Evropská agentura pro železnice (ERA)

Soubor příkladů posuzování rizik a některých možných nástrojů podporujících nařízení CSM

Značka v ERA:	ERA/GUI/02-2008/SAF
Verze v ERA:	1.1
Datum:	06.01.2009

Dokument vypracovala	Evropská agentura pro železnice Rue Marc LEFRANCQ, 120 BP 20392 F-59307 Valenciennes Cedex Francie
Typ dokumentu:	Průvodce
Status dokumentu:	Veřejný

	Jméno	Funkce
Vydal	Marcel VERSLYPE	Výkonný ředitel
Zkontrolovali	Anders LUNDSTRÖM Thierry BREYNE	Vedoucí bezpečnostního oddělení Vedoucí sektoru posuzování bezpečnosti
Dokument sestavil (autor)	Dragan JOVICIC	Bezpečnostní oddělení – projektový úředník

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

INFORMACE O DOKUMENTU

Historie změn

Tabulka 1: Status dokumentu.

Datum verze	Autor (autoři)	Číslo oddílu	Popis změny
Název a struktura původního dokumentu: *Pokyny pro uplatňování doporučení k 1. souboru CSM*			
Pokyny Verze 0.1 15.02.2007	Dragan JOVICIC	Všechny	První verze pokynů pro uplatňování související s verzí 1.0 prvního souboru doporučení CSM. Toto je také první verze dokumentu předaného pracovní skupině CSM k formálnímu přezkumu.
Pokyny Verze 0.2 07.06.2007	Dragan JOVICIC	Všechny	Změna členění dokumentu tak, aby odpovídal struktuře verze 4.0 doporučení CSM. Aktualizace zohledňující proces formálního přezkumu verze 1.0 doporučení provedeného pracovní skupinou CSM.
		Všechny	Aktualizace dokumentu o doplňující informace získané v průběhu interních jednání ERA a rovněž v souvislosti s požadavky pracovního týmu a pracovní skupiny CSM na rozpracování nových bodů.
		obr. 1	Změna vyobrazení znázorňujícího „rámec řízení bezpečnosti pro první soubor společných bezpečnostních metod“ v souladu s připomínkami, které vyplynuly z přezkumu, a terminologií ISO.
Pokyny Verze 0.3 20.07.2007	Dragan JOVICIC	Přílohy	Změna členění příloh a vytvoření příloh nových. Nová příloha pro soustředění všech schémat, která ilustrují průvodce a usnadňují jeho čtení a přispívají k snazšímu porozumění jeho obsahu.
		Všechny oddíly	Dokument byl aktualizován s cílem: • rozpracovat v maximální možné míře stávající oddíly x, • dále rozpracovat aspekty označované jako „prokázání shody systému s bezpečnostními požadavky“, • zajistit vazbu na V-cyklus norem CENELEC (tj. obrázek 8 a obrázek 10 normyEN 50 126), • rozvíjet dále potřebu spolupráce a koordinace mezi různými subjekty odvětví železniční dopravy, jejichž činnosti mohou mít dopad na bezpečnost železničního systému, • předložit vysvětlení týkající se důkazů (např. bezpečnostní záznamník a doklad bezpečnosti), které mají prokázat subjektům pro posuzování správné uplatňování procesu posuzování rizik CSM. Dokument byl aktualizován také na základě prvního interního přezkumu provedeného agenturou.
Pokyny Verze 0.4 16.11.2007	Dragan JOVICIC	Všechny oddíly	Dokument byl aktualizován v návaznosti na proces formálního přezkumu podle připomínek přijatých k verzi 0.3 od následujících členů pracovní skupiny CSM a organizací CSM, které s nimi byly telefonicky dohodnuty: • belgické, španělské, finské, norské, francouzské a dánské vnitrostátní bezpečnostní orgány (NSA), • SIEMENS (člen UNIFE), • norský provozovatel infrastruktury (Jernbaneverket – člen EIM).
Pokyny Verze 0.5 27.02.2008	Dragan JOVICIC	Všechny oddíly	Dokument byl aktualizován podle připomínek přijatých k verzi 0.3 od následujících členů pracovní skupiny CSM a organizací CSM, které s nimi byly telefonicky dohodnuty: • CER, • nizozemské vnitrostátní bezpečnostní orgány (NSA).
		Všechny oddíly	Dokument byl aktualizován v souladu s podepsanou verzí doporučení CSM. Dokument byl aktualizován podle připomínek, které vyplynuly z interního přezkumu agentury a jejichž autorem je Christophe CASSIR a Marcus ANDERSSON.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Tabulka 1: Status dokumentu.

Datum verze	Autor (autoři)	Číslo oddílu	Popis změny
		Všechny oddíly Přílohy	Úplné přečíslování odstavců v dokumentu oproti doporučením. Do dokumentu byly začleněny příklady uplatňování doporučení CSM.
Nový název a struktura dokumentu: *Soubor příkladů posuzování rizik a některých možných nástrojů podporujících nařízení CSM*			
Průvodce Verze 0.1 23.05.2008	Dragan JOVICIC	Všechny	První verze dokumentu vyplývající z rozdělení „pokynů pro uplatňování“ verze 0.5 do dvou vzájemně se doplňujících dokumentů.
Průvodce Verze 02 03.09.2008	Dragan JOVICIC	Všechny	Aktualizace dokumentu v souladu: • s nařízením CSM Evropské komise {Ref. 3}, • připomínky ze semináře ze dne 1. července 2008 s členy Výboru pro interoperabilitu a bezpečnost železnic (RISC), • připomínky od členů pracovní skupiny CSM (norské vnitrostátní bezpečnostní orgány, finské vnitrostátní bezpečnostní orgány, vnitrostátní bezpečnostní orgány Spojeného království a francouzské vnitrostátní bezpečnostní orgány, CER, EIM, Jens BRABAND [UNIFE] a Stéphane ROMEI [UNIFE].
Průvodce Verze 1.0 10.12.2008	Dragan JOVICIC	Všechny	Aktualizace dokumentu v souladu snařízením Evropské komise o hodnocení a posuzování rizik {Ref. 3} přijatého Výborem pro interoperabilitu a bezpečnost železnic (RISC) v průběhu jejich plenárního zasedání dne 25. listopadu 2008.
Průvodce Verze 1.1 06.01.2009	Dragan JOVICIC	Všechny	Aktualizace dokumentu podle připomínek k nařízení CSM vznesených právními a jazykovými službami Evropské komise.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Obsah

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Seznam vyobrazení

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Seznam tabulek

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

0. ÚVOD

0.1. Oblast působnosti

0.1.1. Cílem tohoto dokumentu je poskytnout další vysvětlení k „nařízení Komise o přijetí společné bezpečnostní metody pro hodnocení a posuzování rizik, jak je uvedeno v čl. 6 odst. 3 písm. a) směrnice Evropského parlamentu a Rady 2004/49/ES" {Ref. 3}. Toto nařízení bude v dokumentu označováno jako „nařízení CSM“.

0.1.2. Tento dokument není právně závazný a jeho obsah nelze vykládat jako jediný způsob, jak dosáhnout požadavků CSM. Cílem dokumentu je doplnit Průvodce pro uplatňování nařízení CSM {Ref. 4} v otázkách způsobu, jakým by proces nařízení CSM mohl být používán a uplatňován. Poskytuje doplňující praktické informace, aniž by jakýmkoli způsobem diktoval povinné postupy, které by měly být dodržovány, či zaváděl právně závazné postupy. Tyto informace mohou být užitečné pro všechny subjekty[(1)], jejichž činnosti mohou mít dopad na bezpečnost železničních systémů a které musí přímo nebo nepřímo používat CSM. Tento dokument uvádí příklady posuzování rizik a prezentuje některé možné nástroje, které podporují uplatňování CSM. Příklady jsou uváděny pouze jako orientační vodítko. Příslušné subjekty mohou používat jiné metody nebo mohou i nadále používat své vlastní stávající metody a nástroje pro dosažení souladu s CSM, pokud je považují za vhodnější.
Příklady a doplňující informace obsažené v tomto dokumentu také nejsou vyčerpávající a nepostihují veškeré možné situace, v souvislosti s nimiž jsou navrhovány významné změny, a tento dokument lze chápat pouze jako čistě informativní.

0.1.3. Tento informativní dokument je třeba chápat pouze jako doplňkový nástroj podporující uplatňování nařízení CSM. Pokud bude tento dokument používán, jeho obsah je třeba chápat ve spojení s nařízením CSM {Ref. 3} a souvisejícím průvodcem {Ref. 4} s cílem dále přispět ke snazšímu uplatňování CSM, avšak nenahrazuje nařízení CSM.

0.1.4. Tento dokument byl zpracován Evropskou agenturou pro železnice (ERA) za pomoci odborníků železničních svazů a vnitrostátních bezpečnostních orgánů (NSA) z pracovní skupiny CSM. Představuje rozpracovaný soubor podnětů a informací získaných ERA v průběhu interních jednání a jednání s pracovní skupinou CSM a pracovními týmy CSM. V případě potřeby ERA tento dokument přezkoumá a aktualizuje, aby do něj promítla pokrok v oblasti evropských norem, změny nařízení CSM o posuzování rizika a případnou zpětnou vazbu ze zkušeností týkajících se uplatňování nařízení CSM. Vzhledem k tomu, že v době vzniku tohoto dokumentu nelze předjímat časový průběh tohoto procesu změn, jeho uživatel by se měl obrátit na ERA pro informace o nejaktuálnějším vydání tohoto dokumentu, které je k dispozici.

0.2. Otázky nespadající do oblasti působnosti tohoto dokumentu

0.2.1. Tento dokument nedává pokyny jak organizovat, provozovat nebo navrhovat (a vyrábět) železniční systém nebo jeho části. Nedefinuje také žádné smluvní dohody nebo ujednání, které mohou případně existovat mezi některými subjekty v otázkách uplatňování procesu řízení rizik. Smluvní ujednání týkající se konkrétního projektu nespadají do oblasti

(1) *Dotčené subjekty jsou zadavatelé v souladu s jejich definicí v čl. 2 písm. r) směrnice 2008/57/ES o interoperabilitě železničního systému ve Společenství nebo výrobci, v nařízení souhrnně označovaní jako „navrhovatelé“, nebo jejich dodavatelé či poskytovatelé služeb.*

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

působnosti nařízení CSM, ani do oblasti působnosti souvisejícího průvodce či tohoto dokumentu.

0.2.2. Přestože výše uvedená smluvní ujednání nespadají do oblasti působnosti tohoto dokumentu, jsou-li dohodnuta mezi příslušnými subjekty, mohou být zakotvena v příslušných smlouvách na začátku projektu, aniž by tím však byla dotčena ustanovení CSM. Mohou se týkat například:

(a) nákladů spojených s řízením rizik souvisejících s bezpečností na rozhraní mezi subjekty,
(b) nákladů spojených s přenosem nebezpečí a se souvisejícími bezpečnostními opatřeními mezi subjekty, které na začátku projektu nejsou známy,
(c) otázek způsobu řízení sporů, které mohou vzniknout v průběhu projektu,
(d) apod.

Pokud dojde k neshodám nebo sporům mezi navrhovatelem a jeho subdodavateli v průběhu postupu projektu, lze poukázat na příslušné smlouvy s cílem přispět k vyřešení jakéhokoli sporu.

0.3. Zásada pro tento dokument

0.3.1. Přestože se tento dokument může z hlediska seznamování se s jeho obsahem jevit jako samostatný, nenahrazuje nařízení CSM {Ref. 3}. Pro snadnější orientaci je v tomto dokumentu přímo citován každý článek nařízení CSM. {Ref. 4}. V následujících odstavcích jsou pak uvedeny doplňující informace s cílem usnadnit porozumění textu nařízení tam, kde je to považováno za potřebné.

0.3.2. Znění článků a jejich nejpodstatnějších odstavců nařízení CSM je zkopírováno do textových rámečků tohoto dokumentu a uvedeno kurzívou s použitím fontu „Bookman Old Style“ . Toto formátování umožňuje snadněji rozlišit původní text nařízení CSM {Ref. 3} od doplňujících výkladů uvedených v tomto dokumentu. Text Průvodce pro uplatňování nařízení CSM {Ref. 4} není zkopírován do tohoto dokumentu.

0.3.3. Struktura tohoto dokumentu se pro snazší orientaci uživatele řídí strukturou nařízení CSM

0.4. Popis dokumentu

0.4.1. Dokument je rozdělen do těchto částí:

(a) kapitola 0., která definuje oblast působnosti dokumentu a uvádí seznam referenčních dokumentů,
(b) příloha I a příloha II poskytují doplňující informace k příslušným oddílům nařízení CSM {Ref. 3} a souvisejícího průvodce {Ref. 4},
(c) nové přílohy dále rozpracovávají některé konkrétní aspekty a uvádějí příklady.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

0.5. Referenční dokumenty

Tabulka 2: Tabulka referenčních dokumentů

{Zn. č.}	Název	Odkaz na dokument	Verze
{Ref. 1}	Směrnice Evropského parlamentu a Rady 2004/49/ES ze dne 29. dubna 2004 o bezpečnosti železnic Společenství a o změně směrnice Rady 95/18/ES o vydávání licencí železničním podnikům a směrnice 2001/14/ES o přidělování kapacity železniční infrastruktury, zpoplatnění železniční infrastruktury a o vydávání osvědčení o bezpečnosti (směrnice o bezpečnosti železnic)	2004/49/ES Úř. věst. L 164, 30.4.2004, s. 44, směrnice naposledy pozměněná v Úř. věst. L 220, 21.6.2004, s. 16	–
{Ref. 2}	Směrnice Evropského parlamentu a Rady 2008/57/ES ze dne 17. června 2008 o interoperabilitě železničního systému ve Společenství	2008/57/ES Úř. věst. L 191, 18.7.2008, s. 1	–
{Ref. 3}	Nařízení Komise (ES) č.352/2009 ze dne 24. dubna 2009 o přijetí společné bezpečnostní metody pro hodnocení a posuzování rizik, jak je uvedeno v čl. 6 odst. 3 písm. a) směrnice Evropského parlamentu a Rady 2004/49/ES	ES 352/2009	24. dubna 2009
{Ref. 4}	Průvodce pro uplatňování nařízení Komise o přijetí společné bezpečnostní metody pro hodnocení a posuzování rizik, jak je uvedeno v čl. 6 odst. 3 písm. a) směrnice o bezpečnosti železnic	ERA/GUI/01-2008/SAF	1.0
{Ref. 5}	Směrnice Evropského parlamentu a Rady 2008/57/ES ze dne 17. června 2008 o interoperabilitě železničního systému ve Společenství	2008/57/ES Úř. věst. L 191, 18.7.2008, s. 1	–
{Ref. 6}	Systém řízení bezpečnosti (SMS) – hodnotící kritéria pro železniční podniky a provozovatele infrastruktury	Hodnotící kritéria SMS Část A Osvědčení o bezpečnosti a schválení z hlediska bezpečnosti	31. 5. 2007
{Ref. 7}	Železniční aplikace – Sdělovací a zabezpečovací systémy a systémy zpracování dat – Elektronické zabezpečovací systémy	EN 50129	únor 2003
{Ref. 8}	Železniční aplikace – Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS) – část 1: norma jako taková	EN 50126-1	září 2006
{Ref. 9}	Železniční aplikace – Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS) část 2: Pokyny k uplatňování normy EN 50126-1 pro bezpečnost	EN 50126-2 (pokyny)	Návrh v konečném znění (srpen 2006)
{Ref. 10}	Standardní směrnice pro výpočet rizika spojeného s přepravou nebezpečných věcí po železnici	Směrnice OTIF schválená výborem odborníků RID	24. listopadu 2005.
{Ref. 11}	Kritérium přijatelnosti rizik pro technické systémy	Poznámka 01/08	1.1 (25. 1. 2008)
{Ref. 12}	Bezpečnostní oddělení ERA: Studie proveditelnosti – Přiřazení bezpečnostních cílů (subsystémům TSI) a konsolidace TSI z bezpečnostního hlediska WP1.1 – posouzení proveditelnosti přiřazení společných bezpečnostních cílů	WP1.1	1.0
{Ref. 13}	Železniční aplikace — Klasifikační systém pro kolejová vozidla — část 4: EN 0015380, část 4: Funkční skupiny.	EN 0015380 část 4	

0.6. Běžné definice, termíny a zkratky

0.6.1. Obecné definice, termíny a zkratky používané v tomto dokumentu lze najít v běžném slovníku.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

0.6.2. Nové definice, termíny a zkratky v tomto průvodci jsou definovány v oddílech v následujících pasážích tohoto dokumentu.

0.7. Zvláštní definice

0.7.1. Viz čl. 3.

0.8. Zvláštní termíny a zkratky

0.8.1. V tomto oddílu jsou definovány nové zvláštní termíny a zkratky, které jsou v tomto dokumentu používány často.

Tabulka 3: Tabulka termínů.

Termín	Definice
Agentura	Evropská agentura pro železnice (ERA)
Průvodce	Průvodce pro uplatňování nařízení Komise (ES) č.352/2009 ze dne 24. dubna 2009 o přijetí společné bezpečnostní metody pro hodnocení a posuzování rizik, jak je uvedeno v čl. 6 odst. 3 písm. a) směrnice Evropského parlamentu a Rady 2004/49/ES.
Nařízení CSM	Nařízení Komise (ES) č.352/2009 ze dne 24. dubna 2009 o přijetí společné bezpečnostní metody pro hodnocení a posuzování rizik, jak je uvedeno v čl. 6 odst. 3 písm. a) směrnice Evropského parlamentu a Rady 2004/49/ES" {Ref. 3}.

Tabulka 4: Tabulka zkratek.

Zkratka	Význam
CCS	Řízení a zabezpečení
CSM	Společná bezpečnostní metoda (společné bezpečnostní metody)
CST	Společné bezpečnostní cíle
EC	Evropská komise
ERA	Evropská agentura pro železnice
IM	Provozovatel infrastruktury (Provozovatelé infrastruktury)
ISA	Nezávislý posuzovatel bezpečnosti
OTIF	Mezivládní organizace pro mezinárodní železniční přepravu
MS	Členský stát
NOBO	Oznámený subjekt
NSA	Vnitrostátní bezpečnostní orgán
QMP	Proces řízení jakosti
QMS	Systém řízení jakosti
RISC	Výbor pro interoperabilitu a bezpečnost
RU	Železniční podnik (železniční podniky)
SMP	Proces řízení bezpečnosti
SMS	Systém řízení bezpečnosti
SRT	Bezpečnost v železničních tunelech
TBC	Bude doplněno
TSI	Technická specifikace pro interoperabilitu

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

VYSVĚTLENÍ ČLÁNKŮ NAŘÍZENÍ CSM

čl. 1 Účel

čl. 1 odst. 1

Toto nařízení stanoví společnou bezpečnostní metodu pro hodnocení a posuzování rizik (CSM), jak je uvedeno v čl. 6 odst. 3 písm. a) směrnice 2004/49/ES.

[G 1] Další vysvětlení se nepovažuje za nutné.

čl. 1 odst. 2

Cílem CSM pro hodnocení a posuzování rizik je udržení nebo zvyšování úrovně bezpečnosti železnic Společenství podle potřeby a praktické proveditelnosti. CSM by měla usnadnit přístup na trh pro služby železniční dopravy prostřednictvím harmonizace:

(a) procesů řízení rizik používaných k posouzení úrovní bezpečnosti a shody s bezpečnostními požadavky;
(b) výměny informací týkajících se bezpečnosti mezi jednotlivými účastníky v železničním odvětví s cílem zajistit bezpečnost mezi jednotlivými rozhraními, která mohou v tomto odvětví existovat;
(c) důkazů vyplývajících z použití procesu řízení rizik.

[G 1] Další vysvětlení se nepovažuje za nutné.

čl. 2 Oblast působnosti

čl. 2 odst. 1

CSM pro hodnocení a posuzování rizik se vztahuje na jakoukoli změnu železničního systému v členském státě, jak je uvedeno v bodě 2 písm. d) přílohy III směrnice 2004/49/ES, která je považována za významnou ve smyslu článku 4 tohoto nařízení. Tyto změny mohou být technické, provozní nebo organizační povahy. U organizačních změn se posuzují pouze ty změny, které by mohly mít dopad na provozní podmínky.

[G 1] CSM se vztahuje na železniční systém jako celek a týká se posuzování následujících změn železničních systémů, pokud jsou hodnoceny jako významné na základě uplatnění čl. 4:

(a) výstavba nových tratí nebo změny existujících tratí,
(b) zavádění nových a/nebo upravených technických systémů,
(c) provozní změny (jako například nové nebo upravené provozní předpisy a postupy údržby);
(d) změny v rámci organizací železničních podniků/provozovatelů infrastruktury.

Termínem „systém“ se v CSM rozumí všechny aspekty systému, včetně, kromě jiného, jeho vývoje, provozu, údržby atd., až do jeho vyřazení z provozu nebo likvidace.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 2] CSM se vztahuje na významné změny

(a) „malých a jednoduchých“ systémů, které mohou být tvořeny několika technickými subsystémy nebo prvky a
(b) „velkých a složitějších“ systémů (např. takových, jejichž součástí mohou být stanice a tunely).

čl. 2 odst. 2

Pokud se významné změny týkají strukturálních subsystémů, na něž se vztahuje směrnice 2008/57/ES, CSM pro hodnocení a posuzování rizik se použije:

(a) vyžadují-li posouzení rizik příslušné technické specifikace pro interoperabilitu (dále jen „TSI“). V takovém případě TSI tam, kde je to vhodné, specifikuje, které části CSM se použijí;
(b) k zajištění bezpečného začlenění strukturálních subsystémů, na něž se vztahují TSI, do stávajícího systému podle čl. 15 odst. 1 směrnice 2008/57/ES.

Použití CSM v případě uvedeném v prvním pododstavci písm. b) však nesmí vést k požadavkům, které jsou v rozporu s požadavky stanovenými v příslušných TSI, jež jsou závazné.

Pokud však použití CSM vede k požadavku, který je v rozporu s požadavkem stanoveným v příslušném TSI, navrhovatel informuje příslušný členský stát, který může rozhodnout, že požádá o revizi TSI v souladu s čl. 6 odst. 2 nebo článkem 7 směrnice 2008/57/ES nebo o výjimku v souladu s článkem 9 uvedené směrnice.

[G 1] Například v souladu se směrnicí o bezpečnosti železnic {Ref. 1} a směrnicí o interoperabilitě železnic {Ref. 2} musí nový typ kolejových vozidel pro vysokorychlostní trať vyhovovat požadavkům TSI pro vysokorychlostní kolejová vozidla. Přestože na většinu prvků posuzovaného systému se vztahuje TSI, stěžejní problém lidského faktoru souvisejícího s kabinou strojvedoucího není v TSI upraven. Aby bylo tedy zajištěno, že budou určena a přiměřeným způsobem usměrňována všechna rozumně předvídatelná nebezpečí související s problematikou lidského faktoru (tj. s rozhraními mezi strojvedoucím, kolejovým vozidlem a zbývající částí železničního systému), měl by být uplatněn proces CSM.

čl. 2 odst. 3

Toto nařízení se nevztahuje na:

(a) podzemní dráhy, tramvaje a další městské kolejové systémy;
(b) sítě, které jsou funkčně oddělené od ostatního železničního systému a jsou určeny pouze pro místní, městskou nebo příměstskou osobní dopravu, ani na železniční podniky s provozem pouze na těchto sítích;
(c) železniční infrastrukturu v soukromém vlastnictví, která je určena pouze pro používání vlastníkem pro jeho vlastní nákladní dopravu;
(d) historická vozidla, která jsou provozována na vnitrostátních sítích za předpokladu, že splňují vnitrostátní bezpečnostní pravidla a předpisy, aby byl zajištěn bezpečný provoz těchto vozidel;
(e) historické, muzeální a turistické železnice, které jsou provozovány na vlastní síti, včetně dílen, vozidel a pracovníků.

[G 1] Další vysvětlení se nepovažuje za nutné.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

čl. 2 odst. 4

Toto nařízení se nevztahují na systémy a změny, které jsou ke dni vstupu tohoto nařízení v platnost v pokročilé fázi vývoje ve smyslu čl. 2 písm. t) směrnice 2008/57/ES.

[G 1] Další vysvětlení se nepovažuje za nutné.

čl. 3 Definice

Pro účely tohoto nařízení se použijí definice stanovené v článku 3 směrnice 2004/49/ES.

Použijí se rovněž tyto definice:

(1) „rizikem“ se rozumí míra výskytu nehod a mimořádných událostí vedoucích k újmě (zapříčiněných nebezpečím) a stupeň závažnosti této újmy (EN 50126-2)*;*

(2) „analýzou rizik“ se rozumí systematické používání všech dostupných informací k určení nebezpečí a odhadu rizik (ISO/IEC 73)*;*

(3) „hodnocením rizik“ se rozumí postup založený na analýze rizik s cílem určit, zda bylo dosaženo přijatelného rizika (ISO/IEC 73)*;*

(4) „posuzováním rizik“ se rozumí celkový postup zahrnující analýzu a hodnocení rizik (ISO/IEC 73)*;*

(5) „bezpečností“ se rozumí odstranění nepřijatelného rizika újmy (EN 50126-1)*;*

(6) „řízením rizik“ se rozumí systematické uplatňování politik, postupů a praktik řízení na úkoly týkající se analýzy, hodnocení a usměrňování rizik (ISO/IEC 73)*;*

(7) „rozhraním“ se rozumí všechny body vzájemného působení během doby životnosti systému nebo subsystému, včetně provozu a údržby, kde jednotliví účastníci železničního odvětví vzájemně spolupracují za účelem řízení rizik;

(8) „účastníky“ se rozumí všechny subjekty, které se přímo nebo prostřednictvím smluvních ujednání podílejí na uplatňování tohoto nařízení podle čl. 5 odst. 2;

(9) „bezpečnostními požadavky“ se rozumí bezpečnostní vlastnosti (kvalitativní nebo kvantitativní) systému a jeho provozu (včetně provozních předpisů) nezbytné ke splnění cílů v oblasti bezpečnosti stanovených právními předpisy nebo dotyčnou společností;

(10) „bezpečnostními opatřeními“ se rozumí soubor opatření ke snížení míry výskytu nebezpečí nebo ke zmírnění jeho důsledků s cílem dosáhnout a/nebo zachovat přijatelnou úroveň rizika;

(11) „navrhovatelem“ se rozumí železniční podniky nebo provozovatelé infrastruktury v rámci opatření pro usměrňování rizik, která musí provést podle článku 4 směrnice 2004/49/ES, smluvní subjekty nebo výrobci, když požádají oznámený subjekt, aby provedl postup ověřování „ES“ v souladu s čl. 18 odst. 1 směrnice 2008/57/ES, nebo žadatel o povolení k uvedení vozidel do provozu;

(12) „zprávou o posouzení bezpečnosti“ se rozumí dokument, který obsahuje závěry posouzení, jež s ohledem na posuzovaný systém provedl subjekt pro posuzování;

(13) „nebezpečím“ se rozumí stav, který by mohl vést k nehodě (EN 50126-2)*;*

(14) „subjektem pro posuzování“ se rozumí nezávislá a způsobilá osoba, organizace nebo subjekt, který provede 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 zjištěná nebezpečí,

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

související opatření, jejich původ a odkaz na organizaci, která je má řídit;

(17) „identifikací nebezpečí“ se rozumí postup ke zjištění, zdokumentování a charakterizaci nebezpečí (ISO/IEC Guide 73)*;*

(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: analýza četnosti, důsledků a jejich integrace (ISO/IEC 73)*;*

(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, lidská obsluha a její úkony nejsou do technického systému zahrnuty; Postup údržby je popsán v příručkách údržby, sám o sobě však není součástí technického systému;

(23) „katastrofickým důsledkem” se rozumí smrtelné nehody a/nebo četná těžká zranění a/nebo velké škody na životním prostředí v důsledku nehody (Tabulka 3 from EN 50126)*;*

(24) „schválením bezpečnosti“ se rozumí stav přidělený změně navrhovatelem na základě zprávy o posouzení bezpečnosti, kterou předložil subjekt pro posuzování;

(25) „systémem“ se rozumí jakákoli část železničního systému, na které dochází ke změně;

(26) „oznámeným vnitrostátním předpisem“ se rozumí jakýkoli vnitrostátní předpis oznámený členskými státy podle směrnice Rady 96/48/ES[4], směrnice Evropského parlamentu a Rady 2001/16/ES[5] a směrnice 2004/49/ES a 2008/57/ES

[G 1] Další vysvětlení se nepovažuje za nutné.

čl. 4 Významné změny

čl. 4 odst. 1

Pokud v některém členském státě neexistuje oznámený vnitrostátní předpis pro určení, zda je změna významná či nikoli, navrhovatel posoudí možný dopad dané změny na bezpečnost železničního systému.

Pokud navrhovaná změna nemá žádný dopad na bezpečnost, nemusí se proces řízení rizik popsaný v článku 5 použít.

[G 1] Pokud neexistuje žádný oznámený vnitrostátní předpis, odpovědnost za rozhodnutí nese navrhovatel. Významnost změny je založena na odborném posouzení. Například, pokud je zamýšlená změna existujícího systému složitá, může být hodnocena jako významná, pokud

(4) *Úř. věst. L 235, 17.9.1996, s. 6.*

(5) *Úř. věst. L 110, 20.4.2001, s. 1.*

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

je vysoké riziko dopadu na existující funkce[6] systému, přestože změna jako taková nemusí nutně souviset do značné míry s bezpečností.

čl. 4 odst. 2

Pokud navrhovaná změna má dopad na bezpečnost, navrhovatel pomocí odborného posouzení rozhodne o významnosti změny na základě těchto kritérií:

(a) důsledek selhání: věrohodný nejhorší scénář v případě selhání posuzovaného systému s přihlédnutím k existenci bezpečnostních bariér mimo systém;

(b) nový prvek použitý při zavádění změny: to se týká jak toho, co je inovativní v železničním odvětví, tak i toho, co je nové pouze pro organizaci zavádějící změnu;

(c) složitost změny;

(d) sledování: nemožnost sledovat zavedenou změnu během celé doby životnosti systému a provést vhodné zásahy;

(e) vratnost: nemožnost navrátit systém do stavu před změnou;

(f) adicionalita: posouzení významnosti změny s přihlédnutím ke všem nedávným změnám posuzovaného systému souvisejícím s bezpečností, které nebyly posouzeny jako významné.

Navrhovatel uchovává odpovídající dokumentaci ke zdůvodnění svého rozhodnutí.

[G 1] **Příklady drobných změn:** Po uvedení systému do provozu by jednorázové zvýšení maximální rychlosti na trati o 5 km/h mohlo být považováno za nevýznamné. Pokud by však maximální rychlost na trati byla i nadále zvyšována po jednotlivých krocích vždy o 5 km/h, součet následných změn (hodnocených jednotlivě jako nevýznamné změny) by se mohl stát ve vztahu k původním požadavkům na bezpečnost systému významnou změnou.

[G 2] Aby bylo možné vyhodnotit, zda je soubor několika následných (nevýznamných) změn významný, pokud je bereme jako celek, musí být posouzena veškerá nebezpečí a související rizika spojená se všemi změnami. Soubor posuzovaných změn může být považován za nevýznamný, pokud je výsledné riziko obecně přijatelné.

[G 3] Práce agentury na problematice významných změn prokázala, že:

(a) není možné stanovit harmonizované mezní hodnoty nebo předpisy, ze kterých by mohlo vycházet rozhodování o významnosti příslušné změny, a
(b) není možné sestavit vyčerpávající seznam významných změn,
(c) rozhodnutí nemůže být platné pro všechny navrhovatele a pro všechny technické, provozní, organizační a okolní podmínky.

Je proto nezbytně nutné, aby odpovědnost za rozhodnutí v této věci byla ponechána na navrhovatelích, kteří podle čl. 4 odst. 3 směrnice o bezpečnosti železnic {Ref. 1}, nesou odpovědnost za bezpečné provozování jejich části železničního systému a usměrňování rizik s tím spojených.

[G 4] Jako vodítko pro navrhovatele je v oddílu C.2. přílohy C uveden příklad „hodnocení a uplatňování kritérií“.

---

(6) *Vzhledem k tomu, že funkce systému nejsou vždy nezávislé, změny některých funkcí mohou mít dopad také na jiné funkce systému, přestože by se mohlo zdát, že s příslušnými změnami přímo nesouvisejí.*

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 5] CSM nesmí být použita, pokud změna související s bezpečností není považována za významnou. To ovšem neznamená, že by navrhovatel neměl činit žádné kroky. Navrhovatel provádí určitý typ (předběžných) analýz rizik s cílem rozhodnout, zda je příslušná změna významná. Tyto analýzy rizik, stejně jako jakákoli zdůvodnění a argumentace, musí být zdokumentovány, aby vnitrostátní bezpečnostní orgán mohl provést audit. Hodnocení významnosti změny a rozhodnutí, že změna není významná, nesmí být předmětem nezávislého posouzení subjektem pro posuzování.

čl. 5 Proces řízení rizik

čl. 5 odst. 1

Proces řízení rizik popsaný v příloze I se použije:

(a) u významné změny popsané v článku 4 včetně uvedení strukturálních subsystémů uvedených v čl. 2 odst. 2 písm. b) do provozu;

(b) pokud se na toto nařízení vztahují TSI, jak jsou uvedeny v čl. 2 odst. 2 písm. a), za účelem stanovení procesu řízení rizik popsaného v příloze I.

[G 1] Další vysvětlení se nepovažuje za nutné.

čl. 5 odst. 2

Proces řízení rizik popsaný v příloze I uplatňuje navrhovatel.

[G 1] Další vysvětlení se nepovažuje za nutné.

čl. 5 odst. 3

Navrhovatel zajistí, aby rizika, způsobená dodavateli a poskytovateli služeb včetně jejich subdodavatelů, byla řízena. Za tímto účelem může navrhovatel požadovat, aby se dodavatelé a poskytovatelé služeb včetně svých subdodavatelů podíleli na procesu řízení rizik popsaném v příloze I.

[G 1] Další vysvětlení se nepovažuje za nutné.

čl. 6 Nezávislé posouzení

čl. 6 odst. 1

Nezávislé posouzení správného uplatňování procesu řízení rizik popsaného v příloze I a výsledků tohoto uplatňování provádí subjekt, který splňuje kritéria stanovená v příloze II. Není-li tento subjekt pro posuzování dosud určen právními předpisy Společenství nebo vnitrostátními předpisy, navrhovatel jmenuje vlastní subjekt pro posuzování, kterým může být jiná organizace nebo vnitřní oddělení.

[G 1] Požadovaná úroveň nezávislosti nezbytná pro subjekt pro posuzování závisí na úrovni bezpečnosti, která je požadována pro posuzovaný systém. Zatímco na harmonizaci právních

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

předpisů vztahujících se na tuto problematiku se doposud čeká, osvědčené postupy pro tuto oblast lze najít v normě IEC61508-1:2001 článek 8 nebo v § 5.3.9. normy EN 50 129 {Ref. 7}. Míra nezávislosti závisí na závažnosti důsledků nebezpečí spojeného s daným zařízením a novosti jeho výskytu. Oddíl § 9.7.2 v normě EN 50 126-2 a norma EN 50129 definují úroveň nezávislosti řídících systémů. V zásadě lze tuto definici použít také pro jiné systémy.

[G 2] ERA doposud pracuje na definování funkcí a odpovědnosti jednotlivých subjektů pro posuzování (NSA, NOBO a ISA) a také nezbytných rozhraní mezi nimi. V rámci tohoto vymezení bude stanoveno, kdo (pokud to je možné) mezi jednotlivými subjekty pro posuzování bude pověřen jakou činností a jakým způsobem ji bude provádět. V konečném důsledku to umožní definovat jak:

(a) kontrolovat, na základě důkazu, že procesy řízení rizik a posuzování rizik, na které se vztahují CSM, jsou správně uplatňovány a
(b) podporovat navrhovatele v jeho rozhodnutí přijmout významné změny v rámci posuzovaného systému.

čl. 6 odst. 2

Je nutno zamezit překrývání práce mezi posuzováním shody systému řízení bezpečnosti podle směrnice 2004/49/ES, posuzováním shody prováděným oznámeným subjektem nebo vnitrostátním orgánem podle směrnice 2008/57/ES a nezávislým posuzováním bezpečnosti prováděným subjektem pro posuzování podle tohoto nařízení.

[G 1] ERA předloží doplňující informace v souvislosti s definováním rolí a odpovědnosti subjektů pro posuzování.

čl. 6 odst. 3

Bezpečnostní orgán může vystupovat jako subjekt pro posuzování, pokud se významné změny týkají těchto případů:

(a) vozidlo potřebuje povolení k uvedení do provozu podle čl. 22 odst. 2 a čl. 24 odst. 2 směrnice 2008/57/ES;

(b) vozidlo potřebuje dodatečné povolení k uvedení do provozu podle čl. 23 odst. 5 a čl. 25 odst. 4 směrnice 2008/57/ES;

(c) osvědčení o bezpečnosti musí být aktualizováno z důvodu změny typu nebo prodloužení provozu podle čl. 10 odst. 5 směrnice 2004/49/ES;

(d) osvědčení o bezpečnosti musí být revidováno z důvodu významných změn v bezpečnostním regulačním rámci podle čl. 10 odst. 5 směrnice 2004/49/ES;

(e) schválení z hlediska bezpečnosti musí být aktualizováno z důvodu významných změn v infrastruktuře, signalizaci nebo dodávce energie nebo zásadách provozu a údržby podle čl. 11 odst. 2 směrnice 2004/49/ES;

(f) schválení z hlediska bezpečnosti musí být revidováno kvůli významným změnám v bezpečnostním regulačním rámci podle čl. 11 odst. 2 směrnice 2004/49/ES.

[G 1] Další vysvětlení se nepovažuje za nutné.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

čl. 6 odst. 4

V případě, že se významné změny týkají strukturálního subsystému, pro který je nutné povolení k uvedení do provozu podle čl. 15 odst. 1 nebo článku 20 směrnice 2008/57/ES, může bezpečnostní orgán vystupovat jako subjekt pro posuzování, pokud navrhovatel již tento úkol nezadal oznámenému subjektu v souladu s čl. 18 odst. 2 uvedené směrnice.

[G 1] Další vysvětlení se nepovažuje za nutné.

čl. 7 Zprávy o posouzení bezpečnosti

čl. 7 odst. 1

Subjekt pro posuzování předloží navrhovateli zprávu o posouzení bezpečnosti.

[G 1] Další vysvětlení se nepovažuje za nutné.

čl. 7 odst. 2

V případě uvedeném v čl. 5 odst. 1 písm. a) vnitrostátní bezpečnostní orgán zohlední zprávu o posouzení bezpečnosti v rozhodnutí o povolení k uvedení subsystémů a vozidel do provozu.

[G 1] Další vysvětlení se nepovažuje za nutné.

čl. 7 odst. 3

V případě uvedeném v čl. 5 odst. 1 písm. b) je nezávislé posouzení součástí úkolu oznámeného subjektu, není-li v TSI stanoveno jinak.
Pokud není nezávislé posouzení součástí úkolu oznámeného subjektu, zohlední zprávu o posouzení bezpečnosti oznámený subjekt pověřený vydáváním osvědčení o shodě nebo smluvní subjekt pověřený vydáváním prohlášení ES o ověření.

[G 1] Další vysvětlení se nepovažuje za nutné.

