Safety Analysys Using STAMP/STPA for Electronic Interlockings

Tetsuya Takata, Kyosan Electric Manufacturing Co., Ltd.Akira Asano, Kyosan Electric Manufacturing Co., Ltd.

Hideo Nakamura, The University of Tokyo

SUMMARY

Fail-safe technology has been the foundation of the safety of previous signal systems. The fundamental principle is to build systems so that when a malfunction occurs in part of the system, red signals are always triggered and trains are stopped. In recent systems, however, software is essential, and the scale of that software is growing in size. At present, there is no such thing as fail-safe software, and high reliability is ensured through approaches such as writing easy-to-understand software and carrying out thorough inspection. In this paper, STAMP（Systems-Theoretic Accident Model and Processes）/STPA is used to conduct analysis on signal systems with large-scale software. Detailed safety analysis is carried out with STAMP/STPA, using electronic interlocking system as an example. Then an assessment approach is described, suited to the purpose of Phase 3: Risk analysis of railway RAMS (IEC62278), as well as a method of summarizing the results of that assessment as a hazard log.

1 INTRODUCTION

The mainstream of today's railway systems including conventional systems are computer control systems and their logic is implemented by software. So far, safety evaluation (design verification and validity confirmation) of software systems has been conducted by analysis method and test method. Validity confirmation by test method checks conformance to requirements by directly running the test of safety requirements. Validity check by analysis method includes top-down logical analysis of the mechanism by tracing back causes from results (such as FTA: Fault Tree Analysis), and bottom-up analysis from causes to results of processes by accumulating facts obtained from research (such as FMEA: Failure Mode and Effect Analysis). Confirmation methods by these analyses, however, will not be sufficient with only a breakdown of simple causes using a tree structure, because the huge growth of a system size increases the scale of major software constituting the system and the relationship between the components have become diverse. On the other hand, validity of Systems Theoretic Accident Model and Processes (STAMP) based on system theory supporting software intensive systems has drawn attention recently.

Advantages of STAMP include easy identification of causes of accidents arising from total system design and mismatch of interfaces between modules (accidents caused by interactions of the components in a today's system that has more complicated interactions between components because of increased number of components), such as technologies, human errors and linkage mismatch between projects that were hard to be found by conventional fault evaluation models such as FTA and FMEA.

For level crossing control systems, an analysis example using STAMP is given in First STAMP/STPA [2]. But to analyze signal systems of larger software size, concrete analysis methods such as rule-setting have to be prepared in addition to the flow described in the document above. In this article, we take an electronic interlocking device as an example, propose a specific analysis method based on the actual design processes, describe a method of summarizing the results of that assessment as hazard logs, and investigate the possibility of its applicability to the Phase 3 (Risk analysis) of IEC62278 (2002)[1], the international standard on railway reliability, availability, maintainability and safety.

2 ANALYSIS TARGET

2.1 What is the electronic interlocking device?

To securely achieve safety of train operation, the mechanical health of the running vehicles should come first, followed by perfect railway tracks, meaning no breakage of rails or obstacles on rails. On top of these, a clearance between the preceding train and the next train shall be kept to avoid train collisions, and arrangement between trains facing each other between stations in a single track section shall be made thoroughly (train interval control).
If divergences exist in a station yard, prescribed tracks shall be secured and derailing or approaching to other tracks shall not occur during operation of trains or vehicles (train route control).

In a station yard, many railways are connected like a concentrated and divergent network and the system is arranged so that all the tracks required for train operations can be configured while confirming safety. Therefore, at divergent sections and intersections, many switches required to configure tracks as well as many various signals, signs, and sign markers to indicate each track is installed.

In addition, arrival and departure of trains and shunt operation of vehicles are conducted simultaneously as much as track layout inside a yard premises permits. In pursuit of higher efficiency, restrictions on switching of switches and on handling of relevant signals have increased so much and become complex. Because of this, signals and switches are interrelated so that they will not be operated by an operator (lock) when he/she makes mistakes in operation. Further, signals and levers of switches are interrelated, with certain sequences in their operation and that locking relation is added and is called linkage. Those signals and levers of switches are operated with keeping the linkage relationship with each other (interlocking). Devices with this linking relationship are called interlocking devices and those controlled by micro computers are called electronic interlocking devices. They correspond to the Apparatus to Interlock Signals, etc. in the Ministerial Ordinance to Provide Performance-Based Technical Regulatory Standards on Japanese Railways (the Technical Standard) [3].

