Hazard and Risk Analysis of Human-Machine Interfaces of Railway Interlocking System

G. Tarnai, B. Sághi

Department of Control and Transport Automation, Budapest University of Technology and Economics, Budapest, Hungary

Abstract

In this paper such a quantitative approach for hazard and risk analysis will be proposed, which was developed for the allocation of safety requirements for the functions of a railway interlocking remote control system.

1 Safety and Risk

Safety is defined in the relating CENELEC standards as being free from intolerable accidental risk, or being free from intolerable risk of hazards [1], [2]. Risk is the combination of

- frequency or probability of events (or combination of events), which can lead to a hazard and
- the possible consequence of a hazard, i.e. the severity of the damage.

The model of an event chain from the safe state, via the activation of the hazard and the accident up to damage is shown on Figure 1. In this model three states can be identified (P, A and S). The source of the hazard in state P is passive (this state is free from any hazard); in state A the hazard source becomes active (hazardous state), while state S is the damage, which is resulted by an accident.

\[ P_{p}(t+\Delta t)=P_{p}(t) - P_{p}(t) \cdot a \cdot \Delta t \]

\[ P_{A}(t+\Delta t)=P_{A}(t) + P_{p}(t) \cdot a \cdot \Delta t - P_{A}(t) \cdot b \cdot \Delta t \]

\[ P_{S}(t+\Delta t)=P_{S}(t) + P_{A}(t) \cdot b \cdot \Delta t \]

Figure 1. Event chain of an accident

In this model, \( a \cdot \Delta t \) equals to the probability, that the hazard source becomes active in the following \( \Delta t \), assuming that it was passive at the moment \( t \). Similarly, \( b \cdot \Delta t \) represents the probability, that the accident will occur and result in a damage in the period of \( \Delta t \) (system is in state S), assuming that at the moment \( t \) the hazard was active, but no accident occurred yet.

The probability \( b \cdot \Delta t \) represents the well known fact, that the activation of a hazard does not lead directly to, or does not necessarily lead immediately to an accident, and thus result in a damage. In most of the cases an active hazard results in an accident only if certain events occur contemporarily or a given situation exists simultaneously.

Figure 1 also shows, how to calculate the probability of system states \( P_{s}(t+\Delta t) \) for the moment \( t+\Delta t \), assuming, that \( P_{s}(t) \) is known.

Railway signaling and connecting safety critical systems prevent the effect of the hazards by establishing safety functions (e.g. interlocking). The random hardware and systematic hardware and software failures of these systems may lead to the inadequate performing of the safety function, and thus cause additive
hazards. Therefore, for all functions of these systems, the inadequate performing of which can be dangerous, the necessary level of protection from random and systematic failures must be defined [2].

The level of protection from random failures can be defined by the tolerable hazard rate (THR, [h⁻¹]), which shows the tolerable frequency of the given hazard. The level of protection from systematic failures can be defined by safety integrity levels (SIL). The connection of these two components of safety integrity is defined in [2], and is shown on

<table>
<thead>
<tr>
<th>THR (per function and hours)</th>
<th>Safety Integrity Level (SIL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(10^{-9} \leq \text{THR} &lt; 10^{-8})</td>
<td>4</td>
</tr>
<tr>
<td>(10^{-8} \leq \text{THR} &lt; 10^{-7})</td>
<td>3</td>
</tr>
<tr>
<td>(10^{-7} \leq \text{THR} &lt; 10^{-6})</td>
<td>2</td>
</tr>
<tr>
<td>(10^{-6} \leq \text{THR} &lt; 10^{-5})</td>
<td>1</td>
</tr>
<tr>
<td>(10^{-5} \leq \text{THR})</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 1. Components of safety integrity

While the level of protection from random failures has a quantitative characteristic, the level of protection from systematic failures is embodied by different strictness of development, test and acceptance procedures for the different integrity classes, which must be applied during the construction of the given safety critical system [3].

