Európska železničná agentúra

Zbierka príkladov posudzovania rizík a niektorých možných nástrojov na podporu nariadenia o CSM

Referencia v ERA:	ERA/GUI/02-2008/SAF
Verzia v ERA:	1.1
Dátum:	6. 1. 2009

Dokument vypracovala:	Európska železničná agentúra Boulevard Harpignies, 160 BP 20392 F-59307 Valenciennes Cedex Francúzsko
Druh dokumentu:	príručka
Stav dokumentu:	verejný

	Meno	Funkcia
Povolil	Marcel VERSLYPE	výkonný riaditeľ
Kontroloval	Anders LUNDSTRÖM Thierry BREYNE	vedúci bezpečnostného oddelenia vedúci sekcie posudzovania bezpečnosti
Napísal (autor)	Dragan JOVICIC	úradník bezpečnostného oddelenia, zodpovedný za projekt

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

INFORMÁCIE O DOKUMENTE

Záznam o zmenách a doplneniach

Tab. 1: Stav dokumentu.

Verzia Dátum	Autor(i)	Číslo časti	Opis úprav
Starý názov a štruktúra dokumentu: *„Usmernenie k používaniu odporúčania o 1. súbore CSM"*			
Usmernenie, verzia 0.1 15. 2. 2007	Dragan JOVICIC	Všetky	Prvá verzia usmernenia k používaniu súvisiaca s verziou 1.0 „1. súboru odporúčaní k CSM". Toto je zároveň prvá verzia dokumentu predloženého pracovnej skupine pre CSM na formálne preskúmanie.
Usmernenie, verzia 0.2 7. 6. 2007	Dragan JOVICIC	Všetky	Reorganizácia dokumentu, aby sa zhodoval so štruktúrou verzie 4.0 odporúčania k CSM. Aktualizácia podľa odporúčania pracovnej skupiny pre CSM po procese formálneho preskúmania verzie 1.0.
		Všetky	Aktualizácia dokumentu o doplňujúce informácie zhromaždené počas interných rokovaní ERA, ako aj o požiadavky osobitnej pracovnej skupiny pre CSM a pracovnej skupiny na vývoj nových bodov.
		Obr. 1	Úprava obrázka znázorňujúceho „rámec riadenia rizík pre prvý súbor spoločných bezpečnostných metód" v súlade s pripomienkami kontroly a v súlade s terminológiou ISO.
Usmernenie, verzia 0.3 20. 7. 2007	Dragan JOVICIC	Dodatky	Reorganizácia dodatkov a vypracovanie nových dodatkov. Nový dodatok na zhrnutie všetkých diagramov, ktoré znázorňujú a uľahčujú čítanie a pochopenie príručky.
		Všetky časti	Dokument aktualizovaný s cieľom: • dopracovať čo najviac existujúcich častí x; • ďalej rozpracovať spôsob preukazovania súladu systému s požiadavkami na bezpečnosť; • vytvoriť odkaz na V-cyklus CENELEC (t. j. na Obr. 8 a Obr. 10 normy EN 50 126); • ďalej rozvíjať potrebnú spoluprácu a koordináciu medzi rôznymi aktérmi v sektore železníc, ktorých činnosti môžu ovplyvniť bezpečnosť železničného systému; • vysvetliť doklady (napr. záznam nebezpečenstiev a bezpečnostná dokumentácia), ktorými by sa malo orgánom pre posudzovanie preukazovať správne uplatňovanie procesu posudzovania rizík podľa nariadenia o CSM; Dokument bol aktualizovaný aj podľa prvého interného preskúmania v agentúre.
Usmernenie, verzia 0.4 16. 11. 2007	Dragan JOVICIC	Všetky časti	Dokument aktualizovaný po procese formálneho preskúmania podľa pripomienok členov pracovnej skupiny pre CSM alebo organizácií k verzii 0.3, ktoré telefonicky odsúhlasili: • belgický, španielsky, fínsky, nórsky, francúzsky a dánsky NBO; • SIEMENS (člen UNIFE); • nórsky manažér infraštruktúry (Jernbaneverket – člen EIM).
Usmernenie, verzia 0.5 27. 2. 2008	Dragan JOVICIC	Všetky časti	Dokument aktualizovaný podľa pripomienok členov pracovnej skupiny pre CSM alebo organizácií k verzii 0.3, ktoré telefonicky odsúhlasili: • CER, • holandský NBO.
		Všetky časti	Dokument aktualizovaný v súlade s podpísanou verziou odporúčania týkajúceho sa CSM. Dokument aktualizovaný podľa pripomienok Christopha CASSIRA a Marcusa ANDERSSONA na internom preskúmaní v agentúre.
		Všetky časti Dodatky	Úplné prečíslovanie odsekov dokumentu vs odporúčanie Zahrnutie príkladov uplatňovania odporúčania CSM.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Tab. 1: Stav dokumentu.

Verzia Dátum	Autor(i)	Číslo časti	Opis úprav
Nový názov a nová štruktúra dokumentu: *„Zbierka príkladov posudzovania rizík a niektorých možných nástrojov na podporu nariadenia o CSM“*			
Príručka, verzia 0.1 23. 5. 2008	Dragan JOVICIC	Všetky	Prvá verzia dokumentu vyplývajúca z rozdelenia verzie 0.5 „usmernenia k používaniu“ na dva vzájomne sa dopĺňajúce dokumenty.
Príručka, verzia 0.2 3. 9. 2008	Dragan JOVICIC	Všetky	Aktualizácia dokumentu v súlade: • s nariadením Európskej komisie o CSM {Ref. 3}; • s pripomienkami z pracovného seminára konaného 1. júla 2008 s členmi výboru pre interoperabilitu a bezpečnosť železníc (*Railway Interoperability and Safety Committee;* RISC); • s pripomienkami členov pracovnej skupiny pre CSM (nórskeho, fínskeho, britského a francúzskeho NBO, CER, EIM, Jensa BRABANDA [UNIFE] a Stéphana ROMEI [UNIFE]).
Príručka, verzia 1.0 10. 12. 2008	Dragan JOVICIC	Všetky	Aktualizácia dokumentu v súlade s nariadením Európskej komisie o CSM na hodnotenie a posudzovanie rizík {Ref. 3}, ktoré schválil Výbor pre interoperabilitu a bezpečnosť železníc (RISC) na svojom plenárnom zasadnutí 25. novembra 2008.
Príručka, verzia 1.1 6. 1. 2009	Dragan JOVICIC	Všetky	Aktualizácia dokumentu podľa pripomienok právnych a jazykových útvarov Európskej komisie k nariadeniu o CSM.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Obsah

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Zoznam obrázkov

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Zoznam tabuliek

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

0. ÚVOD

0.1. Rozsah pôsobnosti

0.1.1. Účelom tohto dokumentu je poskytnúť ďalšie vysvetlenie nariadenia Komisie o prijatí spoločnej bezpečnostnej metódy na hodnotenie a posudzovanie rizík podľa článku 6 ods. 3 písm. a) smernice Európskeho parlamentu a Rady 2004/49/ES {Ref. 3}. Uvedené nariadenie sa v tomto dokumente označuje ako „nariadenie o CSM“.

0.1.2. Tento dokument nie je právne záväzný a jeho obsah sa nesmie vykladať ako jediný spôsob splnenia požiadaviek CSM. Účelom tohto dokumentu je doplniť príručku na uplatňovanie nariadenia o CSM {Ref. 4} o postup, ktorým je možné nariadenie o CSM využívať a uplatňovať. Sú v ňom uvedené ďalšie praktické informácie, ktorými sa nestanovujú žiadne povinné postupy ani žiadna právne záväzná prax. Tieto informácie môžu využiť všetci aktéri[(1)], ktorých činnosť môže ovplyvniť bezpečnosť železničných systémov a ktorí priamo alebo nepriamo musia uplatniť CSM. V tomto dokumente sú uvedené príklady posudzovania rizík a niektoré možné nástroje, ktoré napomáhajú uplatňovanie CSM. Tieto príklady sú uvedené len pre informáciu a pomoc. Aktéri môžu použiť alternatívne metódy alebo môžu ďalej používať svoje vlastné existujúce metódy a nástroje na dosiahnutie súladu s CSM, ak ich považujú za vhodnejšie.
Príklady a doplňujúce informácie v tomto dokumente nie sú vyčerpávajúce ani nepokrývajú všetky možné situácie, pri ktorých sa navrhujú významné zmeny, a preto možno tento dokument považovať len za čisto informatívny.

0.1.3. Tento informačný dokument je len doplňujúcou pomôckou na uplatňovanie nariadenia CSM. Mal by sa používať v spojení s nariadením o CSM {Ref. 3} a so súvisiacou príručkou {Ref. 4} na uľahčenie ďalšieho uplatňovania CSM, ale nenahrádza nariadenie o CSM..

0.1.4. Dokument vypracovala Európska železničná agentúra (ERA) s podporou odborníkov pracovnej skupiny pre CSM zo združenia železníc a národných bezpečnostných orgánov. Predstavuje vypracovanú zbierku myšlienok a informácií, ktoré sa v agentúre nazhromaždili počas interných rokovaní a porád s pracovnou skupinou pre CSM a osobitnými pracovnými skupinami pre CSM. ERA bude podľa potreby dokument revidovať a aktualizovať tak, aby vyjadroval pokrok vo vývoji európskych noriem, zmeny v posudzovaní rizík podľa nariadenia o CSM a možný prínos zo skúseností pri uplatňovaní nariadenia o CSM. Keďže v čase zostavovania nebolo možné uviesť harmonogram procesu revízií, informácie o poslednom dostupnom vydaní tohto dokumentu môže čitateľovi poskytnúť Európska železničná agentúra.

0.2. Mimo rozsahu pôsobnosti

0.2.1. V tomto dokumente nie je usmernenie o organizovaní, prevádzkovaní alebo navrhovaní (a výrobe) systému železníc ani jeho častí. Dokument nevymedzuje ani zmluvné dohody ani dohody, ktoré môžu niektorí aktéri vzájomne uzavrieť o uplatňovaní postupu riadenia rizík.

---

(1) Príslušnými aktérmi sú obstarávatelia podľa článku 2 písmena r) smernice 2008/57/ES o interoperabilite systému železníc v Spoločenstve alebo výrobcovia, uvedení v nariadení ako „navrhovatelia“, alebo ich dodávatelia a poskytovatelia služieb.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Zmluvné dohody o konkrétnych projektoch sú mimo rozsahu pôsobnosti nariadenia o CSM, súvisiacej príručky a tiež tohto dokumentu.

0.2.2. Aj keď príslušní aktéri môžu mimo pôsobnosti tohto dokumentu dohodnúť opatrenia, ktoré zakotvia v príslušných zmluvách na začiatku projektu, nebudú mať žiadny vplyv na ustanovenia o CSM. Môže sa to týkať napríklad:

a) nákladov na riadenie rizík súvisiacich s bezpečnosťou na rozhraniach medzi aktérmi;
b) nákladov na prevod nebezpečenstiev a súvisiacich bezpečnostných opatrení medzi aktérmi, ktoré na začiatku projektu neboli známe;
c) spôsobu riešenia konfliktov, ktoré môžu vzniknúť počas projektu;
d) atď.

Ak by medzi navrhovateľom a jeho subdodávateľmi došlo k nezhode alebo ak počas plánovania a realizácie projektu vznikne spor, odkaz na príslušné zmluvy pravdepodobne pomôže vyriešiť akýkoľvek spor.

0.3. Zásada pre tento dokument

0.3.1. Aj keď sa tento dokument môže javiť ako samostatný dokument na účely výkladu, nenahrádza nariadenie o CSM {Ref. 3}. Na ľahšiu orientáciu je v tomto dokumente uvedený každý Čl. nariadenia o CSM. Podľa potreby je príslušný Čl. vopred vysvetlený v príručke na uplatňovanie nariadenia o CSM {Ref. 4}. Keď je to potrebné na hlbšie pochopenie nariadenia o CSM, ďalšie informácie sú potom uvedené v nasledujúcich odsekoch.

0.3.2. Články a ich príslušné odstavce z Nariadenia o CSM sú skopírované do textových rámčekov v tejto príručke s použitím typu písma „Bookman Old Style“ v kurzíve, rovnako, ako v tomto texte. Toto formátovanie umožňuje jednoducho rozoznať pôvodný text Nariadenia o CSM {Ref. 3} od dodatočných vysvetlení, ktoré sú uvedené v tomto dokumente. Text z Príručky na uplatňovanie nariadenia o CSM {Ref.4} nie je skopírovaný do tohto dokumentu

0.3.3. Štruktúra tohto dokumentu sa zhoduje so štruktúrou nariadenia o CSM, aby sa čitateľovi uľahčila orientácia.

0.4. Opis dokumentu

0.4.1. Dokument je rozdelený na tieto časti:

a) kapitolu 0., ktorá vymedzuje rozsah pôsobnosti tohto dokumentu so zoznamom referenčných dokumentov;
b) prílohu I a prílohu II, v ktorých sú ďalšie informácie k príslušným častiam nariadenia o CSM {Ref. 3} a súvisiaceho návodu {Ref. 4};
c) nové dodatky, v ktorých sa ďalej rozvíjajú niektoré konkrétne stránky a uvádzajú príklady.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

0.5. Referenčné dokumenty

Tab. 2: Tab. referenčných dokumentov.

{Ref. č.}	Názov	Odkaz	Verzia
{Ref. 1}	Smernica Európskeho parlamentu a Rady 2004/49/ES z 29. apríla 2004 o bezpečnosti železníc Spoločenstva a o zmene a doplnení smernice Rady 95/18/ES o udeľovaní licencií železničným podnikom a smernici 2001/14/ES o prideľovaní kapacity železničnej infraštruktúry, vyberaní poplatkov za používanie železničnej infraštruktúry a bezpečnostnej certifikácii (smernica o bezpečnosti železníc)	2004/49/ES Ú. v. EÚ L 164, 30.4.2004, s. 44 v znení opravy uverejnenej v Ú. v. EÚ L 220, 21.6.2004, s. 16.	-
{Ref. 2}	Smernica Európskeho parlamentu a Rady 2008/57/ES zo 17. júna 2008 o interoperabilite systému železníc v Spoločenstve	2008/57/ES Ú. v. EÚ L 191, 18.7.2008, s. 1.	-
{Ref. 3}	Nariadenie Komisie (ES) č.352/2009 z 24. apríla 2009 o prijatí spoločnej bezpečnostnej metódy na hodnotenie a posudzovanie rizík podľa článku 6 ods. 3 písm. a) smernice Európskeho parlamentu a Rady 2004/49/ES	ES č. 352/2009	24. apríla 2009
{Ref. 4}	Príručka na uplatňovanie nariadenia Komisie o prijatí spoločnej bezpečnostnej metódy hodnotenia a posudzovania rizík, uvedenej v článku 6 ods. 3 písm. a) smernice o bezpečnosti železníc	ERA/GUI/01-2008/SAF	1.0
{Ref. 5}	Smernica Európskeho parlamentu a Rady 2008/57/ES zo 17. júna 2008 o interoperabilite systému železníc v Spoločenstve	2008/57/ES Ú. v. EÚ L 191, 18.7.2008, s. 1.	-
{Ref. 6}	Systém riadenia bezpečnosti – Kritériá posudzovania pre železničné podniky a manažérov infraštruktúry	Kritériá posudzovania SMS Časť A: Bezpečnostné osvedčenia a povolenia	31. 5. 2007
{Ref. 7}	Dráhové aplikácie – Komunikačné a signalizačné systémy a systémy na spracovanie údajov – Elektronické signalizačné systémy súvisiace s bezpečnosťou.	EN 50129	Február 2003
{Ref. 8}	Dráhové aplikácie – Stanovenie a preukázanie bezporuchovosti, pohotovosti, udržiavateľnosti a bezpečnosti (RAMS – Časť 1: norma sama	EN 50126-1	September 2006
{Ref. 9}	Dráhové aplikácie – Stanovenie a preukázanie bezporuchovosti, pohotovosti, udržiavateľnosti a bezpečnosti (RAMS) – Časť 2: Návod na používanie EN 50126-1 na bezpečnosť	EN 50126-2 (usmernenie)	Konečný návrh (august 2006)
{Ref. 10}	Všeobecné a podobné usmernenie týkajúce sa výpočtu rizika súvisiaceho s prepravou nebezpečného tovaru po železnici	Usmernenie OTIF, schválené výborom expertov RID	24. 11. 2005
{Ref. 11}	Kritérium akceptovania rizík pre technické systémy	Poznámka 01/08	1.1 (25. 1. 2008)
{Ref. 12}	ERA Safety Unit: Štúdia uskutočniteľnosti – „Prideľovanie bezpečnostných cieľov (v TSI subsystémoch) a konsolidácia TSI z hľadiska bezpečnosti“ WP1.1 – Posúdenie uskutočniteľnosti prideľovania spoločných bezpečnostných cieľov	WP1.1	1.0
{Ref. 13}	„Dráhové aplikácie – Systém klasifikácie koľajových vozidiel – Časť 4: EN 0015380 časť 4: Funkčné skupiny“.	EN 0015380, časť 4	

0.6. Štandardné vymedzenie pojmov, termínov a skratiek

0.6.1. Všeobecné vymedzenie pojmov, termínov a skratiek použitých v tomto dokumente je možné nájsť v bežnom slovníku.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

0.6.2. Nové vymedzenie pojmov, termínov a skratiek je v tejto príručke uvedené v nasledujúcich odsekoch.

0.7. Osobitné vymedzenie pojmov

0.7.1. Pozri Článok 3.

0.8. Osobitné termíny a skratky

0.8.1. Tento odsek vymedzuje nové osobitné termíny a skratky, ktoré sa často používajú v tomto dokumente.

Tab. 3: Tab. termínov.

Termín	Vymedzenie pojmu
agentúra	Európska železničná agentúra (ERA)
príručka	príručka na uplatňovanie nariadenia Komisie (ES) č. 352/2009 z 24. apríla 2009 o prijatí spoločnej bezpečnostnej metódy na hodnotenie a posudzovanie rizík, uvedenej v článku 6 ods. 3 písm. a) smernice Európskeho parlamentu a Rady 2004/49/ES
nariadenie o CSM	nariadenie Komisie (ES) č. 352/2009 z 24. apríla 2009 o prijatí spoločnej bezpečnostnej metódy na hodnotenie a posudzovanie rizík, uvedenej v článku 6 ods. 3 písm. a) smernice Európskeho parlamentu a Rady 2004/49/ES {Ref. 3}.

Tab. 4: Tab. skratiek.

Skratka	Význam	
CCS	Control Command and Signalling	systém riadenia, príkazov a signalizácie
CSM	Common Safety Method(s)	spoločná bezpečnostná metóda
CST	Common Safety Targets	spoločné bezpečnostné ciele
EC / EK	European Commission	Európska komisia
ERA	European Railway Agency	Európska železničná agentúra
IM / MI	Infrastructure Manager(s)	manažér infraštruktúry
ISA	Independent Safety Assessor	nezávislý posudzovateľ bezpečnosti
OTIF	Intergovernmental Organisation for International Carriage by Rail	Medzivládna organizácia pre medzinárodnú železničnú dopravu
MS / ČŠ	Member State	členský štát
NOBO	Notified Body	notifikovaný orgán
NSA	National Safety Authority	národný bezpečnostný orgán
QMP	Quality Management Process	proces riadenia kvality
QMS	Quality Management System	systém riadenia kvality
RISC	Railway Interoperability and Safety Committee	Výbor pre interoperabilitu a bezpečnosť železníc
RU / ŽP	Railway Undertaking(s)	železničný podnik
SMP	Safety Management Process	proces riadenia bezpečnosti
SMS	Safety Management System	systém riadenia bezpečnosti
SRT	Safety in Railway Tunnels	bezpečnosť v železničných tuneloch
TBC	To be completed	v tejto zbierke sa nepoužíva
TSI	Technical Specifications for Interoperability	technické špecifikácie interoperability

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

VÝKLAD ČLÁNKOV NARIADENIA O CSM

Článok 1. Účel

Článok 1 ods. 1

Týmto nariadením sa ustanovuje spoločná bezpečnostná metóda hodnotenia a posudzovania rizík (CSM), ako sa uvádza v článku 6 ods. 3 písm. a) smernice 2004/49/ES.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

Článok 1 ods. 2

Účelom spoločnej bezpečnostnej metódy hodnotenia a posudzovania rizík je zachovať alebo zlepšiť úroveň bezpečnosti železníc Spoločenstva v prípade, že je to potrebné a reálne uskutočniteľné. Spoločná bezpečnostná metóda zjednoduší prístup služieb železničnej dopravy na trh prostredníctvom harmonizácie::

a) procesov riadenia rizík, ktoré sa používajú na posúdenie úrovní bezpečnosti a na posúdenie zhody s požiadavkami na bezpečnosť;
b) výmeny informácií súvisiacich s bezpečnosťou medzi jednotlivými aktérmi v rámci železničného sektora s cieľom riadiť bezpečnosť medzi jednotlivými rozhraniami, ktoré v tomto sektore môžu existovať;
c) výsledkov vyplývajúcich z uplatňovania procesu riadenia rizík.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

Článok 2. Rozsah pôsobnosti

Článok 2 ods. 1

Spoločná bezpečnostná metóda hodnotenia a posudzovania rizík sa uplatňuje na každú zmenu železničného systému v členskom štáte, ako sa uvádza v bode 2 písm. d) prílohy III k smernici 2004/49/ES, ktorá sa považuje za významnú v zmysle článku 4 tohto nariadenia. Môže ísť o zmeny technickej, prevádzkovej alebo organizačnej povahy. V prípade organizačných zmien sa do úvahy berú len tie zmeny, ktoré by mohli mať vplyv na prevádzkové podmienky.

[G 1] CSM sa uplatňuje na celý železničný systém a ak sú zmeny vyhodnotené podľa Článok 4 ako významné, vzťahuje sa na posudzovanie týchto zmien:

a) stavby nových tratí alebo zmeny existujúcich tratí;
b) zavedenie nových a/alebo upravených technických systémov;
c) prevádzkové zmeny (napr. nové alebo upravené prevádzkové predpisy a postupy údržby);
d) zmeny v organizáciách ŽP/MI.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Termín „systém“ sa v CSM vzťahuje na všetky stránky systému o. i. vrátane jeho vývoja a výstavby, prevádzky, údržby atď. až do jeho vyradenia z prevádzky alebo odstránenia.

[G 2] CSM sa vzťahuje na významné zmeny:

a) „malých a jednoduchých“ systémov, ktoré môžu pozostávať z niekoľkých technických subsystémov alebo prvkov a
b) „veľkých a zložitejších“ systémov (medzi ktoré môžu patriť napr. stanice a tunely).

Článok 2 ods. 2

Keď sa významné zmeny týkajú štrukturálnych subsystémov, na ktoré sa vzťahuje smernica 2008/57/ES, spoločná bezpečnostná metóda hodnotenia a posudzovania rizík sa uplatňuje:

a) ak sa posúdenie rizík požaduje v príslušných technických špecifikáciách interoperability (TSI). V tomto prípade sa v TSI, ak je to potrebné, špecifikuje, ktoré časti CSM sa uplatňujú;
b) s cieľom zabezpečiť bezpečnú integráciu štrukturálnych subsystémov, na ktoré sa uplatňujú príslušné TSI, do existujúceho systému na základe článku 15 ods. 1 smernice 2008/57/ES.

Uplatňovanie spoločnej bezpečnostnej metódy, ako sa uvádza v prvom pododseku písm. b), však nesmie viesť k požiadavkám, ktoré by boli v rozpore s požiadavkami ustanovenými v príslušných TSI, ktoré sú záväzné.

Ak však uplatňovanie spoločnej bezpečnostnej metódy vedie k požiadavke, ktorá je v rozpore s požiadavkou stanovenou v príslušnej TSI, navrhovateľ informuje príslušný členský štát, ktorý sa môže rozhodnúť, že požiada o revíziu TSI v súlade s článkom 6 ods. 2 alebo článkom 7 smernice 2008/57/ES alebo o výnimku v súlade s článkom 9 uvedenej smernice.

[G 2] Napr. vozový park nového typu pre vysokorýchlostné trate musí spĺňať TSI Vysokorýchlostné železničné dráhové vozidlá v súlade so smernicou o bezpečnosti železníc {Ref. 1} a smernicou o interoperabilite železníc {Ref. 2}. Hoci TSI pokrýva väčšinu posudzovaného systému, netýka sa kabíny vodiča, ktorá je rozhodujúcou otázkou v súvislosti s ľudskými činiteľmi. Preto je na zistenie a primerané kontrolovanie všetkých odôvodnene predvídateľných nebezpečenstiev súvisiacich s otázkami ľudského činiteľa (t. j. rozhraní medzi vodičom, vozidlami a zvyškom železničného systému) potrebné použiť proces CSM.

Článok 2 ods. 3

Toto nariadenie sa nevzťahuje na:

a) metrá, električky a iné ľahké železničné systémy;
b) siete, ktoré sú funkčne oddelené od zvyšného systému železníc a určené len na miestnu, mestskú alebo prímestskú osobnú dopravu, ani na železničné podniky, ktoré svoju činnosť vykonávajú len na týchto sieťach;
c) železničnú infraštruktúru, ktorá je v súkromnom vlastníctve a využíva ju len jej vlastník na vlastnú nákladnú dopravu;
d) historické vozidlá prevádzkované na vnútroštátnych sieťach za predpokladu, že zodpovedajú vnútroštátnym bezpečnostným predpisom a úpravám v záujme zaistenia bezpečnej premávky takýchto vozidiel;
e) historické, múzejné a turistické železnice využívajúce vlastnú sieť vrátane údržbárskych dielní, vozidiel a zamestnancov.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Článok 2 ods. 4

Toto nariadenie sa nevzťahuje na systémy a zmeny, ktorými sú ku dňu nadobudnutia účinnosti tohto nariadenia projekty v pokročilej fáze vývoja, ako sa vymedzuje v článku 2 písm. t) smernice 2008/57/ES.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

Článok 3. Vymedzenie pojmov

Na účely tohto nariadenia sa uplatňujú vymedzenia pojmov v článku 3 smernice 2004/49/ES.

