PŘÍSPĚVEK K ANALÝZE RIZIKA MODULU AUTOMATICKÉHO VEDENÍ VLAKU

CONTRIBUTION TO RISK ANALYSIS OF AUTOMATIC TRAIN CONTROL MODULE

Jan Famfulík[1], Jana Míková[2]

Anotace: Příspěvek je věnován metodám hodnocení rizika dle ČSN EN 61508. S využitím principu ALARP je stanovena třída rizika a následně s využitím diagramu rizika je určena úroveň integrity bezpečnosti SIL. Příspěvek uvádí příklad využití těchto postupů u zařízení automatického vedení vlaku.

Klíčová slova: úroveň integrity bezpečnosti, SIL, ALARP, automatické vedení vlaku

Summary: The contribution deals with methods of risk assessment according to the standard ČSN EN 61508. The risk category is assessed with use of ALARP principle and subsequently the safety integrity level SIL is determined using a risk diagram. The contribution presents an example of these procedures utilization for automatic train control module.

Key words: safety integrity level, SIL, ALARP, automatic train control

1. ÚVOD

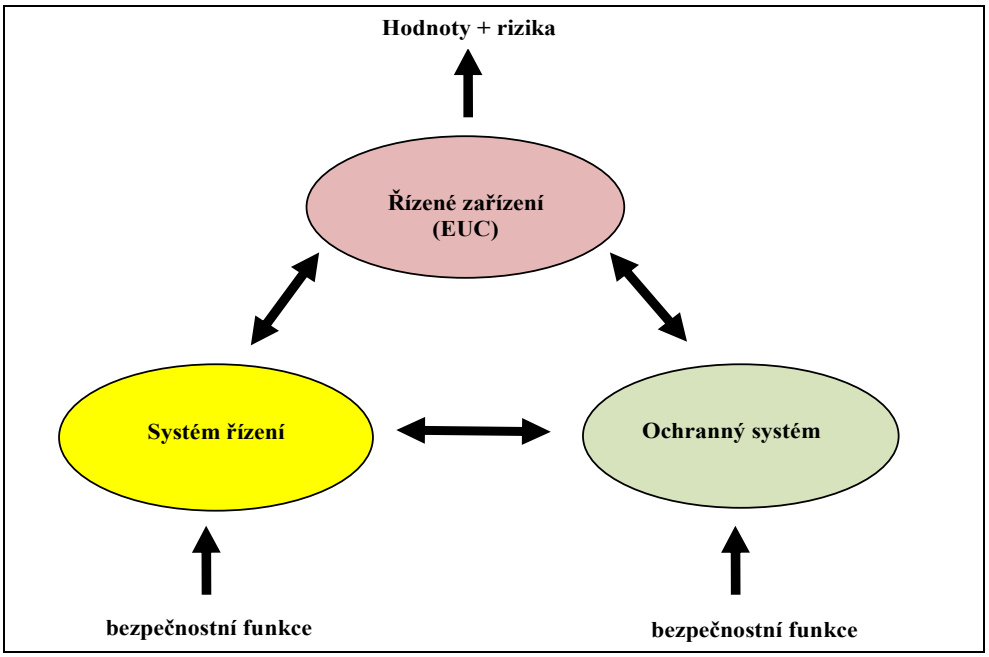
V současné době ve všech odvětvích průmyslu se do popředí zájmu dostávají otázky týkající se zajištění bezpečné funkce řídicích systémů a procesů. Pojem funkční bezpečnost podle platných norem IEC představuje mezinárodně platný bezpečnostní standard pro zařízení, kde elektrické, elektronické a programovatelné elektronické jednotky plní bezpečnostní funkce. Hlavním cílem správné aplikace funkční bezpečnosti je snížení rizika možnosti zranění lidí, velkých materiálních ztrát nebo poškození životního prostředí. Problémem je navrhnout takový systém, který by zabránil vzniku nebezpečných poruch, nebo alespoň ve smyslu bezpečnosti kontroloval jejich výskyt.