Consequently, in order to define the safety requirements, a hazard and risk analysis has to be carried out. For the methods of hazard and risk analysis and for the risk-based allocation of safety integrity requirements various methods have been elaborated [4], [6]. In this paper such a quantitative approach will be proposed, which was developed and applied in praxis for the analysis of a railway signaling control systems, which can control a relay based interlocking system locally or remotely [5].

2 Preparation of the Analysis

In order to perform the analysis definitely, and to be able to adequately evaluate the results of the analysis, several tasks have to be performed prior to the analysis.

As hazards can be embodied by the effects of the system onto its environment, as a first step the environment of the examined system, the relevant interfaces and their functions has to be identified. In our case study, this interface, the border of the examined control system and the controlled interlocking system in command direction are the outputs of the control system, which operate the push-button relays of the interlocking system. In the indication direction this border are the inputs of the examined system, which read in the state of the interlocking relay contacts.

The hazard and risk analysis must be performed for each function of the preliminarily defined interfaces, i.e. the consequences of possible failure of these functions must be analyzed. Hazards, which originate outside of the examined system (e.g. the failure of the controlled interlocking system), are not considered in this analysis.

The analysis can be performed independently from the architecture of the examined system. This point is especially important, as this analysis has to be performed in such an early phase of the life cycle, in which the internal structure of the system is not yet defined, i.e. a preliminary hazard and risk analysis must be carried out.

For practical reasons, it is necessary to define such traffic and operational factors, events and situations, the contemporary existence or occurrence of which affect the frequency or probability of an accident or the severity of the damage, which can be caused by the failure of the control system. Such factors are:

- frequency of so called critical commands (e.g. call-on signals);
- traffic and operational data (e.g. frequency and typical length of shunting movements, frequency and length of typical failures of interlocking system).

Consecutively, some initial conditions must be defined, which are relevant when evaluating the hazardous effect of the examined functions. These conditions, in our case, are in connection with the architecture and functionality of the controlled interlocking system on one hand, and with the operational rules of the railway on the other hand. Should these initial conditions be changed in the future, the analysis has to be performed repeatedly. The initial conditions are taken into consideration in course of the calculation of risk reduction factors in the ongoing analysis.

3 Method of the Analysis

Phases of the analysis are represented on Figure 2.

Figure 2. Phases of the analysis

Phase 1: Identification of the potential hazards, caused by the examined system

In course of the identification of the possible hazards, the outgoing point is, that the system may affect its environment in an unwanted way, so that its wide or narrow environment can be endangered, in our case, primarily the passengers and personnel that takes part in the railway transportation.

It is considered potentially hazardous
- if the interlocking system receives a faulty command; i.e. such a command is received because of the failure of the examined control system, that does not correspond to the intention of the operator, and the faulty state of which is not recognized by the interlocking system (Figure 3); or
- if the indicated state of the interlocking system and the transportation process does not correspond to the real state (faulty indication); as a consequence, the inaccurately informed operator may give out such critical command, which evades the interlocking logic and thus it may endanger the traffic.

A faulty command output may happen in the following ways:
- object mistake: the intended function is carried out on an unintended object;
- function mistake: an unintended function is carried out on the intended object;
- unintended output of a command: the control system “itself” gives out a command without any operator actions.
In some special cases (e.g. operation ‘signals to danger’) the fail of operation can also be dangerous (i.e. the equipment does not give out the intended command).

Phase 2: Identification of the potential hazards, caused by the examined system

In this phase the possible consequences of the identified potential hazards will be determined. Practically it means, that to all hazardous failure modes (object mistake, function mistake, unintended command output, and incorrect indication) of all commands and indications the possible consequence is identified (e.g. derailment or collision) and its severity is defined.

The severity levels are characterized by the severity categories, which are suggested in [1], and are shown in Table 2.