Uplatňujú sa aj tieto vymedzenia pojmov:

(1) „riziko“ znamená mieru výskytu nehôd a incidentov, ktoré majú za následok ujmu (spôsobenú nebezpečenstvom) a stupeň závažnosti tejto ujmy (EN 50126-2)*;*

(2) „analýza rizík“ znamená systematické využívanie všetkých dostupných informácií na identifikáciu nebezpečenstva a na odhad rizika (ISO/IEC 73)*;*

(3) „hodnotenie rizík“ znamená postup založený na analýze rizík s cieľom určiť, či sa dosiahlo prijateľné riziko (ISO/IEC 73)*;*

(4) „posudzovanie rizík“ znamená celkový proces obsahujúci analýzu rizík a hodnotenie rizík (ISO/IEC 73)*;*

(5) „bezpečnosť“ znamená neprítomnosť neprijateľného rizika ujmy (EN 50126-1)*;*

(6) „riadenie rizík“ znamená systematické uplatňovanie politík, postupov a praxe riadenia na úlohy týkajúce sa analýzy, hodnotenia a kontroly rizík (ISO/IEC 73)*;*

(7) „rozhrania“ znamenajú všetky body vzájomného pôsobenia počas životnosti systému alebo subsystému vrátane prevádzky a údržby, v ktorej budú spolupracovať jednotliví aktéri železničného sektora s cieľom riadiť riziká;

(8) „aktéri“ znamenajú všetky strany, ktoré sú priamo alebo prostredníctvom zmluvných úprav zapojené do uplatňovania tohto nariadenia v súlade s článkom 5 ods. 2;

(9) „požiadavky na bezpečnosť“ znamenajú potrebné bezpečnostné charakteristiky (kvalitatívne alebo kvantitatívne) systému a jeho prevádzky (vrátane prevádzkových pravidiel) na účely splnenia cieľov bezpečnosti, ktoré stanovujú právne predpisy alebo daná spoločnosť

(10) „bezpečnostné opatrenia“ znamenajú súbor akcií buď na zníženie miery výskytu nebezpečenstva, alebo na zmiernenie jeho následkov s cieľom dosiahnuť a/alebo zachovať prijateľnú úroveň rizika;

(11) „navrhovateľ“ znamená železničné podniky alebo manažérov infraštruktúry v rámci opatrení na kontrolu rizík, ktoré musia implementovať v súlade s článkom 4 smernice 2004/49/ES; obstarávateľov alebo výrobcov, keď vyzvú notifikovaný orgán, aby uplatňoval postup overovania ES v súlade s článkom 18 ods. 1 smernice 2008/57/ES, alebo žiadateľa o povolenie na uvedenie vozidiel do prevádzky

(12) „správa o posúdení bezpečnosti“ znamená dokument obsahujúci závery posúdenia, ktoré vykonal orgán pre posudzovanie na posudzovanom systéme;

(13) „nebezpečenstvo“ znamená okolnosť, ktorá by mohla viesť k nehode (EN 50126-2)*;*

(14) „orgán pre posudzovanie“ znamená nezávislú a spôsobilú osobu, organizáciu alebo subjekt uskutočňujúci vyšetrovanie s cieľom dospieť k dôkaznému posúdeniu schopnosti systému spĺňať jeho požiadavky na bezpečnosť;

(15) „kritériá akceptovania rizík“ znamenajú referenčný rámec, v ktorom sa posudzuje prijateľnosť konkrétneho rizika. Tieto kritériá sa používajú s cieľom určiť, či je úroveň rizika dostatočne nízka na to, aby nebolo potrebné prijímať žiadnu okamžitú akciu na jeho ďalšie zníženie;

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(16) „záznam o nebezpečenstve“ znamená dokument, v ktorom sú zaznamenané nebezpečenstvá a ktorý obsahuje odkazy na zistené nebezpečenstvá, s nimi súvisiace opatrenia, ich pôvod a odkaz na organizáciu, ktorá ich musí riadiť;

(17) „identifikácia nebezpečenstva“ znamená proces zistenia, súpisu a charakterizácie nebezpečenstiev (ISO/IEC Guide 73)*;*

(18) „zásada akceptovania rizika“ znamená pravidlá používané s cieľom dospieť k záveru, či riziko súvisiace s jedným alebo viacerými špecifickými nebezpečenstvami je, alebo nie je prijateľné;

(19) „kódex postupov“ znamená písomný súbor pravidiel, ktoré sa pri správnom uplatňovaní môžu použiť na kontrolu jedného alebo viacerých špecifických nebezpečenstiev;

(20) „referenčný systém“ znamená systém, pri ktorého používaní sa preukázala prijateľná úroveň bezpečnosti a vo vzťahu ku ktorému možno porovnaním hodnotiť prijateľnosť rizík vyplývajúcich z posudzovaného systému;

(21) „odhad rizika“ znamená proces používaný na meranie úrovne analyzovaných rizík a pozostáva z týchto krokov: odhad frekvencie, analýza dôsledkov a ich začlenenie (ISO/IEC 73)*;*

(22) „technický systém“ znamená výrobok alebo súbor výrobkov vrátane koncepčnej, implementačnej a podpornej dokumentácie; vývoj technického systému sa začína špecifikovaním jeho požiadaviek a končí sa jeho prijatím; hoci sa berie do úvahy návrh relevantných rozhraní s ľudským správaním, ľudskí operátori ani ich činnosti nie sú zahrnuté do technického systému; proces údržby sa opisuje v príručkách údržby, sám však nie je súčasťou technického systému;

(23) „katastrofický dôsledok“ znamená straty na životoch a/alebo početné závažné zranenia a/alebo veľké škody na životnom prostredí v dôsledku nehody (Table 3 from EN 50126)*;*

(24) „akceptovanie bezpečnosti“ znamená status, ktorý pridelil navrhovateľ zmene na základe správy o posúdení bezpečnosti, ktorú vydal orgán pre posudzovanie;

(25) „systém“ znamená každú časť železničného systému, ktorá podlieha zmene;

(26) „oznámený vnútroštátny predpis“ znamená každý vnútroštátny predpis, ktorý členské štáty oznámia podľa smernice Rady 96/48/ES[4], smernice Európskeho parlamentu a Rady 2001/16/ES[5] a smerníc 2004/49/ES a 2008/57/ES.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

Článok 4. Významné zmeny

Článok 4 ods. 1

Ak v členskom štáte neexistuje žiadny oznámený vnútroštátny predpis na vymedzenie toho, či určitá zmena je, alebo nie je významná, navrhovateľ zváži možný vplyv danej zmeny na bezpečnosť železničného systému.

Ak navrhovaná zmena nemá žiadny vplyv na bezpečnosť, postup riadenia rizík opísaný v článku 5 sa nemusí uplatňovať.

(4) Ú. v. ES L 235, 17.9.1996, s. 6.

(5) Ú. v. ES L 110, 20.4.2001, s. 1.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

[G 1] Ak neexistuje notifikovaný vnútroštátny predpis, za rozhodnutie zodpovedá navrhovateľ. Významnosť zmeny sa opiera o odborný posudok. Napríklad, ak je zamýšľaná zmena v existujúcom systéme zložitá, možno ju hodnotiť ako významnú, keď je vysoké riziko, že ovplyvní existujúce funkcie(6) systému, hoci samotná zmena nevyhnutne nemusí úzko súvisieť s bezpečnosťou.

Článok 4 ods. 2

Ak navrhovaná zmena má vplyv na bezpečnosť, navrhovateľ pomocou odborného posudku rozhodne o významnosti zmeny na základe týchto kritérií:

a) dôsledok zlyhania: hodnoverný scenár najhoršej situácie v prípade zlyhania posudzovaného systému so zohľadnením existencie bezpečnostných bariér mimo systému;

b) inovácie použité pri implementácii zmeny: týka sa to inovácií v železničnom sektore, ako aj toho, čo je nové len pre organizáciu, ktorá implementuje zmenu;

c) zložitosť zmeny;

d) monitorovanie: možnosť monitorovať implementovanú zmenu počas životnosti systému;

e) vratnosť: možnosť vrátiť systém do stavu pred zmenou;

f) adicionalita: posúdenie významnosti zmeny vzhľadom na všetky aktuálne úpravy posudzovaného systému týkajúce sa bezpečnosti, ktoré sa neposúdili ako významné.

Navrhovateľ uchováva zodpovedajúcu dokumentáciu na zdôvodnenie svojho rozhodnutia.

[G 1] **Príklad malých zmien:** po uvedení systému do prevádzky nemusí byť zvýšenie maximálnej rýchlosti na trati o 5 km/h významné. Ak sa však maximálna rýchlosť ďalej zvyšuje po 5 km/h, suma po sebe nasledujúcich zmien (hodnotených jednotlivo ako nevýznamné zmeny) by mohla byť významnou zmenou vzhľadom na vstupné požiadavky na bezpečnosť systému.

[G 2] Ak sa má vyhodnotiť, či je súbor viacerých po sebe nasledujúcich (nevýznamných) zmien významný, pri ich posudzovaní ako celku sa musia posúdiť všetky nebezpečenstvá a súvisiace riziká spojené so všetkými zmenami. Súbor posudzovaných zmien je možné považovať za nevýznamný, ak je výsledné riziko všeobecne prijateľné.

[G 3] Práca agentúry, pokiaľ ide o významné zmeny, ukazuje, že:

a) nie je možné zistiť harmonizované prahové hodnoty ani pravidlá, na základe ktorých by bolo možné rozhodnúť o významnosti konkrétnej zmeny;
b) nie je možné zostaviť vyčerpávajúci zoznam významných zmien;
c) rozhodnutie nemôže platiť pre všetkých navrhovateľov a všetky technické, prevádzkové, organizačné a environmentálne podmienky.

Preto má podstatný význam prenechanie zodpovednosti za rozhodnutie na navrhovateľa, ktorý v súlade s článkom 4 ods. 3 smernice o bezpečnosti železníc {Ref. 1} zodpovedá za bezpečnú prevádzku a kontrolu rizík spojených s jeho časťou systému.

[G 4] Navrhovateľovi môže pomôcť príklad „hodnotenia a použitia kritérií“, uvedených v časti C.2. dodatku C.

(6) *Keďže funkcie v systéme nie sú vždy nezávislé, zmeny niektorých funkcií môžu ovplyvniť iné funkcie systému, hoci by sa mohlo zdať, že sa ich zmeny priamo nedotkli.*

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

[G 5] CSM sa nesmie uplatniť, ak sa zmena súvisiaca s bezpečnosťou, nepovažuje za významnú. To ale neznamená, že sa nedá nič robiť. Navrhovateľ pred rozhodnutím o významnosti zmeny určitým spôsobom (predbežne) riziká analyzuje. Tieto analýzy rizík, ako aj akékoľvek odôvodnenia a argumenty je potrebné dokumentovať, aby sa NBO umožnil audit. Hodnotenie významnosti zmeny a rozhodnutie, že zmena je nevýznamná, musí nezávisle posúdiť orgán pre posudzovanie.

Článok 5. Proces riadenia rizík

Článok 5 ods. 1

Proces riadenia rizík opísaný v prílohe I sa uplatňuje:

a) v prípade významnej zmeny, ako sa uvádza v článku 4, vrátane uvádzania štrukturálnych subsystémov do prevádzky, ako sa uvádza v článku 2 ods. 2 písm. b);

b) v prípade, že sa TSI, ako sa uvádza v článku 2 ods. 2 písm. a), odvoláva na toto nariadenie s cieľom predpísať proces riadenia rizík opísaný v prílohe I.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

Článok 5 ods. 2

Proces riadenia rizík opísaný v prílohe I uplatňuje navrhovateľ.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

Článok 5 ods. 3

Navrhovateľ zabezpečí, aby riziká, ktoré spôsobia dodávatelia a poskytovatelia služieb vrátane ich subdodávateľov, boli riadené. Na tento účel môže navrhovateľ požiadať, aby sa dodávatelia a poskytovatelia služieb vrátane ich subdodávateľov zúčastňovali na procese riadenia rizík opísanom v prílohe I.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

Článok 6. Nezávislé posúdenie

Článok 6 ods. 1

Nezávislé posúdenie správneho uplatňovania procesu riadenia rizík opísaného v prílohe I a výsledkov tohto uplatňovania vykoná orgán, ktorý spĺňa kritériá uvedené v prílohe II. V prípade, že Spoločenstvo alebo vnútroštátna legislatíva ešte neurčili orgán pre posudzovanie, navrhovateľ vymenuje vlastný orgán pre posudzovanie, ktorým môže byť iná organizácia alebo interný odbor.

[G 1] Požadovaná úroveň nezávislosti, ktorú má mať orgán pre posudzovanie, závisí od úrovne bezpečnosti, ktorá sa pre posudzovaný systém požaduje. Očakávajúc harmonizáciu v tejto oblasti, možno nájsť najlepší postup v tejto problematike v ustanovení článku 8 normy IEC61508-1:2001 alebo v odseku § 5.3.9 európskej normy EN 50 129 {Ref. 7}. Stupeň

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

nezávislosti závisí rovnako od závažnosti dôsledkov nebezpečenstva spojeného so zariadením, ako aj s jeho inováciou. V článku § 9.7.2 EN 50 126-2 a v EN 50 129 je vymedzená úroveň nezávislosti pre signalizačné systémy. V zásade by toto vymedzenie bolo možné využiť aj pri iných systémoch.

[G 2] V agentúre sa stále pracuje na vymedzení úloh a povinností rôznych orgánov pre posudzovanie (NBO, NOBO a ISA) a potrebných rozhraní medzi nimi. Vymedzia, kto (podľa možnosti) z týchto orgánov pre posudzovanie, čo a ako má robiť. Napokon to umožní vymedziť:

a) ako na základe dôkazov skontrolovať, či sa správne uplatňovali procesy riadenia rizík a posudzovania rizík, na ktoré sa vzťahuje spoločná bezpečnostná metóda (CSM) a
b) ako podporiť navrhovateľa v jeho rozhodovaní o prijatí významnej zmeny v rámci posudzovaného systému.

Článok 6 ods. 2

Je potrebné zabrániť zdvojeniu práce pri posudzovaní zhody systému riadenia bezpečnosti, ako sa vyžaduje v smernici 2004/49/ES, posudzovaní zhody, ktoré vykonáva notifikovaný orgán alebo vnútroštátny orgán podľa ustanovení smernice 2008/57/ES, a akomkoľvek nezávislom posúdení bezpečnosti, ktoré vykonáva orgán pre posudzovanie v súlade s týmto nariadením.

[G 1] Ďalšie informácie vyplynú z práce agentúry o úlohách a povinnostiach orgánov pre posudzovanie.

Článok 6 ods. 3

Bezpečnostný orgán môže konať ako orgán pre posudzovanie, keď sa významné zmeny týkajú týchto prípadov:

a) ak vozidlo musí mať povolenie na uvedenie do prevádzky, ako sa uvádza v článku 22 ods. 2 a článku 24 ods. 2 smernice 2008/57/ES;

b) ak vozidlo musí mať dodatočné povolenie na uvedenie do prevádzky, ako sa uvádza v článku 23 ods. 5 a článku 25 ods. 4 smernice 2008/57/ES;

c) ak sa bezpečnostné osvedčenie musí aktualizovať z dôvodu podstatnej zmeny druhu alebo rozsahu prevádzky, ako sa uvádza v článku 10 ods. 5 smernice 2004/49/ES;

d) ak sa bezpečnostné osvedčenie musí revidovať z dôvodu podstatných zmien regulačného rámca v oblasti bezpečnosti, ako sa uvádza v článku 10 ods. 5 smernice 2004/49/ES;

e) ak sa bezpečnostné povolenie musí aktualizovať z dôvodu podstatných zmien infraštruktúry, signalizácie alebo zásobovania energiou, alebo zásad ich prevádzky a údržby, ako sa uvádza v článku 11 ods. 2 smernice 2004/49/ES;

f) ak sa bezpečnostné povolenie musí revidovať z dôvodu podstatných zmien regulačného rámca v oblasti bezpečnosti, ako sa uvádza v článku 11 ods. 2 smernice 2004/49/ES.

[G 2] Ďalšie vysvetlenie sa nepovažuje za potrebné.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Článok 6 ods. 4

Keď sa významné zmeny týkajú štrukturálneho subsystému, ktorý musí mať povolenie na uvedenie do prevádzky, ako sa uvádza v článku 15 ods. 1 alebo v článku 20 smernice 2008/57/ES, bezpečnostný orgán môže konať ako orgán pre posudzovanie, ak navrhovateľ už nepridelil túto úlohu notifikovanému orgánu v súlade s článkom 18 ods. 2 uvedenej smernice.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

Článok 7. Správy o posúdení bezpečnosti

Článok 7 ods. 1

Orgán pre posudzovanie poskytne navrhovateľovi správu o posúdení bezpečnosti .

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

Článok 7 ods. 2

V prípade, na ktorý sa odkazuje v článku 5 ods. 1 písm. a), správu o posúdení bezpečnosti zohľadňuje vnútroštátny bezpečnostný orgán vo svojom rozhodnutí povoliť uvedenie subsystémov a vozidiel do prevádzky.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

Článok 7 ods. 3

V prípade, na ktorý sa odkazuje v článku 5 ods. 1 písm. b), nezávislé posúdenie je súčasťou úlohy notifikovaného orgánu, ak sa v TSI neustanovuje inak.
Ak nezávislé posúdenie nie je súčasťou úlohy notifikovaného orgánu, správu o posúdení bezpečnosti zohľadňuje notifikovaný orgán zodpovedný za vydanie osvedčenia o zhode alebo obstarávateľ zodpovedný za vypracovanie vyhlásenia o overení ES.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

Článok 7 ods. 4

V prípade, že systém alebo jeho časť už boli prijaté na základe procesu riadenia rizík uvedeného v tomto nariadení, výslednú správu o posúdení už nespochybní žiadny iný orgán pre posudzovanie zodpovedný za vykonanie nového posúdenia toho istého systému. Uznanie je podmienené preukázaním, že systém sa bude používať za rovnakých funkčných, prevádzkových a environmentálnych podmienok ako systém, ktorý je už schválený, a že sa uplatnili rovnocenné kritériá akceptovania rizika.

[G 1] Táto zásada vzájomného uznávania už bola prijatá v normách CENELEC: pozri časť § 5.5.2 v norme EN 50 129 a časť § 5.9 v norme EN 50 126-2. V CENELEC uplatňujú zásadu vzájomného schvaľovania alebo vzájomného uznávania navrhovatelia alebo nezávislí

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

bezpečnostní posudzovatelia na všeobecné a podobné výrobky a všeobecné a podobné použitia[7] pod podmienkou, že bolo posúdenie bezpečnosti a preukázanie bezpečnosti vykonané v súlade s požiadavkami noriem CENELEC.

[G 2] Vzájomné uznávanie sa musí uplatňovať aj pri prijímaní nových alebo upravených systémov, ak bolo posúdenie rizík a preukázanie súladu systému s požiadavkami na bezpečnosť vykonané v súlade s ustanoveniami nariadenia o CSM {Ref. 3}.

Článok 8. Riadenie kontroly rizík/interné a externé audity

Článok 8 ods. 1

Železničné podniky a manažéri infraštruktúry zahrnú audity uplatňovania spoločnej bezpečnostnej metódy hodnotenia a posudzovania rizík do svojej pravidelnej schémy auditu systému riadenia bezpečnosti, ako sa uvádza v článku 9 smernice 2004/49/ES.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

Článok 8 ods. 2

V rámci úloh vymedzených v článku 16 ods. 2 písm. e) smernice 2004/49/ES národný bezpečnostný orgán sleduje uplatňovanie spoločnej bezpečnostnej metódy hodnotenia a posudzovania rizík.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

Článok 9. Spätná väzba a technický pokrok

Článok 9 ods. 1

Každý manažér infraštruktúry a každý železničný podnik vo svojej výročnej správe o bezpečnosti, na ktorú sa odkazuje v článku 9 ods. 4 smernice 2004/49/ES, stručne informuje o svojich skúsenostiach s uplatňovaním spoločnej bezpečnostnej metódy hodnotenia a posudzovania rizík. Správa obsahuje aj súhrn rozhodnutí týkajúcich sa úrovne významnosti zmien.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

---

(7) *Ďalšie vysvetlenie pojmov „všeobecný a podobný výrobok a všeobecné a podobné použitie“ a príslušných zásad pozri v tomto dokumente v odseku [G 5] v časti 1.1.5 a v poznámkach pod čiarou (9) a (10) na strane 27, ako aj na Obr. 3.*

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Článok 9 ods. 2

Každý národný bezpečnostný orgán vo svojej výročnej správe o bezpečnosti, na ktorú sa odkazuje v článku 18 smernice 2004/49/ES, informuje o skúsenostiach navrhovateľov s uplatňovaním spoločnej bezpečnostnej metódy hodnotenia a posudzovania rizík a prípadne o vlastných skúsenostiach.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

Článok 9 ods. 3

Európska železničná agentúra sleduje uplatňovanie spoločnej bezpečnostnej metódy hodnotenia a posudzovania rizík a zhromažďuje ohlasy na toto uplatňovanie, prípadne dáva Komisii odporúčania na jeho zlepšenie.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

Článok 9 ods. 4

Európska železničná agentúra predloží Komisii najneskôr do 31. decembra 2011 správu, ktorá obsahuje:

a) analýzu skúseností s uplatňovaním spoločnej bezpečnostnej metódy hodnotenia a posudzovania rizík vrátane prípadov, keď navrhovatelia dobrovoľne uplatnili spoločnú bezpečnostnú metódu pred príslušným dňom uplatňovania stanoveným v článku 10;
b) analýzu skúseností navrhovateľov, pokiaľ ide o rozhodnutia týkajúce sa úrovne významnosti zmien;
c) analýzu prípadov, keď sa použili kódexy postupov, ako sa opisuje v oddiele 2.3.8 prílohy I;
d) analýzu celkovej účinnosti spoločnej bezpečnostnej metódy hodnotenia a posudzovania rizík.

Bezpečnostné orgány pomáhajú agentúre určovať prípady uplatňovania spoločnej bezpečnostnej metódy posudzovania a hodnotenia rizík.

[G 2] Ďalšie vysvetlenie sa nepovažuje za potrebné.

Článok 10. Nadobudnutie účinnosti

Článok 10 ods. 1

Toto nariadenie nadobúda účinnosť dvadsiatym dňom nasledujúcim po jeho uverejnení v Úradnom vestníku Európskej únie.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Článok 10 ods. 2

Toto nariadenie sa uplatňuje od 1. júla 2012.

Od 19. júla 2010 sa však uplatňuje:

a) na všetky významné technické zmeny, ktoré sa dotýkajú vozidiel, ako sa uvádza v článku 2 písm. c) smernice 2008/57/ES;

b) na všetky významné technické zmeny, ktoré sa dotýkajú štrukturálnych subsystémov, ak sa to vyžaduje v článku 15 ods. 1 smernice 2008/57/ES alebo v TSI.

[G 2] Ďalšie vysvetlenie sa nepovažuje za potrebné.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

PRÍLOHA I – VYSVETLIVKY K PROCESU UVEDENÉMU V NARIADENÍ O CSM

1. VŠEOBECNÉ ZÁSADY UPLATNITEĽNÉ NA PROCES RIADENIA RIZÍK

1.1. Všeobecné zásady a povinnosti

1.1.1. Proces riadenia rizík, na ktorý sa vzťahuje toto nariadenie, vychádza z definície posudzovaného systému a obsahuje tieto činnosti:

a) proces posudzovania rizík, v ktorom sa identifikujú nebezpečenstvá, riziká, súvisiace bezpečnostné opatrenia a z toho vyplývajúce požiadavky na bezpečnosť, ktoré má spĺňať posudzovaný systém;
b) preukázanie súladu systému s identifikovanými požiadavkami na bezpečnosť a;
c) riadenie všetkých identifikovaných nebezpečenstiev a súvisiacich bezpečnostných opatrení.

Proces riadenia rizík je iteračný a znázorňuje sa v diagrame v dodatku. Proces sa končí preukázaním súladu systému so všetkými požiadavkami na bezpečnosť potrebnými na akceptovanie rizík spojených s identifikovanými nebezpečenstvami.

[G 2] Obr. 1 ilustruje rámec riadenia rizík pre CSM a súvisiaci proces posudzovania rizík. Každý blok (každá činnosť) na tomto obrázku sa podľa potreby ďalej opisuje v samostatnej časti tohto dokumentu.

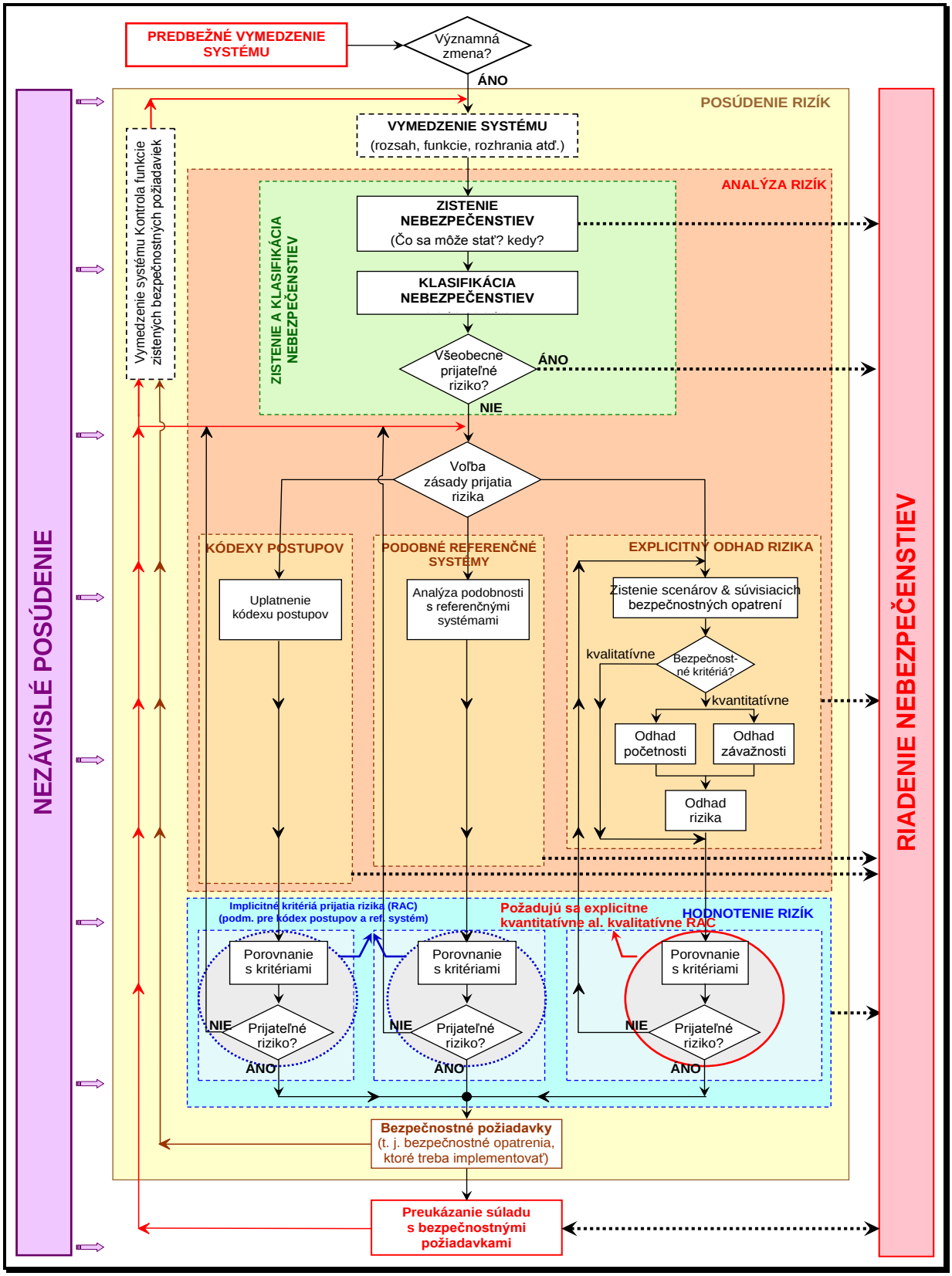
[G 3] CENELEC upozorňuje, že procesy riadenia rizík a hodnotenia rizík sú opísané v bezpečnostnom pláne. Ak to ale z hľadiska projektu nie je vhodné, môže byť takýto opis uvedený v inom príslušnom dokumente. Pozri časť 1.1.6.