2.2 Before the analysis

Since an electronic interlocking device is an existing system and its components are determined, it is possible to analyze which component is the root cause of the accident. With progress of technology, if development is to be started with new technologies and ideas combined, it is not possible to analyze just focusing on the components. And as the scale of newly developed systems is growing with the number of the components increasing, and interactions between the components have become complex, we cannot understand a system by just understanding roles of its components only. STAMP is thought to be effective as a mean to solve this issue.

Features of STAMP include easy identification of causes of accidents due to total system design caused by a mismatch of interfaces of components including system mechanism, technologies, human errors and linkage mismatch between projects that were hard to be found by conventional fault evaluation models such as FTA and FMEA. Hazard analysis that identifies hazards (accident factors) before the accident occurs is conducted with the hazard analysis tool called STPA (System Theoretic Process Analysis).

3 FLOW OF SAFETY ANALYSIS

3.1 Definition of accidents

As described above, an electronic interlocking device is a device to control tracks of a train in a station premises where switches are installed.

Figure 1 describes this as a conceptual diagram.

Based on this conceptual diagram, accidents caused by track control are defined as follows.

(A1) Situation where trains collide into each other

(A2) Situation where a train derails

(A3) Situation where trains contact

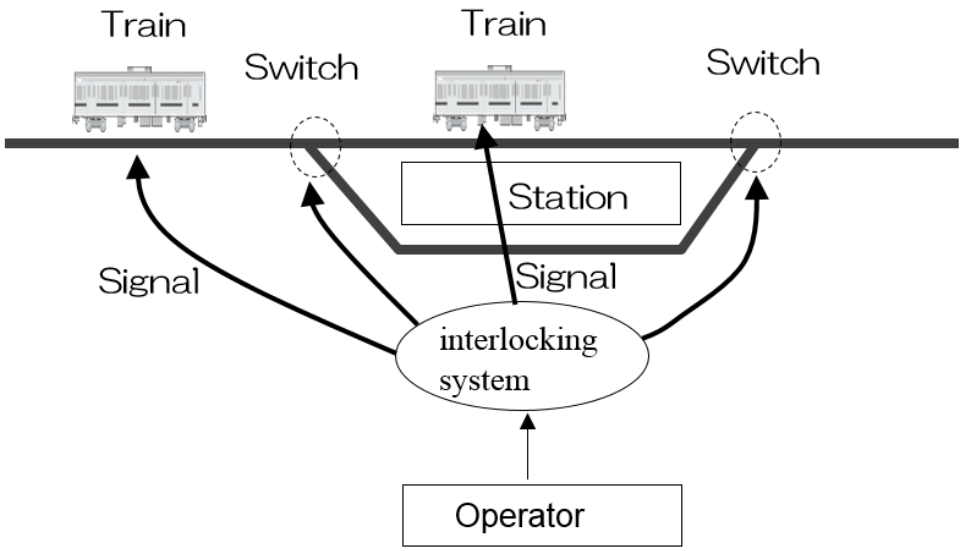

Figure 1. Conceptual diagram of electronic

To demonstrate safety of products and systems in the international market during the process of safety analysis, it is requested to build safety systems in accordance with risk-based designs widely used in international industries. In the risk-based design method, hazard extraction and risk assessment are performed, and whether the risk is acceptable or not is decided based on the ALARP (As Low As Reasonably Practicable) principle. Also, in the railway industry, this idea is indicated in the international standard of the railway RAMS (IEC62278) which makes over-all assessments of Reliability, Availability, Maintainability, and Safety over a product life-cycle from the design stage of the product through usage stage until the end of the product life, and tries to achieve each goal.

On the other hand, STAMP/STPA adopted as analysis methods can provide more persuasive analysis because it can analyze a cause of an accident originating from total system design or mismatch of interfaces between components that was hard to find with accident assessment models such as conventional FTA or FMEA, from the behavior of the interfaces during failure of the software modules. However, the existing issue with the usage of STAMP/STPA is that there is no distinction of assessment between conditions extracted as unsafe control instructions possibly causing a hazard from those that are actually unrealistic and those that are possible and need attention.