Problematika funkční bezpečnosti je řešena v normě ČSN EN 61508 Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů (Functional safety of electrical/electronic/programmable electronic systems). Přestože se norma omezuje na bezpečnostní prvky závislé na hardwaru a softwaru E/E/PE systémů, její zásady jsou obecné a tvoří základ bezpečnosti i jiných systémů, a proto je tato norma obecným dokumentem určeným pro všechna odvětví průmyslu.

Principy výše uvedené normy lze chápat jako správnou metodu řízení zaměřeného na funkční bezpečnost. Norma ČSN EN 61508 vychází z modelu na Obr. 1. Výchozí je řízené zařízení, které spolu se svým řídicím systémem vytváří určité hodnoty (např. systém

[1] Ing. Jan Famfulík, Ph.D., Vysoká škola báňská – Technická Univerzita Ostrava, Fakulta strojní, Institut dopravy, 17. listopadu 15, 708 03 Ostrava – Poruba, Tel: +420 596 994 553, E-mail: jan.famfulik@vsb.cz
[2] Ing. Jana Míková, Ph.D., Vysoká škola báňská – Technická Univerzita Ostrava, Fakulta strojní, Institut dopravy, 17. listopadu 15, 708 03 Ostrava – Poruba, Tel: +420 596 994 553, E-mail: jana.mikova@vsb.cz

automatického vedení vlaku u hnacích vozidel), ale které je současně zdrojem nebezpečí pro své okolí.



Zdroj: [2]

Obr. 1 - Riziko a bezpečnostní funkce k jeho zmenšení

2. ANALÝZA RIZIKA

Požadavky na bezpečnostní funkce musíme přidělit přístrojovým systémům bezpečnosti a jejich ochranným vrstvám, přičemž musíme dodržet všechny požadavky na proces přiřazení těchto bezpečnostních funkcí. Pro každou nebezpečnou událost se musí stanovit nutné snížení rizika, přičemž toto snížení může být určeno kvantitativním a/nebo kvalitativní způsobem.

2.1. Problém určení meze přijatelnosti rizika

S problémem snížení rizika souvisí otázka, jaké riziko je přijatelné. Principiálně musí být přijatelnost rizika založená na všeobecně uznávaných zásadách. Například norma ČSN EN 50126 doporučuje použití následujících principů:

Princip ALARP

Tento princip je používán ve Velké Británii. Zkratka ALARP znamená „co nejnižší rozumně dosažitelné riziko“ a označuje, že se vývojář musí snažit dosáhnout co nejnižšího rizika a u hazardních stavů, kde se nepodaří dosáhnout všeobecně uznávané hodnoty, může být riziko uznáno (není-li hodnota příliš vysoká), pokud se prokáže, že jej nelze rozumným způsobem dále snížit. Prokázání lze opřít o použití nejnovějších technických prostředků, platných standardů apod.

Princip GAMAB

Tento princip je používán ve Francii, říká, že nové zařízení musí být při celkovém hodnocení nejméně tak bezpečné, jako kterýkoli stávající ekvivalentní systém. Je zde ponechána určitá volnost, některý jednotlivý parametr může být u nového zařízení mírně horší, ale nesmí jít o parametr zásadní a celkově musí jít o snížení rizika oproti stávajícímu stavu.

Princip MEM

Tento princip je používán v Německu. Zkratka MEM znamená „minimální endogenní úmrtnost – Rm“, což je úmrtnost způsobená technologickými příčinami, např. pracovními stroji, dopravou ale i sportem a jinými aktivitami ve volném čase. Nepatří sem nemoci či vrozené vady apod. Tato endogenní úmrtnost je minimální pro věkovou skupinu 5 až 15 let ve vyspělých zemích a byla stanovena hodnota: Rm = 2 x 10^{-4} úmrtí/(osoba x rok). Hazardní stavy nového zařízení, by neměly tato číslo významně zvýšit. Akceptovaná hodnota je např. Rz = 10^{-5} úmrtí/(osoba x rok). Aplikací zvoleného principu získáme pro dané zařízení tzv. tolerovanou četnost rizik.

