

Miroslav Šídlo<sup>1</sup>

## **Proces nezávislého posuzování technických změn na železničních subsystémech ve vztahu k procesu řízení rizik**

**Klíčová slova:** *riziko, management rizik, analýza rizika, posuzování rizika, hodnocení rizika, řízení rizika, riziková funkce, proces řízení rizika, kodex správné praxe, referenční systém, odhad rizika*

### **Úvod**

Rámec prováděcího nařízení Komise EU č. 402/2013 v platném znění, označované též jako CSM on Risk Assessment, CSM RA [1] s odkazem na směrnici 2004/49/ES uplatňuje tzv. Definice. Definice jsou uvedené v čl. 3 CSM RA a pro pochopení vztahů procesu řízení rizik a procesu nezávislého posuzování považuji za důležité některé definice v úvodu tohoto článku citovat.

### **1. Důležité definice (citace z CSM RA, s uvedením původního číselného označení)**

- 1) „rizikem“ se rozumí četnost výskytu nehod a mimořádných událostí vedoucích k újmě (zapříčiněných nebezpečím) a stupeň závažnosti této újmy;
- 2) „analýzou rizik“ se rozumí systematické používání všech dostupných informací k určení nebezpečí a odhadu rizik;
- 3) „hodnocením rizik“ se rozumí postup založený na analýze rizik s cílem určit, zda bylo dosaženo přijatelné úrovně rizika;
- 4) „posuzováním rizik“ se rozumí celkový postup zahrnující analýzu a hodnocení rizik;
- 6) „řízením rizik“ se rozumí systematické uplatňování politik, postupů a praktik řízení na úkoly týkající se analýzy, hodnocení a usměrňování rizik;
- 12) „zprávou o posouzení bezpečnosti“ se rozumí dokument, který obsahuje závěry posouzení, jež s ohledem na posuzovaný systém provedl subjekt pro posuzování;

---

<sup>1</sup> Autor článku, Ing. Miroslav Šídlo (\*1957) je absolventem ČVUT v Praze, kde vystudoval obor Přístrojová, regulační a automatizační technika, se zaměřením na leteckou přístrojovou techniku. V průběhu své profesní praxe se věnoval konstrukci leteckých přístrojů, řízení různých provozů a managementu spolehlivosti služeb. V současné době je vedoucím Subjektu pro posuzování bezpečnosti Technické ústředny dopravní cesty, organizační jednotky SŽDC.

13) „nebezpečím“ se rozumí stav, který by mohl vést k nehodě;

**14) „subjektem pro posuzování“ se rozumí nezávislá a způsobilá externí nebo interní osoba, organizace nebo subjekt provádějící šetření s cílem dospět na základě důkazů k rozhodnutí, zda systém splňuje bezpečnostní požadavky;**

15) „kritérii přijatelnosti rizik“ se rozumí referenční pokyny, na základě nichž se posuzuje přijatelnost určitého rizika; tato kritéria se používají k určení, zda je úroveň rizika dostatečně nízká, takže není nutno přijmout okamžitá opatření k jejímu dalšímu snížení;

16) „záznamem o nebezpečí“ se rozumí doklad, v němž jsou zaznamenána a kde jsou odkazy na zjištěná nebezpečí, související opatření, jejich původ a odkaz na organizaci, která je má řídit;

18) „zásadou přijatelnosti rizik“ se rozumí pravidla používaná s cílem dospět k závěru, zda riziko spojené s jedním či více konkrétními nebezpečími je, či není přijatelné;

**19) „kodexem správné praxe“ se rozumí písemný soubor pravidel, která, jsou-li správně uplatňována, lze použít k řízení jednoho či více konkrétních nebezpečí;**

**20) „referenčním systémem“ se rozumí systém, u něhož byla při používání prokázána přijatelná úroveň bezpečnosti a podle něhož lze porovnáním vyhodnotit přijatelnost rizik vyplývajících z posuzovaného systému;**

**21) „odhadem rizika“ se rozumí postup používaný k měření úrovně analyzovaných rizik, který se skládá z těchto kroků: odhad četnosti, analýza důsledků a jejich integrace;**

22) „technickým systémem“ se rozumí výrobek nebo soubor výrobků včetně výkresové, prováděcí a podpůrné dokumentace; vývoj technického systému začíná stanovením požadavků a končí jeho schválením; ačkoli se bere v úvahu návrh příslušných rozhraní s lidským chováním, **nejsou lidská obsluha a její úkony do technického systému zahrnuty; postup údržby je popsán v příručkách údržby, sám o sobě však není součástí technického systému.**

### *1.1 Definice ostatní*

Bezpečnost drážních zařízení a subsystémů zpravidla souvisí s problematikou spolehlivosti zařízení. Problematika zabezpečení udržitelnosti zařízení je popsána v normách řady ČSN IEC 60300-3-10. Podrobně jsou v řadách norem rozpracovány rovněž analýzy spolehlivosti zařízení:

- analýza forem a důsledků poruch (FMEA) je popsána v ČSN EN 60812
- analýza stromu poruchových jevů je popsána v ČSN EN 61025
- stanovení a prokázání bezporuchovosti, pohotovosti, udržitelnosti a bezpečnosti drážních zařízení v ČSN EN 50126-1, oprava 2:2012
- základní pojmy a definice jsou rovněž zapracovány do Mezinárodního elektrotechnického slovníku, kapitola Spolehlivost a jakost služeb (IEC 50)

V posledních letech minulého století začala IEC vydávat sadu norem IEC 300 (Management spolehlivosti) a navazujících norem, které souvisejí s tvorbou programů bezporuchovosti, pohotovosti, udržitelnosti a bezpečnosti (RAMS). Pro drážní zařízení a prokázání jeho bezporuchovosti, pohotovosti udržitelnosti a bezpečnosti platí norma ČSN EN 50126-1, oprava 2:2012 (dále jen **Norma**), která má status české technické normy.

Z hlediska předpovědi ukazatelů bezpečnosti subsystémů jsou mimořádně důležité analýzy bezpečnosti, které se provádějí v etapě návrhu a zavedení. Etapa Provoz a údržba nespadá pod proces CSM RA.

**Takové analýzy bývají označovány za prediktivní analýzy bezpečnosti.** Prediktivní analýzy jsou potřebné pro vyhodnocení a stanovení ukazatelů bezpečnosti a spolehlivosti subsystému a pro posouzení, zda byly splněny specifikované požadavky v době prokazování shody. Existují různé metodologické postupy při provádění analýzy bezpečnosti:

- Induktivní postup je založen na provádění analýzy od elementárních problémů k problémům globálním a obecným. Aplikace induktivního postupu je uvedena u aplikace metody FMEA při ověřování přesnosti jednoznačného odhadu rizik.
- Deduktivní postup je založen na provádění analýzy od obecných a globálních problémů směrem k elementárním problémům. Od analýzy poruch systému na nejvyšší úrovni členění se postupuje směrem k analýze jejich příčin a stanovení podílu chování elementárních prvků na takových poruchách. Deduktivní postup je uplatněn např. v metodě stromu poruch. Metoda není použita v tomto článku.