[G 4] Proces posudzovania rizík sa začína predbežným vymedzením systému. Počas vypracovania projektu sa predbežné vymedzenie systému postupne aktualizuje a nahradí sa vymedzením systému (definíciou systému). Ak neexistuje žiadne predbežné vymedzenie systému, na vykonanie posúdenia rizík sa použije formálne vymedzenie systému. Potom ale je užitočné, aby sa na začiatku projektu stretli všetci aktéri, ktorých sa významná zmena týka a aby sa dohodli na:

a) celkových systémových zásadách, funkciách systému atď. V zásade by toto mohlo byť opísané v predbežnom vymedzení systému;
b) organizácii projektu;
c) rozdelení úloh a povinností jednotlivých už zúčastnených aktérov, podľa potreby vrátane NBO, NOBO a ISA.

Takáto koordinácia, napr. počas predbežného vymedzovania systému, umožní navrhovateľovi a podľa potreby subdodávateľom, NBO, NOBO a ISA včas sa dohodnúť na kódexoch postupov alebo referenčných systémoch, ktoré sú prijateľné na využitie v rámci projektu.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu



Obr. 1: Rámec riadenia rizík v nariadení o CSM {Ref. 3}.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

1.1.2. Tento iteračný proces riadenia rizík:

a) obsahuje príslušné činnosti na zabezpečenie kvality a vykonáva ho spôsobilý personál;
b) nezávisle ho posudzuje jeden orgán alebo viaceré orgány pre posudzovanie.

[G 1] Systémy riadenia bezpečnosti (*Safety Managment Systems;* SMS) železničného podniku a manažéra infraštruktúry ustanovujú procesy a postupy, ktorými sa:

a) monitoruje, či je systém bezpečný počas celého svojho životného cyklu (t. j. počas svojej prevádzky a údržby);
b) zaisťuje bezpečné zrušenie alebo výmena súvisiaceho systému.

Tento proces nie je súčasťou CSM posudzovania rizík.

[G 2] Na implementáciu CSM je potrebné, aby všetky zúčastnené strany boli spôsobilé (t. j. mali náležité zručnosti, znalosti a skúsenosti). V organizáciách aktérov železničného sektora je stála potreba riadenia spôsobilosti:

a) u manažérov infraštruktúry a v železničných podnikoch to patrí do pôsobnosti ich systému riadenia bezpečnosti (SMS) podľa odseku 2 písm. e) prílohy III k smernici o bezpečnosti železníc {Ref. 1};
b) iní aktéri, ktorých činnosti môžu ovplyvniť bezpečnosť železničného systému, hoci SMS nie je povinný, majú vo všeobecnosti aspoň na úrovni projektu (pozri odsek [G 1] v časti 5.1) proces riadenia kvality (QMP) a/alebo proces riadenia bezpečnosti (SMP), ktoré sa vzťahujú na túto požiadavku.

[G 3] Nasledujúce odseky normy CENELEC EN 50126-1 {Ref. 8} ustanovujú usmernenie o spôsobilosti:

a) podľa článku § 5.3.5 písm. b): *„všetky osoby majúce zodpovednosť v rámci procesu manažmentu RAMS musia byť spôsobilé na plnenie svojich povinností“;*
b) podľa článku § 5.3.5 písm. d): “požiadavky tejto normy sa musia zaviesť do obchodných postupov na základe systému manažmentu kvality (QMS) spĺňajúceho požiadavky *EN ISO 9001, EN ISO 9002 alebo EN ISO 9003 príslušnej pre uvažovaný systém“*. Príklad aspektov, ktoré systém riadenia kvality kontroluje, je uvedený v článku § 5.2 normy EN 50 129 {Ref. 7}.

Tieto sa vzťahujú na činnosti zaisťovania kvality, ako aj na spôsobilosť a odbornú prípravu personálu/osôb, vyžadovanú na podporu procesu, v ktorom sa uplatňuje CSM.

[G 4] Orgán pre posudzovanie veľmi často sleduje proces posudzovania rizík od samého začiatku projektu, ale pokiaľ to nevyžadujú vnútroštátne právne predpisy členského štátu, takéto včasné zapojenie posudzujúceho orgánu nie je povinné, i keď sa odporúča. Stanovisko nezávislého orgánu pre posudzovanie by mohlo byť užitočné pred prechodom z jedného kroku posúdenia rizík na nasledujúci. Ďalšie podrobnosti o nezávislom posudzovaní pozri v Článok 6.

1.1.3. Navrhovateľ zodpovedný za proces riadenia rizík, požadovaný týmto nariadením, vedie záznam o nebezpečenstve v súlade s oddielom 4.

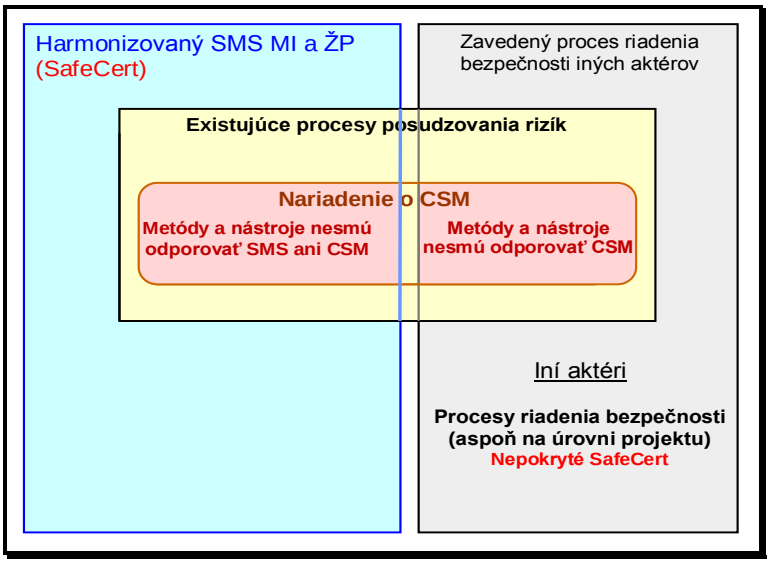
[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

1.1.4. Aktéri, ktorí už majú zavedené metódy alebo nástroje na posudzovanie rizík, ich môžu ďalej uplatňovať, pokiaľ sú kompatibilné s ustanoveniami tohto nariadenia a s výhradou týchto podmienok:

a) metódy alebo nástroje na posudzovanie rizík sa opisujú v systéme riadenia bezpečnosti, ktorý schválil národný bezpečnostný orgán v súlade s článkom 10 ods. 2 písm. a) alebo článkom 11 ods. 1 písm. a) smernice 2004/49/ES, alebo;
b) metódy alebo nástroje na posudzovanie rizík sa požadujú v TSI alebo sú v súlade s verejne dostupnými uznanými normami uvedenými v notifikovaných vnútroštátnych predpisoch.

[G 2] Obr. 2 predstavuje vzťah medzi CSM a „procesmi systému riadenia bezpečnosti a posudzovania rizík“.



Obr. 2: Harmonizovaný SMS a CSM.

1.1.5. Bez toho, aby bola dotknutá občianskoprávna zodpovednosť v súlade s právnymi požiadavkami členských štátov, je za proces posudzovania rizík zodpovedný navrhovateľ. Navrhovateľ predovšetkým rozhoduje so súhlasom príslušných aktérov, kto bude zodpovedať za splnenie požiadaviek na bezpečnosť vyplývajúcich z posudzovania rizík. Toto rozhodnutie závisí od typu bezpečnostných opatrení zvolených na kontrolu rizík na prijateľnej úrovni. Preukázanie súladu s požiadavkami na bezpečnosť sa uskutočňuje v súlade s oddielom 3.

[G 1] Ak je navrhovateľ manažérom infraštruktúry alebo železničným podnikom, niekedy môže byť potrebné zapojiť do procesu[8] ďalších aktérov (pozri časť 1.2.1). V niektorých prípadoch si manažér infraštruktúry alebo železničný podnik pravdepodobne objedná činnosti posudzovania rizík alebo ich časť v subdodávke. Úlohy a povinnosti každého aktéra sa zvyčajne dohodnú medzi príslušnými aktérmi v začiatočnej fáze projektu.

(8) *Toto je v súlade s dodatkom A.4 k norme CENELEC EN 50 129 {Ref. 7}.*

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

[G 2] Je dôležité poznamenať, že navrhovateľ vždy ostáva zodpovedný za uplatnenie CSM, akceptovanie rizika, a teda za bezpečnosť systému. Jeho úlohou bude zabezpečiť, aby:

a) zúčastnení aktéri v plnom rozsahu spolupracovali tak, aby boli zabezpečené všetky potrebné informácie;
b) bolo jasné, kto musí plniť jednotlivé požiadavky CSM (napr. prevezme analýzu rizík alebo vedenie záznamov o nebezpečenstve).

Ak sa aktéri nedohodnú, ktoré požiadavky na bezpečnosť majú plniť, môžu požiadať o stanovisko NBO. Ale zodpovednosť za nájdenie riešenia stále ostáva na navrhovateľovi a nemožno ju preniesť na NBO. Pozri aj časť 0.2.2..

[G 3] Ak je úloha objednaná ako subdodávka, subdodávateľ nie je povinný mať vlastnú organizáciu bezpečnosti, ak nie je manažérom infraštruktúry alebo železničným podnikom, alebo najmä ak má malú štruktúru/veľkosť alebo ak je obmedzený jeho podiel na celkovom systéme. Zodpovednosť za riadenie rizík vrátane posudzovania rizík a činností riadenia nebezpečenstiev môže zostať na organizácii vyššej úrovne (t. j. na zákazníkovi subdodávateľa). Subdodávateľ však vždy zodpovedá za poskytovanie správnych informácií vzťahujúcich sa na jeho činnosť a potrebných pre organizáciu vyššej úrovne na budovanie dokumentácie o riadení rizík.
Spolupracujúce organizácie sa tiež môžu dohodnúť, že ustanovia spoločnú organizáciu bezpečnosti, napr. s cieľom optimalizovať náklady. V takom prípade bude riadiť bezpečnostné činnosti všetkých zúčastnených organizácií len jedna organizácia. Zodpovednosť za presnosť informácií (o nebezpečenstvách, rizikách a bezpečnostných opatreniach), ako aj za riadenie implementácie bezpečnostných opatrení zostáva organizácii kontrolujúcej nebezpečenstvá, s ktorými sú tieto bezpečnostné opatrenia spojené.

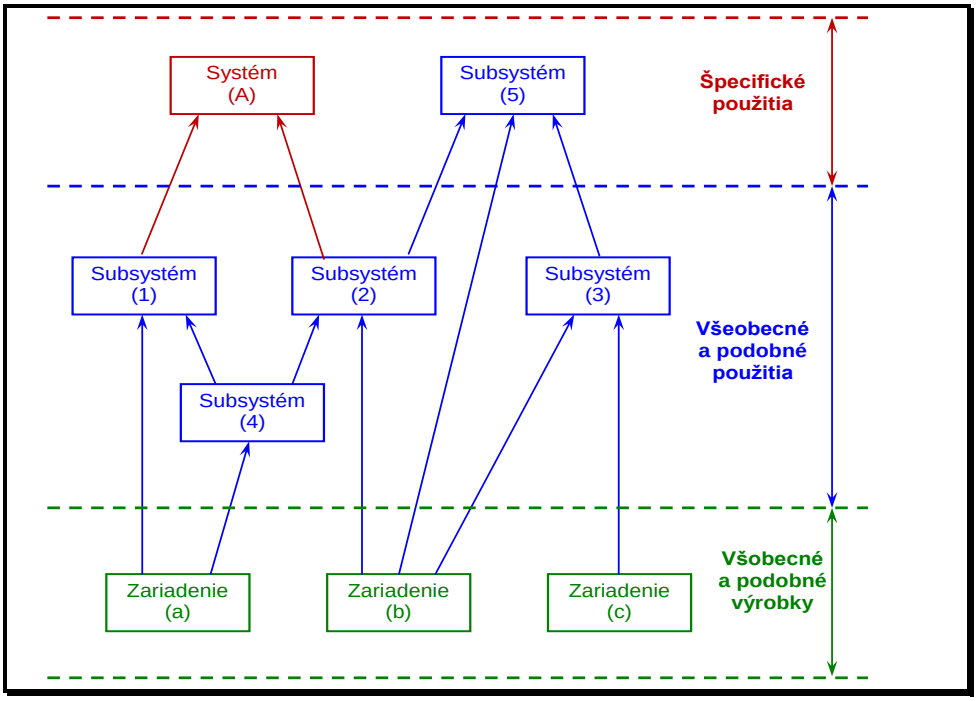
[G 4] Navrhovateľ zvyčajne stanoví „úrovne bezpečnosti“ a „požiadavky na bezpečnosť“ pridelené aktérom zúčastneným na projekte a rôznym subsystémom a zariadeniam týchto aktérov:

a) v zmluvách medzi navrhovateľom a príslušnými aktérmi (subdodávateľmi);
b) v bezpečnostnom pláne alebo inom príslušnom dokumente na rovnaký účel, s opisom celkovej organizácie projektu a povinností každého aktéra vrátane navrhovateľových: pozri časť 1.1.6;
c) v zázname o nebezpečenstve navrhovateľa: pozri časť 4.1.1.

Toto pridelenie „úrovní bezpečnosti“ a „požiadaviek“ systému podriadeným subsystémom a zariadeniam, a teda príslušným aktérom vrátane navrhovateľa samého, je možné spresniť/rozšíriť počas fázy „preukázania súladu systému s požiadavkami na bezpečnosť“: pozri Obr. 1. V porovnaní s V-cyklom CENELEC (pozri časť 2.1.1 a Obr. 5 na strane 33), táto činnosť zodpovedá fáze 5, ktorá sa zaoberá „prideľovaním systémových požiadaviek“ jednotlivým subsystémom a prvkom.

[G 5] Článok 5 ods. 2 umožňuje, aby okrem ŽP a MI, ďalší aktéri prevzali celkovú zodpovednosť za súlad s CSM podľa svojich vlastných potrieb. Za všeobecné a podobné výrobky alebo všeobecné a podobné použitia[9] môže napríklad výrobca vykonať posúdenie rizík na základe „vymedzenia všeobecného a podobného systému“ a potom špecifikovať úrovne bezpečnosti a požiadavky na bezpečnosť, ktoré všeobecné a podobné výrobky a všeobecné a podobné použitia musia spĺňať.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu



Obr. 3: Príklad závislostí medzi bezpečnostnými dokumentáciami (podľa obrázka 9 normy EN 50 129).

[G 6] CENELEC upozorňuje, že výrobca zabezpečuje dokumentárny dôkaz o posúdení rizík v bezpečnostných preukazoch a zázname o nebezpečenstve všeobecného a podobného výrobku (resp. všeobecného a podobného použitia[9]). Tieto bezpečnostné preukazy a záznamy o nebezpečenstve obsahujú všetky predpoklady[10] a zistené „obmedzenia

---

(9) *Termíny „všeobecné a podobné aplikácie“ a „všeobecné a podobné výrobky“ sú prevzaté z noriem CENELEC, podľa ktorých je možné rozlišovať tri rôzne kategórie „bezpečnostných preukazov“ (pozri Obr. 3):*

a) ***Bezpečnostná dokumentácia všeobecného a podobného výrobku*** *(nezávislého od použitia). Všeobecný a podobný výrobok je možné opakovane použiť na rôzne nezávislé aplikácie;*

b) ***Bezpečnostná dokumentácia všeobecnej a podobnej aplikácie*** *(pre triedu použitia). Všeobecnú a podobnú aplikáciu je možné opakovane použiť v triede/druhu použitia so spoločnými funkciami;*

c) ***Bezpečnostná dokumentácia špecifického použitia*** *(pre špecifickú aplikáciu). Špecifická aplikácia/ špecifické použitie je použitie len na jednom určitom zariadení.*

Viac informácií o ich vzájomnej závislosti pozri v časti 9.4 a na obrázku 9.1 usmernenia k norme CENELEC 50 126-2 {Ref. 9}.

(10) *Tieto predpoklady a obmedzenia použitia určujú medze a platnosť „bezpečnostných posúdení“ a „bezpečnostných analýz“ spojených s bezpečnostnými dokumentáciami príslušného všeobecného a podobného výrobku a príslušnej všeobecnej a podobnej aplikácie. Ak ich posudzovaná špecifická aplikácia nespĺňa, je potrebné zodpovedajúce „bezpečnostné posúdenia“ a „bezpečnostné analýzy“ (napr. analýzy príčin) aktualizovať alebo nahradiť novými.*

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

používania“ (t. j. podmienky aplikácie súvisiace s bezpečnosťou), ktoré je možné uplatniť na generické výrobky (resp. generickú aplikáciu). Preto vždy, keď sa generický výrobok a generická aplikácia používajú v prevádzke v konkrétnej aplikácii, je potrebné pri každej konkrétnej aplikácii preukázať súlad so všetkými týmito predpokladmi(10) a „obmedzeniami použitia“ (alebo bezpečnostnými podmienkami príslušnej aplikácie).

1.1.6. Prvým krokom procesu riadenia rizík je identifikovať v dokumente, ktorý má vypracovať navrhovateľ, úlohy jednotlivých aktérov, ako aj ich činnosti riadenia rizík. Navrhovateľ koordinuje úzku spoluprácu medzi jednotlivými zúčastnenými aktérmi v súlade s ich príslušnými úlohami s cieľom riadiť nebezpečenstvá a s nimi spojené bezpečnostné opatrenia.

[G 1] Pokiaľ sa v zmluvách na začiatku projektu nedohodne inak, veľmi často býva v každom projekte dokument, v ktorom sa opisujú činnosti riadenia rizík. Príslušný dokument sa aktualizuje a reviduje vždy po vykonaní významných úprav pôvodného systému.

[G 2] Tento dokument ustanovuje organizačnú štruktúru, rozdelenie povinností personálu, procesy, postupy a činnosti, ktoré spoločne zaisťujú, aby posudzovaný systém vyhovoval stanoveným úrovniam bezpečnosti a požiadavkám na bezpečnosť. Dokument musí byť v súlade s CSM, pretože podporuje orgán pre posudzovanie a poskytuje mu usmernenie. Normy CENELEC odporúčajú, aby sa tento druh informácií zaradil do bezpečnostného plánu alebo iného dokumentu, obsahujúceho časť venovanú týmto témam.

[G 3] V bezpečnostnom pláne alebo inom príslušnom dokumente navrhovateľ uvádza najmä celkovú organizáciu projektu. Opisuje rozdelenie úloh a povinností medzi zúčastnenými aktérmi. Môže odkazovať na podrobné informácie v bezpečnostných plánoch alebo organizácii bezpečnosti rôznych zúčastnených aktérov. Zvyčajne sa prípadná deľba povinností medzi rôznych aktérov prerokuje a dohodne počas predbežného vymedzovania systému (t. j. na začiatku projektu).

[G 4] Bezpečnostný plán je živý dokument, ktorý sa počas projektu podľa potreby aktualizuje.

[G 5] Viac podrobností o obsahu bezpečnostného plánu možno nájsť v norme EN 50 126-1 {Ref. 8} a príslušnom usmernení EN 50 126-2 {Ref. 9}.

Continuation of the footnote

> *Toto je v súlade s nasledujúcou všeobecnou bezpečnostnou zásadou: „Vždy, keď sa návrh špecifického (sub-)systému zakladá na všeobecných alebo podobných použitiach a všeobecných alebo podobných výrobkoch, musí sa preukázať, že špecifický (sub)systém spĺňa všetky predpoklady a obmedzenia použitia (v CENELEC nazývané bezpečnostnými podmienkami použitia), ktoré sú exportované do zodpovedajúcich bezpečnostných preukazov všeobecného alebo podobného použitia a všeobecného alebo podobného výrobku (pozri Obr. 3).“*

Ak na úrovni subsystému nie je možné dosiahnuť súlad špecifickej aplikácie s niektorými predpokladmi a obmedzeniami použitia (napr. v prípade požiadaviek prevádzkovej bezpečnosti), je možné preniesť zodpovedajúce predpoklady a obmedzenia použitia na vyššiu úroveň (t. j. obvykle na úroveň systému). Tieto predpoklady a obmedzenia použitia sú potom jasne identifikované v „bezpečnostnom preukaze špecifického použitia“ príslušného subsystému. V týchto príkladoch závislosti je podstatné zabezpečiť, aby bezpečnostné podmienky každého bezpečnostného preukazu príslušného použitia boli splnené v bezpečnostnom preukaze vyššej úrovne alebo sa preniesli do podmienok použitia bezpečnostného preukazu najvyššej úrovne (t. j. do bezpečnostného preukazu systému).

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

1.1.7. Hodnotenie správneho uplatňovania procesu riadenia rizík opísaného v tomto nariadení patrí do zodpovednosti orgánu pre posudzovanie.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

1.2. Riadenie rozhraní

1.2.1. Pre každé rozhranie relevantné pre posudzovaný systém a bez toho, aby boli dotknuté špecifikácie rozhraní vymedzené v príslušných TSI, príslušní aktéri v železničnom sektore spolupracujú s cieľom identifikovať a spoločne riadiť nebezpečenstvá a súvisiace bezpečnostné opatrenia, ktoré sa na týchto rozhraniach musia riešiť. Riadenie spoločných rizík na rozhraniach koordinuje navrhovateľ.

[G 1] Napríklad, ak železničný podnik z prevádzkových dôvodov potrebuje, aby manažér infraštruktúry vykonal vymedzené zmeny infraštruktúry, ŽP monitoruje podľa požiadaviek uvedených v odseku 2 písm. g) prílohy III k smernici o bezpečnosti železníc {Ref. 1} aj celú prácu s cieľom zaistiť správne vykonanie očakávaných zmien. Vedúca úloha ŽP však nezbavuje príslušného MI povinnosti informovať ostatné železničné podniky, ak sa aj ich dotkne príslušná zmena infraštruktúry. MI pravdepodobne bude musieť vykonať posúdenie rizík v súlade s nariadením o CSM, ak je podľa neho súvisiaca zmena významná.

[G 2] Prechody povinností medzi rôznymi aktérmi sú možné a za určitých okolností dokonca nevyhnutné. Keď sú však do systému zapojení viacerí aktéri, veľmi často sa určí jeden, ktorý zodpovedá za systém ako celok. Medzi subsystémami a prevádzkami sú vždy závislosti, ktorých zistenie si vyžaduje osobitné úsilie. Preto je potom potrebné, aby niekto prevzal celkovú zodpovednosť za analýzy bezpečnosti a mal tiež prístup ku všetkej príslušnej dokumentácii. Všeobecne má celkovú zodpovednosť za systematické a úplné posúdenie rizík zrejme navrhovateľ, ktorý má v úmysle zaviesť významnú zmenu.

[G 3] Hlavné kritériá, ktoré sa musia dohodnúť v súvislosti s riadením rozhrania medzi príslušnými aktérmi, sú:

a) vedenie, ktoré zvyčajne zabezpečuje navrhovateľ, ktorý má úmysle zaviesť významnú zmenu;
b) požadované vstupy;
c) metódy zisťovania nebezpečenstiev a posudzovania rizík;
d) požadovaní účastníci s potrebnou spôsobilosťou (t. j. kombináciou znalostí, zručností a praktickej skúsenosti – pozri vymedzenie „spôsobilosti personálu“ v odseku [G 2] písm. b) k článku 3 v {Ref. 4});
e) očakávané výstupy.

Tieto kritériá sú opísané v bezpečnostných plánoch (alebo iných relevantných dokumentoch) podnikov, ktoré sa zaoberajú jednotlivými rozhraniami.

[G 4] Príklady rozhraní sú uvedené v časti C.3. dodatku C, ako aj príklad uplatnenia týchto hlavných kritérií na riadenie rozhrania medzi výrobcom vlakov a manažérom infraštruktúry alebo železničným podnikom.

[G 5] Riadenie rozhraní musí pri návrhu týchto rozhraní zohľadniť aj riziká, ktoré môžu vzniknúť na rozhraniach prevádzkovaných človekom (počas prevádzky a údržby).

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

1.2.2. Ak na účely splnenia požiadaviek na bezpečnosť niektorý aktér identifikuje nutnosť bezpečnostného opatrenia, ktoré sám nemôže implementovať, po dohode s iným aktérom môže presunúť riadenie súvisiaceho nebezpečenstva na tohto druhého aktéra pomocou procesu opísaného v oddiele 4.

[G 1] Proces prenosu nebezpečenstiev a s nimi spojených bezpečnostných opatrení medzi aktérmi je možné uplatniť aj na nižších úrovniach životného cyklu podľa CENELEC na Obr. 5 na strane 33. Možno ho uplatniť napr. vždy, keď je potrebná výmena týchto informácií medzi aktérom a jeho subdodávateľmi. Rozdiel oproti tomu istému procesu na úrovni systému je v tom, že navrhovateľ nepotrebuje byť informovaný o všetkých prenosoch nebezpečenstiev a s nimi spojených bezpečnostných opatrení na úrovni subsystémov. Navrhovateľ je informovaný, len keď prenášané nebezpečenstvá a s nimi spojené bezpečnostné opatrenia majú vzťah s rozhraniami vysokej úrovne (t. j. keď ovplyvnia rozhranie s navrhovateľom).

1.2.3. Pokiaľ ide o posudzovaný systém, každý aktér, ktorý zistí, že určité bezpečnostné opatrenie nie je v súlade alebo je neadekvátne, zodpovedá za notifikáciu tejto skutočnosti navrhovateľovi, ktorý potom informuje aktéra implementujúceho bezpečnostné opatrenie.

[G 1] Systém riadenia bezpečnosti (SMS) ŽP a MI obsahuje opatrenia a postupy, ktorými sa zabezpečuje správne zvládnutie nesúladu alebo nevhodnosti bezpečnostných opatrení. Tieto opatrenia a postupy preto nie sú súčasťou CSM.

