# ANALÝZA RIZIKA ŽELEZNIČNÉHO SIGNALIZAČNÉHO SYSTÉMU
# RISK ANALYSES FOR RAILWAY SIGNALLING SYSTEM

Karol Rástočný
*Katedra riadiacich a informačných systémov, Elektrotechnická fakulta, Žilinská univerzita, Veľký diel, 010 26 Žilina, e-mail: karol.rastocny@fel.utc.sk*

**Abstrakt** Európske normy pre železničné aplikácie definujú úlohy pre jednotlivé fázy životného cyklu, ktoré treba vykonať (neuvádzajú však ako), aby sa dosiahla schopnosť systému bezpečne a spoľahlivo plniť požadované funkcie. Akými bezpečnostnými vlastnosti má systém disponovať možno určiť len na základe analýzy rizika. V článku je uvedený postup, ktorý možno použiť pri analýze rizika pre železničné signalizačné systémy.

**Summary** The European standards for railway applications define tasks for individual phases of the life-cycle that must be performed (without specifying how) in order to achieve ability of the system to perform required functions safely and reliably. Safety characteristics of the system can only be performed on the base of risk analysis. In the paper there is given a procedure usable in risk analysis for railway signalling systems.

## 1. ÚVOD

Aj keď pre železničné signalizačné systémy je charakteristické správanie fail-safe, treba vzhľadom na dosiahnutú úroveň poznania, obmedzené technické a ekonomické možnosti reálne pripustiť, že určité riziko existuje a prakticky sa ani nedá úplne vylúčiť.

Definovať bezpečnostné požiadavky na systém znamená poznať akceptovateľné riziko a riziko vyplývajúce z riadeného procesu. Všeobecne sa odporúča (napríklad, normy [1], [2], [3], [4], [5], [6], [7]), aby sa v počiatočných fázach životného cyklu systému vykonala analýza rizika. To znamená, že pre jednotlivé požadované riadiace funkcie systému treba identifikovať nebezpečenstvá, z nich vyplývajúce nežiadúce dôsledky a určiť riziko spojené s riadením procesu.

## 2. SPÔSOBY HODNOTENIA RIZIKA

### 2.1 Kvalitatívne hodnotenie rizika

Existuje mnoho všeobecne uznávaných postupov na kvalitatívne hodnotenie rizika.

*Tab. 1 Klasifikácia rizika podľa EN 50 126*
*Tab. 1 Risk classification according to the EN 50 126*

| Početnosť výskytu nebezpečenstva | | | | |
|---|---|---|---|---|
| Častá | Nežiadúce | Neprípustné | Neprípustné | Neprípustné |
| Pravdepodobná | Prípustné | Nežiadúce | Neprípustné | Neprípustné |
| Občasná | Prípustné | Nežiadúce | Nežiadúce | Neprípustné |
| Malá | Zanedbateľné | Prípustné | Nežiadúce | Nežiadúce |
| Nepravdepodobná | Zanedbateľné | Zanedbateľné | Prípustné | Prípustné |
| Vysoko nepravdepodobná | Zanedbateľné | Zanedbateľné | Zanedbateľné | Zanedbateľné |
| | Nevýznamné | Okrajové | Kritické | Katastrofické |
| | Úrovne závažnosti dôsledkov nebezpečenstva | | | |

*Tab.2 Kvalitatívna interpretácia úrovní rizika*
*Tab. 2 Qualitative interpretation of risk levels*

| Úroveň rizika | Interpretácia |
|---|---|
| Neprípustné | Riziko musí byť odstránené. |
| Nežiadúce | Riziko smie byť akceptované len vtedy, ak je zníženie rizika prakticky nedosiahnuteľné a prevádzkovateľ systému s tým súhlasí. |
| Prípustné | Riziko možno prijať len vtedy, ak prevádzka systému je primerane kontrolovaná a prevádzkovateľ systému s tým súhlasí. |
| Zanedbateľné | Riziko možno akceptovať aj bez súhlasu prevádzkovateľa systému. |

Norma [1] uvádza postup na stanovenie úrovne rizika tabuľkovou formou. Kombinácia početnosti výskytu nebezpečenstva so závažnosťou jeho dôsledkov vedie k určeniu úrovne rizika (tab. 1) a následne k opatreniam na redukciu rizika, ktoré musia byť pre danú úroveň vykonané. Interpretácia úrovní rizika je v tab. 2.

