GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 45.060
S 04

GB/T 21562.2-2015

Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS) - Part 2: Guide to the application for safety

轨道交通 可靠性、可用性、可维修性和安全性规范及示例

第 2 部分：安全性的应用指南

Issued on: December 31, 2015 **Implemented on: July 01, 2016**

Issued by: General Administration of Quality Supervision, Inspection and Quarantine;
Standardization Administration of the People's Republic of China.

Table of Contents

Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS) - Part 2: Guide to the application for safety

1 Scope

1.1 This part of GB/T 21562 gives guidance on the safety process requirements of railway application systems specified in GB/T 21562-2008 and on the specific issues involved in the safety activities at various stages of the system life cycle (see 1.3). This part applies to all systems covered by the scope of GB/T 21562-2008. This part assumes that users are familiar with safety issues, but GB/T 21562-2008 lacks detailed guidance on certain safety issues.

1.2 GB/T 21562-2008 is the basic RAMS standard for the top level of the system. This part is a supplement to GB/T 21562-2008 and applies only to the safety issues stated in 1.3.

1.3 This part only gives guidance on the following issues within the scope of GB/T 21562-2008:

a) The establishment of top-level generic risk models for the overall system of railway application to its major components (such as signals, rolling stock, and infrastructure, etc.), the definition of model components and their interactions;

b) The establishment of general function hazard checklists for railway application systems (including high-speed lines, light rail and subways, etc.);

c) The application of risk acceptance principle in GB/T 21562-2008;

d) Application and examples of qualitative assessment of functional safety and tolerable risks in railway application systems;

e) The functional safety requirements and the definitions of assigning the safety objectives to the subsystems (e.g. railway application vehicles, door systems, braking systems, etc.);

f) The application of safety integrity levels at all stages of the system's life cycle;

Failures due to errors in any safety life cycle activity, within any phase, which cause it to fail under some particular combination of inputs or under some particular environmental condition.

[GB/T 21562-2008, Definition 3.42]

GB/T 20438.4-2006 gives a different definition of this term, but there is no substantial difference between the two, it is specifically defined as: failure to determine the cause, only the design or manufacturing process, operating procedures, documents or other related factors are modified, it is possible to eliminate this failure.

Note 1: Repair maintenance without change usually cannot eliminate the cause of failure.

Note 2: Systematic failure can be caused by simulating the cause of failure.

Note 3: Examples of systematic failures including human errors:

- Safety requirements specifications;
- Hardware design, manufacture, installation and operation;
- Software design and implementation.

Note 4: The failures of safety-related systems are classified into two types: random failure and system failure.

3.1.12

Tolerable risk

The maximum level of risk of a product that is acceptable to the railway authority.

[GB/T 21562-2008, Definition 3.43]

The railway authority (RA) is responsible for negotiating risk acceptance criteria and risk acceptance level with the safety regulatory authority (SRA) and providing it to the railway support industry (RSI) (see 5.3.2). The risk acceptance level is usually defined by the SRA or negotiated between the RA and the SRA. The risk acceptance level depends on national laws or regulations.

3.2 Other safety terms

This clause lists the safety terms not defined in GB/T 21562-2008 but used in

Although each has a different meaning, these terms are closely related to each other. To avoid misunderstandings, the following differences in these terms shall be considered:

- Failure is the termination of the individual's ability to perform the required functions;

  Note 1: After a failure occurs, the individual has a fault.

  Note 2: “Failure” is an event that is different from “fault” as a state.

- A fault is an individual condition manifested in the inability to perform the required function, but it is not included in the period of preventative maintenance, other planned actions, or loss of ability due to lack of external resources;

  Note 3: Fault is usually the cause of the individual's own failure, but it can also exist without causing any failure.

- Errors are differences between calculated, observed, measured values or status and the actually determined or theoretically correct values or states;

  Note 4: Errors may be due to fault individuals, such as calculation errors caused by fault computer equipment.

- Human errors or mistakes are human activities that produce unexpected results.

  The fault may be an incorrect signal value or an incorrect decision in the system. If a fault occurs, its resulting errors (such as incorrect information or system status) may affect the system.

  If the functional unit is no longer able to perform the required function, a failure occurs, i.e. the failure is the result due to internal errors or failures and is observable at the system boundary. Errors or fault do not necessarily lead to failures. For example, internal error checking can correct errors. Therefore, failure is only a functional problem. It is related to the effect and has nothing to do with the physical integrity of the individual.

3.2.8

Functional safety

In the normal operating conditions and fault modes that respond to external stimulus, the safety depending on the system function, as shown in 6.2.

3.2.9

SRA: Safety Regulatory Authority (as defined in 3.1.7)

THR: Tolerate Hazard Rate, also known as the "hazard occurrence rate", the risk caused by this hazard is at an acceptable level (usually judged by accepted organizations as acceptable, such as RA, RSI and SRA negotiation, or SRA itself).

4 Guidelines for the concept of related organizations / entities and systems hierarchy and safety

4.1 Overview

Considering the interaction of the system and its environment, GB/T 21562-2008 defines safety as "avoiding unacceptable risk of harm". This definition covers all aspects of safety, including functional and technical safety, health and safety issues, and human factors.

Clause 4 gives a description of the relevant organizations/entities in the railway application system. It further explains some basic concepts (such as risk, hazard, harm, and safety) in system level, safety, and risk assessment. It supplements the railway application RAMS analysis as well as the impact factors as given in 4.3 and 4.4 of GB/T 21562-2008.

4.2 Related organizations/entities in the system

Depending on the social/policy environment and organizational/management structure associated with the railway application system, there may be several organizations/entities performing different functions in each phase of the system life cycle. For the purpose of guidance, the organizations/entities are divided into three major categories (as defined in GB/T 21562-2008), as shown below (including 3.1.7):

- RA (Infrastructure management and/or railway application operator);

- SRA (Safety regulatory authority);

- RSI (System vendor/installer/manufacturer).

