QUANTITATIVE HAZARD AND RISK ANALYSIS

G. Tarnai[a)], B. Sághi[a)], I. Krbilová[b)]

[a)] *Dept. of Control and Transport Automation, Budapest University of Technology and Economics*
[b)] *Dept. Control and Information Systems, University of Žilina*
e-mail:tarnai@kaut.kka.bme.hu

Summary In this paper a quantitative method for hazard and risk analysis is discussed. The method was developed and introduced for the allocation of safety requirements to the functions of a railway signaling remote control system.

1. INTRODUCTION

In case of safety critical railway systems a *hazard and risk analysis* (HRA) must be performed in order to establish the safety requirements for the system. Based on the analysis, to each safety critical function of the system (those functions, the fault of which can lead to hazard) the safety integrity requirement, concerning random and systematic faults can be established [1], [2].

The analysis and the definition of safety requirements can vary upon different risk parameters used, and so the method can be *quantitative*, *qualitative* or *semi-quantitative* [3], [4].

In this paper a *quantitative method* will be introduced, which was developed and applied for the risk analysis of a railway signaling remote control system [5].

2. MAIN STEPS OF THE ANALYSIS

In the preparation phase of the analysis the following steps must be performed:

- definition of the *interfaces* of the system;
- enlist all potentially *hazardous outputs* of the system (commands and indications);
- definition of possible *failure modes* for the outputs (these are object and function mistake and unintended command output in case of commands, and faulty indication in case of indications);
- the possible *consequence* (severity of damages) of the hazards must be identified; in this sense those damage categories were used, that are suggested by the standard EN 50126 [1].

Risk of a hazard is determined not only by the severity of the damage that it can cause, but also by the occurrence *frequency* or *probability* of the hazard. The calculated risks have to be classified into *risk classes*, and for each risk class the necessary integrity requirements must be defined. This latter can be achieved e.g. by ordering *tolerable hazard rates (THR)* for each risk class.

According to the proposed method, *THR* values are directly ordered to the damage categories, independently from the frequency or probability of the hazard, as the first step (Tab. 1). More serious hazards are so allowed to occur less frequently, thus the tolerable risk level of different hazardous functions can be kept at the same level [6].

Of course, other values of *THR* in the ordering or any other definition of *THR* can be adopted; this will not influence the proposed hazard and risk analysis procedure as a whole.

Tab. 1. Ordering of THR values to damage categories

Consequence (damage)	⇒	**THR [h^{-1}]**
catastrophic	→	10^{-9}
critical	→	10^{-8}
minor	→	10^{-7}
irrelevant	→	10^{-6}

From the *THR* value the tolerable hazard probability of the system can be calculated for the end of the projected life time of the equipment *T*, according to (1).

$$p_h(T) = 1 - e^{-THRT} \qquad (1)$$

In most of the cases a hazard, caused by a faulty function of the examined system will not lead directly to an accident, only if certain events occur contemporarily or a given situation exists simultaneously. The probability of the existence of these traffic or operational situations can be determined statistically, and can be handled as constant probabilities [6]. In course of the analysis, to all hazards, the necessary contemporary events and situations must be identified; furthermore their probability has to be calculated. Finally, the resulting probability p_c has to be calculated, if more than one contemporary event is necessary to evolve an accident. In a simple case the resulting probability can be calculated as a production of single probabilities; otherwise, in a more complicated combination of the contemporary events fault tree analysis can be used to calculate the resulting probability. The probability of an accident at the end of the projected life time of the investigated equipment can be calculated according to (2).

$$p_1(T) = p_c \cdot p_h(T) \qquad (2)$$

Since the reduction factor p_c of the contemporary events were taken into account, the tolerable hazard probability $p_b(T)$ can be bigger by the factor $1/p_c$, than without reduction factors as shown in (3) (Fig. 1, Fig. 2).

$$p_b(T) = \begin{cases} p_h(T)/\,p_c \text{ ,if } p_h(T)/\,p_c < 1 \\ 1\text{, otherwise} \end{cases} \quad (3)$$

This latter case means, that the reduction factors alone fulfil the required THR value, thus it is not needed to prescribe any requirement against the examined system (the required safety is fulfilled even if the equipment is always faulty).

