Concept of Management and Application to Safety-Related Systems by RAMS

Jun YOSHINAGA*

1. INTRODUCTION (RAMS FOR RAILWAY)

1.1 Overview of RAMS

RAMS refers to the four factors of Reliability, Availability and Maintainability (RAM) and Safety. The functional safety standard for the railway sector, IEC 62278, is commonly known as "RAMS".

This standard should perhaps be called "Railway RAMS", but because there is no other international standard that considers Safety in conjunction with RAM and the expression RAMS has also taken root worldwide, the term RAMS will be used in this paper.

The RAMS standard specifies a procedure for achieving and demonstrating (explaining based on appropriate grounds) the requirements for the four factors of RAM and Safety which are required in railway products. Since it has rapidly become a de facto standard in overseas railway projects, applicability to RAMS is required in safety-critical products.

However, because there is no international framework equivalent to the IMO in the railway industry, and use of the RAMS standard is not legally required except in some countries, the general practice is to stipulate the application of RAMS in the specification between the parties concerned. Although RAMS is not required in domestic projects in Japan, the number of railway product manufacturers that are capable of utilizing RAMS is gradually increasing.

In comparison with the functional safety standards in other sectors, one distinctive feature of RAMS in the railway sector is the fact that it notes the importance of maintaining a balance among the four factors of RAM and Safety and with the life cycle cost (LCC), while continuing to prioritize safety.

Based on the example of RAMS for railways, this paper will describe the management methods applied by manufacturers and users in product development and product use by RAMS management methods, and the differences with the conventional thinking of aiming at "zero trouble".

1.2 Reasons for Spread of RAMS

From the standpoint of railway companies in other countries, manufacturers (including integrators) are required to perform product development by procedures that conform to RAMS in order to procure safe products that are free of unexpected risks.

The following will use the development of a chair as a simple example so the reader can understand the general concept of product development based on RAMS. However, it should be noted that the original target of RAMS is products with embedded software programs.

Generally, the procedure when developing a chair is probably to consider the basic shape, and then study the strength and material of the legs.

It can be thought that this study is carried out bearing in mind safety measures for the risk of "failure under load" by considering the "target load that the chair should be able to withstand" and setting "strength of that value or more".

Fig. 1 shows attempts to build three types of chairs. Intuitively, it seems that many risks can be mentioned in chair (2), and chair (3) which has a moving part. Next, let us consider the safety measures for these risks.

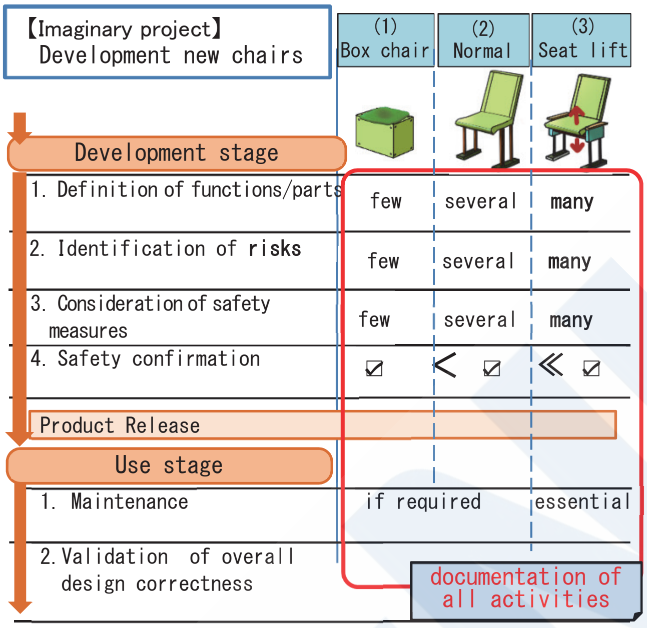
If an "object detection function (i.e., a sensor)" is considered to be an indispensable countermeasure for the risk of "catching one's fingers", which is a concern in chair (3), it would probably be hasty to select an expensive, high-reliability sensor. Rather, it would be more reasonable to create a mechanism which does not overlook possible problems by using multiple affordably-priced sensors. A study of this type corresponds to consideration of the balance of the four factors of RAM and Safety.

Safety measures are not limited simply to hardware and software, but also include various other types of measures, such as the user's method of use, periodic inspections and so on. However, even so, risk which does not exceed a certain level, referred

* National Agency for Automobile and Land Transport Technology, National Traffic Safety and Environment Laboratory (Former Director of the Rolling Stock Industry Planning Office, Railway Bureau, Ministry of Land, Infrastructure, Transport and Tourism)

to as “residual risk”, is permissible (acceptable).

In RAMS, the series of studies outlined above is performed for each part and function in accordance with a planned procedure, and the multilayer verification of the results of implementation is carried out at key points. Finally, the plans, implementation, materials used in judgments, *etc*. of all activities are documented as documentary evidence.



【Imaginary project】 Development new chairs	(1) Box chair	(2) Normal	(3) Seat lift
Development stage			
1. Definition of functions/parts	few	several	many
2. Identification of risks	few	several	many
3. Consideration of safety measures	few	several	many
4. Safety confirmation	☑	< ☑	≪ ☑
Product Release			
Use stage			
1. Maintenance	if required		essential
2. Validation of overall design correctness			

documentation of all activities

Fig. 1 Image of risk-based product development

In the procedures of functional safety standards such as RAMS, the amount of documentation increases when products have complex functions, but it is possible to demonstrate that adequate study and countermeasures for the requirements for RAM and Safety were developed based on the functional safety standard. Moreover, the scope of responsibility of the user and manufacturers is also clear.

In contrast, conventional methods can show a certain level of safety by conformity to a technical standard, *etc*., for example, “conformity to the guideline for furniture”, but the range of risks assumed by the technical standard is not clear.

In overseas projects, the product user is not necessarily an expert, which means that it is necessary to explain the grounds for judging that products are safe and the outlook for the reliability, availability and maintainability (RAM) of the product. In addition, because the common sense of the manufacturer is not the same as the common sense of the user, trouble may gradually develop later when a misunderstanding occurs. For these reasons, the RAMS standard requires preparation of documentation that make it possible to understand the range of risks assumed for the product, the grounds for judgment, and the division of responsibility between the manufacturer and the user. It is important that these points can be confirmed from this documentation.