[G 2] Podobne opatrenia a postupy[(11)], ktoré musia zaviesť ďalší aktéri[(12)] na správne zvládnutie nesúladu a nevhodnosti bezpečnostných opatrení a podľa potreby prenos bezpečnostných opatrení na všetkých príslušných aktérov sa dohodnú na začiatku projektu a podrobne rozvedú v ich bezpečnostnom pláne: pozri časť 0.2.

1.2.4. Aktér implementujúci bezpečnostné opatrenie potom informuje všetkých aktérov, ktorých sa dotýka daný problém, buď v rámci posudzovaného systému, alebo v rámci iných existujúcich systémov využívajúcich rovnaké bezpečnostné opatrenie, pokiaľ je to aktérovi známe.

[G 1] To potom umožní zvládnuť možný nesúlad alebo možnú nevhodnosť bezpečnostného opatrenia v posudzovanom systéme alebo v podobných systémoch, ktorý využíva to isté opatrenie.

1.2.5. Ak nemožno dosiahnuť dohodu medzi dvoma alebo viacerými aktérmi, za nájdenie adekvátneho riešenia je zodpovedný navrhovateľ.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

---

(11) V zásade tieto opatrenia a postupy pokrýva riadenie kvality a/alebo proces riadenia bezpečnosti uvedených aktérov ustanovený aspoň na úrovni projektu (pozri aj Obr. 2).

(12) Pojem „ďalší aktéri“ označuje všetkých ostatných aktérov, ktorí nie sú MI ani ŽP.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

1.2.6.	*Ak aktér nemôže plniť požiadavku v notifikovanom vnútroštátnom predpise, navrhovateľ požiada o radu príslušný orgán.*

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

1.2.7.	*Nezávisle od definície posudzovaného systému je navrhovateľ zodpovedný za zabezpečenie toho, aby sa riadenie rizík vzťahovalo na samotný systém a na integráciu do železničného systému ako celku.*

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

2. OPIS PROCESU POSUDZOVANIA RIZÍK

2.1. Všeobecný opis – zhoda medzi procesom posudzovania rizík CSM a V-cyklom CENELEC

2.1.1. Proces posudzovania rizík je celkový iteračný proces, ktorý obsahuje:

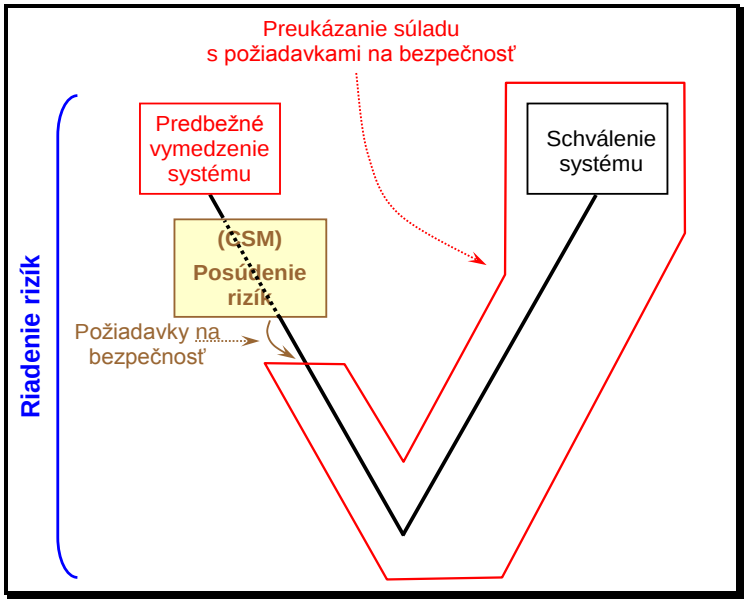
a) definovanie systému;
b) analýzu rizík vrátane identifikácie nebezpečenstva;
c) hodnotenie rizík.

Proces posudzovania rizík je v interakcii s riadením nebezpečenstva podľa oddielu 4.1.

[G 1] Proces riadenia rizík, na ktorý sa vzťahuje CSM, je možné prezentovať ako V-cyklus, ktorý sa začína (predbežným) vymedzením systému a končí schválením systému: pozri Obr. 4.. Tento zjednodušený V-cyklus možno potom nájsť aj na klasickom V-cykle na obrázku 10 v norme EN 50 126-1 {Ref. 8}. Obr. 10 životného cyklu systému CENELEC je pre porovnanie vzťahu s procesom riadenia rizík podľa nariadenia o CSM na Obr. 1, znovu pripomenutý na Obr. 5:

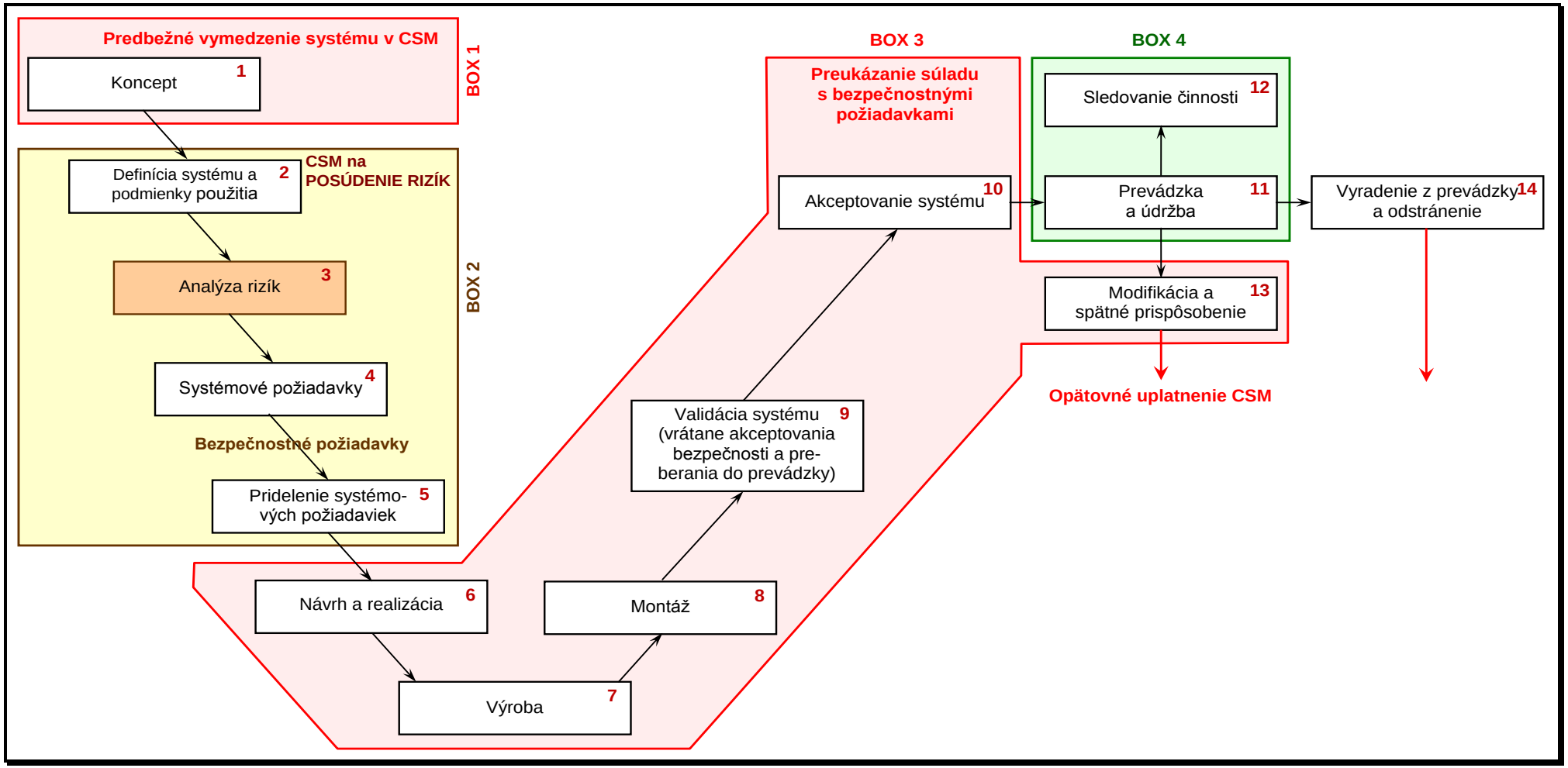
a) „predbežné vymedzenie systému“ CSM na Obr. 1 zodpovedá vo V-cykle CENELEC fáze 1, t. j. vymedzeniu „konceptu“ systému (pozri BOX 1 na Obr. 5);
b) „posúdenie rizík“ CSM na Obr. 1 zahŕňa nasledujúce fázy V-cyklu CENELEC (pozri BOX 2 na Obr. 5):

(1) fázu 2 na Obr. 5: „definíciu systému a podmienky použitia“;
(2) fázu 3 na Obr. 5: „analýzu rizík“;
(3) fázu 4 na Obr. 5: „systémové požiadavky“;
(4) fázu 5 na Obr. 5: „pridelenie systémových požiadaviek“ rôznym subsystémom a komponentom.



Obr. 4: Zjednodušený V-cyklus podľa obrázka 10 v norme EN 50 126.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu



Obr. 5: Obr. 10 V-cyklu z normy EN 50 126 (životný cyklus systému CENELEC).

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

[G 2] Výstupy z procesu posudzovania rizík CSM (po iteráciách – pozri Obr. 1) sú:

a) „vymedzenie systému“ aktualizované o „požiadavky na bezpečnosť“, ktoré vyplynuli z činností „analýzy rizík“ a „hodnotenia rizík“ (pozri časť 2.1.6);
b) „pridelenie systémových požiadaviek“ na rôzne subsystémy a komponenty (fáza 5 na obrázku 5);
c) „záznam o nebezpečenstve“, v ktorom sú zaznamenané:

(1) všetky zistené nebezpečenstvá a s nimi spojené bezpečnostné opatrenia,
(2) vyplývajúce požiadavky na bezpečnosť,
(3) predpoklady, zohľadnené vo vymedzení systému, ktoré určujú hranice a platnosť posúdenia rizík (pozri písm. g) v časti 2.1.2);

d) a vo všeobecnosti všetky dôkazy, ktoré sú výsledkom uplatňovania CSM: pozri časť 5.

Uvedené výstupy posúdenia rizík podľa CSM zodpovedajú bezpečnostným výstupom fázy 4 V-cyklu CENELEC, t. j. špecifikácii systémových požiadaviek na Obr. 5.

[G 3] Vymedzenie systému aktualizované o výsledky posúdenia rizík a záznam o nebezpečenstve tvoria vstupy, na základe ktorých sa systém navrhuje a schvaľuje. „Preukázanie súladu systému s požiadavkami na bezpečnosť“ podľa nariadenia o CSM zodpovedá nasledujúcim fázam V-cyklu CENELEC (pozri BOX 3 na Obr. 5):

a) fáze 6 na Obr. 5: „návrhu a realizácii“;
b) fáze 7 na Obr. 5: „výrobe“;
c) fáze 8 na Obr. 5: „montáži“;
d) fáze 9 na Obr. 5: „validácii (overovaniu) systému“ (vrátane akceptovania bezpečnosti a uvedenia do prevádzky)“
e) fáze 10 na Obr. 5: „akceptovaniu systému“.

[G 4] Preukázanie súladu systému s požiadavkami na bezpečnosť závisí od toho, či je významná zmena technická, prevádzková alebo organizačná. Preto rôzne kroky V-cyklu CENELEC na Obr. 5 pravdepodobne nebudú vhodné pre všetky významné zmeny daného druhu. Podľa toho je potrebné V-cyklus na Obr. 5 posúdiť a na základe primeraného úsudku použiť pre každú konkrétnu aplikáciu to, čo je vhodné (napr. pri prevádzkových a organizačných zmenách nebude výrobná fáza).

[G 5] To znamená, že „preukázanie súladu systému s požiadavkami na bezpečnosť“ podľa nariadenia o CSM neobsahuje iba činnosti „verifikácie a validácie“ (overovania a potvrdenia) skúškami alebo simuláciou. Prakticky pokrýva všetky fázy „6 až 10“ V-cyklu CENELEC (pozri uvedený zoznam a Obr. 5). Zahŕňa činnosti návrhu, výroby, montáže, overovania a potvrdzovania, ako aj s tým spojené činnosti RAMS a akceptovania systému.

[G 6] Hlavnou zásadou pri „preukazovaní súladu systému s požiadavkami na bezpečnosť“ je zameranie posudzovania rizík len na funkcie a rozhrania systému, ktoré súvisia s bezpečnosťou. To znamená, že keď sa v rámci niektorej fázy V-cyklu CENELEC na Obr. 5 vyžadujú činnosti posudzovania rizík a bezpečnosti, zamerajú sa na:

a) funkcie a rozhrania súvisiace s bezpečnosťou;
b) subsystémy a/alebo prvky zapojené do dosahovania funkcií a/alebo rozhraní súvisiacich s bezpečnosťou, posudzovaných počas činností posudzovania rizík vyššej úrovne.

[G 7] Z porovnania s klasickým V-cyklom CENELEC na Obr. 5 potom vyplýva, že:

a) CSM sa kryje s fázami „1 až 10“ a fázou „13“ tohto V-cyklu. Zahŕňa súbor činností vyžadovaných na akceptovanie posudzovaného systému;

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

b) CSM neobsahuje fázy „11“, „12“ a „14“ životného cyklu systému:

(1) fáza „11“ súvisí s „prevádzkou a údržbou“ a fáza „12“ so „sledovaním činnosti“ systému po jeho schválení na základe CSM. Na tieto dve fázy sa vzťahuje systém riadenia bezpečnosti (SMS) ŽP a MI – (pozri BOX 4 na Obr. 5). Ak sa však počas prevádzky, údržby alebo sledovania činnosti systému ukáže potreba systém upraviť, alebo ho uviesť do predchádzajúceho stavu (fáza 13 na Obr. 5), aj keď už je v prevádzke, uplatní sa na nové požadované zmeny znovu CSM v súlade s Článok 2. Preto, ak je zmena významná:

(i) uplatňujú sa na tieto nové zmeny procesy riadenia rizík a posudzovania rizík podľa nariadenia o CSM;
(ii) na tieto nové zmeny je potrebné schválenie v súlade s Článok 6;

(2) „vyradenie z prevádzky a odstránenie“ systému, ktorý je už v prevádzke (fáza 14), by sa tiež dalo považovať za významnú zmenu, a preto by sa na fázu 14 na Obr. 5 znovu mohla uplatniť CSM v súlade s Článok 2.

Viac informácií o obsahu a rozsahu každej fázy alebo činnosti V-cyklu CENELEC, znázorneného na Obr. 5, pozri v časti § 6 normy EN 50 126-1 {Ref. 8}.

2.1.2. Vymedzenie systému by sa malo zaoberať aspoň týmito otázkami:

a) cieľ systému, napr. predpokladaný účel;
b) prípadné funkcie a prvky systému (vrátane napr. ľudských, technických a prevádzkových prvkov);
c) hranica systému vrátane iných interakčných systémov;
d) fyzické (t. j. interakčné systémy) a funkčné (t. j. funkčný vstup a výstup) rozhrania;
e) prostredie systému (napr. energetický a tepelný tok, nárazy, vibrácie, elektromagnetická interferencia, prevádzkové použitie);
f) existujúce bezpečnostné opatrenia a po iteráciách vymedzenie požiadaviek na bezpečnosť, ktoré sa určili na základe procesu posudzovania rizík;
g) predpoklady, ktorými sa ustanoví ohraničenie pre posudzovanie rizík.

[G 2] Ďalšie vysvetlenie sa nepovažuje za potrebné.

2.1.3. Identifikácia nebezpečenstva sa vykonáva na vymedzenom systéme v súlade s oddielom 2.2.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

2.1.4. Prijateľnosť rizík posudzovaného systému sa vyhodnocuje pomocou jednej alebo viacerých zásad akceptovania rizika:

a) uplatňovanie kódexov postupov (oddiel 2.3);
b) porovnanie s podobnými systémami (oddiel 2.4);
c) jednoznačný odhad rizika (oddiel 2.5).

V súlade so všeobecnou zásadou uvedenou v oddiele 1.1.5 orgán pre posudzovanie neuloží navrhovateľovi povinnosť použiť zásadu akceptovania rizika.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

[G 1] Vo všeobecnosti bude navrhovateľ rozhodovať, ktorá zásada akceptovania rizika je najvhodnejšia na kontrolovanie zistených nebezpečenstiev, podľa konkrétnych požiadaviek projektu, ako aj vlastných skúseností s uvedenými troma zásadami.

[G 2] Nie vždy je možné vyhodnotiť prijateľnosť rizík na úrovni systému s použitím jednej z troch zásad akceptovania rizika. Akceptovania rizika sa často bude zakladať na kombinácii týchto zásad. Ak sa pri významnom nebezpečenstve musí na kontrolu súvisiaceho rizika uplatniť viac než jedna zásada akceptovania rizika, príslušné nebezpečenstvo je potrebné rozdeliť na čiastkové nebezpečenstvá tak, aby každé jednotlivé čiastkové nebezpečenstvo kontrolovala len jedna zásada akceptovania rizika.

[G 3] Rozhodnutie o kontrolovaní nebezpečenstva zásadou akceptovania rizika musí prihliadať na nebezpečenstvo a príčiny nebezpečenstva zistené už počas fázy identifikácie nebezpečenstiev. Ak sú teda s nebezpečenstvom spojené dve rôzne a nezávislé príčiny, je potrebné nebezpečenstvo rozdeliť na dve rôzne čiastkové nebezpečenstvá. Každé čiastkové nebezpečenstvo potom bude kontrolovať jedna zásada akceptovania rizika. Dve čiastkové nebezpečenstvá je potrebné zapísať a viesť v zázname o nebezpečenstve. Ak je napríklad nebezpečenstvo zapríčinené chybou návrhu, možno ho zvládnuť uplatnením kódexu postupov, ale ak je príčinou nebezpečenstva chyba údržby, iba kódex postupov nemusí byť dostatočný; potom je potrebné uplatniť inú zásadu akceptovania rizika.

[G 4] Zníženie rizika na prijateľnú úroveň si pravdepodobne vyžiada viacero iterácií (postupných krokov) medzi fázou analýzy rizík a fázou hodnotenia rizík, kým sa nezistia vhodné bezpečnostné opatrenia.

[G 5] Prítomné zostatkové riziko zistené zo skúseností v teréne na existujúcich systémoch a systémoch založených na uplatnení kódexov postupov sa uznáva za prijateľné. Riziko vyplývajúce z explicitného odhadu rizík je založené na posudku odborníka a rôznych predpokladoch, ktoré odborník počas analýz vzal do úvahy, alebo na údajoch databáz z oblasti nehôd alebo prevádzky. Zostatkové riziko podľa explicitného odhadu rizík preto nemožno potvrdiť priamo skúsenosťou v teréne. Takéto preukazovanie si vyžaduje čas na prevádzkovanie, sledovanie a nadobudnutie reprezentatívnych skúseností s príslušným systémom. Vo všeobecnosti uplatňovanie kódexov postupov a porovnania s podobnými referenčnými systémami má výhodu vyhnutia sa prehnanému špecifikovaniu zbytočne prísnych požiadaviek na bezpečnosť, ktoré môže mať pri explicitnom odhadovaní rizík za následok neprimerane opatrné (bezpečnostné) predpoklady. Môže sa však stať, že posudzovaný systém nebude musieť spĺňať niektoré požiadavky na bezpečnosť kódexov postupov alebo podobných referenčných systémov. V takom prípade by bolo uplatnenie explicitného odhadovania rizík výhodou, ktorá zabráni zbytočnému predimenzovaniu posudzovaného systému a umožní nákladovo priaznivejšiu konštrukciu, o ktorú by sa predtým nebolo možné pokúsiť.

[G 6] Ak zistené nebezpečenstvá a s nimi spojené riziká posudzovaného systému nemožno kontrolovať uplatnením kódexov postupov ani podobných referenčných systémov, vykoná sa explicitný odhad rizík na základe kvantitatívnych a kvalitatívnych analýz nebezpečných udalostí. Takáto situácia vznikne, keď je posudzovaný systém úplne nový (alebo je inovačný jeho návrh) alebo keď sa systém odchyľuje od kódexu postupov alebo referenčného systému. Explicitným odhadovaním rizík sa potom vyhodnotí, či je riziko prijateľné (t. j. ďalšia analýza nie je potrebná), alebo či sú potrebné ďalšie bezpečnostné opatrenia na ďalšie zníženie rizika.

[G 7] Usmernenie o znižovaní rizík a prijímaní rizík je možné nájsť aj v časti § 8 usmernenia EN 50 126-2 {Ref. 9}.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

[G 8] Je potrebné, aby orgán pre posudzovanie vyhodnotil použitú zásadu akceptovania rizika a jej uplatnenie.

2.1.5. Pri hodnotení rizík navrhovateľ preukáže, že zvolená zásada akceptovania rizika sa uplatňuje zodpovedajúcim spôsobom. Navrhovateľ tiež skontroluje, či sa zvolené zásady akceptovania rizík používajú dôsledne.

[G 1] Ak je napríklad pre softvér komponentu ako požiadavka na bezpečnosť uvedené uplatnenie vývojového procesu SIL 4 podľa normy EN 50 128, bude potrebné preukázať, že normou odporúčaný proces je splnený. Pritom bude napríklad potrebné preukázať, že:

a) sú splnené požiadavky na nezávislosť organizácie návrhu, overovania a validácie softvéru;
b) sa uplatnili správne metódy pre úroveň integrity bezpečnosti SIL 4 podľa normy EN 50 128;
c) atď.

[G 2] Ak sa napríklad pri výrobe elektromagnetických ventilov núdzových bŕzd musí použiť špecializovaný kódex postupov, bude potrebné preukázať, že všetky požiadavky kódexu postupov sú počas výrobného procesu splnené.

2.1.6. Uplatňovanie týchto zásad akceptovania rizík určí možné bezpečnostné opatrenia, vďaka ktorým riziko (riziká) posudzovaného systému sú prijateľné. Spomedzi týchto bezpečnostných opatrení sa tie opatrenia, ktoré boli zvolené na kontrolu rizika (rizík), stávajú požiadavkami na bezpečnosť, ktoré musí systém spĺňať. Dodržiavanie týchto požiadaviek na bezpečnosť sa preukazuje v súlade s oddielom 3.

[G 1] Je možné rozlíšiť dva druhy bezpečnostných opatrení:

a) „preventívne bezpečnostné opatrenia“ predchádzajúce vzniku nebezpečenstiev alebo ich príčin a
b) „zmierňujúce bezpečnostné opatrenia“, ktoré zabraňujú, aby sa nebezpečenstvo rozvinulo do nehody, alebo zmierňujú dôsledky nehôd, keď už nastali (ochranné opatrenia).

Z hľadiska zachovania prevádzkyschopnosti je vo všeobecnosti účinnejšie predchádzanie príčinám.

[G 2] Navrhovateľ bude považovať za najprimeranejšie bezpečnostné opatrenia, ktoré budú najlepším kompromisom medzi nákladmi na zníženie rizika a úrovňou zostatkového rizika. Zvolené bezpečnostné opatrenia sa pre posudzovaný systém stanú požiadavkami na bezpečnosť.

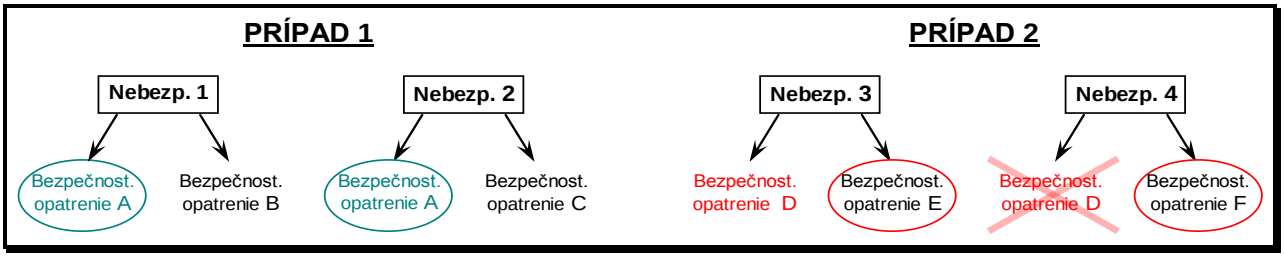
[G 3] Je dôležité overiť si, že bezpečnostné opatrenia vybrané na kontrolovanie jedného nebezpečenstva nie sú v konflikte s inými nebezpečenstvami. Ako je znázornené na Obr. 6, môžu napríklad nastať tieto dva prípady[13]:

---

(13) *Je potrebné poznamenať, že v príručke nie sú uvedené všetky situácie, v ktorých by mohli bezpečnostné opatrenia kolidovať so zistenými nebezpečenstvami. Uvedených je len niekoľko názorných príkladov.*

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

a) PRÍPAD 1: ak bezpečnostné opatrenie (opatrenie A na Obr. 6) môže bezkonfliktne kontrolovať rôzne nebezpečenstvá a ak je to ekonomicky odôvodnené, bolo by možné zvoliť len toto bezpečnostné opatrenie samo za súvisiacu „požiadavku na bezpečnosť“. Celkový počet požiadaviek na bezpečnosť, ktoré treba splniť, je menší ako súčasná implementácia obidvoch opatrení B a C;



Obr. 6: Výber vhodných bezpečnostných opatrení na obmedzenie rizík.

b) PRÍPAD 2: ak bezpečnostné opatrenie môže kontrolovať jedno nebezpečenstvo, ale je v konflikte s iným nebezpečenstvom (opatrenie D na Obr. 6), nemožno ho zvoliť za „požiadavku na bezpečnosť“. Na posudzované nebezpečenstvo sa musia použiť ďalšie bezpečnostné opatrenia (opatrenia E a F na Obr. 6):

(1) typickým príkladom v systéme riadenia a zabezpečenia vlakov je využitie lokalizácie vlaku na trati buď na ovládanie zapínania bŕzd, alebo na povolenie zrýchlenia jazdy vlaku. Použitie čela vlaku (resp. konca vlaku) na lokalizáciu vlaku nie je bezpečné vo všetkých situáciách:

(i) keď má systém riadenia a zabezpečenia vlakov ETCS bezpečne zapnúť záchranné brzdy, použije MAXIMUM SAFE FRONT END (najvzdialenejšie bezpečné čelo vlaku), aby bolo zaručené, že sa čelo vlaku skutočne zastaví pred nebezpečným miestom;

(ii) na druhej strane, keď vlak dostáva povolenie zrýchliť, napr. po obmedzení rýchlosti, systém riadenia a zabezpečenia vlakov ETCS použije MINIMUM SAFE REAR END (najbližší bezpečný koniec vlaku);

(2) iným príkladom je bezpečnostné opatrenie, ktoré by mohlo platiť pre zastavenie vlaku a uvedenie do bezpečného stavu pri poruche takmer za každých okolností okrem tunela alebo mosta. V tomto druhom prípade sa opatrenie D v PRÍPADE 2 na Obr. 6 nesmie uplatniť.