The roles and responsibilities of these organizations may change, or may be outsourced to some other participants or subcontractors, depending on:

- Social, policy or legal considerations;

- Size and complexity of the relevant system or subsystem;

System functions are the activities performed by the system as a whole. Function and structure are internal views that reflect the characteristics of the system and are related to the organization/entity responsible for system design. The environment consists of any object that affects or is affected by the system:

- Any objects that is mechanically or electrically connected or otherwise connected by other methods of the system, such as electromagnetic interference and heat sources;

- People and procedures that affect the system or are affected by the system during system operation.

Correct understanding of the boundary between the system under consideration and the environment as well as its interaction with the interconnected subsystems is a prerequisite for understanding how the system causes accidents and system hazards (see 6.2.2).

4.3.2 Railway application system environment and system level

Railway application systems usually operate in a socio-economic/policy environment. The economics of designing, constructing, implementing, and using the system also depend on the socio-economic/policy environment. Therefore, the system safety shall be considered from the current safety level of the system economy, the current safety level of the social environment, and the social/policy-allowed safety levels. No matter how safe the system is, systems that users cannot afford will reduce the safety in the social environment in which they are located.

Within the socio-economic/policy system, the relevant competent authorities of the railway application system are responsible for the balanced consideration of economy and safety, and formulate safety requirements and targets for the overall system safety risk level. Usually this target may not be suitable at the earlier period of the project, the organization/entity responsible for the system (such as design/configuration) can modify the target and submit it to the relevant authority for approval.

In accordance with the hierarchical structure of the system, the organization/entity responsible for the railway application system (e.g., RA) shall establish the subsystem safety requirements and goals that correspond to the levels of risk allowed by the subsystems. Typically, the responsible organizations/entities for each level of system design/configuration define the safety requirements and goals for their subsystems; in some cases, the RA establishes safety requirements and goals for lower-level subsystems or specific risks.

identified and that their management responsibilities and measures are clearly defined and properly understood by the relevant organizations/entities.

Introducing the concept of "interface hazards" is very important, because these hazards are difficult to find in a single system, but they occur when different systems interact.

4.4.1.5 Hazards at system boundary

Figure 2 describes the relationship between system boundaries, hazards, causes of hazards, and accidents (see Figure A.4 in ISO/IEC 14408:2012). This figure shows that when considering from the subsystem boundary (outside the subsystem), the failure or fault of the subsystem (i.e., the subsystem level hazard) is the cause of the system level hazard (inside the system). By using this concept, the structured hierarchical methods can be used for hazard analysis and hazard tracking in a nesting system, and for hazard identification and cause analysis at multiple system levels. This method is particularly suitable for the system development stage.

The hazards at the system boundary are only relevant to the function of the system under consideration. The description of hazards should consider all interactions with other related systems, these factors may reduce the hazards. Two examples are given below:

a) If a subsystem-related hazard is monitored by other subsystems, the safety requirements for the hazard should consider the mitigation measures implemented by the monitoring equipment and the subsequent risk time;

b) At the subsystem level, the occlusion of axle-boxes on high-speed trains can be regarded as a hazard. If the vehicle is running on a line with equipment monitoring (e.g., a shaft temperature detector), the safety requirements for the hazard should consider the presence of the monitoring equipment and the subsequent risk time.

Therefore, allocating safety requirements within the system is a detailed process that may require repeated iterations to ensure that the relevant responsible parties (such as the team responsible for the development of subsystems) correctly understand the safety requirements.

control risk), so these factors shall be considered comprehensively to establish risk tolerance criteria.

For the railway application system, the relevant authorities can classify people exposed risks in different ways, for example, they can be divided into three groups: passengers, railway application workers (i.e., personnel hired or contracted by RA or RSI, or authorized by RA to perform railway application specific tasks), and the general public. In these groups, the risk acceptance criteria for the three groups may be different due to the different levels of association with the system and the differences in capabilities that result in different risks. At the beginning of the project, it is advisable to consult with the relevant competent authorities to determine the specific criteria.

The level of risk faced by each group may also be affected by many factors. These factors include:

- Personnel exposure, such as the duration and frequency of contact hazards of personnel, as well as the probability of the personnel exposed to hazards to identify hazards, make timely response and actively take measures to avoid accidents;

- The duration of the hazard, such as the duration of the hazard, and the probability of the person being exposed to the hazard;

- Risk-triggering events and/or conditions that may cause accidents, as well as the overall possibility and probability of occurrence;

- A series of events/conditions of the triggering events or follow-up triggering events that may cause accident, and the accidents that result from it are less likely to occur as a whole but the consequences of the accident are serious.

Figure 3 shows an example of the above factors causing the accident to expand. It shall be noted that safety barrier (protection) measures can be set at the hazard level, triggering event level or accident level to reduce the risk. Triggering event and failure of safety barrier are necessary conditions for the accident.

consistent with the basic measurement method, to facilitate risk communication and comparison. For example, the damage occurrence rate depends on the number of people affected (such as the number of employees involved in maintenance and the number of working hours, etc.), traffic density, train mileage, passenger mileage, train or passenger hours, number of trips, number of train operations and landforms (such as number of tunnels, bridges, and crossings). The following subclauses outline the basic concepts of normalization.

4.4.3.2 Event rate (reference base for probability of occurrence)

The RA and the relevant SRA shall, through negotiation or based on the generally acknowledged principles, determine the harm/death rate of different groups affected by railway application. This rate is only used as a reference for event processing and comparison. For example, the unit rate of risk for passengers and public groups can either use the yearly accumulative injury of each group as the basis, or convert it into individual risk.

