도시형자기부상열차 열차제어시스템 RAMS 적용에 관한 연구

A Study on the Application of RAMS for Urban Maglev Signalling System

윤학선* 이기서** 이종우*** 박재영****

Yun, Hak Sun Lee, Key Seo Lee, Jong Woo Park, Jae young

ABSTRACT

In this paper we present a RAMS to be applied to the development of the Urban Maglev Train Signalling System. The RAMS that can be applied to the life cycle of a Signalling system, from the basic design to the dismantlement, shows the whole process of the paper work in detail through the establishment of a goal, analysis and assessment, the verification. In this paper we study about the making a plan, the preliminary hazard analysis, the hazard identification and analysis to guarantee the safety of the Signalling System. The process for the verification of the system safety is divided into several steps based on the target system and the approaching method. The guarantee of the system safety and the improvement of the system reliability is followed by the recommendation of the international standards.

1. 서 론

본 논문에서는 국토해양부 및 한국건설교통기술평가원이 주관하는 국가대형연구개발실용화사업인 “도시형자기부상열차실용화사업” 시범노선에 적용할 열차제어시스템의 RAMS 적용을 위한 설계단계 활동 결과를 제시한다. 도시형자기부상열차실용화사업은 국가 선도 10대과제로 선정되어 2006. 11월 시작되었으며, 2012.11월까지 6년간에 걸쳐 SE, 차량개발, 시범노선 건설을 100% 우리나라의 기술로 수행하게 된다. 지난 2007년 시범노선 선정을 위한 인천, 대전, 광주, 대구 4개 지자체에서 제출한 제안서의 평가에 의해 인천광역시/인천국제공항공사가 선정기관으로 선정되어 인천국제공항이 있는 인천 영종도에 시범노선이 건설될 예정이며, 시범노선 건설 주관연구기관인 한국철도시설공단이 차량을 제외한 노반, 궤도, 역사, 전력, 신호, 통신, 차량기지의 모든 시범노선 건설을 위한 사업을 진행한다.

본 논문에서는 현재 인천 영종도에 건설 예정인 도시형자기부상열차 신호시스템에 대한 RAMS 요구사항을 기본 및 실시설계단계로 도출하여 제시하였다. 기본설계단계에서는 RAMS 개념 및 분석 방법에 대한 이해를 돕고자 전문가 교육을 실시하였고, 예비위험원분석(PHA) 방법을 통해 신호시스템 전체에 대한 안전요구사항을 도출하였다. 실시설계 단계에서는 기본설계 단계에서 도출된 설계 자료를 근거로 해당 하부시스템별 위험원 분석을 실시하였고, 타 프로젝트에서 적용된 데이터를 바탕으로 RAM 목표값을 설정하였다. RAM 목표값 수립을 위하여, 타 프로젝트에서 적용된 신호시스템에 대한 RAM데이터를 분석하고 도시형 자기부상열차의 운영조건을 분석하였다. 구체적이고 신뢰가 높은 RAM 목표값을 설정하기 위해서는 현재 대전 국립중앙과학관과 엑스포과학공원에서 운행중인 자기부상열차 신호시스템에 대한 고장 데이터를 수집하여 분석을 해야 하나, 수집된 고장데이터가 전무한 상태이므로 타 프로젝트에서 적용된 RAM 분석데이터를 참조하는 것으로 제한하였다.

실시설계를 바탕으로 도시형자기부상열차 신호 시스템에 대한 기능 및 시스템 분류를 실시하였다.

† 책임저자 : 정회원, 한국철도시설공단, 자기부상철도사업단, 차장(광운대학교 제어계측공학과 박사과정)
E-mail : kamayun@naver.com
TEL : (042)250-2794 FAX : (042)250-2777
* 정회원, 광운대학교, 정보제어공학과, 교수
* 정회원, 서울산업대학교, 철도전문대학원, 교수
* 정회원, 우송대학교, 철도전기통신공학부, 교수

기능 분류는 신호시스템이 구성하는 기본적인 기능을 나열하여, 시스템 위험원 분석시 기능별 위험원 도출이 가능하도록 수행되었다. 시스템 분류의 목적은 신호시스템을 구성하는 하부시스템을 분류함으로써, 각 하부시스템에 대한 위험원 규명 및 RAM 목표 설정을 체계적으로 수행하고자 함이다.

1.1 위험원 분석

도시형자기부상열차 신호시스템에 대한 잠재적인 위험원을 해당 하부시스템 수준에서 규명하고 각 위험원에 해당하는 위험도를 허용 가능한 수준으로 저감시키기 위한 대책을 마련하였다. 도시형자기부상열차 신호시스템의 실시설계에 대한 위험원 분석은 시스템 위험원 분석 방법을 통해 실시되었다.

1.2 RAM 목표 설정

운영 조건 및 타 프로젝트의 RAM 분석 데이터를 근거로 RAM 목표를 설정하였다. 신호시스템을 포함한 전체 시스템에 대한 최상위 RAM 목표값은 본 프로젝트의 타 과제에서 SE분야에서 수행하는 RAMS에서 제시한 근거를 토대로 도출하였다.