čl. 7 odst. 4

Pokud již systém nebo část systému byly přijaty na základě procesu řízení rizik stanoveném v tomto nařízení, výsledná zpráva o posouzení bezpečnosti nesmí být zpochybněna jiným subjektem pro posuzování, který je pověřen provedením nového posouzení téhož systému. Toto uznání je podmíněno prokázáním, že systém bude používán za stejných funkčních, provozních a environmentálních podmínek jako již schválený systém a že byla použita rovnocenná kritéria přijatelnosti rizik.

[G 1] Tato zásada vzájemného uznávání již byla přijata normami CENELEC: viz oddíl § 5.5.2 v normě EN 50 129 a oddíl § 5.9 v normě EN 50 126-2. V normách CENELEC je zásada vzájemného přijímání či vzájemného uznávání uplatňována navrhovateli nebo nezávislými posuzovateli bezpečnosti ve vztahu ke standardním produktům (výrobkům) a standardním

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

aplikacím[7] za předpokladu, že posuzování bezpečnosti a prokazování bezpečnosti je prováděno v souladu s požadavky norem CENELEC.

[G 2] Vzájemné uznávání musí být uplatňováno také pro uznávání nových nebo upravených systémů, pokud jsou postupy posuzování rizik a prokazování souladu systému s požadavky na bezpečnost prováděny podle ustanovení nařízení CSM {Ref. 3}.

čl. 8 Řízení usměrňování rizik / interní a externí audity

čl. 8 odst. 1

Železniční podniky a provozovatelé infrastruktury zahrnou audity používání CSM pro hodnocení a posuzování rizik do svého programu pravidelných auditů systému řízení bezpečnosti, jak je uvedeno v článku 9 směrnice 2004/49/ES.

[G 1] Další vysvětlení se nepovažuje za nutné.

čl. 8 odst. 2

V rámci úkolů stanovených v čl. 16 odst. 2 písm. e) směrnice 2004/49/ES vnitrostátní bezpečnostní orgán sleduje používání CSM pro hodnocení a posuzování rizik.

[G 1] Další vysvětlení se nepovažuje za nutné.

čl. 9 Zpětná vazba a technický pokrok

čl. 9 odst. 1

Každý provozovatel infrastruktury a každý železniční podnik ve své výroční zprávě o bezpečnosti uvedené v čl. 9 odst. 4 směrnice 2004/49/ES stručně informuje o svých zkušenostech s používáním CSM pro hodnocení a posuzování rizik. Zpráva musí také zahrnovat souhrn rozhodnutí týkajících se úrovně významnosti změn.

[G 1] Další vysvětlení se nepovažuje za nutné.

čl. 9 odst. 2

Každý vnitrostátní bezpečnostní orgán ve své výroční zprávě o bezpečnosti uvedené v článku 18 směrnice 2004/49/ES informuje o zkušenostech navrhovatelů s používáním CSM pro hodnocení a posuzování rizik, případně o svých vlastních zkušenostech.

---

(7) *Viz bod [G 5] v oddílu 1.1.5 a v poznámkách pod čarou [9] a [10] na straně 27 a také obr. 3 tohoto dokumentu, kde lze najít další vysvětlení ohledně termínů „standardní produkt a standardní aplikace“ a s nimi spojených zásad.*

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 1] Další vysvětlení se nepovažuje za nutné.

čl. 9 odst. 3

Evropská agentura pro železnice sleduje a shromažďuje zpětné informace o používání CSM pro hodnocení a posuzování rizik a popřípadě vydává Komisi doporučení za účelem jejího zdokonalení.

[G 1] Další vysvětlení se nepovažuje za nutné.

čl. 9 odst. 4

Evropská agentura pro železnice předá do 31. prosince 2011 Komisi zprávu, která bude obsahovat:

(a) analýzu zkušeností s používáním CSM pro hodnocení a posuzování rizik včetně případů, kdy byla CSM dobrovolně použita navrhovateli před příslušným dnem použitelnosti stanoveným v článku 10;
(b) analýzu zkušeností navrhovatelů týkajících se rozhodnutí o úrovni významnosti změn;
(c) analýzu případů, ve kterých byly použity kodexy správné praxe popsané v bodě 2.3.8 přílohy I;
(d) analýzu celkové účinnosti CSM pro hodnocení a posuzování rizik.

Bezpečnostní orgány pomáhají agentuře zjišťováním případů použití CSM pro hodnocení a posuzování rizik.

[G 1] Další vysvětlení se nepovažuje za nutné.

čl. 10 Vstup v platnost

čl. 10 odst. 1

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v Úředním věstníku Evropské Unie.

[G 1] Další vysvětlení se nepovažuje za nutné.

čl. 10 odst. 2

Toto nařízení se použije ode dne 1. července 2012.

Avšak ode dne 1. července 2010 se použije:

(a) na všechny významné technické změny týkající se vozidel, jak jsou vymezena v čl. 2 písm. c) směrnice 2008/57/ES;
(b) na všechny významné změny týkající se strukturálních subsystémů, pokud to vyžaduje čl. 15 odst. 1 směrnice 2008/57/ES nebo TSI.

[G 1] Další vysvětlení se nepovažuje za nutné.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

PŘÍLOHA I – VYSVĚTLENÍ PROCESU V NAŘÍZENÍ CSM

1. OBECNÉ ZÁSADY VZTAHUJÍCÍ SE NA PROCES ŘÍZENÍ RIZIK

1.1. Obecné zásady a povinnosti

1.1.1. Proces řízení rizik, na nějž se vztahuje toto nařízení, začíná vymezením posuzovaného systému a zahrnuje tyto činnosti:

(a) postup pro posuzování rizik, který určí nebezpečí, rizika, související bezpečnostní opatření a výsledné bezpečnostní požadavky, jež musí posuzovaný systém splňovat;
(b) prokázání shody systému se stanovenými bezpečnostními požadavky a;
(c) řízení všech zjištěných nebezpečí a souvisejících bezpečnostních opatření.

Tento proces řízení rizik se opakuje a je zobrazen ve schématu v dodatku. Proces končí tehdy, je-li prokázána shoda systému se všemi bezpečnostními požadavky, které jsou nezbytné k přijetí rizik spojených se zjištěným nebezpečím.

[G 1] Rámec řízení rizik pro CSM a související proces posuzování rizik jsou znázorněny na obr. 1. Pokud je to považováno za nezbytné, každý box nebo každá činnost na tomto vyobrazení jsou dále popsány v konkrétním oddílu tohoto dokumentu.

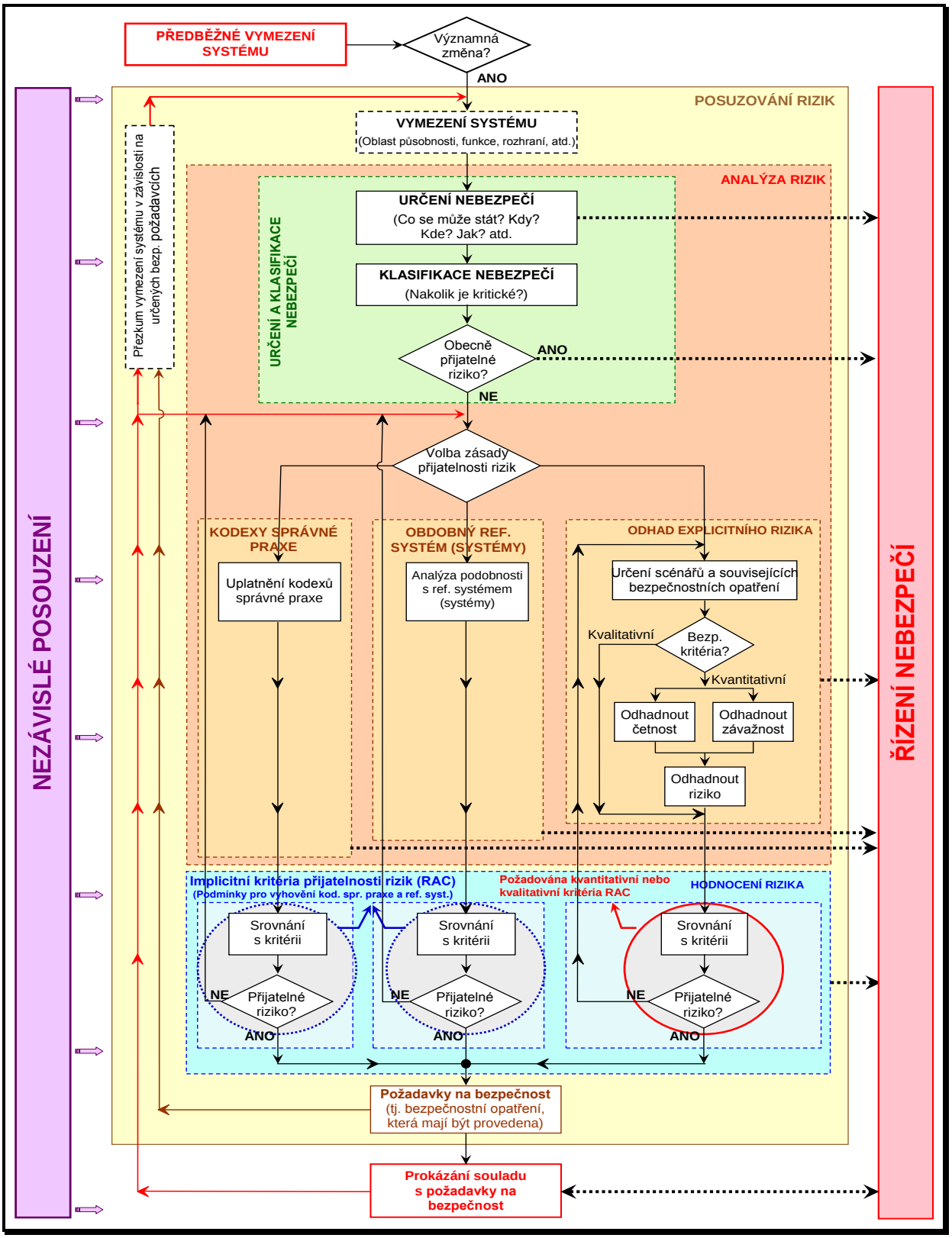
[G 2] Normy CENELEC doporučují, aby procesy řízení rizik a posuzování rizik byly popsány v plánu v oblasti bezpečnosti. Pokud to však pro daný projekt není vhodné, příslušný popis může být uveden v jakémkoli dalším příslušném dokumentu. Viz oddíl 1.1.6.

[G 3] Proces posuzování rizik začíná od předběžného vymezení systému. V průběhu realizace projektu je předběžné vymezení systému postupně aktualizováno a nahrazeno vymezením systému. Pokud předběžné vymezení systému neexistuje, pro posouzení rizika se použije formální vymezení systému. V tomto případě je však užitečné, aby se všechny subjekty dotčené významnou změnou na začátku projektu sešly, aby se dohodly na:

(a) celkových systémových zásadách, systémových funkcích atd. V zásadě by tyto aspekty mohly být popsány v předběžném vymezení systému,
(b) organizaci projektu,
(c) rozdělení rolí a odpovědnosti mezi jednotlivými subjekty, které jsou již do projektu zapojeny, včetně NSA, NOBO a ISA, pokud to připadá v úvahu.

Tato koordinace například v průběhu předběžného vymezení systému dává příležitost navrhovateli, subdodavatelům, NSA, NOBO a ISA, pokud to připadá v úvahu, dohodnout se již v rané fázi na kodexech správné praxe nebo referenčních systémech, které jsou přijatelné pro uplatnění v rámci daného projektu.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu



obr. 1: Rámec řízení rizik v nařízení CSM {Ref. 3}.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

1.1.2. Tento opakující se proces řízení rizik:

(a) zahrnuje příslušné činnosti k zabezpečení jakosti a provádí jej způsobilí pracovníci;
(b) je nezávisle posouzen jedním nebo více subjekty pro posuzování.

[G 1] Systém řízení bezpečnosti železničních podniků a provozovatelů infrastruktury (SMS) stanoví procesy a postupy, které:

(a) sledují bezpečnost systému v průběhu celého jeho životního cyklu (tj. v průběhu jeho provozu a údržby),
(b) zajišťují bezpečnou demontáž nebo nahrazení souvisejícího systému.

Tento proces není součástí postupů CSM v oblasti posuzování rizik.

[G 2] Pro provádění CSM je nezbytné, aby všechny zúčastněné strany byly kvalifikované (tj. měly příslušné dovednosti, znalosti a zkušenosti). Existuje neustálá potřeba zajišťování kvalifikace v organizacích jednotlivých subjektů v odvětví železniční dopravy:

(a) na provozovatele infrastruktury a železniční podniky se vztahuje jejich systém řízení bezpečnosti (SMS) podle přílohy III odst. 2 písm. e) směrnice o bezpečnosti železnic {Ref. 1},

(b) pokud jde o jiné subjekty, jejichž činnosti mohou mít dopad na bezpečnost železničního systému, přestože systém řízení bezpečnosti není povinný, obecně přinejmenším na úrovni projektu (viz bod [G 1] v oddílu 5.1), uplatňují proces řízení jakosti (QMP) a/nebo proces řízení bezpečnosti (SMP), který tomuto požadavku vyhovuje.

[G 3] V následujících oddílech normy CENELEC EN 50 126-1 {Ref. 8} jsou stanoveny pokyny k zajišťování kvalifikace:

(a) podle § 5.3.5. písm. b): *„všichni zaměstnanci s odpovědností v rámci „procesu řízení rizik“* musí být *„kvalifikovaní, aby tuto odpovědnost naplňovali“,*
(b) § 5.3.5. písm. d): požadavky na řízení rizik a posuzování rizik musí být *„zaváděny do podnikatelských procesů podporovaných systémem řízení jakosti (QMS) odpovídajícím požadavkům norem EN ISO 9001, EN ISO 9002 nebo EN ISO 9003 vhodným pro posuzovaný systém“*. Příklad aspektů usměrňovaných systémem řízení jakosti je uveden v oddílu § 5.2. normy EN 50 129 {Ref. 7}.

Tyto normy se vztahují na činnosti zabezpečení jakosti a také na kvalifikaci a školení zaměstnanců/osob, jež jsou potřebné pro podporu procesu, na který se vztahuje CSM.

[G 4] Proces posuzování rizik je často následně kontrolován subjektem pro posuzování, a to od samotného začátku projektu, pokud to však nevyžaduje vnitrostátní právo v příslušném členském státě, takové brzké zapojení subjektu pro posuzování není povinné, přestože se doporučuje. Stanovisko nezávislého subjektu pro posuzování by mohlo být užitečné před tím, než se přejde od jednoho kroku posuzování rizik k následujícímu. Viz článek 6, kde jsou uvedeny další podrobnosti o nezávislém posuzování.

1.1.3. Navrhovatel pověřený procesem řízení rizik musí podle tohoto nařízení vést záznam o nebezpečí podle oddílu 4.

[G 1] Další vysvětlení se nepovažuje za nutné.

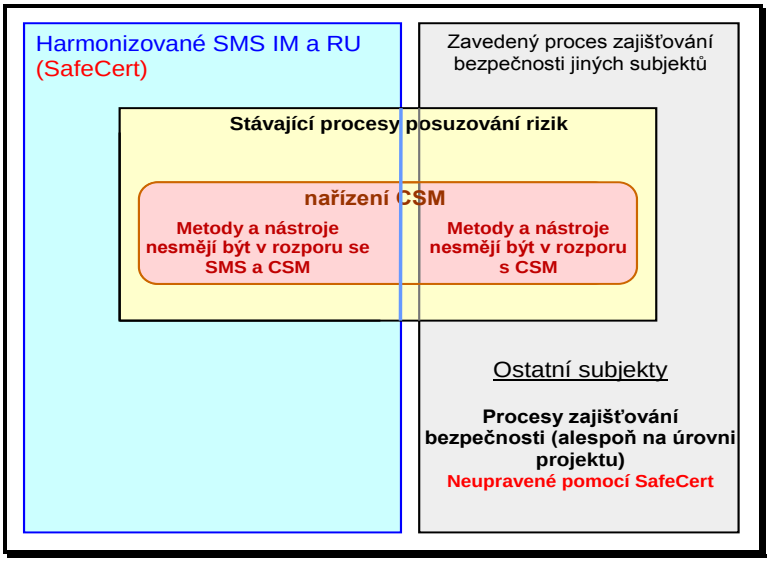
Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

1.1.4. Účastníci, kteří již zavedli metody nebo nástroje pro posuzování rizik, je mohou používat i nadále, jsou-li slučitelné s ustanoveními tohoto nařízení a s výhradou těchto podmínek:

(a) metody nebo nástroje pro posuzování rizik jsou popsány v systému řízení bezpečnosti, který byl schválen vnitrostátním bezpečnostním orgánem v souladu s čl. 10 odst. 2 písm. a) nebo čl. 11 odst. 1 písm. a) směrnice 2004/49/ES, nebo;

(b) metody nebo nástroje pro posuzování rizik jsou vyžadovány TSI nebo splňují veřejně dostupné uznané normy stanovené v oznámených vnitrostátních předpisech.

[G 1] obr. 2 znázorňuje vztah mezi CSM a „systémy řízení bezpečnosti a procesy posuzování rizik“.



obr. 2: Harmonizované SMS a CSM.

1.1.5. Aniž je dotčena občanskoprávní odpovědnost v souladu s právními požadavky jednotlivých členských států, za proces posuzování rizik odpovídá navrhovatel. Navrhovatel se souhlasem dotčených účastníků zejména rozhodne, kdo bude pověřen splněním bezpečnostních požadavků vyplývajících z posouzení rizik. Toto rozhodnutí závisí na druhu bezpečnostních opatření, která byla vybrána k usměrnění rizik na přijatelnou úroveň. Prokázání shody s bezpečnostními požadavky se provádí podle oddílu 3.

[G 1] Jedná-li se v případě navrhovatele o provozovatele infrastruktury nebo železniční podnik, může být někdy nezbytné zapojit do tohoto procesu jiné subjekty[8] (viz oddíl 1.2.1). V některých případech může provozovatel infrastruktury nebo železniční podnik zadat částečně nebo úplně činnosti posuzování rizik subdodavateli. Role a odpovědnost každého subjektu bývají obvykle dohodnuty mezi dotčenými subjekty v rané fázi projektu.

(8) *To je v souladu s přílohou A.4 normy CENELEC 50 129 {Ref. 7}.*

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 2] Je důležité poznamenat, že navrhovatel vždy zůstává odpovědný za uplatňování CSM, za přijetí rizika, a tím i za bezpečnost systému. V rámci této odpovědnosti je povinen zajistit:

(a) plnou spolupráci mezi zúčastněnými subjekty tak, aby byly poskytovány všechny nezbytné informace, a
(b) aby bylo jasné, kdo musí plnit konkrétní požadavky CSM (například provedení analýzy rizik nebo vedení záznamu o nebezpečí).

V případě, že mezi subjekty neexistuje shoda ohledně požadavků na bezpečnost, jež mají plnit, je možné se obrátit na NSA s dotazem na stanovisko. Odpovědnost za nalezení řešení ovšem nese navrhovatel a nelze ji přenést na NSA: viz také oddíl 0.2.2..

[G 3] V případě, že je určitý úkol zadán subdodavateli, subdodavatel není povinen mít vlastní bezpečnostní organizaci, pokud se nejedná o provozovatele infrastruktury nebo železniční podnik nebo zejména tehdy, je-li struktura/rozměr podniku subdodavatele malá nebo v případě, že jeho přínos k systému jako celku je omezený. Odpovědnost za řízení rizik, včetně činností posuzování rizik a řízení nebezpečí může zůstat na organizaci na vyšší úrovni (tj. na zákazníkovi subdodavatele). Subdodavatel je však vždy odpovědný za poskytování správných informací týkajících se jeho činností a nezbytných pro organizaci na vyšší úrovni za účelem vytváření dokumentace řízení rizik.
Spolupracující organizace se mohou také dohodnout na vytvoření společné bezpečnostní organizace například za účelem optimalizace nákladů. V tomto případě bude bezpečnostní činnosti všech zúčastněných organizací řídit pouze jedna organizace. Odpovědnost za přesnost informací (tj. nebezpečí, rizika a bezpečnostní opatření) a také řízení procesu provádění bezpečnostních opatření i nadále nese organizace, která je pověřena usměrňováním nebezpečí, s nimiž jsou tato bezpečnostní opatření spojena.

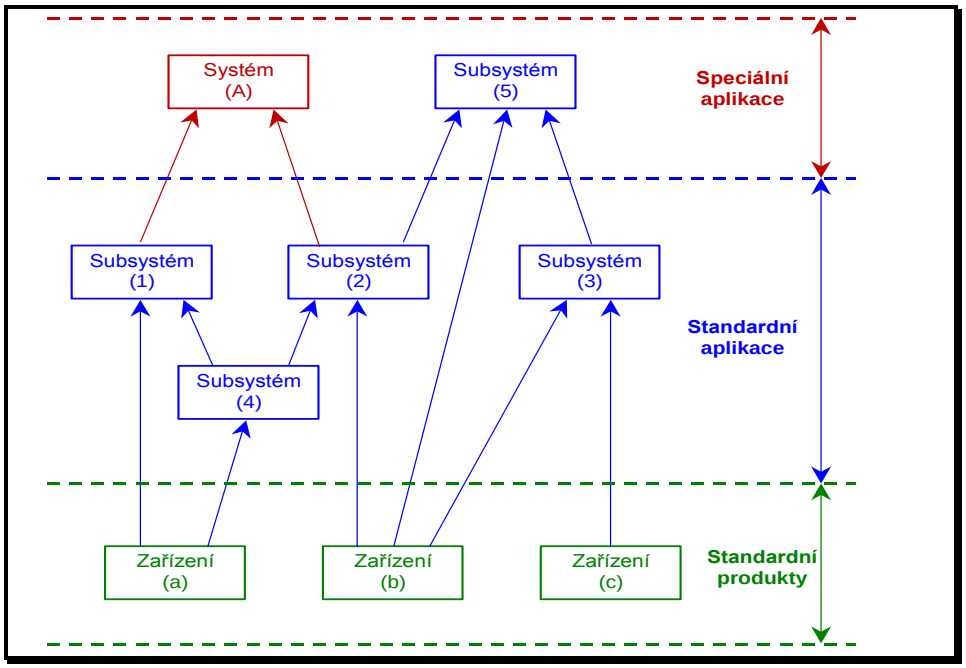
[G 4] Navrhovatel obvykle stanoví „úrovně bezpečnosti“ a „požadavky na bezpečnost“ přiřazené subjektům podílejícím se na projektu a jednotlivým subsystémům a zařízením těchto subjektů:

(a) ve smlouvách mezi navrhovatelem a příslušnými subjekty (subdodavateli),
(b) v plánu v oblasti bezpečnosti nebo jakémkoli příslušném dokumentu se stejným účelem, s popisem celkové organizace projektu a odpovědnosti každého subjektu, včetně odpovědnosti navrhovatele: viz oddíl 1.1.6,
(c) v záznamu o nebezpečí (záznamech o nebezpečí) vedeném navrhovatelem: viz oddíl 4.1.1.

Toto přiřazení „úrovní bezpečnosti“ a „požadavků na bezpečnost“ až na úroveň základních subsystémů a zařízení, a tudíž příslušným subjektům, včetně samotného navrhovatele, může být opětovně definováno/rozšířeno v průběhu „fáze prokázání shody systému s požadavky na bezpečnost“: viz obr. 1. Ve srovnání s V-cyklem norem CENELEC (viz oddíl 2.1.1 a obr. 5 na straně 32) tato činnost odpovídá fázi 5 zabývající se „přiřazením požadavků na systém“ až na úroveň jednotlivých subsystémů a prvků.

[G 5] čl. 5 odst. 2 umožňuje, aby i jiné subjekty než železniční podniky a provozovatelé infrastruktury přejímaly celkovou odpovědnost za soulad s CSM v závislosti na jejich příslušných potřebách. Například v případě standardních produktů nebo standardních aplikací(9) může výrobce provést posuzování rizik na základě „vymezení standardního systému“ s cílem určit úrovně bezpečnosti a požadavky na bezpečnost, které mají splňovat standardní produkty a standardní aplikace.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu



obr. 3: Příklady vztahů vzájemné závislosti mezi doklady bezpečnosti (převzato z obrázku 9 v normě EN 50 129).

[G 6] Normy CENELEC doporučují, aby výrobce poskytoval zdokumentované důkazy v rámci procesu posuzování rizik v dokladech bezpečnosti a záznamech o nebezpečí standardních produktů (či standardních aplikací)[(9)]. Tyto doklady bezpečnosti a záznamy o nebezpečí mají obsahovat všechny předpoklady[(10)] a určená "omezení použití" (tj. podmínky použití

---

(9) *Termíny "standardní aplikace" a "doklady bezpečnosti standardního výrobku" jsou přejaty z norem CENELEC, v rámci kterých lze rozlišovat tři různé kategorie dokladů bezpečnosti (viz obr. 3):*

(a) ***doklad bezpečnosti standardního produktu*** *(nezávislého na aplikaci). Standardní produkt lze opětovně použít pro různé nezávislé aplikace,*

(b) ***doklad bezpečnosti standardní aplikace*** *(pro určitou kategorii aplikace). Standardní aplikaci lze opětovně použít pro určitou kategorii/určitý typ aplikace se společnými funkcemi,*

(c) ***doklad bezpečnosti speciální aplikace*** *(pro speciální aplikaci). Speciální aplikace se používá pouze pro jedno konkrétní zařízení.*

Podrobnější informace o jejich vzájemné závislosti viz oddíl § 9.4. a obr. 9.1 pokynů CENELEC 50 126-2 {Ref. 9}.

(10) *Tyto předpoklady a omezení použití určují hranice a platnost „posuzování bezpečnosti“ a „analýz bezpečnosti“ týkajících se souvisejících dokladů bezpečnosti standardních produktů a standardních aplikací. Pokud posuzovaná konkrétní aplikace těmto požadavkům nevyhovuje, je nezbytné aktualizovat nebo nahradit příslušná „posouzení bezpečnosti“ a příslušné „analýzy bezpečnosti“ (např. příčinné analýzy) novými.*

> *To je v souladu s následující obecnou bezpečnostní zásadou: „Kdykoli je určitá konstrukce systému (subsystému) založena na standardních aplikacích a standardních produktech, musí být prokázáno, že konkrétní systém (subystém) vyhovuje všem předpokladům a omezením použití (v rámci norem CENELEC nazývaným podmínkami použití souvisejícími s bezpečností), které jsou zaznamenány do příslušných dokladů bezpečnosti standardních aplikací a standardních produktů (viz obr. 3).“*

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

související s bezpečností) vztahující se na související standardní produkty (nebo standardní aplikace). Z tohoto důvodu, kdykoli jsou používány standardní produkt a standardní aplikace v provozu konkrétní aplikace, musí být u každé konkrétní aplikace prokázáno dodržování všech těchto předpokladů(10) a „omezení použití“ (nebo podmínek použití souvisejících s bezpečností).

1.1.6. Prvním krokem v procesu řízení rizik je určit v dokumentu, který vypracuje navrhovatel, úkoly jednotlivých účastníků a rovněž jejich činnosti v oblasti řízení rizik. Navrhovatel koordinuje úzkou spolupráci mezi jednotlivými dotčenými účastníky podle jejich příslušných úkolů za účelem řízení nebezpečí a zajištění souvisejících bezpečnostních opatření.

[G 1] Velice často nastává situace, že pokud není na začátku projektu smluvně sjednáno jinak, je pro každý projekt zaveden doklad, který popisuje činnosti řízení rizik. Příslušný doklad je aktualizován a přezkoumán pokaždé, když jsou prováděny významné úpravy původního systému.

[G 2] V tomto dokladu je stanovena organizační struktura, odpovědnost přiřazená zaměstnancům, procesy, postupy a činnosti, které společně zajišťují, aby posuzovaný systém vyhovoval určeným úrovním bezpečnosti a požadavkům na bezpečnost. Doklad musí být v souladu s CSM, protože slouží jako podklad a vodítko pro subjekt pro posuzování. Normy CENELEC doporučují, aby tento typ informací byl součástí plánu v oblasti bezpečnosti nebo jiného dokladu, který obsahuje část věnovanou těmto tématům.

[G 3] Plán navrhovatele v oblasti bezpečnosti nebo jakýkoli jiný příslušný dokument zejména charakterizuje celkovou organizaci projektu. Popisuje rozdělení rolí a odpovědnosti mezi zúčastněné subjekty. Podrobné informace lze vyhledat v plánech voblasti bezpečnosti nebo bezpečnostních organizacích různých zúčastněných subjektů. Rozdělení odpovědnosti mezi jednotlivé subjekty bývá obvykle projednáno a dohodnuto v průběhu případného předběžného vymezení předběžného systému (tj. na začátku projektu).

[G 4] Plán v oblasti bezpečnosti je flexibilní dokument, který je aktualizován, kdykoli je to potřebné v době trvání projektu.

[G 5] Další podrobnosti lze najít v normě EN 50 126-1 {Ref. 8} a souvisejících pokynech k normě 50 126-2 {Ref. 9}, kterými se stanoví obsah plánu v oblasti bezpečnosti.

Continuation of the footnote

Pokud pro určitou aplikaci vyhovění některým předpokladům a omezení použití nelze dosáhnout na úrovni subsystému (např. v případě požadavků na provozní bezpečnost), příslušné předpoklady a omezení použití lze přenést na vyšší úroveň (tj. obvykle na úroveň systému). Tyto předpoklady a omezení použití jsou pak jasně určeny v „dokladu bezpečnosti konkrétní aplikace“ souvisejícího subsystému. U těchto příkladů závislosti je nezbytně nutné zajistit, aby podmínky použití související s bezpečností každého dokladu bezpečnosti byly splněny u dokladů bezpečnosti na vyšší úrovni nebo přeneseny do podmínek použití souvisejících s bezpečností dokladu bezpečnosti na nejvyšší úrovni (tj dokladu bezpečnosti systému).

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

1.1.7. Za vyhodnocení správného uplatňování procesu řízení rizik popsaného v tomto nařízení odpovídá subjekt pro posuzování.

[G 1] Další vysvětlení se nepovažuje za nutné.

1.2. Řízení rozhraní

1.2.1. Pro každé rozhraní, které je důležité pro posuzovaný systém, a aniž jsou dotčeny specifikace rozhraní stanovené v příslušných TSI, dotčení účastníci ze železničního odvětví vzájemně spolupracují s cílem určit a společně řídit nebezpečí a zajistit související bezpečnostní opatření, která jsou nezbytná pro tato rozhraní. Řízení sdílených rizik na rozhraních koordinuje navrhovatel.

[G 1] Pokud například železniční podnik z provozních důvodů potřebuje, aby provozovatel infrastruktury provedl určené změny infrastruktury podle požadavků stanovených v příloze III bodu 2 písm. g) směrnice o bezpečnosti železnic {Ref. 1}, železniční podnik sleduje tuto práci jako celek s cílem zajistit, aby plánované změny byly provedeny správně. Tato řídící funkce železničního podniku však nezbavuje příslušného provozovatele infrastruktury povinnosti informovat jiné železniční podniky, pokud jsou také dotčeny příslušnou změnou infrastruktury. Provozovatel infrastruktury může být dokonce povinen provést posuzování rizik podle CSM, pokud je z jeho hlediska změna významná.

[G 2] Přenesení odpovědnosti mezi různými subjekty je možné a za určitých okolností dokonce nezbytné. Pokud se však na určitém systému podílí několik subjektů, velice často je jeden z nich pověřen odpovědností za systém jako celek. Vždy existují vztahy vzájemné závislosti mezi jednotlivými subsystémy a operacemi, jejichž určení vyžaduje zvláštní úsilí. Je proto nezbytné, aby někdo převzal celkovou odpovědnost za analýzy bezpečnosti a získal také neomezený přístup k veškeré příslušné dokumentaci. Je zřejmé, že navrhovatel, který má v úmyslu zavést významnou změnu, obecně nese celkovou odpovědnost za systematičnost a úplnost procesu posuzování rizik.

[G 3] Hlavní kritéria, na kterých je třeba se dohodnout ve věci řízení rozhraní mezi dotčenými subjekty, jsou:

(a) řídící funkce, již obvykle vykonává navrhovatel, který má v úmyslu zavést významnou změnu,
(b) požadované vstupy,
(c) metody určování nebezpečí a posuzování rizik,
(d) požadované zúčastněné subjekty s potřebnou kvalifikací (tj. kombinací znalostí, dovedností a praktické zkušenosti v daném oboru – viz také definice „kvalifikace zaměstnanců“ v bodě [G 2] písm. b) článku 3 v {Ref. 4}),
(e) očekávané výstupy.

Tato kritéria jsou popsána v plánech v oblasti bezpečnosti (nebo v jakýchkoli jiných příslušných dokumentech) společností, které se zabývají příslušnými rozhraními.

[G 4] Příklady rozhraní jsou uvedeny v oddílu C.3. přílohy C, společně s příkladem uplatňování těchto hlavních kritérií pro řízení rozhraní mezi výrobcem vlaků a provozovatelem infrastruktury nebo železničním podnikem.

[G 5] Součástí řízení rozhraní je také posuzování rizik, která by mohla vzniknout na rozhraních s lidskou obsluhou (užívaných v průběhu provozu a údržby), za účelem navržení těchto rozhraní.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

1.2.2. Pokud účastník zjistí, že ke splnění určitého bezpečnostního požadavku je nutné bezpečnostní opatření, které nemůže provést sám, převede po dohodě s jiným účastníkem řízení souvisejícího nebezpečí na tohoto účastníka, a to postupem popsaným v oddíle 4.

[G 1] Proces přenosu nebezpečí a souvisejících bezpečnostních opatření mezi subjekty je použitelný také na nižších úrovních V-cyklu norem CENELEC na obr. 5 na straně 32. Lze jej použít, kdykoli je nezbytné provést výměnu těchto informací například mezi subjektem a jeho dodavateli. Rozdíl u stejného procesu na úrovni systému spočívá v tom, že navrhovatel nemusí být informován o všech přenosech nebezpečí a souvisejících bezpečnostních opatřeních na úrovni subsystému. Navrhovatel je informován pouze v případě, že se přenášená nebezpečí a související bezpečnostní opatření týkají rozhraní na vysoké úrovni (tj. pokud mají dopad na rozhraní s navrhovatelem).

1.2.3. V případě posuzovaného systému odpovídá kterýkoli účastník, který zjistí, že bezpečnostní opatření není v souladu nebo není přiměřené, za informování navrhovatele, jenž zase informuje účastníka provádějícího bezpečnostní opatření.

[G 1] Systém řízení bezpečnosti železničních podniků a provozovatelů infrastruktury (SMS) se vztahuje na mechanismy a postupy, jejichž účelem je zajistit správné řízení případů nedodržování bezpečnostních opatření nebo jejich nepřiměřenosti. Tyto mechanismy a postupy proto nejsou součástí CSM.

[G 2] Obdobně, pokud jde o mechanismy a postupy[(11)], které mají zavést jiné subjekty[(12)], aby zajistily správné řízení případů nedodržování bezpečnostních opatření nebo jejich nepřiměřenosti a aby byla tato bezpečnostní opatření v případě potřeby přenesena na příslušné subjekty na základě dohody mezi příslušnými subjekty na začátku projektu a podrobně uvedena v jejich plánu v oblasti bezpečnosti: viz oddíl 0.2.

1.2.4. Účastník provádějící bezpečnostní opatření poté informuje všechny účastníky, jichž se týká problém v rámci posuzovaného systému, nebo do té míry, do jaké je to účastníkovi známo, v rámci jiných existujících systémů používajících stejné bezpečnostní opatření.

[G 1] To umožní řídit případné nedodržování bezpečnostního opatření nebo jeho nepřiměřenost v rámci posuzovaného systému nebo v rámci obdobných systémů, které používají totéž opatření.

(11) *V zásadě jsou tyto mechanismy a postupy upraveny procesem řízení jakosti a/nebo procesem zajišťování bezpečnosti těchto subjektů stanoveným alespoň na úrovni projektu (viz také obr. 2).*

(12) *Termín „ostatní subjekty“ označuje všechny dotčené subjekty jiné než provozovatelé infrastruktury a železniční podniky.*

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

1.2.5.	*Nemohou-li dva či více účastníků dospět k dohodě, je odpovědností navrhovatele nalézt přiměřené řešení.*

[G 1] Další vysvětlení se nepovažuje za nutné.

1.2.6.	*Nemůže-li nějaký účastník splnit požadavek v oznámeném vnitrostátním předpise, navrhovatel si vyžádá radu od odpovídajícího příslušného orgánu.*

[G 1] Další vysvětlení se nepovažuje za nutné.

1.2.7.	*Nezávisle na vymezení posuzovaného systému musí navrhovatel zajistit, aby se řízení rizik vztahovalo na samotný systém i na jeho začlenění do železničního systému jako celku.*

[G 1] Další vysvětlení se nepovažuje za nutné.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2. POPIS POSTUPU PRO POSUZOVÁNÍ RIZIK

2.1. Obecný popis – spojitosti mezi postupem pro posuzování rizik CSM a V-cyklem norem CENELEC

2.1.1. Postup pro posuzování rizik je celkový opakující se postup, který zahrnuje:

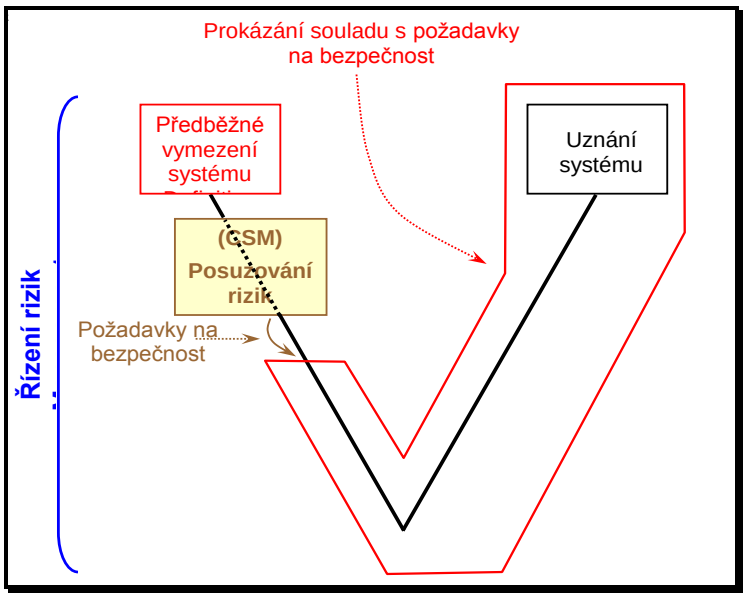
(a) vymezení systému;
(b) t vymezení systému;
(c) vyhodnocení rizik.

Postup pro posuzování rizik je propojen s řízením nebezpečí podle bodu 4.1.

