Research on the Safety Improvement Method for the Company's RAMS Management Business and Public Infrastructure

이종범.조재립

한국표준협회 QM 신뢰성팀 수석전문위원.경희대학교 산업공학과

Jong-Boem Lee. Jai-Rip Cho

Quality Management and Reliability Team, KSA. Dept. of Industrial & Management System Engineering, KyungHee University

Keywords: PHA, RBD, FTA, FMEA, FMECA, SSHA, SHA, HL, SIL, IEC 62278, IEC 62279, IEC 61508

Abstract

The increase in hazard level is attributed to the industrial hazard environment; complete national environmental hazards to human health include climate change. The damage level in Korea from 1993 to 2009 has exceeded the increase in adverse environmental conditions. Priority areas of concern will include those risks that are most likely to occur and are expensive when they do take place such as accident or injury at a community pool. Therefore, in this paper, we suggest the System Engineering method for application to the railway RAMS. Recently, the requirement of high-integrity level of infrastructure has been deemed important.

The systems level approach is defined through the assessment of the RAMS interactions between elements of complex system applications.

I. Introduction

Ensuring infrastructure safety entails acquiring a social safety net, and such can seriously affect firms' sustainable management system. As one of the characteristics of infrastructure construction participated in by a specific firm, construction is carried out in a state wherein the local government concerned and residents have already perceived such. In such construction, when faulty areas or system problems arise on the social safety network dimension, not only do serious safety issues emerge; the social responsibility of such problem-causing firm is also brought to the fore. In this context, reliability, availability, maintainability, and safety (RAMS) meeting the international regulations should be implemented in advance considering the recently identified three bottom lines (corporate governance, <economic>, environmental, social) of sustainable management.

Korea' s corporate competitiveness in the international arena is improving remarkably, and RAMS is implemented as a means of improving each company' s brand value.

The RAMS system has evolved into the IEC 62278 and IEC 62279 systems based on EN50126; it is classified as RAMS system in the hardware sector and RAMS system in the software sector. For IEC 62278 in particular, the RAMS system has developed based on EN 50126, serving as the foundation of the RAMS system in the hardware sector. [1][2]

For the safety of a system, the system is needed the safety evaluation wherein the safety integrity level (SIL) is evaluated. The foundation of SIL evaluation is based on IEC 61508. [3]

The SIL evaluation - which is based on RAMS implementation concerning the social overhead cost (SOC) within Korea - and activities to maintain and complement the relevant system' s subsystem at a certain level of SIL are deemed important and meaningful; implementation still leaves a lot to be desired, however.

There are various methodologies related to the tools for promoting RAMS for infrastructure. However, this paper focuses on the widely applied method for the railway system.

The RAMS application procedure can be broken down into 3 steps: in step 1, it can be carried out focusing on PHA, RBD, FTA, and FMEA; in step 2, the focus is on FMECA, SSHA, and SHA; step 3 focuses on HL and SIL evaluation.

This paper studies the RAMS system application methodology from the system engineering for the safety improvement. Also, this paper introduces the applied methodology of the reliability technique of applying the RAMS system.

II. Overview of the RAMS System

The RAMS system is the procedure for managing RAMS with the interactions among them, system life cycle, and tasks within the cycle. The RAMS system also includes actions to manage and control efficiently the inconsistent sectors among RAMS parameters.

Improving system reliability in infrastructure requires confirming the raw and subsidiary materials' life and failure rate and forecasting the lifespan.

Reliability measure is decided by the reliability function, which demonstrates reliability as a function of t (use time). The resulting value becomes the survival (success) probability in time t. When the total number of survivals in the initial stage is assumed as N, and the number of survivals in given time t is denoted as n (t), R (t) as the number of survivals in time t can be expressed as $R(t)=\frac{n(t)}{N}$. Here, cumulative probability distribution F (t) of failure up to a given time t becomes $F(t)=1-\frac{n(t)}{N}$. If all failures take place in a given time t under the condition of ($t=\infty$), $F(t=\infty)=1$, $R(t)+F(t)=1$ can be derived. Accordingly, to determine the ratio of failure per unit time, F (t) can be differentiated and examined: $f(t)=\frac{dF(t)}{dt}$. Here f (t) becomes failure probability density function $F(t)=\int_0^t f(t)dt$,[4],[5]

$R(t)=\int_t^\infty f(t)dt=1-F(t)$. If $1-R(t)$ is used to substitute F(t) and is differentiated, however, f(t) is expressed as $f(t)=-\frac{dR(t)}{dt}$.

