철도시스템 개발시 필요한 RAMS활동 및 인증 절차

RAMS activities necessary for developing the railway system and the certification process

이훈구*†, 박강훈*, 이수주*, 편선호**, 김용호**

Kang-Hun Park*, Soo-Joo Lee*, Seon-Ho Pyeon*, yong-Ho Kim*, Hoon-koo Lee*†

Abstract In a research study to develop a train detection system performs to enhance your system's security requirements RAMS (Reliability, Availability, Maintaninability and Safety) a description of the procedure leading to the discard from the initial stage of business activity and the content of each step and process and is used to study the role of each institution for the safety assessment.

***Keywords* : Independent safety assessment, RAMS activities, systems life cycle, LOP (List open point)**

초 록 연구는 열차 검지시스템을 개발하는 연구를 수행함에 있어 시스템의 안전요구사항을 높이기 위한 RAMS(Reliability, Availability, Maintaninability and Safety)활동의 초기 단계부터 폐기에 이르는 절차에 대해 설명하고 각 단계의 업무내용 및 절차 그리고 안전성 평가를 위한 각 기관의 역할에 대해 고찰하는데 있다.

주요어 : 독립적 안전성 평가, RAMS활동, 시스템 수명주기, LOP(List open point).

1. 서 론

21세기 최첨단 교통수단인 철도는 인류교통수단에 있어 가장효율적이고 이동성이 뛰어난 교통수단의 하나이다. 따라서 많은 사람들을 이동시키는 철도는 매우 안전한 시스템이 요구되고 있으며, 최첨단 안전설비들이 집약된 교통수단이지만 시스템오류 및 기관사의 실수로 발생할 수 있는 사고의 위험으로부터 자유로울 수가 없는 것이 사실이다. 따라서 시스템 개발시 시스템에 대한 RAMS활동과 기능 안전에 대한 인증이 반드시 요구되는 상황에 이르렀다. 따라서 본 논문에서는 시스템 개발시 RAMS가 적용되어야 하는 필요성과 시스템 개발과정에서 RAMS적용을 통한 단계별 수행내용을 알아본다. 또한 RAMS진행이 올바르게 진행되어가고 있는지 확인과 시스템의 성능검증과 인증을 위한 절차에 대하여 알아보도록 한다.

† 교신저자: ㈜에이알텍 기술연구소(lhk5254@hanmail.net)
* ㈜에이알텍 기술연구소
** ㈜에이알텍 설계사업부

2. 본 론

2.1 RAMS의 목적 및 상호관계

2.1.1 RMAS활동의 목적

RAMS의 목적은 시스템 개발시 요구되는 신뢰성, 가용성, 유지보수성에 대하여 정량적 목표를 만족하도록 관리하여 객관적인 정보를 통해 목표를 입증하고, 시스템의 위험원으로 인한 Risk가 허용할 수 있는 수준으로 건전하게 제어되었음을 객관적인 정보를 통해 입증한다.

2.1.2 RAMS구성 요소

철도 RAMS의 요소인 신뢰성, 가용성, 정비성 및 안전성 사이의 상호작용을 고려하는 것이 중요하다. 안전성과 가용성은 경우에 따라 상호 상충될 수 있는 요소이다. 즉, 상황에 따라 안전성을 높이면 가용성이 낮아지고, 반대로 가용성을 높이면 안전성이 낮아질 수 있다. 그러므로 이들 두 요소 간에 상충되는 것을 잘 관리해야 한다. 시스템을 운용하면서 두 요소의 목표를 달성하기 위해서는 신뢰성과 정비성의 모든 요구사항을 만족해야만 하며, 장기간의 지속적인 운용 및 정비 활동과 시스템의 환경을 관리해야만 한다. 철도 RAMS 요소의 내부 관계는 Fig. 1과 같다.

