수
- 시스템 수명사이클에 걸친 모든 가능한 작동 모드와 요구되는 유지보수
- 인간 요인(Human Factor)

안전성에 대한 기술적인 개념은 다음 다섯 가지 사항을 근거로 설정할 수 있다.

가) 모든 작동, 유지보수, 환경 모드 하에서 시스템의 모든 가능한 위험요소(Hazard)

나) 결과의 심각성을 고려한 각 위험요소의 특성

다) 안전성 및 안전 관련 고장
- 위험요소를 야기하는 모든 시스템 고장 모드
- 각 안전 관련 시스템 고장 모드의 발생 확률
- 사고를 유발할 수 있는 사건, 고장, 작동상태, 환경조건의 연속발생 또는 순차발생
- 사건, 고장, 작동상태, 환경조건들 각각의 발생확률

라) 시스템의 안전 관련 부분의 유지보수성
- 위험요소나 안전 관련 고장모드와 관련된 시스템, 구성요소에 대한 유지보수의 수행
- 안전 관련 파트의 유지보수 활동 동안 오류 발생 확률
- 시스템을 안전 상태로 복구하는데 걸리는 시간

마) 시스템의 안전 관련 파트들의 시스템 작동과 유지보수

- 모든 안전 관련 파트의 효율적인 유지보수와 안전한 작동을 위한 인간 요인 영향
- 안전 관련 파트의 효율적인 유지보수와 안전한 작동을 위한 도구, 시설물, 절차들
- 위험요소를 처리하고 그 피해를 경감하기 위한 효율적인 관리와 수단들

2.2 철도 RAMS에 영향을 미치는 요인

철도 RAMS는 다음 세 가지 방식으로 영향을 받는다.

- 수명사이클의 각 단계에서 시스템 내에서 내부적으로 이입된 고장의 근원(시스템 조건)
- 작동 중 시스템에 가해지는 고장의 근원(작동 조건)
- 유지보수 중 시스템에 가해지는 고장의 근원(유지보수 조건)

다음 그림은 일반적인 고장의 근원의 상호 관계와 영향요인을 보여주고 있다.

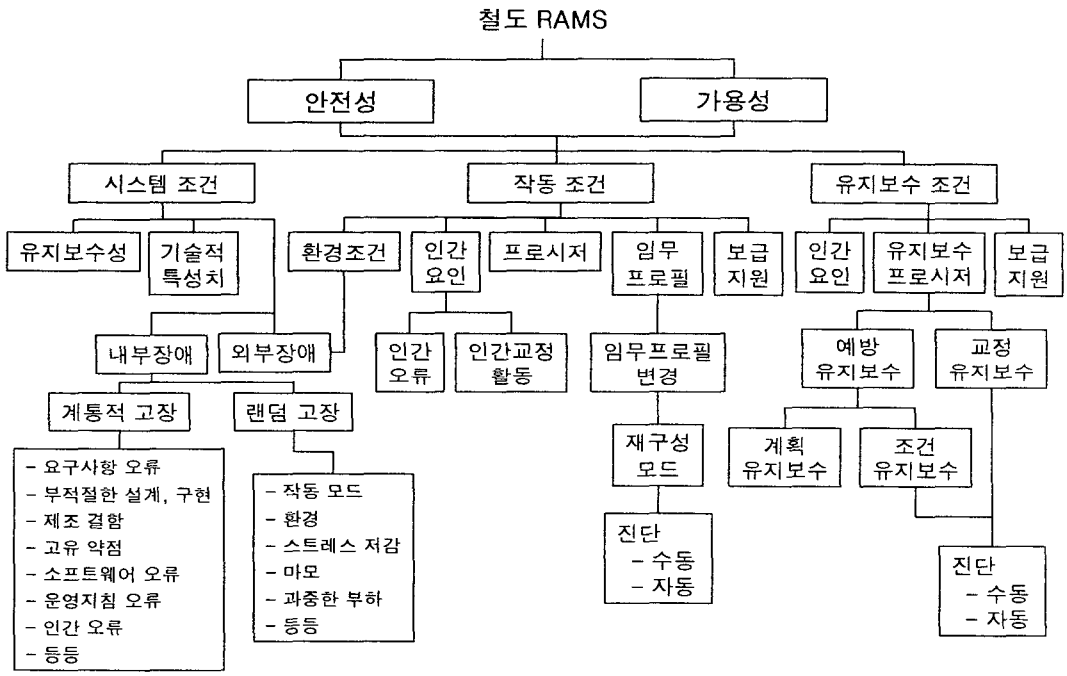

그림 1. 철도 RAMS의 요인

각각의 경우에 적용되는 일반요인들은 반드시 평가되어야 하고 어플리케이션에 구체적인 영향요인들은 체계적으로 도출되어야 한다. 인간 요인은 통합 RAMS 관리 절차의 핵심 양상으로써 고려되어야, 이 평가과정에 포함되어야 한다.

상세 영향요인은 철도 상세요인 체크리스트와 인간요인 체크리스트를 사용하거나 그림 1.을 활용하여 도출해야 한다. 철도 RAMS의 요인과 그 영향은 시스템의 RAMS 요구사항을 사양명세화 하는데 입력값이 된다.