In the example of the chairs, in the unlikely event of an accident, the grounds for safety can be found in the functional safety standard. That is, the documentation demonstrates that the system was developed in accordance with the functional safety standard, and all Safety requirements and RAM requirements (Fig. 2) were satisfied in the manufacturer’s development process. Moreover, it is also possible to investigate the cause of the accident in an objective manner.

On the other hand, in the conventional method, the basis of the development procedure is ISO 9001, and in this case, it seems that considerable labor would be required to demonstrate the validity of the procedure.

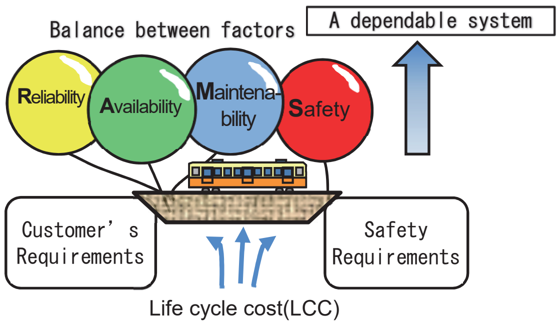


Fig. 2　System development based on functional safety

2.　FUNCTIONAL SAFETY STANDARDS

2.1　Overview

The functional safety described up to this point is one method for ensuring the safety of safety-related systems and devices. In functional safety, it is thought that some kind of risk inherently exists in systems and devices. Functional safety is a method for providing systems and devices in which unacceptable damage will not occur, even if that inherent risk became evident as a result of an accident, human error, *etc*., by using safety functions.

The international standard IEC 61508 series "Functional safety of electrical/electronic/programmable electronic safety-related systems" has been published, and JIS C 0508 is the corresponding standard in Japan.

In Japan, application[1] of new risk management methods in which functional safety is applied to demonstration of the safety of machinery, whose safety had conventionally been confirmed by compliance with safety standards, has now begun accompanying the increasing complexity and difficulty of visualizing risk due to the application of IT technologies.

2.2　Functional Safety Standards by Industrial Sector

Since the object of the functional safety standard IEC 61508 is electrical/electronic/programmable electronic safety-related systems (E/E/PE) used in safety functions in all sectors, it is difficult to understand the image of the work, which is described in highly abstract words.

For this reason, functional safety standards in which the indexes to be studied and the stages of development are matched to the features of actual products have been developed for specific industrial sectors (Table 1), as exemplified by the RAMS standard for railways. It may be noted that a standard for the maritime sector have not been released at this point in time.

Table 1　System of functional safety standards [2) 3)]

Classification	Examples of corresponding standards
Basic safety publication	IEC 61508 (JIS C 0508) "Functional safety of electrical/ electronic/programmable electronic safety-related systems"
Group safety publications	IEC 62278 Railway applications IEC 62279 Railway software safety ISO 26262 Road vehicles, electrical and electronic equipment IEC 62061 Industrial machinery ISO 13849 Safety-related parts of machinery control systems IEC 61513 Nuclear power plants

3.　CONCEPT OF RAMS

3.1　Quality Control of Product Life Cycle

In functional safety, the product life cycle is divided into phases from the conceptual phase of the product though the decommissioning (end-of-life) phase.

Although IEC 61508 is divided into 16 phases, the RAMS standard is divided into 14 phases because some phases were consolidated. The details will be omitted here.

If the phases of the life cycle are generalized and grouped together, they can be classified in 3 phases as shown by the dotted lines in Fig. 3. Product release falls between the “Development stage” and the “Use stage”. With release, product development work is substantially completed, and work generally falls under the category of after-service, such as inspection, repair, *etc*. However, in the case of RAMS, activities that are carried out after release in connection with the RAM elements and Safety are also considered to be part of product development, and the manufacturer is required to prepare an integrated activity plan in advance of such work.

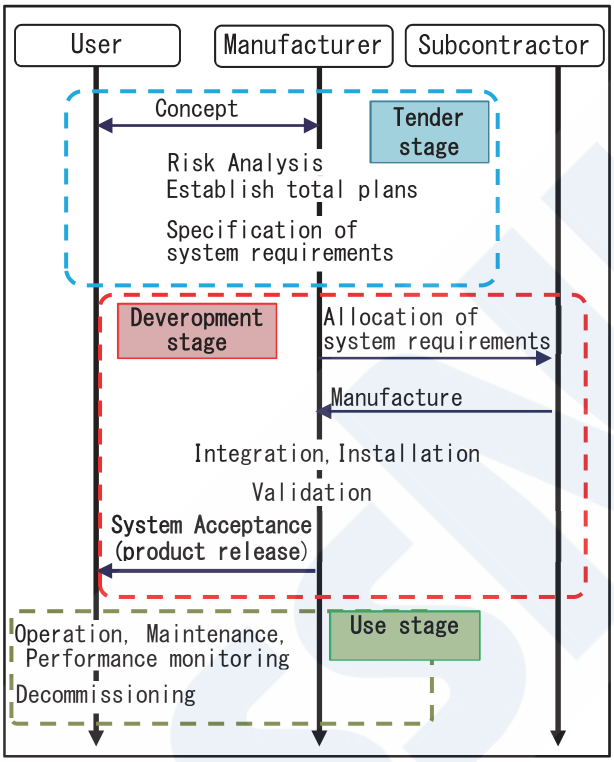

User
Manufacturer
Subcontractor
Concept
Tender stage
Risk Analysis
Establish total plans
Specification of system requirements
Devepopment stage
Allocation of system requirements
Manufacture
Integration, Installation
Validation
System Acceptance (product release)
Operation, Maintenance, Performance monitoring
Decommissioning
Use stage

Fig. 3　Activities in product life cycle

Although the plans prepared for Safety and the RAM elements are called the “Safety Plan”, and the “RAM programme”, the actual names of these documents depend on each project. Both documents plan management activities such the setting of product targets and measures for their achievement, the personnel system, methods for design, manufacturing and validation, and the documentation to be prepared.

For the use stage, the plans also describe methods for confirming the status of the RAM targets calculated in the development stage, and the maintenance methods assumed as preconditions in the development stage. This information is provided to the user, as will be described later.