## **2. Obecné zásady a povinnosti použitelné na proces řízení rizik<sup>2</sup>**

Obecné zásady a povinnosti navrhovatele použitelné na proces řízení rizik definuje CSM RA, Příloha I v několika článcích. Je definován začátek procesu, který začíná vymezením posuzovaného systému a jsou definovány další činnosti, které souvisejí s určením rizik. Činnosti se týkají určení nebezpečí, stanovení bezpečnostních požadavků, stanovení návrhů souvisejících bezpečnostních opatření, prokázání shody systému se stanovenými bezpečnostními požadavky a provádění řízení všech zjištěných nebezpečí a souvisejících opatření.

Příloha I definuje rovněž odpovědnosti:

**Za proces řízení a posuzování rizik odpovídá navrhovatel.**

**Za vyhodnocení správného uplatňování procesu řízení rizik a jeho výsledků odpovídá subjekt pro posuzování.**

Obecný postup pro posuzování rizik je chápán jako opakující se postup, který stanovuje minimální požadavky, které jsou kladené na vymezení systému (v 6-ti bodech), na způsob provádění identifikace nebezpečí u vymezeného systému a na

---

<sup>2</sup> V článku se procesem řízení rizik rozumí **proces řízení rizik změn**, prováděných na stávajících železničních subsystémech.

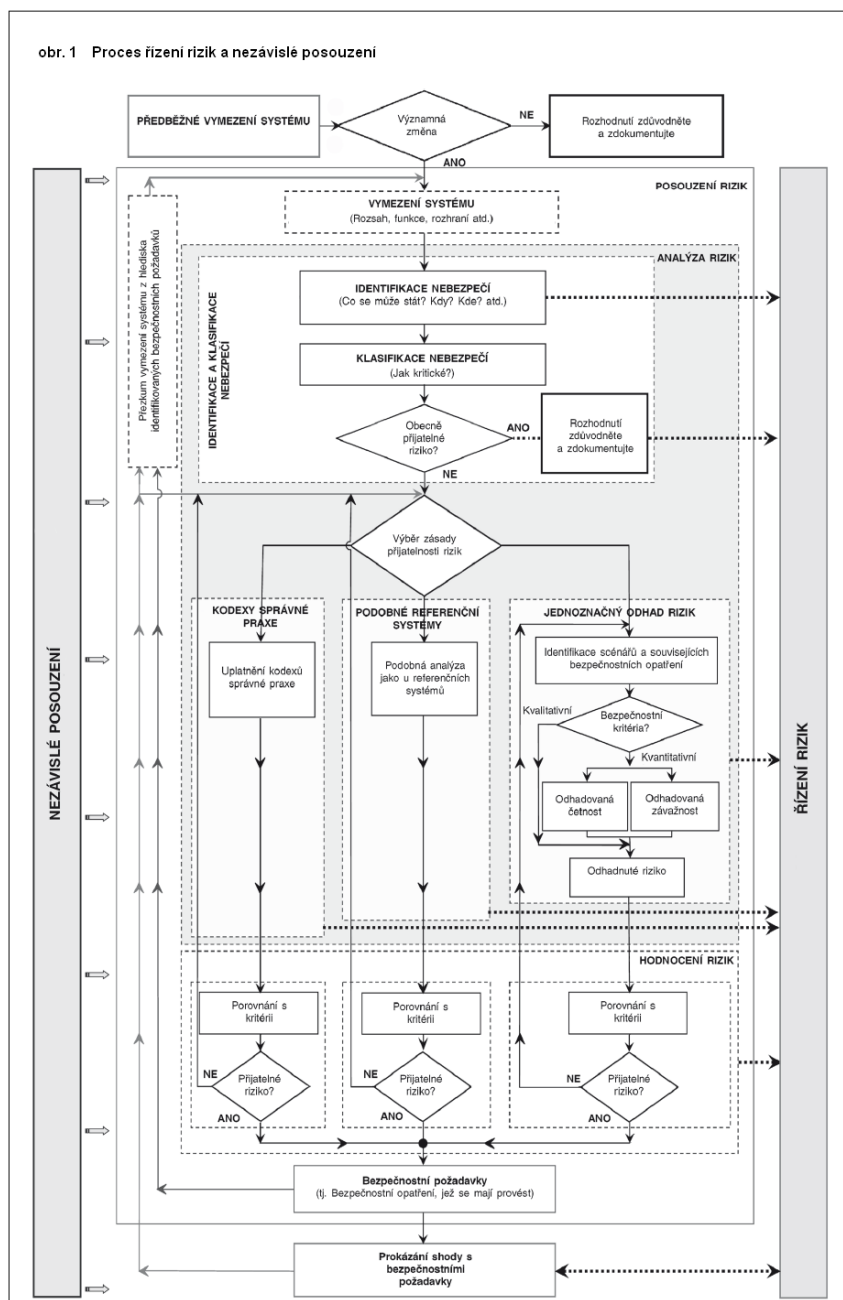
přijatelnost rizik a jejich vyhodnocení pomocí jedné nebo více zásad (uplatnění kodexů správné praxe, porovnání s obdobným systémem, jednoznačný odhad rizik).

**Platí důležitý princip – subjekt pro posuzování nesmí navrhovateli nařídit, aby použil konkrétní zásadu přijetí rizika.**

Obecný postup pro posuzování rizik rovněž stanovuje minimální požadavky na používání kodexů správné praxe, používání referenčních systémů a uplatňování metod jednoznačného odhadu rizik.

Poslední články obecného postupu popisují, jak se provádí prokázání shody s bezpečnostními požadavky (CSM RA, Příloha I, čl. 3), jak se provádí proces řízení nebezpečí (CSM RA, Příloha I, čl. 4), včetně výměny informací a jaké důkazy o uplatňování procesu řízení rizik se dokumentují (CSM RA, Příloha I., čl. 5).

Vztah procesu řízení rizik a jejich nezávislého posouzení je uveden v grafické podobě rovněž v CSM RA, Příloha I, Dodatek. S ohledem na jeho zásadní význam uvádím jeho doslovnou citaci, viz obr. 1:



Obrázek 1: Proces řízení rizik a nezávislé posouzení

### 3. Zásady uplatňované subjektem pro posuzování (dále jen SPB)

SPB je odpovědný za vyhodnocení, že proces řízení rizik byl navrhovatelem správně uplatněn. Dále platí důležitý princip, že SPB nesmí navrhovateli nařídit, aby použil konkrétní zásady přijatelnosti rizik.

SPB se zpravidla řídí konkrétními postupy posuzování, které vycházejí z normy ČSN EN ISO/IEC 17020 a pracovních instrukcí, které se týkají jeho činnosti. Činnost SPB je zpravidla vymezena jeho uznáním nebo akreditací s ohledem na geografickou působnost (např. EU) a v případě posuzování technických změn na

rozsah strukturálních a/nebo funkčních subsystémů a jejich částí. Použité postupy, které nejsou součástí pracovních instrukcí SPB, musí být v rámci prováděné činnosti dokumentovány.

Výstupem SPB je tzv. Zpráva o posouzení bezpečnosti (dále jen ZPB), jejíž definice byla uvedena v tomto článku, kapitola 2., bod 12).