From the above, merging of the risk-based design method required for the risk analysis and exhaustivity of analysis results with STAMP/STPA is considered to be the effective evidence that the electronic interlocking device has been built safely. A procedure is shown below that indicates reduction of risks to an allowable level by systematic extraction (based on the principles described the Section Phase 3: Risk analysis contained in IEC 62278 the International Standard of the railway RAMS) and by comprehensive extraction of hazard risks contained in the system from defined accidents using STAMP/STPA, followed by countermeasures against them.

3.2 Hazard identification (STPA Step 0, Preparation 1)

Hazards for each accident defined are described in Table 1 below.

Table 1. Hazard identification

(A1) Collision between trains	**(H1)** A train is passing over a switch set in the wrong position and running toward a track section ahead that is being occupied by a preceding train.
(A2) Derailment of a train	**(H2)** A train is running on a switch being moved.
(A3) Contact (or collision) between trains	**(H3)** A train makes contact (or a rear-end collision) with another train at the fouling switch within a turnout.

3.3 Construction of control structure diagram (STPA Step 0, Preparation 2)

Creating a Control Structure Diagram based on Figure 1 it is important to draw conceptually without thinking of existing devices. Actors shall be an operator (control panel operator), track control (control body), switches and trains. Figure 2 is a control structure diagram drawn with attention to a device that controls the track approves travel of a train and controls switches on the track.

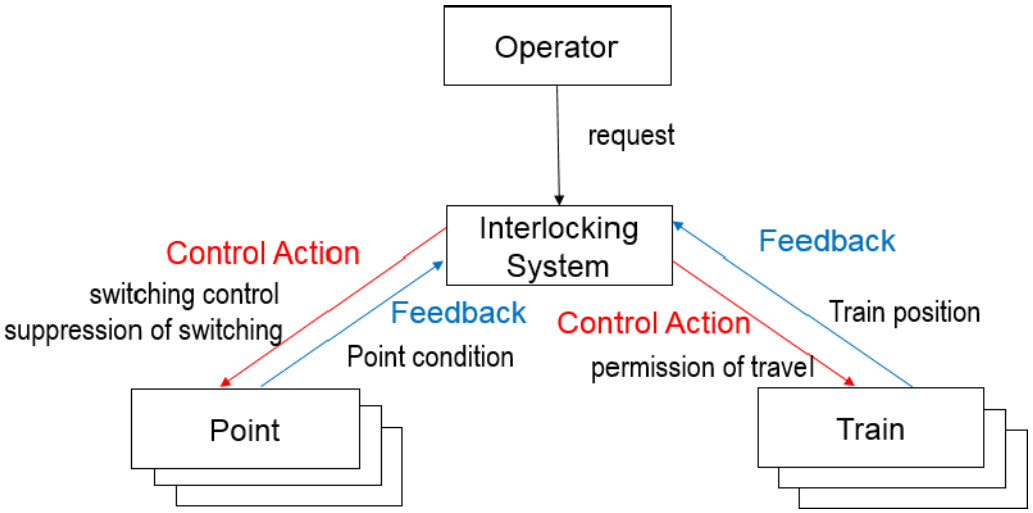

Figure 2. Control structure diagram

3.4 UCA identification (STPA Step 1)

Here, identification is made from the viewpoint of 4 items (Not Provided/Providing causes hazard/Too Early, Too Late, Wrong order causes hazard/ Stopping too soon, applying too long causes hazard) of an Unsafe Control Action (UCA).

At this time, analysis shall be performed by multiple persons repeatedly from various viewpoints extracted here. So, it is important to set description rules.

For example, as shown in Figure 3, a problem has occurred in a travel control that a same state transition expresses 2 controls, to grant permission of travel and not to grant not to grant permission, or non-permission. Because of this, use of standardized names of Control Actions is decided so that contradictory expression is not used in a description of a Control Action. Here, the Control Action of travel permission is decided “to permit”. Similarly, Control Action of suppression of switching is “to lock” against granting lock and against not granting removal of the lock. However, this is a problem with Japanese language. When a range of “over a switch” is used, the range is expressed by structural naming from various viewpoints, which causes a problem of multiple extractions of the same meaning. To fix this, a condition that has a range is defined to clarify whether the condition “is peculiar to the point of time” or “has a range” so that relationships of before and after in time, such as a delay, can be handled as front and rear in a range, and that extraction result will not duplicate.