4.4.3.3 Equivalent death (injury reference basis)

See definition in 3.2.6. The RA and SRA shall make negotiation to determine the relationship between the number of injuries and the number of deaths. This rate is only used as a reference for event processing and comparison. For example, the conversion formula can be: 1 equivalent death = 1 death = 10 major injuries = 100 minor injuries.

5 General risk models and common functional hazard checklists for typical railway application systems

5.1 Overview

This clause introduces the concept of a general risk model, gives guidance on the risk assessment process and application, and gives a hazard checklist.

The railway application system presents many characteristics in the course of transportation services, among which safety is more stringent than forecasting, management and delivery, directly affecting the railway application system and related companies. The social law/regulatory system imposes further restrictions on the performance of the railway application system, to control the human or environmental damage caused by the product or system. Historically, the improvement of safety has been achieved through tragic accident lessons. Today, it systematically focuses on the root causes of safety issues, expands the scope of considerations, understands safety issues in depth, and solves problems in a more proactive manner. The method of drawing lessons from the accident can continue to be retained, but it is not an ideal safety method.

A systematic approach to safety requires an understanding of the risk assessment process, while understanding the structure of the railway application system and its interaction with the environment. Clause 5.3 gives a description of the risk assessment process, and clause 6.2.2 describes the structural principles of the railway application system and other relevant factors.

Clause 5.4 gives some guidance on the depth and type of necessary risk assessment.

5.2 General risk model

Modeling is primarily a simplification and generalization of reality, in order to understand causality and highlight important factors. Modeling is an effective tool for estimating and forecasting the future.

It can create risk models for specific tasks (e.g., hazard occurrences, hazard combinations, operations, subsystems, etc.) in accordance with the risk assessment process for specific applications or the entire railway application system.

Establishing risk prediction/description models for products, processes, or systems is a major step in systematically understanding risk and early safety management. The model essentially appears as an abstract view of the system, irrespective of its qualitative or quantitative characteristics, it should satisfy the following requirements in order to facilitate the implementation of the safety process:

- A systematic description negotiated and agreed by all stakeholders;
- Explicit system elements, boundaries and key external and internal interfaces, preferably using graphic representations;
- Support the construction of a safety-related decision-making environment, while providing a comprehensive record of the system's life cycle.

Most risk assessments only consider the risks of passengers. Because safety risks are directed at people, it is important to identify all affected groups and determine their tolerable risks. Establish a safety risk assessment for all groups that come into contact with the railway application system, assess the risk of each group based on a consistent baseline (such as yearly or per trip/train mileage).

Establishing a risk model for the entire railway application system involves a large amount of work, and due to the diversity of the environment, operations and interfaces with other systems of railway application systems, the differences and quality of available data, the complexity of models, and the overall availability of integrated model tools, as well as for large and complex models that are difficult to identify, it is not appropriate to give a general risk model for the overall railway application system. The remainder of this clause only presents the general risk assessment process and its application, and gives a hazard checklist.

Depending on the purpose of the analysis, risk models that are evaluated using quantitative, qualitative, or synthetic methods are used at different system levels, to perform basic function assessment for the higher level functions and assess the technical plans of the lower level functions.

Appendix D lists the basic steps for establishing a risk model and a graphical example of a railway application system risk prediction model.

5.3 Risk assessment process

5.3.1 Overview

Risk assessment mainly includes hazard identification, risk assessment and risk tolerance judgment. Risk management includes identifying and implementing economic and practical risk control measures, and ensuring that resources are continuously used to control and maintain risks at an acceptable level.

Risk analysis is an important part of the life cycle of the entire system shown in Figure 8 of GB/T 21562-2008 and shall be carried out at different stages of the life cycle. Clause 6.4 of GB/T 21562-2008 gives a summary description based on basic risk concept and risk analysis, assessment and acceptance. The above “risk assessment” includes the “risk analysis”, “risk assessment and acceptance” in 4.6.2 and 4.6.3 of GB/T 21562-2008. The “risk analysis” in the system life cycle shown in Figure 8 of GB/T 21562-2008 shall be regarded as a “risk assessment” in a strict sense, clause 5.3.2 gives a further description of the general risk assessment process, clause 5.4 gives the guidance on the process application and analysis depth and breadth.

Risk assessment using qualitative, quantitative or comprehensive methods is a systematic and structured approach, which is used for:

a) Identify incidents that can directly or indirectly cause casualties related to the operation and maintenance of the system; in the railway application operating environment, these personnel may be passengers, workers or members of the public;

b) Identify hazards that can lead to an accident, i.e. component/subsystem or system failure, physical effects, human error or operating conditions;

c) Formulate measures to deal with or limit all types of hazards that cannot be eliminated;

d) Estimate the frequency of hazards and accidents (if feasible);

e) Estimate the consequences of the accident in the form of casualties. If the risk needs to be reduced, take measures to control or limit:

- Various types of hazards that cannot be eliminated by identifying the cause and accident triggering conditions;

- The consequences of related accidents;

f) Estimate the overall risk associated with a major accident;

g) Estimate the individual risk associated with the exposure group (if feasible);

h) It shall determine the additional measures necessary to reduce the risk to an acceptable level of SRA (e.g., meet the established risk acceptance criteria);

i) Give documents that fully demonstrate the risk assessment methods, assumptions, data, judgments and descriptions.

5.3.2 General procedures

5.3.2.1 Overview

The general procedure is divided into two major steps:

a) The risk assessment process, which consists of the following components:

- System definition;

- Hazard identification, including hazard records;

- Consequence analysis;

- Risk assessment and THR apportionment under appropriate conditions.

b) Hazard control procedures: Hazard control, including causal analysis and common cause analysis.