In activities based on the RAMS standard, those which are carried out in connection with the Quality Management System of an organization are “shall” requirements, indicating that the Quality Management System occupies an important position in RAMS (Fig. 4).

Although both plans are prepared prior to the start of product design and describe general matters, the RAMS standard attaches importance to plans that are consistent throughout the entire life cycle in order to control quality across the total life cycle of the product. For example, if a plan is prepared, it is possible to check the implementation of the plan, and disorderly (unplanned) activities, such as arbitrary additions and revisions to specifications by unplanned procedures, are not permitted (because the validity of disorderly activities cannot be checked, an increase in the potential risk is a possible). Furthermore, these plans make it possible to communicate all necessary information to the user completely. As described later in section 3.2.2, this has also become an important concept for securing software quality.

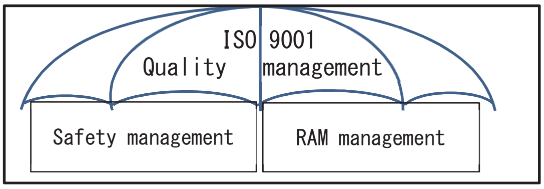


Fig. 4 Ensuring safety under quality management

3.2 Types of Failures and Their Countermeasures

The RAMS standard defines the following two types of failures and applies measures suitable for their distinctive features (Fig. 5). Since it is thought that many devices are now E/E/PE devices with embedded software, both types of measures are necessary in such cases.

(1) Random failures: Failures that occurs probabilistically.

(2) Systematic failures: Failures that occur under a specific combinations of inputs or specific environmental conditions.

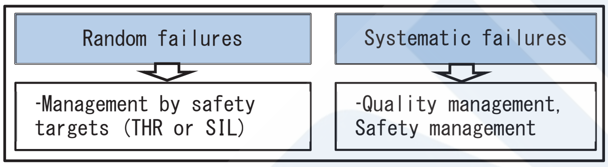

Random failures
-Management by safety targets (THR or SIL)
Systematic failures
-Quality management, Safety management

Fig. 5 Types of failures and their countermeasures

3.2.1 Countermeasures for Random Failures

Random failures occur probabilistically due to poor workmanship or deterioration of hardware. Because the effect assessment will depend on the severity and frequency of the failure, which types of hazards occur with what the degree of severity and frequency (risk) is important.

Therefore, for random failures, the necessary target of the system (THR: Tolerable Hazard Rate, or SIL: Safety Integrity Level) is allocated to each hazard, as shown in Fig. 6 (where the hazard is “loss of guiding function (derailment)”), and safety measures are taken to achieve this target. The safety of the system as a whole is protected by communicating the allocation rate of the system safety requirements to subcontractors.

In practical work, the SIL obtained by converting THR by Table 2 is frequently used. When subsystems are defined, the failure target (target failure rate) for the subsystems may also be decided in advance in some cases.

In allocations, targets that are higher than necessary to individual subsystems will result in unnecessary complexity, and is also a cost factor. Therefore, rational allocation is consistent with the concept of RAMS, which places importance on balance.

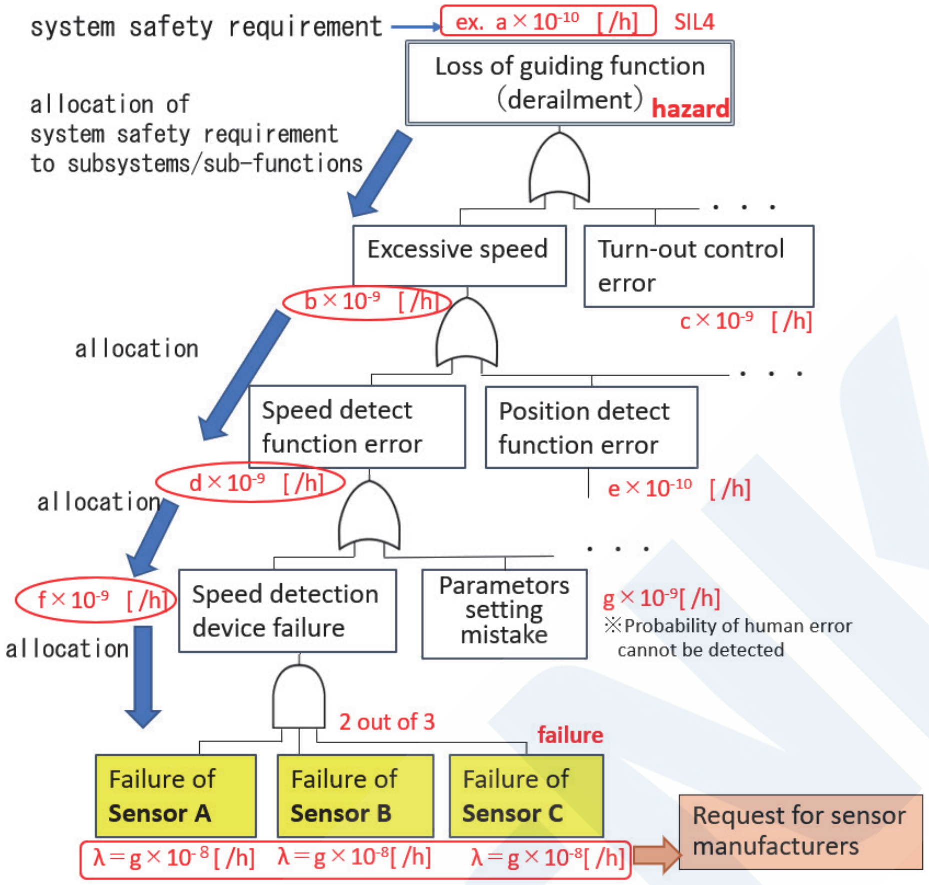

system safety requirement
ex. a×10-10 [/h]
SIL4
Loss of guiding function (derailment)
hazard
allocation of system safety requirement to subsystems/sub-functions
Excessive speed
Turn-out control error
b×10-9 [/h]
c×10-9 [/h]
allocation
Speed detect function error
Position detect function error
d×10-9 [/h]
e×10-10 [/h]
allocation
f×10-9 [/h]
Speed detection device failure
Parametors setting mistake
g×10-9[/h]
※Probability of human error cannot be detected
allocation
2 out of 3
failure
Failure of Sensor A
Failure of Sensor B
Failure of Sensor C
λ=g×10-8[/h]
λ=g×10-8[/h]
λ=g×10-8[/h]
Request for sensor manufacturers