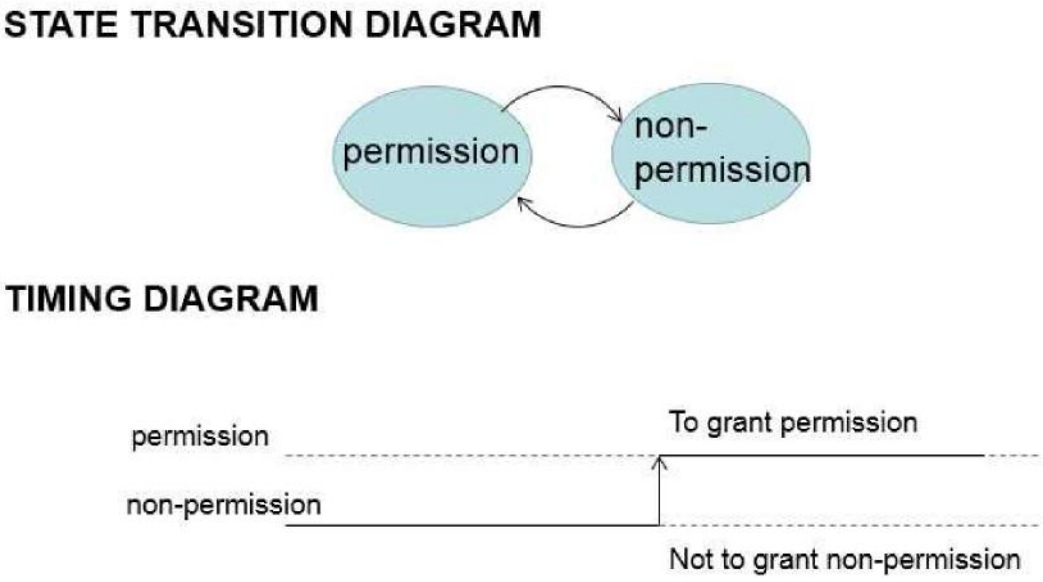

Figure 3. Example 1

Specifically, description rules are made as follows.

Description rules:

A symbol ○○ below denotes a Control Action.

R1. (Not Providing causes hazard)

Not Providing ○○ in a condition of xx causes hazard.

R2. (Providing causes hazard)

Providing ○○ in a condition of xx causes hazard.

R3. (Too early/too late, wrong order causes hazard)

Providing ○○ before a condition of xx causes hazard.

Providing ○○ after a condition of xx causes hazard.

Providing ○○ in wrong order of control actions causes hazard.

R4. (Stopping too soon/applying too long causes hazard)

Stopping of ○○ in a condition of xx causes hazard.

Continuation of ○○ in a condition of xx causes hazard.

The above decision brings a total 9 results of Unsafe Control Actions, i.e. UCA1 to UCA9. Details are as follows.

(UCA1) If suppression of switching is not given while a train is traveling over a switch, the train will derail if the switch operates. (H2)

(UCA2) If switching control is given to the opposite side of the traveling side while a train is traveling over a switch, the train will derail if the switch operates. (H2)

(UCA3) If travel permission is granted and the train moves while the switch is set to a side where another train exists in front, the train will collide (from behind). (H1)

(UCA4) If travel permission is granted and the train moves while a switch is not opened on the trail, the train will derail. (H2)

(UCA5) If travel permission is granted within a contact limit from the trailing and the train moves while another
train is traveling on the opposite side of the switch, the train will contact to the train in front. (H3)

(UCA6) If travel permission is granted and a train travels over a switch while it is switched, the train will derail. (H2)

(UCA7) If travel permission is granted too early before a train in front has passed through a vehicle contact limit, the trains will contact. (H3)

(UCA8) If travel permission is abruptly canceled while a train is traveling based on the permission, the train will go into an unpermitted area. (If an unopened switch exists in the unpermitted area, the train will derail.) (H1, H2)

(UCA9) Though destination request is canceled while progress aspect is issued, the train travels because travel permission continues and stop aspect is not issued. (Collision or derailment if a train exists in the unpermitted area.) (H1)

The condition “If travel permission is granted and the train moves ..., the train will collide (from behind)” is added in the UCA identification stage, to be defined as a precondition for the use of interlocking devices because it is a point to be handled outside of interlocking devices. Specifically speaking, it corresponds to the content of the following section of the Technical Standard.

