A Study on the Application of RAMS for Signalling System (Maglev)

No. 101

Hak Sun Yun, Ryou Sung Kyun , and In Jae Lee
Korea Rail Network Authority, Maglev Railway Project Division, Room No,303, Youngmin Bldg., 120, Joongangro, Jung Gu, Daejeon-si 301-805, KOREA

kamayun@hanmail.net, skryou1@hanmail.net, injae@krnetwork.or.kr

Key Seo Lee
Kwangwoon University, Dept of I&C Engineering, 447-1, Wolgye-Dong, Nowon-Gu, Seoul-si, 139-701, KOREA
kslee@kw.ac.kr

ABSTRACT: This paper presents a RAMS to be applied to the development of the Urban Maglev Train Signalling System in Korea. The RAMS that can be applied to the life cycle of a Signaling 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.

1 INTRODUCTION

1.1 Background

MAGLEV project supervised by the Ministry of Land Transport and Maritime affairs and has been commenced in December 2006 and continued to November 2012 for 6 years with the aim of revenue service.
Test line for this project will be constructed in Youngjong-do and Korea Rail Network Authority has been charged with design and construction for all of railway systems except rolling stock. It is shown with route map in Figure 1.

1.2 Test line

.Location : Youngjong-do
.Route length : 6.113Km(Mainline-double track)
0.750Km(Lead in track-single track)
.Station:6(Island platform:2, Opposite platform:4)
.Depot : 1

Figure 1. Route map of Maglev in youngjongdo, korea.

1.3 Basic specification of signalling system

.Operation Type : ATO Driverless Operation
.Signalling Type : ATP
.Minimum Headway : 90 seconds

1.4 ATP

.Automatic Train Protection
.Train Detection in main line

.Calculation of train speed and transmission track condition data to secure train separation

1.5 ATO

.Automatic Train Operation
.Automatic operation with stable train speed
.Automatic train movement and stopping between stations
.Automatic door operation

1.6 ATS

.Automatic Train Supervision
.Monitoring, control and management of train movement

1.7 Operating mode

.Driverless Operating Mode : ATO without intervention of driver/crew
.Automatic Operating Mode : ATO with intervention of drive/crew (Push starting button whenever departure)
.Manual Operating Mode : Manual operation by ATP
.Emergency Operating Mode: Fully manual operation on emergency (Manual operation without speed limit depending on only driver's attention)
.Shunting Mode: Operation within depot under the restricted speed (Under 15Km/h)

1.8 System configuration

Basic configuration of signalling system is like following in Figure 2.

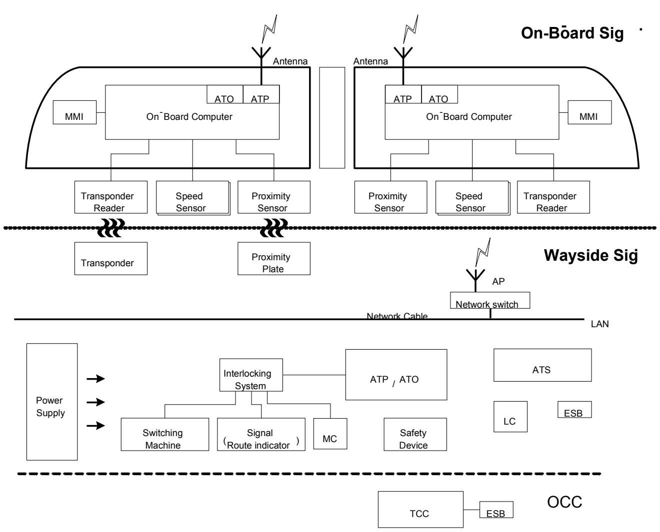

Figure 2. System configuration.

Total signalling system is configured with On-Board System and Wayside System.
On-Board System is equipped on the train and Wayside System is composed with all of sub-system will be installed on the wayside including six stations and 1 depot.

2 METHODOLOGY

2.1 LBS

LBS is the method to breakdown the applicable system into unit with the lowest level to analyze safety and reliability of system systematically.
The result of LBS is used to identify the applicable system for RAMS analysis (eq. FMECA, SHA and so on) with the index such as system, sub-system and components, and MTBF or MTTR of each item are evaluated from the system level identified in LBS.
In this project, signalling system was assigned as system level, on-board system and wayside system as sub-system level, and main component (eq. interlocking) as sub-assembly.