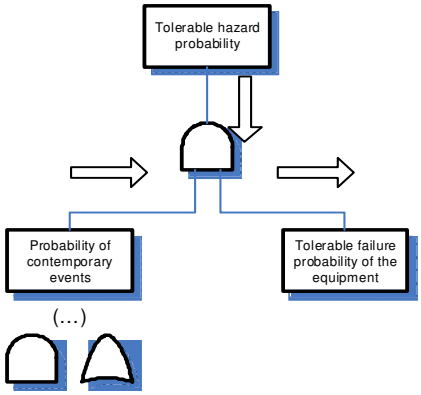

Fig. 1. Calculation of tolerable failure probability

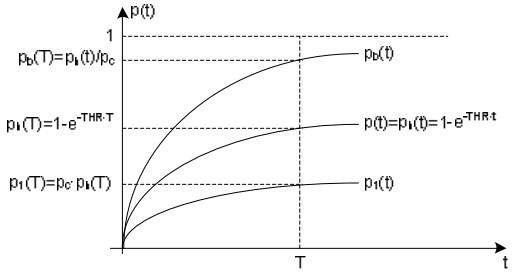

Fig. 2. Failure probabilities

If $p_b(T) \neq 1$, the tolerable failure rate of the equipment can be calculated from the tolerable failure probability of the equipment, as shown by (4).

$$bTHR = \frac{-\ln(1 - p_b(T))}{T} \quad (4)$$

The value *bTHR* represents the required integrity against random hardware faults, regarding the examined function and failure mode. Integrity requirements against systematic and software faults can be determined by using Safety Integrity Levels (SIL), based on the *bTHR* value.

Tab. 2. Ordering of SIL to bTHR values

bTHR **per function and hour**	**Safety Integrity Level (SIL)**
$10^{-9} \leq bTHR < 10^{-8}$	4
$10^{-8} \leq bTHR < 10^{-7}$	3
$10^{-7} \leq bTHR < 10^{-6}$	2
$10^{-6} \leq bTHR < 10^{-5}$	1
$10^{-5} \leq bTHR$	0

The Safety Integrity Level, which can be ordered to the *bTHR* values are shown in Tab. 2. The table is identical with that of the normative Annex A of EN 50129 [2].

3. RESULTS

A detailed analysis for all failure modes of all potentially hazardous functions have to be performed, according to the procedure described above. If a hazard of a failure mode of a function can result in more than one consequence, the most rigorous value have to be considered, which results after taking all, different reduction factors into account.

Based on the results of the analysis, the remote control equipment have to be constructed so, that

- the hazardous failure rate of functions may not exceed the defined tolerable failure rate *bTHR* of the given function (random faults); and
- the guidelines and requirements of the standards EN 50128 and EN 50129 shall be fulfilled, with respect to the defined safety integrity level.

As a summary it can be stated, that the proposed quantitative method requires higher expenditures than the usual qualitative ones. This is because of the necessity of the large amount of initial statistical data. However, the higher expenditures can be traded off by more precise results, which enables to put lower safety requirements against some functions of the system, thus the development and the operation of the system can be less expensive, while the system does not cause more hazards, than tolerable.

REFERENCES

[1] CENELEC: Railway Applications- The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS). EN 50126, 1998.

[2] CENELEC: Railway Applications – Safety Related Electronic Systems for Signalling. EN 50129, 2003.

[3] Braband, Hirao, Luedeke: The relationship between the CENELEC railway signalling standards and other safety standards, SIGNAL+DRAHT, 12/2003

[4] Tarnai, G.: Harmonisation Method of Safety Validation Systems. Komunikacie/ Communications - Scientific Letters of the University of Zilina, 4/99. Zilina, 1999. pp. 12-16.

[5] Lantos, P., T. Mosó: Safety certification procedure according to CENELEC standards. Vezetékek Világa, Hungarian Rail Technology Journal, 2005/4. pp. 3-6. (Hungarian)

[6] Tarnai, G., B. Sághi: Hazard and Risk Analysis in the Railway Interlocking Domain Vezetékek Világa, Hungarian Rail Technology Journal, 2006/1 (Hungarian).