2.1.7. Iteračný proces posudzovania rizík možno považovať za skončený, keď sa preukáže, že všetky požiadavky na bezpečnosť sú splnené a žiadne ďalšie rozumne predvídateľné nebezpečenstvá sa nemusia posudzovať.

[G 1] V závislosti napr. od výberu technických možností pri návrhu systému, jeho subsystémov a zariadení by sa nové nebezpečenstvá mohli zistiť počas „preukazovania súladu s požiadavkami na bezpečnosť“ (napr. použitie určitého druhu náteru môže mať v prípade požiaru za následok únik jedovatých plynov). Tieto nové nebezpečenstvá so spojenými rizikami je potrebné považovať za nové vstupy nového cyklu iteračného procesu posudzovania rizík. V dodatku A.4.3 k norme EN 50 129 sú uvedené ďalšie príklady, keď možno zaviesť nové nebezpečenstvá, ktoré je potrebné kontrolovať.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

2.2. Identifikácia nebezpečenstiev

2.2.1. Navrhovateľ systematicky určuje pomocou rozsiahlej expertízy príslušného tímu všetky rozumne predvídateľné nebezpečenstvá pre celý posudzovaný systém, prípadne jeho funkcie a rozhrania.

Všetky identifikované nebezpečenstvá sa musia zaznamenať do záznamu o nebezpečenstve v súlade s oddielom 4.

[G 1] Nebezpečenstvá sa podľa možnosti vyjadrujú na rovnakej úrovni podrobnosti. Počas predbežnej analýzy nebezpečenstiev sa môže stať, že nebezpečenstvá boli zisťované na rôznych úrovniach podrobnosti (napr. pretože na HAZOP pracovali ľudia s rôznymi skúsenosťami).
Úroveň podrobnosti závisí aj od zásady akceptovania rizika, ktorá sa zvolí na kontrolovanie zistených nebezpečenstiev. Napríklad, ak nebezpečenstvo v plnom rozsahu kontroluje kódex postupov alebo podobný referenčný systém, podrobnejšia identifikácia nebezpečenstva nebude potrebná.

[G 2] Všetky nebezpečenstvá zistené v procese posudzovania rizík (vrátane nebezpečenstiev spojených so všeobecne prijateľnými rizikami), súvisiace bezpečnostné opatrenia a s nimi spojené riziká je potrebné zapísať do záznamu o nebezpečenstve.

[G 3] V závislosti od charakteru analyzovaného systému je možné na identifikáciu nebezpečenstva použiť rôzne metódy:

a) empirickú identifikáciu nebezpečenstva možno uplatniť s využitím minulých skúseností (napr. použitie kontrolných zoznamov alebo zoznamov generických nebezpečenstiev);
b) tvorivú identifikáciu nebezpečenstiev je možné použiť v nových oblastiach záujmu (aktívna prognóza, napr. štruktúrované štúdie „WHAT-IF“ (čo ak?), ako sú FMEA alebo HAZOP).

[G 4] Empirické a tvorivé metódy zisťovania nebezpečenstiev je možné vzájomne kombinovať, a tak zaistiť, aby bol zoznam potenciálnych nebezpečenstiev a uplatniteľných bezpečnostných opatrení úplný.

[G 5] V predbežnom kroku by sa identifikácia nebezpečenstiev mohla začínať brainstormingom, na ktorom by sa zúčastnili odborníci s rôznou kvalifikáciou, pokrývajúcou všetky príslušné aspekty významnej zmeny. Skupina odborníkov môže na analýzu konkrétnej funkcie alebo prevádzkových podmienok použiť empirické metódy.

[G 6] Metódy použité na identifikáciu nebezpečenstiev závisia od vymedzenia systému. Niekoľko príkladov je uvedených v dodatku B.

[G 7] Viac informácií o technikách a metódach identifikácie nebezpečenstiev je možné nájsť v prílohe A.2 a E k usmerneniu EN 50 126-2 {Ref. 9}.

[G 8] Príklad zoznamu generických nebezpečenstiev je uvedený v časti C.17. v dodatku C.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

2.2.2. S cieľom zamerať posudzovanie rizík na najvýznamnejšie riziká sa nebezpečenstvá klasifikujú podľa odhadovaného rizika, ktoré z nich vyplýva. Na základe odborného posúdenia sa nebezpečenstvá súvisiace so všeobecne prijateľným rizikom nemusia ďalej analyzovať, ale zaznamenajú sa do záznamu o nebezpečenstve. Ich klasifikácia musí byť odôvodnená, aby sa umožnilo nezávislé posúdenie orgánom pre posudzovanie.

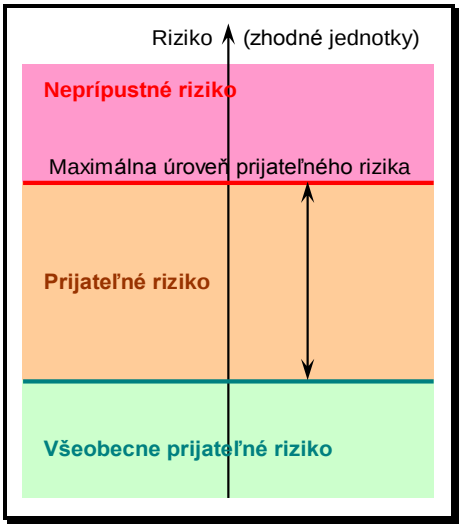
[G 1] V snahe napomôcť procesu posúdenia rizík je možné významné nebezpečenstvá ďalej združiť do rôznych kategórií. Významné nebezpečenstvá je napríklad možné zatriediť alebo zoradiť podľa očakávanej závažnosti rizík, ktoré s nimi súvisia alebo početnosti ich výskytu. Usmernenie pre takéto uplatňovanie je uvedené v normách CENELEC: pozri časť A.2 dodatku A.

[G 2] Analýza a hodnotenie rizík opísané v časti 2.1.4 sa uplatňujú podľa významnosti, začínajúc od nebezpečenstiev najvyššieho stupňa.

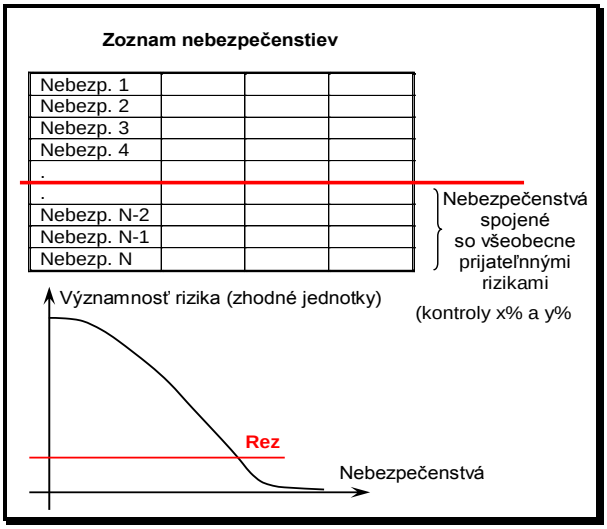
2.2.3. Kritériom je, že riziká vyplývajúce z nebezpečenstiev sa môžu klasifikovať ako všeobecne prijateľné, keď je riziko také malé, že nie je dôvod implementovať akékoľvek dodatočné bezpečnostné opatrenie. V odbornom posúdení sa zohľadňuje, že príspevok všetkých všeobecne prijateľných rizík neprekračuje vymedzený podiel celkového rizika.

[G 1] Napríklad riziko spojené s nebezpečenstvom je možné považovať za všeobecne prijateľné:

a) ak je riziko menšie ako dané percento (napr. x %) maximálneho prijateľného rizika pre tento druh nebezpečenstva. Hodnota x % by mohla vychádzať z najlepšej praxe a skúseností s viacerými metódami analýzy rizík, napr. z pomeru klasifikácií všeobecne prijateľného rizika a neprípustného rizika na krivkách FN alebo v maticiach rizík. Toto je možné znázorniť, ako ukazuje Obr. 7;
b) alebo ak je strata spojená s rizikom taká malá, že implementácia žiadneho ďalšieho bezpečnostného protiopatrenia nie je odôvodnená.



Obr. 7: Všeobecne prijateľné riziká.



Obr. 8: Odfiltrovanie nebezpečenstiev spojených so všeobecne prijateľným rizikom.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

[G 2] Okrem toho, ak sa zistia nebezpečenstvá na rôznych úrovniach podrobnosti (t. j. na jednej strane nebezpečenstvá vysokej úrovne a detailné podružné nebezpečenstvá na strane druhej), musia sa vykonať preventívne opatrenia, ktoré zabránia ich nesprávnej klasifikácii medzi nebezpečenstvá spojené so všeobecne prijateľným rizikom. Príspevok všetkých nebezpečenstiev spojených so všeobecne prijateľným rizikom nemôže prevýšiť daný podiel (napr. y %) na celkovom riziku na úrovni systému. Táto kontrola je potrebná, aby sa nevylúčila opodstatnenosť rozdelením nebezpečenstiev na množstvo podružných nebezpečenstiev nízkej úrovne. V skutočnosti, ak sa jedno nebezpečenstvo vyjadrí ako viacero rôznych „malých" podružných nebezpečenstiev a tieto sa vyhodnotia jednotlivo, každé je ľahko možné klasifikovať ako spojené so všeobecne prijateľným rizikom, ale ak sa vyhodnotia spolu (t. j. ako jedno nebezpečenstvo vysokej úrovne), riziko bude významné. Hodnota podielu (napr. y %) závisí od kritérií akceptovania rizík uplatniteľných na úrovni systému. Môže sa opierať o prevádzkovú skúsenosť s podobnými referenčnými systémami alebo určiť odhadom.

[G 3] Uvedené dve kontroly (t. j. x % a y %) umožňujú zamerať posúdenie rizík na najdôležitejšie nebezpečenstvá a zabezpečiť, aby bolo kontrolované každé významné riziko (pozri Obr. 8). Bez toho, aby boli dotknuté zákonné požiadavky v členskom štáte, navrhovateľ je povinný na základe odborného posudku vymedziť hodnoty x % a y % a nechať ich nezávisle posúdiť orgánu pre posudzovanie. Príkladom rádových veľkostí môže by x = 1 % a y = 10 %, ak sa to podľa odborného posudku považuje za prijateľné.

[G 4] V časti 2.2.2 je požiadavka, aby klasifikáciu medzi „všeobecne prijateľné riziká" nezávisle posúdil orgán pre posudzovanie.

2.2.4. Počas identifikovania nebezpečenstva možno určiť bezpečnostné opatrenia. Musia sa zaznamenať do záznamu o nebezpečenstve v súlade s oddielom 4.

[G 1] Hlavným účelom činnosti je zistenie nebezpečenstiev, ktoré sú spojené so zmenou. Ak už boli identifikované bezpečnostné opatrenia, je potrebné ich zapísať do záznamu o nebezpečenstve. Charakter opatrení závisí od zmeny; môžu byť procedurálne, technické, prevádzkové alebo organizačné.

2.2.5. Identifikáciu nebezpečenstva treba vykonávať len na takej podrobnej úrovni, aká je potrebná na identifikáciu toho, kde sa očakávajú bezpečnostné opatrenia na riadenie rizík v súlade s jednou zo zásad akceptovania rizika uvedených v bode 2.1.4. Iterácia medzi fázami analýzy rizík a hodnotenia rizík preto môže byť nevyhnutná, až kým sa nedosiahne dostatočná úroveň podrobnosti na identifikáciu nebezpečenstiev.

[G 1] Dokonca stále, aj ak je riziko obmedzené na prijateľnú úroveň, môže navrhovateľ rozhodnúť o potrebe podrobnejšieho zistenia nebezpečenstiev. Dôvodom môže byť pravdepodobnosť, že ak sa vykoná podrobnejšia identifikácia nebezpečenstiev, nájdu sa nákladovo efektívnejšie bezpečnostné opatrenia na kontrolu rizík.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

2.2.6. Ak sa na kontrolu rizík používa kódex postupov alebo referenčný systém, identifikácia rizík sa môže obmedziť na:

a) overenie relevantnosti kódexu postupov alebo referenčného systému.
b) identifikáciu odchýlok od kódexu postupov alebo od referenčného systému.

[G 2] Ďalšie vysvetlenie sa nepovažuje za potrebné.

2.3. Použitie kódexov postupov a hodnotenie rizík

2.3.1. S podporou ostatných zúčastnených aktérov a na základe požiadaviek uvedených v bode 2.3.2 navrhovateľ analyzuje, či sa na jedno alebo viaceré nebezpečenstvá náležite uplatňujú príslušné kódexy postupov.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

2.3.2. Kódexy postupov spĺňajú aspoň tieto požiadavky:

a) byť v železničnej oblasti všeobecne uznávané. Ak to tak nie je, kódexy postupov budú musieť byť odôvodnené a orgán pre posudzovanie ich musí považovať za prijateľné;
b) byť dôležité pre kontrolu zvažovaných nebezpečenstiev v posudzovanom systéme;
c) byť verejne prístupné pre všetkých aktérov, ktorí ich chcú používať.

[G 2] Ďalšie vysvetlenie sa nepovažuje za potrebné.

2.3.3. Ak sa v smernici 2008/57/ES vyžaduje súlad s TSI a v príslušnej TSI sa neukladá proces riadenia rizík stanovený v tomto nariadení, možno dané TSI považovať za kódexy postupov na kontrolu nebezpečenstva, ak je splnená požiadavka písmena c) v bode 2.3.2.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

2.3.4. Vnútroštátne predpisy oznámené v súlade s článkom 8 smernice 2004/49/ES a článkom 17 ods. 3 smernice 2008/57/ES možno považovať za kódexy postupov, ak sú splnené požiadavky v bode 2.3.2.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

2.3.5. Ak sa jedno alebo viaceré nebezpečenstvá kontrolujú kódexmi postupov, ktoré spĺňajú požiadavky bodu 2.3.2, riziká súvisiace s týmito nebezpečenstvami sa potom považujú za prijateľné. To znamená, že:

a) tieto riziká sa nemusia ďalej analyzovať;
b) používanie kódexov postupov sa zaznamená do záznamu o nebezpečenstve ako požiadavka na bezpečnosť pre príslušné nebezpečenstvá.

[G 2] Ďalšie vysvetlenie sa nepovažuje za potrebné.

2.3.6. V prípade, ak alternatívny prístup nie je v úplnom súlade s kódexom postupov, navrhovateľ preukáže, že prijatý alternatívny prístup vedie prinajmenšom k rovnakej úrovni bezpečnosti.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

2.3.7. Ak sa riziko v prípade konkrétneho nebezpečenstva nemôže stať prijateľným na základe uplatnenia kódexov postupov, určia sa dodatočné bezpečnostné opatrenia uplatnením jedného alebo dvoch iných zásad akceptovania rizík.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

2.3.8. Keď sa všetky nebezpečenstvá kontrolujú kódexmi postupov, proces riadenia rizík sa môže obmedzovať na:

a) identifikovanie nebezpečenstva v súlade s oddielom 2.2.6;
b) zaevidovanie použitia kódexov postupov v zázname o nebezpečenstve v súlade s oddielom 2.3.5;
c) zdokumentovanie uplatňovania procesu riadenia rizík v súlade s oddielom 5;
d) nezávislé posúdenie v súlade s článkom 6.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

2.4. Použitie referenčného systému a hodnotenie rizík

2.4.1. Navrhovateľ s podporou ostatných zúčastnených aktérov analyzuje, či sa na jedno alebo viacero nebezpečenstiev vzťahuje podobný systém, ktorý by sa mohol prijať ako referenčný systém.

[G 1] Viac informácií o týchto zásadách je možné nájsť v časti § 8 príručky EN 50 126-2 {Ref. 9}.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

2.4.2. Referenčný systém spĺňa aspoň tieto požiadavky:

a) pri jeho používaní sa už preukázalo, že má prijateľnú úroveň bezpečnosti a stále by bol spôsobilý na schválenie v členskom štáte, v ktorom sa zmena má zaviesť;
b) má podobné funkcie a rozhrania ako posudzovaný systém;
c) používa sa v podobných prevádzkových podmienkach ako posudzovaný systém;
d) používa sa v podobných environmentálnych podmienkach ako posudzovaný systém.

[G 1] Napríklad, starý systém riadenia a zabezpečenia vlakov, ktorý sa v praxi osvedčil svojou prijateľnou úrovňou bezpečnosti, by sa mohol nahradiť iným systémom na báze novšej technológie, s lepšou bezpečnostnou výkonnosťou. Preto má pri uplatňovaní referenčného systému vždy význam preveriť, či je ešte stále spôsobilý na schvaľovanie.

[G 2] Napríklad, vzhľadom na určité špecifické aspekty bezpečnosti tunelov alebo bezpečnosti prepravy nebezpečného tovaru, ktoré by mohli závisieť od prevádzkových a environmentálnych podmienok, je pri každom projekte potrebné preveriť, či sa systém bude používať za tých istých podmienok.

2.4.3. Ak referenčný systém spĺňa požiadavky uvedené v bode 2.4.2, potom v prípade posudzovaného systému:

a) riziká súvisiace s nebezpečenstvami, na ktoré sa vzťahuje referenčný systém, sa považujú za prijateľné;
b) požiadavky na bezpečnosť, na ktoré sa vzťahuje referenčný systém, možno odvodiť z analýz bezpečnosti alebo z hodnotenia záznamov o bezpečnosti referenčného systému;
c) tieto požiadavky na bezpečnosť sa zaznamenajú v záznamoch o nebezpečenstve ako požiadavky na bezpečnosť pre príslušné nebezpečenstvá.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

2.4.4. Ak sa posudzovaný systém odchyľuje od referenčného systému, v hodnotení rizík sa preukáže, že posudzovaný systém dosahuje aspoň rovnakú úroveň bezpečnosti ako referenčný systém. Riziká súvisiace s nebezpečenstvami, na ktoré sa vzťahuje referenčný systém, sa v takom prípade považujú za prijateľné.

[G 1] Viac informácií o analýzach podobnosti je možné nájsť v časti § 8.1.3. usmernenia EN 50 126–2 {Ref. 9}.

2.4.5. Ak nemožno preukázať rovnakú úroveň bezpečnosti, ako má referenčný systém, určia sa dodatočné bezpečnostné opatrenia pre odchýlky uplatnením jednej alebo dvoch iných zásad akceptovania rizika.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

2.5. Explicitný odhad a hodnotenie rizík

2.5.1. Ak sa na nebezpečenstvá nevzťahuje jedna ani dve zásady akceptovania rizika opísané v oddieloch 2.3 a 2.4, preukázanie prijateľnosti rizika sa vykoná jednoznačným odhadom rizika a hodnotením. Riziká vyplývajúce z týchto nebezpečenstiev sa odhadujú buď kvantitatívne, alebo kvalitatívne, so zohľadnením existujúcich bezpečnostných opatrení.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

2.5.2. Prijateľnosť odhadovaných rizík sa hodnotí pomocou kritérií akceptovania rizika, buď odvodených z právnych požiadaviek uvedených v právnych predpisoch Spoločenstva, alebo v oznámených vnútroštátnych predpisoch, alebo založených na týchto požiadavkách. V závislosti od kritérií akceptovania rizika sa prijateľnosť rizika môže hodnotiť individuálne pre každé súvisiace nebezpečenstvo alebo globálne pre kombináciu všetkých nebezpečenstiev zvažovaných v jednoznačnom odhade rizika.

Ak odhadované riziko nie je prijateľné, určia sa a implementujú sa dodatočné bezpečnostné opatrenia s cieľom znížiť riziko na prijateľnú úroveň.

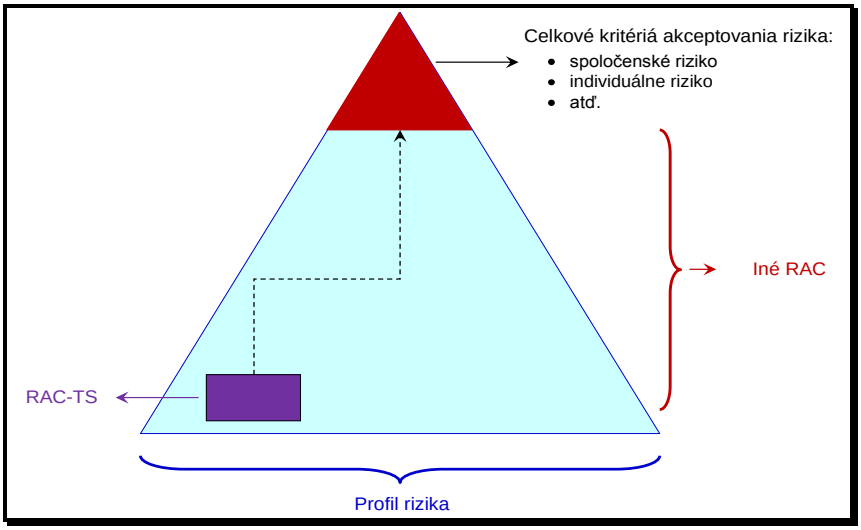
[G 1] Na hodnotenie prijateľnosti rizík posudzovaného systému sú potrebné kritériá akceptovania rizík (pozri bloky „hodnotenia rizík“ na Obr. 1). Kritériá akceptovania rizík môžu byť buď implicitné, alebo explicitné:

a) implicitné kritériá akceptovania rizík: riziká, na ktoré sa podľa častí 2.3.5 a 2.4.3 vzťahuje uplatnenie kódexov postupov a porovnanie s referenčnými systémami, sa implicitne považujú za prijateľné, ak (pozri bodkovanú kružnicu na Obr. 1) sú splnené:

   (1) buď podmienky uplatňovania kódexov postupov uvedené v časti 2.3.2,
   (2) alebo podmienky uplatňovania referenčného systému uvedené v časti 2.4.2;

b) explicitné kritériá akceptovania rizík: na hodnotenie prijateľnosti uplatňovania explicitného odhadovania rizík na kontrolu rizík sú potrebné explicitné kritériá akceptovania rizík (pozri neprerušovanú kružnicu pri tretej zásade na Obr. 1). Možno ich vymedziť na rôznych úrovniach železničného systému: možno ich chápať ako „pyramídu kritérií“ (pozri Obr. 9), začínajúcu od kritérií akceptovania rizika vysokej úrovne (vyjadrených napr. ako spoločenské alebo individuálne riziko), pokračujúcu k subsystémom a prvkom (týkajúcim sa technických systémov) a zahŕňajúcu ľudských prevádzkovateľov počas činností prevádzky a údržby systému a subsystémov. Napriek tomu, že kritériá akceptovania rizika prispievajú k dosiahnutiu bezpečnostnej výkonnosti systému, a teda sú prepojené s CST a NRV, je veľmi ťažké navrhnúť matematický model vzťahov medzi nimi: ďalšie podrobnosti o tom pozri v {Ref. 12}.
   Úroveň, na ktorej sú vymedzené explicitné kritériá akceptovania rizika, musí byť v súlade s dôležitosťou a zložitosťou významnej zmeny. Napríklad nie je potrebné hodnotiť riziko celého železničného systému, keď sa upravuje druh nápravy vozidiel. Vymedzenie kritérií akceptovania rizík by sa malo zamerať na bezpečnosť vozidiel. Na druhej strane by sa veľké zmeny alebo rozšírenia existujúceho železničného systému nemali hodnotiť len vzhľadom na bezpečnostnú výkonnosť jednotlivých funkcií alebo zmien, ktoré sa dopĺňajú. Na úrovni železničného systému by sa tiež malo overiť, či je zmena prijateľná ako celok.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu



Obr. 9: Pyramída kritérií akceptovania rizika (RAC).

[G 2] Explicitné kritériá akceptovania rizika, ktoré sú potrebné na podporu vzájomného uznávania medzi členskými štátmi, sa budú harmonizovať na základe prebiehajúcich prác agentúry, súvisiacich s kritériami akceptovania rizika. Ďalšie informácie budú do tohto dokumentu doplnené, keď budú k dispozícii.

[G 3] Medzičasom je možné hodnotiť riziká s využitím napr. matice rizík, ktorú možno nájsť v časti § 4.6 v norme EN 50 126-1 {Ref. 8}. Je možné použiť aj iné druhy vhodných kritérií za predpokladu, že tieto kritériá sa v posudzovanom prípade považujú za dostatočné na určenie prijateľnej úrovne bezpečnosti.

2.5.3. Ak sa riziko súvisiace s jedným nebezpečenstvom alebo kombináciou viacerých nebezpečenstiev považuje za prijateľné, určené bezpečnostné opatrenia sa zaznamenajú do záznamov o nebezpečenstve.

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

2.5.4. Ak nebezpečenstvá vyplynú zo zlyhaní technických systémov, na ktoré sa nevzťahujú kódexy postupov ani používanie referenčného systému, v prípade návrhu technického systému sa uplatňuje toto kritérium akceptovania rizika:

V prípade technických systémov, pri ktorých má funkčné zlyhanie vierohodný priamy potenciál katastrofického dôsledku, sa súvisiace riziko nemusí ďalej zmenšovať, ak je miera tohto zlyhania menšia alebo sa rovná 10-9 za prevádzkovú hodinu.