[G 1] Proces řízení rizik, na který se vztahuje CSM, může být znázorněn v rámci V-cyklu, který začíná (předběžným) vymezením systému a končí uznáním systému: viz obr. 4. Tento zjednodušený V-cyklus lze následně promítnout do běžného V-cyklu normy EN 50 126-1 {Ref. 8} na obrázku 10. S cílem ukázat spojitost s procesem řízení rizik CSM znázorněným na obr. 1, je V-cyklus norem CENELEC uvedený na obrázku 10 připomenut na obr. 5:

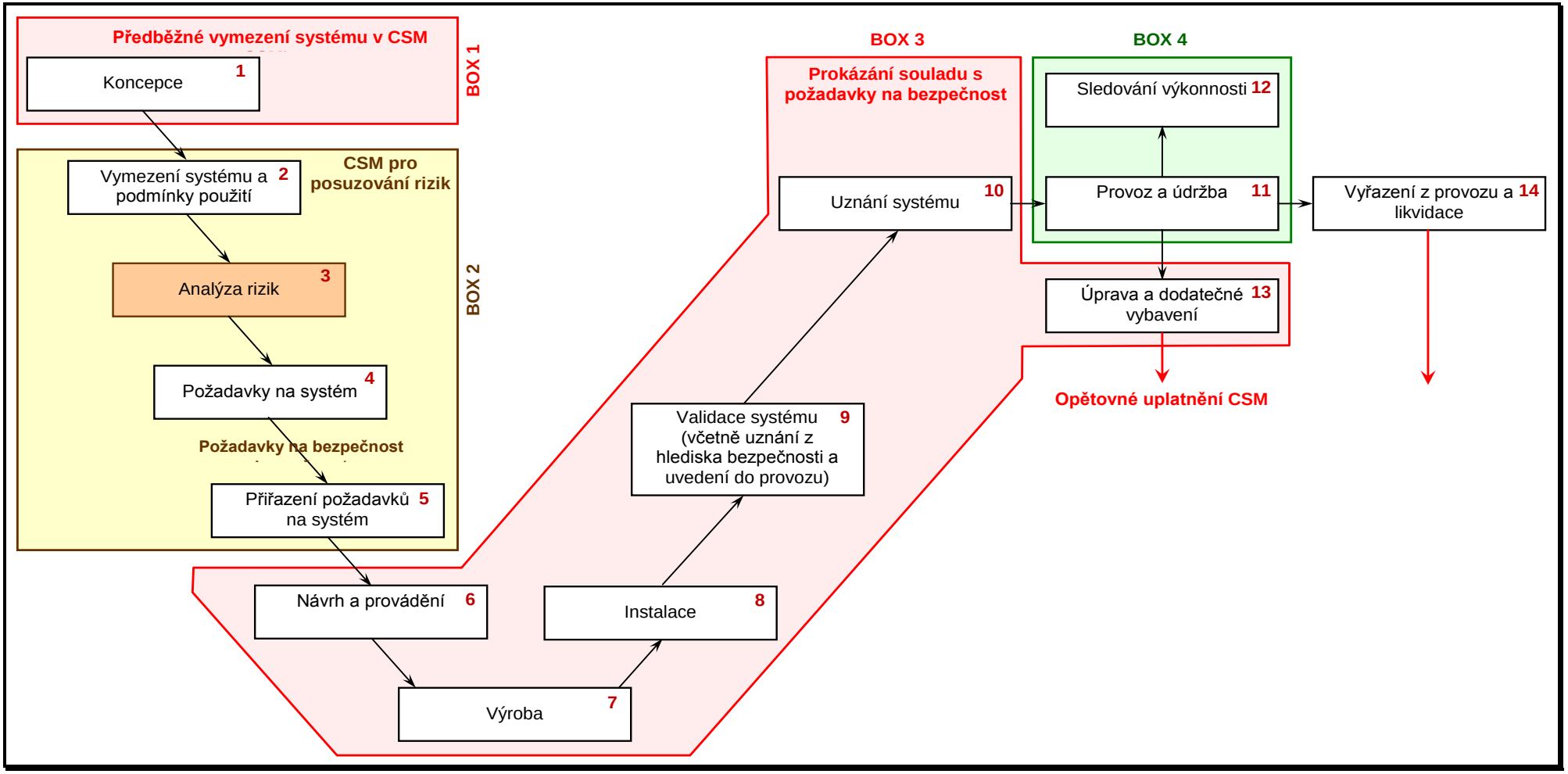
(a) „předběžné vymezení systému“ CSM na obr. 1 odpovídá fázi 1 ve V-cyklu norem CENELEC, tj. definici „koncepce“ systému (viz rámeček 1 na obr. 5),
(b) „posuzování rizik“ CSM na obr. 1 obsahuje tyto fáze V-cyklu norem CENELEC (viz rámeček 2 na obr. 5):

(1) fáze 2 na obr. 5: „vymezení systému a podmínek použití“;
(2) fáze 3 na obr. 5: „analýza rizik“;
(3) fáze 4 na obr. 5: „požadavky na systém“;
(4) fáze 5 na obr. 5: „přiřazení požadavků na systém“ až na úroveň odlišných subsystémů a prvků.



obr. 4: Zjednodušený V-cyklus normy EN 50 126 z obrázku 10.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu



obr. 5: Obrázek 10 V-cyklus normy EN 50 126 (životní cyklus systému CENELEC).

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 2] Výstupy postupu pro posuzování rizik v CSM jsou (po opakování – viz obr. 1):

(a) „vymezení systému“ aktualizované prostřednictvím „požadavků na bezpečnost“, které vyplynou z činností „analýzy rizik“ a „hodnocení rizik“ (viz oddíl 2.1.6),
(b) „přiřazení požadavků na systém“ až na úroveň jednotlivých subsystémů a prvků (fáze 5 na obr. 5),
(c) „záznam o nebezpečí“, který eviduje:

(1) všechna určená nebezpečí a související bezpečnostní opatření;
(2) výsledné požadavky na bezpečnost;
(3) předpoklady, které byly vzaty v úvahu pro systém, a které určují limity a platnost posuzování rizika (viz písm. (g) v oddílu 2.1.2);

(d) a obecně veškeré důkazy o uplatňování CSM: viz oddíl 5.

Tyto výstupy posuzování rizik CSM odpovídají výstupům souvisejícím s bezpečností fáze 4 V-cyklu norem CENELEC, tj. specifikaci systémových požadavků na obr. 5.

[G 3] Vymezení systému aktualizované o výsledky procesu posuzování rizik a záznamu o nebezpečí představuje vstupy, na jejichž základě je systém navržen a přijat. „Prokázání shody systému s bezpečnostními požadavky“ v CSM odpovídá následujícím fázím V-cyklu norem CENELEC (viz rámeček 3 na obr. 5):

(a) fáze 6 na obr. 5: „návrh a provádění“,
(b) fáze 7 na obr. 5: „výroba“,
(c) fáze 8 na obr. 5: „instalace“,
(d) fáze 9 na obr. 5: „validace systému (včetně uznání z hlediska bezpečnosti)“,
(e) fáze 10 na obr. 5: „uznání systému“.

[G 4] Prokázání shody systému s požadavky na bezpečnost závisí na tom, zda je příslušná významná změna technického, provozního nebo organizačního charakteru. Jednotlivé kroky ve V-cyklu norem CENELEC znázorněné na obr. 5 nemusí být vhodné pro všechny významné změny daného typu. V-cyklus na obr. 5 je třeba chápat v tomto smyslu a je třeba jej uplatňovat na základě přiměřeného posouzení vhodnosti pro každé konkrétní použití (např. pro provozní a organizační změny neexistuje žádná fáze výroby).

[G 5] To znamená, že „prokázání shody systému s bezpečnostními požadavky“ v CSM nezahrnuje pouze činnosti „ověření a validace“ prostřednictvím zkoušek nebo simulací. V praxi se vztahuje na všechny fáze „od 6 do 10“ (viz výše uvedený výčet a obr. 5) ve V-cyklu norem CENELEC. Součástí tohoto procesu jsou činnosti návrhu (konstrukce), výroby, instalace, ověření a validace a také související činnosti RAMS (prokázání bezpečnosti, bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti) a uznání systému.

[G 6] V průběhu „prokázání shody systému s bezpečnostními požadavky“ je obecnou zásadou zaměřit posuzování rizik pouze na funkce související s bezpečností a na rozhraní systému. To znamená, že kdykoli jsou požadovány činnosti posuzování rizik a posuzování bezpečnosti v rámci jedné z fází V-cyklu norem CENELEC na obr. 5, jsou zaměřeny na:

(a) funkce a rozhraní související s bezpečností,
(b) subsystémy a/nebo prvky podílející se na dosažení funkcí souvisejících s bezpečností a/nebo rozhraní posuzovaná v průběhu činností posuzování rizik na vyšší úrovni.

[G 7] Ze srovnání s tradičním V-cyklem norem CENELEC na obr. 5 tedy vyplývá, že:

(a) CSM se vztahují na fáze „1 až 10“ a „13“ tohoto V-cyklu. Jejich součástí je soubor činností požadovaných pro uznání posuzovaného systému;

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(b) CSM se nevztahují na fáze „11“, „12“ a „14“ životního cyklu systému:

(1) fáze „11“ se týká „provozu a údržby“ a fáze „12“ „sledování výkonnosti“ systému po jeho přijetí na základě CSM. Na tyto dvě fáze se vztahuje systém řízení bezpečnosti (SMS) pro železniční podniky a provozovatele infrastruktury – (viz rámeček 4 na obr. 5). Pokud se ovšem v průběhu provozu, údržby nebo sledování výkonů systému ukáže jako nezbytné systém upravit a dodatečně vybavit (fáze 13 na obr. 5), zatímco je již v provozu, CSM se použijí opět na nově požadované změny v souladu s čl. 2. Z tohoto důvodu, pokud je změna významná:

(i) jsou procesy řízení rizik a posuzování rizik v CSM aplikovány na tyto nové změny,
(ii) tyto nové změny musí být přijaty v souladu s čl. 6,

(2) „vyřazení z provozu a likvidace“ systému, který je již v provozu (fáze 14), by mohlo být také kvalifikováno jako významná změna a CSM by proto mohly být opět uplatněny v souladu s čl. 2 pro fázi 14 na obr. 5.

Podrobnější informace o rozsahu každé fáze nebo činnosti ve V-cyklu norem CENELEC znázorněných na obr. 5, viz oddíl § 6 normy EN 50 126-1 {Ref. 8}.

2.1.2. Vymezení systému by se mělo zabývat nejméně těmito otázkami:

(a) cíl systému, např. zamýšlený účel;
(b) popřípadě funkce a prvky systému (včetně například lidských, technických a provozních prvků);
(c) hranice systému, včetně ostatních vzájemně se ovlivňujících systémů;
(d) fyzická rozhraní (tj. vzájemně se ovlivňující systémy) a funkční rozhraní (tj. funkční vstup a výstup);
(e) prostředí systému (např. proudění energie a tepla, nárazy, vibrace, elektromagnetické rušení, použití v provozu);
(f) stávající bezpečnostní opatření a po iteraci určení bezpečnostních požadavků zjištěných při postupu pro posuzování rizik;
(g) předpoklady, které stanoví meze pro posouzení rizik.

[G 1] Další vysvětlení se nepovažuje za nutné.

2.1.3. Identifikace nebezpečí se u vymezeného systému provádí podle bodu 2.2.

[G 1] Další vysvětlení se nepovažuje za nutné.

2.1.4. Přijatelnost rizik posuzovaného systému se vyhodnotí pomocí jedné či více z těchto zásad přijatelnosti rizik:

(a) používání kodexů správné praxe (bod 2.3);
(b) porovnání s obdobnými systémy (bod 2.4);
(c) jednoznačný odhad rizik (bod 2.5).

V souladu s obecnou zásadou uvedenou v bodě 1.1.5 subjekt pro posuzování nesmí navrhovateli nařídit, aby použil zásadu přijetí rizika.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 1] Obecně navrhovatel rozhodne, jaká zásada přijatelnosti rizik je nejvhodnější pro kontrolu určených nebezpečí na základě konkrétních požadavků daného projektu a také na základě zkušenosti navrhovatele se třemi zásadami.

[G 2] Není vždy možné hodnotit přijatelnost rizika na úrovni systému prostřednictvím uplatnění pouze jedné ze tří zásad přijatelnosti rizik. Přijatelnost rizik bude často založena na kombinaci těchto zásad. Pokud musí být v případě významného nebezpečí uplatněna více než jedna zásada přijatelnosti rizik pro kontrolu souvisejícího rizika, související nebezpečí musí být rozděleno do dílčích nebezpečí, tak aby každé jednotlivé dílčí nebezpečí bylo přiměřeně usměrňováno pouze jednou zásadou přijatelnosti rizik.

[G 3] Rozhodnutí o usměrňování nebezpečí prostřednictvím zásady přijatelnosti rizik musí zohlednit příslušné nebezpečí a příčiny nebezpečí, které již byly určeny v průběhu fáze určení rizika. Pokud tedy dvě odlišné a nezávislé příčiny souvisejí s týmž nebezpečím, toto nebezpečí musí být dále členěno na dvě různá dílčí nebezpečí. Každé dílčí nebezpečí pak bude usměrňováno jedinou zásadou přijatelnosti rizik. Příslušná dvě dílčí nebezpečí musí být evidována a vedena v záznamu o nebezpečí. Pokud je například nebezpečí způsobeno konstrukční vadou, lze je zvládat uplatněním kodexu správné praxe, zatímco v případě, že příčinou nebezpečí je chyba v údržbě, samotný kodex správné praxe nemusí být dostatečný, v takovém případě je nezbytné uplatnit jinou zásadu přijatelnosti rizik.

[G 4] Snížení rizika na přijatelnou úroveň si může vyžádat několik opakování procesu, od fáze analýzy rizik až po fázi hodnocení rizika, dokud nejsou určena vhodná bezpečnostní opatření.

[G 5] Současné zbytkové riziko, které vyplynulo ze zkušenosti v terénu se stávajícími systémy a systémy založenými na uplatňování kodexů správné praxe, je považováno za přijatelné. Riziko vyplývající z jednoznačného odhadu rizika je založeno na odborném posouzení a na jednotlivých předpokladech, které odborník přijme v průběhu analýz, nebo vychází z databází souvisejících s nehodou či z provozní zkušenosti. Zbytkové riziko vyplývající z jednoznačného odhadu rizika nelze proto potvrdit okamžitě po návratu z terénu. Prokazování tohoto typu vyžaduje určitý čas pro provoz a sledování souvisejícího systému (systémů) a získání dostatečně reprezentativní zkušenosti (zkušeností s ním). Obecně má uplatňování kodexů správné praxe a srovnání s obdobnými referenčními systémy tu výhodu, že nevyžaduje stanovení zbytečně přísných požadavků na bezpečnost, které mohou být důsledkem nadměrně konzervativních (bezpečnostních) předpokladů v jednoznačných odhadech rizika. Může ovšem nastat situace, že některé požadavky na bezpečnost z kodexů správné praxe nebo obdobných referenčních systémů nemusí být v případě posuzovaného systému splněny. V takovém případě by uplatnění jednoznačného odhadu rizika mělo tu výhodu, že by zamezilo zbytečně komplikované konstrukci posuzovaného systému a umožnilo by rentabilnější konstrukci, která doposud nebyla vyzkoušena.

[G 6] Pokud určená nebezpečí a související riziko (rizika) posuzovaného systému nelze usměrňovat uplatněním kodexů správné praxe nebo obdobných referenčních systémů, je proveden jednoznačný odhad rizika na základě kvantitativních nebo kvalitativních analýz nebezpečných událostí. Tato situace vzniká v případě, že posuzovaný systém je zcela nový (nebo je jeho konstrukce inovační) nebo v případě, že se tento systém odchyluje od kodexu správné praxe nebo referenčního systému. Na základě jednoznačného odhadu rizika je následně provedeno hodnocení, zda je riziko přijatelné (tj. další analýza není potřebná), nebo zda jsou potřebná doplňující bezpečnostní opatření, která by riziko dále omezila.

[G 7] Pokyny týkající se omezení rizik a přijatelnosti rizik lze najít také v oddílu § 8. pokynů k normě EN 50 126-2 {Ref. 9}.

[G 8] Použitou zásadu přijatelnosti rizik a její uplatňování musí zhodnotit subjekt pro posuzování.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.1.5. Navrhovatel ve vyhodnocení rizik prokáže přiměřené uplatnění zvolené zásady přijatelnosti rizik. Navrhovatel rovněž ověří, zda jsou zvolené zásady přijatelnosti rizik uplatňovány důsledně.

[G 1] Pokud je například pro software určité konstrukční části stanoven jako požadavek na bezpečnost vývojový proces SIL 4 normy EN 50 128, v procesu prokazování bude muset být doloženo, že je vyhověno procesu doporučovanému touto normou. Může být například požadováno prokázání, že:

(a) požadavky na nezávislost v organizaci konstrukce, ověření a validace softwaru byly splněny,
(b) jsou uplatňovány správné metody normy EN 50 128 pro úroveň integrity bezpečnosti SIL 4
(c) atd.

[G 2] Pokud má být například pro výrobu elektrických ventilů pro nouzovou brzdu použit zvláštní kodex správné praxe, proces prokazování musí doložit, že všechny požadavky z kodexu správné praxe byly v průběhu výrobního procesu splněny.

2.1.6. Uplatňování těchto zásad přijatelnosti rizik určí možná bezpečnostní opatření, která zajišťují, aby riziko (rizika) posuzovaného systému byla přijatelná. Z těchto bezpečnostních opatření se opatření vybraná k usměrňování rizika (rizik) stávají bezpečnostními požadavky, jež musí systém splňovat. Shodu s těmito bezpečnostními požadavky je nutno prokázat v souladu s oddílem 3.

[G 1] Mohou být určeny dva typy bezpečnostních opatření:

(a) „preventivní bezpečnostní opatření“, která brání vzniku nebezpečí nebo jejich příčin, a
(b) „bezpečnostní opatření ke zmírňování nebezpečí“, která brání tomu, aby se nebezpečí vyvinula v nehody nebo omezují důsledky nehod po jejich vzniku (ochranná opatření)

Předcházení příčinám nebezpečí je obecně účinnější z hlediska provozuschopnosti.

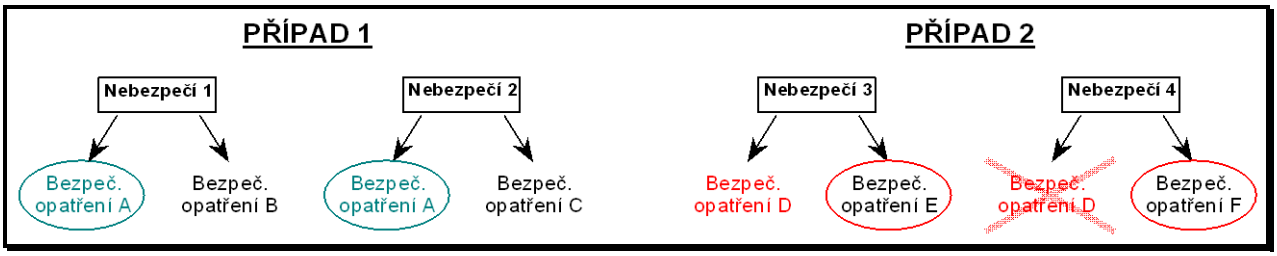
[G 2] Navrhovatel vyhodnotí jako nejvhodnější bezpečnostní opatření, která zajišťují optimální kompromis mezi náklady na omezení rizika a úrovní zbytkového rizika. Zvolená bezpečnostní opatření se stanou bezpečnostními opatřeními pro posuzovaný systém.

[G 3] Je důležité ověřit, zda zvolená bezpečnostní opatření pro usměrňování jednoho nebezpečí nejsou v rozporu s jinými nebezpečími. Jak je znázorněno na obr. 6, mohou nastat například následující dva případy[13]:

(a) PŘÍPAD 1: pokud totéž bezpečnostní opatření (opatření A na obr. 6) může usměrňovat odlišná nebezpečí, aniž by mezi nimi vytvářelo rozpory, a pokud je z ekonomického hlediska oprávněné, související bezpečnostní opatření lze zvolit samostatně jako související „požadavek na bezpečnost“. Celkový počet bezpečnostních opatření, které je třeba plnit, je menší než provádění opatření B a C zároveň,

(13) *Je třeba poznamenat, že průvodce neuvádí veškeré situace, ve kterých by bezpečnostní opatření mohla být v rozporu s jinými určenými nebezpečími. Je zde uvedeno pouze několik ilustrativních příkladů.*

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu



obr. 6: Volba přiměřených bezpečnostních opatření pro usměrňování rizik.

(b) PŘÍPAD 2: naopak, pokud jedno bezpečnostní opatření může usměrňovat jedno nebezpečí, ale vytváří rozpor s jiným nebezpečím (opatření D na obr. 6), nelze je zvolit jako „požadavek na bezpečnost“. Pro posuzované nebezpečí je třeba použít jiná bezpečnostní opatření (opatření E a F na obr. 6):

(1) Typickým příkladem řídícího systému je využívání polohy vlaku na trati buď pro ovládání funkce brzdy nebo pro povolení zvýšení rychlosti vlaku. Použití předního konce vlaku (případně zadního konce vlaku) pro určení jeho polohy není ve všech situací bezpečné:

(i) pokud má řídící systém ETCS bezpečně používat nouzové brzdy, použije systém MAXIMÁLNÍ BEZPEČNOSTI PŘEDNÍHO KONCE, aby zaručil, že přední konec vlaku skutečně zastaví před tím, než dosáhne bodu nebezpečí,

(ii) a naopak, pokud má vlak například povoleno zvýšit rychlost následně po úseku omezení rychlosti, řídící systém ETCS použije systém MINIMÁLNÍ BEZPEČNOSTI ZADNÍHO KONCE.

(2) Jiným příkladem je bezpečnostní opatření, které by mohlo platit pro zastavení vlaku téměř za všech okolností s cílem nastavit stav zabezpečený proti výpadku, s výjimkou tunelu nebo mostu. V tomto druhém případě by nemělo být přijímáno opatření D pro PŘÍPAD 2 na obr. 6.

2.1.7. Opakující se postup pro posuzování rizik je možno považovat za ukončený, je-li prokázáno, že jsou splněny všechny bezpečnostní požadavky a není nutno posoudit žádná další rozumně předvídatelná nebezpečí.

[G 1] Například v závislosti na zvolených technických řešeních konstrukce systému, jeho subsystémů a zařízení, lze určit nová nebezpečí v průběhu „prokazování shody s bezpečnostními požadavky“ (např. používání určitého nátěru by mohlo vést ke vzniku toxických plynů v případě požáru). Tato nová nebezpečí a s nimi související rizika je třeba chápat jako nové vstupy pro nové kolo v opakovaném procesu posuzování rizik. V příloze A.4.3 normy EN 50 129 jsou uvedeny jiné příklady, kdy by mohla být zavedena nová nebezpečí, která by vyžadovala usměrnění.

2.2. Identifikace nebezpečí

2.2.1. Navrhovatel pomocí rozsáhlých odborných znalostí příslušného týmu systematicky určuje veškerá přiměřeně předvídatelná nebezpečí pro celý posuzovaný systém, popřípadě jeho funkce a rozhraní.

Všechna zjištěná nebezpečí je nutno zapsat do záznamu o nebezpečí podle oddílu 4.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 1] Nebezpečí by měla být vyjádřena pokud možno na stejné úrovni podrobnosti. V průběhu předběžných analýz nebezpečí se může stát, že jsou určena nebezpečí na různých úrovních podrobnosti (např. vzhledem k tomu, že v průběhu realizace metody HAZOP (studie nebezpečí a provozuschopnosti) jsou soustřeďováni lidé s odlišnými zkušenostmi).
Úroveň podrobnosti závisí také na zásadě přijatelnosti rizik, která je zvolena pro kontrolu určeného nebezpečí (určených nebezpečí). Pokud je například nebezpečí usměrňováno zcela na základě kodexu správné praxe nebo obdobného referenčního systému, nebude nutné podrobnější určování nebezpečí.

[G 2] Všechna nebezpečí určená v průběhu procesu posuzování rizik (včetně nebezpečí spojených s obecně přijatelnými riziky), související bezpečnostní opatření a související rizika musí být evidována v záznamu o nebezpečí.

[G 3] V závislosti na povaze systému, který má být analyzován, lze uplatnit různé metody pro určování nebezpečí:

(a) lze použít empirické určování nebezpečí na základě využívání zkušenosti z minulosti (např. využívání kontrolních seznamů nebo seznamů standardních nebezpečí),
(b) lze použít tvořivé určování nebezpečí pro nové oblasti potenciálního ohrožení (aktivní tvorba prognóz, např. standardizované studie typu „CO BY SE STALO-KDYBY“, jako například FMEA nebo HAZOP).

[G 4] Empirické a kreativní metody pro určování nebezpečí lze používat společně, aby se navzájem doplňovaly s cílem zajistit, že seznam případných potenciálních nebezpečí a bezpečnostních opatření bude komplexní.

[G 5] Jako předběžný krok by proces určování nebezpečí mohl začít od brainstormingového týmu, který by byl tvořen odborníky s různou kvalifikací týkající se všech příslušných aspektů významné změny. Pokud je to podle názoru komise odborníků nezbytné, mohou být k analýze konkrétní funkce nebo provozního typu systému použity empirické metody.

[G 6] Metody užívané pro určování rizik závisejí na vymezení systému. Některé příklady jsou uvedeny v příloze B.

[G 7] Více informací o technikách a metodách určování nebezpečí lze najít v příloze A.2 a E pokynů k normě EN 50 126-2 {Ref. 9}.

[G 8] Příklad seznamu standardních nebezpečí je uveden v oddílu C.17. přílohy C.

2.2.2. Aby bylo posouzení rizik zaměřeno na nejdůležitější rizika, je nutno nebezpečí klasifikovat podle odhadovaného rizika z nich plynoucího. Na základě odborného posouzení nemusí být nebezpečí spojená s obecně přijatelným rizikem dále analyzována, nýbrž zapsána do záznamu o nebezpečí. Jejich klasifikace musí být odůvodněná, aby bylo možno provést nezávislé posouzení subjektem pro posuzování.

[G 1] Jako prostředek usnadňující proces posuzování rizik lze významná nebezpečí dále sdružovat do různých kategorií. Významná nebezpečí lze například klasifikovat nebo hierarchizovat podle funkce předpokládané závažnosti rizika a četnosti výskytu. Pokyny pro tento postup jsou uvedeny v normách CENELEC: viz oddíl A.2. v příloze A.

[G 2] Analýza rizik a hodnocení rizik, jež jsou popsány v oddílu 2.1.4, jsou uplatňovány podle priorit, počínaje od nebezpečí zařazených do kategorie nejvyšší závažnosti.

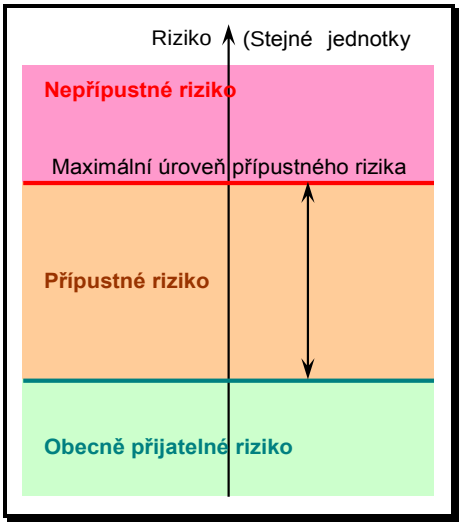
Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.2.3. Jako kritérium mohou být rizika plynoucí z nebezpečí klasifikována jako obecně přijatelná, je-li riziko natolik malé, že není přiměřené provést jakékoli další bezpečnostní opatření. Odborné posouzení zohlední to, aby všechna obecně přijatelná rizika společně nepřekročila stanovenou míru celkového rizika.

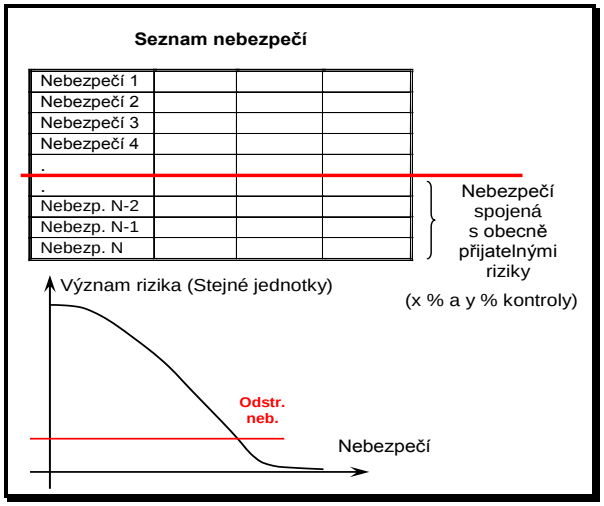
[G 1] Například riziko spojené s určitým nebezpečím může být považováno za obecně přijatelné:

(a) pokud je toto riziko nižší než daný procentuální podíl (např. x %) maximálního přijatelného rizika pro tento typ rizika. Hodnota x % by mohla být založena na správné praxi a zkušenostech s několika přístupy analýzy rizik, např. poměru mezi klasifikacemi obecně přijatelného rizika a nepřípustného rizika v křivkách FN nebo v maticích rizika. Tato situace je znázorněna na obr. 7,

(b) nebo v případě, že ztráta spojená s daným rizikem je tak malá, že není přiměřené zavádět žádné bezpečnostní protiopatření.



obr. 7: Obecně přijatelná rizika



obr. 8: Odfiltrování nebezpečí spojených s obecně přijatelnými riziky.

[G 2] Kromě toho, pokud jsou zjištěna nebezpečí na odlišné úrovni podrobnosti (např. nebezpečí na vysoké úrovni/obecná nebezpečí na jedné straně a detailní dílčí nebezpečí na straně druhé), je třeba učinit preventivní opatření s cílem zamezit jejich chybnému zařazení do kategorie nebezpečí spojených s obecně přijatelným rizikem (přijatelnými riziky). Hodnota všech nebezpečí spojených s obecně přijatelným rizikem (přijatelnými riziky) nesmí překročit daný poměr (např. y %) celkového rizika na úrovni systému. Tato kontrola je nezbytná, aby se zamezilo oslabení účinku této metody rozdělením nebezpečí na mnoho dílčích nebezpečí na nižší úrovni. A skutečně, pokud je jedno nebezpečí vyjádřeno jako mnoho jednotlivých „drobnějších“ dílčích nebezpečí, každé z nich lze snadno klasifikovat jako spojené s obecně přijatelným rizikem (riziky), pokud je hodnotíme samostatně a na druhé straně jako spojené s významným rizikem, pokud je hodnotíme jako celek (tj. jako jedno nebezpečí na vysoké úrovni). Hodnota poměru (např. y %) závisí na kritériích přijatelnosti rizik uplatňovaných na úrovni systému. Může být založena a odhadována na základě provozní zkušenosti obdobných referenčních systémů.

[G 3] Dvě výše uvedené kontroly (tj. ve vztahu k x % a y %) umožňují zaměřit posuzování rizik na nejdůležitější nebezpečí a zajistit také, aby byla veškerá významná rizika usměrňována (viz obr. 8).

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Aniž by tím byly dotčeny právní požadavky v příslušném členském státě, navrhovatel odpovídá za to, aby definoval na základě odborného posouzení hodnoty x % a y % a aby je nechal nezávisle posoudit subjektem pro posuzování. Jako příklad příslušného matematického řádu lze uvést x = 1 % a y = 10 %, pokud to je považováno za přijatelné podle odborného posouzení.

[G 4] V oddílu 2.2.2 se požaduje, aby zařazení do kategorie „obecně přijatelného rizika (přijatelných rizik)“ nezávisle posuzoval subjekt pro posuzování.

2.2.4. Během identifikace nebezpečí je možno určit bezpečnostní opatření. Tato opatření jsou zapsána v záznamu o nebezpečí podle oddílu 4.

[G 1] Hlavním účelem této činnosti je určení nebezpečí, která jsou spojena se změnou. Pokud jsou bezpečnostní opatření již určena, musí být evidována v záznamu o nebezpečí. Povaha opatření závisí na dané změně; opatření mohou být procesní, technická, provozní nebo organizační.

2.2.5. Identifikaci nebezpečí je nutno provést pouze na úrovni podrobnosti, která je nezbytná k určení toho, kde se očekává, že bezpečnostní opatření usměrní rizika v souladu s jednou ze zásad přijatelnosti rizik zmíněných v bodě 2.1.4. Může být proto nutné použít metodu iterace mezi fázemi analýzy rizik a jejich vyhodnocení, dokud není dosaženo dostatečné úrovně podrobnosti pro identifikaci nebezpečí.

[G 1] Dokonce i v případě, že je riziko usměrňováno na přijatelnou úroveň, navrhovatel může přesto rozhodnout, že je nezbytné podrobnější určení nebezpečí. Jedním z důvodů pro toto opatření může být skutečnost, že je pravděpodobné, že se podaří najít rentabilnější bezpečnostní opatření pro usměrnění rizika, pokud bude provedeno podrobnější určení nebezpečí.

2.2.6. Kdykoli se pro usměrnění rizika použije kodex správné praxe nebo referenční systém, lze identifikaci nebezpečí omezit na:

(a) ověření vhodnosti kodexu správné praxe nebo referenčního systému pro daný případ.
(b) zjištění odchylek od kodexu správné praxe nebo referenčního systému.

[G 1] Další vysvětlení se nepovažuje za nutné.

2.3. Používání kodexů správné praxe a hodnocení rizik

2.3.1. Navrhovatel s podporou ostatních dotčených účastníků a na základě požadavků uvedených v bodě 2.3.2 analyzuje, zda je jedno či několik nebezpečí náležitě pokryto používáním příslušných kodexů správné praxe.

[G 1] Další vysvětlení se nepovažuje za nutné.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.3.2. .3.2. Kodexy správné praxe musí splňovat přinejmenším tyto požadavky:

(a) jsou obecně uznávány v železničním odvětví. Pokud tomu tak není, musí být kodexy správné praxe odůvodněny a být přijatelné pro subjekt pro posuzování;
(b) jsou důležité pro usměrňování uvažovaných nebezpečí v posuzovaném systému;
(c) jsou veřejně dostupné pro všechny účastníky, kteří je chtějí používat.

[G 1] Další vysvětlení se nepovažuje za nutné.

2.3.3. Pokud směrnice 2008/57/ES vyžaduje shodu s TSI a příslušná TSI neukládá proces řízení rizik stanovený tímto nařízením, je možno TSI považovat za kodexy správné praxe pro usměrňování nebezpečí, je-li splněn požadavek uvedený v bodě 2.3.2. písm. c).

[G 1] Další vysvětlení se nepovažuje za nutné.

2.3.4. Vnitrostátní předpisy oznámené v souladu s článkem 8 směrnice 2004/49/ES a čl. 17 odst. 3 směrnice 2008/57/ES lze považovat za kodexy správné praxe, jsou-li splněny požadavky bodu 2.3.2.

[G 1] Další vysvětlení se nepovažuje za nutné.

2.3.5. Je-li jedno či více nebezpečí usměrňováno kodexy správné praxe, které splňují požadavky bodu 2.3.2, pak rizika spojená s těmito nebezpečími se považují za přijatelná. To znamená, že:

(a) tato rizika není nutno dále analyzovat;
(b) používání kodexů správné praxe je zapsáno v záznamu o nebezpečí jako bezpečnostní požadavek s ohledem na příslušná nebezpečí.

[G 1] Další vysvětlení se nepovažuje za nutné.

2.3.6. Pokud není alternativní přístup plně v souladu s příslušným kodexem správné praxe, navrhovatel prokáže, že přijatý alternativní přístup vede přinejmenším ke stejné úrovni bezpečnosti.

[G 1] Další vysvětlení se nepovažuje za nutné.

2.3.7. Pokud nelze zajistit, aby při použití kodexů správné praxe bylo riziko u konkrétního nebezpečí přijatelné, je nutno stanovit dodatečná bezpečnostní opatření s použitím jedné nebo dvou dalších zásad přijatelnosti rizik.

[G 1] Další vysvětlení se nepovažuje za nutné.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.3.8. V případě, že jsou všechna rizika usměrňována pomocí kodexů správné praxe, lze proces řízení rizik omezit na:

(a) identifikaci nebezpečí podle bodu 2.2.6;
(b) zápis použití kodexů správné praxe do záznamu o nebezpečí podle bodu 2.3.5;
(c) dokumentaci použití procesu řízení rizik podle oddílu 5;
(d) nezávislé posouzení podle článku 6.

[G 1] Další vysvětlení se nepovažuje za nutné.

2.4. Používání referenčního systému a hodnocení rizik

2.4.1. Navrhovatel s podporou ostatních dotčených účastníků analyzuje, zda se na jedno či více nebezpečí vztahuje podobný systém, který by bylo možno použít jako referenční systém.

[G 1] Podrobnější informace o těchto zásadách lze najít v oddílu § 8 průvodce EN 50 126-2 {Ref. 9}.

2.4.2. Referenční systém splňuje přinejmenším tyto požadavky:

(a) při jeho používání již bylo prokázáno, že zajišťuje přijatelnou úroveň bezpečnosti, a byl by způsobilý pro schválení v členském státě, v němž má být změna zavedena;
(b) má podobné funkce a rozhraní jako posuzovaný systém;
(c) používá se za obdobných provozních podmínek jako posuzovaný systém;
(d) používá se za obdobných environmentálních podmínek jako posuzovaný systém.

[G 1] Například původní řídící systém, který prokázal při používání přijatelnou úroveň bezpečnosti, by mohl být nahrazen jiným systémem, s modernější technologií a lepší výkonností v oblasti bezpečnosti. Je proto vhodné pokaždé při uplatňování referenčního systému ověřit, zda i nadále splňuje kritéria přijatelnosti.

[G 2] Například vzhledem k tomu, že určité aspekty bezpečnosti tunelů nebo bezpečnosti dopravy nebezpečných věcí mohou mít specifickou povahu a mohou záviset na provozních podmínkách a na podmínkách týkajících se životního prostředí, je nezbytné ověřit pro každý projekt, že systém bude používán za stejných podmínek.

2.4.3. Pokud referenční systém splňuje požadavky uvedené v bodě 2.4.2, pak u posuzovaného systému:

(a) rizika spojená s nebezpečími, na něž se vztahuje referenční systém, se považují za přijatelná;
(b) bezpečnostní požadavky pro nebezpečí, na něž se vztahuje referenční systém, lze odvodit z analýz bezpečnosti nebo vyhodnocení záznamů o bezpečnosti referenčního systému;
(c) tyto bezpečnostní požadavky jsou zapsány do záznamu o nebezpečí jako bezpečnostní požadavky pro příslušná nebezpečí.

[G 1] Další vysvětlení se nepovažuje za nutné.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.4.4. Pokud se posuzovaný systém odchyluje od referenčního systému, hodnocení rizik prokáže, že posuzovaný systém dosahuje přinejmenším stejné úrovně bezpečnosti jako referenční systém. Rizika spojená s nebezpečími, na něž se vztahuje referenční systém, se v tomto případě považují za přijatelná.

[G 1] Podrobnější informace o analýzách podobnosti lze najít v oddílu § 8.1.3. pokynů k normě EN 50 126-2 {Ref. 9}.

2.4.5. Nelze-li prokázat stejnou úroveň bezpečnosti jako u referenčního systému, je nutno s použitím jedné či dvou dalších zásad přijatelnosti rizik určit dodatečná bezpečnostní opatření pro odchylky.

[G 1] Další vysvětlení se nepovažuje za nutné.

2.5. Jednoznačný odhad a hodnocení rizik

2.5.1. Pokud se na nebezpečí nevztahuje jedna nebo dvě zásady přijatelnosti rizik popsané v bodech 2.3 a 2.4, prokázání přijatelnosti rizik se provádí jednoznačným odhadem rizik a jejich vyhodnocením. Rizika vyplývající z těchto nebezpečí je nutno odhadnout kvantitativně nebo kvalitativně s přihlédnutím ke stávajícím bezpečnostním opatřením.

[G 1] Další vysvětlení se nepovažuje za nutné.

2.5.2. Přijatelnost odhadovaných rizik se vyhodnotí pomocí kritérií přijatelnosti rizik odvozených nebo vycházejících z právních požadavků stanovených v právních předpisech Společenství nebo v oznámených vnitrostátních předpisech. Podle kritérií přijatelnosti rizik je možno přijatelnost rizika vyhodnotit jednotlivě pro každé související nebezpečí nebo celkově pro kombinaci všech nebezpečí uvažovaných v jednoznačném odhadu rizik.