The execution of the entire process requires an in-depth understanding of the system and its functions, design, operation, maintenance and operating environment. The main responsibility of each procedure is mainly determined by the scope of the organization/entity’s influence on the system or the

5.3.2.2 System definition

The system and its physical and logical boundaries (the interface between the system and other systems and environments) shall be clearly defined. Understanding the boundary between the system and the environment is a prerequisite for understanding how the system causes accidents. The environment includes anything that can affect the system and be affected by the system, such as other systems connected to the system (mechanical, pneumatic, and electronic, etc.), or things that affect through electromagnetic interference, voltage fluctuations, and heat exchange; the environment also includes personnel and programs that may affect system or be affected by system.

A.1 gives further explanation of the system definition.

5.3.2.3 Hazard identification and preliminary hazard analysis

Hazard identification is the basis of risk assessment. In all best practice models for safety engineering and management, hazard identification is a critical step in the overall safety assurance. The lack of systematic and comprehensive identification of hazards can seriously affect the risk assessment process. In the most unfavorable situations, it may also create safety illusions and false sense of trust.

Hazards should be systematically identified to ensure that people, processes, and systems work patterns (normal, degraded, and emergency modes) are covered, and that the results are collated and recorded; then analyzed to eliminate correlations; and grades are assessed based on the impact of each hazard, finally, a set of trusted “C-hazards” with different levels of severity is defined at the railway application system level. Although systematic processes can increase the integrity of hazard identification, they do not guarantee integrity.

All stakeholders should consult and reach consensus on the actual scope of hazard identification activities. In some cases, it may be appropriate to limit the analysis to hazards that can lead to personal injury, but in other situations (such as transporting dangerous goods), it may be more reasonable to include other types of harm in the analysis.

The hazards shall be listed after the hazards have been determined. The hazard information is usually updated in the hazard record (see 5.3.2.4).

Often single hazard is associated with multiple causes. If a large number of hazards are identified, it shall be checked whether the multiple causes of the individual hazard have been identified one by one.

A preliminary hazard analysis is carried out to classify hazards in accordance with a severe sequence of risks, thereby concentrating risk assessment

Consequence analysis is the establishment of intermediate conditions/events and evaluation of hazard development (taking into account any accident triggering factors and/or possible events that may cause the associated losses to rise, for example, after a train derails, there may be a collapse of the bridge on the train, a fire, or release of toxic substance), so as to assess the probability of a “C-hazard” that leads to the accident and the extent to which the accident could result in a loss.

A.4 gives further explanation of the consequences analysis.

5.3.2.6 Risk assessment and apportionment of THRs

Risk assessment and assessment are based on risk acceptance criteria. The risk acceptance criteria shall be based on legal or other requirements agreed by the SRA (e.g., major legal requirements, existing technical standards, existing safety systems or processes, etc.). Clause 7.2 explains how to adopt the relevant technical standards or reference systems as guidelines for approval of safety certification. It shall be based on the risk acceptance criteria to introduce the risk reduction and/or risk avoidance measures, so as to reduce unacceptably high risks to acceptable or tolerable levels. Risk acceptance criteria can also be given qualitatively.

Based on the estimated accident rate and accident-related loss tolerance, the value of the hazard rate for identifying the hazard is recalculated and each hazard tolerance THRs is determined (see 6.3.3). THRs are inputs for hazard control.

There are some situations where it is difficult to determine the THR value:

- For mechanical parts that depend on the material's durability and design tolerance properties during the specified product life cycle;
- Electrical hazards that rely on technical measures (to avoid electric shock and induced voltage) may depend on the insulation and grounding design; in this case, it is difficult to determine the frequency of failure and the measurable hazard rate;
- It is almost impossible to determine the THR in the operational management part (including operators and maintenance personnel, etc.).

For these situations, it shall decide whether to use THR or THRs.

As the responsible agency, the RA shall carry out risk assessment at the railway application system level and shall define the THR of general applications of public systems based on the results of the assessment, that is, the maximum acceptable rate of occurrence of hazards, and it shall meet the requirements of laws and regulations and public safety objectives.

5.4.2 Analysis depth

GB/T 21562-2008 applies to the entire railway application system or subsystem, but the degree of analysis required for safety demonstration depends on the specific subsystem, the degree of inspection in the application, the novelty of design or application, environmental differences, and system boundary condition difference, interface differences, and risk level factors that are presented, so safety demonstration work should be appropriate and sufficient to meet these conditions. The safety plan should specify the depth of analysis and methods for determining the depth of analysis.

The level of detail of the risk assessment shall be commensurate with the risk. Risk assessment does not categorize every trivial hazard and does not expect to identify hazards that exceed the current level of knowledge. Appropriate and adequate risk assessments should be able to reflect a reasonably viable forecast of railway application hazards and reflect the hazards associated with the technologies used (e.g. functional and technical safety). Where practicable, the risk assessment shall be linked to the accident history and cause records.

Due to the large scope and scale of risk assessment, it is difficult to define “appropriate” and “sufficient”, and it is advisable to avoid excessively high accuracy requirements. See 7.2 for guidance on safety proof methods.

The risk assessment process should adopt both qualitative and quantitative assessment methods.

Qualitative risk assessments may satisfy most hazard analyses. Risk ratings (see A.6) can be used to identify the risks that require more in-depth assessments. The sensitivity analysis (see 5.4.6) can also be used to obtain a depth of in-depth assessment. However, hazards that may cause major or catastrophic consequences shall be assessed in whole or in part for quantitative risk, to determine the degree of risk, and help reduce systemic risk. If there are quantitative safety requirements (such as the signal system referred to in GB/T 28809-2012), quantitative risk assessment shall be used. Because the new system lacks sufficient experience to support empirically based qualitative assessment methods, quantitative methods can be used for new systems.

For practical cases, quantitative risk assessment should be considered. Evaluating risk is particularly difficult for accident types that are rare but have serious consequences, such as catastrophic rail traffic accidents. The frequency and severity of some accidents may be very sensitive to little-known factors, and predictive uncertainty is very important for these situations.