[G 1] Ďalšie podrobnosti o RAC-TS, ako aj na ktoré aspekty a funkcie technického systému sa kritérium vzťahuje, sú v samostatnej poznámke agentúry pripojenej k tomuto dokumentu: pozri časť A.3. v dodatku A a referenčný dokument {Ref. 11}.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

2.5.5.	*Bez toho, aby bol dotknutý postup uvedený v článku 8 smernice 2004/49/ES, sa môže prostredníctvom vnútroštátneho predpisu vyžadovať náročnejšie kritérium s cieľom zachovať vnútroštátnu úroveň bezpečnosti. V prípade dodatočných povolení na uvedenie vozidiel do prevádzky sa však uplatňujú postupy článkov 23 a 25 smernice 2008/57/ES.*

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

2.5.6.	*Ak je technický systém vyvinutý uplatnením kritéria 10^{-9} vymedzeného v bode 2.5.4, uplatňuje sa zásada vzájomného uznávania v súlade s článkom 7 ods. 4 tohto nariadenia.* *Ak však navrhovateľ môže preukázať, že vnútroštátna úroveň bezpečnosti v členskom štáte uplatňovania sa môže zachovať s mierou zlyhania vyššou než 10^{-9} na prevádzkovú hodinu, navrhovateľ môže v danom členskom štáte toto kritérium použiť.*

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

2.5.7.	*Jednoznačný odhad rizika a hodnotenie spĺňa aspoň tieto požiadavky:* *a) metódy použité na jednoznačný odhad rizika správne odrážajú posudzovaný systém a jeho parametre (vrátane všetkých prevádzkových režimov);* *b) výsledky by mali byť dostatočne presné, aby slúžili ako pevná podpora pri rozhodovaní, t. j. menšie zmeny vo vstupných predpokladoch alebo podmienkach nemajú za následok značne odlišné požiadavky.*

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

3. PREUKAZOVANIE SPLNENIA POŽIADAVIEK NA BEZPEČNOSŤ

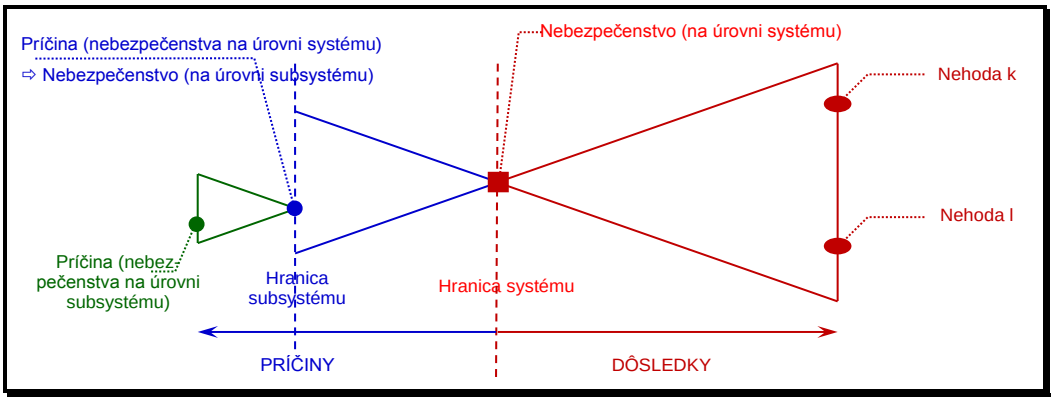
3.1. Pred akceptovaním bezpečnosti danej zmeny sa pod dohľadom navrhovateľa musí preukázať splnenie požiadaviek na bezpečnosť vyplývajúcich z fázy posudzovania rizík.

[G 1] „Preukazovanie súladu systému s požiadavkami na bezpečnosť“ vysvetlené v odsekoch [G 3] až [G 6] v časti 2.1.1 zahŕňa fázy „6 až 10“ V-cyklu CENELEC (pozri BOX 3 na Obr. 5). Pozri odsek [G 3] v časti 2.1.1.

[G 2] Pozri aj odsek [G 4] v časti 2.1.1 tohto dokumentu.

3.2. Toto preukázanie uskutoční každý aktér zodpovedný za splnenie požiadaviek na bezpečnosť, ako sa rozhodlo v súlade s bodom 1.1.5.

[G 1] Príkladom bezpečnostného posudzovania a bezpečnostných analýz, ktoré je možné vykonať na úrovni subsystému, sú analýzy príčin: pozri Obr. 10. Ale na preukázanie súladu subsystému so vstupnými požiadavkami na bezpečnosť je možné použiť akúkoľvek inú metódu.

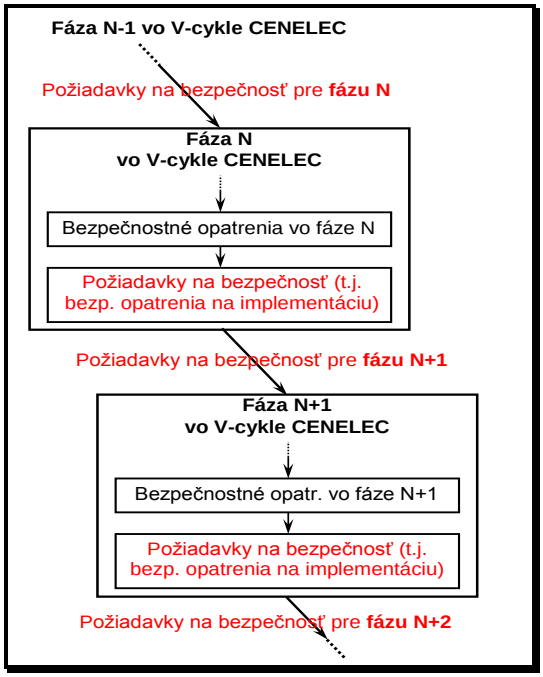


Obr. 10: Obr. A.4 z normy EN 50 129:
Vymedzenie nebezpečenstiev vzhľadom na hranice systému.

[G 2] Hierarchické štruktúrovanie nebezpečenstiev a príčin so zreteľom na systémy a subsystémy je možné zopakovať v každej fáze nižšej úrovne V-cyklu CENELEC na Obr. 5. Činnosti zisťovania nebezpečenstiev a analýzy príčin (alebo iná relevantná metóda), ako aj použitie kódexov postupov, podobných referenčných systémov a explicitných analýz a hodnotení je takisto možné opakovať v každej fáze vývojového cyklu systému s cieľom odvodiť z bezpečnostných opatrení zistených na úrovni subsystému požiadavky na bezpečnosť, ktoré musia byť splnené v najbližšej ďalšej fáze. Toto je znázornené na Obr. 11.

[G 3] Pozri aj odsek [G 4] v časti 2.1.1 tohto dokumentu.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu



Obr. 11: Odvodenie požiadaviek na bezpečnosť pre fázy nižšej úrovne.

3.3.	*Prístup zvolený na preukázanie zhody s požiadavkami na bezpečnosť, ako aj samotné preukázanie nezávisle posúdi orgán pre posudzovanie.*

[G 1] Všetky činnosti uvedené v BOXE 3[(14)] V-cyklu CENELEC na Obr. 5 sa preto tiež posudzujú nezávisle.

[G 2] Druhom a úrovňou podrobnosti nezávislého posúdenia, ktoré vykonávajú orgány pre posudzovanie (t. j. podrobné alebo makroskopické posudzovanie), sa zaoberajú vysvetlivky k Článok 6.

3.4.	*Každá neprimeranosť bezpečnostných opatrení, od ktorých sa očakáva, že splnia požiadavky na bezpečnosť, alebo akékoľvek iné nebezpečenstvo objavené počas preukazovania zhody s požiadavkami na bezpečnosť majú za následok opätovné posúdenie a hodnotenie súvisiacich rizík navrhovateľom v súlade s oddielom 2. Nové nebezpečenstvá sa musia zaznamenať do záznamu o nebezpečenstve v súlade s oddielom 4.*

[G 1] Napríklad spôsob hasenia požiaru by mohol mať za následok nové nebezpečenstvo (zadusenie sa), ktoré bude znamenať nové požiadavky na bezpečnosť (napr. špecifický postup pri evakuácii cestujúcich). Iným príkladom je použitie kaleného skla, aby sa zabránilo rozbitiu okien pri havárii a ohrozeniu cestujúcich črepinami alebo dokonca ich vyhodeniu

(14) *Vzťah medzi činnosťami podľa nariadenia o CSM a činnosťami na Obr. 5 (t. j. V-cyklu CENELEC na obrázku 10 v norme 50 126) je opísaný v časti 2.1.1. Ktoré činnosti podľa normy CENELEC sú súčasťou fázy „preukazovania zhody systému s požiadavkami na bezpečnosť“ podľa nariadenia o CSM vymenúva najmä odsek [G 3] časti 2.1.1.*

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

z vlaku. Novým nebezpečenstvom potom je oveľa ťažšia evakuácia cestujúcich z vagónov, čo môže vyústiť do požiadaviek na bezpečnosť na špeciálny dizajn okien, ktoré umožnia evakuáciu.

[G 2] Príklad prevádzkovej zmeny: vyžaduje sa, aby všetka preprava nebezpečného tovaru bola na trati prechádzajúcej husto osídlenými územiami zakázaná. Namiesto toho by sa preto mala uskutočniť na alternatívnej trase s tunelmi, na ktorej tak vzniknú nebezpečenstvá iného druhu.

[G 3] Iné príklady nových nebezpečenstiev, ktoré by bolo možné zistiť počas preukazovania súladu systému s požiadavkami na bezpečnosť je možné nájsť v dodatku A.4.3 k norme EN 50 129.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

4. RIADENIE NEBEZPEČENSTIEV

4.1. Proces riadenia nebezpečenstiev

4.1.1. Záznam (záznamy) o nebezpečenstve vytvára alebo aktualizuje (ak už existujú) navrhovateľ počas návrhu a implementácie a až do schválenia zmeny alebo do vydania správy o posúdení bezpečnosti. Záznam o nebezpečenstve sleduje pokrok pri monitorovaní rizík súvisiacich s identifikovanými nebezpečenstvami. V súlade s bodom 2 písm. g) prílohy III k smernici 2004/49/ES, keď sa systém schváli a prevádzkuje sa, záznam o nebezpečenstve ďalej udržiava manažér infraštruktúry alebo železničný podnik poverený prevádzkovaním posudzovaného systému ako neoddeliteľnú časť svojho systému riadenia bezpečnosti.

[G 1] CENELEC v normách 50 126-1 {Ref. 8} a 50 129 {Ref. 7} tiež odporúča používanie záznamu o nebezpečenstve na zapisovanie, sledovanie a kontrolovanie relevantných bezpečnostných informácií.

[G 2] Aktér by napríklad mohol mať aj viac záznamov o nebezpečenstve v závislosti od zložitosti systému. Každý záznam o nebezpečenstve podlieha nezávislému posúdeniu orgánu pre posudzovanie. Možným riešením by napríklad mohla byť:

a) „interný záznam o nebezpečenstve“ na riadenie všetkých vnútorných požiadaviek na bezpečnosť uplatniteľných na subsystém, za ktorý aktér zodpovedá. Jeho veľkosť a rozsah riadiacej práce závisia od jej štruktúry a, samozrejme, od zložitosti subsystému. Keďže sa však používa na účely vnútorného riadenia, tento záznam o nebezpečenstve sa nemusí oznamovať ostatným aktérom. Interný záznam o nebezpečenstve obsahuje všetky zistené nebezpečenstvá, ktoré sú pod kontrolou, ako aj súvisiace bezpečnostné opatrenia, ktoré sú overené;
b) „externý záznam o nebezpečenstve“ na prenos nebezpečenstiev a súvisiacich bezpečnostných opatrení (ktoré tento aktér nemôže implementovať sám v celom rozsahu) na ďalších aktérov v súlade s časťou 1.2.2. Tento druhý záznam o nebezpečenstve je zvyčajne menší a vyžaduje si menej riadiacej práce (pozri príklad v časti C.16.4. dodatku C).

[G 3] Ak sa zdá vedenie viacerých záznamov o nebezpečenstve zložité, je iným možným riešením riadenie všetkých nebezpečenstiev a súvisiacich bezpečnostných rizík uvedených v písmenách a) a b) prostredníctvom jediného záznamu o nebezpečenstve, ale s možnosťou dvoch správ o záznamoch o nebezpečenstve (pozri príklad v časti C.16.3. dodatku C), a to:
a) internej správy o záznamoch o nebezpečenstve, ktorá by dokonca nemusela byť nevyhnutná, ak by bol záznam o nebezpečenstve štruktúrovaný tak, aby umožňoval nezávislé posúdenie;
b) externej správy o záznamoch o nebezpečenstve na prenos nebezpečenstiev a súvisiacich bezpečnostných opatrení na ďalších aktérov.

[G 4] Keď je systém na záver projektu schválený, ako je vysvetlené v časti 4.2:

a) všetky nebezpečenstvá, ktoré boli prevedené na ďalších aktérov, sa kontrolujú v externom zázname o nebezpečenstve aktéra, ktorý ich previedol. Keďže sú importované a riadené v interných záznamoch o nebezpečenstve ďalších aktérov, nemusí ich už počas životného cyklu (sub-)systému riadiť posudzovaný aktér;
b) všetky súvisiace bezpečnostné opatrenia by však nemali byť overené v zázname o nebezpečenstve z dôvodov, ktoré sú vysvetlené v odseku [G 9] v časti 4.2. Je skutočne užitočné, aby organizácia, ktorá obmedzenia používania exportuje, v zázname o

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

nebezpečenstve zrozumiteľne zdôraznila, že súvisiace bezpečnostné opatrenia neboli overené.

[G 5] Na druhej strane, všetky interné záznamy o nebezpečenstve sa vedú počas celého životného cyklu (sub-)systému. To umožní sledovať priebeh monitorovania rizík spojených so zistenými nebezpečenstvami počas prevádzky a údržby (sub-)systému, t. j. hneď po jeho uvedení do prevádzky: pozri BOX 4 V-cyklu CENELEC na Obr. 5.

4.1.2. Záznam o nebezpečenstve obsahuje všetky nebezpečenstvá spolu so všetkými súvisiacimi bezpečnostnými opatreniami a predpokladmi týkajúcimi sa systému, identifikovanými počas procesu posudzovania rizík. Obsahuje najmä jasný odkaz na pôvod a na vybrané zásady akceptovania rizika a jasne identifikuje aktéra (aktérov) povereného (poverených) kontrolou každého nebezpečenstva.

[G 1] V informáciách o nebezpečenstvách a s nimi spojených bezpečnostných opatreniach, prijatých od iných aktérov (pozri časť 1.2.2) sú aj predpoklady(15) a obmedzenia používania(15) (nazývané aj podmienky používania súvisiace s bezpečnosťou) poprípade uplatniteľné na bezpečnostné preukazy rôznych subsystémov, všeobecného a spoločného použitia a všeobecných a spoločných výrobkov, ktoré vypracovali výrobcovia.

[G 2] Možný príklad štruktúry záznamu o nebezpečenstve je opísaný v časti C.16. dodatku C.

4.2. Výmena informácií

Všetky nebezpečenstvá a súvisiace požiadavky na bezpečnosť, ktoré nemôže kontrolovať jeden aktér sám, sa oznamujú inému relevantnému aktérovi s cieľom spoločne nájsť primerané riešenie. Nebezpečenstvá zaznamenané v zázname o nebezpečenstve aktéra, ktorý ich presúva, sa „kontrolujú“ len vtedy, keď hodnotenie rizík súvisiacich s týmito nebezpečenstvami vykonáva iný aktér a na riešení sa dohodnú všetci zúčastnení.

[G 1] Napríklad výrobca môže odskúšať a overiť algoritmus odometrického subsystému (počítadla odjazdených kilometrov) palubného zriadenia ETCS v laboratóriu simuláciou teoretických signálov, ktoré by mohli vysielať príslušné odometrické snímacie zariadenia. Úplné overenie odometrického subsystému si však vyžaduje pomoc ŽP a MI na vykonanie overenia s použitím skutočného vlaku a skutočného kolesa vlaku v kontakte s koľajnicou.

[G 2] Ďalšími príkladmi by mohli byť prevody bezpečnostných opatrení prevádzky a údržby technických zariadení z výrobcu na železničné podniky. Bude potrebné, aby tieto bezpečnostné opatrenia implementoval železničný podnik.

[G 3] Aby mohli zúčastnené organizácie spoločne znovu posúdiť tieto nebezpečenstvá, s nimi spojené bezpečnostné opatrenia a riziká, bude užitočné, keď im organizácia, ktorá ich zistila, poskytne všetky vysvetlenia potrebné na správne pochopenie problému. Možno by bolo potrebné zmeniť pôvodné znenie nebezpečenstiev, bezpečnostných opatrení a rizík, aby

(15) *Ďalšie vysvetlenie pojmov bezpečnostné preukazy „všeobecných a podobných výrobkov a všeobecného a podobného použitia“ a „predpoklady a obmedzenia používania" je uvedené v odseku [G 5] v časti 1.1.5 a v poznámkach pod čiarou (9) a (10) na strane 27 tohto dokumentu.*

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

bolo zrozumiteľné bez opätovných spoločných diskusií o ňom. Spoločné posúdenie nebezpečenstiev by mohlo viesť k zisteniu nových bezpečnostných opatrení.

[G 4] Prijímajúci aktér zodpovedný za implementáciu, overovanie a potvrdenie prijatých alebo nových bezpečnostných opatrení zapíše do svojho vlastného záznamu o nebezpečenstve všetky príslušné nebezpečenstvá spojené s bezpečnostnými opatreniami (importovanými aj spoločne zistenými).

[G 5] Keď sa bezpečnostné opatrenie nepodarilo potvrdiť v plnom rozsahu, je potrebné vypracovať jasné obmedzenie používania (napr. zmierňujúce prevádzkové opatrenia) a zapísať ho do záznamu o nebezpečenstve. V skutočnosti je možné, že technické/návrhové bezpečnostné opatrenia:

a) nie sú správne implementované;
b) nie sú úplne implementované;
c) úmyselne nie sú implementované napríklad preto, že rôzne bezpečnostné opatrenia sú implementované namiesto opatrení zapísaných v zázname o nebezpečenstve (napr. z dôvodu nákladov). Pretože nie sú potvrdené, je potrebné tieto bezpečnostné opatrenia zrozumiteľne identifikovať v zázname o nebezpečenstve. Potrebné je dokázať/odôvodniť, prečo sú vhodné bezpečnostné opatrenia, ktoré boli implementované namiesto nich[16], ako aj preukázať, že systém s náhradnými bezpečnostnými opatreniami spĺňa požiadavky na bezpečnosť;
d) atď.

V týchto prípadoch počas riadenia nebezpečenstiev nemožno príslušné technické/návrhové bezpečnostné opatrenia overiť a potvrdiť. Príslušné nebezpečenstvá a bezpečnostné opatrenia je potom potrebné ponechať v zázname o nebezpečenstve otvorené, aby sa zabránilo nesprávnemu použitiu bezpečnostných opatrení pri iných systémoch uplatnením „podobného referenčného systému“ ako zásady akceptovania rizika.

[G 6] „Nesprávne“ alebo „neúplne“ implementované bezpečnostné opatrenia sa zvyčajne zistia už na začiatku životného cyklu systému a opravia sa pred schválením systému. Ak sa však technické bezpečnostné opatrenie zistí prineskoro na správnu a úplnú implementáciu, organizácia zodpovedná za implementáciu a riadenie musí identifikovať a do záznamu o nebezpečenstve zapísať jasné obmedzenie používania posudzovaného systému. Tieto obmedzenia používania bývajú často prevádzkovými obmedzeniami aplikácie posudzovaného systému.

[G 7] Mohlo by tiež byť užitočné zapisovať do záznamov o nebezpečenstve, či sa budú súvisiace bezpečnostné opatrenia správne implementovať v neskoršej etape životného cyklu, alebo či sa systém bude ďalej používať so zistenými obmedzeniami používania. Do záznamov o nebezpečenstve by mohlo byť užitočné zapisovať aj odôvodnenie, prečo neboli príslušné technické bezpečnostné opatrenia implementované správne/úplne.

[G 8] Aktér, ktorý prijme obmedzenia používania:

a) všetky si importuje do svojho záznamu o nebezpečenstve;
b) zabezpečí, aby podmienky používania posudzovaného systému spĺňali všetky prijaté obmedzenia používania;
c) overí a potvrdí, že posudzovaný systém spĺňa tieto obmedzenia používania.

(16) *Ak boli odlišné bezpečnostné opatrenia implementované namiesto pôvodne špecifikovaných, aj tie je potrebné zapísať do záznamu o nebezpečenstve.*

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

[G 9] V závislosti od rozhodnutí dohodnutých zúčastnenými organizáciami:

a) buď sa príslušné technické bezpečnostné opatrenia správne implementujú v neskoršej etape navrhovania;
Organizácia, ktorá exportuje obmedzenia používania, ďalej sleduje správnu technickú implementáciu príslušných bezpečnostných opatrení. V dôsledku toho nie je možné príslušné bezpečnostné opatrenia potvrdiť a s nimi súvisiace nebezpečenstvá nie je možné kontrolovať v záznamoch o nebezpečenstve tejto organizácie, až kým nie sú zodpovedajúce technické bezpečnostné opatrenia implementované v plnom rozsahu. Toto je potrebné zaistiť, dokonca aj keď sa medzitým exportované obmedzenia používania zaviedli do praxe.

b) alebo sa príslušné technické bezpečnostné opatrenia nebudú správne implementovať v neskoršej fáze navrhovania. Systém sa tak bude ďalej používať počas celého svojho životného cyklu so spojenými obmedzeniami používania. V tomto prípade je možné urobiť toto:

(1) organizácia, ktorá obmedzenia používania exportuje, nezapíše do svojho záznamu o nebezpečenstve súvisiace bezpečnostné opatrenia ako „potvrdené“. Takýmto spôsobom sa neprehliadnu súvisiace bezpečnostné obavy, keď sa príslušný systém použije ako referenčný systém v iných projektoch. Tak potom, aj keď iný aktér pripustí odlišné riadenie súvisiacich rizík, je užitočné, ak organizácia, ktorá obmedzenia používania exportuje, vo svojom zázname o nebezpečenstve zrozumiteľne zdôraznila, že súvisiace bezpečnostné opatrenia neboli potvrdené, alebo

(2) je možné opis systému zmeniť tak, aby obsahoval obmedzenia používania v rozsahu uplatnenia systému (t. j. predpokladoch pre systém) a v požiadavkách na bezpečnosť. Umožní to kontrolu nebezpečenstiev. Tak teda, ak sa použije systém ako referenčný systém v inej aplikácii:

(i) nový systém bude musieť byť použitý za rovnakých podmienok (t. j. bude musieť spĺňať obmedzenia použitia spojené s týmito predpokladmi), alebo
(ii) navrhovateľ bude musieť znovu posúdiť odchýlky od uvedených predpokladov.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

5. DÔKAZY O UPLATŇOVANÍ PROCESU RIADENIA RIZÍK

5.1. Navrhovateľ dokumentuje proces riadenia rizík používaný na posúdenie úrovní bezpečnosti a zhody s požiadavkami na bezpečnosť takým spôsobom, aby orgán pre posudzovanie mal k dispozícii všetky potrebné dôkazy preukazujúce správne uplatňovanie procesu riadenia rizík. Orgán pre posudzovanie vypracuje svoje závery v správe o posúdení bezpečnosti.

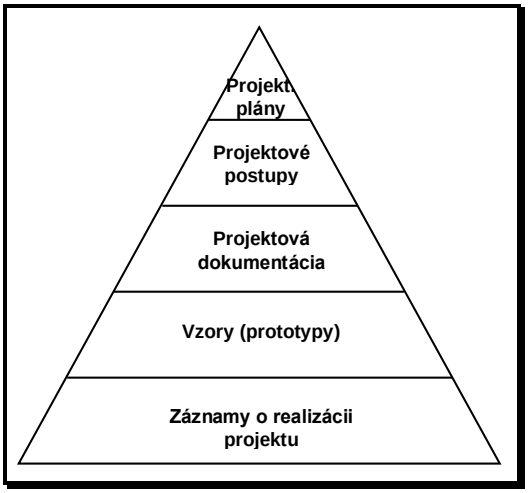
[G 1] Tieto požiadavky už rieši systém riadenia bezpečnosti železničného podniku a manažéra infraštruktúry (SMS). Ostatní aktéri železničného sektora, ktorí sa zúčastňujú na významnej zmene majú prinajmenšom na úrovni projektu proces riadenia kvality (QMP) a/alebo proces riadenia bezpečnosti (SMP), ktoré sa vzťahujú na túto požiadavku, a to aj vtedy, keď SMS nie je povinný. Oba tieto procesy rátajú so štruktúrovanou hierarchiou dokumentácie buď v rámci podniku, alebo aspoň v rámci projektu. Riešia aj dokumentačné potreby riadenia RAMS. Takáto štruktúrovaná dokumentácia môže v podstate pozostávať z týchto častí (pozri Obr. 12):

a) **Projektové plány** vypracované tak, aby opisovali organizáciu, ktorú treba uviesť do prevádzky na riadenie činnosti v rámci projektu.

b) **Projektové postupy**, vypracované tak, aby podrobne opisovali spôsob splnenia špecializovanej úlohy. Postupy a príkazy existujú obvykle v rámci podniku a tak sa používajú. Nové projektové postupy sa vypracujú, len ak je potreba opísať konkrétnu úlohu v rámci konkrétneho projektu.

c) **Dokumentácia vývoja projektu** vypracovaná počas životného cyklu je na Obr. 5.

d) **Podnikové alebo aspoň projektové šablóny** existujú pre rôzne druhy dokumentov, ktoré sa vypracúvajú



Obr. 12: Hierarchia štruktúrovanej dokumentácie.

e) **Projektové záznamy** vypracované počas projektu a potrebné na preukázanie súladu s procesmi riadenia kvality a riadenia bezpečnosti podniku.

Toto je jeden spôsob uspokojenia potrieb dokumentárnych dôkazov. Môžu existovať aj iné spôsoby, pokiaľ spĺňajú kritériá CSM.

[G 2] Normy CENELEC odporúčajú preukázať, že systém spĺňa funkčné požiadavky a požiadavky na bezpečnosť v bezpečnostnom preukaze (*Safety Case*) (alebo v bezpečnostnej správe). Dokonca, aj vtedy, keď nie je povinné, použitie bezpečnostného preukazu poskytuje v štruktúrovanej forme dokument odôvodňujúci:

a) dôkaz o riadení kvality;
b) dôkaz o riadení bezpečnosti;
c) dôkaz o funkčnej a technickej bezpečnosti.

Súčasne má výhodu podpory a príručky pre orgány pre posudzovanie pri nezávislom posudzovaní správnosti uplatňovania CSM.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

[G 3] Bezpečnostný preukaz opisuje, v akých vzájomných vzťahoch sú projektové dokumenty o aplikácii procesov riadenia kvality a/alebo bezpečnosti podniku v procese vývoja systému, s cieľom preukázať bezpečnosť systému. Bezpečnostný preukaz zvyčajne neobsahuje rozsiahle zväzky podrobných dôkazov a doplňujúcej dokumentácie, ale sú v ňom uvedené presné odkazy na tieto dokumenty.

[G 4] **Bezpečnostný preukaz technických systémov:** Normy CENELEC je možné použiť ako usmernenia na písanie a/alebo zostavenie štruktúry bezpečnostných preukazov:

a) pozri normu EN 50 129 {Ref. 7} „Dráhové aplikácie. Komunikačné a signalizačné systémy a systémy na spracovanie údajov. Elektronické signalizačné systémy súvisiace s bezpečnosťou“; aj v dodatku H.2 k usmerneniu EN 50 126–2 {Ref. 9} je návrh štruktúry bezpečnostného preukazu signalizačných systémov;
b) štruktúru bezpečnostného preukazu vozidiel pozri v dodatku H.1 k usmerneniu EN 50 126-2 {Ref. 9};
c) štruktúru bezpečnostného preukazu infraštruktúry pozri v dodatku H.3 k usmerneniu EN 50 126-2 {Ref. 9};

Ako je zjavné z uvedených odkazov, štruktúra aj obsah bezpečnostného preukazu závisia od systému, ktorého bezpečnosť sa nimi má preukazovať.