In general, the failure rate function is expressed as

$$\lambda(t)=\frac{1}{R(t)}\left[-\frac{dR(t)}{dt}\right]=\frac{-R'(t)}{R(t)}$$ [6],[10]

; if integrated by given time t, it is expressed as

$$\int_0^t \lambda(t)dt=\int_0^t -\frac{R'(t)}{R(t)}dt=-\ln\left[R(t)\right]_0^t=-\ln R(t)+\ln R(0)$$

Here, reliability R (t=0) at time t=0 always becomes 1.0. Since ln 1.0 is 0, the integrated function is converted as $\int_0^t \lambda(t)dt=-\ln R(t)$. When the antilogarithm is taken, R(t) is expressed as

$$R(t)=\exp\left[-\int_0^t \lambda(t)dt\right]=\exp[-\lambda t]=e^{-\lambda t}$$ [4],[5],[6]

Availability in infrastructure is

expressed as the ratio of time; when the manufactured and provided system exerts various functions during the period of use by the operator from his/her position, it can be defined as

$$\text{Ao(Availability)}_{\text{O(Operation)}}=\frac{\text{OperationTime}}{\text{Operation Time}+\text{Failure Time}}.$$

However, that the system' s failure time (regarded as mean time to repair) is decided by peculiar availability; hence the importance of peculiar availability in the railway system.[7]

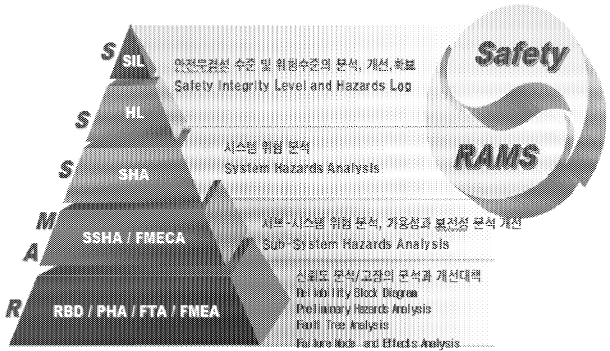
$$\text{Ai(Availability)}_{\text{i(Inherent)}}=\frac{\text{OperationTime}}{\text{Operation Time}+\text{Failure Detection and Repair Time}}$$

Maintainability is a very important activity in infrastructure; it is also managed based on reliability and availability. The measure for the management of maintainability is managed by MTTR and is calculated based on the following formula:

$$MTTR=\frac{1}{\mu} \quad \text{or} \quad \text{MTTR}=\frac{\sum_{i=1}^{n} t_i}{n}.[9]$$

Here, time t_i (i indicates the failure sequence) denotes the time for maintenance; maintainability activity in the promotion of RAMS is generally conducted based on activities for reliability and availability. Work should be carried out based on the FMECA methodology for the maintainability activity.

In the RAMS activity, validating the status of securing safety using safety analysis methods including PHA, SSHA, SHA, and HL and achieving the safety objective are important when ensuring safety.


S
S
S
M
A
R
SIL
HL
SHA
SSHA / FMECA
RBD / PHA / FTA / FMEA
안전무결성 수준 및 위험수준의 분석, 개선,확보
Safety Integrity Level and Hazards Log
시스템 위험 분석
System Hazards Analysis
서브-시스템 위험 분석, 가용성과 보전성 분석 개선
Sub-System Hazards Analysis
신뢰도 분석/고장의 분석과 개선대책
Reliability Block Diagram
Preliminary Hazards Analysis
Fault Tree Analysis
Failure Mode and Effects Analysis
Safety
RAMS

Source : IEC 62278,IEC 62279, EN50126

[Figure 1]

The RAMS system should be executed in 14 steps based on the abovementioned work development. Moreover, Reliability, Availability, Maintainability, and Safety should interact with one another to ensure system reliability and safety. [1][2]

III. Study of the RAMS system application methodology from the System Engineering aspect for system safety improvement

An effort to secure system safety is made through various perspectives and approaches. As the most important field in system engineering, the core engineering field should include design review, manufacture review, inspection and failure analysis, test evaluation, and safety evaluation based on safety standards specifying the system' s technical access.