1.3 Safety 기준 설정

정량적인 RAM 목표가 아닌 정성적인 목표로서 Safety 에 대한 기준을 설정하였다. 본 실용화사업에서 공식적으로 Safety 기준에 해당하는 위험도등급에 대한 제시가 없으므로, EN50126에서 제시하는 위험도 등급을 적용하고 허용 가능한 등급결정을 위해 ALARP 의 원칙이 적용되도록 하였다.

1.4 RAMS 요구사항 도출

시스템 분류, 위험원 분석, RAM 목표 설정 및 Safety 기준 설정을 근거로 RAM 요구사항 및 Safety 요구사항을 도출하였다. RAM 요구사항은 RAM 목표 설정 결과를 근거로 제시되며, Safety 요구사항은 기본설계 단계에서 시행된 예비위험원분석과 실시설계 단계에서 시행되는 시스템 위험원분석에 포함된 저감대책을 근거로 제시되었다. 또한 향후 시스템 공급사에 수행해야할 RAMS 활동에 대한 산출물을 제시하였다.

2. 본 문

2.1 시범노선 개요

그림 1. 도시형자기부상열차실용화사업 시범노선 노선도

- 위　　치: 인천광역시 영종도 인천국제공항 일원
- 총 연 장: 본선 6.113Km(복선), 인입선 0.750Km(단선)
- 정 거 장: 6 개역(섬식 2 개소, 상대식 4 개소)
- 차량기지: 1 개소(인천공항철도 차량기지 인근)

2.2 신호시스템 사양

o 운전방식: ATO 무인운전
o 신호방식: 차상 신호방식
o 최소운전시격: 90 초

2.2.1 자동열차방호(ATP)장치

o 선로를 운행하는 열차의 검지기능
o 열차간격 확보를 위한 속도 계산 및 선로 조건의 Data 를 송신하는 기능

2.2.2 자동열차운전(ATO)장치

o 열차의 안정된 운전속도 패턴으로 자동운행
o 역간 열차의 자동 주행, 자동 정위치 정차
o 출입문의 자동 개폐 기능

2.2.3 자동열차감시(ATS)장치

o 전체 열차 운행을 감시하고 제어하며 운행 관리하는 기능

2.2.4 운전모드

o 완전자동운전모드: ATO 에 의한 무인자동운전(Driverless)
o 자동운전모드: ATO 에 의한 유인운전(출발시에만 승무원 출발버튼 조작)
o 수동운전모드: ATP 에 의한 수동운전
o 비상운전모드: 비상시 완전수동운전(제한속도가 없는 운전사의 주의운전)
o 기지운전모드: 차량 기지내 15Km/h 이하에서 운전

2.3 시스템 구성 및 분류

도시형 자기부상열차 신호시스템을 구성하는 시스템 구성도는 다음 그림 2와 같다.

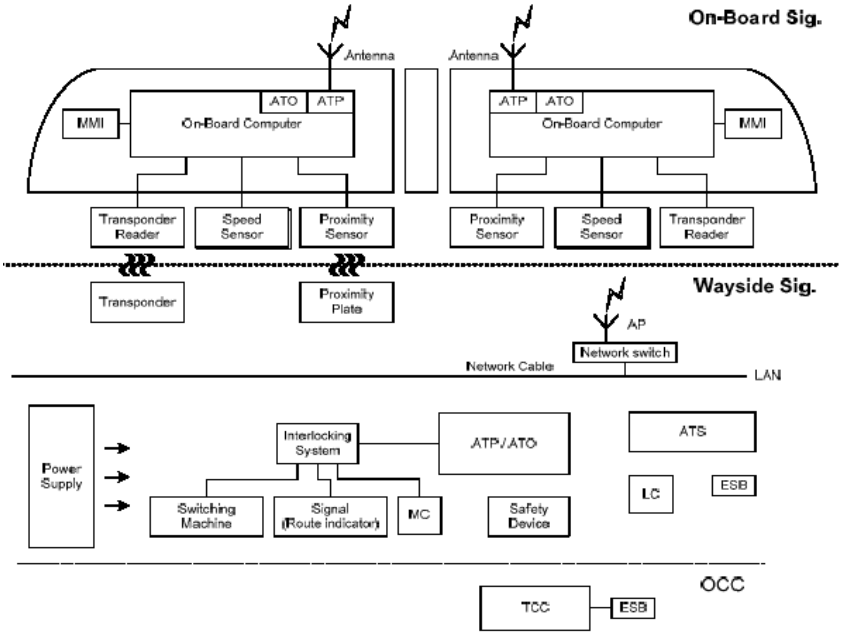

그림 2. 신호시스템 구성도

도시형자기부상열차 신호시스템은 차상신호장치와 지상신호장치로 분류된다. 차상신호장치는 자기부상열차에 탑재되는 신호장치로 구성되며, 지상신호장치는 관제실을 포함한 6 개의 정거장과 1 개의 기지에 설치되는 모든 신호장치로 구성된다.