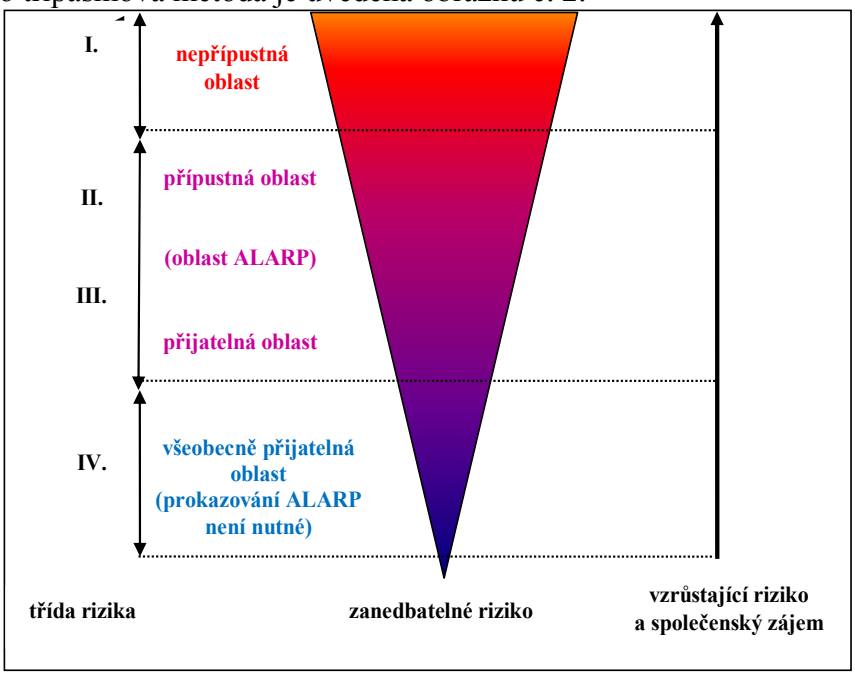
U zařízení posuzovaných podle ČSN EN 61508 nejčastěji používá postup založený na principu ALARP.

2.2. ALARP - koncepce nejnižšího rozumně možného a přijatelného rizika

Princip ALARP je konkrétní metoda pro dosažení přípustného rizika. Kategorizace rizika je ohodnocena do třech různých stupňů následovně [2]:

a) dané riziko je tak velké, že je nutné jej zcela odmítnout,
b) dané riziko je mezi dvěma předchozími stavy a už bylo sníženo na nejnižší možnou úroveň, s přihlédnutím na přínosy, které plynou z jeho přijetí a se zvážením nákladů na jakékoliv jeho další snížení,
c) dané riziko je tak malé (nebo bylo provedeno tak malým), že je bezvýznamné.

V případě a) princip ALARP vyžaduje snížení jakéhokoliv rizika na co nejnižší možnou úroveň nebo na co nejnižší rozumně proveditelnou úroveň. Je-li riziko někde mezi těmito dvěma extrémy, tzn. mezi nepřijatelnou oblastí a oblastí všeobecně přijatelnou, a v případě, že byl použit princip ALARP, potom je výsledné riziko u konkrétní aplikace rizikem přípustným. Tato třípásmová metoda je uvedena obrázku č. 2.



Zdroj: [2]

Obr. 2 - Model ALARP

Z obrázku je patrné, že nad určitou úrovní se riziko považuje za nepřípustné a za žádných okolností ho nelze ospravedlnit. Jestliže takovéto riziko existuje, mělo by být sníženo

tak, aby se dostalo do buď „přípustné, přijatelné“ nebo „všeobecně přijatelné“ oblasti, nebo s ním spojené nebezpečí musí být odstraněno.

Pod úrovní nepřípustná oblast, se nachází přípustná a přijatelná oblast – oblast ALARP, kde je možné provádět dané činnosti. Provádět dané činnosti je dovoleno za předpokladu, že s nimi spojená rizika byla snížena na co nejnižší rozumně proveditelnou úroveň. Všeobecně platí, že čím vyšší je riziko, tím více úsilí se dá očekávat k jeho snížení. Riziko, jež bylo tímto způsobem sníženo, se pokládá za riziko snížené na úroveň, která je „nejnižší rozumně možná“ (ALARP).

Poslední úrovní je všeobecně přijatelná oblast, není nutné podrobně prokazovat ALARP, přesto je nutné věnovat pozornost tomu, aby se riziko na této určité úrovni udrželo.