The stakeholders (organizations/entities) of the system shall be informed of the role and significance of qualitative risk assessment in the following areas:

- Raise awareness of such incidents;

It should create a risk rating matrix (see A.6 and Table E.2) based on the results of the preliminary hazard analysis and determine whether a more detailed analysis (qualitative or quantitative analysis) is required.

When determining the scope, function, and design of the system, it can continuously improve the hazard identification, analyze the causes and results of the hazards, and finally perform the risk assessment.

During each phase of the project, it is advisable to use the available information for analysis as much as possible to give the best decision support, such as whether there are new hazards during and the possible risks of these hazards the implementation, maintenance and operation of the system.

5.4.4 Qualitative risk assessment and quantitative risk assessment

5.4.4.1 Overview

The risk assessment process defined in 5.3.2 is based on a risk assessment framework that can support qualitative, quantitative, or integrated approaches.

Qualitative risk assessment is suitable for systematic failures and is the earliest subjective judgment. Quantitative risk assessments are only used for random failures. Comprehensive methods such as semi-quantitative methods can also be used.

In the above method, if the results are obviously conservative (not underestimating the risk), approximate methods can be used.

In addition to determining safety requirements using the methods described above, risk assessment can be performed through qualitative methods based on existing technical standards, similar systems that are recognized, credible experience, and the judgment of industry experts.

5.4.4.2 Qualitative risk assessment

Qualitative risk assessment mainly depends on the judgement and credible experience of industry experts, and deals with risks in a subjective and crude way. It should carry out risk assessment process to a sufficient depth so that the subjective assessment covers all possible hazards. There is no complete non-quantitative assessment, which is usually done using orders of magnitude.

The advantages of qualitative risk assessment are:

- No detailed quantification, data acquisition or analysis required;

- Simple;

- It is not expensive as relative to quantitative risk assessment.

- Not suitable for assessing systemic failures;

- More expensive than qualitative risk assessments;

- May require a lot of resources.

Qualitative risk assessment can be used to assess most hazards, but for hazards that may cause major or catastrophic consequences, it may be necessary to determine the risk level and help reduce systemic risk through quantitative risk assessment. When selecting quantitative safety requirements (e.g., implementing the signal system of GB/T 28809-2012), it shall use the quantitative risk assessment. The quantitative methods can be used in new systems because the new system does not have enough experience to support empirically based qualitative methods.

Quantitative risk assessment is more time-consuming and resource-intensive than qualitative risk assessment, it is used only when greater credibility is needed.

5.4.5 Using historical data

Risk assessment always depends on some inferences from the past to the future. Historical data can be used for multiple stages and can also be used to check the effectiveness of the risk model when building a risk model. it shall carefully use historical data for the following reasons:

- It is difficult to determine the environmental information of historical data, especially for rare accidents or catastrophic accidents and the environment surrounding early events;

- It is difficult to identify secondary disasters (such as fire, derailment or leakage of hazardous substances) caused by the incident.

Improper use of historical data may affect the effectiveness of the analysis and significantly reduce the risk assessment accuracy.

When using historical data in an assessment, it is advisable to give a clear argument that its use can accurately predict the losses associated with a particular environment.

5.4.6 Sensitivity analysis

When performing risk analysis and subsequent analysis of tolerance, assumptions shall generally be made; due to the lack of data, the quantification of hazard frequency/probability and accident consequences can only be given through judgment, so the methods of assumption and judgment are to a large extent determine the overall risk and tolerance assessment results. Sensitivity analysis can be used to manage the impact of these assumptions and objectives, and safety requirements. At the subsystem level, RSI is responsible for designing/providing equipment and establishing safety objectives and safety requirements for lower-level subsystems/equipment (see 4.2 and 4.3). These safety requirements shall also include the safety requirements for maintenance and operations.

At the beginning of the project life cycle, the information obtained is usually insufficient to support detailed risk assessments, and the analysis is usually limited to the initial identification of hazards, but early discussion of each risk control method can be made. It is advisable to conduct a preliminary hazard analysis before starting a major design activity (see 5.4.3), but the function and structure of the relevant system as well as the interface of the system with personnel and other systems shall be determined in detail before the evaluation.

Risk assessment is a repeated process. As the design is carried out, it is advisable to repeat the assessment at appropriate stages of the design process and to make the assessment to the appropriate depth (see 5.4.2), to cover the changes that have occurred and more details. If a hazard is identified, the design can be modified to eliminate the hazard or reduce the risk.

Phases related to repeated risk assessment shall be recorded in the safety plan. The hazard records should be updated at each stage (see 5.3.2.4) to supplement any newly identified hazards and reflect the status of all hazards, as detailed in stage 1 ~ stage 10 of clause 9.5 and Table 7.

The hazard record should be established at the earliest stage (see 5.3.2.4) and updated at all stages of the project's life cycle.

5.4.7.3 Risk assessment in maintenance and operations phase

Stage 11 of GB/T 21562-2008 covers this assessment, the responsibility for safety at these stages shall be transferred to the relevant organization/entity (see 6.11 of GB/T 21562-2008).

The organizations/entities involved are usually the RA or representatives designated by the RA, but in accordance with the contractual arrangements, the relevant RSI may be required to assume the tasks (see 3.1.7 and 4.2), such as the design, construction and operation as specified in the contract.

For risk assessment, the hazard record and safety requirements in the early stages of the project are the beginning of risk control during maintenance and operations. Safety requirements should include all operational and maintenance information and documentation, including specific training information, eligibility requirements information, specific equipment and facility information. This information shall normally be given by the organization/entity responsible for project design and implementation.

Identifying hazards and eliminating them or reducing them are important risk countermeasures. In order to ensure effective processes and support mutual recognition of safety systems, a common hazard grouping structure should be determined through negotiation.