### 2.2 Kvalitatívne hodnotenie rizika

Vo všeobecnosti možno riziko vyjadriť ako kombináciu intenzity výskytu nebezpečenstiev a ich dôsledkov za určitú časovú jednotku (prípadne vztiahnuté na inú mernú jednotku) [9].

$$R = H \,.\, A \,, \tag{1}$$

kde $H$ je intenzita nebezpečenstiev (neželaných udalostí) a $A$ sú dôsledky nebezpečenstiev.
Pre riziko viažuce sa k *i-tej* neželanej udalosti platí

$$r_i = h_i . a_i , \quad (2)$$

kde $h_i$ je intenzita výskytu *i-tého* nebezpečenstva, $a_i$ sú dôsledky *i-tého* nebezpečenstva.

Ak celkové nebezpečenstvo spojené s používaním systému (vrcholová neželaná udalosť) pozostáva z $n$ dizjunktných nebezpečenstiev, potom platí

$$R = \sum_{i=1}^{n} h_i . a_i . \quad (3)$$

Pravdepodobnosť výskytu *i-tej* neželanej udalosti

$$p_i = \frac{h_i}{\sum_{i=1}^{n} h_i} . \quad (4)$$

Pre celkovú pravdepodobnosť platí

$$\sum_{i=1}^{n} p_i = 1. \quad (5)$$

Ak

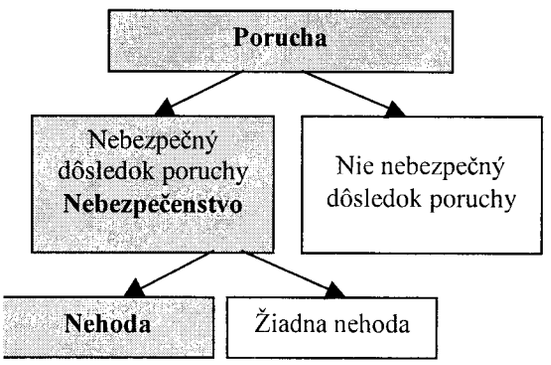
$$E(a) = \sum_{i=1}^{n} a_i . p_i \quad (6)$$

je očakávaná hodnota dôsledkov nebezpečenstiev, potom

$$R = E(a) \sum_{i=1}^{n} h_i . \quad (7)$$

## 3. VZŤAH MEDZI PORUCHOU, NEBEZPEČENSTVOM A NEHODOU

Na obr. 1 je znázornená všeobecná genéza od poruchy až k nehode.




*Obr. 1. Vzťah medzi poruchou, nebezpečenstvom a nehodou*
*Fig. 1. Relationship among failure, hazard and accident*

Je zrejmé, že nie každá porucha systému má primárne za následok nebezpečenstvo a výskyt nebezpečenstva ešte nemusí viesť k nehode. Tento fakt treba rešpektovať pri analýze rizika. Riziko bude závislé od pravdepodobnosti výskytu nebezpečného stavu systému (vlastnosť systému) a od pravdepodobnosti výskytu nehody pri uvažovanom nebezpečenstve (podmienky aplikácie). Ak hodnoty týchto pravdepodobností nie sú známe, možno prijať veľmi pesimistický predpoklad, že každá porucha resp. každé nebezpečenstvo má za následok nehodu.

Aj napriek všetkým bezpečnostným opatreniam treba predpokladať, že systém môže prejsť do nebezpečného stavu (relatívnosť bezpečnosti). Počas trvania nebezpečenstva „sa čaká" na vhodnú prevádzkovú situáciu, aby nebezpečenstvo prerástlo do nehody. Je zrejmé, že pravdepodobnosť nehody bude závisieť aj od času trvania nebezpečenstva. Tento čas je závislý od prevádzkovej situácie a jeho určenie je veľmi problematické. Pri analýze rizika možno určenie času trvania nebezpečenstva „obísť" uvažovaním počtu nehôd za určitú časovú jednotku. Čas trvania nebezpečenstva nemožno stotožniť s časom detekcie jednoduchej poruchy v súvislosti s analýzou dôsledkov viacnásobných porúch systému.