Jedním ze způsobů, jak lze dosáhnout cíle přípustného rizika, je stanovení určitého počtu následků, jimž se přiřadí přípustné četnosti. Toto slaďování následků a jim přiřazených četností by mělo být ve formě diskusí a dohod mezi zainteresovanými stranami. Pro zohlednění koncepce ALARP může být toto slaďování provedeno prostřednictvím tříd rizik viz. Obr. 2. Klasifikace tříd a výklad rizika je uveden v tabulce č. 1.

Pro každou charakteristickou situaci nebo srovnatelnou dopravního průmyslu je nutné sestavit tabulku č. 2, která zahrnuje široký rozsah sociálních, politických a ekonomických činitelů. Každému následku by měla odpovídat určitá četnost a v tabulce by měly být uvedeny třídy rizika.

Tab. 1 - Výklad tříd rizika dle ČSN EN 61508-5

Třída rizika	**Výklad rizika**
Třída I.	Nepřípustné riziko
Třída II.	Nežádoucí riziko, přípustné pouze v případě, že snížení rizika je neproveditelné nebo v případě, že náklady jsou výrazně neúměrné dosaženému zlepšení.
Třída III.	Přípustné riziko v případě, že náklady na snížení rizika by, přesáhly dosažené zlepšení.
Třída IV.	Zanedbatelné riziko

Zdroj: [2]

Tab. 2 - Příklad klasifikace rizika nehod dle koncepce ALARP

Četnost	**Následek**			
	Katastrofální	**Kritický**	**Nepodstatný**	**Zanedbatelný**
Častá	I	I	I	II
Pravděpodobná	I	I	II	III
Příležitostná	I	II	III	III
Málo častá	II	III	III	IV
Nepravděpodobná	III	III	IV	IV
Neuvěřitelná	IV	IV	IV	IV
Poznámka: Tuto tabulku je nutné brát pouze jako příklad toho, jak by taková tabulka mohla být vyplněna. Skutečný stav pro všechny třídy rizika závisí na oblasti použití a také na tom, jaké jsou skutečné hodnoty četnosti pro konkrétní četnosti uvedené v tabulce.				

Zdroj: [2]

3. VYUŽITÍ DIAGRAMU RIZIKA PRO STANOVENÍ MÍRY INTEGRITY BEZPEČNOSTI

V případě použití této kvalitativní metody, je nutné zavést z důvodů zjednodušení omezený počet parametrů, jež ale charakterizují základní vlastnosti nebezpečné situace v případě selhání nebo nedostupnosti systémů souvisejících s bezpečností. U každého se čtyř rizikových parametrů se provede jeho klasifikace, parametry se dále vzájemně kombinují pro rozhodnutí o tom, jaká úroveň integrity bezpečnosti se systémům přiřadí (tab. č. 3). Čím je vyšší úroveň integrity bezpečnosti, tím účinněji dochází ke snížení rizika.

3.1 Diagram rizika - obecné schéma

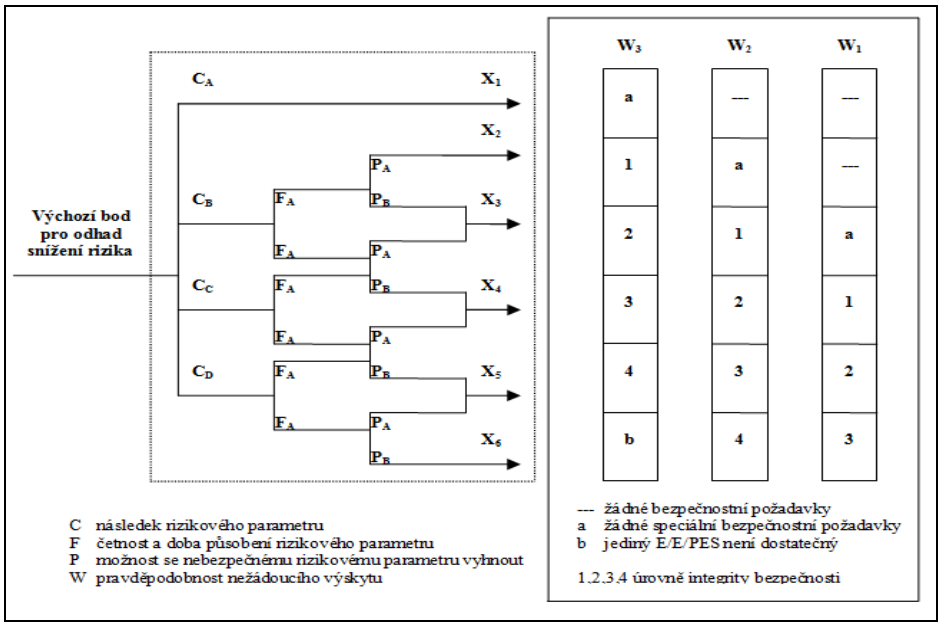
Parametry uvedené na obrázku č. 3 a jejich vyhodnocování jsou potřebné pro každou charakteristickou situaci nebo dané srovnatelné oblasti průmyslu.