Fig. 6 Example of THR allocation to subsystems

Table 2 THR/SIL conversion

Average Tolerable Hazard Rate (THR) targeted by safety function	Corresponding SIL
< $1\text{x}10^{-8}$ [/h] to $1\text{x}10^{-9}$ [/h]	SIL 4
< $1\text{x}10^{-7}$ [/h] to $1\text{x}10^{-8}$ [/h]	SIL 3
< $1\text{x}10^{-6}$ [/h] to $1\text{x}10^{-7}$ [/h]	SIL 2
< $1\text{x}10^{-5}$ [/h] to $1\text{x}10^{-6}$ [/h]	SIL 1
≤ $1\text{x}10^{-5}$ [/h]	SIL 0

Source: IEC 61508-1 Ed. 2.0 Table 2 (with partial revisions)

Remarks: In case of E/E/PE systems that operate in response to requirements (high frequency) and E/E/PE systems that operate continuously.

3.2.2 Risk Reduction Measures for Systematic Failures

Systematic failures are typically failures that are built into a system, such as software bugs and design errors due to mistakes in work instructions. They do not occur probabilistically (randomly), but rather, will invariably occur when a specific set of conditions exists.

As risk reduction measures for this type of failure, measures to prevent built-in failures and detect human error, e.g., inspections, *etc*., are implemented by applying management equivalent to the Tolerable Hazard Rate (THR), or “Techniques and Measures” (hereinafter, “T&M”).

The distinctive feature of the management approach is Verification or Validation at each phase by a competent person. T&M refers to know-how, that is, knowing which measure is necessary when a product with a certain SIL target is to be manufactured, as shown in the related RAMS standard in Table 3. Here, higher SIL values mean a larger number of requirements is applied.

Since products developed by conventional T&M do not agree perfectly with the T&M described in the standard, even products with excellent quality may not conform to the standard. To avoid this situation, it is important, in future development, to conform to the T&M of the functional safety standard as far as possible, and to record the reasons for points where differences occur.

Table 3 Example of T&M of standard

Technique/Measure	SIL0	SIL1	SIL2	SIL3	SIL4
4.Functional testing	M	M	M	M	M
5.Checklists	R	HR	HR	M	M
9.Walkthrough	R	R	R	HR	HR

Symbols:

M: Mandatory

HR: Highly recommended

R: Recommended

Source: IEC 62279 Ed. 2.0 Table A.11 (excerpt)

3.2.3 Risk Analysis for Safety

Although the definition of “safety” in functional safety standards differs in each standard, “safety” is generally defined as “freedom from unacceptable risk”.

“Risk” is defined as the “combination of the probability of occurrence of harm and the severity of that harm”. Therefore, risk increases as the frequency of occurrence increases and the degree of harm becomes more severe. Whether risk is “tolerable” or not is extremely important, and deciding this correctly based on appropriate grounds, such as a field study of the actual condition of existing products, is indispensable for realizing a well-balanced system.

On the other hand, as the “residual risk” (Fig. 7) which remains even after risk reduction measures are taken, a level of risk that can be judged to be tolerable by society (socially acceptable) is allowed to remain in products, and is not reduced to zero.

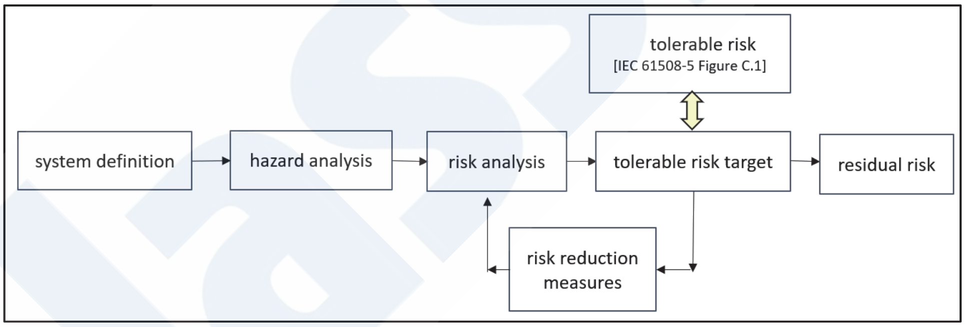


Fig. 7 Flowchart of risk reduction

Fig. 4 is a matrix of the frequency of occurrence of risk and the severity of harm. The manufacturer determines the concrete frequency of occurrence and severity, and takes risk reduction measures to eliminate or reduce risk at least in the categories of “Intolerable” and “Undesirable” based on a Failure Mode and Effects Analysis (FMEA), as shown in the examples in Table 5 and Table 6. In the FMEA, in addition to the Table 5, European manufacturers also study maintenance methods suitable for the part concerned (as discussed in section 5.1 below).

Although the current condition of the failure rate is desired when assigning frequency levels of risk and conducting an FMEA, it is difficult for individual manufacturers to determine this kind of information. In addition, although the target of legal regulations related to safety in the use stage is the actual manifestation of risks, unfortunately, neither laws and ordinance nor the RAMS standard defines the “socially acceptable level” of risks. This means that manufacturers must decide their targets for Safety and RAM by referring to the user’s requirements, the principle of ALARP (“as low as reasonably practicable”) [4)] or the like.

This information is summarized in documentation called a “Safety Case”, as shown in Fig. 8, which is defined as a “documented demonstration that the product complies with the specified safety requirements”.

From the viewpoint of using this information to demonstrate the safety of the product to those concerned, it is desirable to list the conceivable risks in a matter-of-fact manner, without discarding or selecting any particular items. Moreover, it is also necessary to trace the relationship of the risk reduction measures, grounds for judgment reasons and user's safety requirements in the documents of the product, which can be considered a unique feature of the functional safety .