### 3.1 Analýza nebezpečenstiev

Dôležitou časťou analýzy rizika je definovanie hraníc pôsobnosti systému a riadeného procesu. Vzhľadom na tieto hranice možno určiť súvislosť medzi uvažovaným nebezpečenstvom a systémom alebo riadením procesom.

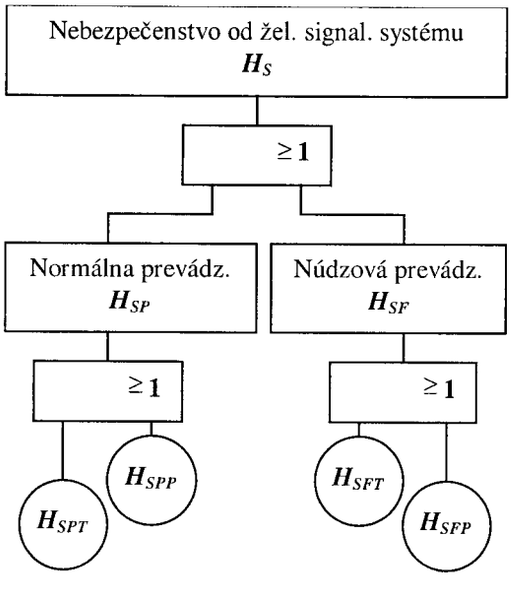
Zlyhanie železničného signalizačného systému je spojené s dvoma druhmi nebezpečenstiev:

- primárne nebezpečenstvá – dôsledkom chybného výkonu riadiacej funkcie systémom môže byť ohrozený dopravný proces;
- sekundárne nebezpečenstvá – systém disponuje ochrannými mechanizmami, ktoré po detekcii poruchy uvedú systém do bezpečného stavu; bezpečný stav je charakterizovaný čiastočným alebo úplným obmedzením vykonávania riadiacich funkcií; v tomto prípade výkon riadiacich funkcií preberá obslužný personál; riziko vyplývajúce z existencie týchto nebezpečenstiev bude, okrem iného, úmerné pravdepodobnosti zlyhania obslužného personálu a času výpadku systému (časti systému).

Pre výpočet rizika je nutné identifikovať nebezpečenstvá súvisiace s riadením dopravného procesu (vytvoriť zoznam nebezpečenstiev). Zoznam nebezpečenstiev možno vytvoriť na základe teoretických úvah a analýz, alebo na základe doterajších skúseností s prevádzkou obdobných systémov a štatistických údajov, najčastejšie však vhodnou kombináciou týchto dvoch možností. Čo treba považovať za nebezpečenstvo záleží od úrovne systémovej analýzy. Výsledok analýzy rizika nezávisí od kvantity identifikovaných nebezpečenstiev, ale závisí od toho, ako je pokrytý celý priestor nebezpečných stavov systému. Zo štatistiky nehôd možno spravidla zistiť, že príčinou nehody bola chybná činnosť vonkajšieho objektu (prestavenie výhybky pred alebo pod idúcim vlakom, nesprávna poloha výhybky, falošné hlásenie voľnosti úseku, ....), aj keď spravidla skutočná

príčina sa nachádza v chybnej logike systému. Na úrovni vonkajších objektov prichádzajú do úvahy, napríklad pre návestidlo, tieto nebezpečenstvá:
- falošné rozsvietenie dovoľujúceho návestného znaku;
- nesvietenie zakazujúceho návestného znaku;
- falošné rozsvietenie viac dovoľujúceho návestného znaku;
- atď.

Príčinou nebezpečenstva vyplývajúceho z prevádzky železničného signalizačného systému môže byť aj omyl obslužného personálu pri výkone bezpečnostne relevantných činností súvisiacich s riadením pohybu vlaku. Vo všeobecnosti možno uvažovať s rôznym podielom obslužného personálu na výkone riadiacich funkcií:
- žiadny - systém je funkčný a v plnom rozsahu kontroluje bezpečnostne relevantné povely vydávané obslužným personálom;
- čiastočný:
  - systém je funkčný, ale jeho technické riešenie neumožňuje v plnom rozsahu kontrolovať všetky bezpečnostne relevantné povely vydávané obslužným personálom;
  - systém je čiastočne funkčný; niektoré bezpečnostne relevantné úkony vykonáva obslužný personál bez následnej kontroly systémom;
- úplný:
  - systém je nefunkčný; všetky bezpečnostne relevantné úkony vykonáva obslužný personál bez následnej kontroly systémom.




