David VALIS, Miroslav KOUCKY
University of Defence, Czech Republic
Technical University of Liberec, Czech Republic

RAMS PROGRAM IN RAIL APPLICATIONS – BRIEF INTRODUCTION

Key words

Safety, RAMS, risk assessment, rail applications.

Summary

Dependability and safety assurance is an essential part of the programme providing technical object quality. Because product improvement should become a continual effort of manufacturers, this aspect should not be dealt with only on the grounds of necessary certification procedures given by standards. Within the scope of technical systems there is introduced the programme RAMS which, in an integrated way, covers the area of dependability and safety during the whole life cycle. More sensitive objects in terms of safety are the ones where tens and hundreds of users meet, not just single ones. Railway transport is regarded as one of such areas, which has gone through a dynamic development recently. The article covers initial steps in the programme RAMS, which are carried out in relation to the rail applications safety.

Introduction

The article is supposed to provide basic information when choosing and implementing safety and risk analysis techniques. It serves as a guide, especially for assessing risk connected with technical systems at the beginning of the programme RAMS introduction used for rail applications.

In every phase of a technical life all legislative and standardised system requirements have been observed, which is the basic and essential presumption when performing safety analysis of a technical system. Furthermore, all opera-

tion conditions and the conditions, under which the object is supposed to be used, were or will be kept.

All the used terms, definitions and abbreviations that are generally known, are defined in the publications listed in the bibliography below.

1. Aims and basic terms of safety and risk analysis

Generally speaking, the aim of safety and risk management is to reduce casualties, diseases, or injuries, damage to property, and consequential loss and impact upon the environment, to avoid or regulate them. In this case, it is about providing safety of the technical system that is supposed to be assessed. An object as a unit, or its parts might be a source of risk. The aim is then to identify objects and elements in the system that can be by their nature the source of risk. In order to identify, assess, and evaluate them, we can use some of the methods introduced in this paper. Next, the possibility of affecting the extent of risk is going to be mentioned.

The basic assumption deals with system failures in analyses, and in order to provide safety and risks, we assess a key property of the object, which is called "safe during a failure".

To manage the risk effectively, it is necessary to analyse its sources first. The risk analysis is a useful tool for the following:

- Risks identification, their sources and approaches to their solution;
- Providing objective information used for making decisions; and,
- Fulfilment of the instruction requirements.

The results of safety and risk analysis will be used by decision-makers. This helps when deciding on risk acceptance and when choosing between measures to reduce a risk threat or to prevent from its occurrence. The basic advantages which might be introduced after the possible safety, risk and its sources analysis are as follows:

- Potential hazards are systematically identified;
- Potential failure modes are systematically identified;
- The extent of risk might be expressed quantitatively or the classification of risks is carried out; and,
- Possible modifications leading to reducing the risk or achieving better overall level of dependability are evaluated.

2. Principle of safety and risk management

Safety and risk analyses are a part of processes dealing with dependability, safety, risk assessment, and management (see Figure 1). They include defining a range of validity, identifying hazards, and estimating safety and risk levels.