- Section 54 “Devices to Ensure Blocks, etc.” of the Technical Standard
- Section 55 “Railway signal devices, etc.” of the Technical Standard
- Section 57 “Apparatus to Automatically Decelerate or Stop Trains” of the Technical Standard

3.5 Risk assessment (Extension of STPA)

In the risk-based design method, all the detected hazards are classified from the viewpoint of occurrence frequency and seriousness of damage, and combination of those decide which area in the ALARP triangle the concerned hazard belongs to. This enables ranking of each hazard, and by taking a quantitative risk assessment approach, whether the goal of the safety of the system is satisfied can be confirmed. Because of this, by interrelating the results extracted with STAMP/STPA, distinction can be made between those impossible in reality and those actually possible and need attention. Specific risk assessment methods are as follows.

When assessing risks, perform assessment of severity level for specified hazards in accordance with criteria of the severity levels. The risk assessment criteria shall be classified in 4 levels as Catastrophic /Critical/Marginal/Insignificant in accordance with Table 3 in 4.6.2.3 of RAMS standard IEC62278.

Next, perform assessment of occurrence frequency also to the extracted UCA based on the criteria of occurrence frequency. The occurrence frequency assessment criteria shall be classified in 6 levels as Frequent/Probable/Occasional/Remote/Improbable/Incredible in accordance with Table2 in 4.6.2.2 of RAMS standard IEC62278.

Perform the risk assessment by multiplying UCA occurrence frequency to the severity level for specified hazard. Risk assessment shall be made in 3 levels as Unacceptable/Undesirable/Acceptable in accordance with Table 6 in 4.6.2.4 of RAMS standard IEC62278.

3.6 HCF identification (STPA Step 2)

For the UCAs defined as “Unacceptable, Undesirable” as a result of the risk assessment, identify causal factors causing UCAs identified in STPA Step 1 as the last stage of STAMP/STPA, and expected accident scenarios. The causal factors that can be the causes indicate deficiencies expected in the flow of control loops and are extracted from viewpoints of 11 items (11 guide words) below[1].

In this step, issues raised include the necessity of a mechanism to detect trains reliably to avoid problems such as “cannot detect a train running over a switch” and “cannot recognize a train correctly.” It should be implemented outside of the interlocking devices and correspond to the content of the following section of the Technical Standard.

- Section 59 “Apparatus to Detect Trains, etc.” of the Technical Standard

3.7 Possible actions and specific methods (Extension of STPA)

For HCF(Hazard Causal Factor) extracted in Step 2, determine and execute specific methods and possible actions to remove causes of occurrence and to reduce risks.
It is understood that the following issues raised in the extraction stage of the possible actions correspond to matters related with locks (for the purpose of safe train operation, applying various locks to signals, switches, etc. by electric means and restricting operation of each device depending on requirements is called electric lock method) implemented by interlocking logic of existing devices.

As this indicates that extraction results analyzed with STAMP/STPA based on the conceptual diagram (Figure 1)contain possible actions in conventional interlocking devices, we consider that exhaustivity of the analysis result with STAMP/STPA is confirmed for the safety requirements of interlocking devices. Specifically:

- "Suppression of switching is not output due to inadequate control algorithm" and "Switching control is output due to inadequate control algorithm" correspond to detector lock by electric lock method.
- "Due to inadequate algorithm, travel permission is abruptly cancelled while the train cannot stop" corresponds to approach lock and stick lock by electric lock method.
- "Non-permission of travel is output but progress aspect is not output" corresponds to indication lock by electric lock method.

Also, in the possible actions listed here, specific process is indicated. Therefore, it is arranged that processes based on other software functions need to support top level functions satisfying SIL4 requirement conforming to IEC62279.

4 RISK MANAGEMENT TOOL

So far, we have described works performed with STAMP/STPA along the flow of risk analysis. But IEC62278 demands to establish continuous risk management processes. Hazard detection and analysis play a key role in the process of detecting hazards inherent to the system, accidental events induced by the hazards, or factors causing final accidents. This process is started in the initial stage of a project, executed repeatedly in each stage of the life cycle to remove hazards comprehensively and to reduce risks.

As a hazard management tool (Hazard Log) to realize the above, we propose to use a Risk Control Table shown in Figure 4 to control the results. Purpose of the preparation of the Control Table is to record all the detected hazards and to track them.