2.3 철도 RAMS 요구사항

철도 RAMS 요구사항을 달성하는 방법은 RAMS에 영향을 미치는 요소들을 관리하는 것이다. 효율적인 관리는 오류의 근원을 방어하는 메커니즘과 프로시저를 구축하는 것이다. 이 방어대책은 랜덤 고장과 계통적 고장 모두 고려해야 한다.

RAMS 요구사항 달성 방법은 오류의 발생 결과 나타난 손상을 최소화하기 위한 사전예방

(precaution) 개념에 기초한다. 사전예방은 다음의 예방과 방호의 조합으로 이루어진다.

- 예방(prevention): 손상의 발생확률을 낮추는 것
- 방호(protection): 손상의 결과에 따른 심각한 정도를 낮추는 것

2.4 위험도(Risk)

위험도는 위험사건의 발생 빈도와 위험요소로 인한 위험한 결과의 심각성, 이 두 가지의 조합으로 규정된다. 위험도 분석은 각각 책임이 부여된 기관에 의해 수명사이클의 각 단계에서 수행되어야 하며 문서화되어야 한다. 이 문서에는 최소한 분석방법론, 가정, 제한사항, 방법론의 타당성 입증, 위험요소 규명 결과, 위험도 추정값과 이의 신뢰구간, Trade-off 연구결과, 데이터와 출처 및 신뢰수준, 참고문헌 등이 포함되어야 한다.

가. 위험도 평가와 수용

위험도 평가는 위험사건의 발생 빈도와 결과의 심각성을 함께 고려하여 위험등급을 매겨서 수행된다. 이를 위해 '빈도-결과 매트릭스'를 사용한다.

위험등급에 따라 어느 수준의 위험을 수용할 것인가는 일반적으로 인정된 위험도 수용 원리에 따라야 한다. 위험도 수용 원리의 대표적인 예로 다음 세 가지가 있다.

- 영국의 ALARP 원리(As Low As Reasonably Practicable)
- 프랑스의 GAMAB 원리(Globalement Au Moins Aussi Bon)
- 독일의 MEM 원리(Minimum Endogenous Mortality)

관련 철도기관은 채택된 원리, 허용 위험도 수준, 위험범주의 분류에 책임을 져야 한다.

다음 표는 위험도 평가와 수용의 전형적인 예를 보여준다.

표 1. 위험도 평가와 수용의 예

위험사건의 발생빈도	위험도 수준			
빈번함	바람직하지 않음	허용할 수 없음	허용할 수 없음	허용할 수 없음
가능성 높음	허용할 수 있음	바람직하지 않음	허용할 수 없음	허용할 수 없음
때때로	허용할 수 있음	바람직하지 않음	바람직하지 않음	허용할 수 없음
가능성 낮음	무시할 만함	허용할 수 있음	바람직하지 않음	바람직하지 않음
가능성 없음	무시할 만함	무시할 만함	허용할 수 있음	허용할 수 있음
있을 수 없음	무시할 만함	무시할 만함	무시할 만함	무시할 만함
	하찮음	중요하지 않음	위급함	치명적임
	위험결과의 심각도			

위험도 평가	위험도 감소/통제
허용할 수 없음	제거되어야 함
바람직하지 않음	위험도 감소가 실행가능하지 않고 철도기관이 동의하면 수용가능함
허용할 수 있음	철도기관의 적절한 관리와 동의로 수용가능함
무시할 만함	어떠한 동의없이도 수용가능함

2.5 안전 무결성(Safety Integrity)

어플리케이션에 대해 안전 수준이 설정되고 위험도 평가 결과 필요한 위험도 감소량이 평가되

면 시스템과 구성요소에 대한 안전 무결성 요구사항을 얻을 수 있다. 안전 무결성은 정량적인 요소들(주로 하드웨어 관련 사항, 랜덤 고장)과 비정량적인 요소들(주로 계통적인 결함과 관련된 사항, 예: 소프트웨어, 사양, 문서, 프로세스 등)의 조합으로 생각할 수 있다.

시스템 내에서 어떤 기능이 안전 무결성을 달성하려면 특별한 구조, 기법, 도구를 적절하고 효과적으로 적용해야 한다. 시스템 내의 안전기능은 IEC 62279나 ENV 50129 등 다른 여러 규격에서 정의된 구조, 기법, 도구를 사용하여 구현되기도 한다.

안전 무결성은 기본적으로 안전 기능에 지정되어 있다. 안전 기능은 안전시스템과 외부 위험감소 장치에 할당된다. 이 할당절차는 전체 시스템의 설계와 비용을 최적화하기 위하여 반복 수행된다.

안전 무결성 수준(SIL: Safety Integrity Level) 개념이 적용되기 전에 다음 사항이 고려되어야 한다.