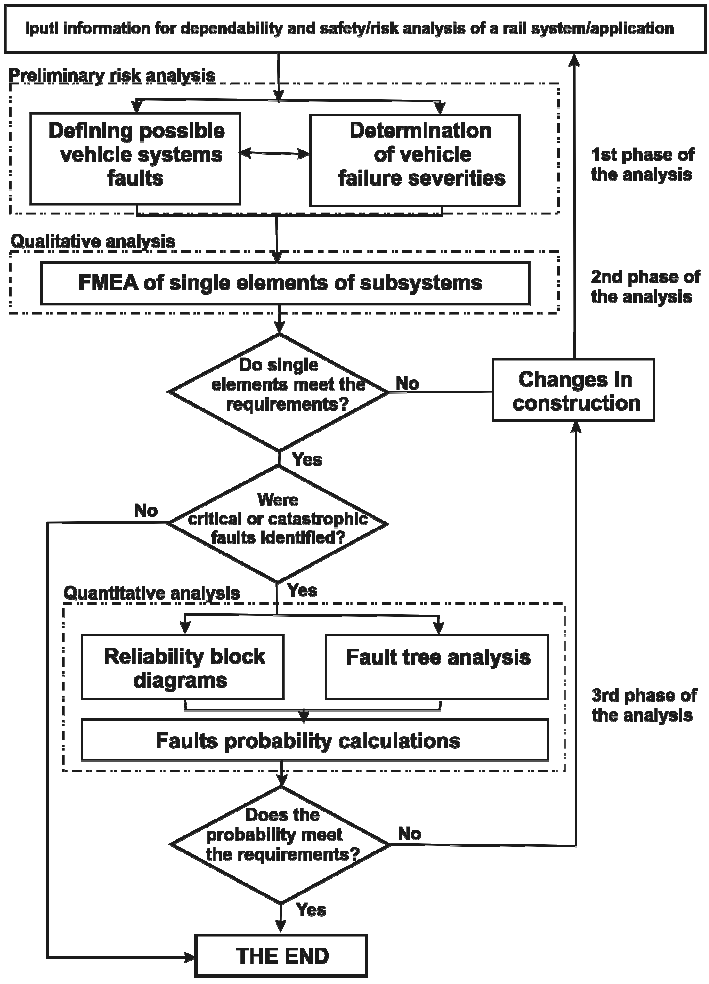

Fig. 1. Procedure for assuring rail vehicle safety

The basic division of hazards is between natural, technological, social and the hazard relating to life style. Although these hazards do not negate each other, we will deal only with the hazard connected with technological conditions.

As the consequences linked with an undesired event are also a part of risk, these also might be put into different categories by their nature as follows:

– Individual consequences (e.g. individuals in society);
– Consequences produced by a job (e.g. workers);
– Social consequences (e.g. a large part of society);
– Damage to property and economic loss (e.g. interruption of activity); and,
– Damage to the environment (e.g. land affection).

The general aim of the safety and/or risk analysis is to provide a reasonable basis for the decision tackling safety and/or risk. Such decisions might be made as part of a more extensive risk management process by means of comparing the results of safety and/or risk analysis with given criteria for accepting safety and/or risk. In many practical applications, it is necessary to consider advantages of single solutions on a case-by-case basis so that a proper decision could be made. The things relating to acceptance criteria are generally very complex and include a wide variety of conditions that are very difficult to determine.

- Parts of a system that significantly contribute to risk and weak elements are identified.
- Understanding of a system and its installation is improved.
- Risk are compared with the risks of alternative systems or technologies.
- Risks and uncertainties are identified and delivered.
- The analysis helps to introduce priorities when improving health and safety levels.
- The analysis becomes a basis for potential rationalisation of preventive maintenance and check.
- Accidents are investigated and their occurrence is prevented.
- The alternatives, such as different measures and technologies used for reducing risk levels, are selected.

3. Application of the safety and risk analysis during life cycle phases

Some specific aims of the safety and/or risk analysis are in connection with single life cycle phases stated below. Concerning life cycle phases, they can be divided according to the basic classification not expanded by some of the standardisation documents (e.g. IEC 50126). These are as follows:

a. The phase of requirement conception and determination/design and development phase:
   - main elements of the system which contribute to risk occurrence including important factors which are related to them are identified;
   - input information used for design process and assessing the design sufficiency is provided;
   - possible safety measures in the design are identified and evaluated;
   - input information used for assessing the sufficiency of submitted virtually dangerous equipment, activities or systems is provided.
   - the information useful for developing procedures applied under regular and emergency conditions is provided;
   - the risk in relation to equipment requirements and other requirements is evaluated; and,
   - alternative design conceptions are evaluated.

b. Production, installation, operation, and maintenance phase:

- experiences are observed and evaluated so that the real performance could be compared with relevant requirements;
- input data used for optimising procedures during regular operation, maintenance/check ,and under emergency conditions are provided;
- the information on parts of the system which significantly contribute to risks, and on the factors which affect them is updated;
- the information on risk importance for operative decision is provided;
- the effects of organisation structure changes, operation practices and procedures, and parts of the system are evaluated; and,
- the effort is aimed at training.

c. Disposal and decommissioning phase:
- the risk related to the activities during disposal is evaluated, and the fulfilment of relevant requirements is provided; and,
- input data for the procedures during disposal are provided.