Table 4　Safety risk assessment matrix

Frequency of occurrence of a hazardous event	Severity of risk			
Frequent	Undesirable	Intolerable	Intolerable	Intolerable
Probable	Tolerable	Undesirable	Intolerable	Intolerable
Occasional	Tolerable	Undesirable	Undesirable	Intolerable
Remote	Negligible	Tolerable	Undesirable	Undesirable
Improbable	Negligible	Negligible	Tolerable	Tolerable
Incredible	Negligible	Negligible	Negligible	Negligible
	Insignificant	Marginal	Critical	Catastrophic
	Severity levels of hazard consequence			

Source: IEC 62278 : 2002 Table 6 (excerpt)

Table 5　Example of functional FMEA

ID	ITEM/Function	Fault	Fault consequence	Existing Measures
R1	Invertor	current velocity data loss	halt	warning
	． ． ．			

Table 6　Example of design FMEA

ID	ITEM /Function	Fault	Potential			Result			
			Sev	Occ	RPN	Mitigation	Sev	Occ	RPN
M1	Invertor	current velocity data loss as a result of wrong input	2	3	6	add input data rationality check function	2	1	2
	． ． ．								

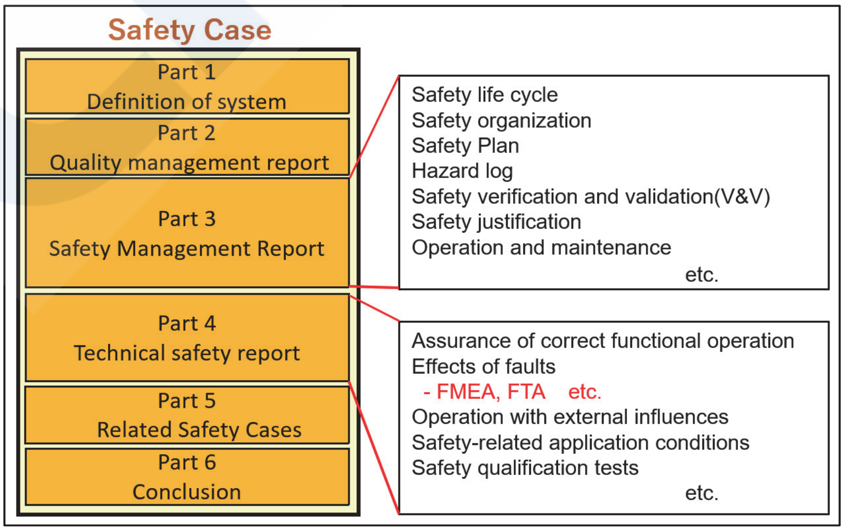


Fig. 8　Composition of Safety Case (documentation demonstrating compliance with safety requirements)

4. CONCEPT OF RAM MANAGEMENT

4.1 Factors of RAM

While assuming the safety of products as a given, product users prioritize Reliability, Availability and Maintainability (RAM), which are related to life cycle cost (LCC). Because particularly high importance is placed on the factors of RAM in railway rolling stock, some procurement specifications specify concrete numerical values.

Because standards do not specific concrete indexes for each of the factors of RAM, and only provide several examples (e.g., CLC/TR 50126-3, EN 50657), an index suitable for the product is selected. The main items are shown in Table 7.

For example, if the non-available ratio of a train is 5 [min/year], the availability (A) requirement is 9.5 x 10^{-6} (9.5 x 10^{-4} [%]). Assuming that a train experiences failures that result in a stop at a rate of 2/100 000 [km of train travel], MTBF (Mean Time Between Failures) = 50 000 [km of train travel] is required.

Table 7 RAM and Safety indexes

	Outline	Main indexes
Reliability (R)	Ability to perform as required for a given time interval under given conditions.	MTBF [h], MDBF[km] (Mean Time Between Failures), $\frac{1}{\lambda_S+\lambda_D} = \frac{1}{\lambda}$ [1/h]
Availability (A)	Ability to be in a state to perform as and when required, under given conditions.	$\frac{MTBF}{(MTBF+MTTR)}$ [%] $\frac{\mu}{\lambda+\mu}$ [%]
Maintainability (M)	Ability to be retained in, or restored to a state in which it can perform as required, under given conditions of use and maintenance.	$\mu = \frac{1}{MTTR}$ [%], MTTR [h] (Mean Time To Repair)
Safety (S)	Ability to be free of unacceptable risk.	λ_D [1/h](Dangerous failure rate) MTBF-H [t] (Mean Time Between Hazards)

In this table, λ means a failure rate. In terms of safety, the “dangerous failure rate” is important. Although there are various classification methods, here, the failure rate used in the table is given by the following Eq. (1), based on the safe failure rate λ_S and the dangerous failure rate λ_D.

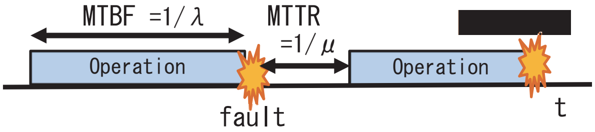
It can be said that “failsafe” design, which enables safe operation during failures, is also an architecture for improvements to reduce the ratio of λ_D.

$$\lambda = \lambda_S + \lambda_D \tag{1}$$

However, λ is to be a constant value over time that satisfies $0 \leq \lambda \leq 1$.

MTBF and MDBF represent the mean time or mean distance (km) that a train travels between the occurrence of failures, as shown in Fig. 9. For example, a system MDBF = 100 000 km means that one failure occurs in each 100 000 km of travel on average.

MTTR in the table shows the time from a failure until the completion of repairs, also including the time necessary to make arrangements for the repairs and maintenance parts, for a system premised on repair or exchange of parts.



MTBF(Mean Time Between Failure) : [h]
MTTR(Mean Time To Repair) : [h]

When MTBF:MTTR = 9:1, Availability (A) = 0.9.

Fig. 9 Concept of Mean Time To Repair

The reciprocal μ of MTTR is the repair completion ratio per unit of time [1/h], and is suitable for cases in which the time until completion of maintenance is probabilistic. In making repairs of railway rolling stock, there are some cases where repairs can be made immediately after a failure, and other cases where repairs must wait until late night. Therefore, this index is used in setting targets for the maintainability of products, for example, MTTR = 20 h (μ = 1/20).

To summarize this section, Reliability (R) is the ratio of the time or distance that a system functions, Availability (A) is the ratio of system operation in total time, and Maintainability (M) is the time required for repairs after a failure or the probability of repair (also including time for movement in addition to the net (actual) maintenance time). However, other indexes are also available.