Following the hazard detection process described above, enter the result (No., ITEM, Hazard, UCA, Hazard Severity Level, Frequency of Occurrence of hazardous event, Qualitative Risk category) to the Control Table. The Control Table can be updated with the risk reduction process of each hazard in sync with progress of the design, secures traceability and transparency of the process (HCF, Determine possible actions, Method), and provides a key grounding for explanation of validity and correctness of technologies. In this way, the Control Table is prepared with the concept of a hazard management method assuming actual usage for risk analysis for safety investigation.

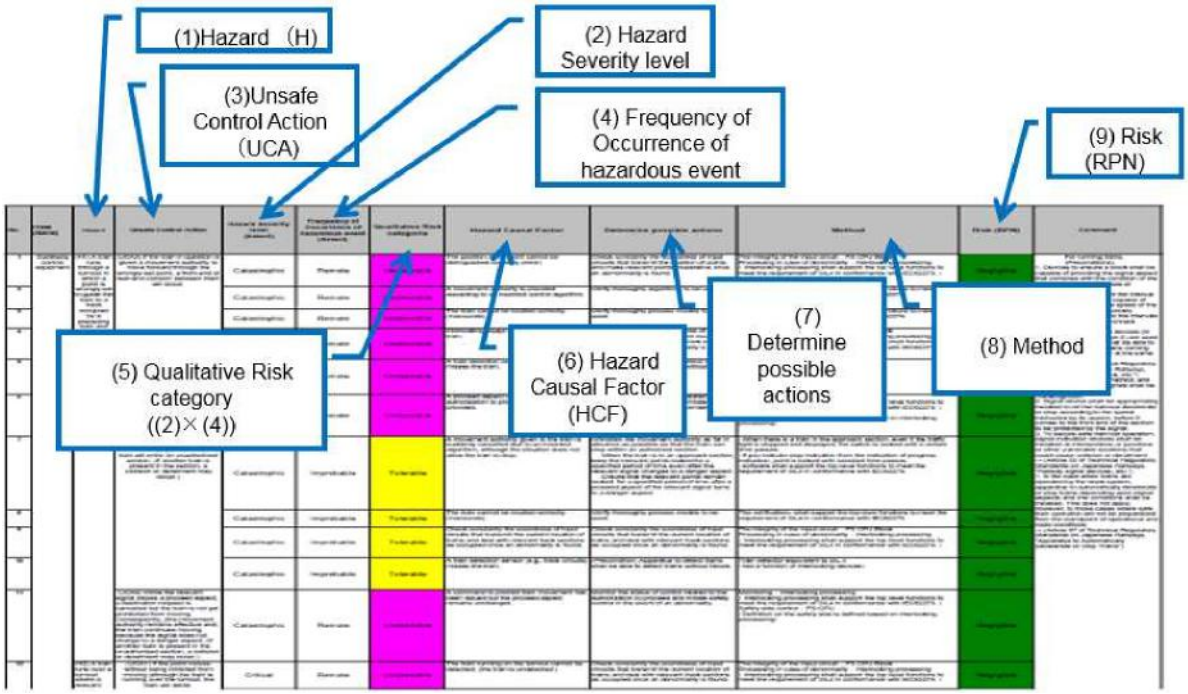

Figure 4. Risk Control Table

5 CONCLUSION

In this article, with an electronic interlocking device as a subject, safety analysis is conducted using STAMP/STPA, followed by its evaluation. Further, by referencing Phase 3 Risk analysis in railway RAMS (IEC62278), the method of supporting the conceptual design of a system is described and risk management activities to summarize the result in hazard logs is introduced. Concerning activities, a risk management process is built and deployed, means for risk detection for rendering risks visible, and for a control process are described. Also, a result is indicated as one of the activities for the safety analysis. As for the outcome, validity of the analysis can be arranged by interrelating the result with "Technical Regulatory Standards on Japanese Railways" and the "Lock based on electric lock method".

6 ACKNOWLEDMENTS

The authors would like to thank people in Kyosan Electric Mfg. for their many advices during the research.

7 REFERENCES

1. Information-Technology Promotion Agency, First STAMP/STPA,1sted., Apr.2016.
2. IEC62278:2002. Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS).
3. Railway Bureau, Ministry of Land, Infrastructure, Transport and Tourism Technical Regulatory Standards on Japanese Railways.