In order to improve efficiency and objectivity of the safety and risk analysis, and to make the comparison with other analyses easier, it is necessary to observe generally valid rules. The analysis process should be performed according to the recommended sequence of acts as follows:
- Definition of the validity extent;
- Identification of hazards and initial consequences evaluation;
- Risk estimation;
- Verification;
- Documentation; and,
- Analysis updating.

The analysis of each rail vehicle system can lead to one of the following outcomes:
- The rail vehicle system meets all safety requirements – the analysis can be submitted then as evidence of meeting relevant requirements.
- The rail vehicle system does not meet the requirements – following the results of the analysis, relevant construction modifications which are to remove discovered imperfections are then suggested (after the changes are performed, it is necessary to repeat all the analysis procedure again).

An example of specific assessment performance is briefly introduced in the following example.

4. An example of using a structure and genesis for application of methods used for safety

In the first phase, we perform a preliminary safety and risks analysis (PHA + FMEA/FMECA). As an illustration, we select one part of a rail vehicle system. This method could be performed hierarchically starting with a vehicle as a whole.

In following part, common use of the method PHA (Preliminary risk analysis) is presented. This method can be carried out and recorded in different ways. However, using table expression, which is put in Table 1, seems to be an appropriate form.

Table 1. PHA method utilisation

Pol. č.	Risk description	Risk effects	Operation phase	Classification of effects	Corrective actions	Occurrence probability	Note
1	Controller spontaneously sends a signal for traction.	Uncontrolled start.	During waiting of a train under voltage	Catastrophic	Validity of continuous signal for traction is confirmed by a logical state of switches.	Almost impossible	Undesired signalling for traction can occur only due to failure of at least three system elements at a time.
2	Controller spontaneously sends a signal for braking.	Undesired braking of a train.	During a train ride.	Critical	Validity of continuous signal for braking is confirmed by a logical state of switches.	Almost impossible	Undesired signalling for traction can occur only due to failure of at least three system elements at a time.
3	Controller makes the brake activation impossible.	It is impossible to brake when using a brake lever and traction MP (TT-FE).	During a train ride.	Marginal	Using highly failure-free elements.	Rare	The train might be braked with an emergency brake.
4	The control unit system cannot be reset.	Undesired emergency braking.	During a train ride	Critical	Using highly failure-free elements	Rare	-
5	The control unit system sends a valid signal although the system was not reset.	In case an operator is not able to drive a train, emergency braking to stop does not occur.	During a train ride	Catastrophic	Using highly failure-free elements. A valid signal is formed by switching (0-1).	Impossible	Failure is signalled for an operator.

Once the assessment of one group has been completed, the assessment of failures might be the next step to be performed. It can be done by either matching the seriousness of failures to rates, or by matching the rates (probabilities) to the seriousness, and a "risk matrix" could be used for this (see e.g. IEC 50126). We always start from the principle that we match the things which can be affected (the matching is viewed as the determination of an acceptable value or magnitude or rate). Some input into analysis might be taken from a draft analysis of FMEA/FMECA. However, as far as the method PHA discovers other sources of risk, these should be examined very thoroughly using continuing quantitative methods, like FTA or RBD.

It is important to mention that the method PHA, as well as other methods, is to be updated during the next life cycle phases. Along with this method, the

risk list, risk sources should be created, and the list should be also continuously updated.

Conclusions

This paper is supposed to help and give an initial insight into the RAMS programme implementation in the technical practise. There are some crucial steps that have to be considered, respected, and repeated while doing dependability and safety/risk analysis. The important attribute of the RAMS programme is understanding its necessity to be carried out during the whole life cycle in each phase precisely. Therefore, we hope this paper will help to make it possible for users to utilise this information in the orientation and decision making process.