Although maintainability is mainly defined in terms of repair, there are cases where maintainability also includes periodic inspections, lubrication (oiling), exchange of worn parts and cleaning work.

4.2 Setting and Allocation of RAM Targets

The allocation of system requirements for safety was described previously in Fig. 6. Among the RAM factors, particularly in the case of user requirements for Reliability, the manufacturer decides the target value of the system and then allocates Reliability targets to the subsystems.

Because an FTA (Fault Tree Analysis) for allocating Reliability rates would be too complex, the theoretical structure is simplified by a Reliability Block Diagram (RBD) according to IEC 61078, and Reliability is calculated for the system as a whole (see section 5.2).

To evaluate whether the result of the Reliability analysis is appropriate or not, the manufacturer also defines the severity and frequency of occurrence of failures for Reliability in the same as in the above Table 4 (Safety risk assessment matrix).

Table 8 shows an example of the risk assessment items related to parts installed in railway rolling stock. The condition of function maintenance is used as a judgment criterion for rolling stock parts. In many cases, MTBF (or MDBF) is used for frequency. Here, however, frequency is classified in terms that can be easily grasped and is easily understood by the user, such as the degree of the effect on safety, or the range of spread of effects.

Table 8 Example of risk assessment for Reliability

Severity	System failure mode	Impact to operation
Serious	Total system failure	Operation is impossible.
Large	Marginal functional failure (limit of acceptability)	Emergency operation
Small	Functional failure that does not reach the limit of acceptability.	Emergency operation
Negligible	Functional failure of a level that can be ignored.	Normal operation

Because Availability (A) is an element which is closely related to Reliability and Maintainability, as can been seen in Table 7, the Availability target exists in a relationship in which the target for Availability is achieved by achieving the targets for Reliability and Maintainability.

Maintainability (M) targets are set for the system and each subsystem, specifying the type of maintenance shown in Table 9 which is to be applied and the frequency of maintenance, based on a judgment considering the maintenance cost, MTTR and degree of involvement in safety.

The factors of RAM and Safety are closely interrelated. The targets of each factor are achieved through repeated study.

Table 9 Main types of maintenance

Type of maintenance	Outline
Preventive maintenance	Maintenance work performed regularly at specified intervals of time, travel distance, *etc*.
Corrective maintenance	Maintenance work performed when a failure or malfunction is detected.
Condition based maintenance	Maintenance work performed on reaching a predetermined index value based on condition monitoring.

5. APPLICATION EXAMPLES OF THE BALANCE OF RAM AND SAFETY

In recent years, the reliability of condition monitoring technologies and general-purpose parts such as memory devices has improved. This chapter presents examples of studies on improvement of the RAM factors by using general parts, *etc*., while also avoiding any substantial effect on safety.

5.1 Reliability and Maintainability

As a result of advances in sensor technology, maintenance of parts that had conventionally been exchanged after a set period has now progressed to "condition based maintenance", in which parts are exchanged when advance signs of potential failure are detected.

As shown in Fig. 10, if it is possible to detect anomalies (signs of potential failure) and perform maintenance within the period (P-F interval) from the detection of a potential failure to the actual failure, it is rational to incorporate this method in functional devices that have characteristics which can easily detection potential failures.

Although this method is not suitable for systems which require a high level of safety, the MTBF of other systems can be extended by maintenance without performing major repairs.

European manufacturers strategically implement reliability improvement measures using maintenance, for example, by studying the reliability of the detection and display function for potential failures at the time of system design and including maintenance methods and cycles suited to the part concerned in the above-mentioned Functional FMEA in Table 5.

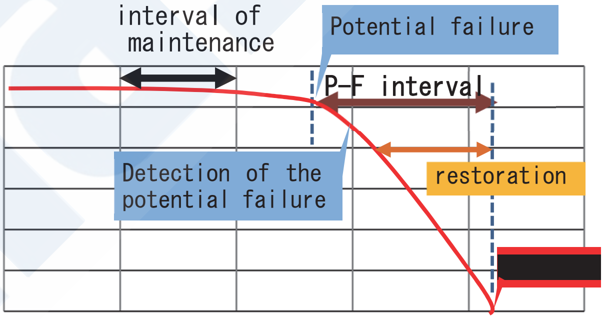


Fig. 10 Maintenance during P-F interval

5.2 Safety and Reliability

Fig. 11 shows an equipment configuration in which the same equipment is connected redundantly which is used in safety-related systems. This is a safety measure in which a "2 out of 3 (2/3) redundant system" is adopted in case the output of 2 units is in agreement in majority logic, and a 1/2 standby system switches to the standby system by a SW (switch) when a failure is detected.

Fig. 12 shows a failure of the total system (condition of function stop), that is, failure of equipment A, B and C that make up the 2 out of 3 redundant system.

These are example of the thinking when studying a system with the aim of cost reduction by using general parts without affecting safety. Here, equipment A, B and C are devices with the same failure rate λ, repair ratio μ, and dangerous failure rate

λ_D, and the failure rate of one of the 2 switches (SW) is expressed by (1 – p).

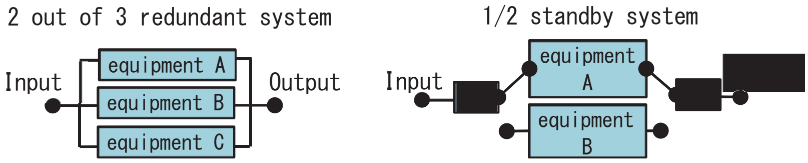


Fig. 11　Block diagram

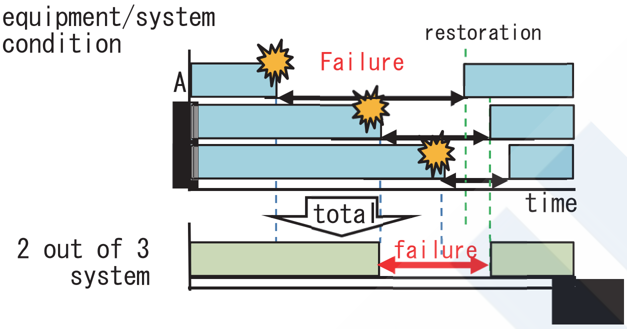


Fig. 12　Failure of 2 out of 3 redundant system

The safety of the 2/3 redundant system, $S_{2/3}$, can be expressed by Eq. (2) because it is the probability of cases other than that where 2 or more of the equipment units cause a dangerous failure at the same time. The safety of the 1/2 standby system, $S_{1/2s}$, can be expressed by Eq. (3) because it is the probability of cases for a switch failure and for the time when a dangerous failure of the equipment unit occurs.