Není-li odhadnuté riziko přijatelné, určí se a provedou dodatečná bezpečnostní opatření ke snížení rizika na přijatelnou úroveň.

[G 1] Abychom mohli zhodnotit, zda rizika spojená s posuzovaným systémem jsou přijatelná nebo ne, potřebujeme kritéria přijatelnosti rizik (viz rámečky „hodnocení rizik“ na obr. 1). Kritéria přijatelnosti rizik mohou být implicitní nebo explicitní:

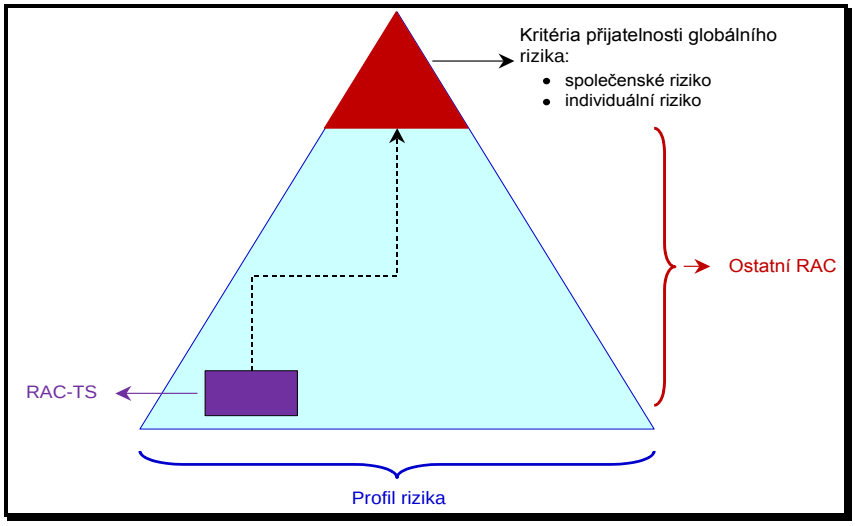
(a) implicitní kritéria přijatelnosti rizik: podle oddílů 2.3.5 a 2.4.3, rizika, na která se vztahuje uplatňování kodexů správné praxe a srovnání s referenčními systémy, jsou kvalifikována implicitně jako přijatelná za předpokladu, že (viz tečkovaný kruh na obr. 1):

(1) jsou splněny podmínky uplatňování kodexů správné praxe v oddílu 2.3.2 ;
(2) jsou splněny podmínky pro použití referenčního systému v oddílu 2.4.2;

(b) explicitní kritéria přijatelnosti rizik: abychom mohli zhodnotit, zda riziko (rizika) usměrňované uplatněním jednoznačného odhadu rizika je přijatelné či ne, potřebujeme explicitní kritéria přijatelnosti rizik (viz kruh plnou čarou na obr. 1 týkající se třetí zásady). Ta lze definovat na různých úrovních železničního systému. Lze je chápat jako "pyramidu kritérií" (viz obr. 9), počínaje od obecných kritérií přijatelnosti rizik (jež

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

představují například společenská nebo individuální rizika), až na úroveň subsystémů a prvků (s cílem postihnout technické systémy) a včetně lidské obsluhy v průběhu provozních činností a činností údržby systému a subsystémů. Přestože kritéria přijatelnosti rizik přispívají k dosažení bezpečnostní výkonnosti systému a vážou se tak na CST a NRV, je velice obtížné vytvořit matematický model postihující jejich vztah: viz {Ref. 12}, kde jsou o tom uvedeny bližší podrobnosti.
Úroveň, na které jsou definována explicitní kritéria přijatelnosti rizik, musí odpovídat významu a složitosti významné změny. Není například nezbytné hodnotit celkové riziko železničního systému, pokud provádíme úpravu určitého typu nápravy kolejových vozidel. Definice kritérií přijatelnosti rizik se může zaměřit na bezpečnost kolejových vozidel. Na druhé straně velké změny nebo doplnění existujícího železničního systému by neměly být hodnoceny pouze na základě bezpečnostní výkonnosti jednotlivých funkcí nebo doplňkových změn. Je třeba také ověřit na úrovni železničního systému, že změna je přijatelná jako celek.



obr. 9: Pyramida kritérií přijatelnosti rizik (RAC).

[G 2] Explicitní kritéria přijatelnosti rizik, která jsou potřebná jako vodítko pro proces vzájemného uznávání, budou mezi členskými státy harmonizována prostřednictvím průběžné práce agentury na kritériích přijatelnosti rizik. Pokud budou k dispozici další informace, budou doplněny do tohoto dokumentu.

[G 3] Mezitím lze rizika hodnotit například za použití matice rizik, kterou lze najít v oddílu § 4.6 normy EN 50 126-1 {Ref. 8}. Lze použít i jiné typy vhodných kritérií, pokud lze předpokládat, že tato kritéria v daném případě zajistí přijatelnou úroveň bezpečnosti.

2.5.3. Je-li riziko spojené s jedním nebezpečím nebo s kombinací několika nebezpečí považováno za přijatelné, zapíší se určená bezpečnostní opatření do záznamu o nebezpečí.

[G 1] Další vysvětlení se nepovažuje za nutné.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.5.4. *Pokud nebezpečí vyplývá ze selhání technických systémů, na něž se nevztahují kodexy správné praxe nebo použití referenčního systému, použije se při návrhu technického systému toto kritérium přijatelnosti rizik:*

U technických systémů, u nichž může věrohodně selhání funkcí přímo vést ke katastrofickému důsledku, související riziko nemusí být dále sníženo, je-li míra tohoto selhání nižší nebo rovna 10^{-9} za hodinu provozu.

[G 1] Další podrobnosti o kritériu RAC-TS, a také o aspektech a funkcích technického systému, na které se toto kritérium vztahuje, jsou uvedeny v samostatné poznámce agentury související s tímto dokumentem: viz oddíl A.3. přílohy A a referenční dokument {Ref. 11}.

2.5.5. *Aniž by byl dotčen postup popsaný v článku 8 směrnice 2004/49/ES, může být vnitrostátním předpisem požadováno náročnější kritérium za účelem udržení vnitrostátní úrovně bezpečnosti. Avšak v případě dodatečných povolení k uvedení vozidel do provozu se použije článek 23 a článek 25 směrnice 2008/57/ES.*

[G 1] Další vysvětlení se nepovažuje za nutné.

2.5.6. *Je-li technický systém vyvinut s použitím kritéria 10^{-9} stanoveného v bodě 2.5.4, použije se zásada vzájemného uznávání podle čl. 7 odst. 4 tohoto nařízení.*

Nicméně, jestliže 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.

[G 1] Další vysvětlení se nepovažuje za nutné.

2.5.7. *Jednoznačný odhad rizik a jejich vyhodnocení splňuje nejméně tyto požadavky:*

(a) *metody použité pro jednoznačný odhad rizik správně odrážejí posuzovaný systém a jeho parametry (včetně všech provozních režimů);*

(b) *výsledky jsou dostatečně přesné, aby mohly sloužit jako řádná podpora při rozhodování, tj. menší změny ve vstupních předpokladech nebo podmínkách nevedou k podstatně odlišným požadavkům.*

[G 1] Další vysvětlení se nepovažuje za nutné.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

3. PROKÁZÁNÍ SHODY S BEZPEČNOSTNÍMI POŽADAVKY

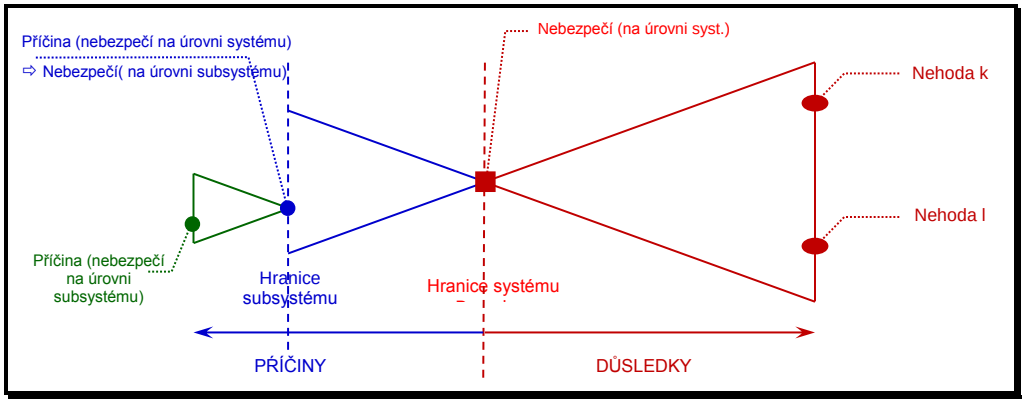
3.1. Před schválením bezpečnosti změny je nutno za dozoru navrhovatele prokázat splnění bezpečnostních požadavků vyplývajících z fáze posuzování rizik.

[G 1] Jak je vysvětleno v bodech [G 3] až [G 6] v oddílu 2.1.1, „prokázání shody systému s bezpečnostními požadavky“ zahrnuje fázi „6 až 10“ V-cyklu norem CENELEC (viz rámeček 3 na obr. 5). Viz bod [G 3] v oddílu 2.1.1.

[G 2] Viz také bod [G 4] v oddílu 2.1.1 tohoto dokumentu.

3.2. Toto prokázání shody provádí účastníci, kteří odpovídají za splnění bezpečnostních požadavků, jak bylo rozhodnuto v souladu s bodem 1.1.5.

[G 1] Příkladem posuzování bezpečnosti a analýz bezpečnosti, které lze provádět na úrovni subsystému jsou přičinné analýzy: viz obr. 10. Pro prokázání shody subsystému se vstupními požadavky na bezpečnost lze ovšem použít jakoukoli jinou metodu.

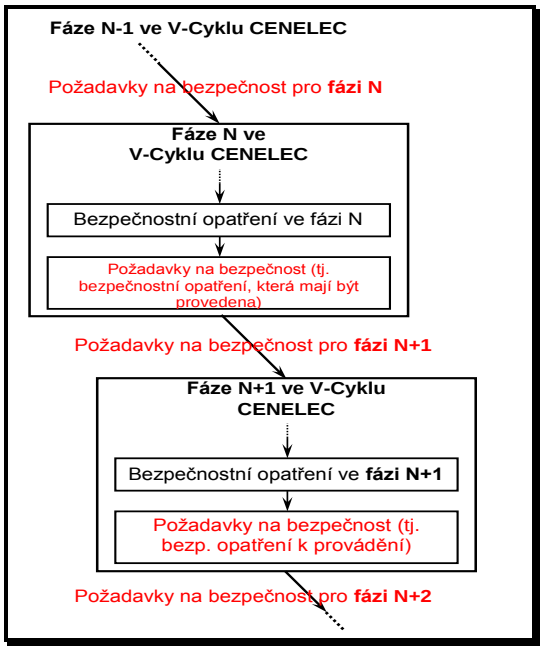


obr. 10: Obrázek A.4 z EN 50 129: Definice nebezpečí ve vztahu k hranici systému.

[G 2] Hierarchickou strukturu nebezpečí a příčin, ve vztahu k systémům a subsystémům, lze opakovat pro každou fázi V-cyklu norem CENELEC na nižších úrovních na obr. 5. Činnosti určování nebezpečí a příčinné analýzy (nebo jakákoli vhodná metoda) a také používání kodexů správné praxe, obdobných referenčních systémů a explicitních analýz a hodnocení, lze také opakovat pro každou fázi cyklu vývoje systému, aby bylo možné odvodit z bezpečnostních opatření určených na úrovni subsystému bezpečnostní opatření, která mají být splněna v další fázi. Tento proces je znázorněn na obr. 11.

[G 3] Viz také bod [G 4] v oddílu 2.1.1 tohoto dokumentu.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu



obr. 11: Odvození požadavků na bezpečnost pro fáze na nižší úrovni.

3.3.	*Přístup zvolený k prokázání shody s bezpečnostními požadavky a samotné prokázání posuzuje nezávisle subjekt pro posuzování.*

[G 1] Všechny činnosti znázorněné v rámečku 3[(14)] V-cyklu norem CENELEC na obr. 5 jsou proto také posuzovány nezávisle.

[G 2] Typ a úroveň podrobnosti pro nezávislé posouzení, které je prováděno subjekty pro posuzování (tj. podrobné nebo makroskopické posouzení), jsou analyzovány v rámci vysvětlení v čl. 6.

3.4.	*Případná nepřiměřenost bezpečnostních opatření, která mají podle očekávání splnit bezpečnostní požadavky, nebo jakákoli nebezpečí zjištěná při prokazování shody s bezpečnostními požadavky vedou k novému posouzení a vyhodnocení souvisejících rizik ze strany navrhovatele podle oddílu 2. Nová nebezpečí jsou zapsána do záznamu o nebezpečí podle oddílu 4.*

[G 1] Například způsob hašení požáru by mohl vést k novému nebezpečí (udušení), ze kterého by vyplynuly nové požadavky na bezpečnost (např. konkrétní postup evakuace cestujících). Jiným příkladem je použití tvrzeného skla, které zabraňuje rozbití oken při haváriích a zranění cestujících rozbitým sklem či dokonce jejich vypadnutí z vlaku. Nové vyvolané nebezpečí pak spočívá v tom, že nouzová evakuace z vagonů okny je mnohem obtížnější, což může vyústit v požadavky na bezpečnost, v nichž se bude prosazovat taková speciální konstrukce určitých oken, aby umožňovala evakuaci.

(14) *Souvztažnost činností mezi CSM a obr. 5 (tj. Obr. 10 V-Cyklu norem CENELEC 50 126) je popsána v oddílu 2.1.1. Zejména bod [G 3] v oddílu 2.1.1 uvádí, které činnosti norem CENELEC jsou obsaženy ve fázi „prokázání souladu systému s bezpečnostními požadavky“ v rámci CSM.*

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 2] Příklad provozní změny: existuje požadavek, aby pro veškerou dopravu nebezpečných věcí platil zákaz průjezdu na trati vedoucí hustě zalidněnými oblastmi. Místo toho by tedy příslušný náklad měl být přepravován jinou trasou, na které jsou tunely, a na níž tedy vznikají odlišné typy nebezpečí.

[G 3] Jiné příklady nových nebezpečí, která lze určit v průběhu prokazování shody systému s požadavky na bezpečnost, lze najít v příloze A.4.3 normy EN 50 129.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

4. ŘÍZENÍ NEBEZPEČÍ

4.1. Proces řízení nebezpečí

4.1.1. Záznam (záznamy) o nebezpečí vytváří nebo aktualizuje (pokud již existují) navrhovatel během období zpracování návrhu a provádění až do přijetí změny nebo do doby předložení zprávy o posouzení bezpečnosti. Záznam o nebezpečí sleduje pokrok při sledování rizik spojených se zjištěným nebezpečím. V souladu s bodem 2 písm. g) přílohy III směrnice 2004/49/ES, jakmile byl systém přijat a je provozován, záznam o nebezpečí dále uchovává provozovatel infrastruktury nebo železniční podnik pověřený provozováním posuzovaného systému jako nedílnou součást svého systému řízení bezpečnosti.

[G 1] Využívání záznamu o nebezpečí pro registraci, řízení a usměrňování informací významných z hlediska bezpečnosti doporučují také normy CENELEC 50 126-1 {Ref. 8} a 50 129 {Ref. 7}.

[G 2] V závislosti na složitosti daného systému by určitý subjekt mohl mít například jeden nebo více záznamů o nebezpečí. V obou případech záznam o nebezpečí (záznamy o nebezpečí) podléhá nezávislému posouzení ze strany subjektu pro posuzování (subjektů pro posuzování). Jedním z možných řešení by bylo například mít k dispozici:

(a) jeden „záznam o vnitřním nebezpečí“ pro řízení všech požadavků na vnitřní bezpečnost vztahující se k subsystému, za který daný subjekt odpovídá. Jeho rozsah a objem řídící práce závisí na jeho struktuře a samozřejmě na složitosti subsystému. Ovšem vzhledem k tomu, že se používá pro účely vnitřního řízení, záznam o nebezpečí nemusí být poskytován ostatním subjektům. Záznam o vnitřním nebezpečí obsahuje všechna určená nebezpečí, která jsou usměrňována a také související bezpečnostní opatření, která podléhají validaci,
(b) jeden „záznam o vnějším nebezpečí“ pro přenos nebezpečí a souvisejících bezpečnostních opatření (která subjekt nemůže plně provádět sám) na jiné subjekty v souladu s oddílem 1.2.2. Tento druhý typ záznamu o nebezpečí bývá obvykle menší a vyžaduje méně řídící práce (viz příklad v oddílu C.16.4. přílohy C).

[G 3] Pokud se zdá být příliš složité zajišťovat správu několika záznamů o nebezpečí, jiným možným řešením je řídit všechna nebezpečí a související bezpečnostní opatření, na která se vztahují výše uvedená písmena (a) a (b) v rámci jediného záznamu o nebezpečí, ale s možností vyhotovení dvou zpráv o záznamech o nebezpečí (viz příklad uvedený v oddílu C.16.3. přílohy C):

(a) jedna zpráva o záznamu o vnitřním nebezpečí, která by dokonce nebyla nutná, pokud je záznam o nebezpečí náležitě členěný, aby umožňoval nezávislé posouzení,
(b) jedna zpráva o záznamu o vnějším nebezpečí pro přenos nebezpečí a souvisejících bezpečnostních opatření na jiné subjekty.

[G 4] Jak jsme již vysvětlili v oddílu 4.2, na konci realizace projektu, kdy je systém přijat:

(a) všechna nebezpečí, která jsou přenesena na jiné subjekty, jsou usměrňována v záznamu o vnějším nebezpečí příslušného subjektu, který uskutečňuje jejich přenos. Vzhledem k tomu, že jsou vložena a jejich řízení je zajišťováno v záznamech o vnitřním nebezpečí jiných subjektů, nemusejí být dále řízena dotčeným subjektem v průběhu životního cyklu příslušného systému (subsystému),
(b) avšak všechna související bezpečnostní opatření by měla podléhat validaci v záznamu o nebezpečí, a to z důvodů, jež jsou vysvětleny v bodě [G 9] oddílu 4.2. Je skutečně užitečné, aby organizace, která odesílá pokyn k omezení použití, jednoznačně ve svém

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

záznamu o nebezpečí zdůraznila, že související bezpečnostní opatření neprošla procesem validace.

[G 5] Na druhé straně, veškeré záznamy o vnitřním nebezpečí jsou vedeny po celou dobu životního cyklu systému (subsystému). To umožňuje sledovat pokrok ve sledování rizik spojených s určenými nebezpečími v průběhu provozu a údržby systému (subsystému), tj. dokonce i po jeho uvedení do provozu: viz rámeček 4 ve V-cyklu norem CENELEC na obr. 5.

4.1.2. Záznam o nebezpečí zahrnuje všechna nebezpečí spolu se všemi souvisejícími bezpečnostními opatřeními a předpoklady týkajícími se systému určenými v rámci postupu pro posuzování rizik. Obsahuje zejména jednoznačný odkaz na původ a na vybrané zásady přijatelnosti rizik a jednoznačně určuje účastníka (účastníky) pověřené usměrňováním těchto nebezpečí.

[G 1] Informace o nebezpečích a souvisejících bezpečnostních opatřeních, která jsou přijata od jiných subjektů (viz oddíl 1.2.2) zahrnují rovněž veškeré předpoklady[15] a omezení použití[15] (nazývané také podmínky pro použití související s bezpečností) vztahující se na různé subsystémy, doklady bezpečnosti standardních aplikací a doklady bezpečnosti standardních produktů, které vydávají výrobci, pokud to připadá v úvahu.

[G 2] Příklad možné struktury záznamu o nebezpečí je popsán v oddílu C.16. přílohy C.

4.2. Výměna informací

Všechna nebezpečí a související bezpečnostní požadavky, jež nemůže jeden účastník usměrnit sám, jsou sdělena druhému příslušnému účastníkovi s cílem nalézt společně přiměřené řešení. Nebezpečí zapsaná v záznamu o nebezpečí účastníka, který je převádí, jsou „usměrněna“ pouze tehdy, pokud hodnocení rizik souvisejících s těmito nebezpečími provádí jiný účastník a řešení je odsouhlaseno všemi dotčenými stranami.

[G 1] Například v případě odometrického subsystému palubního zařízení ETCS může výrobce podrobit procesu validace v laboratoři příslušné algoritmy prostřednictvím simulace teoretických signálů, které by mohly být vytvořeny souvisejícími odometrickými snímacími zařízeními. Ovšem úplná validace odometrického subsystému vyžaduje spolupráci železničních podniků a provozovatelů infrastruktury za účelem provedení validace v reálném prostředí vlaku a skutečného kola vlaku v kontaktu s kolejí.

[G 2] Jako další příklady lze uvést přenos provozních nebo údržbových bezpečnostních opatření pro technická zařízení ze strany výrobců na železniční podniky. Tato bezpečnostní opatření bude muset provést železniční podnik.

[G 3] Aby bylo možné opětovné posouzení těchto nebezpečí, souvisejících bezpečnostních opatření a rizik uskutečněné společně zúčastněnými organizacemi, je užitečné, aby organizace, která je určila, podala všechna vysvětlení, jež jsou nezbytná k jasnému porozumění danému problému. Může se stát, že počáteční formulace nebezpečí, bezpečnostních opatření a potřeb v oblasti rizika budou muset být změněny, aby byly

(15) *Viz bod [G 5] v oddílu 1.1.5 a poznámky pod čarou [9] a [10] na straně 27 tohoto dokumentu, kde jsou uvedena další vysvětlení k termínům doklady bezpečnosti „standardního výrobku a standardní aplikace“, „předpoklady a omezení použití“.*

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

srozumitelné, aniž by bylo nutné je opětovně společně projednávat. Společné opětovné posouzení nebezpečí může vyústit v určení nových bezpečnostních opatření.

[G 4] Přijímající subjekt odpovídající za provádění, ověření a validaci přijatých nebo nových bezpečnostních opatření eviduje ve vlastním záznamu o nebezpečí všechna související nebezpečí se všemi souvisejícími bezpečnostními opatřeními (vloženými i společně určenými).

[G 5] Pokud určité bezpečnostní opatření neprošlo plným procesem validace, v záznamu o nebezpečí musí být vyhotoveno a evidováno jednoznačné omezení jeho použití (např. provozní opatření zmírňující rizika). Může skutečně nastat situace, že technická /konstrukční bezpečnostní opatření:

(a) nejsou správně prováděna, nebo
(b) nejsou prováděna úplně, nebo
(c) nejsou prováděna záměrně, například proto, že jsou prováděna odlišná bezpečnostní opatření místo opatření evidovaných v záznamu o nebezpečí (např. kvůli úspoře nákladů). Vzhledem k tomu, že neprošla procesem validace, musí být tato bezpečnostní opatření jednoznačně určena v záznamu o evidenci. Musí být také předloženy důkazní informace/zdůvodnění, proč jsou bezpečnostní opatření, která byla zavedena místo původních opatření,[16] vhodná, a také prokázáno, že i s těmito náhradními bezpečnostními opatřeními systém odpovídá požadavkům na bezpečnost
(d) atd.

V těchto případech související technická/konstrukční bezpečnostní opatření nelze ověřit a provést jejich validaci v průběhu procesu řízení nebezpečí. Související nebezpečí a bezpečnostní opatření musí tedy v záznamu o nebezpečí zůstat otevřená, aby se zamezilo případnému zneužívání těchto bezpečnostních opatření v souvislosti s jinými systémy uplatňováním zásady přijatelnosti rizik „obdobného referenčního systému“.

[G 6] „Nesprávně“ a/nebo „neúplně“ provedená bezpečnostní opatření bývají obvykle odhalena v počáteční fázi životního cyklu systému a opravena před uznáním systému. Pokud jsou však odhalena příliš pozdě na to, aby bylo možné technická bezpečnostní opatření provést správně a úplně, organizace odpovědná za provádění a řízení musí určit a evidovat v záznamu o nebezpečí jasná omezení použití posuzovaného systému. Tato omezení použití často představují provozní omezující podmínky pro použití posuzovaného systému.

[G 7] V záznamu o nebezpečí by mohlo být také užitečné evidovat, zda budou související bezpečnostní opatření správně uplatněna v pozdější fázi životního cyklu systému, nebo zda bude daný systém i nadále používán s určenými omezeními. Dále by mohlo být užitečné evidovat v záznamu o nebezpečí zdůvodnění proč související technická bezpečnostní opatření nebyla prováděna správně/úplně.

[G 8] Subjekt, který obdrží omezení použití:

(a) je všechna vloží do vlastního záznamu o nebezpečí,
(b) zajistí, aby podmínky pro použití posuzovaného systému byly v souladu se všemi přijatými omezeními použití,
(c) ověří a provede validaci potvrzující, že posuzovaný systém vyhovuje všem těmto omezením použití.

---

(16) *Pokud jsou zaváděna odlišná bezpečnostní opatření místo opatření původně stanovených, musí být také evidována v záznamu o nebezpečí.*

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 9] V závislosti na rozhodnutích, na kterých se dohodnou zúčastněné organizace:

(a) jsou související technická bezpečnostní opatření správně zavedena do konstrukčních prvků v pozdější fázi.
Organizace, která odesílá pokyn k omezení použití, i nadále sleduje správné technické provádění souvisejících bezpečnostních opatření. Z tohoto důvodu související bezpečnostní opatření nelze podrobit validaci a nebezpečí s nimi spojená nejsou usměrňována v záznamu o nebezpečí této organizace, dokud nejsou odpovídající technická bezpečnostní opatření plně provedena. Tento postup musí být zajištěn i v případě, že jsou mezitím odeslaná omezení použití provedena.

(b) nebo související technická bezpečnostní opatření nejsou zavedena do konstrukčních prvků v pozdější fázi. Systém tak bude i nadále používán v průběhu vlastního životního cyklu se souvisejícími omezeními použití. V tomto případě lze učinit tyto kroky:

(1) organizace odesílající pokyn k omezení použití neeviduje ve svém záznamu o nebezpečí související bezpečnostní opatření jako „podrobená validaci“. Díky tomu, jestliže používá související systém jako referenční systém pro ostatní projekty, příslušná potenciální bezpečnostní ohrožení nebudou přehlížena. Takže i v případě, že jiný subjekt souhlasí s tím, že bude související rizika řídit odlišným způsobem, je užitečné, aby organizace, která odesílá pokyn k omezení použití, jasně zdůraznila ve svém záznamu o nebezpečí, že související bezpečnostní rizika neprošla procesem validace, nebo

(2) lze změnit popis systému tak, aby omezení použití bylo promítnuto do rozsahu použití systému (tj. do předpokladů pro systém) a do bezpečnostních požadavků. To umožní usměrnění nebezpečí. Pokud tedy bude tento systém používán jako referenční systém pro jinou aplikaci:

(i) nový systém bude muset být používán za stejných podmínek (tj. vyhovovat požadavku na omezení použití v souvislosti s těmito předpoklady), nebo
(ii) by navrhovatel měl provést další posuzování rizik v případě odchylek od těchto předpokladů.

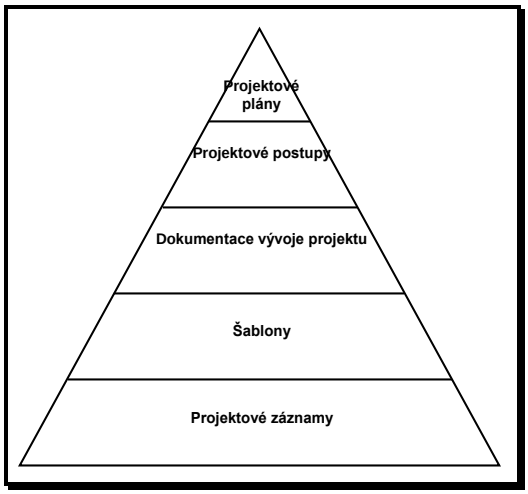
Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

5. DŮKAZY O UPLATŇOVÁNÍ PROCESU ŘÍZENÍ RIZIK

5.1. Proces řízení rizik použitý k posouzení úrovně bezpečnosti a shody s bezpečnostními požadavky dokumentuje navrhovatel tak, aby subjekt pro posuzování měl k dispozici veškeré nezbytné důkazy prokazující správné uplatňování procesu řízení rizik. Subjekt pro posuzování uvede své závěry ve zprávě o posouzení bezpečnosti.

[G 1] Systém řízení bezpečnosti (SMS) provozovatelů infrastruktury a železničních podniků již tyto požadavky řeší. Pokud jde o jiné subjekty působící v odvětví železniční dopravy, které se podílejí na významné změně, i v případě, že systém řízení bezpečnosti není povinný, obecně alespoň na úrovni projektu mají zavedený proces řízení jakosti a/nebo proces řízení bezpečnosti (SMP). Oba tyto procesy jsou založeny na standardizované hierarchii dokumentace buď v rámci podniku, nebo alespoň v rámci projektu. Řeší také dokumentační potřeby řízení RAMS. Taková standardizovaná dokumentace může být v zásadě tvořena následujícími prvky (viz také obr. *12*):

(a) **Projektové plány,** které jsou zpracovány za účelem popisu způsobu, jak organizovat řízení určitých činností v rámci projektu.
(b) **Projektové postupy,** které jsou zpracovány za účelem podrobného popisu způsobu, jak dosáhnout určeného úkolu. Postupy a pokyny obvykle existují v rámci podniku a jako takové jsou uplatňovány. Nové projektové postupy jsou vypracovány pouze v případě, že vznikne potřeba popsat konkrétní úkol v rámci posuzovaného projektu.
(c) **Dokumentace vývoje projektu** zpracovávaná po dobu životního cyklu systému znázorněného na obr. 5.



obr. 12: Standardizovaná hierarchie dokumentace.

(d) Pro různé typy dokumentů, které mají být vyhotoveny, existují **podnikové nebo alespoň projektové šablony.**
(e) **Projektové záznamy** zpracované v průběhu realizace projektu a nezbytné pro prokázání souladu s podnikovými procesy řízení jakosti a řízení bezpečnosti.

Toto je jeden způsob, jak docílit potřeb zdokumentovaných důkazů. Mohou existovat i jiná řešení, pokud jsou splněna kritéria CSM.

[G 2] Normy CENELEC doporučují prokazovat soulad systému s funkčními požadavky a s požadavky na zajištění bezpečnosti v dokladu bezpečnosti (nebo ve zprávě o bezpečnosti). I v případě, že to není povinné, použitý doklad bezpečnosti podává formou standardizovaného dokumentu zdůvodňujícího bezpečnostní aspekty tyto informace:

(a) důkaz o řízení jakosti,
(b) důkaz o řízení bezpečnosti,
(c) důkaz o funkční a technické bezpečnosti.

Jeho výhodou je také skutečnost, že slouží jako podklad a vodítko pro subjekt pro posuzování (subjekty pro posuzování) při nezávislém posouzení správného uplatňování CSM.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 3] Doklad bezpečnosti popisuje a shrnuje, jak projektové dokumenty, které souvisejí s uplatňováním podnikových nebo projektových procesů řízení jakosti a/nebo procesů řízení bezpečnosti navzájem souvisejí v rámci procesu vývoje systému s cílem prokázat bezpečnost systému. Doklad bezpečnosti obvykle neobsahuje rozsáhlé objemy podrobných důkazů a podkladové dokumentace, ale uvádí přesné odkazy na tyto dokumenty.

[G 4] **Doklad bezpečnosti pro technické systémy:** Normy CENELEC lze použít jako pokyny pro sestavení a/nebo strukturu bezpečnostních spisů:

(a) viz norma EN 50 129 {Ref. 7} pro železniční aplikace – sdělovací a zabezpečovací systémy a systémy zpracování dat, příloha H.2 pokynů k normě EN 50 126-2 {Ref. 9} obsahuje také návrh struktury dokladu bezpečnosti pro zabepečovací systémy,
(b) viz příloha H.1 pokynů k normě EN 50 126-2 {Ref. 9} obsahující návrh struktury dokladu bezpečnosti pro kolejová vozidla,
(c) viz příloha H.3 pokynů k normě EN 50 126-2 {Ref. 9} obsahující návrh struktury dokladu bezpečnosti pro infrastruktury.

Z pokynů v těchto odkazech vyplývá, že struktura dokladu bezpečnosti pro technické systémy a také jeho obsah závisí na systému, pro který má být prokázán soulad s bezpečnostními předpisy.

Doklad bezpečnosti, který je zhruba popsán v příloze H pokynů k normě EN 50 126-2 {Ref. 9}, uvádí pouze příklady a nemusí být vhodný pro všechny systémy daného typu. Tento nástin je proto třeba používat na základě přiměřeného posouzení, které prvky se hodí pro každou konkrétní aplikaci (zařízení).

[G 5] **Doklad bezpečnosti pro organizační a provozní aspekty železničních systémů:**

V současné době neexistuje žádná zvláštní norma, která by stanovila strukturu, obsah a pokyny pro vyhotovení dokladu bezpečnosti pro organizační a provozní aspekty železničního systému. Avšak vzhledem k tomu, že účelem dokladu bezpečnosti je prokázat standardizovaným způsobem soulad systému s požadavky na bezpečnost, lze použít týž typ struktury bezpečnostního dokladu jako pro technické systémy. Odkazy v bodě [G 4] oddílu 5.1 skutečně podávají doporučení a uvádějí kontrolní seznam položek k řešení, bez ohledu na typ posuzovaného systému. Řízení organizačních a provozních změn vyžaduje týž typ procesů řízení jakosti a řízení bezpečnosti jako technické změny, s prokázáním shody systému s určenými požadavky na bezpečnost. Požadavky stanovené normami CENELEC, které se nevztahují na organizační a provozní aspekty, jsou ty, které se týkají výhradně technických zařízení konstrukce systému, jako například zásady „zabezpečení hardwaru spojeného se systémem proti výpadku“, elektromagnetická kompatibilita (EMC) atd.

5.2. Dokument vypracovaný navrhovatelem podle bodu 5.1. zahrnuje nejméně:

(a) popis organizace a odborníky jmenované pro provádění postupu pro posuzování rizik,
(b) výsledky jednotlivých fází posuzování rizik a seznam všech nezbytných bezpečnostních požadavků, jež je nutno splnit k usměrnění rizika na přijatelnou úroveň.

[G 1] V závislosti na složitosti systému lze tyto důkazní informace soustředit do jednoho nebo do několika dokladů bezpečnosti. Viz body [G 4] a [G 5] oddílu 5.1, kde je uvedena struktura dokladu bezpečnosti pro technické systémy a pro provozní a organizační aspekty.

[G 2] Viz také oddíl A.4. v příloze A, kde jsou uvedeny možné příklady dokladů.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 3] Životní cyklus technických systémů a subsystémů v odvětví železniční dopravy je obecně předpokládán v trvání přibližně 30 let. Během takto dlouhé doby lze také pravděpodobně očekávat řadu významných změn těchto systémů. Další posuzování rizik by tedy mohlo být provedeno pro tyto systémy a jejich rozhraní s doprovodnou dokumentací, která bude muset být přezkoumána, doplněna a předána mezi jednotlivými subjekty a organizacemi, které používají záznamy o nebezpečí. Z toho vyplývají poněkud přísné požadavky na kontrolu dokumentace a řízení konfigurace.

[G 4] Je tedy prospěšné, aby podnik, který archivuje veškeré informace o posuzování rizik a řízení rizik, zaručil, že výsledky/informace budou uloženy na fyzickém médiu, z nějž bude možné tyto informace načíst/které budou dostupné po celou dobu životního cyklu systému) (např. po dobu 30 let).

[G 5] Hlavní důvody pro tento požadavek jsou kromě jiného:

(a) zajistit, aby všechny bezpečnostní analýzy a bezpečnostní záznamy posuzovaného systému byly po celou dobu životního cyklu systému přístupné. Tedy:

(1) v případě dalších významných změn téhož systému bude k dispozici nejaktuálnější systémová dokumentace;
(2) v případě vzniku jakéhokoli problému v době životního cyklu systému je užitečné mít možnost vyhledat související bezpečnostní analýzy a bezpečnostní záznamy;

(b) zajistit, aby byly k dispozici bezpečnostní analýzy a bezpečnostní záznamy posuzovaného systému v případě, že by byl používán v jiné aplikaci jako obdobný referenční systém.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

PŘÍLOHA II NAŘÍZENÍ CSM

Kritéria, která musí splňovat subjekty pro posuzování

1. *Subjekt pro posuzování se nesmí podílet přímo nebo jako zplnomocněný zástupce na návrhu, výrobě, výstavbě, uvádění na trh, provozu nebo údržbě posuzovaného systému. Tímto není dotčena možnost výměny technických informací mezi tímto subjektem a všemi dotčenými účastníky.*
2. *Subjekt pro posuzování musí provádět posouzení na nejvyšší možné úrovni profesionální důvěryhodnosti a nejvyšší možné technické způsobilosti a nesmějí být vystaveni žádnému tlaku a podnětům, zejména finančním, které by mohly ovlivnit jejich rozhodování nebo výsledky jejich posouzení, zejména ze strany osob nebo skupin osob, jichž se posouzení týkají.*
3. *Subjekt pro posuzování musí vlastnit prostředky potřebné pro řádné vykonávání technických a správních úkonů spojených s posuzováním; má rovněž přístup k vybavení potřebnému pro mimořádná posouzení.*
4. *Pracovníci odpovědní za posuzování musí mít:*
   - *řádné technické a odborné vzdělání,*
   - *dostatečnou znalost požadavků na provádění posouzení a odpovídající zkušenosti s posuzováním v této oblasti,*
   - *schopnost vypracovat zprávy o posouzení bezpečnosti, které představují formální závěry provedených posouzení.*
5. *Musí být zaručena nezávislost pracovníků odpovědných za nezávislé posouzení. Jejich odměňování nesmí záviset na počtu provedených posouzení ani na výsledcích těchto posouzení.*
6. *V případě, že je subjekt pro posuzování externím subjektem vůči organizaci navrhovatele, musí uzavřít pojištění odpovědnosti osob, pokud tuto odpovědnost nepřevzal stát v souladu s vnitrostátními právními předpisy nebo pokud tato posouzení neprovádí přímo členský stát.*
7. *V případě, že je subjekt pro posuzování externím subjektem vůči organizaci navrhovatele, pracovníci tohoto subjektu musejí zachovávat služební tajemství, pokud jde o všechny skutečnosti, které se dozví při plnění svých povinností (s výjimkou příslušných správních orgánů ve státě, v němž vykonávají svou činnost) na základě tohoto nařízení.*

[G 1] Další vysvětlení se nepovažuje za nutné.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

PŘÍLOHA A: DOPLŇUJÍCÍ VYSVĚTLENÍ

A.1. Úvod

A.1.1. Účelem této přílohy je přispět ke snazšímu porozumění tomuto dokumentu. Místo poskytování velkého množství informací v hlavním dokumentu je složitější problematika podrobněji vysvětlena v této příloze.

A.2. Klasifikace nebezpečí

A.2.1. V oddílu § 4.6.3. normy EN 50 126-1 {Ref. 8}, a také v příloze B.2 pokynů k normě EN 50 126-2 {Ref. 9}, jsou uvedeny pokyny pro klasifikaci/hierarchizaci nebezpečí.

A.3. Kritérium přijatelnosti rizik pro technické systémy (RAC-TS)

A.3.1. Horní hranice přijatelnosti rizik pro technické systémy

A.3.1.1. Kritérium RAC-TS je popsáno v oddílu 2.5.4. {Ref. 4}.