*Obr. 2. Strom príčin nebezpečenstva*
*Fig. 2. The tree of hazard causes*

Strom príčin nebezpečenstva súvisiaceho so zlyhaním železničného signalizačného systému (obr. 2) vyjadruje kauzálnu závislosť medzi príčinami vzniku nebezpečenstva. Vo všeobecnosti je spravidla príčinou nebezpečenstva zlyhanie technických alebo organizačných opatrení, ktoré boli vykonané na zaistenie bezpečnosti dopravy.

Kauzálnu závislosť medzi príčinami vzniku nebezpečenstva (základné udalosti) a neželanou vrcholovou udalosťou možno pre strom na obr. 2 opísať logickou funkciou

$$H_S = H_{SPT} + H_{SPP} + H_{SFT} + H_{SFP}, \quad (8)$$

kde $H_{SPT}$ je základná udalosť – zlyhanie technického prostriedku pri normálnej prevádzke, $H_{SPP}$ je základná udalosť – omyl obslužného personálu pri normálnej prevádzke, $H_{SFT}$ je základná udalosť – zlyhanie technického prostriedku pri núdzovej prevádzke, $H_{SFP}$ je základná udalosť – omyl obslužného personálu pri núdzovej prevádzke.

Ak sú známe intenzity výskytu základných udalostí uvedených v rovnici (1), potom možno intenzitu výskytu nebezpečenstva súvisiaceho so zlyhaním železničného signalizačného systému vypočítať zo vzťahu:

$$h_S = h_{SPT} + h_{SPP} + h_{SFT} + h_{SFP}, \quad (9)$$

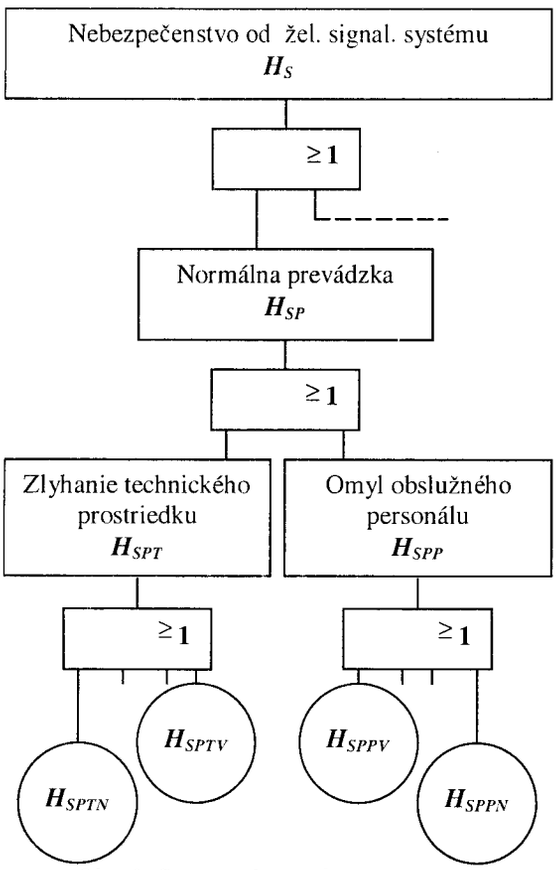
kde $h_i$ je intenzita výskytu *i-tej* základnej udalosti (nebezpečenstva) v strome na obr. 2.

Ak za normálnej prevádzky systému sa obslužný personál nepodieľa na výkone bezpečnostne relevantných funkcií ($h_{SPP} = 0\ h^{-1}$) a za núdzovej prevádzky systému platí, že $h_{SFT} \langle\langle h_{SFP}$, potom

$$h_S = h_{SPT} + h_{SFP}. \quad (10)$$

Ďalší rozvoj časti stromu príčin nebezpečenstva z obr. 2 je znázornený na obr. 3. Zlyhanie technického prostriedku môže mať pôvod napríklad v zlyhaní riadenia návestidla $H_{SPTN}$ alebo v zlyhaní riadenia výhybky $H_{SPTV}$. Omyl obslužného personálu môže mať za dôsledok napríklad chybný povel pre návestidlo $H_{SPPN}$ alebo chybný povel pre výhybku $H_{SPPV}$.