Phase 3: Identification of the potential hazards, caused by the examined system

The tolerable hazard rate ($THR$ [h$^{-1}$]) can be defined by using different methods and approaches [4]. According to the suggested method, $THR$ values are directly ordered to the damage categories, independently from the frequency or probability of the hazard. More critical hazards are so allowed to occur less frequently, thus the tolerable risk level of different hazardous functions can be kept at the same level.

Following this procedure, based on the chapter 4.6 of EN 50126, to each severity categories the tolerable hazard rate ($THR$) of the given severity category is defined. The result of this mapping is shown in Table 2. The table is also in accordance with Table 1 of the normative Annex “A” of EN 50129.

In the case study of the remote control system, the shown Table 2 was used to define the $THR$. 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.
<table>
<thead>
<tr>
<th>Severity level</th>
<th>Consequence</th>
<th>THR [1/h]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>Fatalities and/or multiple severe injuries and/or serious damage in the environment</td>
<td>$10^{-9}$</td>
</tr>
<tr>
<td>Critical</td>
<td>Single Fatality or multiple severe injuries and/or significant damage in the environment</td>
<td>$10^{-8}$</td>
</tr>
<tr>
<td>Marginal</td>
<td>Minor injury and/or significant threat to the environment</td>
<td>$10^{-7}$</td>
</tr>
<tr>
<td>Insignificant</td>
<td>Possible minor injury</td>
<td>$10^{-6}$</td>
</tr>
</tbody>
</table>

Table 2: Definition of THR

**Phase 4: Occurrence probability of an accident**

In the worst case, the $p(t)$ occurrence probability of an accident, caused by a hazardous failure, equals to $p_h(t)$ occurrence probability of the failure, as shown in (1), where $t$ equals to the time elapsed since putting into operation ([h]).

$$p(t) = p_h(t)$$  \hspace{1cm} (1)

Assuming, that the failure probability is of exponential distribution, it can be calculated according to (2), where $\lambda$ equals to the failure rate [h$^{-1}$].

$$p_h(t) = 1 - e^{-\lambda t}$$  \hspace{1cm} (2)

Considering the THR as the upper limit of failure rate, the failure probability is shown on (3).

$$p_h(t) = 1 - e^{-\text{THR} t}$$  \hspace{1cm} (3)

At end of the projected life time of the equipment $T$, $t$ equals to $T$, and thus, the tolerable occurrence probability of the hazard can be calculated according to (4).

$$p_h(T) = 1 - e^{-\text{THR} T}$$  \hspace{1cm} (4)

**Phase 5: Probability of contemporary events**

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 reduction effect of the contemporary events is represented by the probability $b \cdot \Delta t$ in Figure 1.

The probability of the existence of these traffic or operational situation can be determined statistically, and can be handled as constant in time probability. In course of the analysis to all hazards, the necessary contemporary events and situations must be identified in course of the analysis; 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 our investigation this $p_c$ probability takes over the role of the probability $b \cdot \Delta t$ in Figure 1.

In course of the analysis, the following factors were taken into account as reduction factors for the occurrence probability of an accident:

- $f$ traffic or operational factor,
- $k$ operator action frequency of commands,
- $e_1$ first human failure,
- $e_2$ second human failure (independent from the first one).

These factors are constant in time probabilities, their value may vary between 0 and 1. If a factor equals to 1, it means, the event, described by this factor will surely occur at the given moment, thus it is not possible to calculate with its probability reduction effect. Consequently, value 1 must be selected for those factors, which do not affect the occurrence probability of the accident. E.g. in case of an unintended
command output, neither the frequency of operator actions, nor a human failure can be taken into consideration, as reduction factor. If a factor equals to 0, it means that the event, described by this factor will surely not occur. Consequently, an accident cannot occur even if the given failure occurs.

The value of single factors can be calculated, based on statistical traffic data, relevant for the given railway line, station and error logs of the interlocking system. The initial statistical data and the way of calculation must be always clearly demonstrated.