$$\begin{aligned} S_{\frac{2}{3}} &= 1-\left({\lambda_D}^3 + {}_3C_2{\lambda_D}^2(1-\lambda_D)\right) \\ &= 2{\lambda_D}^3 - 3{\lambda_D}^2 + 1 \\ &= (2\lambda_D + 1)(1-\lambda_D)^2 \end{aligned} \tag{2}$$

$$S_{\frac{1}{2s}} = 1-\left(p\cdot\ \lambda_D + (1-p)\right)\ = p(1-\lambda_D) \tag{3}$$

λ_D :dangerous failure rate of equipment[1/h]

p :inverse of failure rate of two switches[1/h]

On the other hand, according to a reference by a US military research institute [5], the dangerous failure rate of the 2/3 redundant system, $\lambda_{2/3}$, can be expressed by Eq. (4), and that of the 1/2 standby system, $\lambda_{1/2}$, can be expressed by Eq. (5).

$$\lambda_{(n-q)/n} = \frac{(n)!\ \ (\lambda)^{q+1}}{(n-q-1)!\,(\mu)^q} \tag{4}$$

$$\lambda_{n/n+1} = \frac{n[n\lambda + (1-p)\mu]\lambda}{\mu + n(p+1)\lambda} \tag{5}$$

n :number of active units (n=3 in Eq.(4), n=1 in Eq (5))
q :number of units allowed to fail (q=1, in Eq.(4))
μ :repair rate[/h]
p: inverse of failure rate of two switches[1/h]

Using Eq. (2) to Eq. (5), reliability and safety were calculated by virtual numerical values, as shown in Table 10, for a system using parts which are highly reliable but require time for repair arrangements, and a system using parts which have a high failure rate but are readily available as “normal equipment”, i.e., general parts. Both systems are virtual.

Although the calculations were based on the assumption that the failure rate of the normal equipment is 5 to 10 times higher (worse) than that of the high-reliability parts, it can be understood that the normal equipment shows values similar to those of the system using the high-reliability equipment, depending on the architecture.

An element that makes a large contribution to improved reliability is shortening of the repair rate μ of the normal equipment from 24 hours to 6 hours, demonstrating that improvement of the repair rate is effective for improving the RAM factors.

Table 10 Example of trial calculation of safety and reliability

	high reliable equipment	normal equipment
Parameters of single equipment	λ=1×10^{-5} λ_D=1×10^{-7} μ=1/24 =4.17×10^{-2} p=1-10^{-5}	λ'=5λ =5×10^{-5} $\lambda_D{}'$=10λ_D =1×10^{-6} μ'=1/4 =2.5×10^{-1} p'=p=1-10^{-5}
2 out of 3 redundant system	$\lambda_{2/3}$=1.44×10^{-8} $s_{2/3}$=1-3×10^{-14} (SIL 4 Corresponding)	$\lambda_{2/3}{}'$=6.00×10^{-8} $s_{2/3}{}'$=1-3×10^{-12} (SIL 4 Corresponding)
1 out of 2 standby system	$\lambda_{1/2}$=2.50×10^{-9} $s_{1/2}$=1-1×10^{-5} (SIL 1 Corresponding)	$\lambda_{1/2}{}'$=1.05×10^{-8} $s_{1/2}{}'$=1-1×10^{-5} (SIL 1 Corresponding)

Remarks: All figures in the above table are virtual value

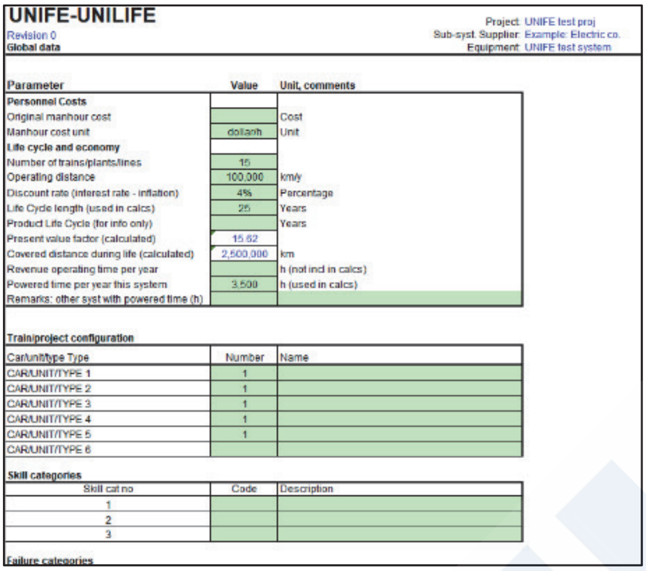
5.3 Calculation of Life Cycle Cost (LCC)

Regarding Life Cycle Cost (LCC), the RAMS standard states that safety shall not to be decided by cost, and notes the importance of a balance of Safety and the RAM factors, but does not provide specific requirements for LCC.

Since LCC is an important concern for users when determining RAM targets, in Europe, a calculation tool that uses the actual values surveyed by the industry in the European region as back data (historical data) has been developed (Fig. 13).

This tool has a structure in which accuracy increases as more detailed conditions are input, and is widely shared and used by manufacturers and users.

In Japan, a tool of this type is not available, and each manufacturer grapples with the issue of LCC independently. Although indispensable, this is a difficult problem because it is difficult for a single company to grasp. While an industry-wide effort is desirable, this is also confidential business information of users.