Ideally, the hazard grouping structure shall meet the following requirements:

- Cover/target the entire railway application system;

- Hazard descriptions help with subsequent hazard identification and cause determination;

- Highly clear;

- Support coverage verification;

- Allow responsibility apportionment for each hazard and its causes;

- Facilitate apportionment of quantified safety goals;

- Can be used by RA or RSI;

- Support assigning risk objectives to system hazards and further assigning THR to lower level functions;

- Improve the efficiency of hazard identification and hazard elimination processes;

- Facilitate comparison of safety analysis results.

Defining a structure that takes into account all the needs of all parties involved is difficult to achieve. At present, safety professionals face a large number of unstructured methods, or multiple types of structures from different perspectives. A widely accepted grouping structure may not be realized.

However, there are different methods used for the hazard grouping structures at the railway application system level, each with its own advantages and disadvantages. The grouping structure shall be further subdivided into lower functional levels, to meet the needs of stakeholders.

Here are some examples of grouping structures:

a) Perform hazard groupings based on the main components of the railway application system (logical decomposition of the railway application system), such as infrastructure, energy, locomotives, control commands and signals;

b) Perform hazard groupings based on their responsibilities, such as RSI, operators, maintenance personnel, and other responsible owners;

and describe it in B.2. This study focuses on identifying the key hazards of railway application safety operations from the perspective of passengers, staff, and neighbors. Based on a large number of identified hazards, they are incorporated into an advanced group called “C-Hazard”, which simplifies hazard analysis without compromising coverage and makes hazard analysis more reasonable.

- Other hazard structures at the railway application system level as shown in B.3 are merged into the following two groups:

  • Identify hazards from a functional perspective;

  • Identify hazards such as overheating, smoke, fire, and electromagnetic interference from the perspective of inherent characteristics.

The functional hazards can be defined in a generic way and used for different elements of the railway application system. For example, the “staying damage” in functional hazards can be used by passengers in trains and operators in signal control rooms.

The hazards produced by inherent characteristics are not related to a specific function, but are related to the inherent characteristics of the technology used (i.e. technical safety and non-functional safety, see 6.2). For example, gated devices may cause electromagnetic interference, but the interference is not due to gating functions, but due to the inherent characteristics of the equipment used (electronic microprocessor devices).

5.5.3 Hazard checklist

B.1 gives a general checklist of hazard identification. B.2 gives an example of a “C-Hazard” checklist after a macro study of a specific railway application. As a general example of analysis, B.2 has identified these hazards at the level of the entire railway application system, and these hazards are generally independent of specific causes (e.g., functional and technical failures). At the railway application system level, hazard identification shall also be carried out for specific groups exposed to risks in system operations.

B.3 gives an example of a function-based hazard identification method. It describes the hazards associated with the identification of environmental conditions and the relationship between railway application system functions and major subsystems. However, it is only an example and not a complete list.

The system-level hazard checklist can only be used as a supportive tool for project or specific hazard identification, it cannot replace necessary safety activities. If system elements, boundaries, and interfaces are defined and risk identification is performed at the functional or implementation level, it is advisable to identify the specific groups exposed to the risks in the system and behavior and may need to supplement the characteristics that determine its performance level (such as reliability, safety, accuracy and real-time, etc.), or it may further verify the relationship between the system and the environment based on relevant requirements (such as the operation and maintenance conditions as shown in Figure 4 of GB/T 21562-2008). Requirements shall specify issues such as distribution of system tasks, maintenance and logistics, human factors (such as personnel qualifications), process environmental conditions, and costs.

The technical implementation of the system can generate other requirements that are not related to system functions. These requirements are called "technical requirements." Technical requirements (e.g., maintainability, environmental conditions, and potential threats caused by the technology/equipment) affect the construction of the system and may involve issues that are not related to functionality (e.g., the existence of sharp edges, voltages, and flammable materials, etc.).

In order to achieve the functional requirements of the system, the design shall be refined into the design of subsystems and equipment. To ensure compatibility between different subsystems/devices, functional requirements shall be refined and technical and other requirements shall be increased accordingly. For the structure of the railway application system that fulfills the functional requirements, see clause 6.2.2.

The characteristics of the system and its elements (user-related features derived from functions, technologies, and related requirements) shall be guaranteed to meet the requirements. System implementations (i.e., technical solutions) may generate additional features introduced by the design (referred to as implementation features).

6.2.2 Railway application system structure and safety requirements

The following is a typical hierarchical system structure of the “railway transportation system”, which will be hierarchically subdivided into physical subsystems. Subsystems at all levels usually refer to those systems that are purchased separately in the traditional railroad market. The railway application system can be divided into similar subsystems:

- Infrastructure (such as tracks, stations, turnouts, level crossings, and civil works, etc.);

- Energy sources (such as power supplies, contact networks, substations, etc.);

- Locomotives;

- Control, command and signal.

The goal of functional and technical safety is:

- Design and build system functions to achieve an acceptable level of safety (referred to as functional safety);

- Its implementation does not produce undesired/unacceptable characteristics (referred to as technical safety).

In accordance with the hazard activation mode, the safety-related features can be classified as follows:

- Inherent risk is usually related to system tasks. For example, at level crossings, the inherent risk is that the interaction between railway application and road traffic may lead to a conflict between railway application and road traffic;

- Danger of degradation of system performance (such as failure of one of the components and excessive wear, etc.), such as train detection device used to control level crossings fails to detect the train passed by;

- Risk of improper response to external threats or stimuli, such as traction transformers containing flammable materials (which emit a large amount of heat in the event of a fire) may threaten the safety of passengers when the train is in a tunnel fire.

For systems, subsystems and equipment, functional and technical requirements that reduce risks to acceptable levels shall be consolidated into safety requirements. These requirements can include SI requirements, which can be defined as quantitative or qualitative requirements.