From the system engineering aspect,

the RAMS system is applied based on the 14 steps defined in IEC 62278 in the infrastructure field so that activities designed to improve system safety can be implemented. Specifically, the activities can be carried out by detecting or improving the sectors that cannot be considered in core technology and design, construction fields with a V-Model concept from the aspects of reliability, availability, maintainability, and safety. The RAMS system has considered the application of the approaches shown in Figure 1.

A different method of analysis tools can be applied to the contents defined in IEC 62278 depending on the approach through different analytical study.

Likewise, different modes can be applied including the addition of IEC 61508 in the existing RAMS system by region, nation, and organization according to the scope, size, type, difficulty, complexity of infrastructure, and social influence scale of SOC or demand of the RAMS system applying IEC 62279.

For the IEC 62278 RAMS work procedure and system, a highly adequate analysis tool based on the system analysis anchored on the findings in this paper has been applied. When a method is already validated, or its documentation is carried out, a methodology that facilitates objectification and numeric data control is applied.

In the case of the electronic system in particular, the foundation of parameters in the reliability stage corresponding to the basic step should be faithfully executed by evaluating the safety and failure rate of PCB ASS' Y based on the parts stress analysis rather than on the parts count method pursuant to MIL-HDBK-217F, 217F-Notice-1, 217F-Notice-2.[11],[12]

In particular, PSA should be based on data anchored on the electric and physical measurements of the product that is actually applied rather than a test. PSA is executed since most parts consist of semiconductor or electronic parts in the case of the signal system; the stress of electrical or electronic parts is concentrated on electric power, voltage, electric current, and temperature, providing raw failure rate data to MIL-HDBK-217D ~ F. This ensures precision and reliability in data validation.

Potential failure analysis and risk analysis are carried out based on the work as per the guidelines of IEC 62278 and IEC 62279. The objectivity of the safety and integrity level evaluation should be ensured by applying the safety integrity level specified in IEC 61508.

IV. Study on the Pattern of Application to the Field

1. The Methodology for the Field Application of the RAMS System

For the worksite application of the RAMS system, this study carried out the following: First, the requirements analysis of the reliability system should be carried out in advance. Specifically, the survey and research of the following as reliability parameters should be conducted beforehand: Failure rate, Mean Up Time (MUT), Mean Time To Failure (MTTF), Mean Distance To Failure (MDTF), Mean Time Between Failure (MTBF), Mean Distance Between Failure (MDBF), Failure Probability (F(t)), and Reliability ((Success Probability) R(t)).

This research analyzed the failure system and failure type pattern through the application of PHA, RBD, FTA, and FMEA for the survey and efficient application of reliability parameters and categorized the reliability parameters and core factors.[1],[2]

Second, for the availability system requirements analysis, availability parameters are analyzed based on such requirements. The applicable availability parameters are Ai, Aa, Ao, Fleet Availability (FA=Available Vehicle/Fleet), and Schedule Adherence (SA). Properly analyzing and managing the various parameters of the availability system require the active utilization of the tool used in the reliability parameter analysis.[1],[2]

Third, for the maintainability requirements analysis, analysis should be conducted. The maintainability parameters include the following: Mean Down Time (MDT), Mean Time/Distance Between Maintenance (MTBM/MDBM), Corrective or Preventive MTBM/MDBM (MTBM(c)/MDBM(c),MTBM(p)/MDBM(p)), Mean Time To Maintain (MTTM), Corrective or Preventive MTTM (MTTM(c)/MTTM (p)), Mean Time To Restore (MTTR), False Alarm Rate (FAR), Fault Coverage (FC), and Repair Coverage (RC). To manage the various parameters of the maintainability system properly, the FMECA and PHA analysis results should be utilized carefully. [1],[2]

Fourth, the management factors for logistics or maintenance support should be analyzed and systematic management, conducted. The logistics support or maintenance support parameters include the following: Operation and Maintenance Cost (O & MC), Maintenance Cost (MC), Maintenance Man Hours (MMH), Logistic and Administrative Delay (LAD), Fault Correction Time, Repair Time, Maintenance Support Performance, Employees for Replacement (EFR), and Probability of Spare Parts on Stock when necessary (SPS).[1],[2]