2.4 방법론

2.4.1 LBS

LBS 는 Logistic Breakdown Structure 의 약어로 장치 계층 구조를 뜻하며, 시스템의 RAM 및 안전성 분석활동을 수행하기 위해 장치의 기능이나 특성에 따라 계층적인 구조로 시스템을 정의된 수준까지 분류하는 작업이다. LBS 는 해당 시스템의 시스템 수준(시스템, 하부시스템, 하부장치 등)과 범위를 구분할 수 있는 지표로써, LBS 를 통해 분류된 각 장치별로 MTTR, MTBF 등을 산출하여 최상위 전체 시스템의 RAM데이터를 산출하고, FMECA, SHA 등 안전성 분석활동의 대상 장치로 활용된다.

본 연구에서는 시스템 수준을 시스템, 하부시스템, 하부장치로 구분하였으며, 자기부상열차 신호시스템을 상위 시스템으로, 장치의 설치 위치 및 기능에 따라 차상신호장치와 지상신호장치를 하부시스템으로, 각 하부시스템을 구성하는 주요 장치들을 하부장치로 구분하였다.

2.4.2 시스템 위험원 분석(SHA)

시스템 위험원 분석(SHA)는 PHA 를 기본으로 수행되는 정성적인 위험도 분석 방법이며, 시스템에 사고를 초래할 수 있는 모든 잠재적인 위험요소와 사건을 규명하는 위험도 분석 방법이다.

도시형 자기부상열차 신호시스템에 대한 시스템 위험원 분석은 다음과 같은 목적을 위해 수행되었다.

o 설계 초기단계에서의 초기 위험원 및 사건 규명
o 시스템의 상세 위험원 규명
o 하부시스템과 관련된 위험원 규명
o 각 위험원의 심각도에 따른 규명된 사건의 등급 결정
o 각 위험원에 대한 허용 가능한 수준의 위험도로 저감시킬 수 있는 대책 수립

시스템 수준에서 위험원을 규명하기 위해, 신호시스템을 구성하는 하부시스템의 주요장치의 기능을 중심으로 시스템 위험원 분석이 수행되었으며 각 기능에 대한 운영조건 정상운행, 저감운행(Degraded) 그리고 비상운행(Emergency)으로 구분하여 분석을 실시하였다. 또한 가능한 많은 위험원 규명을 위해 다음과 같은 원인을 고려하여 시스템 위험원 분석이 수행되었다.

o 위험원이 내재된 구성품
o 다양한 시스템간의 인터페이스
o 운영조건을 포함한 환경요인
o 정상운영, 유지보수 및 비상운영시에 고려되어야 할 위험원
o 시스템의 오동작으로 인한 위험원들

2.4.3 HAZOP

HAZOP 은 위험원 규명을 위한 난상토론방식의 분석 방법이다. 설계에 대한 체계적이고 창의적인 의견이 도출되어야 하며, 설계에 경험이 풍부한 전문가들에 의해 수행된다. 시스템 수명주기 동안 위험원 도출을 위한 각 단계별로 수행되는 분석 방법인 예비위험원 분석, 시스템 위험원분석, 인터페이스 위험원 분석등 다양한 분석방법에 적용이 가능하다.

본 연구에서는 예비위험원 분석을 위해, HAZOP 을 적용하였으며 Guideword 를 사용하여 설계의도에서 벗어난 예외 조항들을 도출함으로써 시스템에 대한 다양한 위험원을 규명하였다.

HAZOP 을 수행하기 위한 일반적인 Guideword 는 다음과 같다.

o NO/NOT: 설계의도에 대한 출력이 없음
o MORE: 설계의도보다 출력이 정량적으로 증가
o LESS: 설계의도보다 출력이 정량적으로 감소
o AS WELL AS: 설계의도보다 출력이 정성적으로 증가
o PART OF: 설계의도보다 출력이 정성적으로 감소
o REVERSE: 설계의도와는 논리적으로 반대되는 출력이 제공
o OTHER THAN: 설계의도와는 전혀다른 출력이 제공

HAZOP은 본 사업에 참여하고 있는 신호분야 설계 전문가 및 Lloyd's Register Rail(Asia)의 컨설턴트가 참여하여 HAZOP 이 실시되었다.

2.4.4 위험도 등급

안전성 기준이 되는 위험도 등급은 위험원 분석 결과를 정량적으로 평가하기 위해 사용된다. 도시형 자기부상열차 RAMS 관리를 수행중인 SE분야에서 전체 위험도등급을 제시하였으며, 신호시스템은 제시된 위험도 등급에 따라 예비위험원 분석을 실시하여 해당 위험원이 허용가능한 수준인가를 평가한다. 본 연구에 적용되는 위험도 등급은 국제기준 및 SE분야 성과물을 참조하여 제시되었으며 해당 내용은 다음과 같다.