Tab. 3 - Vzorové údaje pro sestavení diagramu rizika

Rizikový parametr		Klasifikace	Pozn.
Následek (C)	C_1 C_2 C_3 C_4	Menší zranění Zranění jedné nebo více osob s trvalými následky, smrt jedné osoby Smrt několika osob Smrt velkého počtu osob	Systém klasifikace je vytvořen pro posouzení zranění nebo smrti osob. Pro hodnocení materiálních škod a škod na životním prostředí je nutné vytvořit jiné klasifikační schémata. Musíme brát v úvahu následky nehod a jejich vyléčení.
Četnost a doba vystavení v nebezpečné oblasti (F)	F_1 F_2	Vzácné až častější vystavení v nebezpečné oblasti Časté až trvalé vystavení v nebezpečné oblasti	Parametr zohledňuje: -četnost a dobu, po kterou jsou osoby vystaveny nebezpečí.
Možnost se nebezpečné události vyhnout (P)	P_1 P_2	Možné za určitých podmínek Téměř nemožné	Parametr zohledňuje: - upozornění obsluhy, že systém selhal - možnost zabránit nebezpečné události za určitých podmínek - dostatečná doba k zabránění nebezpečné události
Pravděpodobnost nežádoucího výskytu (W)	W_1 W_2 W_3	Velmi malá pravděpodobnost Malá pravděpodobnost Poměrně vysoká pravděpodobnost	Účelem činitele W je odhad četnosti nežádoucího výskytu bez přidání jakýchkoliv systémů souvisejících s bezpečností, ale včetně všech vnějších prostředků pro snížení rizika. V případě malých zkušeností s EUC se může odhad činitele W provést výpočtem. Pak musíme provést předpověď nejhoršího případu.

Zdroj: [2]

1) Použití parametrů rizika *C*, *F* a *P* vede na několik výstupů X_1, X_2,X_3,…X_n. Každý z těchto výstupů je mapován do jedné ze tří stupnic (W_1,W_2,*a* W_3). Každý stupeň těchto stupnic vyznačuje nutnou integritu bezpečnosti, kterou musí uvažovaný E/E/PE systém související s bezpečností splňovat.
2) Mapování do W1,W2 nebo W3 dovoluje přispět i dalším opatřením pro snížení rizika. Posunutí stupnic u W1,W2,a W3 je nutné z důvodu možností tří různých úrovní snížení rizika, které jsou zajištěny dalšími opatřeními. Stupnice W3 poskytuje minimální snížení rizika zajišťované od jiných opatření (tj. největší pravděpodobnost nežádoucího výskytu), stupnice W2 střední přínos a stupnice W1 maximální přínos. Pro konkrétní mezilehlý výstup diagramu rizika (tj. X1, X2,X3,…nebo X6) a pro konkrétní stupnici W (tj. W1,W2 nebo W3) poskytuje koncový výstup diagramu rizika úroveň integrity bezpečnosti E/E/PE systému souvisejícího s bezpečností (tj. 1, 2, 3 nebo 4) a u daného systému je mírou požadovaného snížení. Toto snížení rizika spolu s dalšími sníženími rizika získanými od jiných opatření, která jsou zároveň zohledněna mechanizmem stupnic W, poskytuje nutné snížení rizika pro danou situaci.



