5th INTERNATIONAL CONFERENCE
TRANSPORT SYSTEMS TELEMATICS TST'05

ZESZYTY NAUKOWE
POLITECHNIKI ŚLĄSKIEJ 2005
TRANSPORT z.59, nr kol. 1691

risk analysis,
railway traffic management

Andrzej BIAŁOŃ[1]

ISSUES OF RISK ANALYSIS IN THE RAILWAY TRAFFIC MANAGEMENT SYSTEMS

This paper discusses the issue of implementation of risk analysis to the technical equipment. Instances are shown of application of risk analysis to the railway traffic management equipment.

PROBLEMATYKA ANALIZY RYZYKA W URZĄDZENIACH STEROWANIA RUCHEM KOLEJOWYM

W artykule omówiono problematykę analizy ryzyka w urządzeniach technicznych. Pokazano przykłady zastosowania analizy ryzyka w urządzeniach sterowania ruchem kolejowym.

1. INTRODUCTION

Risk analysis is more and more often the element that is very important during designing, production and operation of technical equipment. The writings shown in certain standards concerning railway traffic management equipment, especially those related with safety, impose to the engineering teams and manufacturing the equipment an obligation to perform a risk analysis. This may be shown on the example of a standard PN EN 50 126 where a lifecycle of the system (for example, a railway control system (or srk) system) is shown. Risk analysis is here, as shown on Fig.1 a necessary and important element of the lifecycle of this system.

Also during safety analysis necessary for preparation of the safety proof and performed in accordance with standard PN EN 50 129, one of more important elements of this analysis is a risk analysis. Risk analysis and the risk itself is closely related with system safety, thus it is one of the most important elements during taking a decision about system application.

Regulations of Polish and European standards impose an obligation to apply the risk analysis not only during the safety analysis, but also when making a decision about implementation of the system for use and constitutes is obligatory part.

[1] Faculty of Transport, Silesian University of Technology, Krasińskiego 8, 40-019 Katowice, Poland, Andrzej.Bialon@polsl.pl
Railway Scientific and Technical Centre, Chłopickiego 50, 04-275 Warsaw, Poland, abialon@cntk.pl,

Risk analysis is a relatively new area. Its implementation in specific areas of technology varies very much. In the railway control system equipment it is applied since several tens of years. The developed standards concerning safety, such as PN EN 50126 (1999), standard PN EN 50 129 (last update 2003) take the risk analysis into account in their scope.

A general standard where the basic terms concerning risk analysis are shown, is the PN IEC 60300-3-9 „Analiza ryzyka w systemach technicznych" (Risk analysis in technical processes). This standard is a part of standard concerning reliability management and being an application guide.

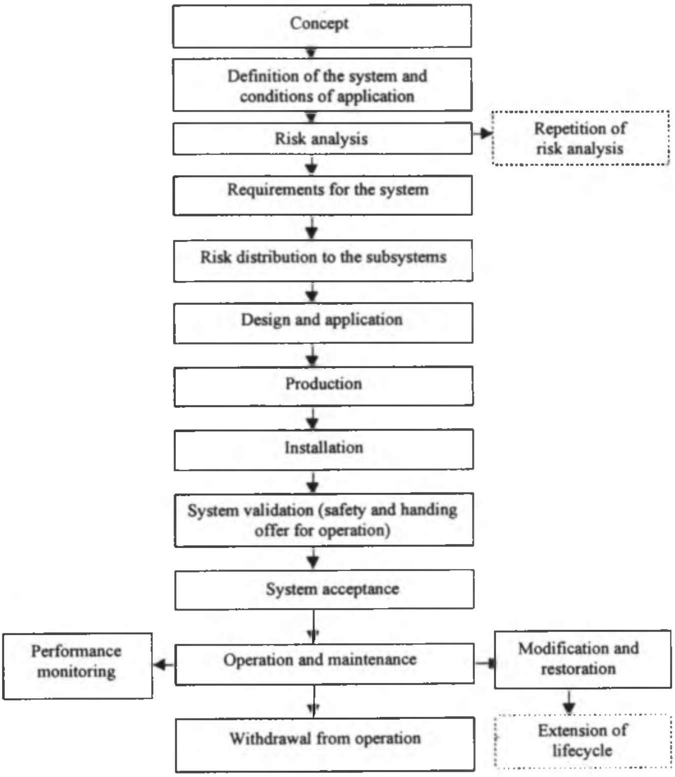
Concept
Definition of the system and conditions of application
Risk analysis
Repetition of risk analysis
Requirements for the system
Risk distribution to the subsystems
Design and application
Production
Installation
System validation (safety and handing offer for operation)
System acceptance
Performance monitoring
Operation and maintenance
Modification and restoration
Withdrawal from operation
Extension of lifecycle