Aj nebezpečenstvá identifikované na úrovni vonkajších objektov systému možno ďalej analyzovať a hľadať príčiny týchto nebezpečenstiev v existencii porúch na nižšej úrovni architektúry systému. Takáto analýza má zmysel len vtedy, ak možno exaktne vyjadriť vzťah medzi pravdepodobnosťou poruchy prvku (modulu) na nižšej úrovni systému a pravdepodobnosťou nebezpečenstva na úrovni vonkajšieho objektu systému. Treba si uvedomiť, že tá istá porucha prvku (modulu) môže mať za následok, v závislosti od stavu systému, výskyt rôznych druhov nebezpečenstiev.




*Obr. 3. Strom príčin nebezpečenstva*
*Fig. 3. The tree of hazard causes*

Intenzita zlyhania technického prostriedku za normálnej prevádzky systému zodpovedá intenzite nebezpečných porúch systému.

Je zrejmé, že intenzita omylov obslužného personálu je podstatne väčšia ako intenzita nebezpečného zlyhania systému, najmä ak ide o fail-safe systém. Intenzita omylu jednotlivca závisí od mnohých objektívnych (počet úkonov, čas na vykonanie úkonu, zložitosť úkonu, ....) aj subjektívnych (zmysel pre zodpovednosť, psychická pohoda, kvalifikačná úroveň, ...) faktorov [8].

### 3.2 Analýza nehôd a ich dôsledkov

Vo všeobecnosti nebezpečenstvá vyplývajúce z používania železničného signalizačného systému môžu viesť k rôznym druhom nehôd. Napríklad:

- narazenie železničného koľajového vozidla do iného železničného koľajového vozidla zozadu;
- narazenie železničného koľajového vozidla do iného železničného koľajového vozidla zboku;
- narazenie železničného koľajového vozidla do iného železničného koľajového vozidla spredu;
- narazenie železničného koľajového vozidla do vozidla cestnej dopravy alebo chodca;
- narazenie vozidla cestnej dopravy do železničného koľajového vozidla (bočný náraz);
- vykoľajenie železničného koľajového vozidla;
- atď.

Tak ako porucha prvku systému môže byť príčinou rôznych nebezpečenstiev, tak aj nebezpečenstvo môže, v závislosti od konkrétnych prevádzkových pomerov, byť príčinou rôznych druhom nehôd. Preto treba pri analýze rizika, každé nebezpečenstvo uvažovať vo vzťahu ku všetkým druhom nehôd, pričom pravdepodobnosť výskytu jednotlivých druhov nehôd pri určitom nebezpečenstve bude spravidla vždy rôzna a závislá od parametrov prevádzky (napríklad intenzity dopravy).

Dôsledkom nehody môžu byť humánne, materiálne alebo iné škody. Ak je reálna hrozba úmrtia človeka alebo výrazného poškodenia jeho zdravia, tak materiálne škody sa spravidla považujú za nepodstatné a potom sa pri analýze rizika ani neuvažujú. Humánne škody možno ohodnotiť počtom smrteľných úrazov

$$S_N = S_M + k_Z.S_Z + k_L.S_L\,, \qquad (11)$$

kde $S_M$ je počet smrteľných úrazov, $S_Z$ je počet ťažkých úrazov, $S_L$ je počet ľahkých úrazov, $k_Z$ je koeficient akceptovania ťažkých úrazov a $k_L$ je koeficient akceptovania ľahkých úrazov. Napríklad, v informatívnej časti normy [1] sú uvažované hodnoty koeficientov $k_Z = 10$ a $k_L = 100$.

Dôsledky nehody závisia od druhu nehody a od konkrétnej prevádzkovej situácie. V podstate však nezávisia od železničného signalizačného systému. Vzhľadom na konkrétnu prevádzkovú situáciu treba pri analýze rizika zohľadniť najmä rýchlosť, pri ktorej k nehode došlo a počet osôb nachádzajúcich sa v zóne ohrozenia.