Podrobnosti, které se týkají obsahu ZPB, používaných slovních formulací a detaily pracovních instrukcí, kterými se řídí činnosti SPB, však přesahují rozsah tohoto článku.

### *3.1 Používání kodexů správné praxe*

Kodexem správné praxe se rozumí písemný soubor pravidel, která, jsou-li správně uplatňována, lze použít k řízení jednoho či více nebezpečí. Kodexy správné praxe musí být v železničním odvětví obecně uznávány. Pokud tomu tak není, musí být řádně odůvodněny a musí být přijatelné pro SPB.

Kodexy musí být vhodné pro usměrňování identifikovaných nebezpečí v posuzovaném systému. Kodexy musí být k dispozici SPB.

Za kodexy správné praxe je možné považovat TSI, pokud jsou vhodné pro usměrňování identifikovaných nebezpečí v posuzovaném systému.

Za kodexy správné praxe lze považovat rovněž vnitrostátní předpisy a odpovídající firemní předpisy, oznámené v souladu s článkem 8 směrnice 2004/49/ES a čl. 17, odst. 3 směrnice 2008/57/ES, které splňují požadavky stanovené v CSM RA, Příloha I., odst. 2.3.2 a).

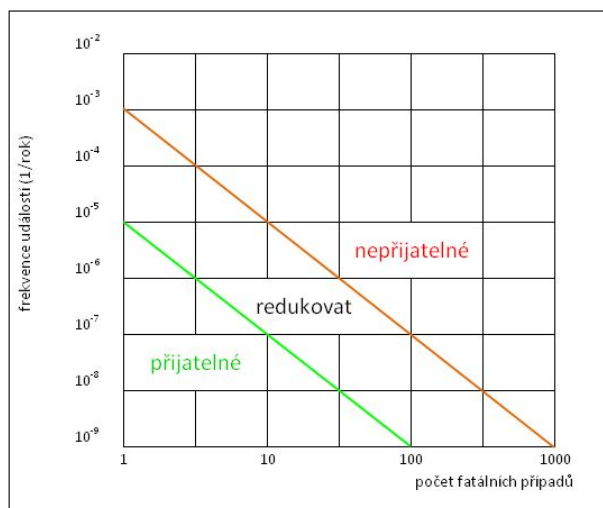
Obecně platí, že pokud je jedno nebo více nebezpečí usměrněno pomocí kodexů správné praxe, není nutné taková rizika dále analyzovat. Použití kodexů správné praxe musí být zapsáno v záznamu o nebezpečí jako bezpečnostní požadavek.

#### *3.1.1 Přijatelnost kodexů správné praxe pro SPB SŽDC-TÚDC*

SPB SŽDC-TÚDC považuje za přijatelné pro řízení rizik v železničním odvětví a na technických systémech celou řadu kodexů. Jedná se především o evropské normy (EN) připravované evropskými normalizačními institucemi CEN/CENELEC/ETSI, které přejímáme jako ČSN EN. Dále pak mezinárodní normy ISO, IEC, doporučení UIC (zprávy, vyhlášky, IRS), méně často normy BS (British Standards) či DIN, původní technické normy (ČSN) a pro konkrétní drážní zařízení také normy TNŽ, které jsou dnes podnikovou normou SŽDC. Mimo norem existuje množství dokumentů, které mají charakter písemného souboru pravidel a splňují ostatní požadavky kladené na kodex. Zmíním zde několik důležitých, např. Vyhlášku č. 100/1995 Sb. Řád určených technických zařízení, Vyhlášku č. 177/1995 Sb. Stavební a technický řád drah (všechny ve znění pozdějších předpisů) a také celou řadu vnitřních předpisů provozovatele Správy železniční dopravní cesty, s.o. (SŽDC), které splňují parametry kodexů správné praxe. Jedná se hlavně o technické a kvalitativní podmínky (TKP) SŽDC, předpisy řady T, E, S, předpisy řady D, Z a předpisy o odborné způsobilosti osob SŽDC Zam1.

Pro SPB je mimo obecných podmínek, které musí kodex splňovat (musí jít o soubor písemných pravidel, musí být prokázáno jeho správné uplatňování, musí být veřejně dostupný všem účastníkům, kteří se podílejí na řízení rizik a SPB), důležité, která nebezpečí jsou kodexem účinně usměrňována. V případě, že byl kodex u provozovatele dříve zaveden, používán pro usměrňování některých rizik a na základě analýzy četnosti a důsledků mimořádných událostí je prokázána jeho účinnost<sup>3</sup>. Za základní kritérium účinnosti kodexu správné praxe je tedy možné považovat nerostoucí charakter frekvence nežádoucích událostí a jejich důsledků. Skutečnost lze znázornit v tzv. F – N křivkách (viz obr. 2). Křivky F – N představují grafický vztah frekvence události (F), při které může nastat určitý počet nežádoucích následků (N). Předpokládejme, že může nastat určitý počet následků (N) a že jako nežádoucí následky nás zajímají úmrtí lidí. Distribuce úmrtí (fatalit), tj. graf vyjadřující četnost určitého počtu úmrtí ukazuje, jak mnoho lidí je vystaveno této hladině rizika. Bod na křivce F - N udává frekvenci (F) výskytu události s úmrtností vyšší než počet (N) lidí.

F – N křivky jsou rovněž vhodným prostředkem pro zobrazení kritérií přijatelnosti rizik. V případě, že jsou v rámci EU nebo členským státem předem stanovena pro řešenou problematiku změn kritéria pro přijetí rizika, ověří SPB SŽDC-TÚDC, zda předchozí používání kodexu vyhovuje takto stanoveným kritériím. V případě, že pro řízení rizik metodou uplatnění kodexů správné praxe nebyla žádná kritéria přijatelnosti rizik stanovena, ověřuje SPB SŽDC-TÚDC, zda kodex historicky splňoval alespoň kritéria tzv. konvence společenského rizika, která je v Evropě obvykle akceptovatelná a byla vypracovaná v Holandsku. V ČR jsem se setkal s takto definovanými kritérii přijatelnosti prvně ve vysokoškolských učebnicích [2] a [3]. Zmíním rovněž dokument [4], který popisuje filosofický základ, parametry a vývoj kritérií v EU. Nicméně, za hrubou hranici akceptovatelnosti společenského rizika SPB SŽDC-TÚDC v mnoha případech považuje hranici označenou limitními čarami grafu<sup>4</sup>, které znázorňují oblasti přijatelných rizik, oblasti rizik, která je nutno dále usměrňovat a oblasti nepřijatelných rizik.



Obrázek 2: F – N křivka pro drážní subsystémy

<sup>3</sup> Cílem společných bezpečnostních metod (CSM RA) v době jejich zavádění bylo udržení parametrů společných bezpečnostních cílů, tedy skutečnosti, aby např. frekvence nežádoucích událostí a jejich důsledků neměla rostoucí charakter.

<sup>4</sup> Převzato z [2] a/nebo [3].