A.3.1.2. Účelem RAC-TS je určit horní hranici přijatelnosti rizik pro technické systémy, pro které nelze odvodit požadavky na bezpečnost, ani z uplatňování kodexů správné praxe, ani ze srovnání s obdobnými referenčními systémy. Toto kritérium proto definuje referenční bod, z nějž lze kalibrovat metody analýzy rizik pro technické systémy. V souladu s popisem v oddílu A.3.6. přílohy A tohoto dokumentu, tento referenční bod či horní hranici přijatelnosti rizik lze použít také pro určení kritérií přijatelnosti rizik pro jiné funkční selhání technických systémů, které nemají hodnověrný přímý potenciál pro vznik katastrofických důsledků (tj. pro jiné závažné důsledky). RAC-TS ovšem není metodou analýzy rizik.

A.3.1.3. RAC-TS je částečně kvantitativní kritérium. Vztahuje se jak na náhodné poruchy hardwaru, tak na systémové poruchy/chyby technického systému. Systémové poruchy/chyby technického systému, které potenciálně vyplývají z chyb lidského faktoru v průběhu procesu vývoje technického systému (tj. specifikace, konstrukce, provádění a validace), jsou tak rovněž zahrnuty do tohoto kritéria. RACT-TS se ale nevztahuje na chyby lidského faktoru v průběhu provozu a údržby technických systémů.

A.3.1.4. Podle příloh A.3 a A.4 normy CENELEC 50 129, systémové poruchy/chyby systémů nejsou kvantifikovatelné a kvantitativní cíl proto musí být prokazován pouze u náhodných poruch, zatímco systémové poruchy/chyby jsou řešeny kvalitativními metodami[(17)]. *„Vzhledem k tomu, že integritu systémových poruch nelze posuzovat kvantitativními metodami, jsou uplatňovány úrovně systémové integrity pro sdružování metod, nástrojů a technik, které v případě, že jsou používány efektivně, mohou být kvalifikovány jako kritérium v dostatečné míře zaručující realizaci systému na deklarované úrovni integrity.“*

---

(17) *Podle norem CENELEC 50 126, 50 128 a 50 129, kvantitativní údaj, který vyjadřuje náhodné hardwarové poruchy, musí být vždy vázaný na příslušnou úroveň integrity bezpečnosti za účelem usměrňování systematických poruch/chyb. Údaj $10^{-9}\,h^{-1}$ RAC-TS proto také vyžaduje, aby byl zaveden přiměřený proces, který by správně usměrňoval také systémové poruchy/chyby. Pro lepší porozumění této poznámce je třeba uvést, že výše uvedený údaj často označuje pouze náhodné hardwarové poruchy technického systému.*

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

A.3.1.5. Obdobně podle norem CENELEC integrita softwaru technických systémů není kvantifikovatelná. Norma CENELEC 50 128 obsahuje pokyny pro proces vývoje softwaru souvisejícího s bezpečností ve funkci požadované úrovně integrity bezpečnosti. Jedná se o procesy návrhu, ověření, validace a zabezpečení jakosti příslušného softwaru.
Pro programovatelný elektronický řídící systém provádějící bezpečnostní funkce je podle normy CENELEC 50 128 nejvyšší možnou úrovní integrity bezpečnosti pro proces vývoje softwaru hodnota SIL 4, což odpovídá kvantitativní přípustné intenzitě nebezpečí $10^{-9}\ h^{-1}$.

A.3.1.6. Vzhledem k tomu, že systémové poruchy/chyby nelze kvantifikovat, je třeba je místo toho usměrňovat kvalitativně zavedením procesů řízení jakosti a řízení bezpečnosti, které musí být slučitelné s úrovní integrity bezpečnosti pro posuzovaný systém.

(a) účelem procesu řízení jakosti je *„minimalizovat výskyt chyb lidského faktoru v každé fázi životního cyklu systému, a tak omezit riziko systémových chyb systému“,*
(b) účelem procesu řízení bezpečnosti je *„omezit dále výskyt chyb lidského faktoru souvisejících s bezpečností v průběhu životního cyklu systému a minimalizovat tak zbytkové riziko systémových chyb souvisejících s bezpečností.“*

A.3.1.7. Pokyny pro usměrňování výskytu systémových poruch/chyb a rovněž pokyny pro případná konstrukční opatření k ochraně proti poruchám se společnou příčinou/se společným režimem (CCF/CMF), jejichž cílem je zajistit, aby se technický systém dostal v případě výskytu takových poruch/chyb do stavu zabezpečeného proti výpadku, jsou uvedeny v příslušných normách:

(a) Norma CENELEC 50 126-1 {Ref. 8} a průvodce touto normou 50 126-2 {Ref. 9} uvádějí přehled článků normy CENELEC 50 129 a jejich použitelnost pro zdokumentovanou evidenci jiných systémů než jsou zabezpečovací systémy: viz tabulka 9.1 v pokynů k normě 50 126-2 {Ref. 9}. Tento seznam obsahuje odkaz na pokyny, jak řešit chyby vyplývající ze systému jako takového a účinek prostředí na posuzovaný systém.

Například techniky/opatření pro konstrukční charakteristiky jsou obsaženy v *„Tabulce E.5: Konstrukční charakteristiky (uvedené v oddílu 5.4)* normy CENELEC 50 129 {Ref. 7}, *„za účelem zamezení chybám a usměrňování chyb, jež jsou způsobeny:*

(1) *„jakýmikoli zbytkovými konstrukčními chybami“;*
(2) *„oklními podmínkami“;*
(3) *„zneužitím nebo provozními chybami“;*
(4) *„jakýmikoli zbytkovými chybami softwaru“;*
(5) *„lidským faktorem“;*

Přílohy D a E normy CENELEC 50 129 {Ref. 7} prezentují techniky a opatření k zamezení systémovým chybám a usměrňování náhodných hardwarových a systémových poruch/chyb u elektronických zabezpečovacích systémů souvisejících s bezpečností. Mnohé z nich lze rozšířit na jiné systémy, než jsou systémy zabezpečovací, a to prostřednictvím odkazu na tyto pokyny v tabulce 9.1 pokynů k normě 50 126-2 {Ref. 9}.

(b) Norma CENELEC 50 128 obsahuje pokyny pro proces vývoje softwaru souvisejícího s bezpečností ve funkci úrovně integrity bezpečnosti (od SIL 0 do SIL 4), která je požadována pro software posuzovaného systému.

A.3.1.8. Kritérium RAC-TS představuje také nejvyšší úroveň integrity, kterou lze požadovat podle norem CENELEC a IEC. Pro snazší orientaci jsou citovány požadavky z norem IEC 61508-1 a CENELEC 50 129:

(a) IEC 61508-1: *„Tato norma stanoví dolní hranici cílových bezpečnostních opatření týkajících se poruch v nebezpečném poruchovém režimu, již lze vyžadovat. Tato opatření jsou určena jako dolní hranice pro úroveň bezpečnosti 4. Je možné, že by se*

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

podařilo dosáhnout konstrukce systémů souvisejících s bezpečností s nižšími hodnotami pro cílová bezpečnostní opatření týkající se poruch u systémů, které nejsou složité, ale vychází se z předpokladu, že údaje v tabulce představují hranici, jíž lze v současné době docílit u poměrně složitých systémů (například programovatelné elektronické systémy související s bezpečností).“

(b) Norma EN 50129: *„K funkci, která má kvantitativní požadavky náročnější než 10^{-9} h^{-1}, by se mělo přistupovat jedním ze dvou následujících způsobů:*

(1) *pokud je možné funkci rozdělit do funkčně nezávislých podfunkcí, přípustnou intenzitu nebezpečí (THR) lze rozdělit mezi tyto podfunkce a každé podfunkci může být přiřazen příslušný faktor SIL;*

(2) *pokud tuto funkci nelze rozdělit, mělo by být vyhověno alespoň opatřením a metodám požadovaným pro SIL 4, a tato funkce by měla být použita v kombinaci s jinými technickými a provozními opatřeními, aby bylo dosaženo nezbytné přípustné intenzity nebezpečí.“*

A.3.1.9. Všechny technické systémy pak musí omezit kvantitativní požadavek na bezpečnost na tento údaj. Pokud existuje potřeba vyšší míry ochrany, nelze jí dosáhnout pouze v rámci jednoho systému. Architektura systému musí být změněna, například zavedením dvou různých souběžných systémů, které provádějí vzájemnou kontrolu vytváření bezpečných výstupů. To ovšem rozhodně zvyšuje náklady na vývoj technického systému.

Poznámka: Pokud jsou zavedeny bezpečnostní funkce, např. čistě mechanické systémy, které na základě provozní zkušenosti případně mohly dosáhnout vyšší míry integrity, pak může být úroveň bezpečnosti charakterizována příslušným kodexem správné praxe nebo mohou být požadavky na bezpečnost stanoveny na základě analýzy podobnosti s existujícím systémem. V rámci CSM je třeba použít kritérium RAC-TS pouze v případě, že neexistuje žádný kodex správné praxe ani referenční systém.

A.3.1.10. Souhrnně tedy můžeme konstatovat, že:

(a) podle norem CENELEC 50 126, 50 128 a 50 129, systémové poruchy/chyby vývojových procesů nejsou kvantifikovatelné,

(b) výskyt systémových poruch/chyb a také jejich zbytkové riziko, musí být usměrňovány a řízeny uplatňováním vhodných procesů řízení jakosti a řízení bezpečnosti, které musí být kompatibilní s úrovní integrity bezpečnosti požadovanou pro posuzovaný systém,

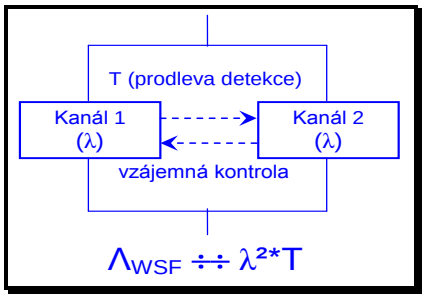
(c) nejvyšší dosažitelnou úrovní integrity bezpečnosti je SIL 4, a to jak pro náhodné poruchy hardwaru, tak pro systémové poruchy/chyby technických systémů,

(d) z této úrovně integrity bezpečnosti SIL 4 vyplývá, že maximální přípustná intenzita nebezpečí (THR) (tj. maximální přípustná míra selhání) pro technické systémy musí být omezena na 10^{-9} h^{-1}.

A.3.1.11. Přípustnou intenzitu nebezpečí 10^{-9} h^{-1} lze dosáhnout technickým systémem, jenž má buď „architekturu zabezpečenou proti výpadku“ (která samozřejmě tento nárok na bezpečnostní výkonnost splňuje) nebo „redundantní architekturu“ (např. dva nezávislé zpracovatelské kanály, které provádějí vzájemnou kontrolu).

U redundantní architektury lze ukázat, že celková nebezpečná porucha (Λ_{WSF}) technického systému je úměrná λ^2*T kde:

(a) λ^2 představuje druhou mocninu intenzity nebezpečných poruch jednoho kanálu,



obr. 13: Redundantní architektura technického systému.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(b) T představuje čas, který potřebuje jeden kanál na zjištění (detekci) nebezpečné chyby (chyb) druhého kanálu. Bývá obvykle násobkem zpracovatelského času/cyklu kanálu. T bývá obvykle mnohem menší než 1 vteřina.

A.3.1.12. Na základě tohoto vzorce (λ^2*T), lze teoreticky prokázat (pokud uvažujeme pouze náhodné hardwarové poruchy daného technického systému – viz také bod A.3.1.13. v příloze A), že kvantitativní požadavek 10^{-9} h^{-1} je pro kritérium RAC-TS dosažitelný. Systémové poruchy/chyby musí být řízeny prostřednictvím příslušného procesu: viz bod A.3.1.6. v příloze A. Například:

(a) uvažujeme-li ukazatel MTBF (*střední doba v hodinách, po kterou se očekává, že bude zařízení bezchybně fungovat*) v hodnotě 10 000 hodin bezporuchovosti pro jeden kanál a při konzervativním předpokladu, že každá porucha kanálu je nebezpečná, nebezpečná porucha kanálu činí 10^{-4} h^{-1},
(b) i v případě, že uvažujeme dobu 10 minut (tj. $\approx 2*10^{-3}$ hodin) pro zjištění nebezpečné poruchy (poruch) druhého kanálu, což je také konzervativní předpoklad.

Celková nebezpečná porucha činí $\Lambda_{WSF} \approx 2 * 10^{-10}$ h^{-1}.

A.3.1.13. V praxi musí pro takovou redundantní architekturu hodnocení kvantitativních celkových nebezpečných hardwarových poruch zohlednit opatření, která jsou přijata v oblasti konstrukce k ochraně proti poruchám se společnou příčinou/se společným režimem (CCF/CMF) a zajistit, aby se technický systém dostal v případě výskytu takových poruch/chyb do stavu zabezpečeného proti výpadku. Toho hodnocení celkové nebezpečné poruchy (Λ_{WSF}) musí tak vzít v úvahu také následující faktory:

(a) konstrukční části společné pro všechny kanály, např. jednoduché nebo společné vstupy do všech kanálů, společný napájecí zdroj, srovnávací obvody, voliče atd.,
(b) dobu potřebnou pro zjištění skrytých poruch. U složitých technických systémů může být tato doba o několik řádů vyšší než 1 vteřina,
(c) dopad poruch se společnou příčinou/se společným režimem (CCF/CMF).

Pokyny týkající se těchto témat lze najít v normách, na které se odkazuje v bodě A.3.1.7. přílohy A tohoto dokumentu.

A.3.2. Vývojový diagram pro zkoušku použitelnosti kritéria RAC-TS

A.3.2.1. Způsob, jak použít kritérium RAC-TS na nebezpečí, která vznikají ze selhání technických systémů je znázorněn na obr. 14.

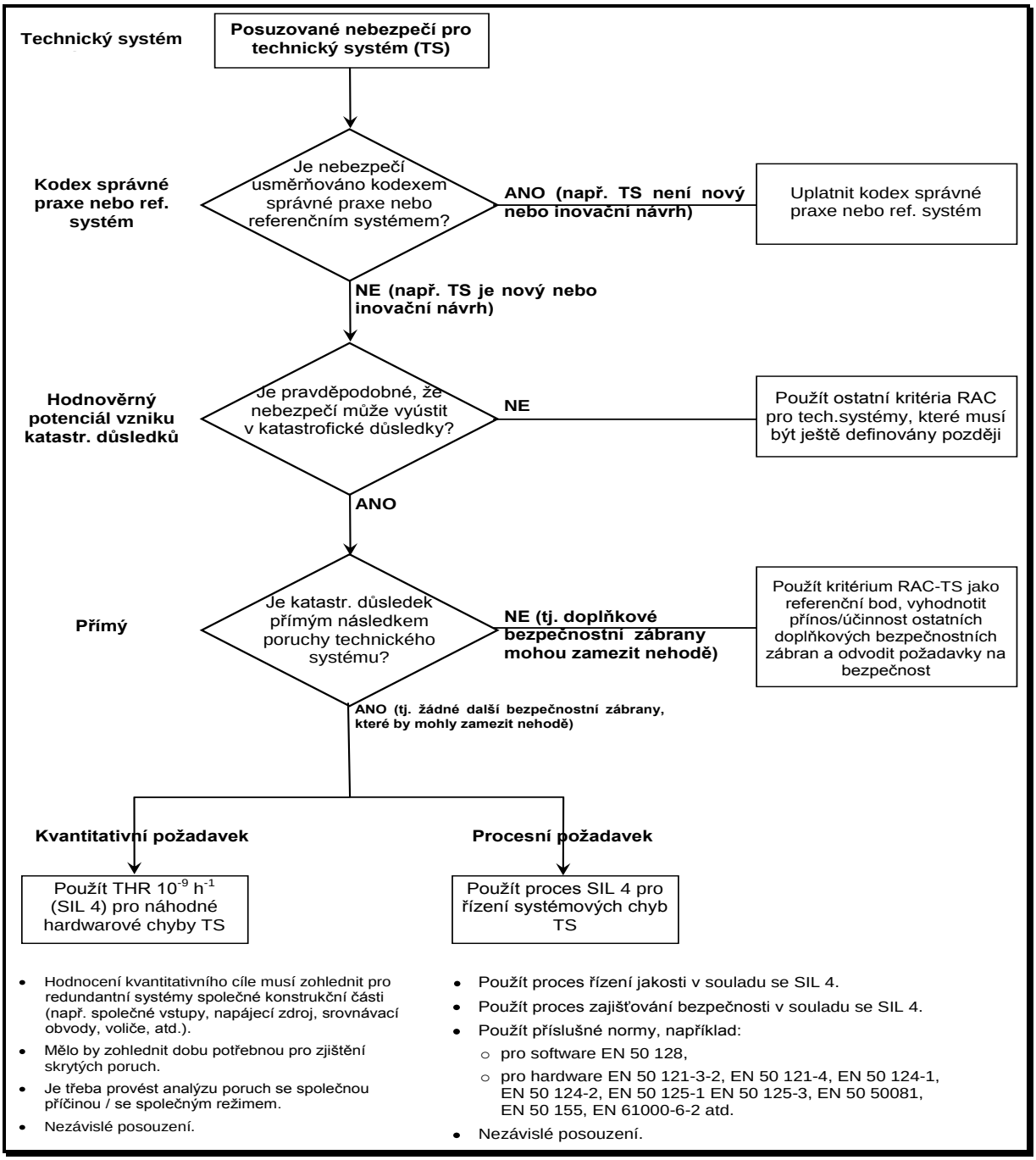
A.3.2.2. Aplikace tohoto vývojového diagramu na konkrétní příklad je uvedena v oddílu C.15. přílohy C.

A.3.3. Definice technického systému v rámci CSM

A.3.3.1. Kritérium RAC-TS se vztahuje pouze na technické systémy. Technický systém je v čl. 3(22) nařízení CSM definován takto:

„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, lidská obsluha a její úkony nejsou do technického systému zahrnuty. Postup údržby je popsán v příručkách údržby, sám o sobě však není součástí technického systému.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu



obr. 14: Vývojový diagram pro zkoušku použitelnosti kritéria RAC-TS.

A.3.4. Vysvětlení definice „technického systému“

A.3.4.1. Následující definice technického systému charakterizuje význam termínu technický systém takto: *„technickým systémem“ se rozumí výrobek nebo soubor výrobků včetně výkresové, prováděcí a podpůrné dokumentace“.* Je tedy tvořen těmito prvky:

(a) fyzické součástky představující technický systém,
(b) případný související software,

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(c) konstrukce a zavádění technického systému, včetně případné konfigurace nebo parametrizace standardního produktu podle speciálních požadavků na konkrétní aplikaci (zařízení),
(d) podkladová dokumentace potřebná pro:

(1) vývoj technického systému;
(2) provoz a údržbu technického systému.

A.3.4.2. Poznámky související s touto definicí dále specifikují další aspekty termínu technický systém:

(a) *„Vývoj technického systému začíná stanovením požadavků a končí jeho schválením“*. Zahrnuje fáze 1 až 10 V-cyklu znázorněné na obr. 10 normy CENELEC 50 126-1 {Ref. 8}.

(b) *„Měl by vzít v úvahu návrh příslušných rozhraní s lidským chováním. lidská obsluha a její úkony však nejsou do technického systému zahrnuty.“* Přestože chyby lidského faktoru v průběhu provozu a údržby technického systému nejsou součástí technického systému jako takového, konstrukce rozhraní s osobami obsluhy (operátorů) je musí vzít v úvahu. Účelem je snížit na minimum pravděpodobnost chyb lidského faktoru kvůli nedostatečné konstrukci příslušných rozhraní s lidskou obsluhou.

(c) *„Údržba nebyla zahrnuta do rozsahu definice termínu technického systému, je však součástí příruček údržby.“* To znamená, že kritérium RAC-TS nemusí být použito na provoz a údržbu technických systémů; ty jsou výrazně závislé na procesech a opatřeních prováděných lidským personálem.
Aby se definice technického systému vztahovala také na údržbu technických systémů, musí zahrnovat všechny příslušné požadavky (např. pravidelná preventivní údržba nebo nápravná údržba v případě poruch), na dostatečné úrovni podrobnosti. Ovšem postup, kterým by měly být potřeby údržby organizovány a naplňovány v souvislosti s příslušným technickým systémem nespadá do definice technického systému, ale do příruček pro údržbu.

A.3.4.3. Viz také oddíl A.3.1. v příloze A.

A.3.5. Funkce technických systémů, na které se vztahuje kritérium RAC-TS

A.3.5.1. Podle definice RAC-TS se toto kritérium vztahuje na nebezpečná selhání funkcí, které má plnit technický systém, jež mohou *„věrohodně **přímo** vést ke katastrofickému důsledku“*: viz oddíl 2.5.4. v {Ref. 4}.

A.3.5.2. Kritérium RAC-TS lze také použít na funkce související s technickými systémy, jejichž selhání **nemohou *„přímo*** *vést ke katastrofickému důsledku“*. V tomto případě musí být kritérium RAC-TS uplatněno jako celkový cíl na soubor událostí, které vedou ke katastrofickým důsledkům. Na základě tohoto celkového cíle musí být odvozena skutečná hodnota, jíž přispívá každá událost k celkové intenzitě selhání, a tudíž intenzita funkčních selhání technického systému, který figuruje v uvažovaném scénáři, podle oddílu A.3.6. v příloze A.
Takové použití RAC-TS však musí být projednáno a odsouhlaseno s pracovní skupinou CSM.

A.3.5.3. Na které funkce technického systému se vztahuje kritérium RAC-TS? Podle normy IEC 61226:2005:

(a) funkce je definována v této souvislosti jako *„konkrétní účel nebo cíl, jehož má být dosaženo, a který lze specifikovat nebo popsat bez odkazu na fyzické prostředky potřebné k jeho dosažení“*,

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(b) funkce (která plní úlohu černé skříňky) převádí vstupní parametry (např. materiál, energii, informace) do výstupních parametrů souvisejících s cílem (např. materiál, energie, informace),
(c) analýza této funkce je nezávislá na její technické realizaci.

A.3.5.4. Kritérium RAC-TS se vztahuje na tyto typy funkcí:

(a) příklady pro palubní subsystém ETCS (*Evropský systém řízení železničního provozu*):

(1) „poskytovat strojvedoucímu informace, které mu umožní řídit vlak bezpečně a v případě překročení dovolené rychlosti zapnout brzdové zařízení“. Na základě informací z trati (dovolená rychlost) a na základě výpočtu rychlosti vlaku palubním ETCS, jsou strojvedoucí a palubní ETCS schopny dohlížet na to, aby vlak nepřekročil dovolenou rychlost. Kritérium RAC-TS se vztahuje na vyhodnocování rychlosti vlaku palubním zařízením vzhledem k tomu, že:

(i) nevzniká žádná další (přímá) zábrana, protože informace poskytované strojvedoucímu jsou také podhodnocené,
(ii) překročení dovolené rychlosti vlaku může vést k vykolejení, což je nehoda, která může mít potenciálně katastrofické důsledky,

(2) „poskytovat strojvedoucímu informace, které mu umožní řídit vlak bezpečně a v případě porušení dovoleného oprávnění k jízdě zapnout brzdové zařízení“;

(b) příklad pro kolejový obvod: „zjistit obsazenost kolejové dráhy“. Kritérium RAC-TS jako takové se bude na tuto funkci vztahovat pouze v případě, že ve funkci stavědla nebude zavedena funkce „sledování posloupnosti“ (*sequence monitoring*),
(c) příklad pro výhybku: „řídit polohu výhybky“.

A.3.5.5. Některé normy také definují funkce, na které by se kritérium RAC-TS mohlo vztahovat. Například:

(a) norma prEN 0015380-4 {Ref. 13} (ModTrain Work) definuje ve své normativní části tři hierarchické úrovně funkcí (rozšířené v přílohách s doplňujícími informacemi až na pět úrovní). Celkově definuje norma prEN 0015380-4 několik stovek funkcí souvisejících s vlaky,
(b) obecně se doporučuje volit funkce z prvních tří úrovní normy prEN 0015380-4 (nikoli však z funkcí nižších) a vzít v úvahu také strukturu členění produktu,
(c) v případě funkcí, které nespadají do oblasti působnosti normy prEN 0015380-4, je třeba rozhodnout o vhodné funkční úrovni na základě srovnání za použití odborného posouzení

Agentura musí dále pracovat na těchto příkladech funkcí z normy prEN 0015380-4 v rámci prací na obecně přijatelných rizicích a kritériích přijatelnosti rizik.

A.3.5.6. Kritérium RAC-TS se vztahuje také například na následující funkci normy prEN 0015380-4: *„řízení naklápění“* (kód = CLB). Tuto funkci lze používat na úrovni systému následujícími dvěma způsoby:

(a) první případ: sklon vlaku má být v zatáčkách měněn za účelem pohodlí cestujících a musí sledovat soulad průjezdného průřezu s infrastrukturou trati,
(b) druhý případ: sklon vlaku má být v zatáčkách měněn pouze za účelem pohodlí cestujících, avšak nemusí sledovat soulad průjezdného průřezu s infrastrukturou trati.

V prvním případě bude kritérium RAC-TS uplatněno, ve druhém však ne, protože selhání funkce naklápění nemá katastrofické důsledky.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

A.3.5.7. Příklad (b) v bodě A.3.5.4. a příklady v bodě A.3.5.6. v příloze A ukazují jasně, že nebude proveditelné vytvářet předem stanovený seznam funkcí, na které se ve všech případech vztahuje kritérium RAC-TS. To bude vždy záviset na tom, jak bude daný systém využívat těchto funkcí subsystému.

A.3.5.8. Příklad uplatňování kritéria RAC-TS je uveden v oddílu C.15. přílohy C.

A.3.6. Příklady uplatňování kritéria RAC-TS

A.3.6.1. Úvod

(a) V této kapitole jsou uvedeny příklady, jak určit míru selhání pro jiné případy závažnosti nebezpečí a jak lze odvodit nižší požadavky na bezpečnost než $10^{-9}\,h^{-1}$. Tento dokument neupřednostňuje ani nepředepisuje žádnou konkrétní metodu. Pouze informuje o způsobu, jímž lze uplatňovat kritérium RAC-TS pro kalibraci některých obecně používaných metod. Je třeba jej dále rozpracovat v rámci činnosti ERA zaměřené na vymezení obecně přijatelných rizik a kritérií přijatelnosti rizik.

(b) Kritérium RAC-TS lze skutečně použít pouze pro malý počet případů, protože v praxi pouze malý počet funkčních selhání technických systémů vede přímo k nehodám s potenciálně katastrofickými důsledky. Aby tedy bylo možné toto kritérium uplatnit pro nebezpečí, které nemá katastrofické důsledky a určit cílovou míru selhání, je možné provést vzájemnou výměnu různých parametrů (např. kalibrací matice rizika u tohoto kritéria), např. závažnosti proti četnosti.

A.3.6.2. Příklad 1: Výměna přímého rizika

(a) kritérium RAC-TS lze použít snadno pro scénáře, které se liší pouze několika nezávislými parametry od referenčních podmínek definovaných v části věnované RAC-TS v oddílu 2.5.4. nařízení CSM {Ref. 3},

(b) předpokládejme, že pro určitý parametr p má vztah k riziku násobný charakter. Dále předpokládejme referenční podmínku p^*, zatímco v alternativním scénáři platí parametr p'. V tomto případě je relevantní pouze poměr (koeficient) parametrů p^*/p' a míra výskytu může být omezena. Tento postup lze opakovat, pokud jsou parametry nezávislé.

(c) Příklad:

(1) předpokládejme, že odborné posouzení stanovilo skutečný potenciál katastrofických důsledků desetkrát nižší než potenciál podle referenčních podmínek v oddílu 2.5.4 nařízení CSM {Ref. 3}. Pak by požadovavaný ukazatel činil $10^{-8}\,h^{-1}$ místo $10^{-9}\,h^{-1}$;

(2) předpokládejme, že je určena bezpečnostní zábrana, kterou zajišťuje jiný technický systém (nezávisle na důsledcích) a která je účinná v 50 % případů;

(3) v tomto případě by požadavek na bezpečnost představoval $5*10^{-7}\,h^{-1}$ (tj. $0{,}5*10^{-8}\,h^{-1}$) místo $10^{-9}\,h^{-1}$.

A.3.6.3. Příklad 2: Kalibrace matice rizika

(a) aby bylo kritérium RAC-TS náležitě uplatňováno v matici rizika, musí se matice vztahovat ke správné úrovni systému (srovnatelné s úrovní stanovenou v oddílu A.3.5. přílohy A),

(b) kritérium RAC-TS definuje v matici rizika jedno pole jako přípustné, což odpovídá této souřadnici (katastrofická závažnost, četnost výskytu $10^{-9}\,h^{-1}$): viz červené pole v tabulce 5. Všechna pole, která se vztahují k vyšší četnosti, musí být označena jako „nepřípustná“. Je třeba poznamenat, že pouze v případě hodnověrného přímého

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

potenciálu vzniku katastrofických důsledků je četnost nehod stejná jako četnost funkčních selhání,

(c) následně lze vyplnit zbytek matice, je však nezbytné vzít v úvahu vlivy jako averze k riziku nebo kalibraci kategorií. V nejjednodušším případě lineární desetinné kalibrace (která je znázorněna šipkou, Tabulka 5), pole označené tímto způsobem jako „přijatelné“ z hlediska kritéria RAC-TS je lineárně extrapolováno do zbytku matice. To znamená, že všechna pole ve stejné úhlopříčce (nebo pod touto úhlopříčkou) jsou také označena jako "přijatelné" riziko. Následující pole lze také označit za „přijatelné“ riziko,

Tabulka 5: Typický příklad kalibrované matice rizika.

Četnost výskytu nehody (způsobené nebezpečím)	**Úroveň rizika**			
Častá (10^{-4} za hodinu)	**Nepřípustné**	**Nepřípustné**	**Nepřípustné**	**Nepřípustné**
Pravděpodobná (10^{-5} za hodinu)	**Nepřípustné**	**Nepřípustné**	**Nepřípustné**	**Nepřípustné**
Příležitostná (10^{-6} za hodinu)	**Přijatelné**	**Nepřípustné**	**Nepřípustné**	**Nepřípustné**
Mizivě pravděpodobná (10^{-7} za hodinu)	**Přijatelné**	**Přijatelné**	**Nepřípustné**	**Nepřípustné**
Nepravděpodobná (10^{-8} za hodinu)	**Přijatelné**	**Přijatelné**	**Přijatelné**	**Nepřípustné**
Krajně nepravděpodobná (10^{-9} za hodinu)	**Přijatelné**	**Přijatelné**	**Přijatelné**	**Přijatelné**
	Nevýznamné	Okrajové	Kritické	Katastrofální
	Úrovně závažnosti důsledků nebezpečí (tj. nehody)			

Hodnocení rizika	**Omezení/usměrnění rizika**
Nepřípustné	Riziko musí být odstraněno.
Přijatelné	Riziko je přijatelné. Je třeba provést nezávislé posouzení.

(d) jakmile je matice vyplněna, může být použita také na nebezpečí, která nemají katastrofické důsledky. Pokud má například jiné funkční selhání závažnost klasifikovanou jako „kritická“, pak podle kalibrované matice rizika by přijatelná četnost nehod neměla být vyšší než „nepravděpodobná“ (či dokonce nižší),

(e) je třeba poznamenat, že použití matice rizika může vést k příliš konzervativním výsledkům, pokud je matice aplikována na četnost funkčních selhání (tj. funkčních selhání, které nevedou přímo k nehodám).

A.3.6.4. Zásada pro kalibraci jiných metod analýzy rizik

Jiné metody analýzy rizik, jako například index RPN (*risk priority number scheme*) nebo graf rizik z VDV 331 či IEC 61508 lze také kalibrovat obdobným postupem, který je uveden v nástinu pro matici rizika:

(a) první krok: klasifikovat referenční bod na základě kritéria RAC-TS v kategorii přijatelného rizika a body s vyšší četností nebo vyšší závažnosti jako nepřípustné z hlediska kritéria RAC-TS,

(b) druhý krok: využít mechanismy výměny (*trade-off*) parametrů u konkrétní metody s cílem extrapolovat přijatelnost rizika do hodnot nebezpečí bez katastrofického potenciálu (za použití výměny lineárních rizik jako výchozího bodu),

(c) třetí krok: pro nebezpečí bez katastrofického potenciálu lze kritérium RAC-TS odvodit z metody analýzy kalibrovaného rizika porovnáním souřadnic (četnosti; závažnosti) s takto získanou FN křivkou.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

A.3.7. Závěry pro kritérium RAC-TS

A.3.7.1. V obecném rámci posuzování rizik navrhovaném CSM jsou nezbytná kritéria přijatelnosti rizik pro stanovení, kdy se zbytková úroveň rizika (rizik) stává přijatelnou, a tudíž kdy má být jednoznačný odhad rizik ukončen.

A.3.7.2. Kritérium RAC-TS je cílovou hodnotou (10^{-9} h^{-1}) pro konstrukci technických systémů.

A.3.7.3. Hlavní účely kritéria RAC-TS jsou:

(a) určit horní hranici přijatelnosti rizik, a tím referenční bod, ze kterého lze kalibrovat metody analýzy rizik pro technické systémy,
(b) umožnit vzájemné uznávání technických systémů vzhledem k tomu, že související riziko a posuzování bezpečnosti bude hodnoceno na základě týchž kritérií přijatelnosti rizik jako ve všech členských státech,
(c) snížit náklady, vzhledem k tomu, že neklade nadměrně vysoké kvantitativní požadavky na bezpečnost,
(d) umožnit konkurenci mezi výrobci. Uplatňování odlišných kritérií přijatelnosti rizik z hlediska funkce, jak v případě navrhovatele, tak členského státu, by vedlo v průmyslu k provádění řady různých prokazování u týchž technických systémů. To by následně ohrozilo konkurenceschopnost výrobců a vedlo k nadměrné nákladnosti výrobků.

A.3.7.4. Částečně kvantitativní požadavek obsažený v kritériu RAC-TS nemusí být u technických systémů vždy prokazován. V rámci CSM je třeba použít kritérium RAC-TS pouze pro technické systémy, u kterých nelze určená nebezpečí přiměřeně usměrňovat ani uplatňováním kodexů správné praxe, ani srovnáním s referenčními systémy. To umožňuje stanovit nižší požadavky na bezpečnost, za předpokladu, že lze zároveň zachovat globální úroveň bezpečnosti.

A.3.7.5. Pouze v případech, kdy neexistují žádné kodexy správné praxe a také žádný referenční systém, je nezbytné uplatňovat harmonizované částečně kvantitativní kritérium přijatelnosti rizik pro technické systémy.

A.3.7.6. Vzhledem k tomu, že úroveň integrity bezpečnosti pro systémové poruchy/chyby je omezena na SIL 4, úroveň integrity bezpečnosti pro náhodné hardwarové poruchy technických systémů musí být také omezena na SIL 4. To odpovídá maximální přípustné intenzitě nebezpečí (THR) 10^{-9} h^{-1} (tj. maximální míře selhání). Podle normy CENELEC 50 129, pokud jsou kladeny vyšší nároky na požadavky na bezpečnost, nelze jim vyhovět pouze v rámci jednoho systému; architektura systému musí být změněna, například zavedením dvou systémů, které nevyhnutelně dramaticky navyšují náklady na příslušný technický systém. Podrobnější informace viz oddíl A.3.1. v příloze A.

A.3.7.7. A konečně, v oddílu A.3.6. přílohy A je v nástinu uveden popis, jak lze RAC-TS použít jako referenční kritérium pro kalibraci konkrétních metod analýzy rizik, jestliže mají technické systémy potenciál vzniku méně závažných důsledků než jsou důsledky katastrofické.

A.4. Důkazy o posuzování bezpečnosti

A.4.1. V tomto oddílu jsou uvedeny pokyny týkající se dokladů, které jsou obvykle poskytovány subjektu pro posuzování za účelem nezávislého posouzení a docílení uznání bezpečnostních opatření/systémů, aniž by tím byly dotčeny vnitrostátní požadavky v příslušném členském státě. Lze je použít jako kontrolní seznam za účelem ověření, že jsou v průběhu uplatňování CSM vzaty v úvahu a zdokumentovány všechny případné související aspekty.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

A.4.2. Plán v oblasti bezpečnosti: Normy CENELEC doporučují, aby byl na začátku projektu vytvořen plán v oblasti bezpečnosti nebo v případě, že to pro daný projekt není vhodné, aby byl v jakémkoli jiném příslušném dokumentu uveden související popis. Pokud jsou na začátku projektu jmenovány subjekty pro posuzování, může být bezpečnostní plán předložen také k jejich vyjádření. Plán v oblasti bezpečnosti v zásadě popisuje tyto skutečnosti:

(a) organizace, která byla zavedena a kvalifikace pracovníků podílejících se na vývoji a na posuzování rizik,
(b) všechny činnosti související s bezpečností, které jsou plánovány v průběhu různých fází projektu, a také očekávané výsledky.

A.4.3. Doklady požadované v rámci fáze vymezení systému:

(a) popis systému:
    (1) vymezení oblasti působnosti/hranic systému;
    (2) popis funkcí;
    (3) popis struktury systému;
    (4) popis provozních a ekologických podmínek;
(b) popis vnějších rozhraní,
(c) popis vnitřních rozhraní,
(d) popis fází životního cyklu,
(e) popis bezpečnostních zásad,
(f) popis předpokladů definujících hranice pro posuzování rizik.

A.4.4. Aby bylo možné uskutečnit posuzování rizik, je při vymezení systému vzat v úvahu kontext zamýšlených změn:

(a) pokud je zamýšlená změna úpravou stávajícího systému, vymezení systému popisuje příslušný systém před provedením změny a také zamýšlenou změnu,
(b) pokud zamýšlená změna představuje konstrukci nového systému, popis se omezuje na vymezení systému, vzhledek k tomu, že neexistuje žádný popis stávajícího systému.

A.4.5. Doklady požadované v rámci fáze určování nebezpečí:

(a) popis a zdůvodnění (včetně omezení) metod a nástrojů pro určování nebezpečí (metoda shora dolů, metoda zdola nahoru, metoda HAZOP atd.),
(b) výsledky:
    (1) seznamy nebezpečí;
    (2) nebezpečí (hranic) systému;
    (3) nebezpečí subsystému;
    (4) nebezpečí rozhraní;
    (5) bezpečnostní opatření, která lze určit v této fázi.

A.4.6. V rámci fáze analýzy rizik je nutné získat také následující důkazy:

(a) pokud jsou pro kontrolu nebezpečí používány kodexy správné praxe, prokázání, že všechny příslušné požadavky z kodexů správné praxe jsou v případě posuzovaného systému splněny. Tím se rozumí také prokázání správného uplatňování příslušných kodexů správné praxe,
(b) pokud jsou pro kontrolu nebezpečí použity obdobné referenční systémy:
    (1) definice požadavků na bezpečnost pro posuzovaný systém z příslušných referenčních systémů;
    (2) prokázání, že posuzovaný systém je používán za obdobných provozních a okolních podmínek jako příslušný referenční systém. Pokud tento krok není proveditelný, prokázání, že odchylky od referenčního systému jsou správně posouzeny;

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(3) důkazy prokazující, že požadavky na bezpečnost z referenčních systémů jsou v posuzovaném systému správně provedeny;

(c) pokud je pro kontrolu nebezpečí použit jednoznačný odhad rizik:

(1) popis a zdůvodnění (včetně omezení) metod a nástrojů pro analýzu rizik (kvalitativní, kvantitativní, částečně kvantitativní, neregresní analýza, ...);
(2) určení stávajících bezpečnostních opatření a faktorů omezování rizika pro každé nebezpečí (včetně aspektů lidského faktoru);
(3) hodnocení a klasifikace rizika pro každé nebezpečí:

(i) odhad důsledků nebezpečí a zdůvodnění (s předpoklady a podmínkami),
(ii) odhad četnosti nebezpečí a zdůvodnění (s předpoklady a podmínkami),
(iii) klasifikace nebezpečí podle jejich kritičnosti a četnosti výskytu,

(4) určení doplňkových vhodných bezpečnostních opatření vedoucích k přijatelným rizikům pro každé nebezpečí (opakovaný proces následně po fázi hodnocení rizika).