도표 1. 발생빈도

범 주	기 술
A. 빈번함 (Frequent)	종종 일어날 것 같음. 위험상태가 계속적으로 경험될 것이다.
B. 가능성이 있는 (Probable)	몇 번 일어날 것 같음. 위험상태가 종종 일어날 것으로 기대할 수 있다.
C. 때때로 (Occasional)	몇 번 일어날 것 같음, 위험상태가 몇 번 일어날 것으로 기대할 수 있다.
D. 가능성이 희박한 (Remote)	시스템 수명주기에서 때때로 일어날 것 같음, 위험상태가 합리적으로 일어날 것으로 기대할 수 있다.
E. 가능성이 없는 (Improbable)	가능성은 있으나 일어날 것 같지 않음, 위험상태가 예외적으로 일어날 것으로 가정할 수 있다.
F. 존재할 수 없는 (Incredible)	극단적으로 일어날 것 같지 않음, 위험상태가 일어나지 않을 것으로 가정할 수 있다.

도표 2. 심각도

범주	사람이나 환경에 대한 결과	서비스에 대한 결과
1. 치명적 (Catastrophic)	재난 및/혹은 다수의 심한 부상 및/혹은 환경에 대한 중요한 손상	
2. 임계적 (Critical)	단일 치명적 손상 및/혹은 심한 부상 및/혹은 환경에 대한 매우 중요한 손상	주요 시스템의 상실
3. 한계적 (Marginal)	사소한 부상 및/혹은 환경에 대한 매우 중요한 위협	심한 시스템 손상
4. 하찮은 (Insignificant)	가능한 사소한 손상	사소한 시스템 손상

도표 3. 위험도(Risk) 등급

발생빈도	리스크수준			
A. 빈번한	Undesirable	Intolerable	Intolerable	Intolerable
B. 가능성이 있는	Tolerable	Undesirable	Intolerable	Intolerable
C. 때때로	Tolerable	Undesirable	Undesirable	Intolerable
D. 가능성이 희박한	Negligible	Tolerable	Undesirable	Undesirable
E. 가능성이 없는	Negligible	Negligible	Tolerable	Tolerable
F. 존재할 수 없는	Negligible	Negligible	Negligible	Negligible
	4.하찮은	3.한계적	2.임계적	1.치명적
	발생결과의 심각도			

도표 4. 허용가능한 수준

위험도 범주	각 범주에 대해 적용된 작용
허용할 수 없는(Intolerable)	반드시 제거되어야 함
바람직하지 않은(Undesirable)	리스크 수준을 낮추는 것이 곤란하고 발주자(원도급)의 동의에 따라 허용가능
허용 가능한(Tolerable)	적절한 통제 및 발주자(원도급)의 동의에 따라 허용가능
하찮은(Negligible)	발주자(원도급)의 동의 없이 허용 가능

2.5 RAM 목표 설정 및 할당

일반적으로 RAM 목표 설정은 분석 대상 시스템에 대한 과거 고장데이터를 분석하고, 주어진 신뢰구간 내 확보된 고장 발생빈도를 이용하여 Chi-square 와 같은 통계학적인 방법을 통해 고장률을 예측한 후 각 하부시스템별 RAM 목표를 할당한다. 그러나 본 연구에서는 현재 각 하부시스템의 RAM 목표 할당을 위한 도시형 자기부상열차 전체 시스템에 대한 RAM 목표 값이나 신호시스템의 고장데이터가 제시되지 않았으므로 유사한 타 프로젝트에서 이용되었던 장치의 고장률을 참조하여 고장률을 예측한 후 신호시스템 전체에 대한 RAM 목표치를 설정하고, 설정된 RAM 목표치에 각 하부시스템 및 하부장치의 고장 발생 비율과 하부시스템에 대한 가중치를 적용하여 목표를 할당한다.

일반적인 신뢰성 예측은 고장률의 정의를 지수함수 형태로 아래에서 정의되는 수식으로 가정하며, 시스템의 신뢰성 블록 다이어그램에서 도출되는 직/병렬 구성에 따라 아래와 같은 수식으로 고장률을 계산한다. 또한 고장률이 지수분포를 따를 때는 정의에 따라 MTBF는 고장률의 역수로 표현될 수 있다.