UNIFE-UNILIFE

Revision 0

Global data

Project: UNIFE test proj
Sub-syst. Supplier: Example: Electric co.
Equipment: UNIFE test system

Parameter	Value	Unit, comments
Personnel Costs		
Original manhour cost		Cost
Manhour cost unit	dollar/h	Unit
Life cycle and economy		
Number of trains/plants/lines	15	
Operating distance	100,000	km/y
Discount rate (interest rate - inflation)	4%	Percentage
Life Cycle length (used in calcs)	25	Years
Product Life Cycle (for info only)		Years
Present value factor (calculated)	15.62	
Covered distance during life (calculated)	2,500,000	km
Revenue operating time per year		h (not incl in calcs)
Powered time per year this system	3,500	h (used in calcs)
Remarks: other syst with powered time (h)		

Train/project configuration

Car/unit/type Type	Number	Name
CAR/UNIT/TYPE 1	1	
CAR/UNIT/TYPE 2	1	
CAR/UNIT/TYPE 3	1	
CAR/UNIT/TYPE 4	1	
CAR/UNIT/TYPE 5	1	
CAR/UNIT/TYPE 6		

Skill categories

Skill cat no	Code	Description
1		
2		
3		

Failure categories

Fig. 13 LCC calculation tool “UNILIFE”

6. ROLES OF USERS IN RAMS

Users of released products use those products in accordance with a document called an SRAC (Safety Related Application Condition), which summarizes the technical requests from the manufacturer to the user.

Although the SRAC is similar to a user’s manual, the SRAC is prepared based on the results of a risk analysis by the manufacturer, and describes the essential use conditions for avoiding manifestation of potential risks in a consistent manner from the viewpoint of preventing risk. The SRAC is also included in the Safety Case prepared by the manufacturer, and issued to the user.

On the user’s side, users are recommended to conduct the field data analysis called FRACAS (Failure Reporting, Analysis and Corrective Action System) shown in green in Fig. 14 on a regular basis. The achievability of the RAM targets is monitored based on the routine maintenance data and failures, *etc*. discovered in operation (shown in purple in Fig. 14), together with operational data.

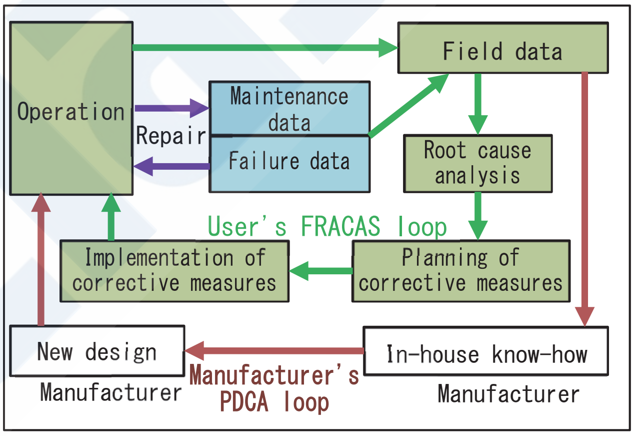


Fig. 14 PDCA cycle based on FRACAS analysis by user

Because there is concern that some type of malfunction or failure may occur if divergence is found as a result of this analysis, a root cause analysis and investigation are conducted, and improvements are carried out by implementing corrective action.

On the manufacturer’s side, the manufacturer investigates whether the RAM and Safety indexes studied in the product design stage are being achieved in response to contact from the user, or as an activity of its own Quality Management System.

If new risks are detected in this process, the product risk data in the Hazard Log are updated, and PDCA activities which utilize this data in future product development are performed.

The occurrence of product failures gradually decreases from a condition in which many initial failures occur and reaches a stable condition with a low failure occurrence rate over time. This is widely known as the “bathtub curve”. In overseas railway projects, a high cost penalty is often imposed for failure to achieve requirements (by contractual terms that impose a financial penalty for breach of contract on the manufacturer for failing to achieve the reliability target required in the product). Therefore, the timing of the judgment of achievement of requirements is important for both sides.

Since the timing of this judgment agreed between the user and the manufacturer in advance, the manufacturer monitors the condition of failure occurrence after product release and predicts the future trend.

If failure to achieve the requirements is predicted, manifestation of some type of malfunction or other risk is a possibility, so it is important to conduct a root cause analysis and take corrective action at an early timing in order to avoid the penalty. Mathematical prediction calculation methods such as the Erlang method, *etc*. are used for this purpose.

As described above, in the RAMS system, a risk-based approach is applied continuously to products, including in the use stage, by planning activities over the entire product lifecycle from product manufacturing, which also includes after product release, and operation, repair, and decommissioning.

As mentioned above, this is also related to the user’s confidential information, which means the range of information available to the manufacturer is frequently limited. Nevertheless, this is also a system that endeavors to improve product quality by identifying risks as far as possible and implementing measures.

7. CONCLUSION

This paper has presented an overview of the “RAMS” functional safety standard for railways, and has introduced techniques and risk-based concepts for ensuring safety by functional safety through RAMS.

Among the product development procedures based on RAMS, this paper has described distinctive concepts such as the types of failures and prioritization of quality control, and has also introduced examples of work performed by manufacturers and integrators, including the procedures for target setting for each of the elements of RAM and Safety and target allocation to parts, and the image of adjustment of each of the RAM factors with an awareness of cost.

The necessity of analysis activities for the RAMS factors based on field data, which are carried out by the user, was also described.

Finally, although it goes without saying, manufacturers in Japan provide prompt, carful after-service even without being asked, and this can be considered to be culture. On the other hand, in functional safety standards such as RAMS, a condition without controls such as planning, etc. is considered to be a disorderly state in which risks exist. Depending on how safety standards such as RAMS are used, they are also considered to provide a tool for demonstrating efforts in connection with product quality, safety and customer orientation which would otherwise remain unknown.

I hope that this paper will serve as a useful reference and can be of assistance in studies in the maritime sector, where technological development is progressing.

REFERENCES

1) Ministry of Health, Labour and Welfare: Securing the Safety of Machinery, Etc. by Functional Safety, https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000140176.html (accessed August 15, 2023)

2) Yoshinobu Sato: Seminar on Human Resources Training for Functional Safety [Basic Region], Functional Safety, Japanese Standards Association, September 2013, p. 24.

3) Takafumi Fukuda: IEC 62061 Overview of Functional Safety Standard for Machinery, Journal of the Japan Society for Safety Engineering, 2009, Vol. 48, No. 6, pp. 379-384.

4) Kenkichi Tamura: Risk in the Maritime Sector – Dealing Skillfully with Risk – , ClassNK Technical Journal, No. 6, 2022 (II), p. 4.

5) Rome Laboratory Air Force Material Command (AFMC), Reliability Engineer’s Toolkit, p. 90.