Fig.1. Lifecycle of a system (such as railway control system)

2. RISK ANALYSIS PROCESS

The standard PN IEC 60300-3-9 recommends implementation of risk analysis in the order of operation as specified below:

- Specification of the scope;
- Identification of hazards and preliminary establishing of consequences;
- Estimation of risk;
- Verification;
- Documenting;
- Update of analysis.

Process of risk analysis is shown on Fig.2.

It is recommended that the consequence analysis include:

- The basis of analysis the undesired events are selected;
- All the consequences caused by the undesired event are described;
- Measures remedying the consequences with the conditions applied to influence these consequences;
- The criteria used for identification of consequences are presented;
- Both direct consequences and those that are likely to occur after a certain time are taken into account;
- The secondary consequences such as relating to the neighbour equipment and systems are taken into account.

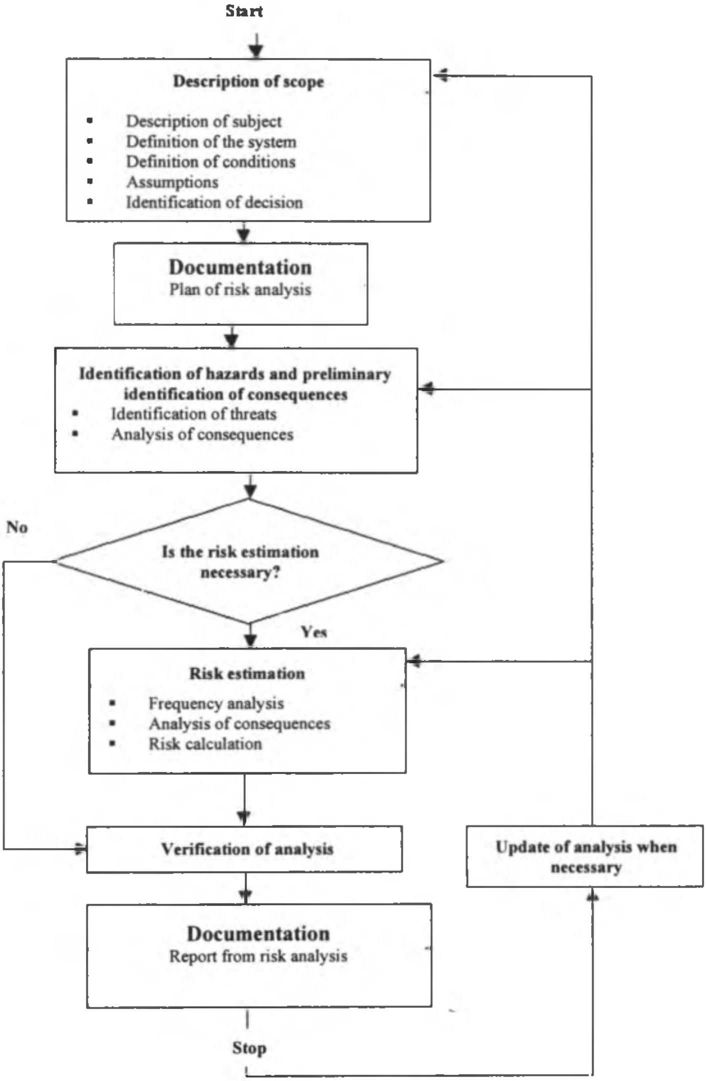

Fig.2. Risk analysis process

2.1. METHODS OF RISK ANALYSIS

For the purpose of risk analysis, risk management and estimation a range of methods is used and some of them are quoted below:

- Analysis of event tree
- Analysis of types and effects of unsuitability as well as analysis of effect and criticality of unsuitability;
- Analysis of unsuitability tree
- Investigation of threats and operational readiness
- Analysis of human reliability;

- Preliminary threat analysis;
- Block diagram of reliability;
- Order of categories;
- Check lists;
- Analysis of failures of similar type;
- Consequence models;
- Delphi method;
- Hazard indicators;
- Simulation Monte Carlo and other SIM methods;
- Comparison in pairs;
- Retrospective data overview.