Za logické je nutné považovat srovnání takto stanoveného kritéria s kritériem uvedeným v CSM RA. CSM RA (viz Příloha I, odst. 2.5.6 a následující) připouští, že v případě kdy navrhovatel může prokázat, že úroveň vnitrostátní bezpečnosti v členském státě, ve kterém má dojít k použití, lze udržet na míře selhání vyšší než  $10^{-9}$  za provozní hodinu, může být toto kritérium navrhovatelem v uvedeném členském státě použito. Kritérium je však uvedeno u použití metody jednoznačného odhadu rizik. Pro akceptovatelnost kodexů správné praxe v CSM RA však žádná kritéria stanovená nejsou. Kvantitativní odhad rizika pro kodexy správné praxe však lze provádět a podle názoru autora by měl být na nové změny prováděné v kodexech uplatňován.

2.5.7 Jednoznačný odhad rizik a jejich vyhodnocení splňuje nejméně.

### *3.2 Používání referenčního systému a hodnocení rizik*

Referenčním systémem se rozumí systém, u něhož byla používáním prokázána přijatelná úroveň bezpečnosti a podle něhož lze porovnáním vyhodnotit přijatelnost rizik, která plynou z posuzovaného systému.

Referenční systém má tedy přijatelnou úroveň bezpečnosti, má obdobné funkce a rozhraní, jako posuzovaný systém a používá se za obdobných environmentálních podmínek jako posuzovaný systém (viz CSM RA, Příloha I, odst. 2.4.2) V takovém případě rizika spojená s nebezpečími, na které se vztahuje referenční systém, jsou považována za přijatelná.

#### *3.2.1 Přijatelnost referenčního systému pro SPB SŽDC-TÚDC*

Pro SPB SŽDC-TÚDC jsou přijatelné referenční systémy, u kterých byla prokázána dříve jeho úroveň bezpečnosti. V případě, že byl referenční systém u provozovatele již dříve zaveden, byl používán a na základě analýzy četnosti a důsledků mimořádných událostí je prokázána jeho bezpečnost při řízení konkrétních nebezpečí, tj. jsou splněna kritéria tzv. F-N křivky podle obr. 2 (viz předchozí odstavec), je referenční systém považován za přijatelný, pokud splňuje i ostatní podmínky stanovené v CSM RA (podobné funkce, rozhraní, prostředí).

### *3.3 Příklady použití jednoznačného odhadu rizik*

Metoda jednoznačného odhadu rizik se používá v případě, že se na identifikovaná nebezpečí nevztahuje jedna ze dvou výše uvedených metod (zásad). V takovém případě musí být kvalitativní nebo kvantitativní metodou<sup>5</sup> stanovena četnost nežádoucích událostí a provedena analýza jejich důsledků.

Platí, že u technických systémů, u kterých může vést selhání ke katastrofickým nehodám, nemusí být riziko dále snižováno, pokud je míra selhání nižší nebo rovna četnosti  $10^{-9}$  za hodinu provozu.

SPB v případě použití metody jednoznačného odhadu rizik přezkoumá následující požadavky:

- 1) Zda metoda použitá pro jednoznačný odhad rizik je vhodná pro analýzu a řízení rizik u posuzované změny.

<sup>5</sup> Případně jak kvalitativní, tak kvantitativní metodou.



- 2) Zda metoda zahrnuje všechny provozní režimy.
- 3) Zda přesnost výsledků u použité metody je dostatečná. Nepřípustné je, aby zejména malá změna v předpokladech vedla ke značným rozdílům v bezpečnostních požadavcích.

#### *Příklad 1 (pro ilustraci)*

U přejezdového zařízení byla provedena analýza rizik a bylo zjištěno, že většina rizik, která plynou z technického provedení montáže přejezdového zabezpečovacího zařízení, byla usměrněna pomocí kodexů správné praxe. V tomto konkrétním případě však byla ještě analyzována další rizika, která plynou z **nerespektování dlouhodobé výstrahy řidičem silničního vozidla**. S ohledem na konfiguraci železničního přejezdu, geografické poměry a provoz na blízké křižovatce se tím odborníků navrhovatele shodl na skutečnosti, že rizika nerespektování výstrahy řidičem jsou v uvedeném případě relevantní, byť jsou v jiných případech (a v členském státě EU) považována za společensky přípustná. **Riziko nevčasného vyklizení prostoru přejezdu bylo klasifikováno jako nepřípustné** a bylo navrženo technické řešení. Technická řešení spočívalo v konkrétním opatření:

- 1) Vybavení kolejového vozidla pagerem. Strojvedoucí, který zastaví na zastávce před přejezdem, odešle povel pro zabezpečení přejezdu v okamžiku, kdy je ukončeno nastupování a vystupování cestujících. Přejezd je následně zabezpečen a vlaková cesta postavena. Tím **dojde k podstatnému zkrácení doby výstrahy přejezdového zabezpečovacího zařízení**.
- 2) Opatření však vede k dalším rizikům. Opatření nebude možné použít v případě, že kolejová vozidla nebudou pagerem vybavena a strojvedoucí nebudou o jejich používání proškoleni. Jako náhradní řešení lze použít hlasovou komunikaci strojvedoucího a dispečera, který řídí dopravu. Přejezdové zařízení je v takovém případě uvedeno do výstrahy dispečerem a další proces je stejný.
- 3) Obdobný případ nastává v okamžiku, kdy pager strojvedoucího je nefunkční. Řešení je obdobné, jako v bodě 2).

Na uvedeném příkladu je demonstrováno, že původně identifikované a metodou jednoznačného odhadu analyzované riziko s klasifikací „nepřípustné“, bylo usměrněno pomocí technických opatření. Původní příčina, tj. dlouhá doba výstrahy kvůli zastávce před přejezdem, byla zkrácena použitím pageru a použitím vazby do zabezpečovacího zařízení. Byla však identifikována další rizika, která plynou z potřebné **vybavenosti vozidel, potřebné spolehlivosti použitých zařízení a dalších aspektů** (např. školení strojvedoucích). Jejich úroveň však byla analyzována a rizika byla klasifikována jako nežádoucí, která však lze přijmout se souhlasem provozovatele dráhy. Navrhovatel proto nařídil delší zkušební provoz, během kterého budou nežádoucí události (spolehlivost pagerů, vybavenost vozidel a nerespektování výstrahy řidičem silničního vozidla) sledovány a po vyhodnocení

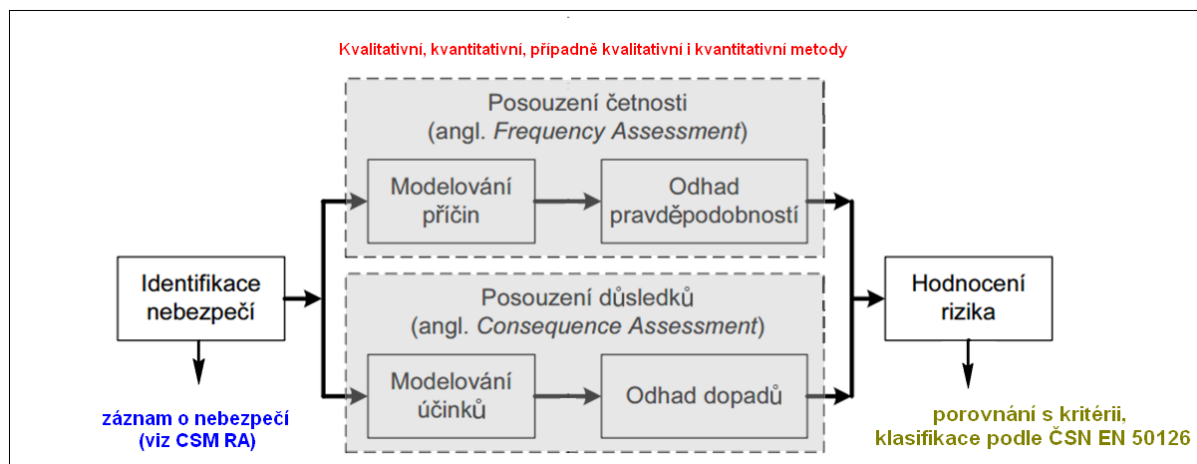
zkušebního provozu bude na základě evidence četnosti nežádoucích událostí provedena nová klasifikace řízeného rizika, případně budou přijata další opatření.