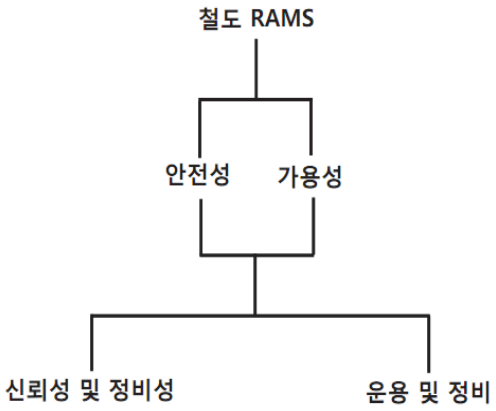

Fig. 1 Railway RAMS elements of internal relations

2.2 시스템 수명주기 활동

2.2.1 시스템 수명주기 및 활동내용

어떠한 시스템이 개발이 된다면 처음 단계인 개념 설계부터 제품의 생산과정 그리고 운용과 사용기간의 경과에 따른 폐기에 이르기까지 시스템의 수명주기는 다음 Fig.2와 같으며, RAMS업무는 각각의 수명주기 단계별 일반적인 프로젝트 업무에 영향을 준다.

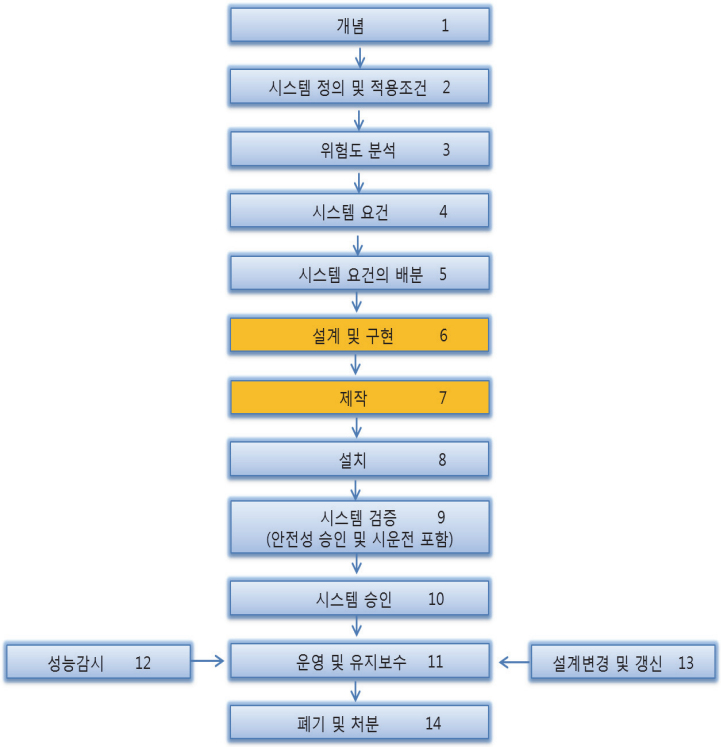

Fig. 2 System Life-Cycle Stages

2.2.2 단계별 적용내용

수명주기별 활동계획은 IEC 62278의 수명주기를 기반으로 관리한다. IEC62278의 수명주기는 시스템 개념설계부터 폐기까지 14단계로 구분하여 각 단계 요구사항을 제시하고 있다. 1단계에서 수행하여야 할 업무는 시스템의 범위와 목적수립, 재정분석과 같이 시스템 초기단계의 수립을 계획하며, 6단계 시스템의 설계 및 구현 단계에서는 시스템 설계확인의 수행, 구현과 검증 수행, 물류지원 업무 등을 수행한다. 14단계 폐기 및 처분의 단계에서는 폐기되고자 하는 설비 또는 제품에 대하여 폐기 및 처분 계획과 사용중지 이행, 폐기 이행 순으로 진행되며, RAM 업무는 특별히 필요치 않다. 다만 안전성 업무로는 안전성 계획 수행, 위험분석 및 위험도 평가 수행과 안전성 계획 이행 절차에 따라 진행되어야 한다. 그외 단계별 수행내용은 IEC62278의 내용을 참고로 한다.

2.3 독립안전성 평가(ISA) 절차

2.3.1 ISA활동 기관의 관계

ISA(Independence Safety Assessment)는 시스템이 지정된 요구 사항을 충족하고 제품의 달성 여부를 확인하며 시스템의 의도 된 목적에 적합 되는지 여부를 판단 하기 위해 분석하는 과정이다. ISA활동은 다음과 같은 고리로서 고객의 요청에 따라 컨설팅을 하게 되는데 조작자(Operator)는 시스템에 대한 수명주기 단계별 문서를 최초 작성하여 검토자를 통하여 고객(Client)또는 컨설팅업체에 검증을 받는다. 컨설팅 업체는 안전성에 필요한 요구문서를 조작자나 권한이 있는 관리자에게 시스템에 대한 LOP(List of Open Points) 작성하고 적합

성 여부를 판단하여 시스템에 대한 문서를 지속적으로 관리한다.