Pri zisťovaní vplyvu rýchlosti na dôsledok nehody možno vychádzať z predpokladu, že štatistiky nehodovosti obsahujú údaj o rýchlosti, pri ktorej k nehode došlo a na základe tohto údaja možno nehody rozdeliť do skupín v závislosti od ich druhu a rýchlosti.

Ak je železničný signalizačný systém funkčný alebo čiastočne funkčný, potom treba pri analýze rizika uvažovať s dôsledkami zodpovedajúcimi najvyššej rýchlosti, pre ktorú je systém vyvíjaný. V prípade nefunkčného systému (žiadne úkony obslužného personálu nekontroluje systém) možno uvažovať pri analýze rizika s rýchlosťou zodpovedajúcou núdzovému režimu (napríklad 40 km.h$^{-1}$).

Určenie vzťahu medzi počtom osôb nachádzajúcich sa v zóne ohrozenia a dôsledkom nehody je veľmi obtiažne. Pri analýze rizika možno vychádzať z počtu osôb priamo zúčastnených na nehode a z významu účasti týchto osôb na nehode (napríklad je rozdiel či pri zrážke vlaku s automobilom uvažovaná osoba sa nachádza vo vlaku alebo v automobile, ....).

Nie každé nebezpečenstvo nutne musí viesť k nehode. Nebezpečenstvo však môže mať za následok rôzne druhy nehôd. Pravdepodobnosť *j-tej* nehody v dôsledku výskytu *i-tého* nebezpečenstva

$$d_{ij} = \frac{K_{ij}}{H_i}\,, \qquad (12)$$

kde $K_{ij}$ je počet nehôd *j-tého* druhu v dôsledku výskytu *i-tého* nebezpečenstva za sledované obdobie, $H_i$ je počet *i-tých* nebezpečenstiev za sledované obdobie.

Štatistiky spravidla neudávajú počet nebezpečenstiev a ich dôsledky, ale udávajú nehody, ich dôsledky a ich príčiny (príčina môže byť totožná s nebezpečenstvom, ktoré zodpovedá určitému nebezpečnému stavu analyzovaného systému). Pri pesimistickom predpoklade, že každé nebezpečenstvo má za následok nehodu

$$d_{ij} = \frac{K_{ij}}{\sum_{j=1}^{m} K_{ij}}, \qquad (13)$$

kde $m$ je počet druhov nehôd, $K_j$ je počet nehôd *j-tého* druhu za sledované obdobie a $H_i \geq \sum_{j=1}^{m} K_{ij}$.

Ak pre výpočet $d_{ij}$ je použitý vzťah (13), potom $\sum_{j=1}^{m} d_{ij} = 1$.

Očakávaná hodnota dôsledkov nehôd pri výskyte *i-tého* nebezpečenstva je daná vzťahom:

$$E_i(a) = \sum_{j=1}^{m} a_{ij}.d_{ij}, \qquad (14)$$

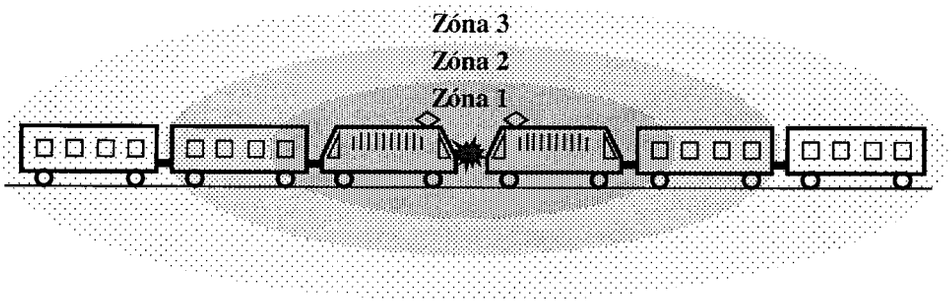
pričom

$$a_{ij} = \frac{S_{ij}}{K_{ij}}, \qquad (15)$$

kde $S_{ij}$ sú uvažované škody *j-tej* nehody v dôsledku výskytu *i-tého* nebezpečenstva.
Potom

$$R = \sum_{i=1}^{n} h_i \cdot \left( \sum_{j=1}^{m} a_{ij}.d_{ij} \right). \qquad (16)$$