### 3.4 Jednoznačný odhad rizik – proces definovaný Normou

Pro stanovení a prokázání bezpečnosti lze použít proces definovaný Normou.

Podle článku 1., odst.1.2 Norma platí u všech drážních zařízení a na všech úrovních použití, od kompletních tratí po hlavní systémy, i pro jednotlivé subsystémy a jejich komponenty.

Důležité postupy jsou definované v čl. 4.6.2.1 (str. 22). Podle tohoto článku Normy postup provádí orgán zodpovědný za konkrétní etapu a musí ji dokumentovat. Definice koncepce rizika, pravděpodobnost výskytu nebezpečí, úroveň závažnosti (následků) a klasifikace rizika je uvedena na str. 22 až 24 Normy. Životní cyklus systému je definován od str. 28 Normy. Norma definuje úkoly spojené s etapami projektu. Zahájení procesu řízení rizik je v etapě koncepce (návrhu) změny. Schématicky lze postup znázornit na obr. 3:



Obrázek 3: Průběh postupů u jednoznačného odhadu rizik

## 4. Posouzení vhodnosti postupů, přesnosti a citlivosti u metody jednoznačného odhadu rizik

Přestože je metoda a proces řízení rizik podle Normy obecně použitelný pro většinu drážních zařízení, mohou se postupy jednotlivých SPB při jeho posuzování lišit.

V poměrné shodě byla odborníky přijata kategorizace úrovně závažnosti nebezpečí podle Normy (odst. 4.6.2.3 a Tabulka 3). Kategorizace stejného významu je dokonce zakotvena v Zákonu o drahách.

V Normě je uvedeno (odst. 4.6.2.2), že typické kategorie pravděpodobnosti nebo četnosti výskytu nebezpečné události a jejich numerické odstupňování, které má být použito, musí být stanoveno provozovatelem dráhy tak, aby bylo vhodné pro uvažované použití. SPB není oprávněn navrhovateli nařídit zásadu pro přijetí rizika.

V případě metody jednoznačného odhadu rizik by však SPB měl uvést v ZPB alespoň stanovisko, zda kategorizace pravděpodobností (nebo změřených četností) výskytu, počet kategorií a jejich numerické odstupňování odpovídá praxi používané v členských zemích EU. SPB však v každém případě uvádí v ZPB stanovisko (závěr), že posoudil a vyhodnotil správné použití metody a riziko považuje použitou metodou za usměrněné.

**SPB SŽDC - TÚDC vždy uvádí své stanovisko se zdůvodněním, pokud dospěl k jinému hodnocení rizika při použití uvedené metody.**

#### *4.1 Riziková funkce a postupy FMEA při uplatnění metody*

Norma formou tabulkového předpisu aplikuje pro drážní zařízení rizikovou funkci jako funkci dvou proměnných v jejím nejjednodušším tvaru:

$$\text{RIZIKO} = f(p_1, p_2) \quad (1)$$

Postup podle Normy stanovuje, jak se má provést odhad pravděpodobnosti výskytu nežádoucí události  $p_1^6$  a jeho kategorizace. Postup Normy rovněž stanovuje, jak se má provést odhad a kategorizace úrovně závažnosti  $p_2$ , jak se má stanovit úroveň rizika pomocí tzv. Matice četnost – následky (viz Norma, Tabulka 4). Norma obsahuje také tzv. kvalitativní kategorizaci rizika a definuje 4 kategorie (klasifikace, hodnocení) rizika (nepřípustné, nežádoucí, přípustné, zanedbatelné) s příkladem (viz odst. 4.6.3.4 a Tabulka 6 Normy) s doporučením, zda musí být riziko odstraněno, přijato za určitých podmínek nebo přijato.

Z hlediska principu můžeme **výše uvedenou metodu aplikovat také jako metodu induktivní**. To znamená, že konkrétní kvalitativní analýza bezpečnosti probíhá od nižší úrovně členění systému k vyšší (od změny na zařízení nebo subsystému k systému). Metoda zkoumá, jakým způsobem mohou objekty na nižší úrovni selhat a jaký důsledek mohou mít taková selhání pro vyšší úroveň systému. Analýza způsobů a důsledků (Failure Mode and Effect Analysis) bývá označována jako kvalitativní FMEA analýza. V případě, že metoda obsahuje odhad kritičnosti důsledků a pravděpodobnosti jejich nastoupení, lze metodu označit jako FMECA (Failure Mode, Effect and Criticality Analysis). Jde však jen o logické rozšíření metody FMEA.

Cíle uvedené metody lze definovat takto:

- lze posoudit důsledky a posloupnosti jevů pro každou zjištěnou formu selhání prvku, ať má jakoukoliv příčinu, a to na různých úrovních systému
- lze určit významnost nebo kritičnost každé formy poruchy vzhledem k funkci (nebo provozuschopnosti a bezpečnosti) systému
- lze klasifikovat zjištěné způsoby poruch podle toho, jak snadno je lze zjistit, diagnostikovat, testovat, nahradit potřebnou funkcionalitu nebo provést provozní opatření
- lze provádět odhady dalších ukazatelů významnosti a pravděpodobnosti poruchy, jsou-li k dispozici provozní data

<sup>6</sup> Poznámka: Pravděpodobnosti  $P_1, P_3$  až  $P_n$  v rovnicích (1) a (2), aniž jsou v textu podrobně specifikovány, mají rozměr četnosti jevu v jednotkách za rok (per year).

Metoda FMEA je tedy neobyčejně účinná metoda analýzy bezpečnosti v případě, že je aplikována zejména v prvních etapách životního cyklu technické změny nebo zařízení.

Metoda může být složitá, pracná a časově náročná v případě komplexního systému s mnoha komponenty a mnoha funkcemi nebo v případech, kdy je aplikována na složitý systém poprvé. Omezením metody je rovněž skutečnost, že nezahrnuje při posuzování technické změny apriori důsledky chyb lidského faktoru. Přesto lze metodou často zjistit citlivé nebo nejméně příznivé vlivy selhání člověka a naznačit potřebné kroky k eliminaci těchto vlivů.