2.2. QUALITATIVE RISK ANALYSIS

There exist a range of qualitative risk estimation method. In each case only these risk factors are taken into account, that have a basic impact on the evaluation of danger results (extent of damage within the protected facility). From among all these factors that have impact on the development of safe requirements for the system that should fulfil its protection function (such as rtms system) we may list :

- Duration of danger *D*;
- Prevention of danger *G;*
- Probability of danger occurrence *W*.

The factor „extent of damage on the protected facility" are criteria describing the facility itself (people, equipment, devices etc) and extent of damage (casualties, material damage etc.) For instance, if the people are protected, the following events (damage) are taken into account.

- S1 – light - light injuries, light professional disease;
- S2 – serious – serious injuries of one or more persons, death of one person;
- S3 – heavy – death of many people;
- S4 – deadly – many casualties and practically destruction of the entire plant or system.

The factor „duration of danger" is understood as duration of danger and in the case of people the duration of remaining in the dangerous zone. It may be specified as:

- *D1* – rare and frequent stay in the dangerous zone ;
- D2 – very frequent or permanent stay in the danger zone.

Factor „prevention of danger" describes the criterion of operation method (with supervision or without it), time course of danger (quick, slow), method of „deturning the danger (with technical and organizational means), practical investigation with negative result (none, low, high), forecasting the danger with a possibility of prevention (possible, ...) on the basis of the above data it is possible to describe the G factor as;

- G1 - possible in predefined conditions;
- G2 - always possible.

Factor „probability of danger occurrence" is defined verbally as probabilities of occurrence of the danger during an activity that will be realized without protection functions, the W factor may be divide as:

- W1 – very low probability;
- W2 – low probability;
- W3 – relatively high probability.

The quoted risk factors enable to produce 48 combinations. It shows that the practically meaningful are 8 combinations of factors *S*, *D*, *G*. For example, for catastrophic conditions (factor S4) the D and G factors have very low impact on full filament of protection properties of the system.

The more of risk factors are taken into consideration and the more accurate is their division and determination, the more objective may be development of requirements for risk reduction and safety of requirements for the system. What risk factors are selected for analysis it depends of the specific control process for which the safe requirements have to be determined.

Generally four-risk level is assumed. They may be assigned measures to be used for each level of risk. It is shown as below:

- ❑ *unacceptable* – reduction of risk is necessary, otherwise the system cannot be used for operation;
- ❑ *undesirable* – risk is acceptable only in the case when the expenses related with its reductions are significantly higher than the effects achieved, or when the reduction of risk is unreachable;
- ❑ *acceptable* – risk is acceptable only n the case when the expenses related with its reduction are much higher than the effects achieved;
- ❑ *negligible* – further expenses for risk reduction are unnecessary.

2.3. QUANTITATIVE RISK ASSESSMENT

There exist many methods of quantitative risk assessment. Part of them is quoted in item 2.1. Generally maybe stated that the risk is a combination of intensity of safety occurrence h and its consequences S.

$$R=h.S$$

The total danger related with use of the system (such as railway control system) consists of many existing dangers and for this reason, for the entire risk we may assume the following:

$$R=\sum_{i=1}^{n} h_i.S_i$$

where hi – intensity of occurrence of i-th danger , S_i consequences of i-th danger,

The probability of occurrence of i-th danger may be described as follows:

$$p_i=\frac{h_i}{\sum_{i=1}^{n} h_i}$$

The expected amount of effects per time unit:

$$E_{(S)}=\sum_{i=1}^{n} S_i \cdot p_i$$

And as a result

$$R = E_{(s)} \cdot \sum_{i=1}^{n} h_i$$

2.4. IDENTIFICATION OF DANGER IN RAILWAY CONTROL SYSTEM EQUIPMENT

For the risk estimation it is necessary to determine dangers related with control of railway traffic process (a „set“ of dangers has to be prepared). The „set“ of dangers may be prepared based upon the analyses and theoretical considerations or based upon the hitherto experiences from the similar systems and statistical data. The most frequently the „set“ of dangers is realized as a combination of both methods. What is to be taken into consideration it depends of system analysis level. The risk analysis result does not depend of quantification of the dangers identified, but of the fact how the space of dangerous system conditions is determined. From the statistics it may be assumed that the reason for accident occurrence was a mistaken action in the object under consideration (setting a point under the running train, incorrect information about track section occupancy etc) or when the cause of accident is an error in the system logic. In the railway facilities related with railway traffic management we may, as an instance, determine the following dangers:

- For sempahore:
  - lighting up of false release signal (release for travel when the stop signal should have been lighted up);
  - failure to set the stop signal;
  - lighting of a ignal allowing for higher speed;
  - etc.
- for points:
  - resetting of a confirmed points;
  - setting of points under the rolling stock;
  - error in information about position of points;
  - etc;
- for track section:
  - error information about non-occupancy of the section;
  - error information about occupancy of the section;
  - etc.