Acknowledgements

Preparation of this paper was significantly supported by the Ministry of Education, Czech Republic project number 1M06047 "The Centre for Production Quality and Dependability" and partially supported by the Czech Science Foundation project number 101/08/P020 "Contribution to Risk Analysis of Technical Sets and Equipment".

Bibliography

1. EN ISO 9001:2001 – Quality management systems – Requirements.
2. IEC 60300-3-9 – Dependability management. Part 3: Application guide. Section 9: Risk analysis of technological systems.
3. IEC 60050(191) International Electrotechnical Vocabulary - Chapter 191: duality and Dependability of Services.
4. IEC 50126 – Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS).
5. IEC 60300-2 – Dependability management – Part 2: Guidelines for dependability management.
6. IEC 60812 Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA).
7. IEC 61025 Fault tree analysis (FTA).
8. EN 61078 Analysis techniques for dependability - Reliability block diagram and boolean methods.
9. ISO 12100-1:2004 Safety of machinery - Basic concepts, general principles for design - Part 1: Basic terminology, methodology.
10. ISO 12100-2:2004 Safety of machinery - Basic concepts, general principles for design - Part 2: Technical principles.

11. ISO 13849-1:2008 Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design.
12. ISO 13849-2:2008 Safety of machinery - Safety-related parts of control systems - Part 2: Validation.
13. ISO 14121-1:2008 Safety of machinery - Risk assessment - Part 1: Principles.
14. ISO 14121-2:2008 Safety of machinery - Risk assessment - Part 2: Practical applications and examples of methods.
15. IEC 60300-3-1 Dependability management - Part 3-1: Application guide - Analysis techniques for dependability - Guide on methodology.
16. ISO 31 000:2009 Ed.1.0 - Risk management — Principles and guidelines on implementation.
17. ISO/IEC 31010:2009 Ed. 1.0: Risk Management - Risk Assessment Techniques.
18. ISO 13824:2009 Ed. 1.0- General principles on risk assessment of systems involving structures.
19. ISO/IEC Guide 73:2002 Ed. 1.0 Risk management – Vocabulary – Guidelines for use in standards.
20. ISO/IEC GUIDE 51:1999 Ed. 1.0 Safety aspects – Guidelines for their inclusion in standards.
21. IEC 61508-(1-7)/:2008 Ed. 2.0 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems.
22. JCSS (Joint Committee on Structural Safety) - Principles, System Representation & Risk Criteria.
23. The National Risk Register
http://www.risksociety.org.nz/what_is_risk_management/.
24. ECSS (European Cooperation for Space Standardization)-Q-ST-40-02C Space product assurance - Hazard analysis.
25. MIL-STD-882D Standard Practice for System Safety.

Recenzent:
Janusz SZPYTKO

Krótkie wprowadzenie do kolejowych aplikacji oprogramowania typu RAMS

Słowa kluczowe

Bezpieczeństwo, RAMS, oszacowanie ryzyka, wdrożenia kolejowe.

Streszczenie

Zapewnienie niezawodności i bezpieczeństwa jest zasadniczą częścią oprogramowania służącego do projektowania. Polepszanie tych parametrów powinno być stale na uwadze producentów w wyniku dynamicznego rozwoju produktów. Problematyka ta powinna rozpatrywana nie tylko ze względu na potrzeby spełniania określonych norm, standardów lub certyfikacji procedur.

W obszarze systemów technicznych z powodzeniem funkcjonuje oprogramowanie typu RAMS, które w zintegrowany sposób pokrywa zapotrzebowanie na obliczenia niezawodności i bezpieczeństwa w ciągu cyklu życia tych systemów. W kontekście bezpieczeństwa bardziej wrażliwe obiekty to te, z których korzysta codziennie tysiące użytkowników. Transport kolejowy jest jednym z takich systemów, który równocześnie podlega dynamicznemu rozwojowi. Ten artykuł przedstawia podstawowe kroki postępowania w modelowaniu bezpieczeństwa w ruchu kolejowym z zastosowaniem aplikacji typu RAMS.