### *Příklad 2*

Výrobce zařízení pro subsystém řízení a zabezpečení navrhuje nikoliv jednoduchou změnu na zařízení subsystému, ale navrhuje nový systém řízení drážní dopravy (např. ETCS). Na základě uplatnění metody jednoznačného odhadu rizik s prvky analýzy FMEA analyzuje, že některá identifikovaná rizika nelze zcela nebo ani zčásti usměrnit pomocí technických, softwarových, automatických řídicích nebo jiných bezpečnostních funkcí. Nicméně, pomocí metody FMEA zjišťuje kritická místa a rozhraní subsystému, která jsou nejcitlivější na nepříznivé vlivy činnosti člověka a naznačuje provozovateli účinné kroky k eliminaci těchto vlivů<sup>7</sup>.

SPB odpovídá za vyhodnocení správného uplatnění procesu řízení rizik. Má-li dospět k názoru, že použitá metoda jednoznačného odhadu rizik je vhodná pro analýzu a řízení rizik, má-li dospět k názoru, že metoda zahrnuje všechny provozní režimy zařízení a má-li zjistit, že přesnost použité metody je dostatečná a málo citlivá na určité změny v předpokladech, může nastat situace, kdy musí být uplatněna ještě další metoda analýzy a řízení rizik, než pouhé stanovení rizikové funkce podle (1).

Riziková funkce, jak plyne např. z uplatnění výše popsané metody FMEA může být rozšířena obecně na tvar:

$$\text{RIZIKO} = f(p_1, p_2, p_3, \dots, p_n) \quad (2)$$

kdy pravděpodobnosti  $p_3$  až  $p_n$  mohou mít například **význam diagnostikovatelności poruchy, význam náhrady potřebné funkcionality, význam časové závislosti poruch**, apod.

### *Příklad 3*

Je uvažováno přejezdové zabezpečovací zařízení, jehož bezpečnost lze klasifikovat jako nepřípustnou, protože nejhorší důsledek selhání (střet kolejového a silničního vozidla) lze považovat za katastrofický a pravděpodobnost výskytu nežádoucí události za občasnou až pravděpodobnou. Je dána skutečností, že nedojde ke

---

<sup>7</sup> Poznámka: Podle nařízení CSM RA (viz definice č. 22) nejsou lidská obsluha a její úkony do technického systému zahrnuty. Postup údržby však musí být v příručkách obsluhy a údržby popsán, sám o sobě však není součástí technického systému.

včasnému vyklizení prostoru přejezdu z různých důvodů. Jedním z nich je blízkost křižovatky se silničním signalizačním zařízením. Křižovatka nemusí umožnit řidiči včasné opuštění přejezdu při výstraze. Dále je zde nutné brát v potaz faktor dobrovolného rizika. Skutečnost, zda riziko je jednotlivcem přijímáno dobrovolně (řidič automobilu) nebo mu je nějakým způsobem vnuceno (nedobrovolné riziko) je velice důležitá v otázkách vnímání rizika i jeho společenské přijatelnosti. V případě dobrovolného rizika příjemce dobrovolně vybírá svůj stupeň spoluzodpovědnosti a ohrožení vlastním rizikem. Takto přijaté riziko může být o dva i více řádů vyšší, než riziko přijímané nedobrovolně (provozovatelem drážního zařízení). Rozlišení mezi dobrovolným a nedobrovolným rizikem má souvislost s přijatelností rizika. Provozovatel se proto rozhodl o snížení míry rizika aplikací legislativně méně obvyklého technického řešení. A sice aplikací detektoru vyklizení přejezdu (radaru) s využitím návěstidel (přejezdnic). Riziková funkce viz rovnice (2) je v takovém případě funkcí více proměnných, tj. pravděpodobnosti výskytu nežádoucí události  $p_1$ , pravděpodobnosti výskytu nejhoršího důsledku  $p_2$  a např. pravděpodobnosti časové závislosti událostí  $p_3$ , pravděpodobností správné funkce detektoru překážek  $p_4$  a dalších. Pravděpodobnost časové závislosti událostí v tomto příkladu chápeme tak, že v případě správné funkce detektoru překážek nenastane současně nežádoucí událost a důsledek, protože v případě nevyklizení přejezdu může být vlak zastaven. Nejedná se však o jistotu, protože přejezd může být, díky dobrovolnému přijetí většího individuálního rizika řidičem, obsazen a nevyklizen i v případě výstrahy a kolejové vozidlo již bude za přejezdnicí. Pravděpodobností  $p_4$  pak chápeme, že nedojde k nejhoršímu důsledku v případě správné funkce detektoru překážky. Přestože takto řízeným rizikem není událost usměrněna na „nemožnou“, došlo k velice významnému snížení míry rizika. Jedná se o tzv. prevenci, protože pravděpodobnost důsledku  $p_2$  nemohla být snížena (kdyby byla snížena, hovořili bychom o ochraně). Součin pravděpodobností  $p_1 \times p_3 \times p_4$  však snížil pravděpodobnost výskytu důsledku z klasifikace „občasná“ nebo „pravděpodobná“ na klasifikaci „malá“ nebo „nepravděpodobná“. A takové riziko může být přijato.

Při posuzování vhodnosti metody jednoznačného odhadu rizik je SPB nucen pracovat s nástroji počtu pravděpodobnosti v rozsahu od definic pravděpodobností jistého a nemožného jevu, přes podmíněnou pravděpodobnost, úplnou pravděpodobnost a pravděpodobnost hypotéz (Bayesova věta). Uvedené metody však mohou posloužit pouze k tomu, aby byla **stanovena nebo upřesněna pravděpodobnost hypotéz za určitých podmínek**. Pravděpodobnost hypotéz za určitých podmínek SPB použije pro zjištění, zda jsou výsledky použitého jednoznačného odhadu rizik dostatečně přesné. Použitý postup je zpravidla součástí konkrétní pracovní instrukce SPB nebo je jeho uplatnění během posuzování dokumentováno. V mnoha případech posuzování však nemusí být metoda pravděpodobnosti hypotéz použita.

Dále je vhodné upozornit na skutečnost, že hlavním a ani původním cílem FMEA analýzy není stanovení příčin poruchy zařízení. K tomu musí být použité jiné metody. **Přesto se však pomocí této metody stanovují všechny pravděpodobné (možné) příčiny, spojené s danou formou poruch**. Identifikace potencionálních příčin forem poruch se stanovuje proto, aby se odhalily důsledky poruch a aby bylo možné navrhnout a stanovit soubor opatření. Forma poruchy však může mít více než jednu

příčinu. **Proto musí být stanoveny a popsány všechny možné nezávislé příčiny pro každou formu poruchy.**

Prioritním (prvním) cílem metody je však kvalitativní (FMEA) nebo kvantitativní (FMECA) analýza důsledků poruch. Zjistí se, vyhodnotí se a zaznamenají se důsledky všech forem poruch. A to jak na stav, funkci nebo činnost posuzovaného prvku, tak na všechny vyšší úrovně subsystému až po úroveň systému jako celku. Podle použitých kritérií se potom každému důsledku přiřadí stupeň závažnosti. Rozlišujeme tzv. lokální důsledek. To je důsledek poruchy na vlastní prvek. **V případě důsledku poruchy na stav, funkci a činnost subsystému pak hovoříme o konečném důsledku.** Abychom mohli vyhodnotit stav celého systému, musíme vyhodnotit důsledky poruch na všech nižších úrovních a je nutné brát v úvahu všechny možné kombinace poruch s **vědomím, že porucha jednoho prvku může mít sama o sobě nezávažné důsledky, ale v kombinaci s jinou poruchou může vést ke katastrofickým důsledkům.**

Celá řada důsledků poruch může být usměrněna pomocí technických prostředků k detekci poruch. Informace z této části analýzy jsou důležité pro návrh celé řady preventivních opatření nebo pro návrhy provozních opatření, návrhy pro údržbu systému, atd. Zvláštní kategorií jsou tzv. skryté poruchy, o kterých není obsluha včas informována a varování přichází až v okamžiku, kdy se od systému očekává plnění jeho bezpečnostních funkcí.