A.4.7. Důkazy požadované v rámci fáze hodnocení rizika:

(a) v okamžiku, kdy je proveden odhad rizika:

(1) definice a zdůvodnění kritérií hodnocení rizika pro každé nebezpečí;
(2) prokázání/zdůvodnění faktu, že bezpečnostní opatření a požadavky na bezpečnost zajišťují, aby každé nebezpečí bylo usměrněno na přijatelnou úroveň (podle výše uvedeného kritéria hodnocení rizika);

(b) podle oddílů 2.3.5 a 2.4.3 v nařízení CSM, rizika, která jsou usměrněna uplatňováním kodexů správné praxe a srovnáním s referenčními systémy jsou implicitně považována za přijatelná, za předpokladu, že (viz tečkovaný kruh na obr. 1):

(1) podmínky uplatňování kodexů správné praxe v oddílu 2.3.2 jsou splněny;
(2) podmínky pro uplatňování referenčního systému stanovené v oddílu 2.4.2 jsou splněny.

Pro tyto dvě zásady přijatelnosti rizik jsou kritéria přijatelnosti rizik implicitní.

A.4.8. Důkazy požadované v rámci fáze usměrňování nebezpečí:

(a) důkazy týkající se všech nebezpečí v záznamu o nebezpečí obsahujícím tyto prvky:

(1) určené nebezpečí;
(2) bezpečnostní opatření zamezující vzniku nebezpečí nebo zmírňující jeho důsledky;
(3) požadavky na bezpečnost v souvislosti s těmito opatřeními;
(4) příslušná součást systému;
(5) subjekt odpovědný za bezpečnostní opatření;
(6) stav nebezpečí (např. nevyřešené, vyřešené, odstraněné, přenesené, usměrněné atd.);
(7) datum důkazu, přezkumu a usměrnění každého nebezpečí;

(b) popis způsobu, jakým budou v průběhu celého životního cyklu systému účinně řízena nebezpečí,
(c) popis výměny informací mezi jednotlivými subjekty z hlediska nebezpečí týkajících se rozhraní a přiřazení odpovědnosti.

A.4.9. Důkazy týkající se jakosti procesu hodnocení rizik a posuzování rizik:

(a) popis osob podílejících se na tomto procesu a jejich kvalifikace,
(b) v případě jednoznačných odhadů rizika, popis informací, údajů a jiných statistik používaných v tomto procesu a zdůvodnění jejich přiměřenosti (např. studie citlivosti používaných údajů).

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

A.4.10. Důkazy dodržování požadavků na bezpečnost:

(a) seznam používaných norem,
(b) popis konstrukce a provozních zásad,
(c) důkazy o uplatňování systému řízení jakosti a řízení bezpečnosti pro daný projekt: viz bod [G 3] oddílu 1.1.2,
(d) shrnutí zpráv o bezpečnostních analýzách (např. analýza příčin nebezpečí) prokazující splnění požadavků na bezpečnost,
(e) popis a zdůvodnění metod a nástrojů (FMECA, FTA, …), které se používají pro analýzu příčin nebezpečí,
(f) přehled zkoušek ověřování a validace bezpečnosti.

A.4.11. Doklad bezpečnosti: Norma CENELEC doporučuje, aby všechny typy výše uvedených důkazů byly přeskupeny a shrnuty v rámci jednoho dokumentu, který bude předložen subjektu pro posuzování: viz bod [G 4] a [G 5] oddílu 5.1.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

PŘÍLOHA B: PŘÍKLADY TECHNIK A NÁSTROJŮ PODPORUJÍCÍCH PROCES POSUZOVÁNÍ RIZIK

B.1. Příklady technik a nástrojů pro realizaci činností posuzování rizik, na které se vztahuje CSM, lze najít v příloze E průvodce normy EN 50126-2 {Ref. 9}. Shrnutí technik a nástrojů obsahuje tabulka E.1. Každá technika je popsána a v případě potřeby je zde uveden odkaz na jiné normy, ze kterých lze získat podrobnější informace.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

PŘÍLOHA C: PŘÍKLADY

C.1. Úvod

C.1.1. Účelem této přílohy je přispět ke snazšímu porozumění tomuto dokumentu. Soustřeďuje všechny shromážděné příklady, jejichž účelem je usnadnit uplatňování CSM.

C.1.2. Příklady posuzování rizik nebo posuzování bezpečnosti, které jsou uvedeny v této příloze, nejsou výsledkem uplatňování procesu CSM, vzhledem k tomu, že byly realizovány ještě před vznikem nařízení CSM. Tyto příklady lze klasifikovat následovně:

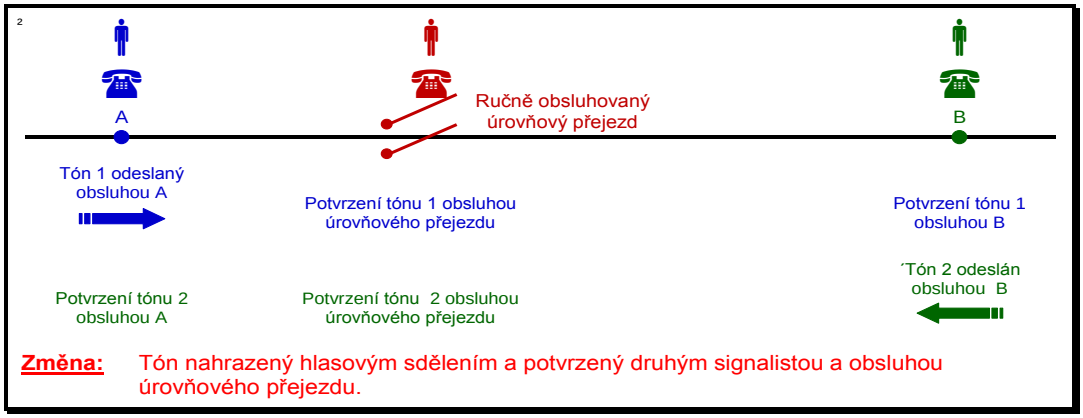
(a) příklady, s odkazem na jejich zdroj, přijaté od odborníků z pracovní skupiny CSM,
(b) příklady, záměrně bez odkazu na jejich zdroj, přijaté také od odborníků z pracovní skupiny CSM. Příslušní odborníci požadovali, aby zdroj zůstal důvěrný,
(c) příklady, jejichž zdroj není uveden a které byly vytvořeny zaměstnanci ERA na základě jejich předchozí osobní odborné zkušenosti.

U každého příkladu je uvedena zjistitelnost ve vztahu mezi uplatňovanými procesem a procesem požadovaným CSM, a rovněž argumentace a přidaná hodnota, kterou lze získat uskutečněním dalších (případných) kroků požadovaných CSM.

C.2. Příklady uplatňování kritérií významných změn v čl. 4 odst. 2

C.2.1. ERA pracuje na definici toho, co lze považovat za „významnou změnu“. Jeden příklad této práce je uveden v tomto oddílu, jak uplatňovat kritéria v čl. 4 odst. 2.

C.2.2. Změna spočívá v úpravě způsobu, kterým na ručně obsluhovaném úrovňovém železničním přejezdu signalisté (hradláři) sdělují informaci o směru přijíždějícího vlaku obsluze úrovňového železničního přejezdu. Tato změna je znázorněna na obr. 15.



obr. 15: Příklad změny, která není významná
Telefonické sdělení pro ovládání úrovňového železničního přejezdu.

C.2.3. Stávající systém: Před provedením zamýšlené změny byla informace o směru přijíždějícího vlaku automaticky oznámena obsluze úrovňového železničního přejezdu vyzváněcím tónem telefonu. Tón byl odlišný podle místa, ze kterého hovor přicházel.

C.2.4. Zamýšlená změna: Vzhledem k tomu, že se původní telefonický systém stává zastaralým a musí být nahrazen novým digitálním, z technického hlediska již příslušnou informaci nelze

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

vyjádřit tónem. Tón je naprosto stejný bez ohledu na to, odkud signalista (hradlář) pochází. Bylo proto rozhodnuto, že téže funkce bude docíleno následujícím provozním postupem:

(a) při odjezdu vlaku signalista informuje ústně obsluhu úrovňového železničního přejezdu o směru přijíždějícího vlaku,
(b) tato informace je ověřena podle jízdního řádu a potvrzena obsluhou úrovňového železničního přejezdu a druhým signalistou, aby se zamezilo případnému nedorozumění ze strany obsluhy.

Zamýšlená změna a související provozní postup jsou znázorněny na obr. 15.

C.2.5. Přestože se tato změna jeví jako změna, která může mít potenciální bezpečnostní dopad, (riziko, že se závora úrovňového železničního přejezdu nezavře včas), ostatní kritéria v čl. 4 odst. 2, jako např:

(a) nízká složitost,
(b) nedostatečná inovace a
(c) snadné sledování,

mohou naznačovat, že zamýšlená změna není významná.

C.2.6. V souvislosti s tímto příkladem je ovšem nezbytné ukázat, že v případě tohoto důležitého úkolu týkajícího se bezpečnosti by nahrazení starého technického systému provozním postupem (se zaměstnanci, kteří provádějí vzájemnou kontrolu) vedlo k obdobné úrovni bezpečnosti. Je otázkou, zda by to vyžadovalo uplatnění úplného procesu CSM, včetně záznamu o nebezpečí, nezávislého posouzení subjektem pro posuzování atd. V tomto případě je sporné, zda by to přineslo jakoukoli přidanou hodnotu, a taková změna by proto nemohla být kvalifikována jako významná.

C.3. Příklady rozhraní mezi subjekty v odvětví železniční dopravy

C.3.1. V následujícím výčtu uvádíme některé příklady rozhraní a důvody ke spolupráci mezi subjekty v odvětví železniční dopravy:

(a) provozovatel infrastruktury – provozovatel infrastruktury: provozovatelé obou infrastruktur by měli například plánovat určitá bezpečnostní opatření pro zajištění bezpečného přejezdu vlaků z jedné infrastruktury do druhé,

(b) provozovatel infrastruktury – železniční podnik: mohly by například existovat speciální provozní předpisy závisející na infrastruktuře, které musí strojvedoucí dodržovat,

(c) provozovatel infrastruktury – výrobce: subsystémy výrobce by mohly mít například omezení použití, která musí provozovatel infrastruktury dodržovat,

(d) provozovatel infrastruktury – poskytovatel služeb: mohly by existovat například konkrétní omezující podmínky týkající se údržby infrastruktury, které musí subdodavatel činností údržby dodržovat,

(e) železniční podnik – výrobce: subsystémy výrobce by mohly mít například omezení použití, která musí železniční podnik dodržovat,

(f) železniční podnik – poskytovatel služeb: mohly by existovat například konkrétní omezující podmínky týkající se údržby infrastruktury, které musí subdodavatel činností údržby dodržovat,

(g) železniční podnik – uživatelé kolejových vozidel: mohla by existovat například speciální omezení použití pro vozidla, která musí dodržovat železniční podnik, jenž tato vozidla provozuje,

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(h) výrobce – výrobce: například řízení technických rozhraní souvisejících s bezpečností mezi subsystémy dvou různých výrobců,

(i) výrobce – poskytovatel služeb: například vedení záznamu o nebezpečí výrobcem, pokud zadává práci subdodavatelsky podniku, který je příliš malý na to, aby měl zavedenou bezpečnostní organizaci posuzovaného projektu,

(j) poskytovatel služeb – poskytovatel služeb: obdobný příklad jako ve výše uvedeném bodě (i).

C.3.2. Poskytovatelé služeb pokrývají všechny činnosti zadané subdodavatelsky provozovatelem infrastruktury, železničním podnikem nebo výrobcem jako je údržba, prodej jízdenek, technické služby atd.

C.3.3. Abychom ilustrovali řízení rozhraní a určení souvisejícího nebezpečí, uvádíme následující příklad. Zabývá se rozhraním mezi výrobcem vlaků a navrhovatelem (železničním podnikem). Popisuje, jakým způsobem by mohla být splněna hlavní kritéria požadovaná vbodě [G 3] oddílu 1.2.1:

(a) vedení: navrhovatel (železniční podnik),

(b) vstupy:

(1) seznam (seznamy) příslušných nebezpečí získaný z obdobných projektů,
(2) popis všech vstupů a výstupů daného rozhraní, včetně charakteristiky výkonnosti,

(c) metody: viz příloha A.2 pokynů k normě EN 50 126-2 {Ref. 9},

(d) požadovaní účastníci:

(1) vedoucí pracovník pro zabezpečení jakosti navrhovatele (železničního podniku),
(1) vedoucí pracovník pro řízení bezpečnosti výrobce vlaků,
(2) projektový útvar navrhovatele vlaků,
(3) projektový útvar výrobce vlaků,
(4) pracovníci údržby navrhovatele vlaků (částečně závisí na analyzovanýchch vstupech/výstupech),
(5) strojvedoucí (částečně závisí na analyzovaných vstupech/výstupech),

(e) výstupy:

(1) zpráva o určení společného dohodnutého nebezpečí,
(2) bezpečnostní opatření pro záznam o nebezpečí s jasným popisem odpovědnosti.

C.4. Příklady metod pro určování obecně přijatelných rizik

C.4.1. Úvod

C.4.1.1. Obecně přijatelná rizika jsou definována v nařízení CSM jako rizika, která jsou *„natolik malá, že není přiměřené provést jakékoli další bezpečnostní opatření (k dalšímu snížení rizika)“*. Pokud jsou při určování nebezpečí některá rizika klasifikována jako spojená s obecně přijatelnými riziky, umožňuje to upustit od dalšího analyzování těchto rizik v dalším procesu posuzování rizik. Definice obecně přijatelných rizik citovaná výše ponechává určitou volnost výkladu. To je také důvod, proč je v nařízení uvedeno, že rozhodnutí o klasifikaci nebezpečí s obecně přijatelnými riziky je ponecháno na odborném posouzení.

C.4.1.2. Je skutečně obtížné definovat obecněji explicitnější kritérium pro obecně přijatelná rizika, které by se vztahovalo na všechny různé potenciální úrovně systému, na nichž by tato nebezpečí mohla být určena, a které by také zohlednilo různé faktory averze k riziku, které mohou převládnout pro různá zařízení. Ovšem vzhledem k tomu, že je důležité zajistit, aby

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

odborná posouzení byla snadno srozumitelná a dohledatelná, určité pokyny, jak definovat rizika jako obecně přijatelná, jsou užitečné. Kritéria pro definování obecně přijatelných rizik mohou být kvantitativní, kvalitativní nebo částečně kvalitativní. V následující pasáži jsou uvedeny příklady, jakým způsobem odvodit kritéria, která umožňují hodnocení obecně přijatelných rizik kvantitativním nebo částečně kvantitativním způsobem.

C.4.1.3. Níže uvedené příklady tuto zásadu ilustrují. Jsou převzaty z přednášky: *Die Gefaehrdungseinstufung im ERA-Risikomanagementprozess", Kurz, Milius, Signal +Draht (100) 9/2008.*

C.4.2. Odvození kvantitativního kritéria

C.4.2.1. Obecně přijatelná rizika bychom mohli definovat jako rizika, která jsou mnohem menší než přijatelné riziko pro danou kategorii nebezpečí. Na základě statistických údajů by bylo možné vypočítat, jaká je běžná (současná) úroveň rizika pro železniční systémy a vypočtenou úroveň označit za přijatelnou. Pokud tuto úroveň rizika vydělíme počtem (N) nebezpečí (např. vycházíme-li z náhodně zvoleného předpokladu, že existuje přibližně N = 100 hlavních kategorií nebezpečí v železničním systému), dostaneme přijatelnou úroveň rizika na jednu kategorii nebezpečí. Dále můžeme konstatovat, že nebezpečí s rizikem, které je o dva řády nižší než přijatelná úroveň rizika na jedno nebezpečí (to je parametr x % v bodě [G 1] oddílu 2.2.3), by bylo považováno za obecně přijatelné riziko.

C.4.2.2. Je však třeba ověřit, že souhrn všech nebezpečí spojených s obecně přijatelným rizikem (riziky) překračuje daný poměr (např. y %) celkového rizika na úrovni systému: viz oddíl 2.2.3 a vysvětlení v bodě [G 2] oddílu 2.2.3.

C.4.3. Hodnocení obecně přijatelných rizik

C.4.3.1. Mezní hodnoty pro obecně přijatelná rizika, odvozená z výše uvedených příkladů, lze následně použít pro kalibraci kvalitativních nástrojů, jako je matice rizika, graf rizika nebo index RPN s cílem pomoci odborníkům při rozhodování o klasifikaci rizika v kategorii obecně přijatelných rizik. Je důležité zdůraznit, že pokud disponujeme kvantitativními hodnotami jako kritérii pro obecně přijatelná rizika, neznamená to, že je nezbytné provést přesný odhad nebo analýzu rizik, abychom mohli rozhodnout o obecné přijatelnosti rizik. Právě v této souvislosti se použije odborné posouzení pro provedení hrubého odhadu ve fázi určování nebezpečí.

C.4.3.2. Je však také důležité ověřit, že souhrn všech nebezpečí spojených s obecně přijatelným rizikem (riziky) nepřekračuje daný poměr (např. y %) celkového rizika na úrovni systému: viz oddíl 2.2.3 a vysvětlení v bodě [G 2] oddílu 2.2.3.

C.5. Příklad posuzování rizik významné organizační změny

C.5.1. **Poznámka:** Tento příklad posuzování rizik nebyl vytvořen v důsledku uplatňování procesu CSM, byl realizován ještě před vznikem CSM. Účelem tohoto příkladu je:

(a) určit podobnosti mezi stávajícími metodami posuzování rizik a procesem CSM,
(b) zajistit odvoditelnost ve vztahu mezi stávajícím procesem a procesem požadovaným podle CSM,
(c) uvést zdůvodnění přidané hodnoty vytvořené provedením dalších případných kroků požadovaných CSM.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Je třeba zdůraznit, že tento příklad je uváděn pouze pro informaci. Jeho účelem je pomoci uživateli porozumět lépe procesu CSM. Ale tento příklad by sám o sobě neměl být převáděn do podoby referenčního systému pro jinou významnou změnu nebo jako takový referenční systém používán. Posuzování rizik by mělo být prováděno pro každou významnou změnu v souladu s nařízením CSM.

C.5.2. Tento příklad souvisí s organizační změnou. Změna byla považována příslušným navrhovatelem za významnou. Pro hodnocení změny byl uplatněn přístup založený na posuzování rizik.

C.5.3. Pobočka organizace provozovatele infrastruktury, která vykonávala až do příslušné změny některé činnosti údržby (kromě zabezpečovacích a telematických funkcí), musela být vystavena konkurenci jiných podniků vyvíjejících činnost v témže oboru. Přímým důsledkem byla potřeba snížení stavu a reorganizace zaměstnanců a úkolů v rámci detašované pobočky organizace provozovatele infrastruktury vystavené konkurenci.

C.5.4. Potenciální zdroje ohrožení pro provozovatele infrastruktury, na kterého měla změna dopad:

(a) zaměstnanci provozovatele infrastruktury na které měla změna dopad, měli na starosti nouzovou údržbu a opravy, které si vyžádaly náhlé chyby v infrastruktuře. Tito zaměstnanci také prováděli některé plánované činnosti údržby nebo činnosti údržby v souvislosti s projekty, jako například podbíjení pražců, čištění štěrkového lože, kontrola vegetace,
(b) tyto úkoly byly považovány za zásadně důležité (kritické) pro bezpečnost a přesnost provozu. Musely proto být analyzovány, aby byla určena správná opatření, která zajistí, že se situace nezhorší, vzhledem k tomu, že mnoho zaměstnanců, kteří mají na starosti bezpečnostní záležitosti, z organizace provozovatele infrastruktury odcházejí,
(c) stejná úroveň bezpečnosti a včasnosti vlaků musí být zachovávána v průběhu změny organizace i po této změně.

C.5.5. Ve srovnání s procesem CSM byly podniknuty tyto kroky (viz také obr. 1):

(a) popis systému [oddíl 2.1.2]:
    (1) popis úkolů vykonávaných stávající organizací (tj. organizací provozovatele infrastruktury před provedením změny);
    (2) popis změn plánovaných v organizaci provozovatele infrastruktury;
    (3) rozhraní „pobočky, která má být detašovaná“ s jinými sousedními organizacemi nebo s fyzickým prostředím bylo možné popsat pouze stručně. Hranice nebylo možné prezentovat zcela jednoznačně;
(b) určení nebezpečí [oddíl 2.2]:
    (1) brainstorming (kolektivní řešení problému) skupiny odborníků:
        (i) s cílem zjistit všechna nebezpečí, s příslušným vlivem na riziko vyvolané zamýšlenou organizační změnou,
        (ii) s cílem určit možná opatření k usměrňování rizik,
    (2) klasifikace nebezpečí:
        (i) ve funkci závažnosti souvisejícího rizika: vysoké, střední, nízké riziko,
        (ii) ve funkci dopadu příslušné změny: zvýšené, nezměněné, snížené riziko,
(c) využívání referenčního systému [oddíl 2.4]:

    systém před změnou byl kvalifikován jako disponující dostatečnou úrovní bezpečnosti. Byl proto použit jako „referenční systém“ pro odvození kritérií přijatelnosti rizik pro změnu organizace,

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(d) jednoznačný odhad a hodnocení rizik [oddíl 2.5]:

Pro každé nebezpečí se zvýšeným rizikem kvůli změně organizace jsou určena opatření k omezení rizika. Zbytkové riziko je porovnáno s kritériem RAC z referenčního systému s cílem ověřit, zda je třeba určit další opatření.

(e) prokázání shody systému s požadavky na bezpečnost [oddíl 3]:

(1) analýza rizik a záznam o nebezpečí prokázaly, že nebezpečí nemohou být usměrňována, dokud nejsou ověřena a dokud není prokázáno, že požadavky na bezpečnost (tj. zvolená bezpečnostní opatření) jsou prováděna;
(2) analýza rizik a záznam o nebezpečí byly otevřené (živé) dokumenty. Účinnost zvolených opatření byla sledována v pravidelných intervalech s cílem ověřit, zda byly podmínky změněny a zda je třeba analýzu rizik a hodnocení rizika aktualizovat;
(3) pokud provedená opatření nebyla dostatečně účinná, analýza rizik, hodnocení rizik a záznam o riziku byly opět aktualizovány a sledovány;

(f) řízení nebezpečí [oddíl 4.1]:

Určená nebezpečí a bezpečnostní opatření byla registrována a vedena v záznamu o nebezpečí. Jedním ze závěrů, který vyplynul z tohoto příkladu, bylo zjištění potřeby průběžně aktualizovat analýzu rizik a záznam o nebezpečí v souvislosti s procesem rozhodování a přijímání opatření v průběhu změny organizace. Analýza rizik zahrnovala také riziko, například na rozhraní se subdodavateli a podnikateli.

Struktura a pole používané pro záznam o nebezpečí, společně s ukázkou některých řádků záznamu, jsou uvedeny v oddílu C.16.2. přílohy C.

(g) nezávislé posuzování [čl. 6]:

Bylo realizováno také nezávislé posouzení třetí stranou s cílem:

(1) ověřit, že bylo správně provedeno řízení rizik a posuzování rizik;
(2) ověřit, že organizační změny jsou vhodné a umožní udržovat stejnou úroveň bezpečnosti jako před provedením změny.

C.5.6. Z tohoto příkladu vyplývá, že zásady požadované na základě společné bezpečnostní metody (CSM) jsou stávající metody v odvětví železniční dopravy, které jsou již uplatňovány pro posuzování rizik organizačních změn. Posouzení rizik v tomto příkladu splňuje všechny požadavky CSM. Uplatňuje dvě ze tří zásad přijatelnosti rizik, které jsou povoleny harmonizovaným přístupem CSM:

(a) „referenční systém“ se používá pro určení kritérií přijatelnosti rizik nezbytných pro hodnocení přijatelnosti rizik organizační změny,
(b) „jednoznačný odhad a hodnocení rizik“ s cílem:

(1) analyzovat odchylky provedených změn od referenčního systému;
(2) určit opatření k omezení rizika pro zvýšené riziko vyplývající z příslušné změny;
(3) zhodnotit, zda bylo dosaženo přijatelné úrovně rizika.

C.6. Příklad posuzování rizik významné provozní změny – změna doby řízení

C.6.1. **Poznámka:** Tento příklad posuzování rizik nebyl vytvořen v důsledku uplatňování procesu CSM, byl realizován ještě před vznikem CSM. Účelem tohoto příkladu je:

(a) určit podobnosti mezi stávajícími metodami posuzování rizik a procesem CSM,
(b) zajistit odvoditelnost ve vztahu mezi stávajícím procesem a procesem požadovaným podle CSM,

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(c) uvést zdůvodnění přidané hodnoty vytvořené provedením dalších případných kroků požadovaných CSM.

Je třeba zdůraznit, že tento příklad je uváděn pouze pro informaci. Jeho účelem je pomoci uživateli porozumět lépe procesu CSM. Ale tento příklad by sám o sobě neměl být převáděn do podoby referenčního systému pro jinou významnou změnu nebo jako takový referenční systém používán. Posuzování rizik by mělo být prováděno pro každou významnou změnu v souladu s nařízením CSM.

C.6.2. Tento příklad představuje provozní změnu, v jejímž rámci chtěl železniční podnik zadat nové trasy a případně novou pracovní dobu (včetně systému směn řidičů a jejich pravidelného střídání).

C.6.3. Ve srovnání s procesem CSM byly podniknuty tyto kroky: (viz také obr. 1):

(a) významnost změny [čl. 4]:

Železniční podnik provedl předběžné posouzení rizik a dospěl k závěru, že provozní změna je významná. Vzhledem k tomu, že strojvedoucí museli řídit vlaky na nových trasách a případně i mimo svou běžnou pracovní dobu, nebylo možné opomíjet možnost, že minou bez zastavení návěst „stůj“, překročí dovolenou rychlost nebo budou ignorovat dočasná omezení rychlosti.

Při porovnání tohoto předběžného posouzení rizik s kritérii uvedenými v čl. 4 odst. 2 nařízení CSM, by tato změna mohla být také kvalifikována jako významná na základě těchto kritérií:

(1) význam z hlediska bezpečnosti: změna souvisí s bezpečností, vzhledem k tomu, že dopad změny způsobu práce strojvedoucích by mohl být katastrofický;
(2) důsledek selhání: výše uvedené chyby strojvedoucích by potenciálně mohly vést ke katastrofickým důsledkům;
(3) nový aspekt změny: železniční podniky by případně mohly zavádět nové způsoby práce pro strojvedoucí;
(4) složitost změny: změna doby řízení by mohla být složitá, protože by to vyžadovalo kompletní posouzení a změnu existujících pracovních podmínek;

(b) vymezení systému [oddíl 2.1.2]:

Vymezení systému původně obsahovalo charakteristiku:

(1) stávajících pracovních podmínek: pracovní doby, systému směn atd.;
(2) změny pracovní doby;
(3) otázek týkajících se rozhraní (např. s provozovatelem infrastruktury).

V průběhu různých opakovaných postupů bylo vymezení systému aktualizováno o požadavky na bezpečnost vyplývající z procesu posuzování rizik. Na tomto opakovaném procesu určování nebezpečí a aktualizace původního vymezení systému se podíleli klíčoví představitelé obsluhy (personálu?).

(c) určení nebezpečí [oddíl 2.2]:

Nebezpečí a možná bezpečnostní opatření byla určena na základě kolektivního řešení (brainstormingu) skupinou odborníků, včetně zástupců strojvedoucích, pro nové trasy a systémy směn. Byly zkoumány úkoly strojvedoucích v kontextu nových podmínek s cílem posoudit, zda mají dopad na strojvedoucí, jejich pracovní vytížení, geografický rámec a dobu systému pracovních směn.
Železniční podnik také uskutečnil konzultace se zaměstnaneckými odbory, aby zjistil, zda mohou poskytnout další informace a přezkoumal riziko únavy a úrovně nemocnosti,

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

které by mohly být vyvolány možným nárůstem přesčasů z důvodu prodlouženého provozu na neznámých trasách.
Každému jednotlivému nebezpečí byla přiřazena určitá úroveň závažnosti rizik a důsledků těchto rizik (vysoká, střední, nízká) a byl přezkoumán dopad navrhovaných změn v kontextu těchto kritérií (tj. zvýšené, nezměněné, snížené) riziko.

(d) použití kodexů správné praxe [oddíl 2.3]:

Pro úpravu stávajících pracovních podmínek a určení nových požadavků na bezpečnost byly použity kodexy správné praxe týkající se pracovní doby a rizik spojených s únavou pracovníků. Pro nový systém pracovních směn byly sestaveny potřebné provozní předpisy. Na přípravě upravených provozních postupů a na dohodě o schválení realizace této změny se podílely všechny zúčastněné strany.

(e) prokázání shody systému s bezpečnostními požadavky [oddíl 3]:

Upravené provozní postupy byly zavedeny do systému řízení bezpečnosti železničního podniku. Tyto postupy byly dále sledovány a byl zaveden proces přezkumu s cílem zajistit, aby určená nebezpečí byla i nadále v průběhu provozování železničního systému správně usměrňována.

(f) řízení nebezpečí [oddíl 4.1]:

Viz výše uvedený bod, pokud jde o železniční podniky, proces řízení nebezpečí může být součástí jejich systému řízení bezpečnosti pro registraci a řízení rizik. Určená nebezpečí byla evidována v záznamu o nebezpečí s požadavky na bezpečnost (tj. odkazem na upravené provozní postupy) usměrňující související rizika.
Upravené postupy byly dále sledovány a v případě potřeby přezkoumány s cílem zajistit, aby určená nebezpečí byla i nadále v průběhu provozování železničního systému správně usměrňována.

(g) nezávislé posouzení [čl. 6]:

Procesy posuzování rizik a řízení rizik byly posouzeny kvalifikovanou osobou železničního podniku, která byla nezávislá na procesu posuzování. Tato kvalifikovaná osoba posoudila proces i jeho výsledky, tj. určené požadavky na bezpečnost.

Železniční podnik založil své rozhodnutí uvést nový systém do provozu na zprávě o nezávislém posouzení vyhotovené kvalifikovanou osobou.

C.6.4. Tento příklad ukazuje, že zásady a proces uplatněné železničním podnikem jsou v souladu se společnou bezpečnostní metodou (CSM). Procesy řízení rizik a posuzování rizik vyhověly všem požadavkům CSM.

C.7. Příklad posuzování rizik významné změny

C.7.1. **Poznámka:** Tento příklad posuzování rizik nebyl vytvořen v důsledku uplatňování procesu CSM, byl realizován ještě před vznikem CSM. Účelem tohoto příkladu je:

(a) určit podobnosti mezi stávajícími metodami posuzování rizik a procesem CSM,
(b) zajistit odvoditelnost ve vztahu mezi stávajícím procesem a procesem požadovaným podle CSM,
(c) uvést zdůvodnění přidané hodnoty vytvořené provedením dalších případných kroků požadovaných CSM.

Je třeba zdůraznit, že tento příklad je uváděn pouze pro informaci. Jeho účelem je pomoci uživateli porozumět lépe procesu CSM. Ale tento příklad by sám o sobě neměl být převáděn

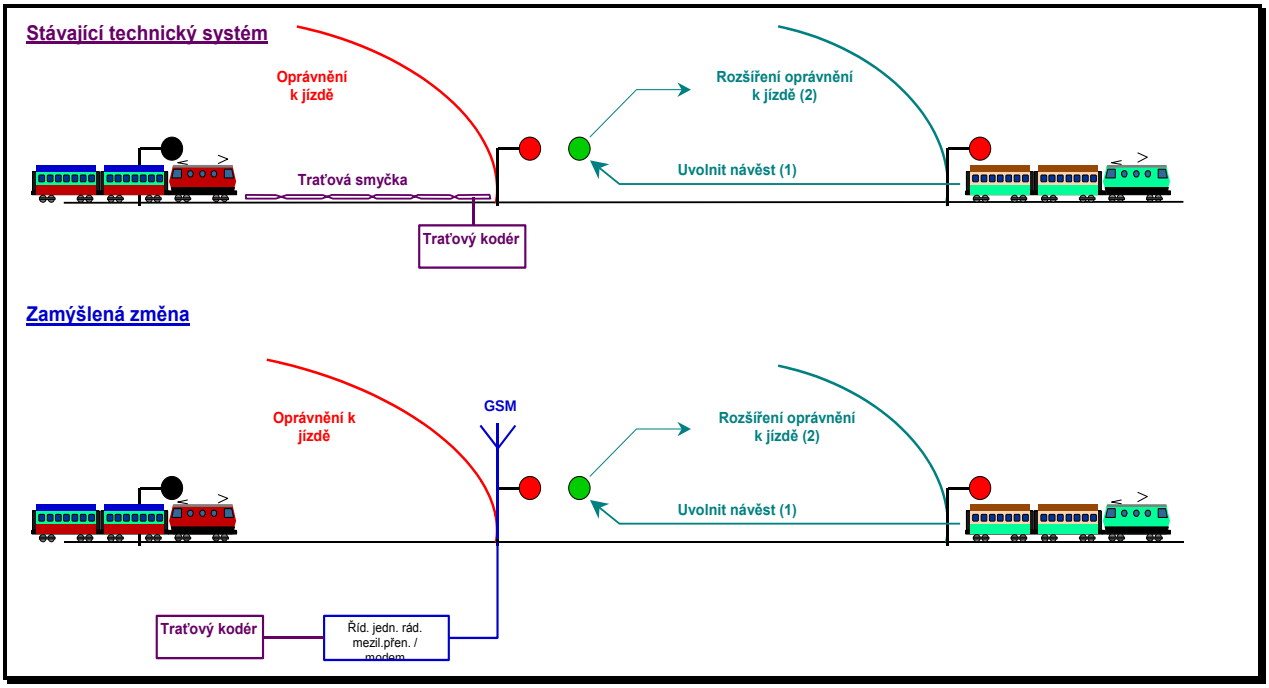
Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

do podoby referenčního systému pro jinou významnou změnu nebo jako takový referenční systém používán. Posuzování rizik by mělo být prováděno pro každou významnou změnu v souladu s nařízením CSM.

C.7.2. Tento příklad se týká technické změny řídícího systému. Příslušný výrobce ji považoval za významnou. Pro hodnocení změny byl uplatněn přístup založený na posuzování rizik.

C.7.3. Popis změny: změna spočívá v nahrazení traťové smyčky umístěné před návěstí prostřednictvím subsystému „rádiový mezilehlý přenos + GSM“ (viz obr. 16).

C.7.4. Potenciální bezpečnostní ohrožení: zachovat úroveň bezpečnosti systému po změně.



obr. 16: Změna traťové smyčky prostřednictvím subsystému rádiového mezilehlého přenosu.

C.7.5. Ve srovnání s procesem CSM byly podniknuty tyto kroky (viz také obr. 1):

(a) posouzení významnosti změny [čl. 4]:

Kritéria v čl. 4 odst. 2 se používají pro posuzování významnosti změny. Pro rozhodnutí, že tato změna je významná, byla určující především kritéria složitosti a nových aspektů změny.

(b) popis systému [oddíl 2.1.2]:

(1) popis existujícího systému: smyčka a její funkce v řídícím systému;
(2) popis změny plánované navrhovatelem a výrobcem;
(3) popis funkčních a fyzických rozhraní smyčky se zbývajícími prvky systému.

Funkce "smyčky+kodéru" ve stávajícím systému spočívá v uvolnění návěsti signalizující blížící se vlak v okamžiku, kdy se úsek za návěstí (tj. před blížícím se vlakem) stane neobsazeným: viz obr. 16.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(c) určení nebezpečí [oddíl 2.2]:

Použije se opakovaný proces posuzování rizik a určování nebezpečí (viz oddíl 2.1.1) na základě kolektivního řešení (brainstormingu) skupinou odborníků s cílem:

(1) určit nebezpečí, s příslušným dopadem na riziko vyvolané zamýšlenou změnou;
(2) určit případná opatření k usměrňování rizik.

S tím jak smyčka, a tím také radiový mezilehlý přenos uvolní návěst, vzniká riziko, že bude poskytnuto nebezpečné oprávnění k jízdě blížícímu se vlaku, zatímco úsek před návěstí je doposud obsazen předchozím vlakem. Riziko musí být usměrněno na přijatelnou úroveň.

(d) použití referenčního systému [oddíl 2.4]:

Systém před provedením změny (smyčka) je kvalifikován jako disponující přiměřenou úrovní bezpečnosti. Používá se proto jako „referenční systém“ pro odvození požadavků na subsystém radiového mezilehlého přenosu.

(e) jednoznačný odhad a hodnocení rizik [oddíl 2.5]:

(1) rozdíly mezi subsystémy „smyčky“ a „rádiového mezilehlého přenosu + GSM“ jsou analyzovány na základě jednoznačného odhadu a hodnocení rizika. Pro subsystém „radiového mezilehlého přenosu + GSM“ byla určena tato nová nebezpečí:

(i) přenos nebezpečné informace hackery ve vzduchové mezeře vzhledem k tomu, že „rádiový mezilehlý přenos + GSM“ je otevřený přenosový subsystém,
(ii) zpožděný přenos nebo přenos přesunutých datových paketů ve vzduchové mezeře,

(2) jednoznačný odhad rizika a používání kritéria RAC-TS pro část řídící jednotky radiového mezilehlého přenosu;

(f) používání kodexů správné praxe [oddíl 2.3]:

(1) norma EN 50159-2 (*Železniční aplikace – Sdělovací a zabezpečovací systémy a systémy zpracování dat – část 2: Komunikace v otevřených přenosových zabezpečovacích systémech*) stanoví požadavky na bezpečnost pro kontrolu nových nebezpečí na přijatelné úrovni, např.:

(i) šifrování a ochrana dat,
(ii) sekvenční zpracování (řazení) zpráv a tzv. časová razítka (*time-stamping*),

(2) například používání normy EN 50 128 pro vývoj softwaru pro řídící jednotku radiového mezilehlého přenosu;

(g) prokázání shody systému s požadavky na bezpečnost [oddíl 3]:

(1) následná kontrola provádění požadavků na bezpečnost prostřednictvím procesu vývoje subsystému "radiového mezilehlého přenosu + GSM";
(2) ověření, že systém, tak jak je konstruovaný a instalovaný, je v souladu s požadavky na bezpečnost;

(h) řízení nebezpečí [článek 4.1]:

Určená nebezpečí, bezpečnostní opatření a výsledné požadavky na bezpečnost vyplývající z posuzování rizik a uplatnění tří zásad přijatelnosti rizik jsou evidovány a vedeny v záznamu o nebezpečí.

(i) nezávislé posouzení [čl. 6]:

Nezávislé posouzení třetí stranou se provádí také za účelem:

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(1) ověření, že postupy řízení rizik a posuzování rizik jsou realizovány správně;
(2) ověření, že technická změna je vhodná a že si systém zachová stejnou úroveň bezpečnosti jako před změnou.