There may also be other qualitative safety requirements, such as compliance with external standards, relevant regulations, and implementation guidelines. Meeting the following requirements can be included into safety requirements:

- Assume that these requirements are met when calculating safety objectives;

- Additional compliance requirements to reduce risk to an acceptable or tolerable level.

System implementation (functions, technologies and impacts) should comply with safety requirements, to ensure safety and demonstrate that the system meets all safety requirements before commercial operations.

Note: Overall system safety considers the overall performance of the system and does not allow disaggregation of safety. Different aspects of safety (e.g., functions, technologies, procedures, and human factors) are interrelated and shall therefore be treated as a whole and be included into safety arguments.

Appendix D

(Informative)

British railway system risk model diagram

D.1 Building a risk model

To construct a risk model, it should use the following basic steps (examples) consistent with the risk assessment process (see clause 5.3):

a) Graphical representation of the systems to be analyzed, key elements, boundaries, internal and external interfaces, application environments, and interactions;

b) Use graphical representations for preliminary hazard identification to ensure that people and processes are taken into account, as well as normal, degraded and emergency operating modes;

c) It should describe and graphically represent the key functions of the system and the interaction of the system with the outside world;

d) Use functional descriptions to identify more detailed hazards;

e) For each identified hazard, maintain a unique numbered record (hazard record), and obtain the cause, consequences, possible risk estimates using the rating form, affected personnel, and possible actions;

f) Merge synergistic hazards, that is to say, the hazards with common or actual relationship are combined into groups and categories and marked as “C-hazard”;

g) Develop a graphical representation of each “C-hazard” chain of causes to ensure that all detailed hazards are assigned to the group under consideration; the chain of causes (cause models) should determine the logical combination of causes to help understand “C-hazard”, including failure of common cause, personnel and subsystems;

h) Under the operating conditions, and under the protection existed in detections, procedures and occasional mitigation measures, carry out a graphical representation of possible upgrades for each “C-hazard”; the consequences model indicates possible outcome events, which may be due to the incidents and accidents caused by the given “C-hazard”;

i) Combine each “C-Hazard” cause and consequences models into one model for the entire UK railway infrastructure and operations was developed at the railway system level. The so-called risk distribution study is based on a number of industry-level hazard identification experiences, and is carefully designed, planned, and implemented through the extensive participation of railway application industries (i.e., RSI and RA). These human-centered studies carefully examine and identify precursors to accidents from the perspective of operating a specific risk group for railways (passengers, staff, and neighboring people), develop safety models based on predictive risks, and provide complete predictions for the railway infrastructure and operations throughout the UK. Establish a “C-Hazard” superset through reasonable organization and conduct analysis of causes, consequences, and losses. When dealing with safety risks, the human-centered method is more suitable for railway systems than failure-based approaches (usually as system safety guidelines).

D.2.2 Modeling techniques

D.2.2.1 Overview

Most quantification models have a rather strict but very inflexible structure, and are not easy to manipulate and perform what-if analysis. The process of building a component model is essentially modeling. Each module (“C-hazard”) consists of quantitative logic structures, that represent the cause chain (cause analysis) and the diffusion scenario (consequence analysis), that is, the prediction of the final accident and event scope and its associated frequency. The frequency and risk of accidents and incidents of each module are summarized by means of tools to form a risk prediction. In order to increase the flexibility of the model structure and avoid creating too many model variables for the intermediate stage of the product or project, it has developed a new method called parametric modeling, to make the investment required for different designs and models of different environments more reasonable.

D.2.2.2 Parametric modeling

The predictive model consists essentially of logical structures that are constructed from a set of hazards or “C-hazards” and related data. If a logical structure has been obtained and reviewed and merged, it is encapsulated and protected through strict configuration control to prevent changes, but the data may be more easily changed than the logical structure of the model, so it requires a new method to put the data into the model. In the predictive quantitative risk model, the basic failure rate can be used as a variable, and the protection strength can be used as a mathematical expression, to evaluate the supplemental data, so that it requires neither a large amount of input nor a variety of models and structures, to obtain different predictions. To reduce the modeling and transformation costs, a single environment can be used. Decomposing data from the internal model structure as much as possible will help ensure the integrity of the data and facilitate the acquisition and review of

Appendix G

(Informative)

Example of establishing risk acceptance criteria

G.1 Example of ALARP application

The following example shows how to apply the ALARP principle.

GB/T 21562-2008 has given the basic idea. Table 6 of GB/T 21562-2008 shows a risk matrix with four risk areas:

- Intolerable;

- Unwanted;

- Tolerable;

- Ignorable.

In the ALARP principle, “intolerable” and “unwanted” are classified into the same type (that is, this is an unacceptable risk area), so only three areas are used:

- Unacceptable, this is equal to an unacceptable area;

- Tolerable, this equals the ALARP area;

- Negligible, this equals a broadly acceptable area.

The basic idea of risk assessment is as follows:

- Reduce unacceptable risks (impossible to approve);

- Negligible risk without further reduction;

- Assessing or calculating risk in “tolerable” areas requires further study of whether increased risk reduction measures can transfer risk to negligible areas and the actual effort required for such safety improvements.

The yellow book of the British engineering safety management system (see reference [21]) describes risk assessment as a process with the following seven stages (see 5.3.2, these processes are in principle the same, but combine some stages together):

a) Hazard identification: identification of specific hazards;

- Mitigate the consequences of accidents (such as motorcycle safety belts) (arrow 1 in Figure G.1);

- Reduce the probability of accidents by increasing safety barriers or using more reliable components (arrow 2 in Figure G.1);

- Perform both (arrow 3 in Figure G.1).

The following examples are non-targeted and will not be specific to a particular application or technology. These examples (see reference [24]) are based on TUEV workshops.