2.2 SHA

System Hazard Analysis(SHA) is a semi-quantitative analysis method performed following PHA and to identify all potential hazards in the system level.
SHA for signalling system of Urban Transit MAGLEV was performed with following aims:
.Identify initial hazards and accidents during the beginning of design phase
.Identify the hazards concerning system
.Identify the hazards concerning sub-system
.Rank the risk per each hazards based on severity and frequency of them
.Establish the safeguard to eliminate the concerned hazard or reduce the risk level of them to acceptable level
To identify all potential hazards in the system level, SHA was performed on the function of main sub-system(eq. On-Board Computer, Interlocking system , wayside ATP/ATO, ATS and TCC) and also on the operating mode such as normal, degraded and emergency.
Following causes are considered to identify the hazards as much as possible:
.Components with the potential hazards
.Interfaces with the various system
.Environmental factor including operating condition
.Various operation mode such as normal, maintenance or emergency
.Malfunction of system

2.3 HAZOP

HAZOP study is the type of brainstorming method to identify hazards.
Multi-disciplinary team shall perform HAZOP study and Systematic and creative opinions shall be evaluated through it.
It could be applied to PHA, SHA and IHA performed per each phase over system life cycle.
In this project, HAZOP study was applied to perform PHA identifying deviations from intended design using guideword.
General guideword for HAZOP study is like below:
.NO/NOT: No par of the intention is achieved
.MORE: Some quantitative increase over what was intended
.LESS: Some quantitative decrease over what was intended
.AS WELL AS: Some qualitative increase over what was intended
.PART OF: Some qualitative decrease over intent
.REVERSE: Logical opposite of intention
.OTHER THAN: Something completely different

2.4 Risk matrix

Risk matrix normally has been used for evaluating the consequences of each hazard semi-qualitatively.
In this project, risk matrix for safety analysis was used with general one based on EN 50126.
All potential hazard from PHA were ranked by the risk matrix to assess whether risk of hazards were reduced to acceptable level.

Table 1. Frequency of Occurrence of Hazardous Events

Category	Description	Hazard Occurrence Frequency (Per annum)
A. Frequent	Likely to occur frequently. The hazard will be continually experienced.	≥100
B. Probable	Will occur several times. The hazard can be expected to occur often.	≥1-<100
C. Occasional	Likely to occur several time. The hazard can be expected to occur several times.	≥10-2-<1
D. Remote	Likely to occur sometime in the system life cycle. The hazard can reasonably expected to occur.	≥10-4-<10-2
E. Improbable	Unlikely to occur but possible. It can be assumed that the hazard may exceptionally occur.	≥10-6-<10-4
F. Incredible	Extremely unlikely to occur. It can be assumed that the hazard may not occur.	<10-6

Table 2. Hazard Severity Level

Severity Level	Consequence to Persons or Environment	System Effect
1. Catastrophic	Fatalities and/or multiple sever injures and/or major damage to the environment.	
2. Critical	Single fatality and/or sever injury and/or significant damage to the environment	Loss of major system
3. Marginal	Minor injury and/or significant threat to the environment.	Severe system(s) Damage
4.Insignificant	Possible minor injury.	Minor system damage

Table 3. Frequency-Consequence Matrix

Frequency	Risk Levels			
A. Frequent	Undesirable	Intolerable	Intolerable	Intolerable
B. Probable	Tolerable	Undesirable	Intolerable	Intolerable
C. Occasional	Tolerable	Undesirable	Undesirable	Intolerable
D. Remote	Negligible	Tolerable	Undesirable	Undesirable
E. Improbable	Negligible	Negligible	Tolerable	Tolerable
F. Incredible	Negligible	Negligible	Negligible	Negligible
	4.Insignificant	3.Marginal	2.Critical	1.Catastrophic
	Severity Levels of Hazard Consequence			

Table 4. Qualitative Risk Categories

Risk Classification	Action
Intolerable	Risk reduction must be achieved or risk eliminated.
Undesirable	High priority to be given to reducing the risk to As Low As Reasonably Practicable (ALARP). Demonstration to be provided that the risk has been reduced to a level that is ALARP.
Tolerable	Risk has been defined as acceptable by technical review. Demonstration to be provided that the risk has been reduced to a level that is ALARP. Lower priority than risks classified as “Undesirable”).
Negligible	No further risk reduction normally required. Risks need to be reviewed on a periodic basis or subsequent to any accidents, incidents or near misses.