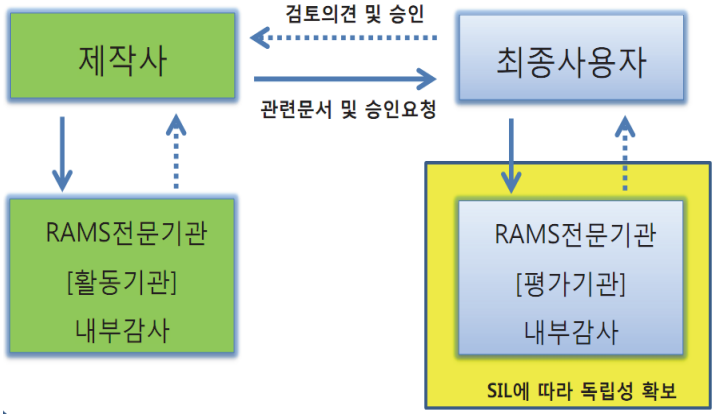

Fig. 3 ISA activity relationship of agency

2.3.2 문서 갱신 처리절차

시스템 개발단계별 절차에 의해 생선된 문서는 인증 및 평가기관에 검증을 받으며, 검증기관은 각각 단계별 수명주기에서 생성되어저야 하는 출력물의 내용을 검토하여 EN50126에서 요구하는 내용이 수록되어 있는지 검토하고 누락된 부분에 대하여 내용을 추가하도록 요구한다. LOP의 작성은 검토기관에서 질의한 내용에 대하여 답변과 조치결과를 수록하여 문제점을 하나씩 해결해 나가는 방식이다.

No.	Topic	Question				Severity	Answer			Status		
		Initial	Date	Chapter or Page	Text		Initial	Date	Text	Initial	Date	Text
1	RMSP	SMO	2012-06-13	General	본 문서를 작성하는 목적이 기술되어야 합니다.	Minor	KHP	2013.01.29	1. 목적에 기술되어 있습니다.	SMO	2013-01-23	pending
2	RMSP	SMO	2012-06-13	Ch1	적용 범위가 잘못 기술되어 있습니다.	Minor	KHP	2013.01.29	3.4 개발 및 RAMS 활동범위에 기술되어 있습니다.	SMO	2013-01-24	pending
3	RMSP	SMO	2012-06-13	Ch2	EN 규격과 IEC 규격이 혼재되어 있습니다. 본 프로젝트와 관련한 적용규격을 명확히 기술하시길 바랍니다.	Major	KHP	2013.01.29	4.1 적용규격에 기술되어 있습니다.	SMO	2013-01-25	pending
4	RMSP	SMO	2012-06-13	General	참조문서 (input documents)가 존재하지 않습니다.	Minor	KHP	2013.01.29	1.3 참고문서에 기술되어 있습니다.	SMO	2013-01-26	pending
5	RMSP	SMO	2012-06-13	General	RAMS 활동의 대상 시스템에 대한 설명이 존재하지 않습니다. (5.3.1절에서 대상 시스템은 확인 하였습니다.)	Major	KHP	2013.01.29	3.2 시스템정의 3.3 시스템 구성에 기술되어 있습니다.	SMO	2013-01-27	pending
6	RMSP	SMO	2012-06-13	Ch 3	본 문서 상에 사용된 약어 및 용어가 모두 정의되어야 하며, 사용되지 않은 약어 및 용어는 제거되어야 합니다.	Minor	KHP	2013.01.29	2.2 약어에 기술되어 있습니다. 사용하지 않는 약어는 제거 되었습니다.	SMO	2013-01-28	pending
7	RMSP	SMO	2012-06-13	Ch 4 4.1	조직도가 명확하지 않습니다. EN 50129 or IEC 62425상의 5.3.3 safety organisation을 기반으로, RAMS 조직이 구성되어야 합니다.	Major	KHP	2013.01.29	5.1 프로젝트 수행조직에 기술되어 있습니다.	SMO	2013-01-29	pending
8	RMSP	SMO	2012-06-13	Ch 4 4.2	RAMS 조직의 구성원에 대한 설명과 각 구성원의 책임 및 역할, 경험, 자격, 적절한 교육 등의 내용이 상세히 기술되어야 합니다.	Major	KHP	2013.01.29	5.1 프로젝트 수행조직 5.2 RAMS 활동조직구성에 기술되어 있습니다.	SMO	2013-01-30	pending
9	RMSP	SMO	2012-06-13	Ch 5	시스템 개발 수명 주기를 기반으로, 각 단계별 RAM 활동에 대한 상세한 내용이 기술되어야 합니다.	Major	KHP	2013.01.29	6. 시스템 수명주기별 RAMS활동에 기술되어 있습니다.	SMO	2013-01-31	pending
10	RMSP	SMO	2012-06-13	Ch 5	RAM 활동 절차에 대하여 재검토가 이루어져야 하며, RAM 분석을 위해 적용되는 모든 기법이 소개되어야 합니다.	Major	KHP	2013.01.29	7. RAMS활동 절차 및 분석 방법에 기술되어 있습니다.	SMO	2013-02-01	pending
11	RMSP	SMO	2012-06-13	Ch 5 5.2.2	시스템 개발 수명 주기를 기반으로, 각 단계별 안전성 활동에 대한 상세한 내용이 기술되어야 합니다. (IEC 62279를 기반으로 한 소프트웨어 포함)	Major	KHP	2013.01.29	6.시스템 수명주기별 RAMS활동에 기술되어 있습니다.	SMO	2013-02-02	pending
12	RMSP	SMO	2012-06-13	Ch 5	안전성 활동 절차에 대하여 재검토가 이루어져야 하며, 안전성 분석을 위해 적용되는 모든 기법이 소개되어야 합니다.	Major	KHP	2013.01.29	Answer 10번과 동일한 질문입니다.	SMO	2013-02-03	pending