- SIL은 안전전문가에 의해 세워져야 한다.
- SIL은 독립형(stand-alone) 장치에 할당되어야 한다. 이 장치는 교체가능한 가장 낮은 등급의 장치이다.
- Off the shelf 제품을 사용할 경우에는 안전 요구사항 등 관련 모든 조건이 대상 시스템에 대해 평가되어야 한다.
- SIL은 제품에 대한 안전의 기대되는 신뢰수준을 뜻한다. SIL이 시스템의 모든 양상을 담고 있지 않으며 SIL만 고려하는 것은 충분하지 않다.

2.6 Fail-Safe

IEC 62278에서 채택하고 있는 안전성에 대한 위험도 관리 접근방식은 Fail-Safe 개념과 일치하며 철도는 처음부터 고유의 Fail-safe 개념을 사용해왔다.

그러나 Fail-safe 개념의 타당성은 경험에 근거하고 있다. 이 개념은 마이크로 프로세서를 사용하는 복잡하고 대형 시스템의 개발과 사용을 제한하고 있다. 고장의 수의 기하급수적인 증가는 결정론적인 접근방식이 실용적이지 않으며 이런 복잡한 시스템에 대해서는 확률론적인 접근방식이 효과적으로 사용될 수 있다.

3. 철도 RAMS의 관리

철도 RAMS는 전체 철도시스템의 많은 측면중의 하나이며, 철도 RAMS는 전체 철도시스템의 모든 양상을 다루는 통합 철도관리 방식의 한 구성요소이다.

철도기관이 사용하는 철도시스템의 허용가능한 안전 위험도는 국가적인 안전기관이 정한 기준에 따른다. 위험을 평가하고 관리하고 최소화하는 것에 대한 일차적인 책임은 철도기관에 있다.

시스템의 수명사이클은 개념설정 단계부터 해체 및 폐기 단계까지 시스템 전체를 포괄하고 각 단계의 업무를 포함하는 연속된 단계들이다. 수명사이클은 동의된 시간 단위 내에서 정당한 가격으로 정당한 제품을 제공할 수 있도록, 시스템이 각 단계를 진행하면서 RAMS를 포함한 시스템의 모든 측면을 계획하고 관리하고 감시하는 구조를 제공한다. 수명사이클 개념은 이 규격의 성공적인 구현을 위한 토대를 제공한다.

IEC 62278에서는 14단계로 이루어진 시스템 수명사이클을 제시하고 있으며 각 단계별 RAMS 업무의 목적, 요구사항, 입력, 산출물, 증명사항을 정의하고 있다. 각 단계별로 해당 기관의 책임사항의 예를 표 2.에 나타냈다.

전형적인 철도 프로젝트에서 책임과 관련하여 일반적인 지침으로서 다음과 같은 것들이 있다.

- 요구사항은 고객이나 합법기관에 의해 작성된다.
- 승인과 수용은 고객과 합법기관에 의해 유사한 과정으로 수행된다.
- 해결책 및 이의 결과와 증명은 정상적으로 계약자에 의해 개발되고 수행된다.

- 검증은 정상적으로 함께 수행된다.

이런 일반적인 규칙들은 관련 기관과 계약 당사자들간의 계약과 합법적인 관계에 따른다.

표 2. 수명사이클의 RAMS 프로세스에서 책임성

	고객/운영기관	인증기관	주 계약자	하부 계약자	공급자
1. 개념	×				
2. 시스템 정의와 적용조건	×				
3. 위험도 분석	×		×		
4. 시스템요구사항	×	(×)			
5. 시스템요구사항의 배분	(×)		×		
6. 설계와 구현			×	(×)	
7. 제조			×	×	×
8. 설치			×	(×)	
9. 시스템 검증	×	×	×	(×)	
10. 시스템 수용	×	×			
11. 운영과 유지보수	×		(×)	(×)	
12. 성능 감시	×		(×)	(×)	
13. 변경과 개조	×		×	×	
14. 해체와 폐기	×		(×)		
×: 전체 책임과 참여 (×): 특정한 책임 또는 일부 참여					

4. 결론

우리나라 철도산업계에도 국제화가 현실로 다가오고 있다. 우리 철도제품의 수출을 위해서는 국제적인 안전인증기관의 공인이 요구되고 있으며, 특히 유럽의 EN 규격이 국제규격화되고 있다. 국제무역에 크게 영향을 받고 아직 자체 기술이 부족한 우리나라는 국제규격에 관한 연구가 시급하다. 국제규격에 관한 연구를 위한 재원, 인력 확보는 물론 보다 조직적이고 지속적인 체계의 구축이 필요하다.

특히, IEC 62278 등과 같은 안전성에 관한 시스템적인 규격에는 시스템 전체와 하부시스템, 장치, 부품에 대해, 시스템의 개념 설정부터 폐기까지에 걸쳐 전반적인 검토가 필요하므로 철도운영기관, 연구기관, 인증기관, 제작업체, 등의 공동 연구와 적용작업이 필요하다.

참고문헌

1. 산업자원부 기술표준원(2003년), 국제전기기술위원회(IEC) 조직 및 현황.
2. IEC(2002), IEC 62278: Railway applications - Specification and demonstration of reliability, availability, maintainability and safety(RAMS).
3. 김종기, 이종우(2002년), "철도신호보안장치 안전성 규격의 발전동향," 한국철도학회지, 제5권, 제4호, pp. 25-30.