Miroslav Šídlo[1]

Zahájení procesu řízení rizik při provádění technických změn na železničních subsystémech

Klíčová slova: *riziko, management rizik, analýza rizika, posuzování rizika, hodnocení rizika, řízení rizika, proces řízení rizika, kodex správné praxe, referenční systém, odhad rizika, identifikace nebezpečí, záznam předpokládaných nebezpečí, záznam o nebezpečí.*

Úvod

Tento článek je volným pokračováním mého článku „Proces nezávislého posuzování technických změn na železničních subsystémech ve vztahu k procesu řízení rizik“, publikovaného v č. 44 VTS ČD koncem roku 2017.

Podle článku 5 „Proces řízení rizik“ prováděcího nařízení Komise EU č. 402/2013 v platném znění, označované též jako CSM on Risk Assessment, CSM RA [1] navrhovatel odpovídá za použití uvedeného nařízení. V článku je uvedeno, že rizika způsobená jeho dodavateli a poskytovateli služeb včetně jejich subdodavatelů byla řízena v souladu s uvedeným nařízením. Za tímto účelem může navrhovatel prostřednictvím smluvních podmínek požadovat, aby se jeho dodavatelé a poskytovatelé služeb, včetně subdodavatelů, podíleli na procesu řízení rizik stanoveném v příloze I. „Obecné zásady použitelné na proces řízení rizik“ CSM RA.

1 Způsob zahájení procesu řízení rizik

1.1 Jedním ze způsobů, jak zahajovat proces řízení rizik, je pochopení a uplatnění přístupu k managementu RAMS.

1.2 V EU poskytuje popis procesu RAMS evropská norma ČSN EN 50126 pro drážní zařízení. Norma ČSN EN 50126 je platná do 3. 7. 2020 a byla již nahrazena normou ČSN EN 50126-1 ed. 2 (datum schválení 1. 6. 2018, datum účinnosti 1. 7. 2018, převzetí v češtině se připravuje). Dále v textu uvádím pouze označení Norma.

1.3 Normu může provozovatel dráhy i drážní průmysl systematicky používat ve všech etapách životního cyklu systému drážního zařízení.

[1] 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.

1.4 Norma není vyžadována u stávajících nemodifikovaných systémů včetně systémů, které byly v souladu s předchozími normami ČSN EN 50126.

1.5 Norma definuje RAMS z hlediska bezporuchovosti, pohotovosti, udržovatelnosti, bezpečnosti a jejich vzájemného působení.

1.6 Norma definuje životní cyklus systému a úkoly, které do něho spadají.

1.7 Norma nedefinuje cíle, ani číselné hodnoty, požadavky nebo řešení pro konkrétní drážní zařízení.

1.8 Norma nespecifikuje požadavky na zajištění bezpečnosti systému a ani pravidla a postupy, které se týkají certifikace drážních výrobků.

1.9 Norma nedefinuje postupy schvalování řídicími orgány pro otázky bezpečnosti (Národní bezpečnostní úřad NSA).

1.10 Proces definovaný Normou předpokládá, že navrhovatelé a dodavatelé mají zavedeny politiky týkající se jakosti, výkonu a bezpečnosti.

1.11 Přístup definovaný Normou je v souladu s aplikacemi požadavků na řízení jakosti podle ČSN EN ISO 9001.

2 Činnosti procesu řízení rizik v prvních 3 etapách životního cyklu

2.1 V etapě č. 1 životního cyklu, kterou označujeme jako „Stanovení koncepce“, se definuje účel a rozsah drážního projektu.

2.2 Obvykle se zpracovává studie proveditelnosti projektu a finanční analýza (business case study).

2.3 Z pohledu bezpečnosti by měly být přezkoumány dříve dosahované parametry bezpečnosti u podobných projektů, měly by být definovány dopady projektu na bezpečnost a měly by být stanoveny cíle bezpečnosti, které budou použity pro stanovení koncepce bezpečnosti.

2.4 Etapa č. 2, nazývaná jako „Definice systému a podmínky použití“, slouží ke stanovení základních charakteristik systému, vypracování popisu systému, ale také strategie provozu a údržby, pracovních podmínek a omezujících faktorů daných stávající infrastrukturou. **Z hlediska bezpečnosti by měla být právě v této etapě definována kritéria přípustnosti rizik**.

2.5 Etapa č. 3 se nazývá etapou „Analýzy rizik“. Norma v této etapě uvádí, že mají být vytvořeny a zavedeny tzv. **Záznamy předpokládaných nebezpečí**. V této etapě se provádí analýzy nebezpečí systému a provádí se hodnocení rizik.

3 Záznam předpokládaných nebezpečí

3.1 Identifikací předpokládaných nebezpečí se rozumí provedení postupu ke zjištění, zdokumentování a charakterizaci nebezpečí.

3.2 Záznamem předpokládaných nebezpečí (nebo stručně záznam o nebezpečí) se rozumí doklad, ve kterém jsou zaznamenána všechna zjištěná nebezpečí, jejich původ (nebo příčina), návrh bezpečnostních opatření a odkaz na organizaci, která je má řídit.

Důležité poznámky:

V záznamech s identifikací nebezpečí se velice často setkávám s těmito dvěma jevy:

1) S konstatováním „byla identifikována tato nebezpečí…“.
2) S kvalitativní klasifikací (hodnocením) rizika bez uvedení kritérií.

Konstatování podle bodu 1) považuji za nešťastné a nedostatečné. Důležitá je metoda, kterou navrhovatel k identifikaci nebezpečí použil. Obvykle se používají výstupy metody struktur „Co se stane, když…“, výstupy z vlastních znalostních databází (proto byly v odstavci 2 tyto analýzy zmíněny), výstupy z tzv. brainstormingu pro identifikaci nebezpečí, výstupy z metody HAZOP (dle ČSN EN 61882) pro studii nebezpečí a provozuschopnosti apod.

Konstatování kvalitativní klasifikace rizika, viz bod 2), např. jako riziko nepřípustné, musí být odstraněno, lze sice považovat za „bezpečné“ rozhodnutí, ale částečně alibisticky popírá metodu analýzy rizik. Podle Normy je stanoven postup jinak. Ve dvou nezávislých procesních cestách se provádí analýza četnosti výskytu nežádoucího jevu v cestě jedné a analýza důsledků cestou druhou. Výstupem první cesty je kvalifikovaný odhad pravděpodobnosti výskytu, výstupem druhé cesty je odhad důsledků. Klasifikace rizika je následně provedena konkrétní metodou s ohledem na předem stanovená kritéria, která pracují s odhadnutou pravděpodobností výskytu a odhadnutým důsledkem. Metoda bývá nazývána jako jednoznačný odhad rizik.

U technických drážních systémů bývá analýza rizika často zastavena, pokud je pravděpodobnost výskytu nižší než 10^{-9}/hodina provozu. V takovém případě už nemusí být podle CSM RA riziko dále zkoumáno a ani snižováno.

3.3 Platí důležitý princip daný nařízením CSM RA:

Subjekt pro posuzování nesmí navrhovateli nařídit, aby použil konkrétní zásadu přijetí rizika.

4 Příklad struktury Záznamu předpokládaných nebezpečí

V rámci posuzování procesu řízení rizik jsem se setkal s různými strukturami dokumentů s identifikací předpokládaných nebezpečí. V etapě č. 1 a č. 2 životního

cyklu subsystému byly vytvořeny jednoduché tabulkové struktury, které obsahovaly tyto sloupce: číslo nebezpečí, popis nebezpečí, možnou příčinu, důsledek, odhad četnosti a klasifikaci rizika.

Pro etapu č. 3 již považuji takovou strukturu za nedostatečnou a přikláním se k následující minimální struktuře sloupců tabulky záznamu: pořadové číslo nebezpečí, název nebezpečí, příčina nebezpečí, nejhorší důsledek, **metoda usměrnění**, četnost výskytu, klasifikace rizika, **návrh na usměrnění**, **výsledek po usměrnění** a **odkaz na organizaci nebo provozní složku**, která má riziko řídit.

Forma vedení záznamu nebyla navrhovatelům stanovena. Doporučuji vést Záznam předpokládaných nebezpečí v elektronické formě a v tabulkové struktuře s uvedenými sloupci.

Účel jednotlivých sloupců je následující:

1) Pořadové číslo nebezpečí slouží k jednoznačné identifikaci nebezpečí při jeho další analýze. Je pravdou, že se velice často vyskytují nebezpečí uvedená s podobnými názvy, která se však liší příčinou (původem) a/nebo v celé řadě parametrů.

2) Název nebezpečí se používá při výměně informací během procesu řízení rizik. Mělo by jít o jednoduchý a výstižný název. Pokud si problematika vyžádá např. podrobný popis nebo samostatnou analýzu, použije se odkaz na potřebné dokumenty.

3) Příčina nebezpečí se používá při výměně informací během procesu řízení rizik. Občas bývá příčina nebezpečí uvedena místo názvu nebezpečí. Tento jev se do identifikace nebezpečí dostal např. z kvalitativní analýzy spolehlivosti metodami FMEA. Má to logiku. Finálním cílem kvalitativní analýzy je vyhledat všechny prvky, jejich příčiny poruch a popsat důsledky, které tyto poruchy mohou mít, a určit jejich vliv na chování, vlastnosti nebo parametry subsystému.

4) Nejhorší důsledek je parametr, který se použije při klasifikaci (vyhodnocení) rizika.

5) Metoda usměrnění je důležitý parametr, který se uplatní při řízení (managementu) rizika. **Podle CSM RA platí, že v případě uplatnění metody kodexu správné praxe nebo při uplatnění metody srovnání s referenčním systémem se další analýza rizika neprovádí**.

Upozorňuji zde na uvedený fakt v souvislosti se situací, kdy navrhovatel provede dělení subsystému do velké hloubky (příliš detailně) a zvolí složité metody analýzy. Analytici se mohou dostat do časových tísní z nadměrného rozsahu prací, ale také do situací, kdy nebudou potřebné informace pro analýzu rizik mít k dispozici. Výsledkem takového počínání může být nejen nedodržení termínů výstupů analýzy, ale hlavně zatížení výsledků nejistotami stochastické povahy. Osobně preferuji použít rozumnou hloubku dělení systému a přesvědčit se o dostupnosti informací. Zpravidla během takto aplikovaného postupu dospějeme k závěrům, že celá řada parametrů navrhované změny podléhá působnosti kodexů správné praxe. Např. bezpečnost

elektrického zařízení je zajištěna jeho provedením podle platných norem nebo požární bezpečnost stavby je zajištěna s uplatněním norem požárně bezpečnostního řešení.

6) Četnost výskytu nežádoucí události je parametr, který se uplatní při hodnocení rizika. Často nejsou k dispozici relevantní statistické údaje a místo četnosti výskytu se pracuje se stanovenou pravděpodobností výskytu.

7) Klasifikace (hodnocení) rizika je výsledek kvantitativního porovnání pravděpodobnosti výskytu nežádoucí události, která může vést k předpokládanému důsledku. Příklad hodnocení rizika s uplatněním tabulky je stanoven v Normě. U každého stupně hodnocení bývají uvedené podmínky, za kterých lze nebo nelze riziko přijmout.

8) Návrh na usměrnění obsahuje způsob, kterým je riziko usměrněno.

Některá rizika lze usměrnit technickými prostředky. Použije se technické zařízení, které plní konkrétní bezpečnostní funkci, tzv. bariéru, která významně snižuje četnost výskytu nežádoucí události. Toho lze dosáhnout např. užitím vhodné architektury zařízení, uplatněním vhodných technik, metod a nástrojů. Obvykle se stanovuje parametr THR a úroveň integrity bezpečnosti SIL zařízení, které plní bezpečnostní funkci. Úroveň SIL bývá uváděna v základních požadavcích na zařízení, které plní bezpečnostní funkci.

Jiná rizika nelze usměrnit jen technickými prostředky. Například riziko narušení nebo zničení prvků tzv. kritické infrastruktury působením člověka (antropogenní hrozba) má vážný dopad na bezpečnost celého subsystému. **Usměrnění lze dosáhnout systémem vzájemně provázaných technických, technologických a režimových opatření** k fyzické ochraně objektu, který dokáže omezit nebo eliminovat následky hrozeb.

9) Výsledkem usměrnění je konstatování, zda bylo riziko zcela usměrněno a byly splněny bezpečnostní požadavky kladené na systém, nebo zda riziko zůstává otevřené.

10) Organizace a její organizační složka, která odpovídá za řízení rizika, musí být v záznamu předpokládaných nebezpečí uvedeny.

V tomto místě se vrátíme do druhé etapy životního cyklu, viz odstavec 2.4 článku 2 tohoto příspěvku.

Etapa č. 2 slouží ke stanovení strategie provozu a údržby, pracovních podmínek a různých omezujících faktorů. Budeme vycházet z principu, že nastavení provozu a údržby, pracovních podmínek a přijatých omezujících faktorů subsystému platí, ale příslušnou **provozně-organizační složkou budou v průběhu dalších etap do záznamu s identifikací předpokládaných nebezpečí doplňovány další řádky tabulky s novými pořadovými čísly**.

Pro jistotu si teď uvědomíme dvě základní charakteristiky **prediktivní analýzy RAMS,** se kterou jsme začali v prvních etapách životního cyklu zařízení pracovat. Drážní systém, ve kterém uplatňujeme Normu, má **interaktivní** a **iterativní** charakter. Závěry z analýz, prováděné v různých etapách životního cyklu, vedou ke změnám v subsystému a ke zvyšování jeho spolehlivosti a bezpečnosti (**iterativní charakter** metody). Informace o vzniku nežádoucích událostí a jejich důsledků často získáváme až z chování obdobných systémů při provozu. Tyto zkušenosti přenášíme do očekávaného chování nového subsystému. Přenášíme tam rovněž **předpověditelné** způsoby chování, které se dosud nevyskytly, které ovšem mají stochastickou povahu. Nejistoty stochastické povahy můžeme však korigovat zpravidla až v reálném provozu (**interaktivní charakter** metody).

5 Další činnosti související se záznamy o nebezpečí

Záznam o nebezpečí zakládá navrhovatel při zpracovávání návrhu změny. Záznamy jsou doplňovány a aktualizovány navrhovatelem a účastníky, kteří se podílejí v průběhu všech etap životního cyklu zařízení na procesu řízení rizik.

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 usměrňováním nebezpečí v procesu řízení rizik.

Platí zásada o výměně informací (viz CSM RA, příloha I., čl. 4.2 Výměna informací). Nebezpečí, která nemůže jeden účastník procesu řízení rizik usměrnit sám, jsou 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).

6 Ostatní aspekty procesu řízení rizik

V ČR lze uplatnit další aspekty, které se týkají procesu řízení rizik. Za kodexy správné praxe lze považovat TSI, pokud jsou vhodné pro usměrňování identifikovaných nebezpečí v posuzovaném systému. Takovou skutečnost uvede navrhovatel v záznamech o identifikovaných nebezpečích.

Za důkaz o usměrnění rizika je považován ES-Certifikát (NoBo), ES-Prohlášení o ověření subsystému a Osvědčení o ověření (DeBo).

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

Závěr

Článek byl zaměřen na jeden ze způsobů zahájení procesu řízení rizik navrhovaných a prováděných změn u železničních subsystémů a na činnost a odpovědnost navrhovatele změny. Zahájení procesu bylo popsáno spolu s vedením jednoduché formy identifikace předpokládaných nebezpečí, což není pouhé založení a vedení dokumentu, ale uplatnění celé řady analytických postupů, jejichž příklady byly uvedeny. Postupy, které přímo souvisí s procesem řízení rizik a uplatňováním nařízení CSM RA, jsou vnitrostátním uznávacím orgánem (NSA CZ – Drážní úřad) upřesňovány vydávanými metodickými pokyny pro navrhovatele.

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

Citované normy:

ČSN IEC 60050(192):2016	Mezinárodní elektrotechnický slovník, část 192: Spolehlivost
ČSN EN 61882:2016	Studie nebezpečí a provozuschopnosti (studie HAZOP) – Pokyn k použití
ČSN EN 61025:2007	Analýza stromu poruchových stavů (FTA)
ČSN EN 60812:2007	Techniky analýzy bezporuchovosti systémů – Postup analýzy způsobů a důsledků poruch (FMEA)
ČSN EN 50126-1:2001	Drážní zařízení – stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS)
ČSN EN 50126-1 ed. 2	Drážní zařízení – stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS) – Část 1: Obecný RAMS postup
ČSN EN ISO 9001, ČSN EN ISO 9002 ČSN EN ISO 9003	Systémy managementu kvality - Požadavky

Seznam zkratek:

CSM RA	Prováděcí nařízení Komise (EU) č. 402/2013 v platném znění Commission implementing regulation (EU) No. 402/2013 on the **C**ommon **S**afety **M**ethod for **R**isk evaluation and **A**ssessment
EU	**E**vropská **U**nie
FMEA	Analýza způsobů a důsledků (**F**ailure **M**ode and **E**ffects **A**nalysis)
FMECA	**F**ailure **M**ode, **E**ffects and **C**riticality **A**nalysis
FTA	Analýza stromu poruchových stavů (**F**ault **T**ree **A**nalysis) Norma Zkrácené označení (použité v textu) pro ČSN EN 50126-1 ed. 2
RAMS	bezporuchovost, pohotovost, udržovatelnost a bezpečnost (**R**eliability, **A**vailability, **M**aintainability, **S**afety)
SIL	Úroveň integrity bezpečnosti (**S**afety **I**ntegrity **L**evel)
SPB	**S**ubjekt pro **p**osuzování **b**ezpečnosti
SPB SŽDC–TÚDC	interní Subjekt pro posuzování bezpečnosti státní organizace SŽDC, s. o., TÚDC
THR	Tolerovaná intenzita nebezpečí (**T**olerable **H**azard **R**ate)
TSI	Technická specifikace pro interoperabilitu
ZPB	**Z**práva o **p**osouzení **b**ezpečnosti

Praha, červen 2018

Lektorovali: Ing. Jiří Jelének
IO č. 4061 VÚKV a.s.

Aleš Pokorný
Drážní úřad