2.5.1 신뢰성 예측

a. 지수분포에 따른 신뢰도 함수

$$R_{sys}(t) = e^{-\lambda_{sys} t}$$

λsys : 시스템고장률, t : 시간

b. 직렬 구성에 따른 고장률 산출

$$\lambda_S = \lambda_1 + \lambda_2 + \lambda_3 + \ldots\ldots + \lambda_N$$

N : 직렬 구성 개수

c. 병렬 구성에 따른 고장률 산출

$$\lambda_{\frac{(N-q)}{N}} = \frac{\lambda}{\sum_{i=N-q}^{N} \frac{1}{i}}$$

N : 병렬 구성 개수

q : 고장발생 허용 가능한 장치의 개수

2.5.2 유지보수성 예측

하부 시스템의 조합으로 이루어진 시스템의 유지보수성은 장치 계층 구조를 통해 도출된 하부장치를 기준으로 산출된다. 유지보수성에 대한 예측은 다음과 같은 수식에 의해 계산된다.

$$MTTR = \frac{\sum_{i=1}^{N} (\lambda_i \times MTTR_i)}{\sum_{i=1}^{N} \lambda_i}$$

MTTR: 시스템의 평균 수리시간

λi: 시스템을 구성하고 있는 하부시스템의 고장률

MTTRi: 하부시스템의 평균수리시간

N: 하부시스템의 개수

2.5.3 가용성 예측

도시형 자기부상열차의 가용도 예측은 RAMS 관련 규격인 EN50126 에서 정의하는 아래 가용도 산출수식을 기반으로 예측한다. 시스템 가용도는 MTBF 와 MTTR 로 산출한다.

$$A = \frac{MTBF}{MTBF + MTTR} \times 100\%$$

MTBF: 시스템의 평균 수명시간

MTTR: 시스템의 유지보수도

2.5.4 Chi-square

일반적으로 Chi-square 분석은 주어진 신뢰구간 내에서 활용이 가능한 고장의 발생 수에 대한 제한된 데이터를 근거로 시스템의 고장률을 추정할 때 사용된다.

Chi-square 에서 사용되는 일반 수식은 다음과 같다.

$$\hat{\theta} \geq \frac{2T}{\chi^2(\alpha, 2r+2)}$$

^

Θ: 평균수명

T : 총 시험 시간

α: 유의수준(신뢰수준=100×(1- α)%)

r : 고장 개수

T=n(시료 수)×h(시험 시간)를 근거로, 상기 수식을 다음과 같이 적용한다.

$$\hat{\theta} \geq \frac{2nh}{\chi^2(\alpha, 2r+2)}$$

신뢰구간과 고장 개수에 따라 산출되는 추정수명(Θ)의 최소 값이 각 하부시스템의 평균 수명 목표 이상으로 나오게 되는 신뢰 구간과 고장 개수를 선정하여 최대 고장 허용 개수를 결정한다.

2.6 분석결과

2.6.1 장치 계층 구조(LBS)

도시형자기부상열차 신호시스템의 하부 시스템은 차상신호장치와 지상신호장치로 분류된다. 분석된 장치 계층 구조는 다음 그림과 같다.

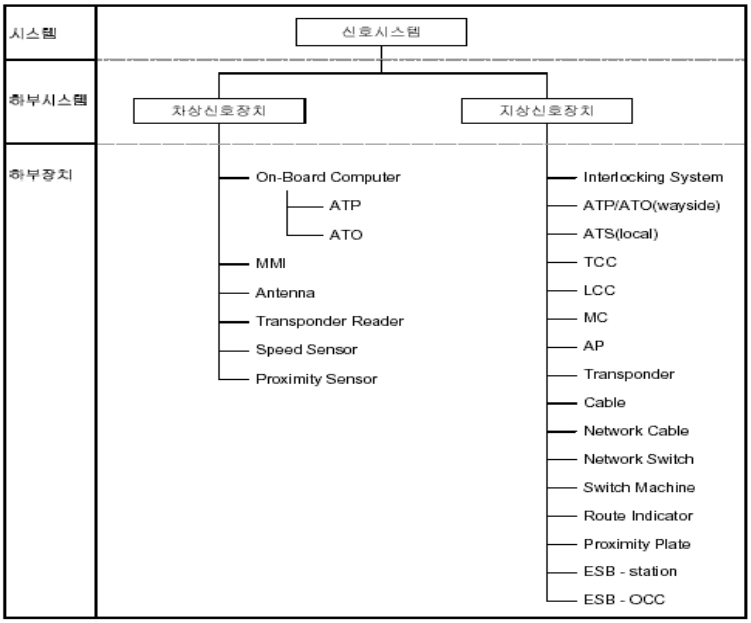

그림 3. 신호시스템 장치계층 구조

2.6.2 차상신호장치

차상신호장치는 도시형 자기부상열차에 탑재되는 장치로써 LBS 분석결과 총 6 개의 하부장치로 구성되며, 하부장치 중 On-Board Computer 장치는 ATP 와 ATO 장치로 구성된다. 차상신호장치 하부시스템 전체는 이중계로 구성되며, 단위별 차상신호장치의 하부장치 종류와 수량은 다음과 같다.

도표 5. 차상신호장치 구성품

하부장치	설 명	수량	비고
On-Board Computer	차상 컴퓨터 장치	1	
ATP	자동 열차 보호장치	1	
ATO	자동 열차 운행장치	1	
MMI	기관사와 차상신호장치간 인터페이스 장치	1	
Antenna	무선 안테나	1	
Transponder Reader	트랜스폰더 리더	1	
Speed Sensor	속도 센서	2	
Proximity Sensor	정위치 검지기	1	

2.6.3 지상신호장치

지상신호장치는 6 개의 정거장과 1 개의 차량기지에 설치되는 신호장치로 구성되며, 하부장치 종류와 수량은 다음과 같다.