C.7.6. Tento příklad ukazuje, že tři zásady přijatelnosti rizik, které požaduje společná bezpečnostní metoda, se používají jako navzájem se doplňující faktory s cílem definovat požadavky na bezpečnost posuzovaného systému. Posuzování rizik v daném příkladu splňuje všechny požadavky CSM souhrnně znázorněné na obr. 1, včetně vedení záznamu o nebezpečí a nezávislého posouzení bezpečnosti třetí stranou.

C.8. Příklad švédské směrnice BVH 585.30 pro posuzování rizik v železničních tunelech

C.8.1. **Poznámka:** Tento příklad posuzování rizik nebyl vytvořen v důsledku uplatňování procesu CSM, byl realizován ještě před vznikem CSM. Účelem tohoto příkladu je:

(a) určit podobnosti mezi stávajícími metodami posuzování rizik a procesem CSM,
(b) zajistit odvoditelnost ve vztahu mezi stávajícím procesem a procesem požadovaným podle CSM,
(c) uvést zdůvodnění přidané hodnoty vytvořené provedením dalších případných kroků požadovaných CSM.

Je třeba zdůraznit, že tento příklad je uváděn pouze pro informaci. Jeho účelem je pomoci uživateli porozumět lépe procesu CSM. Ale tento příklad by sám o sobě neměl být převáděn do podoby referenčního systému pro jinou významnou změnu nebo jako takový referenční systém používán. Posuzování rizik by mělo být prováděno pro každou významnou změnu v souladu s nařízením CSM.

C.8.2. Účelem tohoto příkladu je porovnat proces CSM se směrnicí BVH 585.30 používanou švédským provozovatelem infrastruktury Banverket pro navržení a ověření dostatečné úrovně bezpečnosti při plánování a výstavbě nových železničních tunelů. Společné body a rozdíly ve vztahu k CSM jsou uvedeny v následujícím výčtu; podrobné požadavky na posuzování rizik lze najít ve směrnici BVH 585.30.

C.8.3. Ve srovnání s procesem CSM na obr. 1:

(a) směrnice BVH 585.30 prezentuje následující společné body:

(1) popis systému [oddíl 2.1.2]:

Směrnice požaduje podrobný popis systému obsahující:

(i) popis tunelu,
(ii) popis trati,
(iii) popis typu kolejových vozidel (včetně doprovodu vlaku),
(iv) popis dopravy a zamýšlených operací,
(v) popis externí asistence (včetně záchranných služeb),

(2) určení nebezpečí [oddíl 2.2]:

Směrnice nepožaduje výslovně určení nebezpečí. Požaduje určení rizika a "katalog nehod" obsahující typy určených potenciálních nehod, u kterých se předpokládá, že by měly významný dopad na úroveň tunelu a které musí být podrobeny následnému posouzení. Příklady nehod:

(i) vykolejení osobního vlaku,
(ii) vykolejení nákladního vlaku,

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(iii) nehoda, ve které figuruje náklad nebezpečných věcí,
(iv) požár ve voze,
(v) srážka mezi osobním vlakem a lehkým/těžkým předmětem
(vi) atd.

(3) neexistuje žádné ustanovení o uplatňování kodexů správné praxe nebo obdobných referenčních systémů. Vychází se z předpokladu, že analýza rizik by měla být provedena v každém případě;

(4) jednoznačný odhad a hodnocení rizik [oddíl 2.5]:

(i) obecně směrnice doporučuje sestavit pro každý typ nehody úplnou stromovou strukturu událostí, na základě kvantitativní analýzy rizik. Ovšem vzhledem k tomu, že záměrem analýzy rizik je analyzovat úroveň globální bezpečnosti tunelu, nikoli analyzovat bezpečnost individuálně na podrobnějších úrovních, důsledky všech scénářů jsou shrnuty s cílem dojít k celkové úrovni rizika pro tunel,
(ii) přijatelnost této úrovně globálního rizika pro tunel musí být porovnána s následujícím kvantitativním explicitním kritériem rizika: *„Železniční doprava na jeden kilometr tunelů musí být stejně bezpečná jako železniční doprava na jeden kilometr otevřených železničních tratí, kromě úrovňových železničních přejezdů“*. Toto kritérium je převedeno do F-N křivky založené na historických údajích o železničních nehodách ve Švédsku a je extrapolováno tak, aby zahrnovalo také důsledky, které nejsou uvedeny ve statistikách,
(iii) vedle tohoto kritéria pro úroveň globálního rizika tunelu, existují také další požadavky, které musí být splněny speciálně v případě evakuace v tunelech a v souvislosti s možnostmi záchranných služeb:

- ověřit, že i za eventuality „hodnověrného scénáře, který by mohl nastat v nejhorším případě“, je možná záchrana vlastními silami při vzniku požáru ve vlaku (kritéria pro toto posuzování jsou také stanovena),
- tunel by měl být naplánován tak, aby pro daný soubor scénářů umožnil záchranné činnosti,

(5) výstup z posuzování rizik [oddíl 2.1.6]:

Výstupy z posuzování rizik jsou:

(i) seznam bezpečnostních opatření na základě minimálních požadavků TSI-SRT a vnitrostátních předpisů, které je třeba použít pro konstrukci tunelu, a;
(ii) všechna další bezpečnostní opatření, která byla analýzou rizik určena jako nezbytná, s uvedením jejich účelu. Ve směrnici se uvádí, že o opatřeních by se mělo rozhodnout podle následujího pořadí priorit:

- zabránit (předcházet) nehodám,
- omezit důsledky nehod,
- usnadnit evakuaci,
- usnadnit záchranné činnosti.

(6) řízení nebezpečí [oddíl 4.1]:

Směrnice nevyžaduje výslovně vedení záznamu o nebezpečí. To souvisí se skutečností, že úroveň posuzování je globální a nebezpečí proto nejsou hodnocena a usměrňována individuálně. Přijatelnost globálního rizika pro tunel je hodnocena, aniž by bylo kritérium přijatelnosti globálního rizika přiřazeno různým typům nehod nebo souvisejícím nebezpečím.

Existuje však seznam všech bezpečnostních opatření, jak těch vyplývajících z požadavku „minimální normy“, tak těch, která byla určena jako nezbytná analýzou

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

rizik: viz výše uvedený bod (a)(5)(ii). V seznamu bezpečnostních opatření by mělo být uvedeno, zda se týkají infrastruktury tunelu, trati, provozu kolejových vozidel a také jaký je jejich zamýšlený účinek podle číslovaného seznamu v bodě (a)(5)(ii). Směrnice však nepožaduje uvést výslovně, jaká nebezpečí bezpečnostní opatření usměrňují a kdo odpovídá za která opatření.

(7) nezávislé posouzení [čl. 6]:

Nezávislé posouzení třetí stranou je závazné za účelem:

(i) kontroly, že proces posuzování rizik doporučený směrnicí BVH 585.30 je realizován správně,
(ii) posouzení přijatelné analýzy rizik,
(iii) kontroly, že je jasně stanoveno, jak by mělo být v rámci projektu prováděno budoucí řízení bezpečnosti.

Konečný dokument analýzy rizik podepisuje nezávislý posuzovatel a také bezpečnostní koordinátor projektu.

(b) Směrnice BVH 585.30 se liší v těchto aspektech:

(1) prokázání shody systému s bezpečnostními požadavky [oddíl 3]:

Směrnice BVH 585.30 nevyžaduje ani sledování, jakým způsobem jsou prováděny určené požadavky na bezpečnost, ani ověřování, že konečná konstrukce tunelu splňuje stanovené požadavky na bezpečnost. Popisuje pouze, jakým způsobem by tyto požadavky měly být předány, aby bylo zaručeno, že budou provedeny ve fázi výstavby.

Směrnice stanoví požadavky na bezpečnost, které mají být používány s cílem ověřit, že analýza rizik byla provedena vhodným a transparentním způsobem a že ji lze pro projekt přijmout.

C.8.4. Závěrem lze konstatovat, že ze srovnání s CSM vyplynuly tyto skutečnosti:

(a) směrnice BVH 585.30 vyhovuje požadavkům stanoveným v příslušných částech CSM, přestože jejich oblast působnosti a účel nejsou přesně stejné,
(b) směrnice BVH 585.30 posuzuje úroveň celkového rizika železničního tunelu,
(c) nebezpečí nejsou usměrňována individuálně a je tak menší důraz na řízení nebezpečí,
(d) požadavek prokázání souladu a ověření správného provádění všech bezpečnostních opatření není stanoven tak výslovně. Ve směrnici se ovšem uvádí, že role bezpečnostního koordinátora v rámci projektu (role a kvalifikace, které jsou požadovány BVH 585.30) spočívá v ověření, že závěry analýzy rizik jsou promítnuty do projektové dokumentace a nákresů a také v kontrole jejich správného provádění ve fázi výstavby;

C.8.5. CSM jsou obecnější než směrnice BVH 585.30 v tom smyslu, že nabízejí uplatňování tří různých zásad přijatelnosti rizik. Ovšem uplatňování směrnice BVH 585.30 v rámci CSM nepředstavuje žádný problém, protože směrnice je slučitelná s použitím třetí zásady jednoznačného odhadu rizika.

C.9. Příklad posuzování rizik na úrovni systému pro kodaňské metro

C.9.1. **Poznámka:** Tento příklad posuzování rizik nebyl vytvořen v důsledku uplatňování procesu CSM, byl realizován ještě před vznikem CSM. Účelem tohoto příkladu je:

(a) určit podobnosti mezi stávajícími metodami posuzování rizik a procesem CSM,
(b) zajistit odvoditelnost ve vztahu mezi stávajícím procesem a procesem požadovaným podle CSM,

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(c) uvést zdůvodnění přidané hodnoty vytvořené provedením dalších případných kroků požadovaných CSM.

Je třeba zdůraznit, že tento příklad je uváděn pouze pro informaci. Jeho účelem je pomoci uživateli porozumět lépe procesu CSM. Ale tento příklad by sám o sobě neměl být převáděn do podoby referenčního systému pro jinou významnou změnu nebo jako takový referenční systém používán. Posuzování rizik by mělo být prováděno pro každou významnou změnu v souladu s nařízením CSM.

C.9.2. Tento příklad se týká úplného a komplexního systému automaticky řízeného metra (bez strojvůdce), včetně souvisejících technických subsystémů (např. subsystém „Vlakové zabezpečovací zařízení“ a subsystém „Kolejová vozidla“) a také provozování a údržby systému. Byl uplatněn přístup založený na posuzování rizik za účelem hodnocení systému a souvisejících subsystémů. Projekt se týkal rovněž osvědčení o uznání SMS podniku, který měl daný systém provozovat. Jedná se o schopnost železničního podniku a provozovatele infrastruktury bezpečně provozovat systém jako celek a zachovávat jeho bezpečnost po celou dobu životního cyklu systému.

C.9.3. Ve srovnání s procesem CSM byly uplatněny tyto kroky (viz také obr. 1):

(a) popis systému [oddíl 2.1.2]:

(1) popis požadavků na výkonnost systému;
(2) popis provozních předpisů;
(3) jasný popis rozhraní a odpovědnosti mezi jednotlivými subjekty, zejména mezi technickými subsystémy;
(4) definice požadavků na systém na obecné úrovni (z hlediska přijatelné četnosti nehod a definice nejnižší prakticky použitelné oblasti, tzv. ALARP);

(b) určení nebezpečí [oddíl 2.2]:

(1) předběžná analýza nebezpečí na úrovni systému;
(2) funkční analýza na úrovni systému kladoucí důraz na všechny subsystémy, nejenom ty, u kterých je bezpečnost zjevně životně důležitá/kritická (např. subsystém „Vlakové zabezpečovací zařízení“ a subsystém „Kolejová vozidla“) a které se podílejí na bezpečnostních funkcích a hrají aktivní roli při řízení bezpečnosti cestujících a doprovodu vlaku;
(3) intenzivní koordinace mezi subjekty (dodavatelé, dodavatelé technických subsystémů a stavebních prací):

(i) určovat systematicky všechna prakticky předvídatelná nebezpečí,
(ii) určovat možná opatření pro usměrnění všech rizik spojených s určenými nebezpečími na přijatelnou úroveň.

(c) používání správné praxe [oddíl 2.3]:

Byly použity odlišné kodexy správné praxe, norem a předpisů, např.:

(1) předpis BOStrab pro projektování a provozování kolejové dopravy ve městech (německý předpis, který se vztahuje na městské systémy kolejové dopravy) a pro provozování automaticky řízených vozů;
(2) normy VDV (*Verband Deutscher Verkehrsunternehmen,* německé kodexy správné praxe) týkající se požadavků na zařízení pro řízení bezpečnosti cestujících na stanicích v případě automaticky řízených vozů;
(3) normy CENELEC pro železniční systémy (EN 50 126, 50 128 a 50 129). Tyto normy se vztahují zejména na technické železniční systémy. Avšak vzhledem k tomu, že obsahují metodický přístup, který má obecnou platnost, byly v hojné míře přijaty pro kodaňské metro:

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(i) norma EN 50 126 se používala pro činnosti řízení bezpečnosti a posuzování rizik celého železničního systému,
(ii) norma EN 50 129 se používala pro celý zabezpečovací systém,
(iii) norma EN 50 128 se používala pro vývoj softwaru (včetně ověření a validace) technických subsystémů;

(4) normy požární ochrany pro tunely (NEPA 130);
(5) normy pro stavební práce (normy Euro Kodex).

(d) používání referenčního systému [oddíl 2.4]:

Metro mělo dosáhnout úrovně bezpečnosti odpovídajících moderních systémů v Německu, ve Francii nebo ve Spojeném království. Tyto existující systémy byly použity jako obdobné referenční systémy pro odvození kritérií přijatelnosti rizik z hlediska přijatelné četnosti nehod pro kodaňské metro.

(e) jednoznačný odhad a hodnocení rizik [oddíl 2.5]:

(1) pro odhad rizik souvisejících s konkrétními nebezpečími;
(2) pro řízení nouzové ventilace v tunelech (včetně lidského faktoru a činnosti požárních sborů);
(3) pro určení opatření k omezení rizika;
(4) pro hodnocení, zda pro celý systém bylo dosaženo přijatelné úrovně rizika;

(f) prokázání shody systému s bezpečnostními požadavky [oddíl 3]:

(1) soulad řídících a technických činností s komplexností systému pro prokázání bezpečnosti systému;
(2) přiřazení požadavků na bezpečnost systému až na úroveň technických subsystémů a stavebních prací a rovněž na všechny funkce metra související s bezpečností;
(3) prokázání, že každý subsystém splňuje, z hlediska konstrukce, požadavky na jeho bezpečnost;
(4) pro bezpečnostní funkce, které vykonává více než jeden subsystém, prokázání shody s požadavky na bezpečnost nemohlo být uzavřeno na úrovni subsystému. Bylo provedeno na úrovni systému prostřednictvím začlenění odlišných subsystémů, nástrojů a postupů;
(5) prokázání, že celkový systém vyhovuje požadavkům na bezpečnost na obecné úrovni;

(g) řízení nebezpečí [oddíl 4.1]:

Určená nebezpečí, související bezpečnostní opatření a výsledné požadavky na bezpečnost byly registrovány a řízeny prostřednictvím ústředního záznamu o nebezpečí. Za tento záznam o nebezpečí odpovídal vedoucí pracovník pro celkovou bezpečnost projektu. Provozní nebezpečí, která vznikla v průběhu projektové fáze a fáze instalace, a také nebezpečí související s provozem a údržbou byla evidována v záznamu o nebezpečí.

(h) důkazy týkající se postupů řízení rizik a posuzování rizik [oddíl 5]:

Výsledky procesu posuzování rizik byly formálně zdokumentovány a opatřeny dokladem bezpečnosti v souladu s požadavky norem CENELEC:

(1) doklad celkové bezpečnosti systému;
(2) doklad bezpečnosti pro každý technický subsystém (včetně zabezpečovacích subsystémů a stavebních prací);
(3) doklad bezpečnosti pro stavební práce (stanice, tunely, viadukty, náspy);
(4) doklad bezpečnosti zařízení;
(5) doklad bezpečnosti vozidel;

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(6) doklad bezpečnosti provozovatele (prokazující osvědčení o uznání SMS železničního podniku a provozovatele infrastruktury, tj, prokázání schopnosti navrhovatele provozovat systém a zajišťovat jeho bezpečnost);

(i) nezávislé posouzení [čl. 6]:

Celkový proces byl podroben následné kontrole a byl posouzen nezávislým posuzovatelem bezpečnosti, který jednal z pověření orgánu pro technický dohled (tj. dánského ministerstva dopravy). Role nezávislého posuzovatele bezpečnosti jsou nastíněny v příslušných kodexech správné praxe. V jejich rámci byly učiněny tyto kroky:

(1) ověření správného řízení rizik a posuzování rizik;
(2) ověření, že systém je vhodný pro daný účel a že bude bezpečně provozován a že bude zachovávána jeho bezpečnost po celou dobu životního cyklu systému;
(3) doporučení, aby byl systém schválen orgánem pro technický dohled.

C.9.4. Projekt jako celek byl podporován vhodným procesem řízení jakosti.

C.9.5. V rámci projektu byly důkazy od dodavatelů (tj. doklady bezpečnosti a podrobná podkladová dokumentace pro technické subsystémy a stavební práce) poskytnuty vedoucímu pracovníkovi pro řízení bezpečnosti navrhovatele. Organizace pro řízení bezpečnosti a nezávislý posuzovatel bezpečnosti, jehož závěry byly zveřejněny ve zprávě o posouzení, následně tyto doklady podrobili přezkumu.
Zpráva o nezávislém posouzení bezpečnosti byla přezkoumána vedoucími pracovníky pro řízení bezpečnosti navrhovatele a byla předložena navrhovateli, který předal všechny soubory orgánu pro technický dohled (tj. dánskému ministerstvu dopravy) ke konečnému schválení.

C.9.6. Tento příklad dokládá, že zásady požadované společnou bezpečnostní metodou představují stávající metody v odvětví železniční dopravy. Posuzování rizik v tomto příkladu splňuje všechny požadavky CSM. Uplatňuje zejména všechny tři zásady přijatelnosti rizik, které povoluje harmonizovaný přístup CSM.

C.10. Příklad směrnice OTIF pro výpočet rizika v rámci přepravy nebezpečných věcí po železnici

C.10.1. **Poznámka:** Tento příklad posuzování rizik nebyl vytvořen v důsledku uplatňování procesu CSM, byl realizován ještě před vznikem CSM. Účelem tohoto příkladu je:

(a) určit podobnosti mezi stávajícími metodami posuzování rizik a procesem CSM,
(b) zajistit odvoditelnost ve vztahu mezi stávajícím procesem a procesem požadovaným podle CSM,
(c) uvést zdůvodnění přidané hodnoty vytvořené provedením dalších případných kroků požadovaných CSM.

Je třeba zdůraznit, že tento příklad je uváděn pouze pro informaci. Jeho účelem je pomoci uživateli porozumět lépe procesu CSM. Ale tento příklad by sám o sobě neměl být převáděn do podoby referenčního systému pro jinou významnou změnu nebo jako takový referenční systém používán. Posuzování rizik by mělo být prováděno pro každou významnou změnu v souladu s nařízením CSM.

C.10.2. Celková filozofie směrnice OTIF je v souladu s účelem CSM, ale tato směrnice má omezenou oblast působnosti. Cílem *„směrnice OTIF je dosáhnout jednotnějšího přístupu posuzování rizik v případě přepravy nebezpečných věcí v členských státech COTIF, a díky*

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

tomu zajistit srovnatelnost jednotlivých posuzování rizik.“ Podporuje tedy vzájemné uznávání posuzování rizik přepravy nebezpečných věcí po železnici mezi členskými státy COTIF.

C.10.3. Ve srovnání s CSM a vývojovým diagramem na obr. 1:

(a) směrnice OTIF prezentuje tyto společné body:

(1) jedná se o společný přístup k posuzování rizik, nicméně založený pouze na jednoznačném odhadu rizika (tj. třetí zásada přijatelnosti rizik CSM);
(2) posuzování rizik OTIF tvoří tyto prvky:

(i) fáze analýzy rizik, která obsahuje:

- fázi určení nebezpečí,
- fázi odhadu rizik,

(ii) fáze hodnocení rizik založená na kritériích (přijatelnosti) rizik, která nejsou doposud harmonizovaná. Tato kritéria mohou být skutečně ovlivňována řadou specifických vnitrostátních rysů,

(b) směrnice OTIF se liší v těchto aspektech:

(1) oblast působnosti jejího uplatňování je odlišná. Zatímco CSM by měly být používány pouze pro významné změny železničního systému, směrnice OTIF by měla být uplatňována pro posuzování rizik přepravy nebezpečných věcí po železnici, ať již se jedná o významnou změnu železničního systému, či nikoliv;
(2) neexistuje možnost volit mezi třemi zásadami přijatelnosti rizik pro usměrňování rizika (rizik). Jedinou povolenou zásadou je zásada třetí, tj. jednoznačný odhad rizika. Kromě toho musí být založena výhradně na kvantitativním odhadu, nikoli na kvalitativním odhadu. Kvalitativní analýza rizik může být vhodná pouze pro srovnání alternativ (bezpečnostních) opatření pro omezení rizik;
(3) je požadováno uplatnění zásady ALARP s cílem určit, zda by další bezpečnostní opatření mohla dále omezit posuzované riziko za přiměřenou cenu;
(4) neexistuje žádná koncepce „nebezpečí spojených s obecně přijatelnými riziky“, která by umožňovala zaměřit činnost posuzování rizik na nebezpečí, která nejvíce přispívají k celkové úrovni rizik. Směrnice ovšem doporučuje omezit počet možných scénářů nehod na přiměřený počet základních scénářů (viz oddíl § 3.2 v {Ref. 10});
(5) tento proces se zaměřuje na posuzování rizik, avšak nezahrnuje:

(i) proces volby a provádění (bezpečnostních) opatření k usměrnění rizika,
(ii) proces přijetí rizika,
(iii) proces prokázání shody systému s bezpečnostními požadavky,
(iv) proces sdělení informace o riziku jiným zainteresovaným subjektům (viz následující body),

(6) nezabývá se vydáváním pokynů ohledně důkazů podle procesu posuzování rizik;
(7) neexistuje žádný požadavek na řízení nebezpečí;
(8) neexistuje žádný požadavek na nezávislé posouzení správného uplatňování společného přístupu, které by provedla třetí strana.

C.10.4. Ze srovnání směrnice OTIF a CSM vyplývá, že jsou obě slučitelné, přestože jejich oblast působnosti a účel přesně neodpovídají. CSM je obecnější než směrnice OTIF, a v tomto smyslu flexibilnější. Na druhé straně CSM se vztahuje také na větší počet činností řízení rizik:

(a) umožňuje uplatňovat tři zásady přijatelnosti rizik, které jsou založeny na stávajících postupech na železnicích: viz oddíl 2.1.4,
(b) uplatňování CSM je požadováno pouze pro významné změny a další analýza rizik je požadována pouze pro nebezpečí, která nesouvisejí s obecně přijatelným rizikem,

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(c) součástí CSM je volba a provádění bezpečnostních opatření, o kterých se předpokládá, že budou usměrňovat určená nebezpečí a související rizika,
(d) harmonizuje proces řízení rizik, včetně:

(1) harmonizace kritérií přijatelnosti rizik, jež je řešena v rámci práce ERA na otázkách obecně přijatelných rizik a kritérií přijatelnosti rizik;
(2) prokázání shody systému s bezpečnostními požadavky;
(3) výsledky a důkazy v rámci procesu posuzování rizik;
(4) výměna informací souvisejících s bezpečností mezi zúčastněnými subjekty na rozhraní;
(5) vedení všech určených nebezpečí a souvisejících bezpečnostních opatření v záznamu o nebezpečí;
(6) nezávislé posouzení správného uplatňování CSM třetí stranou.

C.10.5. Uplatňování směrnice OTIF v rámci CSM (v případě přepravy nebezpečných věcí je pro provozovatele infrastruktury nebo pro železniční podnik významnou změnou) však nepředstavuje žádný problém, protože je slučitelné s použitím třetí zásady pro jednoznačný odhad rizika.

C.11. Příklad posuzování rizik v případě žádosti o schválení nového typu kolejových vozidel

C.11.1. **Poznámka:** Tento příklad posuzování rizik nebyl vytvořen v důsledku uplatňování procesu CSM, byl realizován ještě před vznikem CSM. Účelem tohoto příkladu je:

(a) určit podobnosti mezi stávajícími metodami posuzování rizik a procesem CSM,
(b) zajistit odvoditelnost ve vztahu mezi stávajícím procesem a procesem požadovaným podle CSM,
(c) uvést zdůvodnění přidané hodnoty vytvořené provedením dalších případných kroků požadovaných CSM.

Je třeba zdůraznit, že tento příklad je uváděn pouze pro informaci. Jeho účelem je pomoci uživateli porozumět lépe procesu CSM. Ale tento příklad by sám o sobě neměl být převáděn do podoby referenčního systému pro jinou významnou změnu nebo jako takový referenční systém používán. Posuzování rizik by mělo být prováděno pro každou významnou změnu v souladu s nařízením CSM.

C.11.2. Tento příklad posuzování rizik se týká žádosti o schválení nového typu kolejových vozidel. Analýza rizik byla provedena za účelem hodnocení rizik souvisejících s novým nákladním vagonem.

C.11.3. Změna byla motivována snahou zvýšit účinnost, kapacitu, výkonnost a spolehlivost přepravy volně loženého zboží na konkrétní nákladní trati. Vzhledem k tomu, že vagony byly určeny k přeshraniční dopravě, bylo nutné získat také souhlas různých vnitrostátních bezpečnostních orgánů (NSA). Navrhovatelem byl provozovatel nákladní dopravy, jehož vlastníkem byl zase podnik, který vyráběl zboží, jež mělo být přepravováno.

C.11.4. Práce na projektu zahrnovala konstrukci, výrobu, montáž, uvedení do provozu a ověření nových kolejových vozidel. Byla provedena analýza rizik s cílem ověřit, že nová konstrukce splňuje požadavky na bezpečnost pro každý subsystém a také pro systém jako celek.

C.11.5. V analýze rizik se odkazuje na postupy normy CENELEC EN 50 126 a definice a hodnocení rizik jsou prováděny podle této normy.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.11.6. Ve srovnání s procesem CSM byly uplatněny tyto kroky:

(a) popis systému [oddíl 2.1.2]:

Pro každou z konstrukčních fází byly stanoveny požadavky na dokumentaci ověřování bezpečnosti a popis konstrukce systému:

(1) koncepční fáze: předběžný popis provozních požadavků provozovatele;

(2) specifikační fáze: funkční specifikace, příslušné technické normy, plán testování a ověřování. Součástí této fáze jsou také požadavky provozovatele na používání a údržbu vagonu;

(3) výrobní fáze: technická dokumentace výrobce, včetně nákresů, norem, výpočtů, analýzy atd. Podrobná analýza nových a inovačních konstrukcí nebo nových oblastí použití;

(4) ověřovací fáze:

(i) ověřování technické výkonnosti vagonu výrobcem (zprávy o zkouškách, výpočty, ověření souladu s normami a funkčními požadavky),
(ii) dokumentace o opatřeních omezujících riziko a zprávy o zkouškách za účelem prokázání slučitelnosti vagónů s železniční infrastrukturou,
(iii) údržba a školicí dokumentace, uživatelské příručky atd.,

(5) fáze uznání a přejímky:

(i) prohlášení o bezpečnosti a bezpečnostní důkazy výrobce (doklad bezpečnosti),
(ii) přejímka nákladního vagonu a jeho dokumentace provozovatelem,

(b) určení nebezpečí [oddíl 2.2]:

tento postup byl uplatňován průběžně ve všech fázích konstrukce. Nejprve byl použit přístup „zdola nahoru“, v jehož rámci různí výrobci hodnotili sled rizik vyplývající z poruch součástek v rámci jejich subsystému. Rozdělení na subsystémy mělo tuto strukturu:

(1) podvozek,
(2) brzdový systém,
(3) ústřední spřáhlo,
(4) atd.

Následně byl uplatněn doplňkový přístup „shora dolů“ s cílem najít mezery nebo chybějící informace. Rizika, která nebylo možné okamžitě přijmout, byla převedena do záznamu o nebezpečí za účelem dalšího řešení a klasifikace.

(c) využívání zásad přijatelnosti rizik [oddíl 2.1.4]:

Byl proveden jednoznačný odhad rizika systému jako celku. Pro posuzování jednotlivých nebezpečí však bylo možné použít kodexy správné praxe nebo obdobné referenční systémy. Je prosazována zásada, že každý nový subsystém by měl být bezpečný přinejmenším tak, jako subsystém, který nahrazuje a v důsledku toho je vytvořen nový úplný systém s vyšší úrovní bezpečnosti než u předchozího systému. Pro znázornění určených nebezpečí byla použita matice rizika normy EN50126. Byla také použita různá kritéria přijatelnosti rizik, kromě jiného:

(1) jediná porucha by neměla vést k situaci, která by mohla mít závažný dopad na lidi, materiál nebo okolní prostředí;

(2) pokud této situaci nelze zamezit technickými konstrukčními prostředky, mělo by se předcházet jejímu vzniku provozními předpisy nebo požadavky na údržbu. Tento požadavek se vztahoval pouze na nebezpečí, v případě kterých bylo možné určit vzniklou poruchu ještě před tím, než vytvoří nebezpečnou situaci;

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(3) v případě konstrukčních částí s vysokou pravděpodobností poruchy nebo v těch případech, ve kterých poruchy nelze odhalit předem nebo jim předejít zachováváním provozních předpisů, by měly by být zvažovány další bezpečnostní funkce a zábrany;
(4) redundantní systémy s konstrukčními částmi, u kterých mohou vzniknout neodhalitelné poruchy v průběhu provozu, by měly být chráněny opatřeními údržby, aby se předešlo snížené redundantnosti systémů;
(5) o výsledné konečné úrovni bezpečnosti rozhodlo vedení, které při svém rozhodování vycházelo z kvantitativní a kvalitativní analýzy rizik;

(d) prokázání shody systému s bezpečnostními požadavky [oddíl 3]:

Všechna určená rizika a nebezpečí byla registrována a tento seznam byl průběžně konzultován a aktualizován. Zbývající nebezpečí byla registrována v záznamu o nebezpečí společně s příslušným seznamem opatření k omezení rizik, která měla být přijata v procesu konstrukce, provozování a údržby. Na základě těchto postupů byla vyhotovena závěrečná zpráva o bezpečnosti s ověřením, že požadavky na bezpečnost byly provedeny;

(e) řízení nebezpečí [oddíl 4.1]:

Jak je uvedeno výše, nebezpečí a s nimi související bezpečnostní opatření byla registrována v záznamu o nebezpečí sledujícím všechna určená nebezpečí a bezpečnostní opatření. Nebezpečí související s riziky, která byla přijatelná bez zavádění opatření, však nebyla zařazena do záznamu o nebezpečí;

(f) nezávislé posuzování [čl. 6]:

V dokumentaci přijaté v souvislosti s touto významnou změnou nebyla žádná zmínka o nezávislém posouzení.

C.11.7. Tento příklad posuzování rizik je založen na normě CENELEC EN 50126 a proto je v náležitém souladu s procesem CSM. Posuzování rizik v tomto příkladu vyhovuje všem požadavkům CSM, kromě požadavku na nezávislé posouzení, což nebylo v přijaté dokumentaci jednoznačně vysvětleno. Explicitní kritéria přijatelnosti rizik byla použita a jasně uvedena.

C.12. Příklad posuzování rizik významné provozní změny – vlak obsluhovaný pouze strojvedoucím

C.12.1. **Poznámka:** Tento příklad posuzování rizik nebyl vytvořen v důsledku uplatňování procesu CSM, byl realizován ještě před vznikem CSM. Účelem tohoto příkladu je:

(a) určit podobnosti mezi stávajícími metodami posuzování rizik a procesem CSM,
(b) zajistit odvoditelnost ve vztahu mezi stávajícím procesem a procesem požadovaným podle CSM,
(c) uvést zdůvodnění přidané hodnoty vytvořené provedením dalších případných kroků požadovaných CSM.

Je třeba zdůraznit, že tento příklad je uváděn pouze pro informaci. Jeho účelem je pomoci uživateli porozumět lépe procesu CSM. Ale tento příklad by sám o sobě neměl být převáděn do podoby referenčního systému pro jinou významnou změnu nebo jako takový referenční systém používán. Posuzování rizik by mělo být prováděno pro každou významnou změnu v souladu s nařízením CSM.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.12.2. Tento příklad představuje provozní změnu, v jejímž rámci železniční podnik rozhodl, že vlak bude obsluhován pouze strojvedoucím (vlak obsluhovaný pouze strojvedoucím, *Driver Only Operated*, DOO) na trase, na které před tím působil ještě průvodčí, který pomáhal strojvedoucímu s vypravením vlaku.

C.12.3. Ve srovnání s procesem CSM byly uplatněny tyto kroky (viz také obr. 1):

(a) význam změny [čl. 4]:

Železniční podnik provedl předběžné posouzení rizika, které vyústilo v závěr, že provozní změna je významná. Vzhledem k tomu, že strojvedoucí musel vlak obsluhovat sám, bez pomoci, možné riziko, že cestující by mohli být zachyceni mezi dveřmi nebo spadnout na trať (např. pokud by se dveře otvíraly na špatné straně), nebylo možné ignorovat.

Při srovnání tohoto předběžného posouzení rizika s kritérii čl. 4 nařízení CSM, by tato změna mohla být také klasifikována jako významná, a to na základě těchto kritérií:

(1) relevantnost z hlediska bezpečnosti: změna souvisí s bezpečností, protože dopad požadavku na zcela odlišný způsob řízení provozu vlaku by mohl být katastrofický;
(2) důsledek selhání: případný účinek výkonů strojvedoucího by mohl vést ke katastrofickým důsledkům, pokud není provoz vlaku účinně usměrňován;
(3) nový prvek: provoz vlaku obsluhovaného pouze strojvedoucím by mohl vyžadovat inovační způsoby provozu vlaků, jejichž rizika musí být posouzena;

(b) vymezení systému [oddíl 2.1.2]:

Popsané vymezení systému:

(1) stávající systém vysvětlující jasně, které úkoly plnil strojvedoucí a které ostatní úkoly byly vykonávány doprovodem vlaku (nebo průvodčím), pomáhajícím strojvedoucímu;
(2) změna odpovědnosti strojvedoucího vzhledem k vyřazení doprovodu vlaku;
(3) technické požadavky na systém, které musí řešit změny provozu;
(4) existující rozhraní mezi doprovodem vlaku pomáhajícím strojvedoucímu, strojvedoucím a traťovými zaměstnanci provozovatele infrastruktury.

V průběhu různých opakování bylo vymezení systému aktualizováno o požadavky na bezpečnost vyplývající z procesu posuzování rizik. Na tomto opakovaném procesu určování nebezpečí a aktualizace vymezení systému se podílely klíčové osoby (včetně strojvedoucích, zástupců doprovodu/zaměstnanců a provozovatele infrastruktury).

(c) určení nebezpečí [oddíl 2.2]:

Nebezpečí a možná bezpečnostní opatření byla určena prostřednictvím kolektivního řešení (brainstormingu) skupinou odborníků, včetně, kromě jiných:

(1) zástupců strojvedoucích a doprovodu vlaku/zaměstnanců z hlediska jejich provozní zkušenosti;
(2) zástupců provozovatele infrastruktury, protože změna by mohla mít dopad i na infrastrukturu, například v důsledku změn ve stanicích (např. instalace zrcadel/kamerových systémů na nástupištích).

Podrobně byly zkoumány také další úkoly, které má plnit strojvedoucí, s cílem určit všechna předvídatelná nebezpečí, která by mohla vzniknout následně po vyřazení doprovodu vlaku. Proces určování nebezpečí se zaměřil zejména na otázku, která klíčová provozní nebezpečí by mohla vznikat na stanicích, na existujících trasách, na kterých doprovod vlaku nebo traťoví zaměstnanci byli nápomocni v různých činnostech strojvedoucímu, včetně bezpečného vypravení vlaků, na konkrétní otázky týkající se

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

strojvedoucího, kolejových vozidel (např. kontrola otevírání/zavírání dveří), požadavků na údržbu atd.

Každému z určených nebezpečí byla přiřazena úroveň závažnosti rizik a důsledků (vysoká, střední, nízká) a dopad navrhovaných změn zkoumaných v kontextu těchto kritérií (zvýšené, nezměněné, snížené) riziko.

(d) používání kodexů správné praxe [oddíl 2.3] a používání obdobných referenčních systémů [oddíl 2.4]:

Pro definování požadavků na bezpečnost pro určená nebezpečí byly použity jak kodexy správné praxe (tj. soubor norem pro vlak obsluhovaný pouze strojvedoucím), tak obdobné referenční systémy. Požadavky na bezpečnost se týkaly těchto aspektů:

(1) revidované provozní postupy pro strojvedoucího, které musí zajišťovat bezpečný provoz vlaků bez pomoci jiného personálu;
(2) jakékoli další zařízení nezbytné ve vlaku nebo na trati pro zajištění bezpečného a spolehlivého způsobu vypravení vlaku;
(3) kontrolní seznam, který zajistí vhodnost kabiny strojvedoucího, při zohlednění rozhraní mezi železničním systémem (vlakovým i traťovým) a strojvedoucím.

Potřebné provozní předpisy byly revidovány v souladu s požadavky příslušných kodexů správné praxe a příslušných referenčních systémů. Na revidovaných provozních postupech a na dohodě o pokračování v realizaci změny se podílely všechny potřebné strany.

(e) prokázání shody systému s bezpečnostními požadavky [oddíl 3]:

Systém byl zaveden v souladu s určenými bezpečnostními požadavky (další zařízení a revidované postupy). Ty byly ověřeny jako vhodný prostředek k zajištění dostatečné úrovně bezpečnosti pro posuzovaný systém.

Revidované provozní postupy byly zavedeny do systému řízení bezpečnosti železničního podniku. V případě potřeby byly sledovány a přezkoumány s cílem zajistit, aby určená nebezpečí byla i nadále správně usměrňována v průběhu provozu železničního systému.

(f) řízení nebezpečí [oddíl 4.1]:

Viz výše uvedený bod, pokud jde o železniční podniky, proces řízení nebezpečí může být součástí jejich systému řízení bezpečnosti pro zaznamenávání a řízení rizik. Určená nebezpečí byla registrována v záznamu o nebezpečí, s požadavky na bezpečnost usměrňujícími související riziko, tj. odkazy na další zařízení ve vlaku a na trati a rovněž na revidované provozní postupy.
Revidované postupy byly sledovány a v případě potřeby přezkoumány s cílem zajistit, aby určená nebezpečí byla v průběhu provozování železničního systému i nadále správně usměrňována.

(g) nezávislé posouzení [čl. 6]:

Proces posuzování rizik a proces řízení rizik byly posouzeny kvalifikovanou osobou železničního podniku, která byla nezávislá na procesu posuzování. Kvalifikovaná osoba posoudila proces i jeho výsledky, tj. určené bezpečnostní požadavky.

Železniční podnik vycházel při svém rozhodnutí o uvedení nového systému v platnost ze zprávy o nezávislém posouzení vyhotovené kvalifikovanou osobou.