The reason for danger during operation of the railway control system maybe also an error of operation personnel during the activities related directly with train traffic management It is possible to determine the impact of operation personnel on realization of traffic management functions:

- none –The system operates correctly and controls the safety in full range and at any command issued by the personnel;
- partial:
  - system operates but its technical solution does not allow for a full control of all personnel commands (also incorrect ones);
  - system operates partially, some of realized safety functions are performed by the personnel without system supervision;
  - total – system does not operate, all operations related with safety are performed by the service personnel without being controlled by the system.

2.5. ANALYSIS OF DANGER RESULTS

As the malfunction may be a reason for various dangers, the danger, depending of concrete operating conditions, may be reason of various consequences. For this reason, during srk analysis each danger has to be analysed from the point of view of all possible consequences, whereas the probability of occurrence of similar consequences will be various and will depend of operating conditions (for example of traffic intensity).

General danger related with use (operating) of an railway control system may lead to various consequences, and namely:

- driving the traction vehicle into the rear of preceding traction vehicle;
- collision of a traction veihicle with side of another traction vehicle;
- front collision of traction vehicles;
- collision of traction vehicle with road vehicle;
- running over a pedestrian
- derailing of traction vehicle
- etc,.

The consequence of accident my be material damage, hazard to the people or other damage. If here exist a real threat of human death or significant injury, then material damage may be disregarded and should not be taken into consideration for risk analysis. The exposure of human health may be determined as number of death cases:

$$S_N = S_M + k_Z.S_Z + k_L.S_L$$

where S_M is a number of death cases; S_Z number of heavy injuries, S_L number of light injuries;, k_Z ratio of acceptance of heavy injuries and k_L ratio of acceptance of light injuries. For example in the information part of standard PN EN 50 126 the ratios are given $k_Z = 10$ and $k_L = 100$.

3. SUMMARY

As shown in the material presented, the risk analysis is a quite complicated and broad area. This applies to all technical systems. For the systems related with safety, including railway control systems, there us no specific guidelines for performance of works related with risk analysis. It seems necessary that the works are performed for Polish railways to implement the risk analysis during designing, production and operation of devices related with safety. This applies to the railway control system equipment in the first order. The risk analysis is necessary during taking decisions on implementation of the railway control system to operation. This is required by both regulations and it is recommended by need to take rational decisions about implementation of the systems. In the nearest future there may be a possibility that during the railway investment project co-financed by the European funds the risk analysis is one of the conditions for granting the co-financing.

BIBLIOGRAPHY

[1] PN EN 50 126 „The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS). Railway application" 1999.

[2] PN EN 30 129 „Communication, signaling and processing systems – Safety related electronic systems for signaling. Railway application" 2003.

[3] PN EN 61508 – 1 Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych systemów związanych z bezpieczeństwem- Część 1; wymagania ogólne. 2003.

[4] PN EN 61508-3 „ Functional safety of electrical/electronic/programmable electronic safety systems. Part 5. Exemples of methods for the determination of safety Integrity levels" 2001.

[5] PN IEC 60300-3-9 „Analiza ryzyka w systemach technicznych" Zarządzanie niezawodnością. Przewodnik zastosowań. 1999.

[6] ZAHRADNÍK, J RÁSTOČNÝ, K, KUNHART M. „Bezpečnosť železničných zabezpečovacich systémov" Żylina 2004.

[7] RÁSTOČNÝ, K: Analýza rizík železničného signalizačného systému. AEEE No. 3-4 Vol.2/2003. ŽU v Žiline.

[8] ZAHRADNÍK, J.; HANUSOVÁ, N.; BARIOVÁ, H.: Analýza rizík v železničnej doprave. 6. sympózium s medzinárodnou účasťou "Železnice na prelome tretieho tisícročia", 27. - 28. 5. 1999, Žilina, Zborník prednášok.

Reviewer: Ph. D. Jerzy Mikulski