Osnova bezpečnostného preukazu, ktorá je uvedená v prílohe H k usmerneniu EN 50 126-2 {Ref. 9}, je len príkladom a nemusí byť vhodná pre všetky systémy daného druhu. Preto je potrebné osnovu primerane posúdiť a použiť z nej len to, čo je vhodné pre každú špecifickú aplikáciu.

[G 5] **Bezpečnostný preukaz organizačných a prevádzkových aspektov železničných systémov:**

V súčasnosti neexistuje žiadna špecializovaná norma, ktorá by stanovila štruktúru alebo obsah ani usmernenie na písanie bezpečnostného preukazu organizačných a prevádzkových stránok železničného systému. Keďže účelom bezpečnostného preukazu je štruktúrovanou formou preukázať súlad systému s požiadavkami na bezpečnosť, možno použiť rovnakú formu štruktúry bezpečnostného preukazu ako pri technických systémoch. V odkazoch odseku [G 4] v časti 5.1 sú uvedené odporúčania a kontrolný zoznam bodov, kam sa obrátiť, bez ohľadu na druh posudzovaného systému. Riadenie organizačných a prevádzkových zmien si vyžaduje rovnaký spôsob riadenia kvality a procesy riadenia bezpečnosti ako riadenie technických zmien s preukázaním, že systém spĺňa stanovené požiadavky na bezpečnosť. Požiadavky noriem CENELEC, ktoré sa nedajú uplatniť na organizačné a prevádzkové stránky, súvisia výhradne so zariadeniami na návrh technických systémov, ako sú napr. „inherentná bezpečnosť technického zariadenia pri poruche“, elektromagnetická kompatibilita (EMC) atď.

5.2. Dokument vypracovaný navrhovateľom podľa bodu 5.1 obsahuje aspoň:

a) opis organizácie a expertov vymenovaných na vykonávanie procesu posudzovania rizík,
b) výsledky jednotlivých fáz posudzovania rizík a zoznam všetkých potrebných požiadaviek na bezpečnosť, ktoré sa musia splniť s cieľom kontrolovať riziko na prijateľnej úrovni.

[G 1] Tieto dôkazy je možné, v závislosti od zložitosti systému, zaradiť do jednej alebo viacerých bezpečnostných preukazov. Štruktúru bezpečnostného preukazu technických systémov a ich prevádzkových a organizačných stránok pozri v odsekoch [G 4] a [G 5] v časti 5.1.

[G 2] Možné príklady dôkazov pozri aj v časti A.4. dodatku A.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

[G 3] Očakávaná životnosť technických systémov a subsystémov v železničnom sektore je približne 30 rokov. Počas takého dlhého obdobia je možné očakávať viaceré významné zmeny na týchto systémoch. Na týchto systémoch a ich rozhraniach by tak mohli vykonať ďalšie posudzovanie rizík so sprievodnou dokumentáciou rôzni aktéri a organizácie, ktoré používajú záznam o nebezpečenstve . To znamená skôr prísne požiadavky na kontrolu dokumentácie a riadenie konfigurácie.

[G 4] Je teda užitočné, keď podnik, ktorý archivuje všetky informácie o posudzovaní rizík a riadení rizík, zaručí fyzickú podporu uchovávaných výsledkov/informácií, ktoré sú čitateľné/prístupné počas celej životnosti systému (napr. počas 30 rokov).

[G 5] Hlavné dôvody tejto požiadavky, okrem iného, sú:

a) zabezpečenie, aby všetky bezpečnostné analýzy a bezpečnostné záznamy o posudzovanom systéme boli prístupné počas celej životnosti systému, a to:

   (1) v prípade ďalších významných zmien toho istého systému, aby bola k dispozícii posledná aktuálna dokumentácia systému;
   (2) v prípade akéhokoľvek problému počas životnosti systému, aby bolo možné vrátiť sa k príslušným analýzam bezpečnosti a k bezpečnostným záznamom;

b) zabezpečenie, aby bezpečnostné analýzy a bezpečnostné záznamy posudzovaného systému boli prístupné v prípade, keď sa použije pri inej aplikácii ako podobný referenčný systém.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

PRÍLOHA II K NARIADENIU O CSM

Kritériá, ktoré musia spĺňať orgány pre posudzovanie

1. *Orgán pre posudzovanie nesmie byť priamo ani ako splnomocnený zástupca zapojený do návrhu, výroby, výstavby, uvádzania na trh, prevádzky alebo údržby požadovaného systému. To nevylučuje možnosť výmeny technických informácií medzi týmto orgánom a zúčastnenými aktérmi.*

2. *Orgán pre posudzovanie musí vykonávať posudzovanie čo najsvedomitejšie a s čo najväčšou možnou technickou spôsobilosťou a nesmie byť vystavený žiadnemu tlaku ani podnetom najmä finančného druhu, ktoré by mohli ovplyvniť jeho úsudok alebo výsledky jeho posudzovania, a to najmä zo strany osôb alebo skupín osôb, ktorých sa posudzovanie dotýka.*

3. *Orgán pre posudzovanie musí vlastniť prostriedky, ktoré sú nevyhnutné na primerané vykonávanie technických a správnych úloh spojených s posudzovaním; mal by mať aj prístup k výbave potrebnej na mimoriadne posudzovanie.*

4. *Pracovníci zodpovední za posudzovanie musia mať:*

   - *riadny technický a odborný výcvik,*
   - *uspokojivé znalosti o požiadavkách týkajúcich sa posudzovania, ktoré vykonávajú, ako aj dostatočnú prax v týchto posudzovaniach,*
   - *schopnosť vypracúvať správy o posúdení bezpečnosti, z ktorých pozostávajú formálne závery vykonaného posúdenia.*

5. *Nezávislosť pracovníkov zodpovedných za nezávislé posudzovania musí byť garantovaná. Žiadny úradník sa nesmie odmeňovať na základe počtu vykonaných posúdení ani výsledkov týchto posúdení.*

6. *Ak je orgán pre posudzovanie externým orgánom vo vzťahu k organizácii navrhovateľa, musí mať poistenie občianskoprávnej zodpovednosti, pokiaľ táto zodpovednosť nie je pokrytá vnútroštátnymi právnymi predpismi daného štátu alebo pokiaľ posudzovanie nevykonáva priamo tento daný členský štát.*

7. *Ak je orgán pre posudzovanie externým orgánom vo vzťahu k organizácii navrhovateľa, pracovníci tohto orgánu sú viazaní povinnosťou mlčanlivosti v súvislosti so všetkým, čo sa dozvedia pri výkone svojich povinností (s výnimkou príslušných správnych orgánov v štáte, v ktorom vykonávajú svoju činnosť) na základe tohto nariadenia.*

[G 1] Ďalšie vysvetlenie sa nepovažuje za potrebné.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

DODATOK A: ĎALŠIE VYSVETLENIA

A.1. Úvod

A.1.1. Účelom tohto dodatku je uľahčiť čítanie tohto dokumentu. Namiesto rozsiahlych informácií v dokumente samom je zložitejšia problematika vysvetlená v tomto dodatku.

A.2. Klasifikácia nebezpečenstiev

A.2.1. Usmernenie ku klasifikácii/zaraďovaniu nebezpečenstiev je uvedené v časti § 4.6.3 normy EN 50 126-1 {Ref. 8}, ako aj v dodatku B.2 k usmerneniu EN 50 126-2 {Ref. 9}.

A.3. Kritérium akceptovania rizika pre technické systémy (RAC-TS)

A.3.1. Horná hranica prijateľnosti rizika pre technické systémy

A.3.1.1. Kritérium akceptovania rizika pre technické systémy RAC-TS je opísané v časti 2.5.4 príručky {Ref. 4}.

A.3.1.2. Účelom RAC-TS je stanovenie hornej hranice prípustného rizika pre technické systémy, pre ktoré nie je možné odvodiť požiadavky na bezpečnosť s použitím kódexov postupov ani porovnaním s podobnými referenčnými systémami. V dôsledku toho kritérium vymedzuje referenčný bod, na základe ktorého je možné kalibrovať metódy analýzy rizík pre technické systémy. V časti A.3.6 dodatku A tohto dokumentu sa píše, že tento referenčný bod alebo hornú hranicu prijateľnosti rizík je možné použiť na určenie kritéria akceptovania rizika ďalších funkčných porúch technických systémov, ktoré nemajú vierohodný priamy potenciál katastrofických dôsledkov (t. j. ďalších závažných následkov). Ale RAC-TS nie je metóda analýzy rizík.

A.3.1.3. RAC-TS je semikvantitatívne kritérium. Uplatňuje sa na náhodné poruchy hardvéru a systematické poruchy/chyby technického systému. Ním sú pokryté aj systematické poruchy/chyby technického systému, ktoré môžu byť zapríčinené chybami človeka v procese vývoja technického systému (t. j. v špecifikácii, návrhu, implementácii a validácii). RAC-TS sa ale nevzťahuje na ľudské chyby v prevádzke a údržbe technických systémov.

A.3.1.4. Podľa dodatkov A.3 a A.4 k norme CENELEC 50 129 nie sú systematické poruchy/chyby kvantifikovateľné, a teda sa kvantitatívny cieľ musí preukazovať len pri náhodných poruchách hardvéru, kým systematické poruchy/chyby sa riešia kvalitatívnymi metódami[17]. *„Pretože kvantitatívnymi metódami nie je možné posudzovať integritu systematických porúch, úrovne integrity bezpečnosti sa používajú na skupinové metódy, nástroje a techniky, o ktorých sa usudzuje, že keď sa používajú efektívne, zabezpečia primeranú úroveň spoľahlivosti stanovenej úrovne integrity pri realizácii systému.“*

A.3.1.5. Podobne, podľa noriem CENELEC, ani integrita softvéru technických systémov nie je kvantifikovateľná. V norme CENELEC 50 128 je uvedené usmernenie k procesu vývoja

---

(17) *Podľa noriem CENELEC 50 126, 50 128 a 50 129 na zvládnutie systematických porúch/chýb sa musia kvantitatívne údaje o náhodných poruchách hardvéru vždy spájať s úrovňou integrity bezpečnosti. Preto údaj $10^{-9}\ h^{-1}$ RAC-TS si tiež vyžaduje, aby sa primeraný proces zaviedol aj na správne zvládnutie systematických porúch/chýb. Ale na uľahčenie znenia tejto poznámky, často odkazuje len na náhodné poruchy hardvéru technického systému.*

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

softvéru súvisiaceho s bezpečnosťou, fungujúceho na požadovanej úrovni integrity bezpečnosti. Usmernenie zahŕňa procesy navrhovania, verifikácie, validácie a zaisťovania kvality softvéru.
Na implementáciu bezpečnostných funkcií programovateľného elektronického riadiaceho systému, podľa normy CENELEC 50 128 je SIL 4 najvyššou možnou úrovňou integrity bezpečnosti procesu vývoja softvéru, ktorá zodpovedá hodnote $10^{-9}\,h^{-1}$ kvantitatívnej tolerovateľnej intenzity nebezpečenstiev.

A.3.1.6. Preto vzhľadom na to, že systematické poruchy/chyby nie je možné kvantifikovať, je potrebné zaobchádzať s nimi kvalitatívne zavedením kvalitatívnych a bezpečnostných procesov, ktoré sú zlučiteľné s úrovňou integrity bezpečnosti požadovanej pre posudzovaný systém:

a) účelom kvalitatívneho procesu je *„minimalizovať incidenciu chýb človeka v každej etape životného cyklu, a tým znížiť riziko systematických chýb systému“*;

b) účelom bezpečnostného procesu je *„ďalej znížiť incidenciu chýb človeka, ktoré počas životného cyklu súvisia s bezpečnosťou, a tým minimalizovať zostatkové riziko systematických chýb, ktoré súvisia s bezpečnosťou“*.

A.3.1.7. Usmernenie na riadenie výskytu systematických porúch/chýb, ako aj usmernenie týkajúce sa možných projektových opatrení na ochranu pred poruchami so spoločnými príčinami (*Common Cause/Mode Failures; CCF/CMF*) a na zaistenie, aby sa technický systém uviedol do bezpečného stavu v prípade týchto porúch/chýb je uvedené v normách:

a) v norme CENELEC 50 126-1 {Ref. 8} a v príručke 50 126-2 {Ref. 9} k nej je uvedený zoznam ustanovení normy CENELEC 50 129 a ich uplatniteľnosť na dokumentované dôkazy iných ako signalizačných systémov: pozri tabuľku 9.1 v príručke 50 126-2 {Ref. 9}. V tomto zozname sú odkazy na usmernenie o riešení porúch samotného systému a účinkov prostredia na posudzovaný systém;

Napríklad techniky/opatrenia týkajúce sa návrhových vlastností sú uvedené v *„tabuľke E.5*: *Vlastnosti návrhu (uvádzané v 5.4)“* normy CENELEC 50 129 {Ref. 7} *„na zabránenie poruchových stavov a riadenie poruchových stavov spôsobených:*

(1) *„akýmikoľvek pretrvávajúcimi poruchovými stavmi návrhu“;*
(2) *„podmienkami prostredia“;*
(3) *„chybným použitím alebo prevádzkovými omylmi“;*
(4) *„akýmikoľvek pretrvávajúcimi poruchovými stavmi softvéru“*
(5) *„ľudskými faktormi“.*

V dodatkoch D a E k norme CENELEC 50 129 {Ref. 7} sú uvedené techniky a opatrenia na zabránenie vzniku systematických chýb a na kontrolu náhodných a systematických porúch/chýb hardvéru elektronických signalizačných systémov súvisiacich s bezpečnosťou. Mnohé z nich možno rozšíriť aj na iné ako signalizačné systémy odkazom na tieto usmernenia v tabuľke 9.1 príručky 50 126-2 {Ref. 9}.

b) v norme CENELEC 50 128 je uvedené usmernenie k procesu vývoja bezpečnostného softvéru fungujúceho na úrovni integrity bezpečnosti (SIL 0 až SIL 4), ktorá sa požaduje pre softvér posudzovaného systému.

A.3.1.8. RAC-TS predstavuje aj najvyššiu úroveň integrity, ktorú je možné vyžadovať tak podľa noriem CENELEC, ako aj IEC. Tu sú na uľahčenie porovnania citáty z noriem IEC 61508-1 a CENELEC 50 129:

a) IEC 61508-1: *„Táto norma ustanovuje dolnú medzu cieľových poruchových kritérií v režime nebezpečnej poruchy, ktoré sa môžu nárokovať. Kritériá špecifikované ako dolné medze hladiny integrity bezpečnosti 4 (t. j. priemerná pravdepodobnosť*

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

poruchy 10^{-5} vykonávania určitej funkcie na požiadanie alebo pravdepodobnosť nebezpečnej poruchy 10^{-9} za hodinu). Pri nezložitých systémoch je možné dosiahnuť návrhy bezpečnostných systémov s nižšími hodnotami cieľových poruchových kritérií, ale údaje v tabuľke reprezentujú medzu, ktorá sa môže v súčasnosti dosiahnuť pri relatívne zložitých systémoch (napríklad pri programovateľných bezpečnostných systémoch).“

b) EN 50129: *„Funkcia, ktorá má kvantitatívne požiadavky väčšie ako $10^{-9}h^{-1}$, sa musí spracovať jedným z nasledujúcich spôsobov:*

(1) *ak sa môže funkcia rozdeliť na funkčne nezávislé podfunkcie, môže sa THR rozdeliť medzi tieto podfunkcie a každej z týchto podfunkcií priradiť SIL;*
(2) *ak sa funkcia nemôže rozdeliť, musia sa prinajmenšom splniť opatrenia a metódy požadované pre SIL 4 a funkcia sa musí použiť v kombinácii s ďalšími technickými a prevádzkovými opatreniami, aby sa dosiahla nevyhnutná THR.“*

A.3.1.9. Pre všetky technické systémy je potom potrebné obmedziť kvantitatívnu požiadavku na bezpečnosť na tento údaj. Ak je potrebná vyššia úroveň ochrany, nemôže ju spĺňať len jeden systém. Architektúru systému je potrebné zmeniť, napr. s použitím dvoch nezávislých paralelných systémov, ktoré vzájomne krížovo kontrolujú generovanie bezpečných výstupov. Toto však nepochybne zvyšuje náklady na vývoj technického systému.

Poznámka: Ak existujú funkcie, napr. čisto mechanické systémy, ktoré podľa skúseností z prevádzky môžu dosahovať vyššiu úroveň integrity, potom je možné opísať úroveň bezpečnosti určitým kódexom postupov alebo možno požiadavky na bezpečnosť stanoviť na základe analýzy podobnosti s existujúcim systémom. RAC-TS je potrebné uplatňovať v rozsahu pôsobnosti CSM, len ak neexistuje žiadny kódex postupov ani referenčný systém.

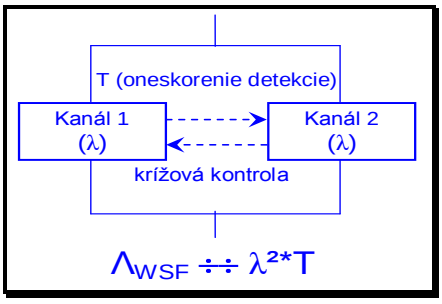
A.3.1.10. Napokon je možné zhrnúť toto:

a) podľa noriem CENELEC 50 126, 50 128 a 50 129 systematické poruchy/chyby vo vývoji nie sú kvantifikovateľné;

b) výskyt systematických porúch/chýb, ako aj ich zostatkové riziko je potrebné kontrolovať a riadiť uplatňovaním primeraných procesov riadenia kvality a bezpečnosti, ktoré sú zlučiteľné s úrovňou integrity bezpečnosti požadovanej pre posudzovaný systém;
c) najvyššia dosiahnuteľná úroveň integrity bezpečnosti je SIL 4 tak pre náhodné poruchy hardvéru, ako aj systematické poruchy/chyby technických systémov;
d) táto najvyššia medza úrovne integrity bezpečnosti SIL 4 znamená, že aj maximálnu tolerovateľnú intenzitu nebezpečenstva (THR), (t. j. maximálnu poruchovosť) technických systémov je potrebné obmedziť na 10^{-9} h^{-1}.

A.3.1.11. Tolerovateľnú intenzitu nebezpečenstva 10^{-9} h^{-1} môže dosiahnuť buď technický systém s „bezpečnou architektúrou“ (ktorá má takú bezpečnostnú výkonnosť podľa definície), alebo s „redundantnou architektúrou“ (napr. s dvoma nezávislými spracovateľskými kanálmi, ktoré sa navzájom krížovo kontrolujú).

Pri redundantnej architektúre je možné ukázať, že celková pravdepodobnosť nebezpečnej poruchy technického systému (Λ_{WSF}) je úmerná λ^2*T, kde:
a) λ^2 je intenzita nebezpečných porúch jedného kanála na druhú;



Obr. 13: Redundantná architektúra technického systému.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

b) T je čas potrebný na to, aby jeden kanál zistil nebezpečnú poruchu druhého kanála. Zvyčajne je násobkom spracovacieho času/cyklu kanála. Obvykle je T oveľa menšie ako 1 sekunda.

A.3.1.12. Vychádzajúc zo vzťahu (λ^2*T) je teoreticky možné ukázať (ak uvážime len náhodné poruchy hardvéru technického systému – pozri aj odsek A.3.1.13. v dodatku A.), že kvantitatívnu požiadavku 10^{-9} h^{-1} kritéria RAC-TS je možné splniť. Systematické poruchy/chyby musí riadiť proces: pozri odsek A.3.1.6. v dodatku A. Napríklad:

a) pri bezporuchovosti kanála so stredným časom medzi dvoma poruchami (MTBF) 10 000 hodín a opatrnom predpoklade, že každá porucha kanála je nebezpečná, je pravdepodobnosť nebezpečnej poruchy kanála $10^{-4}h^{-1}$;
b) dokonca aj pri 10 minútach (t. j. $\approx 2*10^{-3}$ hodiny) potrebných na zistenie nebezpečnej poruchy na druhom kanáli, čo je tiež opatrný predpoklad.

Celková pravdepodobnosť nebezpečnej poruchy $\Lambda_{WSF} \approx 2 * 10^{-10}$ h^{-1}.

A.3.1.13. V praxi je pri takejto redundantnej architektúre a kvantitatívnom hodnotení celkovej pravdepodobnosti nebezpečných porúch hardvéru potrebné uvážiť opatrenia, ktoré sa v návrhu prijmú na ochranu pred poruchami so spoločnými príčinami (CCF/CMF) a na zaistenie, aby sa technický systém v prípade takejto poruchy/chyby so spoločnými príčinami vrátil do bezpečného stavu. Pri hodnotení pravdepodobnosti celkovej nebezpečnej poruchy (Λ_{WSF}) je potrebné posúdiť aj:

a) prvky spoločné pre všetky kanály, napr. jediný alebo spoločný vstup do všetkých kanálov, spoločné zásobovanie energiou, komparátory, rozhodovacie členy atď.
b) čas potrebný na detekciu „spiacich“ alebo latentných porúch. Pri komplexných technických systémoch môže byť tento čas rádovo niekoľko násobne prevyšovať 1 sekundu;
c) vplyv porúch so spoločnou príčinou (CCF/CMF).

Usmernenie na tieto témy je možné nájsť v normách, ktoré sú citované v odseku A.3.1.7. dodatku A k tomuto dokumentu.

A.3.2. Vývojový diagram testu uplatniteľnosti RAC-TS

A.3.2.1. Spôsob uplatňovania RAC-TS na nebezpečenstvá spôsobené poruchami technických systémov možno znázorniť, ako ukazuje Obr. 14.

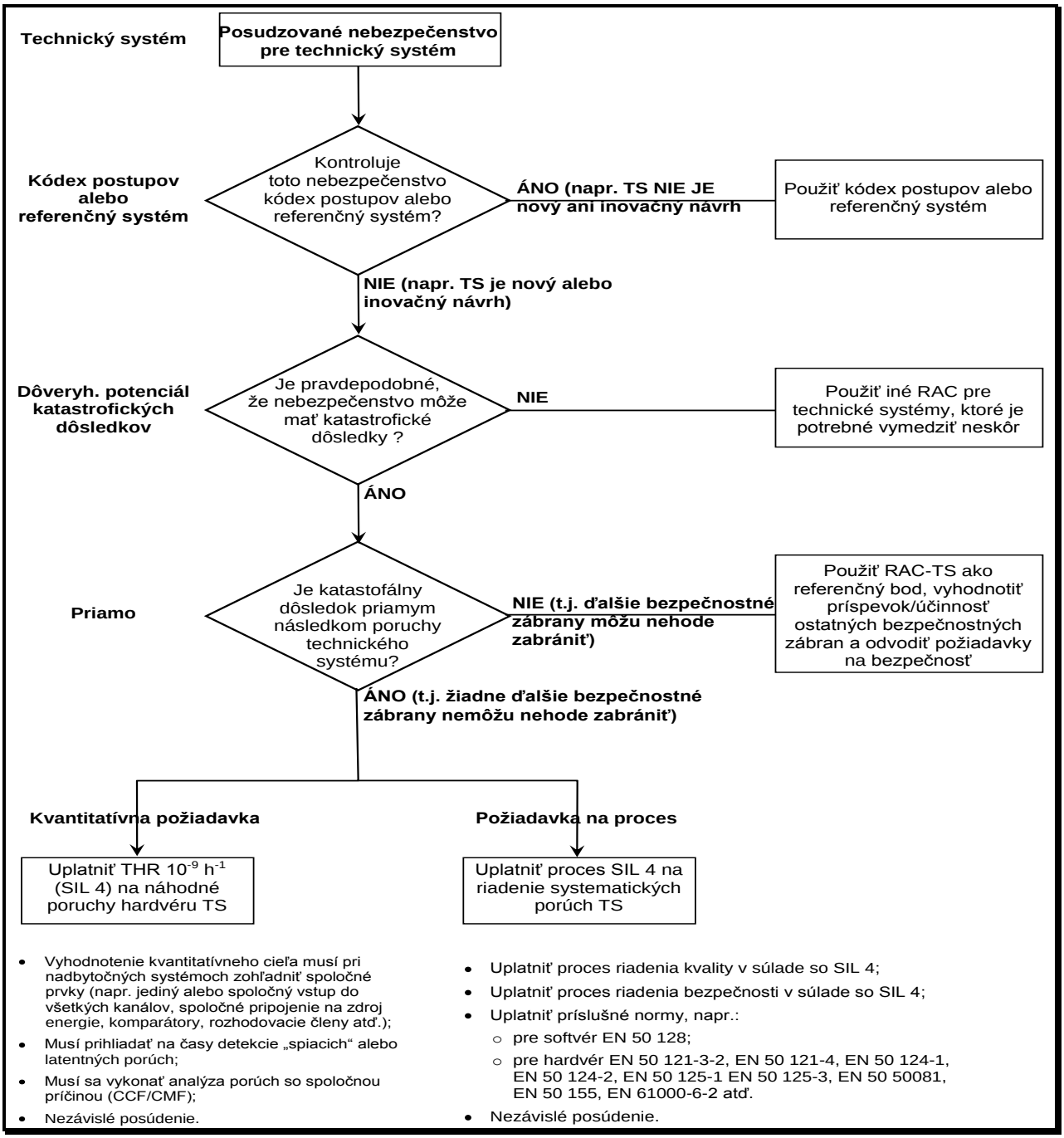
A.3.2.2. Použitie tohto vývojového diagramu je uvedené na príklade v časti C.15 dodatku C.

A.3.3. Vymedzenie technického systému podľa nariadenia o CSM

A.3.3.1. Kritérium RAC-TS platí len pre technické systémy. Toto je definícia „technického systému“ uvedená v bode **Error! Reference source not found.** článku 3 nariadenia o CSM:

„„technický systém“ znamená výrobok alebo súbor výrobkov vrátane koncepčnej, implementačnej a podpornej dokumentácie; vývoj technického systému sa začína špecifikovaním jeho požiadaviek a končí sa jeho prijatím; hoci sa berie do úvahy návrh relevantných rozhraní s ľudským správaním, ľudskí operátori a ich činnosti nie sú zahrnuté do technického systému; proces údržby sa opisuje v príručkách údržby, sám však nie je súčasťou technického systému.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu



Obr. 14: Vývojový diagram testu uplatniteľnosti RAC-TS.