Should a hazard result in different consequences with different severities, and for the different consequences different reduction factors can be taken into account, then always the most restrictive calculated tolerable equipment hazard rate must be taken into account.

Should it be the case, that to the occurrence of an accident numerous, not exclusive situations are necessary, and one of the events has by magnitude less probability to occur, then the additive hazard, produced by the lower probability event, can be ignored. Otherwise e.g. fault tree analysis can be used to determine the resulting probability.

The resulting reduction factor (probability $p_c$) in case of exclusive events can be calculated according to (5). Obviously, this value varies between 0 and 1.

$$p_c = f \cdot k \cdot e1 \cdot e2$$  \hspace{1cm} (5)

**Phase 6: Affect of contemporary events on accident occurrence**

The occurrence probability of the accident at the end of the projected life time of the equipment $T$ can be calculated as shown by (6)

$$p_a(T) = p_c \cdot p_b(T)$$  \hspace{1cm} (6)

However, this also means, that the hazardous failure probability of the examined system $p_b(t)$, at the moment $T$ may be by the factor $1/p_c$ bigger, than without taking the reduction factors into account, as shown in (7).

$$p_b(T) = \begin{cases} p_a(T) / p_c, \text{ if } p_a(T) / p_c < 1 \\ 1, \text{ otherwise} \end{cases}$$  \hspace{1cm} (7)

This latter case ($p_b(T)=1$) means, that the reduction factors alone fulfill 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).

**Phase 7: Tolerable hazard rate of the random failures of the equipment**

If $p_b(T) \neq 1$, then the tolerable failure rate of the equipment $bTHR$ can be determined, based on the tolerable failure probability of the equipment $p_b(t)$ by using the equations (8). The frequency $bTHR$ represents to the required intensity of protection from random failures, with respect to the investigated function and failure mode. The equations are graphically demonstrated on Figure 4.

$$e^{-bTHR \cdot T} = 1 - p_b(T)$$

$$bTHR = \frac{-\ln(1 - p_b(T))}{T}$$  \hspace{1cm} (8)
Phase 8: Determination of integrity level for systematic failures

Integrity requirements against systematic hardware and software failures can be determined by using Safety Integrity Levels (SIL), based on the $bTHBR$ value. The Safety Integrity Level, which can be ordered to the $bTHR$ values are shown in Table 3. The table is identical with that of the normative annex A of EN 50129.

<table>
<thead>
<tr>
<th>$bTHR$ (per function and hour)</th>
<th>Safety Integrity Level (SIL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$10^{-9} \leq bTHR &lt; 10^{-8}$</td>
<td>4</td>
</tr>
<tr>
<td>$10^{-8} \leq bTHR &lt; 10^{-7}$</td>
<td>3</td>
</tr>
<tr>
<td>$10^{-7} \leq bTHR &lt; 10^{-6}$</td>
<td>2</td>
</tr>
<tr>
<td>$10^{-6} \leq bTHR &lt; 10^{-5}$</td>
<td>1</td>
</tr>
<tr>
<td>$10^{-5} \leq bTHR$</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 3. Ordering of SIL to $bTHR$ values

3 Results

A detailed analysis for all failure modes of all potentially hazardous functions have to be performed, according to the procedure described above. In the praxis all possible failure modes of all commands and indications are investigated on separate analysis sheets. In course of the case study, we had to analyze 28 commands, from which 13 were safety critical, and 77 indications from which 20 were safety critical. The whole analysis consisted of almost 50 analysis sheets. An example of the sheets is shown on Figure 5.

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

- hazardous failure rate of functions may not exceed the defined tolerable failure rate $bTHR$ of the given function (random failures); 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 the necessity of the large amount of initial statistical data. However the higher expenditures can be traded off by the fact, that we can form less rigorous
requirements against some functions of the system, what may result in a less expensive development and operation of the system, while the required safety is respected at the same time.

References