2.5 RAM Target & Apportionment

RAM target can be developed with stochastic method such as Chi-square through failure data analysis by using the existing failure data.
But, RAM target was developed by using RAM target and apportionment rate of similar project in other country because RAM target or failure data for signalling system were not in korea.
Reliability function is assumed with exponential function and failure rate for each sub-system is calculated by using RBD.

2.6 Reliability Prediction

a Reliability function of exponential distribution

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

λ_{sys} : System Failure Rate, t : Time

b Failure Rate of system with series configuration
$\lambda_S = \lambda_1 + \lambda_2 + \lambda_3 + ... + \lambda_N$
N : Number of system with series configuration

c Failure Rate of system with parallel configuration

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

N : Number of active on-line units
q : Number of on-line active units which are allowed to fail without system failure

2.7 Maintainability Prediction

Maintainability is the probability that a given maintenance , for an item under given conditions of use can be carried out within a stated time interval when the maintenance is performed under stated conditions and using stated procedures and resources. Normally, MTTR is used for terms and basic equation for maintainability Prediction is like following:

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

MTTR: Mean Time To Repair system
λ_i: Failure Rate of i_{th} Sub-system
$MTTR_i$: Mean Time To repair Sub-system
N: Number of Sub-system

2.8 Availability Prediction

Availability is calculated by using basic equation on EN 50126 as internal standard of RAMS and basically by the combination of MTBF and MTTR.

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

MTBF: Mean Time Between Failure
MTTR: System Maintainability

2.9 Chi-Square

Chi-square analysis provides a means of estimating, within a given confidence interval, the failure rate, where only limited data about the number of failures is available.

Basic equation is following:

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

θ : the estimated mean time between failure
T : the time period for which data is available
α : confidential interval
r : number of failure

Following equation is evaluated with T=n(number of degrees freedom)×h(testing time):

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

Number of allowable failure can be determined by setting confidential interval and number of failure for each sub-system, where failure estimated mean time between failure based on confidential interval and no. of failure as minimum value

3 ANALYSIS RESULT

3.1 Logistic Breakdown Structure

Sub-system can be classified by On-Board Signal System and Wayside Signal System and details are following.

3.2 LBS of On-Board Signalling system

On-Board Signalling System will be equipped on train and is composed with 6 sub-systems. On-Board Computer of sub-systems is classified with ATP and ATO equipment, and has redundant configuration.
Details are following:

Table 5. System Breakdown of On-Board Signalling System

Sub-System	Quantity	Remark
On-Board Computer	1	
ATP	1	
ATO	1	
MMI	1	
Antenna	1	
Transponder Reader	1	
Speed Sensor	2	
Proximity Sensor	1	

3.3 LBS of Wayside Signalling system

Table 6. System Breakdown of Wayside Signalling System

Sub-System	Quantity	Remark
Interlocking System	2	
ATP/ATO(wayside)	2	Redundant
ATS(local)	1	Redundant
TCC	1	Redundant
LC	1	
MC	1	
AP	30	
Transponder	200	Redundant
Terminal Box	30	
Cable	-	
Network Cable	-	
Network Switch	16	
Switch Machine	22	
Route Indicator	21	
Proximity Plate	24	
Power Supply	4	
Emergency Stop Button – Station	6	
Emergency Stop Button – OCC	1	

3.4 RAM Target

3.4.1 Reliability & Maintainability Target

RAM target is achieved by using the data of other project, which is similar with this Intercity MAGLEV project and by considering the result of LBS and design configuration.

a Reliability Target

Reliability Target is using MTBSAF (Mean Time Between Service Affecting Failure) and apportioned by using the apportionment rate of similar project.