Ak vývoj nového systému je založený na analýze rizika vychádzajúcej z existujúcich štatistických údajov, ktoré sú závislé od intenzity dopravy (vplýva na počet nehôd) a počtu prepravovaných osôb (vplýva na dôsledky nehody), potom treba zaistiť, aby vypočítané hodnoty tolerovateľných intenzít nebezpečných porúch systému rešpektovali prípadné zmenu intenzity dopravy a počtu prepravovaných osôb v závislosti od miesta aplikácie systému. Takúto vlastnosť systému možno dosiahnuť tak, že pri výpočte rizika sa predpokladá, že každé nebezpečenstvo vedie k nehode a že dôsledky $a_{ij}$ sa prepočítajú na jedného normovaného účastníka nehody. Normovanie zohľadňuje zónu a počet ohrozených osôb nachádzajúcich sa v príslušnej zóne (obr. 4).




*Obr. 4. Príklad rozloženia zón ohrozenia pri čelnej zrážke vlakov*
*Obr. 4. Example of arrangement of endangering zones in head-on train collision*

Napríklad, nech sú uvažované tri zóny ohrozenia, potom

$$N_N = k_1.N_1 + k_2.N_2 + k_3.N_3, \qquad (17)$$

kde $N_i$ je počet ohrozených osôb nachádzajúcich sa v *i-tej* zóne a $k_i$ je koeficient prislúchajúci *i-tej* zóne ohrozenia. Potom dôsledky *j-tého* druhu nehody pri výskyte *i-tého* nebezpečenstva prepočítané na jedného normovaného účastníka nehody normovaného účastníka nehody

$$a_{ij}^{l} = \frac{a_{ij}}{N_N}. \qquad (18)$$

Pri analýze rizika navrhovaného systému treba vychádzať z predpokladaných podmienok aplikácie systému a dôsledky prepočítať na predpokladaný počet osôb nachádzajúcich sa v zónach ohrozenia

$$a_{ij} = a_{ij}^{l}.N_N^P, \qquad (19)$$

kde $N_N^P$ je prepočítaný počet osôb v závislosti od predpokladaného počtu osôb nachádzajúcich sa v zónach ohrozenia.

Vo všeobecnosti možno riziko spojené s používaním systému rozdeliť na

$$R_S = R_{SPT} + R_{SPP} + R_{SF}, \qquad (20)$$

kde $R_S$ je riziko vyplývajúce s používania železničného signalizačného systému, $R_{SPT}$ je riziko, keď systém je funkčný (neuvažuje sa s intenzitou omylov obslužného personálu; uvažuje sa s dôsledkami nehody pre najvyššiu rýchlosť) $R_{SPP}$ je riziko, keď systém je čiastočne funkčný (uvažuje sa s intenzitou omylov obslužného personálu aj s intenzitou zlyhania technického prostriedku; uvažuje sa s dôsledkami nehody pre najvyššiu rýchlosť) a $R_{SF}$ je riziko, keď systém je nefunkčný (uvažuje sa len intenzitou omylov

obslužného personálu; uvažuje sa s dôsledkami nehody pre rýchlosť zodpovedajúcu núdzovému režimu).

## 4. AKCEPTOVATEĽNÉ RIZIKA

Z dôvodu bezpečnosti sa požaduje, aby

$$R_S \leq R_{AK}, \qquad (21)$$

kde $R_{AK}$ je akceptovateľné riziko pre použitie systému.

Kritériá akceptovania rizika môžu byť implicitné aj explicitné. Explicitné kritériá požadujú ohodnotenie rizika, zatiaľ čo pre implicitné kritériá musí byť dokázané, že nový systém je minimálne tak bezpečný ako zavedený referenčný systém.