도표 6. 지상신호장치 구성품

하부장치	설명	수량	비고
Interlocking System	연동장치	4	
ATP/ATO(wayside)	선로변 ATP/ATO 장치	3	이중계
ATS(local)	로컬 ATS 장치	1	이중계
TCC	열차 제어 컴퓨터	1	이중계
LC	로컬 컨트롤(Local Control)	3	
MC	유지보수 콘솔	3	
AP	무선 통신 장치	30	
Transponder	트랜스폰더	200	이중계
Terminal Box	장치간 연결을 위한 터미널 박스	30	
Cable	장치 연결 케이블	-	
Network Cable	랜선	-	
Network Switch	네트워크 스위치	16	
Switch Machine	분기기	22	
Route Indicator	진로표시기	21	
Proximity Plate	정위치 정차 검지기	24	
Power Supply	전원 공급장치	4	
Emergency Stop Button- Station	역에 설치된 비상정지버튼	6	
Emergency Stop Button - OCC	OCC 에 설치된 비상정지버튼	1	

2.7 RAM 목표

2.7.1 신뢰도 및 유지보수도 목표

도시형 자기부상열차 신호시스템과 유사한 타 프로젝트의 신뢰성 데이터를 참조하여 신호시스템 전체의 RAM 목표치와 하부시스템별 RAM 목표치를 다음과 같이 설정하였으며, 이는 상기의 시스템 계층 구조에 제시된 시스템의 수량과 직/병렬 연결 방식을 고려하였다.

a. 신뢰도 목표

RAM 목표치로 선정된 MTBSAF 는 서비스에 영향을 미치는 고장발생간 평균시간을 의미하며, 도출된 비율에 따라 RAM 목표치를 설정한다.

도표 7. 시스템 서비스 영향 고장률

항 목	서비스영향고장률	MTBSAF	비 고
신호시스템	6.91 $\times 10^{-6}$	14,944.81	
차상신호장치	27.00 $\times 10^{-6}$	55,555.56	27%
지상신호장치	48.91 $\times 10^{-6}$	20,444.52	73%

RAM 목표치 설정에 참고된 타 프로젝트 시스템 하부 장치의 종류가 상이할 수 있으므로 제시된 수치는 향후 제시될 고장 데이터와 해당 분야 전문가의 엔지니어적 판단에 의해 산출된 RAM 목표치로 대체될 수 있다. 전체 신호시스템의 서비스 영향 고장률에 대한 각 하부시스템별 하부장치의 MTBSAF는 다음과 같으며, 이는 상기의 시스템 계층 구조에 제시된 각 하부장치의 수량과 직/병렬 연결 방식을 고려하였다.

도표 8. 하부장치 고장발생 비율

차상신호장치		지상신호장치	
하부장치	MTBSAF	하부장치	MTBSAF
On-Board Computer	50,000	Interlocking System	250,000
MMI	500,000	wayside ATP/ATO	500,000
Antenna	1,000,000	ATS	1,500,000
Transponder reader	1,000,000	TCC	750,000
Speed Sensor	500,000	LC	166,667
Proximity Sensor	1,000,000	MC	166,667
		AP	200,000
		Transponder	750,000
		Terminal Box	3,333,333
		Cable	765,580
		Network Cable	4,166,667
		Network Switch	187,500
		Switch Machine	454,545
		Route Indicator	476,190
		Proximity Plate	416,667
		Power Supply	125,000
		Emergency Stop Button - Station	1,666,667
		Emergency Stop Button - OCC	10,000,000

b. 유지보수도 목표

유지보수도는 각 하부장치별 제시된 유지보수도 데이터가 없으므로 전체 신호시스템의 유지보수도를 1 시간 이내로 가정한다.

c. 가용도 목표

본 사업에서 제시한 서비스 가용도는 열차출발계획 건수와 정시출발 건수를 고려하여 98% 이상의 열차 정시성을 확보하도록 목표치가 설정되어 있다.

$$SA = \frac{(PD - MD + \frac{1}{2}UD)}{PD} \geq 98\%$$

SA: Service Availability

PD: Planned Departure

MD: Missed Departure

UD: Unplanned Departure

제시한 서비스 가용도를 기준으로 도시형 자기부상열차의 가용도는 EN50126 의 정의에 따라 시스템의 MTBF 와 MTTR 을 통해 98% 이상을 확보할 수 있도록 목표를 설정한다. 상기에서 제안한 시스템의 MTBSAF를 기준으로 유지보수도를 1 시간으로 가정하여 다음과 같이 신호시스템의 가용도 목표를 설정한다.

$$A = \frac{MTBSAF}{MTBSAF + MTTR} \times 100\% = \frac{14{,}944.81}{14{,}944.81 + 1} \times 100\%$$

$$= 99.99\%$$

제시한 서비스가용도 98%이상의 열차 정시성 확보와 관련한 RAM 성능목표와 비교하여 설정된 신호시스템의 가용도는 99.99%로 제시한다.