Assume that the system analysis shows that for a particular risk, it has the following characteristics:

- In the event of an accident, the average loss of the estimated damage is 1000000 yuan (if the person is slightly or moderately injured, or the equipment and articles are damaged);

- The estimated accident rate is 4 x 10^{-3}/year;

- Running time is 10 years.

In accordance with ALARP, which of the following options is most effective:

- Option 1: Risk reduction is performed by monitoring equipment to control the safety of the process. Assume that this will reduce the accident rate to 2 x 10^{-4}/year, the value of this equipment is 30000 yuan.

- Option 2: Implement protective measures. This can reduce the damage from 1000000 yuan to 500000 yuan. The measure is worth 6000 yuan.

- Option 3: Improving operating instructions and warnings can reduce the risk time and increase safety awareness. It is estimated that the accident rate can be reduced by 50%. The cost is 1000 yuan.

- Option 4: Add control personnel to continuously monitor the process. It is estimated that this will reduce the accident rate to 1 x 10^{-5}/year. The cost of this person is 25000 yuan/year.

The solution can calculate the actual total risk (10 years) in accordance with formula (G.1).

Risk = Annual incidence × Loss of harm × Number of years..........(G.1)

Risk 0=4 x 10^{-3}/year x 1000000 yuan x 10 years = 40000 yuan (risk 0 means risk when no mitigation measures are taken)

For option 1:

References

[1] GB/T 7826 Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)

[2] GB/T 20438.5-2006 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 5: Examples of methods for the determination of safety integrity levels

[3] GB/T 25162.3 Railway application - Reliability, availability, serviceability and safety specifications and examples - Part 3: Locomotive RAM application guide

[4] IEC 60300-3-1 Dependability management - Part 3-1: Application guide - Analysis techniques for dependability - Guide on methodology

[5] IEC 60300-3-9 Dependability management - Part 3: Application guide - Part 9: Risk analysis of technological systems

[6] IEC 61025 Fault tree analysis (FTA)

[7] IEC 61078 Analysis techniques for dependability - Reliability block diagram method

[8] IEC 61160 Formal design review

[9] IEC 61165 Application of Markov techniques

[10] IEC 61703 Mathematical expressions for reliability, availability, maintainability and maintenance support terms

[11] IEC 61882 Hazard and operability studies (HAZOP studies) - Application guide

[12] ISO/IEC guide 51 Safety aspects - Guidelines for their inclusion in standards

[13] CLC/TR 50506 (all parts) Railway application - Communication, signaling and processing systems - Application guide for EN50129

[14] Deterministic and Probabilistic approaches in Risk Analysis. The Walloon Region's hybrid approach. G. Van Malder

[15] Monte Carlo Simulation in Environmental Risk Assessment Science, Policy and Legal Issues. Susan R. Poulter, University of Utah College of Law

[16] Information theory, Inference, and learning Algorithms. On-line textbook by David MacKay. http://www.inference.phy.cam.ac.uk/mackay/itila/book.html

[17] Probabilistic Risk Assessment: What Is It and Why Is It worth Performing It? Dr. Michael Stamatelatos, NASA Office of Safety and Mission Assurance

[18] NPRD-95-Non-electronic Parts Reliability Data (published by Reliability Analysis Centre) and NSWC-94/L07- Handbook of reliability prediction procedures for Mechanical Equipment

[19] Krebs, H: Minimale Endogene Mortalitat-einuniverselles Sicherheitskriterium, ETR 49 December 2000

[20] Schabe, H: Different Principles Used for Determination of Tolerable Hazard Rates, Contribution to the WCRR 2001

[21] Engineering Safety Management Systems, Yellow book; Published by Railtrack on behalf of the UK rail industry (RSI and RA)

[22] Procedures for formal design reviews: with emphasis on RAMS, using some general and application specific checklists as appropriate. e.g. IEC 61160

[23] Procedures for performing hazard & safety/risk analysis. Some of these are described in:

US MIL HDBK 882D System safety program requirements

US MIL HDBK 764(MI) System safety engineering, design guide for army materiel

UK Def Stan 00-56 Safety Management Requirements for Defense Systems, UK Ministry of Defense

[24] TUEV Seminar: given by the German “RW TUEV Information stechnik, Dept. Safety Approval Services” (example included with their kind permission)

[25] Leveson, N.G.: Software - System safety and computers, Addison-Wesley, 1995 (hazard concept)

[26] Kumamotu, H and Henley, E.: Probabalistic risk assessment and management for engineers and scientists, IEEE press,1996 (general risk concept)

[27] Schneider, J.: Sicherheit und Zuverlassigkeit im Bauwessen, Teubner, Stuttgart, 1996 (risk assessment of other technologies)

[28] Abernathy: The Weibull Handbook, 2002 (general failure rates)

[29] System Safety Analysis Handbook, 2nd edition, System Safety Society, 1998

[30] Villemeur, A.: Reliability, Availability, Maintainability and Safety Assessment,

This is an excerpt of the PDF (Some pages are marked off intentionally)

Full-copy PDF can be purchased from 1 of 2 websites:

1. https://www.ChineseStandard.us

- SEARCH the standard ID, such as GB 4943.1-2022.
- Select your country (currency), for example: USA (USD); Germany (Euro).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Tax invoice can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with download links).

2. https://www.ChineseStandard.net

- SEARCH the standard ID, such as GB 4943.1-2022.
- Add to cart. Only accept USD (other currencies - https://www.ChineseStandard.us).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with PDFs attached, invoice and download links).

Translated by: Field Test Asia Pte. Ltd. (Incorporated & taxed in Singapore. Tax ID: 201302277C)

About Us (Goodwill, Policies, Fair Trading…): https://www.chinesestandard.net/AboutUs.aspx

Contact: Wayne Zheng, Sales@ChineseStandard.net

Linkin: https://www.linkedin.com/in/waynezhengwenrui/

------ The End ------