Fifth, for the safety system requirements analysis, the safety system parameters for safety management should be managed well. The parameters include Mean Time Between Hazardous Failure (MTBF(H)), Mean Time Between "Safety System Failure" (MTBSF), Hazard Rate (H(t)), Safety-Related Failure Probability (Fs(t)), Probability of Safety Functionality (Ss(t)), and Time to Return to Safety (TTRS).[1],[2],[3]

To analyze and manage the safety system parameters properly, tools such as SSHA, SHA, and HL should be applied.

2. Introduction to the Applied Methodology of the Reliability and Safety Improvement Technique

Although the technique to be applied in the stage of securing reliability is the same as that applied in the general manufacturing industry, the concrete approaches to the implementation methods vary. The techniques that are mainly used include PHA, RBD, FTA, and FMEA. Looking into the process of the techniques, we can see that PHA is based on MIL-STD-882D; nonetheless, it needs to be executed in a more detailed manner than MIL-STD-882D in classifying and applying the cycle and risk size, which should be suitable for the infrastructure. [8]

For the techniques in the reliability and safety improvement stage, FMECA, SSHA, and SHA -- which apply modes that are different from the methods applied in MIL-STD -- are applied.

FMECA is applied based on the raw data provided in MIL-STD. Note, however, that work is carried out focusing on what maintenance activities will be conducted particularly the item types in the maintenance stage based on the identified matters in PHA and FMEA in the RAMS system.[13]

SSHA (SubSystem Hazard Analysis) is applied to analyze the subsystem hazards; it is carried out based on PHA and FMECA. The analysis results are reflected on SHA (System Hazard Analysis). SSHA implementation results refer to the activities for securing the safety of subsystem or parts; the opinions of the firm concerned and experts must always be reflected on the implementation process.[14]

The form and related data applied in each stage are based on IEC62278. For the form application types, the sheet of the type recommended by related standards has been used.

Complying with the work type based on sheet use is expected to make work management efficient following the RAMS job implementation.

V. Conclusion

The RAMS system in the railway field as set forth in IEC 62278 targets various parts, subsystems, and systems applied to the railway. Although the RAMS system in the railway field is applied to other SOC fields, however, the basic application to the field is considered to remain unchanged.

The application of the RAMS system is based on IEC 62278 and IEC 62279. As an action to accomplish the ultimate objective of RAMS, a system meeting the safety management objectives of hardware and software should be established by simultaneously applying IEC 61508.

References

[1] International Electrotechnical Commission (2002). IEC 62278: Railway Applications - Specification and Demonstration of Reliability, Availability, Maintainability, and Safety (RAMS).

[2] International Electrotechnical Commission (2002). IEC 62279: Railway Applications - Communications, Signaling, and Processing Systems - Software for Railway Control and Protection Systems.

[3] International Electrotechnical Commission (1998). IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems.

[4] O' CONNER (1995). Practical Reliability Engineering, pp.117~173.

[5] E.E. LEWIS (1994). Introduction to Reliability Engineering, pp.361~400.

[6] Elsayed A. Elsayed (1996). Reliability Engineering, pp.151~185.

[7] Evan Marcus and Hal Stern (2003). Blueprints for High Availability, pp.31~60.

[8] Bryan Dodson and Dennis Nolan (1999). Reliability Engineering Handbook, pp.137~285.

[9] Boris V. Gnedenko and Igor A. Ushakov (1993). Probabilistic Reliability Engineering, pp.87~100.

[10] John D. Kalbfleisch and Ross L. Prentice (2002). The Statistical Analysis of Failure Time Data (second edition), pp.31~48.

[11] John Cadick, Mary Capelli-Schellpfeffer, and Dennis Neitzel (2006). Electrical Safety Handbook, pp.1.2~1.26, 5.1~5.24.

[12] Milton Ohring (1998). Reliability and Failure of Electronic Materials and Devices, pp.13~29, 202~206.

[13] D.H. Stamatis (1995). Failure Mode and Effects Analysis, pp.1~295.

[14] Nancy G. Leveson (1999). Safeware: System Safety and Computers, pp. 313~358.