2.8 시스템 위험원 분석 결과

2.8.1 위험원 규명

도시형 자기부상열차 신호시스템의 상세 설계에 대한 위험원 분석은 2차에 걸친 시스템 위험원 분석 회의를 통해 실시되었으며, HAZOP 방법을 사용하여 전문가들과의 난상토의를 통해 총 63 개의 위험원이 다음과 같이 규명되었다.

도표 9. 시스템 위험원 분석 결과

대상 장치	규명된 위험원 개수	초기 위험도 등급에 따른 위험원 개수			
		허용할 수 없는 (In)	바람직하지 않은 (Un)	허용 가능한 (To)	하찮은 (Ne)
On-Board Computer	16	10	6	-	-
Interlocking System	10	5	5	-	-
wayside ATP/ATO	15	10	5	-	-
ATS	11	11	-	-	-
TTC	11	11	-	-	-
합계	63	47	16	-	-

2.9 시스템별 안전성 요구사항

2.9.1 차상신호장치

시스템 위험원 분석으로부터 도출된 On-Board Computer 장치의 16 개 위험원에 대한 차상신호장치의 저감대책 즉 안전성 요구사항은 22 개 항목이다.

2.9.2 지상신호장치

a. Interlocking System

시스템 위험원 분석으로부터 도출된 Interlocking System 의 10 개 위험원에 대한 지상신호장치의 저감대책 즉 안전성 요구사항은 23 개 항목이다.

b. wayside ATP/ATO

시스템 위험원 분석으로부터 도출된 wayside ATP/ATO 의 15 개 위험원에 대한 차상신호장치의 저감대책 즉 안전성 요구사항은 27 개 항목이다.

c. ATS

시스템 위험원 분석으로부터 도출된 ATS 의 11 개 위험원에 대한 차상신호장치의 저감대책 즉 안전성 요구사항은 22 개 항목이다.

d. TCC

시스템 위험원 분석으로부터 도출된 TCC 의 11 개 위험원에 대한 차상신호장치의 저감대책 즉 안전성 요구사항은 21 개 항목이다.

2.10 RAMS 요구사항

신호시스템 공급자는 시스템의 안전성 및 신뢰성을 보증하기 위해 다음과 같은 일반 요구사항을 만족해야 한다.

o 공급 시스템에 대한 RAMS 활동을 EN 50126, EN50128, EN50129 에 부합하도록 수행해야 한다.

o 공급 시스템은 국내 철도 안전관련 법, 시행령, 시행규칙을 만족해야 한다.

o 공급시스템은 국내 철도시설 안전기준에 관한 규칙 및 안전세부기준을 만족해야 한다.

2.10.1 신뢰성 목표

시스템 장치계층 구조에 따라 차상신호장치와 지상신호장치로 크게 분류되어 각각의 목표를 다음과 같이 제시한다.

o 차상 신호시스템의 MTBSAF 는 50,000 시간 이상이어야 한다.

o 지상 신호시스템의 MTBSAF 는 20,000 시간 이상이어야 한다.

2.10.2 유지보수성 목표

현장교체가능한 장치를 기준으로 MTTR 이 1 시간 이내이어야 한다. 단, 물류시간과 같은 제반 시간은 제외되어야 한다.

2.10.3 가용성 목표

신호시스템 전체에 대한 서비스 가용도는 99.9%이상이어야 한다.

2.10.4 안전성 목표

신호시스템에 대한 정성적인 안전성 목표는 EN 50126 에서 제시한 위험도 등급을 기준이 적용되며, ALARP 의 원칙에 따라 허용 가능한 위험도 등급에 부합하도록 저감대책을 수립해야 한다.

2.11 RAMS 활동 요구사항

2.11.1 RAM 활동 요구사항

신호시스템 공급자는 EN 50126 에서 권고하는 시스템 수명주기에 따라 개발된 시스템을 공급해야 하며, 설계 단계에서 RAM 예측업무를 수행해야 한다. 또한 시운전 혹은 영업운전기간 동안 정해진 시간을 통해 신뢰성 및 유지보수성에 대한 입증시험을 수행해야 한다.

2.11.2 Safety 활동 요구사항

신호시스템 공급자는 EN50126 에서 권고하는 시스템 수명주기에 따라 개발된 시스템을 공급해야 하며, 설계, 제조 및 설치 단계에서 안전성 분석이 수행되어야 한다. 또한 시운전기간 동안 안전성 입증시험을 수행해야 한다.

2.11.3 소프트웨어 보증활동 요구사항

신호시스템 공급자는 EN50128 에 따라 시스템에 탑재되는 소프트웨어에 대한 보증업무를 수행해야 한다.