Table 7. Service Affecting Failure Rate

Item	Service Affecting Failure Rate	MTBSAF	Apportionment Rate
Signalling System	**66.91×10^{-6}**	**14,944.81**	
On-Board	27.00×10^{-6}	55,555.56	27%
Wayside	48.91×10^{-6}	20,444.52	73%

Reliability Target is using MTBSAF and achieved by considering the result of LBS and design configuration like following:

Table 8. Failure Rate of Sub-System

On-Board		Wayside	
Sub-System	MTBSAF (hour)	Sub-System	MTBSAF (hour)
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 Maintainability Target

Maintainability is assumed with 1 hour because maintainability of sub-system is not provided

3.4.2 Availability Target

Service availability established with over 98% considering number of planned departure and on-time departure.

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

SA: Service Availability
PD: Planned Departure
MD: Missed Departure
UD: Unplanned Departure

Availability target for Intercity MAGLEV was recommended with over 98% considering the equation in EN 50126.

Assumed maintainability is 1 hour by referring MTBSAF suggested above, Availability of Signalling System for Intercity MAGLEV is suggested by

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

$= 99.99\%$
following:

3.5 Result of SHA

3.5.1 Hazard identification

Hazard identification for signalling system of Urban MAGLEV has been performed through 4 PHA meetings with signalling experts from KRNA
using HAZOP study and 98 hazards were identified in this design phase like below:

Table 9. Result of hazard identification

Applicable Sub-system	No. of hazards identified	No. of hazards per initial risk rank			
		Intolerable	Undesirable	Tolerable	Negligible
On-board computer	16	10	6	- -	- -
Interlocking system	10	5	5	- -	- -
Wayside ATP/ATO	15	10	5	-	-
ATS	11	11	-	-	-
TTC	11	11	-	-	-
Sum	63	47	16	-	-

4 RAMS REQUIREMENT

4.1 General

System supplier shall meet the following general requirements to assure safety and reliability.

.RAMS Analysis shall be carried out to comply with EN 50126, EN50128, EN50129

.System shall be developed to comply with local regulation.

4.2 RAMS Target

Reliability Target

Reliability target for On-Board System and Wayside System is suggested separately like following:

.MTBSAF of On-Board System shall be over 50,000 hours

.MTBSAF of Wayside System shall be over 20,000 hours.

Maintainability Target

MTTR of LRU shall be less than 1 hour. (Logistic time is not considered)

Availability Target

Availability of Signalling system shall be over 99.9%.

Safety Target

Qualitative safety target based on EN 50126 shall be applied for risk assessment and Mitigation measure to reduce the risk level to acceptable level with ALARP principle.

4.3 RAMS Management Requirement

RAM Management

System supplier shall provide system following system life cycle from EN 50126 and carry out RAM analysis per each phase.

And System supplier shall demonstrate reliability and maintainability during commissioning phase or revenue service.

Safety Management

System supplier shall provide system following system life cycle from EN 50126 and carry out Safety analysis per each phase.

And System supplier shall validate safety during commissioning phase.

S/W Assurance

System supplier shall carry out S/W assurance to comply with EN 50128.

Safety Assurance Certificate

System supplier shall provide system with safety certificate from independent authority.

Corrective Action & Reliability Growth

System supplier shall establish FRACAS and suggest program to enhance reliability with corrective action.

Safety Design

System supplier shall design sub-system to meet with safety requirements from SHA.

Deliverables

System supplier shall produce following deliverables to comply with EN 50126.

5 CONCLUSIONS

LBS, SHA, RAM target and safety requirement development were carried out to establish RAMS requirement in this project.

22 safety requirements for On-Board System and 93 safety requirements for Wayside System were developed through 63 hazards by carrying out SHA.

System supplier shall meet with developed safety requirement for later detail design of sub-system.

RAM target was developed by using one of similar system in other project because RAM target and failure data were not in Korea.

Therefore, RAM target suggested in this project can be updated if it provide the specific RAM data later.

It was concluded that system supplier shall perform RAMS activity to comply with EN 50126 and to meet safety requirements developed in this project, and if necessary, ISA for system supplier's RAMS activity is recommend.

REFERENCES

EN 50126 : Railway applications- The specification and demonstration of Reliability, Availability, Maintainability and Safety(RAMS)

EN 50128 : Railway applications- Communication, signalling and processing systems- Software for railway control and protection systems

EN 50129 : Railway applications- Communication, signalling and processing systems- Safety related electronic systems for signalling