Zdroj: [2]

Obr. 3 - Diagram rizika

3.2 Příklad využití diagramu rizika pro stanovení míry integrity bezpečnosti

Metoda diagramu rizika byla použita pro určení úrovně rizika u modulu automatického vedení vlaku (AVV). Systém automatického vedení vlaku (AVV) je určen pro automatizaci řízení kolejových vozidel na tratích Českých drah.

Soubor zařízení systému AVV se skládá z funkční (mobilní), traťové a datové části [1]. Mobilní část systému AVV tvoří řídicí počítač, snímače signálů traťových informačních bodů, zadávací klávesnice a displej na stanovišti strojvedoucího. Jádrem řídicího počítače jsou výkonné mikroprocesory. Traťovou část tvoří soubor adresných traťových informačních bodů. Adresná informace je kódována v zabezpečeném kódu a je přenášena na vozidlo pomocí stejnosměrného magnetického pole. Datová část (tzv. Route Map) obsahuje popisy tratí a data z jízdních řádů vlaků a je uložena v mobilní části zařízení (v paměťovém poli řídicího počítače).

Systém AVV poskytuje mimo funkce ručního řízení vozidel ještě funkci řízení vozidla s automatickou regulací rychlosti jízdy (základní režim řízení vozidla) a funkci automatického cílového brzdění a vedení vlaku. Tento systém také umožňuje optimalizovat spotřebu trakční energie při jízdě vlaku.

Systém automatického vedení vlaku realizuje řadu dílčích funkcí. Jednotlivé funkce, resp. jejich selhání, představují různou míru rizika. Proto je nutné provést analýzu rizika jednotlivých funkcí systému, která umožní identifikovat funkce AVV, u kterých v důsledku poruchy je riziko v nepřípustné oblasti [3].

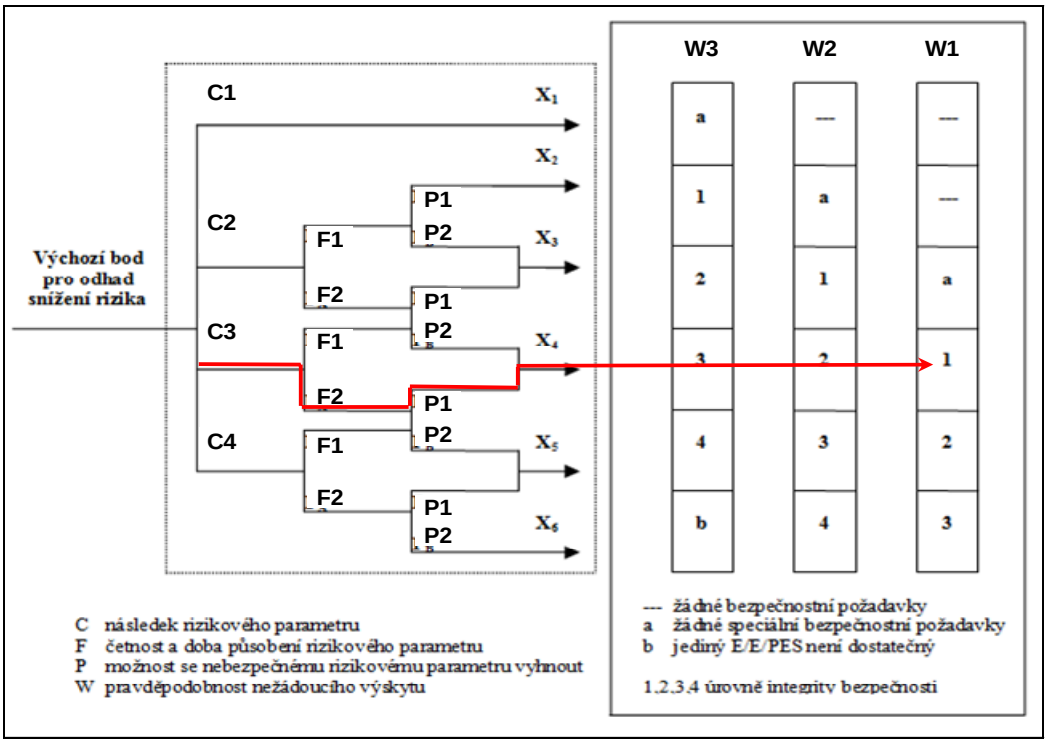
Po provedení analýzy je nutné u některých funkcí provést redukci rizika pomocí dalších technických opatření. Je nutné např. zvýšit diagnostické pokrytí pro identifikaci náhodných poruch hardware, nebo systém navrhnout jako redundantní. Navržené technické opatření vedoucí k redukci rizika jsou klasifikovány pomocí stupně úrovně integrity bezpečnosti (SIL). Úroveň bezpečnosti bezpečnostních funkcí (Safety Integry Llevel – SIL) je vyjádřena číslem z intervalu 1 až 4 Vyšší číslo značí vyšší úroveň integrity bezpečnosti. Čím nebezpečnější mohou být důsledky poruchy bezpečnostních funkcí, tím vyšší musí být stanovená úroveň bezpečnosti.

Příklad klasifikace úrovně rizika a stanovení parametru úrovně integrity bezpečnosti jsou uvedeny v tabulce č. 4 a na obr. č. 4. Při hodnocení úrovně rizika je nutné zahrnout i vliv lidského činitele, v tomto případě strojvedoucího.

Tab. 4 - Vzorové údaje pro sestavení diagramu rizika

Funkce:	4_CRV	Regulace záporného poměrného tahu na základě požadavku (hl. jízdní páka, modul ARR).
Příčina poruchy:	LOG_01	Ztráta signálu při přenosu a zpracování v bloku logiky.
Diagram rizika – parametry rizika		
Parametr	Kategorie	Zdůvodnění
Následek (C)	C3	Porucha může v krajním případě způsobit vykolejení vozidla (zranění osob – C2) nebo projetí návěsti Stůj, nebezpečí srážky vozidel (smrt několika osob – C3). Volí se závažnější následek.
Režim vyžádání (F)	F2	Funkce regulace záporného poměrného tahu je trvalá funkce modulu UniAVV.
Možnost vyhnutí nebezpečné události (P)	P1	Není-li funkce regulace záporného poměrného tahu k dispozici (vlak nebrzdí), strojvedoucímu je tato situace signalizována (tlak v hlavním potrubí), může situaci zabránit (použití rychlobrzdy) a má k tomu dostatečný čas (účinek rychlobrzdy je vyšší než při provozním brzdění).
Pravděpodobnost výskytu (W)	W1	Velmi malá pravděpodobnost z důvodu využití elektronických systémů.

Zdroj: Autoři



Zdroj: Autor

Obr. 4 - Příklad přiřazení úrovně integrity bezpečnosti (SIL) funkci systému AVV

Z obrázku č. 4 vyplývá, že pro posuzovanou funkci ie dostačuiící pro snížení rizika technické opatření na úrovni integrity bezpečnosti SIL1.

4. ZÁVĚR

V České republice prozatím nedošlo k sjednocení názorů na použití metodiky hodnocení minimálního přijatelného rizika. Pro AVV se byl využit princip ALARP, který umožňuje k hodnocení rizika využít kvalitativních i kvantitativních metod.

POUŽITÁ LITERATURA

[1] Myslivec, I. a kol. *Automatické vedení vlaku AVV*. Vědeckotechnický sborník ČD, vol. 5, 1998. ISSN 1214-9047. [cit. 2009-09-19].
Dostupné z: < http://www.cdrail.cz/VTS/CLANKY/502.pdf>

[2] ČSN EN 61508 Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů. Český normalizační institut, Praha, 2002.

[3] FAMFULÍK, J. KRZYŽANEK, R. MÍKOVÁ, J. *Analýza rizika modulu automatického vedení vlaku UniAVV*. Dílčí řešitelská zpráva projektu FT – TA4/036. Ostrava, 2009.

Tento příspěvek vznikl v rámci řešení projektu FT – TA4/036, který je spolufinancován Ministerstvem průmyslu a obchodu České republiky z resortního programu TANDEM.

Recenzenti: RNDr. Jan Hula
MSV Elektronika s.r.o., Studénka
prof. Ing. Milan Lánský, DrSc.
Univerzita Pardubice, DFJP, Katedra dopravních prostředků a diagnostiky