Table 1 LOP and actions create resultsl

3. 결 론

앞에서 철도 시스템의 기능안전 규격, 시스템 수명주기 단계별 RAMS활동 그리고 기능 안전 개념과 안전성 승인 조건에 대해 설명하였다. 이러한 내용은 안전성 평가 또는 SIL 인증을 수행할 때 기반이 되는 개념이다. 안전 관련 시스템에 대한 SIL인증 절차는 개발된 제품의 안전성 적합 여부를 평가하는 것이 아니라 제품 개발의 개념 단계에서 구현 단계에 걸쳐 안전 관련 활동을 모두 심사하는 것이다. SIL 인증을 받기 위해서는 시스템 개발 단계별로 많은 활동이 요구되므로 기술적인 검토뿐만 아니라 충분한 시간과 인력의 지원을 고려하는 것이 중요하다.

ACKNOWLEDGMENT

이 논문은 국토교통과학기술진흥원에서 지원한 ”하이브리드궤도회로 개발”과제에 의해 수행되었습니다.

참고문헌

[1] IEC 61508, Functional Safety of Electrical/Electronic / Programmable Electronic Safety Related Systems, 2010.

[2] EN 50126, Railway Applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS), 1999.

[3] EN 50128, Railway Applications – Communication, signalling and processing systems - Software for railway control and protection systems, 2011.

[4] EN 50129, Railway Applications – Communication, signalling and processing systems - Safety related electronic systems for signalling, 2003.

[5] Safety-Critical Computer Systems, Neil Storey, 1996.

[6] Basic and applied for certification SIL RAMS 'books, T Ayoub issues de-Korea Co., Ltd., 2013.

[7] Basic and applied for certification SIL RAMS 'books, T Ayoub issues de-Korea Co., Ltd., 2013.

[8] IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related system,2010.

[9] 하이브리드 궤도회로 H/W 기능 인증을 위한 시험방법 개발, 한국철도학회 춘계학술대회 논문집 2013년

[10] “SIL 인증을 위한 RAMS 기초 및 응용” TUV코리아2012

[11] A Practice for RAMS in the Railway Signaling Shstem, 한국철도기술연구원,2010.