Přestože může být metoda jednoznačného odhadu rizik poměrně pracná, může být v mnoha případech jedinou metodou, pomocí které lze identifikovaná rizika řídit a pomocí vhodných opatření usměrnit na přijatelnou úroveň<sup>8</sup>.

Aby byly výsledky analýzy přehledné a mohly být v dalších etapách snadno využitelné, měla by forma a obsah dokumentace odpovídat charakteru analyzovaného zařízení nebo subsystému. Mimo formálních informací, které souvisejí s identifikací použitého prvku (ID číslo, název,...) je důležitý popis funkce použitého prvku, tedy činnosti prvku, prostřednictvím kterých plní svůj účel. Je nezbytné uvádět nejenom očekávané a přijatelné funkce, které prvek plní, ale také funkce, které jsou nepřijatelné, chybové, které jsou poruchou prvku nebo jeho mezním stavem. Forma poruchy by měla být popsána jako jev, jehož prostřednictvím je porucha pozorována. Rozsah a úplnost popisu, klasifikace a kategorizace poruch by měla odpovídat účelu, kterému analýza slouží. Důležité je, aby do analýzy byly zahrnuté všechny možné formy poruch a žádná nebyla předem vyloučena jako krajně nepravděpodobná. V tomto okamžiku lze zpravidla provést tzv. kategorizaci forem poruch. Příklady jsou uvedené např. v ČSN EN 60812. Podrobné kategorizace poruch mohou být velice dobrým základem pro jakoukoliv další podrobnou analýzu a v případě potřeb je lze zpravidla rozšiřovat a jednotlivé formy poruch dále členit.

Podrobná kategorizace forem poruch zařízení je zpravidla vhodným důkazem, kterým navrhovatel v návrhu, studii nebo projektové dokumentaci doloží chování vyprojektovaného zařízení nebo subsystému ve všech provozních stavech.

---

<sup>8</sup> Poznámka: Metoda FMEA bývá v praxi často zcela nebo zčásti uplatňována, aniž by byla takto označována a patřičně dokumentována.

**Provedená analýza metodou FMEA je vhodným důkazem správně provedené kategorizace konečného důsledku poruchy subsystému. Použitím metody jsou zpravidla zjištěny všechny možné, předpověditelné a nezávislé příčiny poruchy zařízení.** SPB v případě takto provedených a dokumentovaných analýz má k dispozici důkazy, které potřebuje k rozhodnutí, zda systém splňuje či nesplňuje bezpečnostní požadavky.

#### *4.2 Uplatnění deduktivních metod*

Pravděpodobnost, s jakou nežádoucí vrcholová událost může v provozu drážního subsystému nastat během specifikovaného časového intervalu může být stanovena také pomocí tzv. analýzy stromu poruchových stavů (Fault Tree Analysis, FTA). Strom poruch patří mezi tzv. deduktivní metody. Metoda využívá tzv. teorie orientovaných grafů. Strom poruch má tvar logického diagramu, který znázorňuje logické vztahy mezi vrcholovou událostí (top event), nazývanou kořenem stromu a mezi příčinami tohoto jevu. Příčiny mohou být v běžných, očekávaných poruchách systému, v náhodných poruchách, v chybách provozních parametrů, v provozních podmínkách či v chybách obsluhy. Správně sestavený strom poruch znázorňuje všechny relevantní kombinace poruch a poruchových jevů, které mohou vést ke vzniku uvažované vrcholové události. Výhodou metody FTA je, že vede analytika poruchy k popisu logiky vývoje poruchy v systému, tím k odhalení všech kauzálních vazeb mezi prvky subsystému a poruchou. Proto lze takovou metodou odhalit slabá místa systému, a to v etapě návrhu a vývoje systému. Metoda je standardizována českou technickou normou ČSN IEC 1025 Analýza stromu poruchových stavů. Praktické použití zjednodušují rovněž softwarové nástroje, které jsou k dispozici. Nevýhodou metody je, že efektivně ji dokáže aplikovat pouze vysoce kvalifikovaný analytik s poměrně hlubokými znalostmi analyzovaných subsystémů.

Metodou FTA může být modelován poruchový stav i provozuschopný stav. Prakticky bývají modely poruchových stavů jednodušší než modely provozuschopných stavů. Je důležité si uvědomit, že v případě modelování provozuschopného stavu se zkoumají podmínky, které jsou nutné pro požadovanou funkci systému.

Cílem analýzy příčin vrcholové události je identifikace všech událostí, které by mohly být bezprostředními příčinami. Výstupem v takovém případě může být rovněž nově identifikované nebezpečí<sup>9</sup>.

Kvantitativní FTA lze provést v situaci, kdy jsou známy parametry elementárních událostí. Cílem kvantitativní FTA je stanovení pravděpodobnosti výskytu vrcholové události, případně dalších ukazatelů, které budou vrcholovou událost charakterizovat<sup>10</sup>.

SPB SŽDC-TÚDC nemá dosud pro posuzování procesu řízení rizik metodou FTA úplné pracovní instrukce. Proto každé posuzování přesnosti a správného použití

---

<sup>9</sup> Poznámka: Nově identifikované nebezpečí musí být zapsáno v seznamu nebezpečí. Při uplatnění kvantitativní FTA může být uvedeno s pravděpodobností výskytu v daném časovém intervalu.

<sup>10</sup> Poznámka: Výpočet stromu poruch je obvykle poměrně pracnou a komplikovanou záležitostí a ruční provedení výpočtu lze snad předpokládat jen u jednoduchých případů. Často používané metody řešení FTA jsou: metoda přímého výpočtu, metoda minimálních kritických řezů a simulační metody Monte Carlo.

metody FTA musí být v části tvorby stromu poruchových stavů, v části kvalitativní analýzy i v části kvantitativní analýzy dokumentováno. Při posuzování je nutné předpokládat velice intenzivní a těsnou spolupráci posuzovatele s analytikem, který provádí analýzu rizik i s pracovníky, kteří provádějí výpočet stromu poruch.

## **5. Činnost SPB při prokazování shody s bezpečnostními požadavky**

Prokázání shody provádějí účastníci procesu řízení rizik, kteří odpovídají za splnění bezpečnostních požadavků za dozoru navrhovatele.

### **Přístup zvolený k prokázání shody s bezpečnostními požadavky a vlastní prokázání shody posuzuje nezávisle na navrhovateli SPB.**

Nepřiměřenost bezpečnostních opatření nebo jejich neúplnost nebo jakákoliv další nebezpečí zjištěná v průběhu prokazování shody s bezpečnostními požadavky zpravidla vždy vedou k novému posouzení a vyhodnocení rizik ze strany navrhovatele. Nová nebezpečí musí být zapsána do záznamu o nebezpečí.

## **6. Činnosti související se záznamy o nebezpečí**

Záznamy o nebezpečí vytváří navrhovatel během zpracovávání návrhu změny. Záznamy jsou doplňovány a aktualizovány účastníky, kteří se podílejí na procesu řízení rizik.

Záznamy jsou zpracovávány až do přijetí změny nebo do doby předložení zprávy o posouzení bezpečnosti.

Byl-li systém přijat a je provozován, záznam o nebezpečí dále uchovává provozovatel subsystému nebo podnik pověřený provozováním subsystému, jako nedílnou součást svého systému řízení bezpečnosti.

Záznam o nebezpečí obsahuje všechna identifikovaná nebezpečí společně se souvisejícími bezpečnostními požadavky a předpoklady, které se týkají systému v rámci postupu pro posuzování rizik. Záznam o nebezpečí obsahuje jednoznačný odkaz na původ nebezpečí, např. na analýzu stavů a poruch zařízení při uplatnění metody FMEA a na vybrané zásady přijatelnosti rizik (uplatněné metody) a jednoznačně určuje účastníky pověřené usměřováním nebezpečí v procesu řízení rizik.

Platí zásada, že nebezpečí, která nemůže jeden účastník procesu řízení rizik usměrnit sám, jsou taková nebezpečí sdělena druhému účastníkovi s cílem nalezení přiměřeného řešení. Nebezpečí zapsaná v záznamu o nebezpečí, která jeden z účastníků převádí, lze považovat za usměrněná pouze tehdy, pokud jejich usměrnění provádí jiný účastník a řešení je odsouhlaseno všemi dotčenými stranami (viz CSM RA, Příloha I, článek 4.2).



## 7. Důkazy o uplatňování procesu řízení rizik

**Proces řízení rizik, který je použitý k posouzení úrovně bezpečnosti a shody s bezpečnostními požadavky, dokumentuje navrhovatel změny tak, aby SPB měl k dispozici veškeré nezbytné důkazy, které prokazují vhodné uplatnění procesu řízení rizik.**

Podle CSM RA, Příloha I, odst. 5.2 dokumentace obsahuje minimálně:

- popis organizace a odborníky jmenované pro provedení postupu řízení rizik
- výsledky jednotlivých fází posuzování rizik a seznam všech bezpečnostních požadavků
- prokázání shody s jednotlivými bezpečnostními požadavky
- podklady, které se týkají integrace zařízení do systému, podklady pro provoz a údržbu systému a posouzení rizika

SPB uvede závěry o uplatnění procesu řízení rizik v ZPB.

## 8. Ostatní náležitosti procesu řízení rizik

V ČR platí další náležitosti, které se týkají procesu řízení rizik. Protože (viz odstavec 4.1) lze za kodexy správné praxe považovat TSI, pokud jsou vhodné pro usměrňování identifikovaných nebezpečí v posuzovaném systému, lze TSI použít pro usměrňování nebezpečí. Takovou skutečnost uvede navrhovatel v záznamech o identifikovaných nebezpečích. Za důkaz o usměrňování rizika je považován ES-Certifikát (NoBo), ES-Prohlášení o ověření subsystému a Osvědčení o ověření (DeBo).

SPB provede posouzení vhodnosti odpovídající TSI a dalších náležitostí pro usměrňování konkrétního nebezpečí a v ZPB uvede své stanovisko.

## Závěr

Článek byl zaměřen na proces řízení rizik navrhovaných a prováděných změn u železničních subsystémů, na činnost a odpovědnost navrhovatele a na činnost a odpovědnost subjektu, který provádí nezávislé posuzování procesu řízení rizik a bezpečnostních parametrů šetřením objektivních důkazů a s cílem dospět k rozhodnutí, zda systém splňuje bezpečnostní požadavky.

## Literatura:

- [1] Prováděcí nařízení Komise (EU) č. 402/2013 ze dne 30. dubna 2013 o společné bezpečnostní metodě pro hodnocení a posuzování rizik a o zrušení nařízení (ES) č. 352/2009
- [2] BABINEC, F. Management rizika, Slezská Universita v Opavě, Ústav matematiky, 2005
- [3] BERNATÍK, A. Prevence závažných havárií II., VŠB-TUO, 2006
- [4] TRBOJEVIC, V. M. Risk criteria in EU, Risk Support Limited, London, dostupný z: <http://www.risk-support.co.uk/B26P2-Trbojevic-final.pdf>

## Citované normy:

ČSN IEC 60050(192):2016	Mezinárodní elektrotechnický slovník, část 192: Spolehlivost
ČSN EN 60300-1 ed.2:2015	Management spolehlivosti – Část 1: Návod pro management a použití
ČSN EN 60300-3-10:2011	Management spolehlivosti – Část 3-10: Návod k použití - Udržovatelnost
ČSN EN 60812:2007	Techniky analýzy bezporuchovosti systémů – Postup analýzy způsobů a důsledků poruch
ČSN EN 61025:2007	Analýza stromu poruchových stavů (FTA)
ČSN EN 50126-1:2012	Drážní zařízení – stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS)

## Seznam zkratek:

CSM RA	Prováděcí nařízení Komise (EU) č. 402/2013 v platném znění Commission implementing regulation (EU) No. 402/2013 on the <b>C</b> ommon <b>S</b> afety <b>M</b> ethod for <b>R</b> isk evaluation and <b>A</b> ssessment
EU	Evropská Unie
ETCS	Evropský vlakový zabezpečovací systém ( <b>E</b> uropean <b>T</b> rain <b>C</b> ontrol <b>S</b> ystem)
FMEA	Analýza způsobů a důsledků ( <b>F</b> ailure <b>M</b> ode and <b>E</b> ffects <b>A</b> nalysis)
FMECA	<b>F</b> ailure <b>M</b> ode, <b>E</b> ffects and <b>C</b> riticality <b>A</b> nalysis
FTA	Analýza stromu poruchových stavů
IRS	Mezinárodní železniční řešení ( <b>I</b> nternational <b>R</b> ailway <b>S</b> olution)
RAMS	bezporuchovost, pohotovost, udržovatelnost a bezpečnost ( <b>R</b> eliability, <b>A</b> vailability, <b>M</b> aintainability, <b>S</b> afety)
SPB	Subjekt pro posuzování bezpečnosti



SPB SŽDC –TÚDC interní Subjekt pro posuzování bezpečnosti státní organizace  
SŽDC, s.o., TÚDC  
ZPB Zpráva o posouzení bezpečnosti

Praha, září 2017

Lektorovali: Aleš Pokorný  
Dražní úřad

Ing. Jan Jelének, doc. Ing. P. Fuchs, CSc.  
IO č. 4061 VÚKV a.s.