2.11.4 안전성 인증활동 요구사항

신호시스템 공급자는 독립적인 인증기관으로부터 해당 시스템에 대한 안전성 인증을 받아야 한다.

2.11.5 시스템 고장 조치활동 요구사항

신호시스템 공급자는 고장 보고 및 교정조치 시스템(FRACAS)을 구축하고 고장 방지 및 재발을 최소화하기 위한 활동을 수행해야 한다. 또한 교정조치를 통해 시스템 신뢰성 향상을 위한 방안을 제시해야 한다.

2.11.6 안전 설계 요구사항

신호시스템 공급자는 시스템별 안전성 요구사항에 각 하부시스템에 대한 안전 설계를 수행해야 한다.

2.11.7 산출물 요구사항

신호시스템 공급자는 EN50126 에서 권고하는 시스템 수명주기에 따라 다음과 같은 산출물을 제출해야 한다.

도표 10. RAMS 활동 산출물

<table>
<tr><th>단계</th><th>RAMS 활동 산출물</th><th>S/W 보증활동 산출물</th><th>비고</th></tr>
<tr><td>기본
설계</td><td>RAMS Plan
V&V Plan
PHA
Verification Report
(기본설계)</td><td rowspan="3">S/W Quality Assurance Plan
S/W Configuration Management Plan
S/W Verification Plan
S/W Validation Plan
S/W Integration Test Plan
S/W & H/W Integration Test Plan
S/W Requirement Specification
S/W Requirement Test Specification
Verification Report(S/W Requirement)
S/W Design Specification
Verification Report(S/W Design)
S/W Module Design Specification
S/W Module Test Specification
Verification Report(S/W Module Design)</td><td></td></tr>
<tr><td>상세
설계</td><td>System Breakdown List
SHA
SSHA
IHA
SIL Allocation Report
Verification Report
(상세설계)</td><td></td></tr>
<tr><td>제작</td><td>FMECA
FTA
RBD
RAM Analysis Report
O&SHA
Verification Report(제작)</td><td></td></tr>
<tr><td>시험</td><td>Safety Validation Report</td><td>S/W Module Test Report
S/W Integration Test Report
S/W & H/W Integration Test Report
Validation Report</td><td></td></tr>
<tr><td>시운전</td><td>RAM Demonstration Report (FRACAS 포함)
Hazard Log
Safety Case</td><td></td><td>RAM Demonstration Report 는 사업 공정에 따라 제출시기가 변경될 수 있다.</td></tr>
</table>

3. 결론

도시형 자기부상열차 신호시스템의 상세설계에 대한 RAMS 요구사항 개발은 시스템 분류, 시스템별 위험원 분석, 안전요구사항 도출 그리고 RAM 목표설정을 중심으로 수행되었다. 신호시스템의 하부시스템별 위험원은 총 63 개로 규명되었고, 안전성 요구사항의 경우 각 주요 하부시스템별로 차상신호장치 22 개 및 지상 신호장치 93 개가 도출되었다. 도출된 안전성 요구사항은 각 주요 하부시스템의 상세설계시에 반영되어야 하며, 향후 시스템 공급자가 반드시 만족해야하는 사항이다.

RAM 목표설정의 경우, 유사한 타 프로젝트에서 분석된 RAM 데이터를 기준으로 수립되었다. 또한 하부시스템별 정확한 RAM 목표 설정을 위해, 자기부상열차에 대한 고장 데이터가 수집되어 분석되어야 하지만, 데이터의 부재로 인해 유사한 타 프로젝트에서 분석된 RAM 데이터를 역시 활용하였다. 그러나 향후 신호시스템 전체에 대한 RAM 목표를 제시한다면, 제시된 RAM 목표를 근거로 재 산출이 이루어 질 수 있다. 향후 신호시스템 공급자는 상세설계에서 도출된 RAMS 요구사항을 근거로 시스템 수명주기별 RAMS 활동이 수행되어야 하며, 필요시 독립 기관으로부터의 안전인증을 받을 것을 권고한다.

감사의 글

본 연구는 국토해양부 대형국가연구개발실용화사업 “도시형자기부상열차실용화사업”의 일환으로 수

행 되었습니다.

참고문헌

1. 김종기, 이종우, 임훈(2003), “철도RAMS의 적용에 관한 고찰”, 한국철도학회. 춘계학술대회 논문집, pp.505-510
2. 김종기, 신덕호, 이기서(2006), “열차제어시스템의 안전계획 수립에 관한 연구” 한국철도학회논문집. 제9권, 제3호, pp.264-270
3. EN 50126 : Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety(RAMS)
4. EN 50128 : Railway applications - Communication, signalling and processing systems Software for railway control and protection systems
5. EN 50129 : Railway application s- Communication, signalling and processing systems- Safety related electronic systems for signalling
6. 김수명, 이덕규, 이경학, 이기서, 신석균(2006), "철도시스템 RCM 적용을 위한 신뢰성 및 안전성 분석 활동에 관한 연구", 한국철도학회논문집, v.9, no.6, pp.739-745