C.12.4. Tento příklad ukazuje, že zásady a proces uplatněné železničním podnikem jsou v souladu se společnou bezpečnostní metodou. Proces řízení rizik a proces posuzování rizik splnil všechny požadavky CSM.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.13. Příklad používání referenčního systému pro odvození požadavků na bezpečnost pro nové systémy elektronických stavědel v Německu

C.13.1. **Poznámka:** Tento příklad posuzování rizik nebyl vytvořen v důsledku uplatňování procesu CSM, byl realizován ještě před vznikem CSM. Účelem tohoto příkladu je:

(a) určit podobnosti mezi stávajícími metodami posuzování rizik a procesem CSM,
(b) zajistit odvoditelnost ve vztahu mezi stávajícím procesem a procesem požadovaným podle CSM,
(c) uvést zdůvodnění přidané hodnoty vytvořené provedením dalších případných kroků požadovaných CSM.

Je třeba zdůraznit, že tento příklad je uváděn pouze pro informaci. Jeho účelem je pomoci uživateli porozumět lépe procesu CSM. Ale tento příklad by sám o sobě neměl být převáděn do podoby referenčního systému pro jinou významnou změnu nebo jako takový referenční systém používán. Posuzování rizik by mělo být prováděno pro každou významnou změnu v souladu s nařízením CSM.

C.13.2. Za účelem odvození standardních požadavků na bezpečnost pro budoucí systémy elektronických stavědel, Deutsche Bahn (*Německé dráhy*) provedly analýzu rizik již schváleného elektronického systému. Tento systém byl již dříve schválen podle německých kodexů správné praxe (Mü 8004).

C.13.3. Analýza rizik byla provedena v souladu s normami CENELEC (EN 50126 a EN 50129), a zahrnovala tyto kroky:

(a) vymezení systému,
(b) určení nebezpečí,
(c) analýza a kvantifikace nebezpečí.

C.13.4. Pokud jde o vymezení systému, byla věnována péče definování hranic systému, jeho funkcí a rozhraní. Nejnáročnějším úkolem bylo vymezit systém způsobem, který by byl nezávislý na vnitřní architektuře systému stavědla a zároveň zůstal kompatibilní s existujícími systémy stavědel. Zvláštní pozornost byla proto věnována jasnému definování rozhraní s vnějšími systémy, které jsou v interakci se systémem stavědla, aniž by byly podrobně specifikovány vnitřní funkce systému stavědla.

C.13.5. Nebezpečí pak byla určena pouze na rozhraních, aby zůstala standardní (tj. aby zamezila jakékoli závislosti na konkrétních architekturách). Byla posuzována pouze nebezpečí vyplývající z technických chyb. Pro každé rozhraní tak byla určena dvě standardní nebezpečí:

(a) ze stavědla byl přenesen chybný výstup do rozhraní,
(b) (správný) vstup je na rozhraní poškozen.

C.13.6. Těmto standardním nebezpečím pak byla dána pro každé rozhraní konkrétnější charakteristika.

C.13.7. V následující fázi byly hodnoty, kterými části existujícího systému přispěly ke každému určenému nebezpečí, analyzovány a sestaveny do stromové chybové struktury. To umožnilo na základě odhadované míry selhání konstrukčních částí vypočítat intenzitu výskytu každého

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

nebezpečí a použít tyto hodnoty jako přípustné intenzity nebezpečí (THR) pro budoucí generace systémů elektronických stavědel.

C.13.8. Vnitrostátní bezpečnostní orgán (EBA) provedl následnou kontrolu a posouzení analýzy rizik.

C.13.9. V rámci analýzy rizik byla provedena také analýza řídících a zobrazovacích funkcí elektronického systému. Existující schválený systém stavědla byl opět použit jako referenční systém pro odvození požadavků na bezpečnost funkcí obsluhy strojních zařízení (MMI) pro usměrňování náhodných poruch a chyb a pro usměrňování systémových chyb. V důsledku toho byly určeny úrovně integrity bezpečnosti (SIL) pro různé funkce: pro funkce MMI ve standardním režimu, pro funkce MMI v režimu řízení-uvolnění (za zhoršených podmínek), a pro zobrazovací funkčnost.

C.13.10. Vnitrostátní bezpečnostní orgán (EBA) provedl následnou kontrolu a posouzení i v případě této analýzy rizik.

C.13.11. Tyto příklady posuzování rizik ilustrují, jak lze použít druhou zásadu přijatelnosti rizik (referenční systém) CSM pro odvození požadavků na bezpečnost pro nové systémy. Kromě toho byly založeny na normách CENELEC, a proto dobře korespondují s procesem CSM. Posuzování rizik v těchto příkladech splňuje požadavky CSM týkající se fází, na které se vztahují. Avšak vzhledem k tomu, že jejich součástí není žádná konstrukční činnost, není zde ani odkaz na vedení záznamu o nebezpečí, ani prokázání shody posuzovaného systému s určenými požadavky na bezpečnost.

C.13.12. Další informace o těchto analýzách rizik lze najít v těchto dokumentech:

(a) Ziegler, P., Kupfer, L., Wunder, H.: *Erfahrungen mit der Risikoanalyse ESTW (DB AG)*, Signal+Draht, 10, 2003, s. 10–15 a

(b) Bock, H., Braband, J., and Harborth, M.: *Safety Assessment of Vital Control and Display Functions in Electronic Interlockings, in Proc. AAET2005 Automation, Assistance and Embedded Real Time Platforms for Transportation*, GZVB, Braunschweig, 2005, s. 234–253 (Posuzování bezpečnosti životně důležitých řídících a zobrazovacích funkcí u elektronických stavědel, v dokumentu *Proc. AAET2005 Automatizované, asistenční a vložené platformy v reálném čase pro odvětví dopravy*, GZVB, Braunschweig, 2005, s. 234—253).

C.14. Příklad explicitního kritéria přijatelnosti rizik pro řízení provozu vlaku na základě radiového spojení (FFB) v Německu

C.14.1. **Poznámka:** Tento příklad posuzování rizik nebyl vytvořen v důsledku uplatňování procesu CSM, byl realizován ještě před vznikem CSM. Účelem tohoto příkladu je:

(a) určit podobnosti mezi stávajícími metodami posuzování rizik a procesem CSM,
(b) zajistit odvoditelnost ve vztahu mezi stávajícím procesem a procesem požadovaným podle CSM,
(c) uvést zdůvodnění přidané hodnoty vytvořené provedením dalších případných kroků požadovaných CSM.

Je třeba zdůraznit, že tento příklad je uváděn pouze pro informaci. Jeho účelem je pomoci uživateli porozumět lépe procesu CSM. Ale tento příklad by sám o sobě neměl být převáděn do podoby referenčního systému pro jinou významnou změnu nebo jako takový referenční systém používán. Posuzování rizik by mělo být prováděno pro každou významnou změnu v souladu s nařízením CSM.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.14.2. Analýza rizik v souladu s normami CENELEC byla provedena pro zcela nový provozní postup, který byl plánován (ale nikdy nebyl zaveden) v Německu pro konvenční železniční trati. Tato koncepce spočívala v bezpečném zajišťování provozu vlaků pouze prostřednictvím rádiového ovládání (trasy a vlaku). Vzhledem k tomu, že nebyly k dispozici existující kodexy správné praxe (přijaté strojírenské předpisy) a referenční systémy pro takový nový systém, byl proveden jednoznačný odhad rizika za účelem prokázání bezpečnosti tohoto nového postupu. Bylo nutné potvrdit, že úroveň rizika pro cestující z titulu zavedení nového systému by nepřekročila hodnotu přijatelného rizika (explicitní kritérium přijatelnosti rizik).

C.14.3. Toto explicitní kritérium přijatelnosti rizika bylo odhadnuto na základě statistik nehod v Německu, které bylo možné připsat zabepečovacím a řídícím systémům a jeho hodnověrnost byla také ověřena podle kritéria MEM. Takové prokázání bezpečnosti je v souladu s požadavkem německého orgánu EBO docílit „stejné úrovně bezpečnosti“ v případě odchylek od strojírenských předpisů. I tato analýza rizik byla podrobena následné kontrole a posouzení vnitrostátním bezpečnostním orgánem (EBA).

C.14.4. Tento příklad posuzování rizik ukazuje, jak lze odvodit explicitní kritérium globálního rizika (pro třetí zásadu přijatelnosti rizik v CSM) pro nové systémy bez příslušných kodexů správné praxe nebo referenčních systémů. Analýza rizik, která byla následně provedena pro tento nový systém, je založena na normách CENELEC a proto dobře koresponduje s procesem CSM. Posuzování rizik v tomto příkladu splňuje požadavky CSM, není zde ovšem odkaz na vedení záznamu o nebezpečí ani na prokázání souladu posuzovaného systému s určenými požadavky na bezpečnost.

C.14.5. Další informace o této analýze rizik lze najít v dokumentu: Braband, J., Günther, J., Lennartz, K., Reuter, D.: *Risikoakzeptanzkriterien für den FunkFahrBetrieb (FFB)* (Kritéria přijatelnosti rizik pro systém FFB), Signal + Draht, č. 5, 2001, s. 10—15.

C.15. Příklad zkoušky použitelnosti kritéria RAC-TS

C.15.1. Účelem této přílohy je ukázat na příkladu funkce palubního subsystému ETCS, jak používat kritérium v oddílu 2.5.4 a jak určit, zda je kritérium RAC-TS použitelné.

C.15.2. Palubní subsystém ETCS je technický systém. Posuzována je tato funkce: *„poskytnout strojvedoucímu informace, které by mu umožnily řídit bezpečně vlak a v případě překročení dovolené rychlosti zapnout brzdové zařízení“*.

Popis funkce: Na základě informací získaných z trati (dovolená rychlost) a rychlosti vlaku vypočítané palubním systémem ETCS:

(a) strojvedoucí řídí vlak a zajišťuje, aby rychlost vlaku nepřekročila dovolenou rychlost,
(b) palubní subsystém ETCS souběžně dohlíží na to, aby vlak nikdy nepřekročil dovolenou nejvyšší rychlost. V případě překročení dovolené rychlosti automaticky zapíná brzdu.

Strojvedoucí i palubní subsystém ETCS používají vyhodnocení rychlosti vlaku, kterou vypočte palubní subsystém ETCS.

C.15.3. Otázka: „Vztahuje se kritérium RAC-TS na vyhodnocení rychlosti vlaku palubním subsystémem?“

C.15.4. Použití vývojového diagramu na obr. 14 a odpovědi na jednotlivé otázky:

(a) Posuzované nebezpečí pro technický systém:

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

„Překročení bezpečné rychlosti, o němž dostává informaci ETCS“ (viz UNISIG SUBSET 091).

(b) Je možné nebezpečí usměrňovat prostřednictvím kodexu správné praxe nebo referenčního systému?

NE. Vychází se z předpokladu, že systém ETCS je svou konstrukcí nový a inovační. Neexistují proto žádné kodexy správné praxe nebo referenční systémy, které by umožňovaly usměrňovat nebezpečí na úroveň přijatelného rizika.

(c) Je pravděpodobné, že by toto nebezpečí mohlo vyústit v katastrofický důsledek?

ANO, vzhledem k tomu, že *„překročení bezpečné rychlosti, v té podobě, v níž je sdělované systému ETCS“,* může mít za následek vykolejení vlaku, které může potenciálně vést k *„usmrcení a/nebo četným vážným zraněním a/nebo významným škodám na životním prostředí“*.

(d) Je katastrofický důsledek přímým následkem selhání technického systému?

ANO, pokud neexistují žádné další bezpečnostní zábrany. Totéž vyhodnocení rychlosti vlaku, které vypočte palubní subsystém ETCS, má k dispozici strojvedoucí i funkce palubního subsystému ETCS ovládající brzdu. Za předpokladu, že strojvedoucí řídí vlak (z důvodu výkonu) maximální rychlostí, kterou trať povoluje, pak tedy ani strojvedoucí, ani palubní subsystém ETCS neodhalí, že vlak překročil dovolenou rychlost, pokud je údaj o rychlosti vlaku podhodnocený. Taková situace představuje potenciální ohrožení vykolejením vlaku s katastrofickými důsledky.

(e) Závěry:

(1) pro kvantitativní požadavky: použijte THR 10^{-9} h^{-1} pro náhodné hardwarové poruchy palubního subsystému ETCS s cílem zajistit, aby:

(i) hodnocení tohoto kvantitativního cíle zohlednilo pro redundantní systémy společné konstrukční části (např. jednoduché nebo společné vstupy do všech kanálů, společný napájecí zdroj, srovnávací obvody, voliče atd.),
(ii) doba zjištění skrytých poruch byla zohledněna,
(iii) byla provedena analýza poruch se společnou příčinou/se společným režimem (CCF/CMF),
(iv) bylo provedeno nezávislé posouzení,

(2) pro požadavky na procesy: použijte proces SIL 4 pro řízení systémových poruch/chyb palubního subsystému ETCS. To vyžaduje uplatňování:

(i) procesu řízení jakosti v souladu se SIL 4,
(ii) procesu řízení bezpečnosti v souladu se SIL 4,
(iii) příslušných norem, např.:

- pro vývoj softwaru je třeba použít normu EN 50 128,
- pro vývoj hardwaru je třba použít normy EN 50 121-3-2, EN 50 121-4, EN 50 124-1, EN 50 124-2, EN 50 125-1 EN 50 125-3, EN 50 50081, EN 50 155, EN 61000-6-2,

(3) nezávislé posouzení procesu (procesů).

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.16. Příklady možného členění záznamu o nebezpečí

C.16.1. Úvod

C.16.1.1. Minimální požadavky, které mají být registrovány v záznamu o nebezpečí, jsou určeny v oddílu 4.1.2 nařízení CSM. Jsou vyznačeny stínovaným pozadím u příkladů záznamů o nebezpečí uvedených v následujících pasážích tohoto dokumentu.

C.16.1.2. Mohou existovat různé způsoby, jak členit záznam o nebezpečí, a také jakékoli další informace, které by mohly charakterizovat příslušná nebezpečí a související bezpečnostní opatření. Pro nebezpečí a související bezpečnostní opatření může být například vyčleněno jedno pole na jednu položku informace. Ať je však použito jakékoli členění, je důležité, aby záznam o nebezpečí uváděl jasné vazby mezi nebezpečími a souvisejícími bezpečnostními opatřeními. Jedním z možných řešení je, aby záznam o nebezpečí obsahoval pro každé nebezpečí a pro každé bezpečnostní opatření, alespoň pole s:

(a) jasným popisem, včetně odkazů na jeho zdroj a na zásadu přijatelnosti rizik zvolenou pro usměrňování souvisejícího nebezpečí. Toto pole umožňuje porozumět příslušnému nebezpečí a souvisejícím bezpečnostním opatřením a také zjistit, ve kterých analýzách bezpečnosti jsou určena.

Vzhledem k tomu, že záznam o nebezpečí se používá a vede po celou dobu životního cyklu systému (tj. v průběhu provozu a údržby systému), je prospěšné, aby existovala jasná zjistitelnost vztahu nebo vazba mezi každým nebezpečím a:

(1) souvisejícím rizikem,
(2) příčinami nebezpečí, pokud jsou již určeny,
(3) souvisejícími bezpečnostními opatřeními a rovněž předpoklady definujícími hranice posuzovaného systému,
(4) souvisejícími analýzami bezpečnosti, ve kterých je nebezpečí určeno.

Kromě toho musí být jasná a dostatečná formulace bezpečnostních opatření (zejména těch, která mají být přenesena na jiné subjekty než na navrhovatele). Termín „jasná a dostatečná“ znamená, že lze porozumět bezpečnostním opatřením i souvisejícím nebezpečím, a také otázce, jaká rizika mají tato opatření usměrňovat, aniž by bylo třeba vracet se do souvisejících analýz bezpečnosti.

(b) zásada přijatelnosti rizik použitá pro usměrňování nebezpečí s cílem podporovat vzájemné uznávání a pomoci subjektu pro posuzování posoudit správné uplatňování CSM,

(c) jasná informace o stavu: V tomto poli se uvádí, zda je související nebezpečí/bezpečnostní opatření doposud otevřené nebo usměrněné/podrobené validaci.

(1) otevřené nebezpečí/bezpečnostní opatření je sledováno, dokud není usměrněno/podrobeno validaci;
(2) na druhou stranu, usměrněná nebezpečí/bezpečnostní opatření nebo nebezpečí/bezpečnostní opatření podrobená validaci již nejsou sledována, pokud nedojde k významným změnám v provozu nebo údržbě systému: viz bod [G 6](b) v oddílu 2.1.1. Pokud k těmto změnám dojde:

(i) CSM se opět uplatní na požadované změny v souladu s čl. 2. Viz také bod [G 6](b)(1) v oddílu 2.1.1,
(ii) všechna usměrněná nebezpečí a bezpečnostní opatření jsou opětovně posouzena s cílem ověřit, že příslušné změny na ně nemají dopad. Pokud na ně dopad mají, související nebezpečí a bezpečnostní opatření jsou znovu otevřena a vedena v záznamu o nebezpečí.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Může se stát, že jsou zavedena odlišná bezpečnostní opatření místo opatření registrovaných v záznamu o nebezpečí (např. z důvodu nákladů). Zavedená bezpečnostní opatření jsou následně registrována v záznamu o nebezpečí s důkazy/zdůvodněním, proč jsou vhodná a prokázáním, že s těmito opatřeními systém vyhovuje požadavkům na bezpečnost.

(d) odkaz na související důkazy o usměrnění nebezpečí nebo validaci bezpečnostního opatření: Toto pole umožňuje dohledat později důkazy o schválení postupu usměrňování určitého nebezpečí a o validaci souvisejícího bezpečnostního opatření (bezpečnostních opatření),

Nebezpečí může být usměrněno v záznamu o nebezpečí pouze v případě, že všechna související bezpečnostní opatření, která jsou spojena s tímto nebezpečím, jsou podrobena validaci předem.

(e) organizace nebo subjekt (subjekty) odpovědné za řízení tohoto nebezpečí.

C.16.1.3. Další příklad možného obsahu záznamu o nebezpečí je uveden v příloze A.3. pokynů k normě EN 50126-2 {Ref. 9}.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.16.2. Příklad záznamu o nebezpečí pro organizační změnu v oddílu C.5. v příloze C

Tabulka 6: Příklad záznamu o nebezpečí pro organizační změnu v oddílu C.5. v příloze C.

Popis nebezpečí	**Bezpečnostní opatření**	**Priorita/ Bezpečnost Včasnost**	**Provádění**[18]	**Poznámky**	**Odpo-vědnost** [18]	**Zdroj**	**Použitá zásada přijatelnosti rizik**	**Odpo-vědnost za ověření**	**Způsob ověření**	**Stav xx.xx.xx**
Snížená motivace mezi zaměstnanci, kteří zůstali v podniku. Proces odchodu zaměstnanců tak neustále pokračuje. Demotivovaní / vyčerpaní vedoucí pracovníci	Nové kolo motivační práce pro zaměstnance, která musí být realizována v menších skupinách. Přerozdělení finančních prostředků tak, aby byl podnik pověřen smyslupnými úkoly, které bude plnit. Častější kontroly provozovatelem trati. Vyčlenit potřebné finanční prostředky s cílem zajistit, aby klíčoví zaměstnanci v průběhu tohoto procesu v podniku setrvali. Věnovat zvláštní pozornost zajištění postupů předávání informací a znalostí mezi odcházejícími zaměstnanci a těmi, kteří převezmou úkoly, atd.	Vysoká/ Vysoká	Koordinováno XYZ. Regiony musí přezkoumat opatření ke zvýšení kontroly tratí, překrývání odpovědnosti mezi zaměstnanci a následné kontroly provedené provozovate-lem trati	Zvýšený počet kontrol musí být zakotven ve smlouvách. Atd.	Ředitel podniku	Zpráva o metodě HAZID R_X realizo-vané postupy brain-stormin-gu	není relevantní				Změna podmínek okolností toto riziko významně omezila. Byla provedena analýza pracovního prostředí a uskutečněno školení zaměstnanců.
Subdodavatelé podnikatelů, kteří postrádají dovednosti, kvalifikaci a zavedené postupy řízení jakosti	Zvýšená poptávka po doložené kvalifikaci. Systematická kontrola plněných úkolů	Vysoká/ Střední	Provozovatel infrastruktury musí zajistit koordinaci. Regiony musí zavést opatření vyžadující příslušnou kvalifikaci a kontrolu práce	Prováděno následnou kontrolou smluv. Vstup do plánování revizí.	Provozova tel infra-struktury	Zpráva o metodě HAZID R_X realizo-vané postupy brain-stormin-gu	není relevantní	Vedoucí pracovník pro otázky bezpečnosti		Zvýšený důraz na rutinní postupy kontrol (2 provozní kontroly za měsíc na jednu provozní oblast)
Nejisté rozdělení rolí a	Definovat role a odpovědnost. Zmapovat všechna rozhraní a určit, kdo za	Střední/ Střední	V každém regionu	Prováděno smlouvou o	Regionál-ní ředitelé	Zpráva o metodě	není relevantní	Vedoucí pracovník		Regiony předložily svou

(18) *Tyto dva sloupce se týkají informací/pole o subjektech, které řídí usměrňování určených nebezpečí.*

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Tabulka 6: Příklad záznamu o nebezpečí pro organizační změnu v oddílu C.5. v příloze C.

Popis nebezpečí	**Bezpečnostní opatření**	**Priorita/ Bezpečnost Včasnost**	**Provádění**[18]	**Poznámky**	**Odpo-vědnost** [18]	**Zdroj**	**Použitá zásada přijatelnosti rizik**	**Odpo-vědnost za ověření**	**Způsob ověření**	**Stav xx.xx.xx**
odpovědnosti na rozhraní mezi podnikem a provozovatelem infrastruktury (provozovatelem trati).	jednotlivá rozhraní odpovídá.		samostatně	údržbě a strategickým plánem reorganizace		HAZID R_X realizo-vané postupy brain-stormin-gu		pro otázky bezpečnosti		strategii.

C.16.3. Příklad úplného záznamu o nebezpečí palubního řídícího subsystému

C.16.3.1. V tomto oddílu je uveden příklad záznamu o jednotlivém nebezpečí (viz bod [G 3] v oddílu 4.1.1) pro účely řízení:

(a) všech požadavků na vnitřní bezpečnost vztahujících se na subsystém, za který příslušný subjekt nese odpovědnost, a
(b) všech určených nebezpečí a souvisejících bezpečnostní opatření, která subjekt nemůže provádět a která musí být přenesena na jiné subjekty.

Tabulka 7: Příklad záznamu o nebezpečí vyhotoveného výrobcem pro palubní řídící subsystém.

HZD č.	**Zdroj**	**Popis nebezpečí**	**Doplňující informace**	**Odpovědný subjekt**	**Bezpečnostní opatření**	**Použitá zásada přijatelnosti rizik**	**Odesláno**	**Stav**
1	Zpráva o metodě HAZOP R_X	Byla nastavena příliš vysoká maximální rychlost vlaku (Vmax)	Chybná konkrétní konfigurace palubního subsystému (pracovníci údržby). Chybně zavedená palubní data (strojvedoucí)	Železniční podnik	• Určit postup pro schvalování konfiguračních dat palubního subsystému. • Určit provozní postup pro proces zavádění dat strojvedoucím.	Jednoznačný odhad rizika	Ano	Usměrněno (odesláno železničnímu podniku) Viz také oddíl C.16.4.2. v příloze C.
2	Zpráva o	Brzdné křivky (tj. oprávnění k jízdě)	Postup pro konkrétní konfiguraci palubního systému závisí na:	Železniční podnik	• Určit správně požadavky na systém ve vymezení systému.	Jednoznačný odhad rizika	Ano	Usměrněno (odesláno

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Tabulka 7: Příklad záznamu o nebezpečí vyhotoveného výrobcem pro palubní řídící subsystém.

HZD č.	Zdroj	Popis nebezpečí	Doplňující informace	Odpovědný subjekt	Bezpečnostní opatření	Použitá zásada přijatelnosti rizik	Odesláno	Stav
	metodě HAZOP R_X	v konfiguračních datech palubního subsystému jsou nastaveny příliš volně	• mírách bezpečnosti zavedených pro brzdový systém vlaku, • reakční prodlevě brzdového systému vlaku (ta je přímo závislá na délce vlaku, zejména u nákladních vlaků).		• Zavést dostatečné míry bezpečnosti pro brzdový systém konkrétního vlaku.			železničnímu podniku) Viz také oddíl C.16.4.2. v příloze C.
3	Zpráva o metodě HAZOP R_X	• Je nastavena příliš vysoká maximální rychlost (Vmax) • Brzdné křivky (tj. oprávnění k jízdě) v konfiguračních datech palubního subsystému jsou nastaveny příliš volně	Neprovedení aktualizace průměru vlakových kol v konkrétní konfiguraci palubního subsystému (pracovníci údržby).	Železniční podnik	• Určit postup pro měření průměru vlakových kol pracovníky údržby., • Určit postup pro pravidelné aktualizace průměru vlakových kol v palubním subsystému.,	Jednoznačný odhad rizika	Ano	Usměrněno (odesláno železničnímu podniku) Viz také oddíl C.16.4.2. v příloze C.
			Porucha v postupu výrobce týkajícím se přípravy a přesouvání konfiguračních dat do palubního subsystému.	Výrobce	Určit postup pro aktualizaci průměru vlakových kol v konfiguračních datech palubního subsystému.	Jednoznačný odhad rizika	Ano	Usměrněno postupem P_X.
4	Zpráva o metodě HAZOP R_X	Vjezd vlaku ve vysoké rychlosti (160 km/h, pokud boční traťové návěstidlo signalizuje volno) na trať bez aktivního palubního subsystému a bez boční traťové návěsti.	Jedinou možnou formou kontroly je ostražitost strojvedoucího. Vjezd do úseku trati vybaveného ATP závisí na potvrzení strojvedoucím před úsekem přechodu. Pokud strojvůdce vjezd nepotvrdí, palubní řídící subsystém automaticky zapne brzdy vlaku.	Provozovatel infrastruktury	Provozovatel infrastruktury musí zajistit, aby vlaky, které nejsou vybaveny aktivním palubním řídícím subsystémem, nevjely na příslušnou trať. Určit postup řízení provozu.	Jednoznačný odhad rizika	Ano	Usměrněno (odesláno provozovateli infrastruktury) Viz také oddíl C.16.4.2. v příloze C.
				Železniční podnik	Zajistit školení strojvedoucích pro vjezd do úseku trati vybaveného traťovým ATP.	Jednoznačný odhad rizika	Ano	Usměrněno (odesláno železničnímu podniku) Viz také oddíl C.16.4.2. v příloze C.
5	Zpráva o metodě HAZOP R_X	Nastavená maximální rychlost vlaku (Vmax), která se zobrazuje strojvedoucímu, je příliš vysoká.	Informace zobrazené na rozhraní strojvedoucího jsou sledovány palubním řídícím subsystémem SIL 4, který zapíná nouzové brzdy v případě rozporu mezi zobrazenou a předpokládanou hodnotou. V případě nedodržení oprávnění k jízdě palubní řídící	Výrobce	Vyvinout palubní řídící subsystém SIL 4.	Jednoznačný odhad rizika	Ano	Doklad bezpečnosti prokazující, že subsystém SIL 4 byl posouzen nezávislým posuzovatelem

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Tabulka 7: Příklad záznamu o nebezpečí vyhotoveného výrobcem pro palubní řídící subsystém.

HZD č.	Zdroj	Popis nebezpečí	Doplňující informace	Odpovědný subjekt	Bezpečnostní opatření	Použitá zásada přijatelnosti rizik	Odesláno	Stav
			subsystém zapne nouzové brzdy.					bezpečnosti.
6	Zpráva o metodě HAZOP R_X	Vlak odjíždí bez rozhraní strojvůdce/stroj.	Ztráta redundantní architektury palubního subsystému	Výrobce	Vyvinout palubní řídící systém SIL 4.	Jednoznačný odhad rizika	Ano	Doklad bezpečnosti prokazující, že subsystém SIL 4 byl posouzen nezávislým posuzovatelem bezpečnosti.
atd.								

C.16.4. Příklad záznamu o nebezpečí pro předání informací jiným subjektům

C.16.4.1 V tomto oddílu je uveden příklad záznamu o nebezpečí pro přenos určených nebezpečí a souvisejících bezpečnostních opatření, která posuzovaný subjekt nemůže zavést, na jiné subjekty. Viz bod [G 1] v oddílu 4.1.1.
Tento příklad je stejný jako příklad v oddílu C.16.3. v příloze C. Jediný rozdíl spočívá v tom, že všechna vnitřní nebezpečí a bezpečnostní opatření, která by mohla být usměrňována posuzovaným subjektem, jsou odstraněna.

C.16.4.2. Poslední sloupec v Tabulka 8 se používá pro splnění požadavků v oddílu 4.2 nařízení CSM. Existují různá řešení, jako toho dosáhnout. Jedním ze způsobů může být odkaz na evidenci, kterou používá subjekt přijímající odeslané bezpečnostní informace. Jiným způsobem může být uskutečnění jednání dvou subjektů s cílem najít společně vhodné řešení pro usměrňování souvisejícího rizika (rizik). O výsledcích takového jednání může být podána zpráva ve formě dohodnutého dokumentu (například zápisu z jednání), na který může subjekt odesílající informace související s bezpečností odkázat v souvislosti s uzavřením nebezpečí v jeho záznamu o nebezpečí.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Tabulka 8: Příklad záznamu o nebezpečí pro předání informací souvisejících s bezpečností jiným subjektům.

HZD č.	Zdroj nebezpečí		Popis nebezpečí	Doplňující informace	Odpovědný subjekt	Bezpečnostní opatření	Připomínky příjemce
	č. v Tabulka 7	Ostatní					
1	č. 1	Zpráva o metodě HAZOP R_X	Byla nastavena příliš vysoká maximální rychlost vlaku (Vmax).	Chybná konkrétní konfigurace palubního subsystému (pracovníci údržby). Chybně zavedená palubní data (strojvedoucí).	Železniční podnik	• Určit postup pro schvalování konfiguračních dat palubního subsystému. • Určit provozní postup pro proces zavádění dat strojvedoucím.	• Konfigurační data palubního řídícího subsystému závisí na fyzické charakteristice kolejového vozidla. • Míry bezpečnosti jsou následně použity na tato data v koordinaci mezi provozovatelem infrastruktury a železničním podnikem. • Tato data jsou následně přesunuta do palubního subsystému v souladu s příslušným postupem výrobce v průběhu instalace, začlenění do kolejových vozidel a uznání řídícího subsystému. • Strojvedoucí jsou školeni a hodnoceni podle postupu D_P. • Strojvedoucí jsou provozovatelem infrastruktury hodnoceni také podle předpisů použitelných na infrastrukturu provozovatele infrastruktury.
2	č. 2	Zpráva o metodě HAZOP R_X	Brzdné křivky (tj. oprávnění k jízdě) v konfiguračních datech palubního subsystému jsou nastaveny příliš volně.	Postup pro konkrétní konfiguraci palubního systému závisí na: • mírách bezpečnosti zavedených pro brzdový systém vlaku, • reakční prodlevě brzdového systému vlaku (ta je přímo závislá na délce vlaku, zejména u nákladních vlaků).	Železniční podnik	• Určit správně požadavky na systém ve vymezení systému. • Zavést dostatečné míry bezpečnosti pro brzdový systém konkrétního vlaku.	Viz výše uvedené připomínky k řádku 1.
3	č.3	Zpráva o metodě HAZOP R_X	• Je nastavena příliš vysoká maximální rychlost (Vmax). • Brzdné křivky (tj. oprávnění k jízdě) v konfiguračních datech palubního subsystému jsou nastaveny příliš volně.	Neprovedení aktualizace průměru vlakových kol v konkrétní konfiguraci palubního subsystému (pracovníci údržby).	Železniční podnik	• Určit postup pro měření průměru vlakových kol pracovníky údržby. • Určit postup pro pravidelné aktualizace průměru vlakových kol v palubním subsystému.	• Údržba palubního řídícího subsystému je prováděna v souladu s „Postupem údržby MP_Z“. • Průměr vlakových kol je aktualizován v určených intervalech podle postupu P_W. • Pokud jde o proces zavádění dat, jsou strojvedoucí školeni a hodnoceni podle „Postupu P_{DE}“.
4	č. 4	Zpráva o metodě HAZOP	Vjezd vlaku ve vysoké rychlosti (160 km/h, pokud boční traťové návěstidlo	Jedinou možnou formou kontroly je ostražitost strojvedoucího. Vjezd do úseku trati vybaveného ATP závisí na potvrzení	Provozovatel infrastruktury	Provozovatel infrastruktury musí zajistit, aby vlaky, které nejsou vybaveny aktivním palubním řídícím	Řízení provozu v rámci infrastruktury provozovatele infrastruktury je upraveno souborem předpisů R_{TM}.

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Tabulka 8: Příklad záznamu o nebezpečí pro předání informací souvisejících s bezpečností jiným subjektům.

HZD č.	Zdroj nebezpečí		Popis nebezpečí	Doplňující informace	Odpovědný subjekt	Bezpečnostní opatření	Připomínky příjemce
	č. v Tabulka 7	Ostatní					
		R_X	signalizuje volno) na trať bez aktivního palubního subsystému a bez boční traťové návěsti.	strojvedoucím před úsekem přechodu. Pokud strojvedoucí vjezd nepotvrdí, palubní řídící subsystém automaticky zapne brzdy vlaku.		subsystémem, nevjely na příslušnou trať. Určit postup řízení provozu.	
					Železniční podnik	Zajistit školení strojvedoucích pro vjezd do úseku trati vybaveného traťovým ATP.	• Strojvedoucí jsou školeni v pravidelných intervalech podle postupu provozovatele infrastruktury P_{IM_DP}. • Strojvedoucí jsou provozovatelem infrastruktury hodnoceni také podle souboru předpisů (S_R) použitelných na infrastrukturu provozovatele infrastruktury.
atd.							

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.17. Příklad seznamu standardních nebezpečí pro provoz železnic

C.17.1. ROSA (Analýza bezpečnosti pro optimalizaci provozu železnic), projekt v rámci DEUFRAKO (francouzsko-německé spolupráce), se pokusil o sestavení seznamu standardních a komplexních nebezpečí týkajících se standardního provozu železnic. Cílem a náročným úkolem tohoto projektu byla snaha definovat příslušná nebezpečí maximálně podrobně a zároveň odhlédnout od specifičnosti francouzských a německých železnic. Tento seznam byl sestaven na základě stávajících aktuálních seznamů z obou zemí (SNCF a DB) a byl také vzájemně kontrolován se seznamy nebezpečí z jiných zemí. Bez ohledu na deklarovaný cíl toho seznamu, být komplexní a standardní, jej zde uvádíme pouze jako orientační příklad, který může sloužit jako vodítko pro jiné subjekty, pokud mají určit nebezpečí po konkrétní projekt. Předpokládá se, že nebezpečí uvedená v tomto seznamu by pravděpodobně musela být dále rozpracována nebo doplněna, aby byly zohledněny specifické rysy určitého projektu.

C.17.2. Nebezpečí uvedená v následujícím návrhu seznamu jsou nazývána "výchozí nebezpečí", čímž se rozumí nebezpečí, u kterých lze provést analýzu důsledků i přičinnou analýzu s cílem určit bezpečnostní opatření/zábrany a požadavky na bezpečnost pro usměrňování nebezpečí.

C.17.3. Seznam nebezpečí projektu ROSA:

SPH 01	Počáteční chybné určení nejvyšší dovolené rychlosti (související s infrastrukturou)
SPH 02	Chybné určení nejvyšší dovolené rychlosti (související s vlakem)
SPH 03	Chybné určení brzdné dráhy/chybný profil rychlosti/chybné brzdné křivky
SPH 04	Nedostatečné zpomalení (fyzické příčiny)
SPH 05	Chybný příkaz k nepřiměřené rychlosti/k brzdění
SPH 06	Chybně zaznamenaná rychlost (chybná rychlost vlaku)
SPH 07	Porucha sdělování nejvyšší dovolené rychlosti
SPH 08	Vlak se vzdaluje
SPH 09	Chybný směr jízdy/záměrný zpětný pohyb – (kombinace SPH 08 a SPH 14)
SPH 10	Chybně zaznamenaná absolutní/relativní poloha
SPH 11	Porucha detekce vlaků
SPH 12	Ztráta integrity vlaku
SPH 13	Možná chybná trasa vlaku
SPH 14	Porucha přenosu/sdělování jízdního řádu/oprávnění k jízdě
SPH 15	Konstrukční porucha vodicí kolejnice
SPH 16	Rozbitý díl výhybky
SPH 17	Chybný příkaz výhybky
SPH 18	Chybný stav výhybky
SPH 19	Předmět systému na vodicí kolejnici/v oblasti volného pohybu (kromě štěrkového lože)
SPH 20	Cizí předmět na vodicí kolejnici/v oblasti volného pohybu
SPH 21	Uživatel silniční dopravy na LC
SPH 22	Účinky tlakové vlny na štěrkovém loži
SPH 23	Vliv aerodynamických sil na vlak
SPH 24	Zařízení/prvek/zatížení narušuje oblast volného pohybu vlaku
SPH 25	Nevhodný rozměr oblasti volného pohybu vlaku (krajnice)
SPH 26	Chybné rozložení zatížení
SPH 27	Rozbité kolo, rozbitá náprava
SPH 28	Horká náprava/kolo/ložisko
SPH 29	Porucha podvozku/zavěšení, tlumení
SPH 30	Porucha rámu vozidla/vozidlové skříně
SPH 31	Vstup nepovolaných osob (bezpečnostní aspekt)

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

SPH 32	Oprávněná osoba přechází koleje
SPH 33	Zaměstnanci pracující na kolejích
SPH 34	Neoprávněná osoba naruší kolejiště (nedbalost)
SPH 35	Pád osoby z kraje nástupiště na koleje
SPH 36	Tlaková vlna/osoba je příliš blízko kraje nástupiště
SPH 37	Zaměstnanci pracují blízko koleje, např. na sousední koleji
SPH 38	Osoba opouští vlak úmyslně (kromě výměny cestujících)
SPH 39	Osoba vypadne z (postranních) dveří
SPH 40	Osoba vypadne ze dveří u zadní stěny
SPH 41	Vlak odjíždí/popojíždí s otevřenými dveřmi (nenarušená oblast volného pohybu vlaku)
SPH 42	Osoba spadne do prostoru přechodového můstku mezi dvěma vozy
SPH 43	Cestující se vyklánějí ze dveří
SPH 44	Cestující se vyklánějí z okna
SPH 45	Zaměstnanci/zřízenci se vyklánějí ze dveří
SPH 46	Zaměstnanci/zřízenci se vyklánějí z okna
SPH 47	Posunovači na voze se vyklánějí ze schůdků
SPH 48	Osoba padá/vylézá z nástupiště do prostoru mezi vozidlem a nástupištěm
SPH 49	Osoba vypadne z vlaku/opustí vlak na úseku, kde není nástupiště
SPH 50	Osoba vypadne z vlaku v oblasti dveří při výměně cestujících
SPH 51	Dveře vlaku se zavírají s osobou zachycenou v prostoru dveří
SPH 52	Vlak se pohybuje v době výměny cestujících
SPH 53	Možnost zranění osoby ve vlaku
SPH 54	Nebezpečí požáru/výbuchu (ve vlaku) – kategorie nehody, důsledek SPH 55, SPH 56)
SPH 55	Nepřiměřená teplota (ve vlaku)
SPH 56	Otrava alkoholem/udušení (ve vlaku)
SPH 57	Zabití elektrickým proudem (ve vlaku)
SPH 58	Osoba vypadne na nástupiště (kromě výměny cestujících)
SPH 59	Nepřiměřená teplota (na nástupišti)
SPH 60	Otrava alkoholem/udušení (na nástupišti)
SPH 61	Zabití elektrickým proudem (na nástupišti)

Evropská agentura pro železnice ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu