한국철도학회논문집
제14권 제6호(2011년 12월) pp. 515-525

도시형자기부상열차 열차제어시스템 RAMS 분석에 관한 연구

A Study on the RAMS Analysis of Urban Maglev Train Control System

윤학선† · 이기서[1] · 류승균[2] · 양동인[3]
Hak-Sun Yun · Key-Seo Lee · Sung-Kyun Ryou · Dong-In Yang

Abstract In this study, Urban maglev is applied to inductive-loop speed and position detection system for the top-level classification system for the entire system, and performed functional analysis On-board signal equipment, Wayside-signal equipment divided by the reliability, availability, maintainability, and safety through analysis of the proposed formula. RDB and by applying a system service for each device was calculated to availability, safety analysis. The PHA, FMEA, HAZOP over the Top Event of the FTA is performed by presenting the results. This also shows approach methods and relative activities for project to accomplish and ensure the system requirements.

Keywords : Urban Maglev, RAMS, Train Control System, Safety analysis

초 록 도시형 자기부상열차 실용화사업에 적용된 유도무선루프방식 열차제어시스템에 대하여 최상위 레벨에서 전체 시스템에 대한 시스템 분류, 기능 분석을 시행하고 차상신호설비, 지상신호설비로 나누어 신뢰도, 가용도, 유지보수도 및 안전도를 수식을 통하여 분석한 결과를 제시하였다. RAM 분석은 신뢰도 블록도(RBD)를 각 장치별로 적용하여 시스템 서비스 가용도를 산출하였고, 안전도 분석은 PHA(예비위험원 분석), FMEA (고장모드영향분석), HAZOP을 통한 각각의 정상사상(Top Event)의 FTA(고장트리분석)을 시행하고 그 결과를 제시하여 RAMS 목표 값에 도달함을 수식을 통하여 증명하였다.

주요어 : 도시형자기부상열차, RAMS, 열차제어시스템, 안전성 분석

1. 서 론

본 논문에서는 국가 R&D사업으로 인천광역시 영종도(인천국제공항)일원에 시행중인 도시형자기부상 열차실용화 사업 시범노선에 적용된 무인운전이 가능한 유도루프방식 열차제어시스템에 대하여 최상위 레벨 (Top Event)에서 전체 시스템에 대한 분류, 기능 분석을 시행하고 차상신호설비, 지상신호설비로 나누어 신뢰도, 가용도, 유지보수도 및 안전도를 분석한 결과가 도시형자기부상철도 RAMS 요구사항을 만족하는지 제시하였다. RAMS 활동은 시스템에 요구된 정량적 목표를 만족하도록 관리하여 객관적인 정보를 통해 목표달성을 입증하고(RAM), 시스템의 위험원으로 인한 리스크가 허용할 수 있는 수준으로 건전하게 제어되었음을 객관적인 정보를 통해 입증 (Safety)하는 절차이다. RAM 분석을 위하여 미국방성 MIL-HDBK-217FN2에서 제시한 방법론을 토대로, Reliability Workbench 분석 툴을 활용하여 RAM Prediction 분석을 위한 Reliability Prediction module, RAM Modeling 분석을 위한 Reliability Block Diagram(신뢰도 블록도) module을 이용하여 각 장치 별로 시스템의 서비스 가용도를 산출하였고, 안전도 분석을 위하여 PHA(예비위험원 분석), FMEA(고장모드영향분석), HA ZOP Study를 수행하고 각각의 정상 사상(Top Event)의 FTA(고장트리분석)을 Fault Tree module을 이용하여 그 결과를 분석하여, 도시형자기부상열차 신호시스템이 요구되는 RAMS 목표 값에 도달함을 수식을 통하여 증명하였다. 열차제어시스템 전체에 대하여 RAMS 분석을 시행하고 안전 무결성 등급에 대한 인증을 획득하는 것은 도시형 자기부상열차 실용화 사업 시범노선 건설사업이 국내 최초로 수행하는 것이다.

†교신저자 : 한국철도시설공단 녹색철도연구원
E-mail : kamayun@naver.com
[1]광운대학교 정보제어공과대학 로봇학부
[2]한국철도시설공단
[3]국토해양부 해양조사원

2. 열차제어시스템 RAMS 분석

2.1 열차제어시스템의 장치별 구성에 따른 분류

열차제어시스템의 장치별 하드웨어 및 소프트웨어 분류는 그림 1과 같다. 최상위 레벨인 열차제어 시스템에 Subsystem으로 차상신호설비, 지상신호설비, 관제설비, 신호기계실설비, 전원설비, 안전설비로 나뉠 수 있다. 구체적으로 언급하면 차상신호설비는 차상 ATP/ATO장치, 화면표시장치, ATP/TD장치, ATO Local 장치, 속도 검출기, ATO 데이터장치 등으로 구성되며, 지상신호설비는 지상ATP장치와 그 부속장치, 지상ATO 장치 및 그 부속장치, 전자연동장치는 연동 논리랙, 현장 단말랙, Local console 등으로 구성되며, 관제 설비는 TCC, DCC, Operator console, Programmer console, Supervisor console, Wall controller, Depot console 등으로

구성되며, 신호기계실 설비의 FT/OT랙, IFR랙으로 전원설비는 UPS, Battery, 분전반 등으로 구성되며, 추가 안전설비로 강풍, 강우 검지장치로 구성된다[1,2].

2.2 RAMS 목표[1]

본 논문에서 제시된 RAMS 값은 도시형 자기부상 철도 전체 시스템에 대한 RAMS 목표 값 달성을 위하여 1세부과제에서 각 서브시스템 별로 할당된 목표 값에 대하여 실시설계 단계에서 분석한 결과를 도시형 자기부상열차 실용화 사업 RFP에 반영한 결과 값이다.

2.2.1 신뢰도 목표

타 사업 및 유사 경량철도시스템의 경험을 토대로 열차제어시스템의 안전성 및 신뢰성을 보증하기 위하여 시스템 계층 구조에 따라 지상신호시스템과 차상신호시스템으로 크게 분류하여 신뢰도 목표를 설정하였다.

- 지상신호시스템의 MTBSAF는 20,000시간 이상 이어 야 한다.
- 차상신호시스템의 MTBSAF는 50,000시간 이상 이어 야 한다.

2.2.2 유지보수도 목표

유지보수도는 현장 교체 가능한 장치를 기준으로 MTTR이 1시간 이내 이어야 한다.

2.2.3 가용성 목표

자기부상철도시스템 전체에서 요구하는 서비스 가용도 98%를 만족하기 위하여 열차제어시스템에 대한 서비스 가용도는 99.99% 이상 되도록 설정하였다.

2.2.4 안전성 목표

안전성 목표는 임의대로 정할 수 있으나, 본 논문에서는 국제적으로 인정받는 IEC62278, 62279, EN50129 등에서 요구하는 표준 및 절차에 따라 시스템의 Safety 목표를 설정하였다.자기부상열차 열차제어시스템을 모델로 실제로 설계에 반영된 Hardware 및 Software Safety 활동과 Software Quality Assurance를 시행하였다. 하드웨어 및 소프트웨어에 대하여 안전 무결성 등급(Safety Integrity Level)을 할당하여 SIL 4 수준을 만족하도록 설정하였다.

2.3 RAM 분석

2.3.2 RAM 분석 조건

열차제어시스템 RAM 분석 활동은 다음의 조건을 기반으로 수행하였다.

1. 여분(Redundancy)을 갖지 않는 하부 구성요소는 직렬구성을 기본으로 한다. 단, 동일한 동작 수행을 위한 여분구조는 병렬로 구성한다.
2. 신뢰도 예측을 위한 고장률 분포함수는 기본적 으로 지수분포함수(Exponential Distribution)로 가정 한다.
3. 정량적인 분석을 위한 신뢰도 및 유지보수도 데이터는 다음 수준의 데이터들을 참조한다. 즉, 수준 1에 해당하는 데이터 참조가 불가능할 경우, 수준 2에 해당하는 데이터를 참조한다. 하위 수준도 동일한 의미로 해석된다
   ① 수준 1(F): 현장운영 실적에 따른 현장 데이터(Field Data) 또는 공급업체 제공 데이터
   ② 수준 2(T): 해당 구성요소의 시험 데이터(In-house test or lab test data)
   ③ 수준 3(P): PCB기반의 부품정보 활용을 통한 예측 데

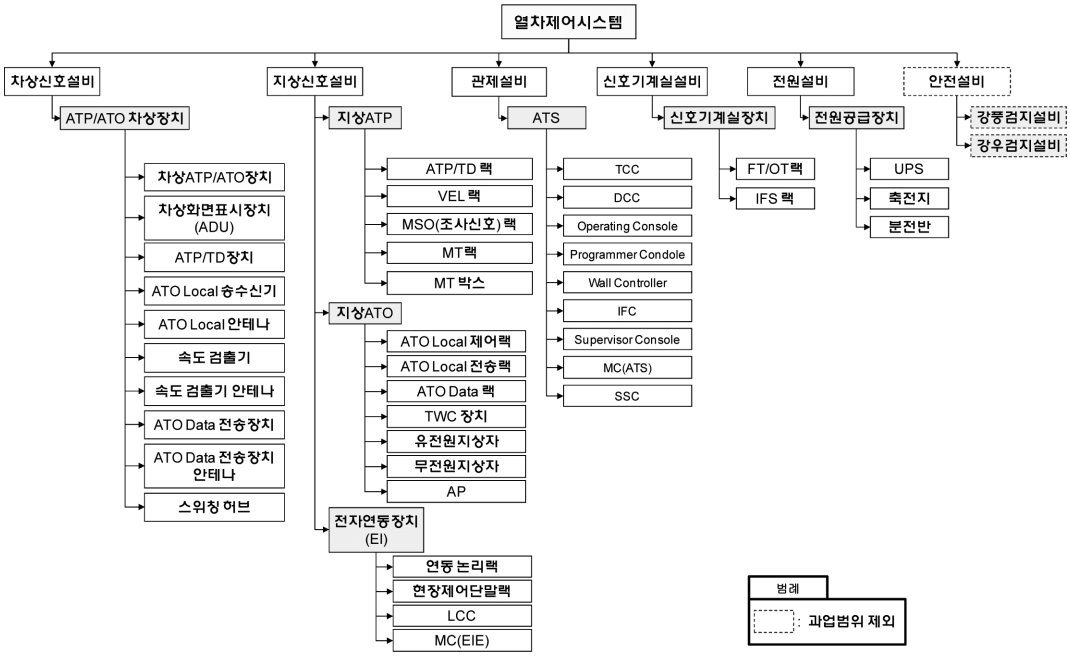


Fig. 1 Classification by equipment of train control system

이터(Prediction Data) 및 표준 라이브러리 데이터
④ 수준 4(S): 유사장치 데이터

4. 신뢰도 예측은 MIL-HDBK-217FN2를 기준으로 하며, 고장률 단위는 '고장건수/1,000,000 Hrs(FPMH)'이다.

MTBSAF 예측에 있어서, 서비스에 영향을 주는 고장(Service Affecting Failure)의 정의는 열차운행 계획 대비 한 역사를 기준으로 10분 이상의 도착지연을 초래하는 고장으로 정의한다. 단, 타 분야 시스템, 장치의 기능 및 인터페이스 오류(타 설비 기능 오류 및 Vandalism, Terrorism 포함)로 인한 도착지연은 포함하지 않는다.

5. 유지보수도 분석을 위한 MTTR 예측은 MIL-HDBK-472를 근거로 하되, 정량적인 데이터 분석은 경험에 근거한 엔지니어링 판단(Experience based engineer ing judgment)을 통해 1시간 이내에 수행 될 것으로 가정한다.

6. 정량적인 MTTR 예측 시, 현장 또는 차량기지에서 유지보수에 소요되는 시간만을 고려한다. 즉, 물류 (Logistics Delay Time) 및 행정소요시간 (Adminis-trative Delay Time)은 분석에서 제외한다. 단, 서비스 가용도(SA) 산출을 위한 물류 및 제반 소요 시간은 다음가정사항을 참고하였다.

· OCC 운영자(관제 요원)의 개입 시: 0분
· 차상 안전요원 개입 시: 0.5분
· 역사 순회점검요원의 개입 시: 2분
· 유지보수 직원이 개입 시: 20분

2.3.3 RAM 분석 수식

2.3.3.1 신뢰도 분석 수식[7,9,10]

신뢰도 분석을 위한 매개변수는 고장률(λ), 평균수명(MTBF) 및 MTBSAF이며, 다음 식 1, 2, 3, 4를 적용한다.

$$\lambda_s = \sum_{i=1}^{N} (\lambda_{p_i} \times Qty_{p_i}) \tag{1}$$

λ_s: 시스템 고장률(FPMH), λ_p: 부품 및 구성요소 고장률(FPMH), Qty_p: 부품 및 구성요소 수량

$$\lambda_{(n-q)/n} = \frac{[n! \times (\lambda)^{q+1}]}{[((n-q)-1)! \times \mu^q]} \tag{2}$$

λ: 고장률(FPMH), n: 전체 유니트 수, q: 고장이 허용되는 유니트 수, μ: 구성요소 평균수리율

1) 단일계 고장률 계산식

$$\lambda_i = \frac{1}{MTBF_i} \tag{3}$$

λ_i: 구성요소 고장률(FPMH), $MTBF_i$: 구성요소 평균수명(Hr)(재사용하는 경우)

2) 다중계 고장률 계산식

식 1에 n=2(전체 모듈 개수), q=1(대기여분의 모듈 개수) 대입하여 전개하면

$$\lambda_{(2-1)/2} = \frac{[2! \times (\lambda)^{(\lambda)(1+1)}]}{[((2-1)-1)! \mu^1]} = \frac{2! \times (\lambda)^2}{\mu}$$

결과적으로

$$\lambda_{1/2} = 2(\lambda)^2 \times MTTR \tag{4}$$

λ: 구성요소 고장률(FPMH), $MTTR$: 구성요소 평균수리시간

2.3.3.2 유지보수도 분석 수식

유지보수도 분석을 위한 매개변수로 MDT와 MTTR은 다음 식 5와 6을 적용한다.

$$MDT = MTTR + LDT + ADT \tag{5}$$

$$MTTR_s = \frac{\sum_{i=1}^{N} (\lambda_{P_i} \times Qty_{p_i} \times MTTR_{P_i})}{\sum_{i=1}^{N} (\lambda_{P_i} \times Qty_{p_i})} \tag{6}$$

$\lambda_{차상장치} = \lambda_{MCI} + \lambda_{예비\ ATP/TD\ Tx/RX\ to\ AP} + \lambda_{MC2}$

$MTTR_S$: 시스템 평균수리시간, $MTTR_P$: 부품 및 구성요소 평균수리시간, Qty_P:부품 및 구성요소 수량

참고로, 평균수리시간(MTTR)과 평균수리율(μ)과의 관계는 식 7과 같다.

$$MTTR_i = \frac{1}{\mu_i}, \quad \mu_i = \frac{1}{MTTP_i} \tag{7}$$

$MTTR_i$: 구성요소의 평균수리시간, μ_i: 구성요소의 평균 수리율

2.3.3.3 가용도 분석 수식

가용도 분석을 위한 매개변수는 SA(%)이며, 서비스 가용도 분석을 위해 식 8을 적용한다.

$$SA(\%) = \frac{MTBSAF}{MTBSAF + MDT} \times 100\% \tag{8}$$

SA(%) : 해당 장치의 서비스 가용도, MDT: 해당 장치의 가동중지 시간,

$MTBSAF$: 해당 장치의 평균수명(서비스 영향 고려한)

2.4 차상신호설비 RAM 분석

2.4.1 신뢰도 분석

차상신호설비의 신뢰도 분석을 위한 신뢰도 블록도는 그림 2와 같다. 단, 신뢰도 블록도는 전체 구성요소 가운데 서비스에 영향을 미치는 구성 요소만으로 작성되었다. 그림 2의 신뢰도 블록도에서 MC1과 MC2의 구성은 동일하다. MC1에 위치하는 차상ATP/ATO 장치는 ATP/ATO Controller가 Redundancy (Hot-Standby)로 구성되어 있으며, 전체적으로 량당 Redundancy 형태를 가진다. 그림 2의 Redundancy에 해당하는 부분은 다음과 같이 분석되었다.

$\lambda_{ATP/TD\ Tx/Rx\ to\ AP} = \lambda_{ATP/TD\ Tx/Rx} + \lambda_{VEL} + \lambda_{VEL\ Ant} + \lambda_{ATO\ Local\ Tx/Rx} + \lambda_{ATO\ Local\ Ant} + \lambda_{Switching\ Hub} + \lambda_{AP} = 57.77E\text{-}08$

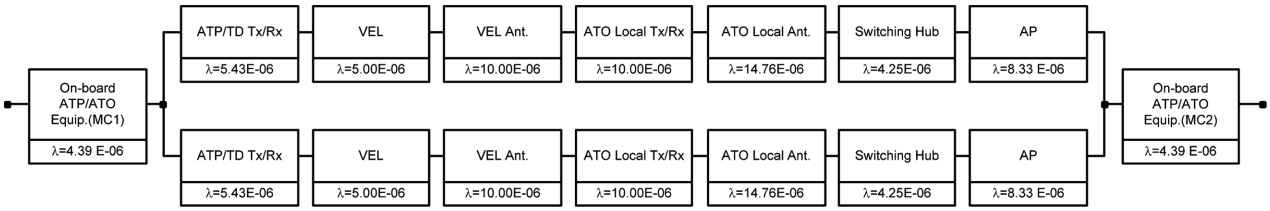


Fig. 2 Reliability Block Diagram of On-board signaling equipment

이중계 시스템 신뢰도 블록도에 대한 계산을 식 4를 적용하면 다음과 같이 산출된다.

$$\lambda_{\text{Redundancy for ATP/TD Tx/Rx to AP}} = 6.7\text{E-}08$$

위의 분석 결과를 기반으로 차상신호설비 전체의 고장률은 다음과 같이 산출되었다.

$$= 4.39\text{E} - 06 + (6.67\text{E} - 08) + 4.39\text{E} - 06$$
$$= 8.85\text{E} - 06$$

결과적으로, 서비스에 영향을 미치는 고장을 분석 하여 산출한 결과, MTBSAF는 다음과 같이 산출 되었다.

$$MTBSAF_i = \frac{1}{\lambda_i} \Rightarrow \frac{1}{\lambda_{On-Board\ Equipment}} = \frac{1}{8.85E-6}$$
$$= 1.13E+05Hr$$

2.4.2 가용도 분석

차상신호설비의 서비스 가용도(SA) 분석은 위에서 분석된 MTBSAF와 MTTR 및 물류지연시간(LDT)과 행정소요시간(ADT)을 포함한 MDT를 근거로 분석한다.

식 5에 의하여 MDT 산출은 MTTR 및 LDT 및 ADT를 근거로 다음과 같이 산출된다.

$$MDT = MTTR + (LDT + ADT) = 1.00 + 0.33$$
$$= 1.33Hr$$

여기서 LRU수준에서의 현장교체가능시간은 최대 1시간 이하로 LDT 및 ADT는 없는 것으로 가정하였다. 즉, $MDT \cong MTTR$ 로 가정하였다.

결론적으로 식 8에 의하여 차상신호설비 서비스 가용도는 다음과 같이 산출된다.

$$SA(\%) = \frac{MTBSAF}{MTBSAF + MDT} \times 100\%$$
$$= \frac{1.13E05}{1.13E05 + 1.08} \times 100\% = 99.9990\%$$

2.4.3 차상신호설비 RAM 분석 결과

위의 신뢰도 분석 결과 및 유지보수도 가정사항을 토대로 분석한 차상신호설비 RAM 분석 결과는 다음 표 1과 같이 산출되었다.

Table 1 RAM analysis of On-board signaling equipment

Items	MTBSAF (hr)	MTTR (hr)	MDT (hr)	Service Availability (%)
On-board equipment	1.13E+05	1	1.33	99.9990

2.5 지상신호설비 RAM 분석

지상신호설비의 RAM 분석은 지상ATP/ATO장치, 전자연동장치와 관제설비를 포함한 각 구성 요소의 고장률을 기반(유사 시스템 데이터 및 예측데이터 등)으로 한 MTBSAF 분석과 유지보수도 가정을 통한 MTTR 및 MDT 분석 결과에 따른 서비스 가용도 분석 등의 절차로 산출하였다.

2.5.1 신뢰도 분석

지상신호설비의 신뢰도 블록도는 그림 3과 같다. 신뢰도 블록도는 전체 구성요소 가운데 서비스에 영향을 미치는 구성 요소만으로 작성되었다.

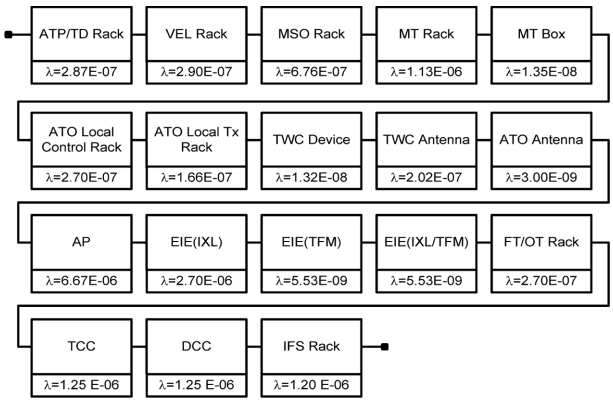


Fig. 3 RBD of train wayside signaling equipment

위 그림 3의 지상신호설비 신뢰도 블록도를 토대로 지상신호설비 전체의 고장률은 다음과 같이 산출되었다.

$$\lambda_{\text{선로변장치}} = 11\lambda_{\text{ATP/TD랙}} + 3\lambda_{\text{VEL랙}} + 3\lambda_{\text{MSO랙}} + 16\lambda_{\text{TWC장치}} + 16\lambda_{\text{TWC Ant}} + 50\lambda_{\text{ATO Ant}} + \lambda_{\text{Total of AP}} + 2\lambda_{\text{EIE(IXL)}} + 4\lambda_{\text{EIE(TFM)}} + 12\lambda_{\text{FT/OT Rack}} + \lambda_{\text{TCC}} + \lambda_{\text{DCC}} + \lambda_{\text{IFS Rack}}$$
$$= 3.13\text{E} - 06 + 8.70\text{E} - 07 + 2.03\text{E} - 06 + 3.40\text{E} - 06 + 2.33\text{E} - 06 + 1.89\text{E} - 06 + 1.33\text{E} - 6 + 2.12\text{E} - 07 + 3.24\text{E} - 06 + \lambda_{\text{Total of AP}} + 5.40\text{E} - 06 + 2.21\text{E} - 08$$

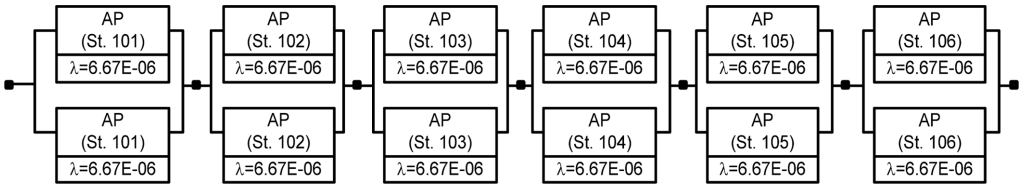


Fig. 4 RBD of Access Point installation in station

위의 수식에서 전체 AP, TCC, DCC 및 IFS에 대한 고장률 계산은 각각의 장치에 대한 분석 결과에 의한다.

2.5.2 Access Point 신뢰도 분석

각 역사, 차량기지 및 역간 선로변에 설치되어 차량과 통신하는 AP는 그림 4와 같이 3가지 유형으로 신뢰도 블록도가 구성된다. 즉, 각 역사, 차량기지 및 선로 변에 이중계 원리를 적용하여 AP를 설치하여 차량과의 통신상의 데이터 손실이 없도록 구성하였다. 그림 4의 1개 역사 내 이중계 구조의 AP 고장률 값은 식 4에 의해 다음과 같이 산출되며, 타 역사에서의 고장률 데이터도 동일하게 적용된다. 단, 이때 MTTR은 1로 가정하였다.

$$\lambda_{\text{Redundancy of AP(St 101)}} = 2 \times (\lambda_{\text{AP(St 101)}})^2 = 8.90\text{E} - 11$$

위 결과값을 타 역사 AP에 동일하게 적용하면 6개 역사 전체에 대한 AP고장률은 다음과 같이 산출된다.

$$\lambda_{\text{AllStation}} = 6 \times \lambda_{\text{Redundancy of AP(St. 101)}} = 5.34\text{E} - 10$$

차량기지 AP의 고장률은 식 2에 따라 선로변 AP 고장률은 식 4에 의해 다음과 같이 산출된다

$$\lambda_{\text{Depot}} = 3 \times (\lambda_{\text{Teackside}})^2 \times \text{MTTR} = 2.67\text{E} - 10$$
$$\lambda_{\text{Teackside}} = 7 \times 2 \times (\lambda_{\text{Teackside}})^2 \times \text{MTTR} = 6.23\text{E} - 10$$

위에서 산출된 신뢰도 블록도 및 수식에 의해 각 역사, 차량기지 및 선로변에 설치되는 Access Point에 대한 전체 고장률은 다음과 같이 산출된다.

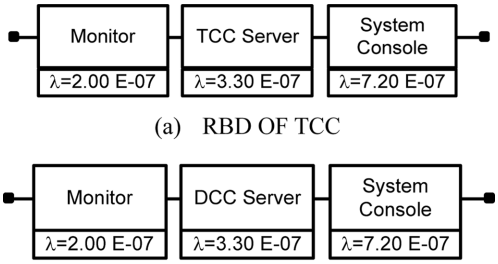
$$\lambda_{\text{Total of AP}} = \lambda_{\text{AllStation}} + \lambda_{\text{Depot}} + \lambda_{\text{Trackside}}$$
$$= 5.34\text{E} - 10 + 2.67\text{E} - 10 + 6.23\text{E} - 10$$
$$= 133\text{E} - 09$$

2.5.3 TCC 및 DCC 신뢰도 분석

Train Control Computer와 Data Control Computer는 모니터, 서버 및 컴퓨터 장치(콘솔: console)로 이루어져 있으며 신뢰도 블록도 구성은 다음 그림 5와 같다.

위의 신뢰도 블록도에 따라 TCC 및 DCC 고장률은 다음과 같이 구해진다.

$$\lambda_{\text{TCC}} = \lambda_{\text{DCC}} + \lambda_{\text{모니터}} + \lambda_{\text{TCC or CDD 서버}} + \lambda_{\text{System콘솔}}$$
$$= 2.00\text{E} - 07 + 3.30\text{E} - 07 + 7.20\text{E} - 07$$
$$= 12.5\text{E} - 06$$



(a) RBD OF TCC

(b) RBD OF DCC

Fig. 5 RBD of TCC & DCC

2.5.4 Inter Face System 신뢰도 분석

전자연동장치와 관제설비와의 인터페이스를 담당하는 IFS의 신뢰도 블록도는 그림 6과 같다.

그림 6의 신뢰도 블록도와 식 4에 따라 IFS의 고장률은 다음과 같이 산출된다.

$$\lambda_{\text{IFS}} = \lambda_{\text{모니터}} + \lambda_{\text{KVM모듈}} + 2\text{x}(\lambda_{\text{IFS서버}})^2 + 2\text{x}(\lambda_{\text{스위칭허브}})^2$$
$$= 2.00\text{E} - 07 + 1.00\text{E} - 06 + 2.18\text{E} - 13 + 4.21\text{E} - 09$$
$$= 1.20\text{E} - 06$$

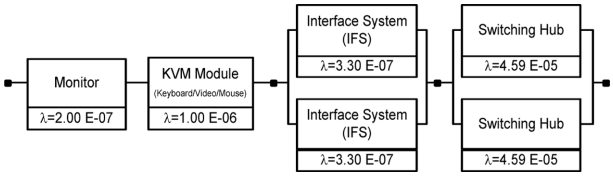


Fig 6 RBD of Inter face system

2.5.5 유지보수도 분석

유지보수도 분석은 현장교체가능장치(LRU)수준에서 수리 또는 교체활동을 통한 운행정지시간이 1시간을 초과하지 않는 것으로 가정하였다.

2.5.6 가용도 분석

지상신호설비의 서비스 가용도(SA) 분석은 위에서 분석된 MTBSAF와 MTTR 및 물류지원시간과 행정소요시간을 포함한 MDT를 근거로 분석하였다. 식 5에 근거하여 MDT 산출은 MTTR 및 LDT 및 ADT를 근거로 다음과 같이 산출되었다.

$$\text{MDT} = \text{MTTR} + (\text{LDT} + \text{ADT}) = 1.00 + 0.33$$
$$= 1.33 \text{ Hr}$$

결론적으로, 수식 8을 적용한 지상신호설비 서비스 가용도는 다음과 같이 산출되었다.

$$SA(\%) = \frac{MTBSAF}{MTBSAF+MDF} \times 100\%$$
$$= \frac{2.31E04}{2.31E04+1.33} \times 100\% = 99.9942\%$$

2.5.7 지상신호설비 RAM 분석 결과

지상신호설비의 고장률은 수식상에 전체 AP, TCC, DCC 및 IFS 분석값을 적용함으로써 다음과 같은 결과를 얻을 수 있다.

$$\lambda_{\text{Wayside Equip}} = 4.33E - 05$$

위의 신뢰도 분석결과 및 유지보수도 가정사항에 의한 지상신호설비 RAM 분석 결과는 다음 표 2와 같다.

Table 2 RAM analysis of train wayside signaling equipment

Items	MTBSAF (hr)	MTTR (hr)	MDT (hr)	Service Availability (%)
Wayside Equipment	2.31E+04	1	1.33	99.9942

2.6 안전성(Safety) 분석

열차제어시스템에 대한 정성적인 안전성 목표는 IEC 62278에서 제시한 위험도 등급 기준을 적용하여, EN 50129에서 제시하는 SIL-4 기준에 부합함을 입증하도록 하였으며, ALARP의 원리에 따라 허용 가능한 위험도 등급에 부합하도록 저감대책을 수립하는 것으로 검토하였다. 표 3, 4, 5는 자기부상 열차 열차제어시스템 Safety 분석에 사용되는 위험도 발생빈도, 위험요인 심각도, 위험도 평가 기준으로 제시한 사항이다[3-5,11,12].

2.6.1 안전 무결성 수준 결정 방법론

안전성 요구사항을 토대로 안전성 분석을 통한 전체 열차제어시스템 및 서브시스템의 안전 무결성 수준 결정은 표6과 같으며, 표 4의 방법론을 토대로 하였다.

2.6.2 HAZOP (HAZard and OPerability Study)

HAZOP은 위험요인 규명을 위해 주로 활용되는 brain storming 방식의 분석 방법이다. 이는 설계에 대한 체계적이고 창의적인 의견 도출 및 설계 경험이 풍부한 전문 엔지니어들의 기술사항을 바탕으로 수행된다.

HAZOP은 시스템 수명주기 동안 위험요인 도출을 위한 각 단계별로 수행되는 분석방법인 예비 위험요인 분석(PHA), 시스템 및 서브시스템 위험요인 분석(SHA/SSHA), 인터페

Table 3 Probability of hazards

분 류	위험 사건 발생빈도	발생빈도(연간)
A 빈번한	자주 발생할 것 같은. 지속적으로 발생	빈도 ≥ 100
B 있음직한	수 차례 발생. 자주 발생할 것으로 예측	100 > 빈도 ≥ 1
C 때때로	수 차례 발생할 것 같은	1 > 빈도 ≥ 10^{-2}
D 아주 적은	수명주기 동안 가끔 발생할 것 같은	10^{-2} > 빈도 ≥ 10^{-4}
E 희박한	가능하나 발생하지 않을 것 같은	10^{-4} > 빈도 ≥ 10^{-6}
F 가능성이 없는	극히 발생하지 않을 것 같은	10^{-6} > 빈도

]

Table 4 Severity of Hazards

심각도 수준	사람 및 환경에 미치는 결과	사망자수
4 치명적인	다수의 사상 및 환경에 대한 중대한 손상	다수 사망(1명 초과)
3 중대한	단수의 사상 및 환경에 대한 상당한 영향	1명 사망 혹은 다수 중상
2 제한적	경상 및 환경에 대한 상당한 위협	1명 중상
1 경미한	경미한 부상의 가능성	다수 경상

Table 5 Risk matrix

심각도 / 발생빈도		1	2	3	4
		경미한	제한적	중대한	치명적인
A	빈번한	Undesirable	Unacceptable	Unacceptable	Unacceptable
B	있음직한	Tolerable	Undesirable	Unacceptable	Unacceptable
C	때때로	Tolerable	Undesirable	Undesirable	Unacceptable
D	아주 적은	Acceptable	Tolerable	Undesirable	Undesirable
E	희박한	Acceptable	Acceptable	Tolerable	Tolerable
F	가능성이 없는	Acceptable	Acceptable	Acceptable	Acceptable

Table 6 Safety integrity level theory of train control system

심각도수준	잠재사고(PA)의 발생빈도	SIL
4 및 3	고장 및 위험상황이 잠재사고발생에 직접적인 영향을 초래함.	4
	잠재사고 발생을 초래하는 기능고장 및 위험상황 발생빈도가 높음	2
2	고장 및 위험상황이 잠재사고발생에 직접적인 영향을 초래함.	2
	잠재사고 발생을 초래하는 기능고장 및 위험상황 발생빈도가 낮음	0
1	고장 및 위험상황이 잠재사고발생에 직접적인 영향을 주지 않음.	0

Table 7 Guideword of HAZOP

Guide word	description	Remark
NO/Not	설계의도에 대한 출력이 없음	
More	설계의도보다 출력이 정량적으로 증가	
Less	설계의도보다 출력이 정량적으로 감소	
As Well As	설계의도보다 출력이 정성적으로 증가	
Part Of	설계의도보다 출력이 정성적으로 감소	
Reverse	설계의도와는 논리적으로 반대되는 출력이 제공	
Other Than	설계의도와는 전혀 다른 출력이 제공	
Too Late	설계의도보다 출력이 과도하게 느림	
Too Fast	설계의도보다 출력이 과도하게 빠름	
Too Much	설계의도보다 출력이 과도하게 많음	
Too Little	설계의도보다 출력이 과도하게 적음	

이스 위험요인 분석(IHA), 운영 및 지원상의 위험요인 분석(O&SHA) 등 다양한 분석 방법에 적용된다.

본 고에서는 예비 위험요인 분석(PHA)을 위하여 HAZOP 방법론을 적용하였으며 다음 표 7과 같은 가이드워드(Guideword)를 사용하여 설계의도에서 벗어난 예외항목들을 도출함으로써, 위험요인을 규명하였다.

2.6.3 위험요인 발생빈도와 안전 무결성 수준과의 관계

위험요인 발생빈도에 대해 년간 발생빈도 분류를 참고하여 표 8과 같은 안전 무결성 수준 Matrix를 나타내었다.

2.6.4 안전 무결성 수준 결정

안전 무결성 수준 결정 방법론 및 HAZOP 등을 시행하여 위험도 발생빈도, 위험요인 심각도, 위험도 평가 기준에 따라 자기부상열차제어시스템 및 서브 시스템의 주요 기능에 따른 안전 무결성 수준(SIL)에 대하여 표 9, 10과 같이 분류하였다.

2.6.5 안전 무결성 수준의 검증

기능별 안전 무결성 수준에 대해서 EN 50129에 언급된 기준으로 정량적인 안전 무결성 수준의 적합성을 검증한다. 표

Table. 8 SIL of risk matrix

심각도 / 발생빈도		1	2	3	4
		경미한	제한적	중대한	치명적
F	가능성 없는	SIL 0	SIL 0	SIL 2	SIL 2
E	희박한	SIL 0	SIL 0	SIL 2	SIL 2
D	아주 적은	SIL 0	SIL 0	SIL 2	SIL 2
C	때때로	SIL 0	SIL 2	SIL 4	SIL 4
B	있음직한	SIL 0	SIL 2	SIL 4	SIL 4
A	빈번한	SIL 0	SIL 2	SIL 4	SIL 4

Table. 9 SIL of Train control system hardware

No.	Items	SIL	Remark
1	ATP 차상장치	4	
2	ATP 지상장치	4	
3	ATO 차상장치	2	
4	ATO 지상장치	2	
5	ATS 장치	2	

Table 10 SIL of Train control system software

No.	Element list	SIL	Remark
1	ATP 차상설비 소프트웨어	4	
2	ATP 지상설비 소프트웨어	4	
3	ATO 차상설비 소프트웨어	2	
4	ATO 지상설비 소프트웨어	2	
5	ATS 소프트웨어	2	

Table 11 Table of safety integrity level [EN50129]

THR (/Hr 및 /기능)	SIL	THR(/10^9Hr) 기준
10^{-9} THR < 10^{-8}	4	1 ≤ THR < 10
10^{-8} THR < 10^{-7}	3	10 ≤ THR < 100
10^{-7} THR < 10^{-6}	2	100 ≤ THR < 1,000
10^{-6} THR < 10^{-5}	1	1,000 ≤ THR < 10,000

11의 Tolerable Hazard Rate (/10^9Hr) 기준은 백만시간(10^9시간)을 기준으로 했을 때 허용 가능한 위험요인 발생 건수에 대해서 언급한 것이다.

2.7 결합 트리 분석(Fault Tree Analysis)

결함 트리 분석은 시스템의 기능 고장으로 인해 위험 요인을 초래하는 근본 원인을 규명하는 접근방법으로 하향식 접근방법(Top-Down Approach 또는 Deductive Method)에 따른 결함 트리 기법을 활용하여 분석한다. 결함 트리 분석(FTA)을 위해서 GATE(유형 1), EVENT(유형 2), 설명(유형 3)의 3가지 기호들이 사용된다. 그림 7, 8, 9는 주요 기능에 대한 Fault Tree Analysis 결과를 보여주고 있다.

원인분석을 위한 결함 트리 분석을 위하여 “자동 열차보

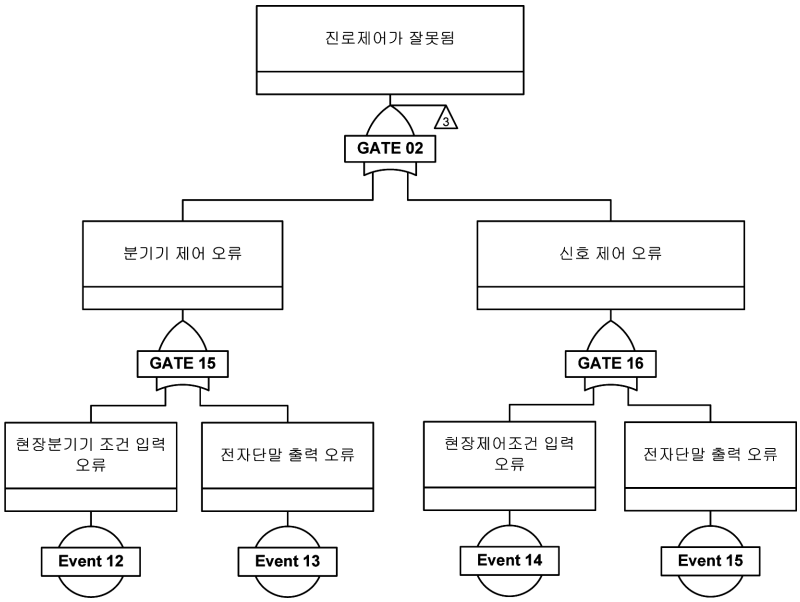


Fig. 7 FTA of route control

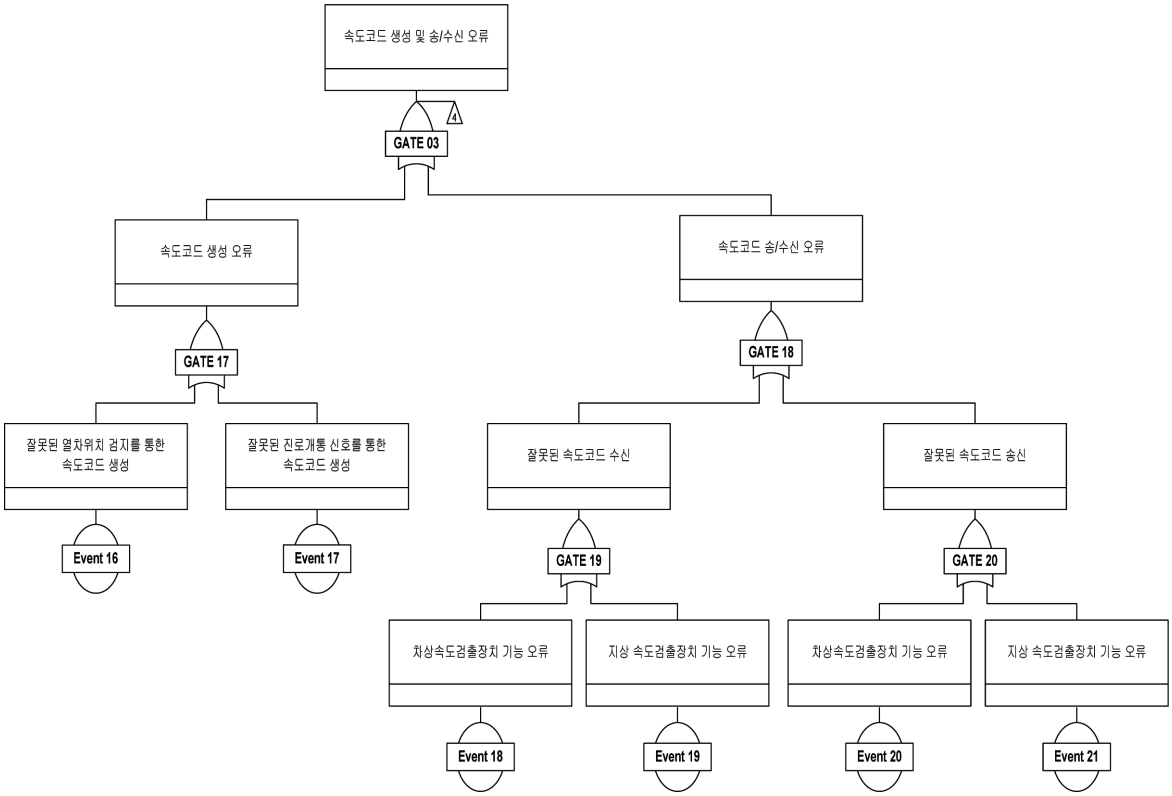


Fig. 8 FTA of speed code generation

호(ATP)기능 구현이 잘못됨"을 정상상태로 하여 분석을 한 결과 27개의 기본 이벤트가 규명되었으며, 각각의 이벤트에 대해 Top Event를 초래하게 되는 Cut Set 을 규명하기 위해 최소 Cut Set (MCS)를 규명하였다. 추가로 Event 5, 6, 7, 8, 9, 10, 11은 동일한 이벤트로 인해 다른 고장을 초래하는 공통원인 고장으로 규명되었다. 본 결함 트리 분석을 통하여 규명된 27개의 공통원인고장은 Hazard Log에 관리되어 현장설치시험 및 시운전 단계별로 각 이벤트에 대하여 시스템상에서 보호되도록 구현되었는지 검증되고 관리될 것이다.

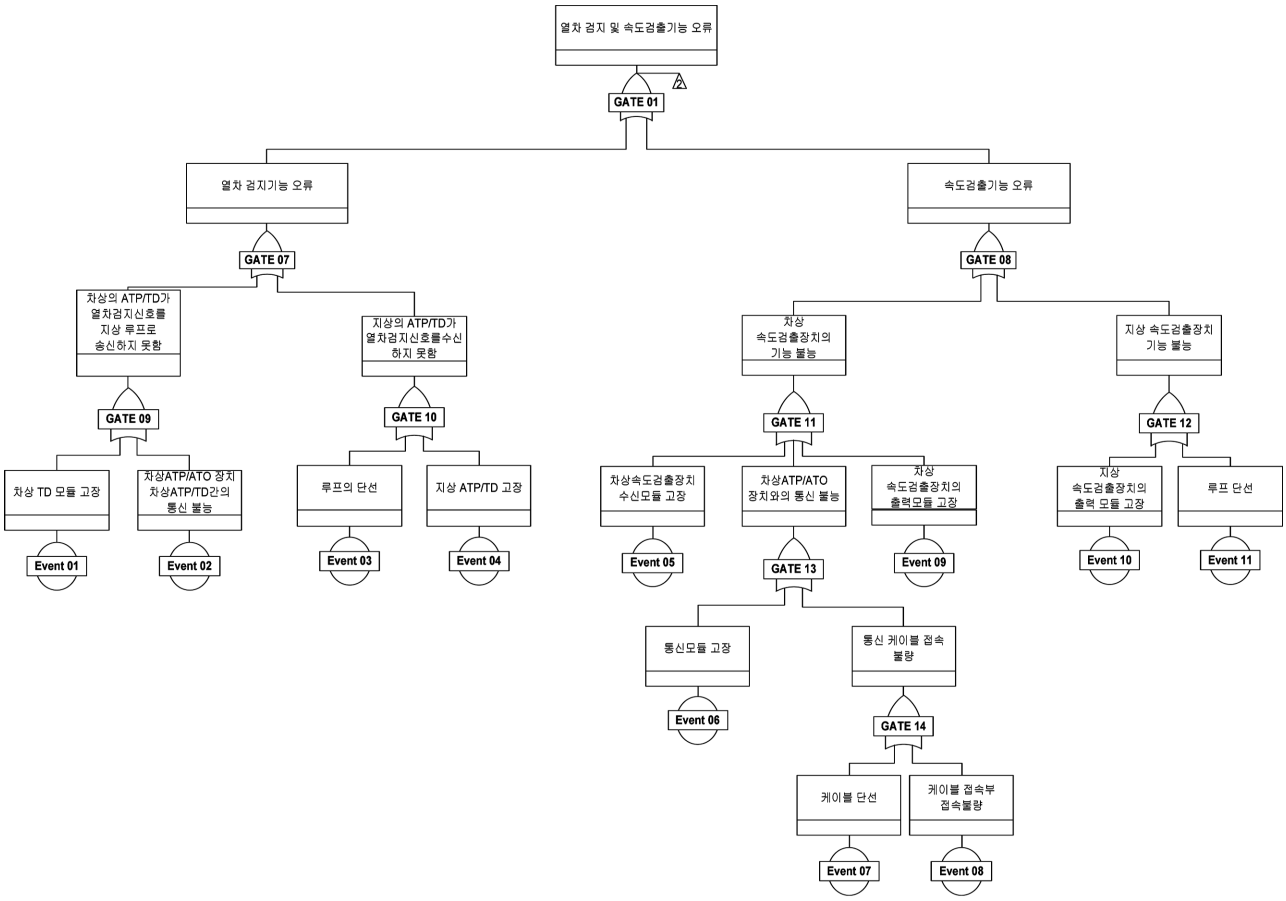


Fig. 9 FTA of Train speed and position detection

Table 12 Event of fault tree analysis

이벤트	설 명	MCS & CCF
Event 01	차상 TD 모듈 고장	GATE09, GATE07, GATE01
Event 02	차상ATP/ATO-ATP/TD 간 통신 불능	GATE09, GATE07, GATE01
Event 03	루프의 단선	GATE10, GATE07, GATE01
Event 04	지상 ATP/TD 고장	GATE10, GATE07, GATE01
Event 05	차상속도검출장치 수신모듈 고장	GATE11, GATE08, GATE01/ GATE21, GATE06
Event 06	통신모듈 고장	GATE13, GATE11, GATE08, GATE01/GATE12, GATE21, GATE06
Event 07	케이블 단선	GATE14, GATE13, GATE11, GATE08, GATE01/GATE13, GATE12, GATE21, GATE06
Event 08	케이블 접속부 접속불량	GATE14, GATE13, GATE11, GATE08, GATE01/GATE13, GATE12, GATE21, GATE06
Event 09	차상 속도검출장치의 출력모듈 고장	GATE11, GATE08, GATE01/GATE21, GATE06
Event 10	지상 속도검출장치의 출력모듈 고장	GATE12, GATE08, GATE01/GATE22, GATE06
Event 11	루프 단선	GATE12, GATE08, GATE01 / GATE22, GATE06
Event 12	현장분기기 조건 입력 오류	GATE15, GATE02
Event 13	전자단말 출력 오류	GATE15, GATE02
Event 14	현장제어조건 입력 오류	GATE16, GATE02
Event 15	전자단말 출력 오류	GATE16, GATE02

Table 12 Event of fault tree analysis

이벤트	설 명	MCS & CCF
Event 16	잘못된 열차위치 검지를 통한 속도코드 생성	GATE17, GATE03
Event 17	잘못된 진로개통 신호를 통한 속도코드 생성	GATE17, GATE
Event 18	차상속도검출장치 기능 오류	GATE19, GATE18, GATE03
Event 19	지상 속도검출장치 기능 오류	GATE19, GATE18, GATE03
Event 20	차상속도검출장치 기능 오류	GATE20, GATE18, GATE03
Event 21	지상 속도검출장치 기능 오류	GATE20, GATE18, GATE03
Event 22	열차제동장치 고장	GATE04
Event 23	케이블 단락 오류	GATE04
Event 24	차상 ATP/ATO 장치 출력 오류	GATE04
Event 25	차상ATP/ATO 제어기에 잘못된 출입문 개방방향 명령 송신	GATE05
Event 26	차상ATP/ATO제어기가 잘못된 출입문 방향 개방	GATE05
Event 27	차량 출입문 고장	GATE05

3. 결 론

이상과 같이 최상위 레벨(Top Event)에서 전체 시스템에 대한 RAMS 분석 결과 도시형자기부상열차 열차제어시스템이 요구하는 목표값을 달성함을 알 수 가 있었다. 차상신호설비의 서비스 가용도(SA) 분석은 위에서 분석된 MTBSAF와 MTTR 및 물류지원시간과 행정소요시간을 포함한 MDT를 근거로 분석한 결과 MTBSAF는 1.13E+05로 산출되었고 서비스 가용도는 99.9990%로 산출되었다.

지상신호설비의 서비스 가용도(SA) 분석은 위에서 분석된 MTBSAF와 MTTR 및 물류지원시간과 행정소요시간을 포함한 MDT를 근거로 분석한 결과 MTBSAF는 2.31E+04로 산출되었고 서비스 가용도는 99.9942% 로 산출되었다.

결함 트리 분석을 위하여 “자동 열차보호(ATP)기능 구현이 잘못됨”을 정상상태로 하여 분석을 한 결과 27개의 기본 이벤트가 규명되었으며, 각각의 이벤트에 대해 Top Event를 초래하게 되는 컷ôV을 규명하기 위해 최소 컷ôV(MCS)를 규명하였다.

마지막으로 안전도 분석 결과에 따라 열차제어 시스템 전체가 안전 무결성 등급(SIL) 4를 만족하도록 설계되었으며, 각 장치에 따라 적절하게 SIL(안전 무결성 등급) 할당이 되었음을 분석하였다.

본 논문에서 제시한 설계단계에서 분석 산출된 RAM 목표 값은 2012년 09월부터 시범노선에서 시작되는 시운전 및 영업운행을 통하여 입증될 것이며, 독립된 안전성 평가기관(ISA으로부터 안전 무결성 등급 SIL-4에 대한 평가 및 인증이 이루어질 것이다.

후 기

본 논문은 국토해양부(건설교통기술 평가원) 에서 주관하고 있는 ‘도시형 자기부상열차 실용화사업’ 시범노선 구축(3-0)과제 연구비 지원으로 수행되었 습니다. 도움주신 여러분께 감사 드립니다.

참고문헌

[1] Request For Proposal, ‘Bid of Urban Maglev Demo- nstration line Train control system (2009.2) Korea Rail Network Authority.

[2] Approved document & drawing ‘of Urban Maglev Demonstration line Train control system (2009.2) Korea Rail Network Authority.

[3] ‘Urban Maglev program subsystem RAMS requirement (2010.10) Doc. No.M1201-SE+RM-101-0008, Rev. 01, KIMM.

[4] IEC62425, ‘Railway applications-Communication, Signalling and Processing systems-Safety related electronic systems for Signalling (2007), IEC.

[5] IEC62278, ‘Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety(RAMS) (1999) IEC

[6] IEC62279, ‘Railway Applications - Communications, signaling and processing systems. Software for railway control and protection systems (2002) British Standard Institute.

[7] MIL-HDBK-217F Notice 2, ‘Reliability prediction of electronic devices (1995) Department of Defense of the U.S.A

[8] MIL-HDBK-472, ‘Maintainability prediction of electronic devices (1996) Department of Defense of the U.S.A

[9] Reliability Toolkit: commercial Practices Edition, A Practical Guide for commercial Products and Military Systems Under Acquisition Reform (1996) RiAC

[10] Joel Manary, Operational Availability Hand book (2004) RiAC, 2004

[11] J.K Kim, D.k Shin, K.S Lee (2006) A Study on the Safety Plan for a Train Control System, *Journal of the Korean Society for Railway*, 9(3), pp. 249-338.

[12] K.D. Shin, J.W Lee (2010) Software Quality Assurance Activities of Automatic Train Control System to meet Requirements of the IEC 62279 Standard, *Journal of the Korean Society for Railway*, 13(4), pp. 357-469.

부 록

약어 정의

RAMS : Reliability, Availability, Maintainability, Safety
MTBSAF : Mean Time Between Service Affecting Failure
SIL : Safety Integrity Level
FMECA : Failure Mode, Effects and Criticality Analysis
PHA : Preliminary Hazard Analysis
SHA : System Hazard Analysis
SSHA : Subsystem Hazard Analysis
FTA : Fault Tree Analysis
MTTR : Mean Time To Repair
LDT : Logistic Delay Time
ADT : Administrative Delay Time
MDT : Mean Down Time
SA : Service Availability
FR : Failure Rate
FPMH : Failure Per Million Hour
RBD : Reliability Block Diagram
MCS : Minimal Cut Set
CCF : Common Cause Failure

접수일(2011년 7월 1일), 수정일(2011년 10월 28일),
게재확정일(2011년 11월 7일)