Norma [1] uvádza niekoľko pravidiel (ALARP, GAMAB, MEM) na hodnotenie akceptovateľného rizika. Všeobecne možno konštatovať, že systém sa považuje za bezpečný vtedy, keď individuálne riziko pre každého jednotlivca prichádzajúceho do styku so systém je menšie ako definovaná hraničná hodnota. Napríklad pravidlo MEM (*minimum endogeneous mortality*) je založené na odhade individuálneho rizika a vychádza z predpokladu, že k úmrtiu jednotlivca môže dôjsť v dôsledku choroby, vrodenej vady alebo „technologickej príčiny" (činnosti jednotlivca spojené s dopravou, športom, pracovnou činnosťou, ...). Úmrtnosť spôsobená „technologickými príčinami" sa označuje ako endogenná úmrtnosť. Táto úmrtnosť je v rozvinutých krajinách najmenšia pre vekovú skupinu 5 – 15 rokov a zodpovedá jej hodnota rizika $2.10^{-4}$ smrteľných úrazov / osobu . rok. Keďže podľa normy [1] nemá použitie technického systému výšiť toto riziko viac ako o 5 %, možno pre výpočet rizika použiť hodnotu akceptovateľného rizika úmrtnosti jednotlivca $R_{AKJ} \leq 1.10^{-5}$ smrteľných úrazov / osoba . rok.

Určenie hraničnej hodnoty akceptovateľného rizika je najmä legislatívny problém.

## 5. ZÁVER

Analýza rizika musí byť uskutočnená niekoľkokrát (s rôznou hĺbkou) počas vývoja systému. V počiatočnej fáze vývoja systému slúži na definovanie akceptovateľných intenzít nebezpečenstiev systému alebo jeho jednotlivých častí. V ďalších fázach vývoja systému slúži na kontrolu, či skutočné hodnoty intenzít nebezpečenstiev systému alebo jeho jednotlivých častí sú akceptovateľné.

Na základe výsledkov kvantitatívnej analýzy rizika možno jednotlivým častiam systému priradiť úroveň integrity bezpečnosti (*SIL - Safety Integrity Level*) [3].

Ak sa požaduje, aby riziko ohrozenia jednotlivca systémom nepresiahlo počas celého užitočného života systému definovanú hodnotu, potom treba stanoviť krajné (limitné) hodnoty pre tie podmienky aplikácie systému, ktoré majú vplyv na veľkosť ohrozenia jednotlivca (intenzita dopravy, traťová rýchlosť, ...). To znamená, že systém bude pracovať s menším rizikom, ako bolo vypočítané, ak konkrétna aplikácia systému bude vyhovovať definovaným okrajovým podmienkam, ktoré boli uvažované pri analýze rizika. Prakticky možno postupovať tak, že okrajové podmienky sa zvolia v závislosti od kategórie tratí, pre ktoré je systém určený.

Článok bol spracovaný za podpory grantovej úlohy VEGA 1/8182/01: Teoretické podklady pre výpočet akceptovateľného rizika v riadení dopravného procesu, najmä železničného.

## LITERATÚRA

[1] STN EN 50 126: Dráhové aplikácie. Stanovenie a preukázanie bezporuchovosti, pohotovosti, udržiavatelnosti a bezpečnosti (RAMS). 1999.

[2] STN EN 50 128: Dráhové aplikácie. Komunikačné a signalizačné systémy a systémy na spracovanie údajov. Softvér pre železničné riadiace a ochranné systémy. 2003.

[3] STNP ENV 50 129: Dráhové aplikácie. Pevné inštalácie. Elektronické signalizačné systémy súvisiace s bezpečnosťou. 2001.

[4] STN EN 50 159-1: Dráhové aplikácie. Pevné inštalácie. Komunikačné, signalizačné a procesné systémy. Časť 1: Komunikácia súvisiaca s bezpečnosťou v uzavretých prenosových systémoch. 2003.

[5] STN EN 50 159-2: Dráhové aplikácie. Pevné inštalácie. Komunikačné, signalizačné a systémy na spracovanie údajov. Časť 2: Komunikácia súvisiaca s bezpečnosťou v otvorených prenosových systémoch .2003.

[6] STN IEC60300-3-9: Manažérstvo spoľahlivosti. Časť 3: Návod na používanie. Oddiel 9: Analýza rizika technických systémov. 2000.

[7] STN EN 61508: Funkčná bezpečnosť elektrických/elektronických/programovateľných elektronických bezpečnostných systémov. 2002.

[8] Gertman, D. I.; Blackman, H. S.: Human Reliability & Safety Analysis Data Handbook. John Wiley & Sons, Inc., 1993.

[9] Vose, D.: Risk Analysis. John Wiley & Sons, Ltd., 2000.

[10] Bradley, J.: Elimination of Risk in Systems.Tharsis Books, 2002.