A.3.4. Vysvetlenie vymedzenia pojmu „technického systému“

A.3.4.1. V tomto vymedzení pojmu technického systému je opísaný rozsah a obsah technického systému: *„technický systém znamená výrobok alebo súbor výrobkov vrátane koncepčnej, implementačnej a podpornej dokumentácie.“* Podľa neho, súčasti systému sú a tvoria ho:

a) fyzické časti, ktoré tvoria technický systém;
b) príslušný softvér (ak je jeho súčasťou);

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

c) návrh a realizáciu technického systému vrátane prípadnej konfigurácie alebo parametrizácie všeobecného a spoločného výrobku vzhľadom na konkrétne požiadavky konkrétneho použitia;
d) potrebnú pomocnú dokumentáciu na:

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

A.3.4.2. Poznámky pripojené k tomuto vymedzeniu špecifikujú ďalší obsah a rozsah technického systému:

a) *„vývoj technického systému sa začína špecifikovaním jeho požiadaviek a končí sa jeho prijatím;“* Jeho súčasťou je 10 fáz V-cyklu znázorneného na obrázku 10 normy CENELEC 50 126-1 {Ref. 8};

b) *„napriek tomu, že návrh príslušných rozhraní zohľadňuje ľudské správanie, ľudskí operátori a ich činnosti nie sú zahrnuté do technického systému;“* Napriek tomu, že chyby zapríčinené ľudským činiteľom počas prevádzky a údržby technického systému nie sú súčasťou technického systému samého, návrh rozhraní musí zohľadňovať človeka ako prevádzkovateľa. Účelom je zníženie pravdepodobnosti chýb človeka zapríčinených nevhodným návrhom príslušných rozhraní s človekom ako prevádzkovateľom na minimum;

c) *„proces údržby sa opisuje v príručkách údržby, sám však nie je súčasťou technického systému;“* To znamená, že RAC-TS sa nemusí uplatňovať na prevádzku a údržbu technického systému; tieto úzko súvisia s procesmi a činnosťami, ktoré vykonáva personál.
V záujme podpory údržby technických systémov však vymedzenie technického systému musí obsahovať príslušné požiadavky (napr. na pravidelnú preventívnu údržbu alebo opravy v prípade porúch), na dostatočnej úrovni podrobnosti. Súčasťou vymedzenia technického systému nie je spôsob organizácie a vykonávania údržby súvisiaceho technického systému, ktorý je v zodpovedajúcich návodoch na údržbu.

A.3.4.3. Pozri časť A.3.1. dodatku A.

A.3.5. Funkcie technických systémov, na ktoré sa vzťahuje kritérium RAC-TS

A.3.5.1. Podľa definície RAC-TS sa toto kritérium uplatňuje na nebezpečné poruchy funkcií, ktoré má technický systém plniť, ak tieto poruchy *„majú vierohodný **priamy** potenciál katastrofického dôsledku“*: pozri časť 2.5.4 v {Ref. 4}.

A.3.5.2. RAC-TS sa môže uplatniť aj na funkcie, na ktorých sa zúčastňujú technické systémy, ktorých poruchy nemajú *„priamy potenciál katastrofického dôsledku“*. V tomto prípade je potrebné RAC-TS uplatniť ako celkový cieľ súboru udalostí, ktorý vedie ku katastrofálnemu dôsledku. Skutočný príspevok každej udalosti, a teda funkčné poruchy technického systému, ktorý sa zúčastňuje na posudzovanom scenári, je potrebné odvodiť podľa časti A.3.6 dodatku A vzhľadom na uvedený celkový cieľ.
Takéto použitie kritéria RAC-TS je potrebné prerokovať a dohodnúť v rámci pracovnej skupiny pre CSM.

A.3.5.3. Na ktoré funkcie technického systému sa vzťahuje RAC-TS? Podľa normy IEC 61226:2005:

a) je v tomto kontexte funkcia vymedzená ako *„špecifický účel alebo cieľ, ktorý sa má dosiahnuť a ktorý je možné špecifikovať alebo opísať bez odkazu na fyzické prostriedky, ktorými sa dosiahol“;*

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

b) funkcia (považovaná za čiernu skrinku) prenáša vstupné parametre (napr. materiál, energiu, informácie) do výstupných parametrov súvisiacich s cieľom (napr. materiálu, energie, informácií);
c) analýza funkcie nezávisí od jej technickej realizácie.

A.3.5.4. RAC-TS je uplatniteľné na tieto druhy funkcií:

a) príklady vozidlového subsystému ETCS:

(1) „poskytnúť vodičovi údaje, ktoré mu umožnia viesť vlak bezpečne a zapnúť brzdy v prípade prekročenia dovolenej rýchlosti“. Na základe informácií (o dovolenej rýchlosti) prijatých z traťového subsystému a výpočtu rýchlosti vlaku palubným ETCS, sú vodič a palubný ETCS schopní riadiť vlak tak, aby neprekročil stanovenú dovolenú rýchlosť. Na vyhodnotenie rýchlosti vlaku palubným zariadením sa uplatňuje RAC-TS, pretože:

(i) už neexistuje žiadna ďalšia (priama) prekážka, keby vodič poskytnutú informáciu nedocenil;
(ii) prekročenie dovolenej rýchlosti by mohlo mať za následok vykoľajenie vlaku, ktoré je nehodou s potenciálnymi katastrofickými dôsledkami;

(2) „poskytnúť vodičovi informácie, ktoré mu umožňujú viesť vlak bezpečne a zapnúť brzdy v prípade porušenia udeleného oprávnenia na pohyb“.

b) príklad traťového obvodu: „zistiť obsadenie traťového úseku“. RAC-TS samo bude možné uplatniť na túto funkciu, len ak zabezpečovacie zariadenie nebude mať implementovanú funkciu *„sequence monitoring“* (sledovanie radenia);
c) príklad bodu: „kontrolovať polohu bodu“.

A.3.5.5. Niektoré normy vymedzujú aj funkcie, na ktoré by sa mohlo kritérium RAC-TS uplatňovať. Napríklad:

a) v normatívnej časti návrhu európskej normy EN 0015380-4 {Ref. 13} (ModTrain Work) sú vymedzené tri úrovne hierarchických funkcií (rozšírené v informačných prílohách na päť úrovní). V návrhu prEN 0015380-4 je spolu vymedzených niekoľko stoviek funkcií súvisiacich s vlakmi;
b) vo všeobecnosti sa odporúča vybrať funkcie z prvých troch úrovní podľa návrhu prEN 0015380-4 (ale nie nižších) aj s prihliadnutím na štruktúru rozpisu výrobkov;
c) pri funkciách, ktoré nie sú v rozsahu pôsobnosti návrhu prEN 0015380-4, je potrebné rozhodnúť o funkčnej úrovni na základe porovnania s využitím odborného posudku.

Je potrebné, aby agentúra v rámci prác na všeobecne prijateľných rizikách a kritériách akceptovania rizika ešte dopracovala uvedené príklady funkcií z návrhu prEN 0015380-4.

A.3.5.6. RAC-TS je možné uplatňovať aj napr. na tieto funkcie podľa návrhu prEN 0015380-4: *„control tilting (kontrola naklonenia)“* (kód = CLB). Funkciu by bolo možné využiť na úrovni systému týmito dvoma spôsobmi:

a) v prvom prípade: vlak sa musí nakláňať v zákrutách kvôli pohodliu cestujúcich a musí sa sledovať zhoda prierezu vlaku s gabaritom traťovej infraštruktúry;
b) v druhom prípade: vlak sa musí nakláňať v zákrutách len kvôli pohodliu cestujúcich ale nemusí sa sledovať zhoda prierezu vlaku s gabaritom traťovej infraštruktúry.

RAC-TS sa bude uplatňovať len v prvom prípade, v druhom nie, pretože porucha funkcie kontroly nakláňania nemá katastrofické dôsledky.

A.3.5.7. Príklad b) v odseku A.3.5.4. a príklady v odseku A.3.5.6. dodatku A jasne ukazujú, že nebude možné vopred vytvoriť zoznam funkcií, na ktoré sa vo všetkých príkladoch uplatňuje RAC-TS. Vždy to bude závisieť od toho, ako bude systém využívať funkcie subsystému.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

A.3.5.8. Príklad uplatnenia kritéria RAC-TS je uvedený v časti C.15. dodatku C.

A.3.6. Príklady uplatnenia RAC-TS

A.3.6.1. Úvod

a) V tejto kapitole sú príklady určovania poruchovosti s ďalšími závažným nebezpečnými dôsledkami a možnosti odvodenia nižších požiadaviek na bezpečnosť než $10^{-9}\,h^{-1}$. Tento dokument neuprednostňuje ani neukladá použitie určitej metódy. Iba pre informáciu ukazuje možnosti uplatnenia kritéria RAC-TS na kalibrovanie niektorých často používaných metód. Je potrebné, aby ho agentúra ďalej rozvíjala v práci o všeobecne prijateľných rizikách a kritériách akceptovania rizika.

b) V skutočnosti je možné RAC-TS uplatniť priamo len v malom počte prípadov, lebo v praxi funkčné poruchy technických systémov často nevedú priamo k nehodám s potenciálne katastrofickými dôsledkami. Preto je možné na uplatnenie kritéria na nebezpečenstvá bez katastrofických dôsledkov a na určenie cieľovej poruchovosti vykonať zámeny (napr. použitím tohto kritéria na kalibrovanie matice rizík) medzi rôznymi parametrami, napr. medzi závažnosťou a početnosťou.

A.3.6.2. Príklad 1: Priama zámena rizík

a) Kritérium RAC-TS je možné ľahko uplatniť na scenáre, ktoré sa od referenčných podmienok, vymedzených pre RAC-TS v časti 2.5.4 nariadenia o CSM {Ref. 3}, líšia iba niekoľkými nezávislými parametrami;

b) Predpokladajme, že určitý parameter p má charakter násobku rizika. Predpokladajme, že p* existuje v referenčnej podmienke a p' je možné použiť v alternatívnom scenári. V tomto prípade je relevantný iba podiel parametrov p*/p' a početnosť výskytu je možné znížiť. Tento postup je možné opakovať, ak sú parametre nezávislé.

c) Príklad:

(1) Predpokladajme, že odborným posudkom bol posúdený skutočný potenciál katastrofických dôsledkov ako desaťnásobne menší než potenciál za referenčných podmienok uvedených v časti 2.5.4 nariadenia o CSM {Ref. 3}. Potom namiesto $10^{-9}\,h^{-1}$ bude požiadavka $10^{-8}\,h^{-1}$.

(2) Predpokladajme, že bola zistená ďalšia bezpečnostná prekážka, ktorou je iný technický systém (nezávisle od dôsledkov) a ktorá je účinná v 50 % prípadov;

(3) Požiadavka na bezpečnosť by potom namiesto $10^{-9}\,h^{-1}$ bola $5*10^{-7}\,h^{-1}$ (t. j. $0{,}5*10^{-8}\,h^{-1}$).

A.3.6.3. Príklad 2: Kalibrovanie matice rizík

a) Na náležité uplatnenie kritéria RAC-TS v matici rizík sa musí matica vzťahovať na správnu systémovú úroveň (porovnateľnú s podmienkami uvedenými v časti A.3.5. v dodatku A).

b) RAC-TS vymedzuje v matici rizík ako prijateľné jedno pole, ktoré zodpovedá súradnici (katastrofická závažnosť; početnosť výskytu $10^{-9}\,h^{-1}$): pozri červené pole v Tab. 5. Všetky polia, ktoré súvisia s vyššou početnosťou, sa označia ako „neprijateľné“. Treba poznamenať, že len v prípade dôveryhodného priameho potenciálu katastrofických dôsledkov je početnosť nehôd rovnaká ako početnosť funkčných porúch.

c) Zvyšok matice sa môže vyplniť, ale musí sa prihliadnuť na účinky, ako je neochota prijať riziko alebo odstupňovanie kategórií. V najjednoduchšom prípade pri lineárnom desiatkovom odstupňovaní (ako ukazuje šípka v Tab. 5) je pole, uvedeným spôsobom podľa kritéria RAC-TS označené ako „prijateľné“, lineárne extrapolované na zvyšok matice. To znamená, že všetky polia na tej istej uhlopriečke (alebo pod touto

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

uhlopriečkou) sú tiež označené ako „prijateľné“. Polia pod nimi možno tiež označiť za „prijateľné“.

Tab. 5: Typický príklad kalibrovanej matice rizík.

Početnosť výstkytu nehody (spôsobenej nebezpečenstvom)	**Úroveň rizika**			
Častá ($10^{-4}.h^{-1}$)	neprijateľná	neprijateľná	neprijateľná	neprijateľná
Pravdepodobná ($10^{-5}.h^{-1}$)	neprijateľná	neprijateľná	neprijateľná	neprijateľná
Občasná ($10^{-6}.h^{-1}$)	prijateľná	neprijateľná	neprijateľná	neprijateľná
Malá ($10^{-7}.h^{-1}$)	prijateľná	prijateľná	neprijateľná	neprijateľná
Nepravdepodobná ($10^{-8}.h^{-1}$)	prijateľná	prijateľná	prijateľná	neprijateľná
Veľmi nepravdepodobná ($10^{-9}.h^{-1}$)	prijateľná	prijateľná	prijateľná	prijateľná
	nevýznamná	okrajová	kritická	katastrofálna
	Úrovne závažnosti dôsledkov nebezpečenstva (t. j. nehody)			

Hodnotenie rizika	**Zníženie rizika/kontrola**
neprijateľné	Riziko sa musí znížiť.
prijateľné	Riziko je prijateľné. Vyžaduje sa nezávislé posúdenie.

d) Keď je matica vyplnená, možno ju uplatniť aj na nekatastrofické nebezpečenstvá. Ak napr. iná funkčná porucha má závažnosť klasifikovanú ako „kritická“, potom by podľa kalibrovanej matice rizík nemala byť prijateľná početnosť nehôd „nepravdepodobná“ (alebo veľmi nepravdepodobná).

e) Treba pripomenúť, že použitie matice rizík môže viesť k prehliadnutiu opatrných výsledkov, keď sa matica uplatní na početnosti funkčných porúch (t. j. na funkčné poruchy, ktorých priamym dôsledkom nemusí byť nehoda).

A.3.6.4. Zásada pri kalibrovaní iných metód analýzy rizík

Aj ďalšie metódy analýzy rizík, napr. navrhovanú schéma číslovania priority rizík alebo graf uvedený v normách VDV 331 alebo IEC 61508, je možné kalibrovať podobným postupom, ako bolo naznačené pri matici rizík:

a) prvý krok: klasifikácia referenčného bodu podľa kritéria RAC-TS ako prijateľného a bodov s vyššou početnosťou alebo vyššou závažnosťou ako neprijateľných podľa RAC-TS;
b) druhý krok: použitie mechanizmov zámeny určitej metódy na extrapoláciu prijateľnosti rizika nekatastrofických nebezpečenstiev (použitím lineárnej zámeny rizík ako východiskového bodu);
c) tretí krok: pre nekatastrofické nebezpečenstvá je potom možné odvodiť RAC-TS z kalibrovanej metódy analýzy rizík porovnaním súradnice (početnosti; závažnosti) so získanou krivkou FN.

A.3.7. Závery pre RAC-TS

A.3.7.1. Vo všeobecnom rámci posudzovania rizík, navrhovanom nariadením o CSM, sú potrebné kritériá akceptovania rizika na určenie, kedy sa zostatková úroveň rizika/rizík stáva prijateľnou, a teda kedy sa má skončiť explicitné odhadovanie rizík.

A.3.7.2. RAC-TS je cieľovou hodnotou ($10^{-9}\,h^{-1}$) návrhu technického systému.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

A.3.7.3. Hlavnými účelmi RAC-TS sú:

a) stanovenie hornej hranice prijateľnosti rizika a nadväzne referenčný bod, na základe ktorého je možné pre technické systémy kalibrovať metódy analýzy rizík;
b) umožnenie vzájomného uznávania technických systémov, pretože posudzovanie súvisiaceho rizika a bezpečnosti sa bude hodnotiť podľa toho istého kritéria akceptovania rizika vo všetkých ČŠ;
c) úspora nákladov, pretože si nevyhnutne nevyžaduje vysoké kvantitatívne požiadavky na bezpečnosť;
d) uľahčenie hospodárskej súťaže medzi výrobcami. Použitie rôznych kritérií akceptovania rizika buď vo funkcii navrhovateľa, alebo členského štátu by mohlo viesť odvetvie k vykonávaniu množstva rôznych skúšok na tých istých technických systémoch. Následkom by bolo ohrozenie konkurencieschopnosti výrobcov a zbytočné predraženie výrobkov.

A.3.7.4. Semikvantitatívna požiadavka obsiahnutá v RAC-TS sa pri technických systémoch nemusí preukazovať vždy. V rozsahu pôsobnosti nariadenia o CSM sa RAC-TS v skutočnosti uplatňuje len na technické systémy, ktorých nebezpečenstvá nie je možné vhodne kontrolovať uplatnením kódexov postupov ani porovnaním s referenčnými systémami. To umožňuje stanoviť nižšie požiadavky na bezpečnosť, ak sa podarí zachovať celkovú bezpečnostnú úroveň.

A.3.7.5. Harmonizované semikvantitatívne kritérium pre technické systémy je potrebné, len keď neexistuje žiadny kódex postupov ani referenčný systém.

A.3.7.6. Vzhľadom na to, že úroveň integrity bezpečnosti pre systematické poruchy/chyby technických systémov je obmedzená na SIL 4, musí sa na SIL4 obmedziť aj úroveň integrity bezpečnosti náhodných porúch hardvéru. To zodpovedá maximálnej tolerovateľnej intenzite nebezpečenstva (THR) $10^{-9}h^{-1}$ (t. j. maximálnej poruchovosti). Ak sa podľa normy CENELEC 50129 kladú na bezpečnosť náročnejšie požiadavky, nie je ju možné dosiahnuť len jedným systémom; je potrebné zmeniť architektúru systému, napr. použitím dvoch systémov, ktoré bude mať za následok nevyhnutné dramatické zvýšenie nákladov. Viac podrobností pozri v časti A.3.1. v dodatku A.

A.3.7.7. V časti A.3.6 dodatku A sa naznačuje možnosť použitia RAC-TS ako referenčného bodu na kalibrovanie určitých metód analýzy rizík, keď technickým systémom hrozia menej závažné dôsledky poruchy ako katastrofické.

A.4. Dôkazy o posúdení bezpečnosti

A.4.1. Táto časť je usmernením týkajúcim sa dôkazov, ktoré sa zvyčajne predkladajú orgánu pre posudzovanie, so zámerom umožniť mu nezávislé posúdenie a vydať akceptovanie bezpečnosti bez toho, aby boli dotknuté vnútroštátne požiadavky v členskom štáte. Možno ju využiť ako kontrolný zoznam na overenie, že pri uplatnení CSM sú pokryté a dokumentované všetky relevantné súvisiace stránky.

A.4.2. Bezpečnostný plán: CENELEC upozorňuje, že bezpečnostný plán sa vypracúva na začiatku projektu, alebo ak to z hľadiska projektu nie je vhodné, môže byť takýto opis uvedený v inom príslušnom dokumente. Ak sú orgány pre posudzovanie vymenované na začiatku projektu, možno im predložiť na vyjadrenie aj bezpečnostný plán. Bezpečnostný plán v zásade opisuje:

a) zavedenú organizáciu a spôsobilosť ľudí, ktorí sa zúčastňujú na vývoji a na posudzovaní rizík;

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

b) všetky činnosti súvisiace s bezpečnosťou, ktoré sú naplánované počas rôznych fáz projektu, ako aj ich očakávané výstupy.

A.4.3. Dôkazy vyžadované ako výstup fázy vymedzenia systému:

a) opis systému:

(1) vymedzenie rozsahu pôsobnosti/hraníc systému;
(2) opis funkcií;
(3) opis štruktúry systému;
(4) opis prevádzkových a environmentálnych podmienok;

b) opis vonkajších rozhraní;
c) opis interných rozhraní;
d) opis fáz životného cyklu;
e) opis bezpečnostných zásad;
f) opis predpokladov vymedzenia hraníc pre posudzovanie rizík.

A.4.4. Ak sa má umožniť posúdenie rizík, je potrebné, aby vymedzenie systému zohľadnilo kontext zamýšľanej zmeny:

a) ak je zamýšľaná zmena úpravou existujúceho systému, vymedzenie systému opisuje systém pred zmenou a tiež zamýšľanú zmenu;
b) ak je zamýšľaná zmena konštrukciou/výstavbou nového systému, opis sa obmedzí na vymedzenie systému, pretože tu nebude opis žiadneho existujúceho systému.

A.4.5. Dôkazy vyžadované ako výstup fázy identifikácie nebezpečenstiev:

a) opis a odôvodnenie (vrátane obmedzení) metód a nástrojov na identifikáciu nebezpečenstiev (metóda zhora nadol, zdola nahor, HAZOP atď.);
b) výsledky:

(1) zoznam nebezpečenstiev,
(2) systémové (hraničné) nebezpečenstvá,
(3) nebezpečenstvá subsystémov,
(4) nebezpečenstvá rozhraní,
(5) bezpečnostné opatrenia, ktoré bude možné identifikovať počas tejto fázy.

A.4.6. Aj tieto dôkazy je potrebné zabezpečiť vo fáze analýzy rizík:

a) keď sa na kontrolovanie nebezpečenstiev používajú kódexy postupov, preukázanie, že posudzovaný systém spĺňa všetky relevantné požiadavky kódexov postupov. Súčasťou toho je preukázanie správneho uplatnenia príslušných kódexov postupov;

b) keď sa na kontrolovanie nebezpečenstiev používajú podobné referenčné systémy:

(1) vymedzenie požiadaviek na bezpečnosť relevantných referenčných systémov kladených na posudzovaný systém;
(2) preukázanie, že sa posudzovaný systém používa v podobných prevádzkových a environmentálnych podmienkach ako relevantný referenčný systém. Ak to nemožno preukázať, preukázanie správnosti posúdenia odchýlok od referenčného systému;
(3) dôkaz o správnosti implementácie požiadaviek na bezpečnosť referenčného systému v posudzovanom systéme;

c) keď sa na kontrolovanie nebezpečenstiev používa explicitný odhad rizík:

(1) opis a odôvodnenie (vrátane obmedzení) metódy a nástrojov na analýzu rizík (kvalitatívnych, kvantitatívnych, semikvantitatívnych, neregresnej analýzy…);
(2) identifikáciu existujúcich bezpečnostných opatrení a faktorov, ktoré znižujú riziká každého nebezpečenstva (vrátane stránok ľudského činiteľa);

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(3) hodnotenie a hierarchiu rizík každého nebezpečenstva:

(i) odhad dôsledkov nebezpečenstva a odôvodnenie (s predpokladmi a podmienkami);
(ii) odhad početnosti nebezpečenstva a odôvodnenie (s predpokladmi a podmienkami);
(iii) hierarchiu nebezpečenstiev podľa ich závažnosti a početnosti výskytu;

(4) identifikácia ďalších primeraných bezpečnostných opatrení, ktoré povedú k prijateľným rizikám každého nebezpečenstva (iteračný proces po fáze vyhodnotenia rizík).

A.4.7. Dôkazy vyžadované ako výstup z vyhodnotenia rizík:

a) keď sa riziká odhadujú explicitne:

(1) vymedzenie a odôvodnenie kritérií hodnotenia za každé nebezpečenstvo;
(2) preukázanie/odôvodnenie, že bezpečnostné opatrenia a požiadavky na bezpečnosť pokrývajú každé nebezpečenstvo na prijateľnej úrovni (podľa uvedeného kritéria hodnotenia rizík);

b) podľa častí 2.3.5 a 2.4.3 v nariadení o CSM sa riziká, na ktoré sa vzťahuje uplatňovanie kódexov postupov a porovnanie s referenčnými systémami, považujú implicitne za prijateľné, ak sú splnené (pozri bodkovanú kružnicu na Obr. 1):

(1) podmienky uplatňovania kódexov postupov uvedené v časti 2.3.2;
(2) podmienky uplatňovania referenčného systému uvedené v časti 2.4.2.

Kritériá akceptovania rizika sú pri týchto dvoch zásadách akceptovania rizika implicitné.

A.4.8. Dôkazy o riadení nebezpečenstiev:

a) zápis všetkých nebezpečenstiev v zázname o nebezpečenstve, ktorý obsahuje tieto položky:

(1) identifikáciu nebezpečenstva,
(2) bezpečnostné opatrenia, ktoré bránia vzniku nebezpečenstva alebo zmierňujú jeho dôsledky,
(3) požiadavky na bezpečnostné opatrenia,
(4) príslušnú časť systému,
(5) aktéra zodpovedného za bezpečnostné opatrenia,
(6) stav nebezpečenstva (napr. otvorené, vyriešené, vymazané, presunuté, kontrolované atď.),
(7) dátum zápisu, revízie, kontroly každého nebezpečenstva;

b) opis spôsobu efektívneho riadenia nebezpečenstiev počas celého životného cyklu;
c) opis výmeny informácií o nebezpečenstvách medzi stranami na rozhraniach a pridelenie zodpovednosti.

A.4.9. Dôkazy o kvalite procesu hodnotenia a posudzovania rizík:

a) opis osôb, ktoré sa na procese zúčastňujú a ich spôsobilosti;
b) pri explicitných odhadoch rizík opis informácií, štatistických a iných údajov použitých v procese a odôvodnenie ich vhodnosti (napr. štúdiou citlivosti použitých údajov).

A.4.10. Dôkazy o splnení požiadaviek na bezpečnosť:

a) zoznam použitých noriem;
b) opis návrhu a zásad prevádzky;
c) dôkazy o uplatňovaní systému riadenia kvality a systému riadenia bezpečnosti v projekte: pozri odsek [G 3] v časti 1.1.2;

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

d) zhrnutie správ o bezpečnostnej analýze (napr. analýza príčin nebezpečenstiev) preukazujúce splnenie požiadaviek na bezpečnosť;
e) opis a odôvodnenie metód a nástrojov (FMECA, FTA…), ktoré boli použité na analýzu príčin nebezpečenstiev;
f) zhrnutie testov verifikácie a validácie bezpečnosti.

A.4.11. Bezpečnostný preukaz: CENELEC upozorňuje, že všetky predošle uvedené dôkazy sú znovu zoradené a zhrnuté v jednom dokumente, ktorý sa predkladá orgánu pre posudzovanie: pozri odseky [G 3] a [G 5] v časti 5.1.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

DODATOK B: PRÍKLADY TECHNÍK A NÁSTROJOV NA PODPORU PROCESU POSUDZOVANIA RIZÍK

B.1. Príklady techník a nástrojov na vykonanie činností posudzovania rizík metódou CSM je možné nájsť v prílohe E k príručke EN 50126-2 {Ref. 9}. Prehľad techník a nástrojov je uvedený v tabuľke E.1. Každá technika je opísaná a podľa potreby je uvedený odkaz na viac informácií v ďalších normách.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

DODATOK C: PRÍKLADY

C.1. Úvod

C.1.1. Účelom tohto dodatku je uľahčiť čítanie tohto dokumentu. Sú v ňom uvedené všetky zozbierané príklady, ktorých cieľom je uľahčiť uplatňovanie CSM.

C.1.2. Príklady posudzovania rizík alebo bezpečnosti, ktoré sú uvedené v tomto dodatku, nie sú výsledkom uplatňovania postupu podľa CSM, pretože boli vykonané pred existenciou nariadenia o CSM. Príklady je možné roztriediť takto:

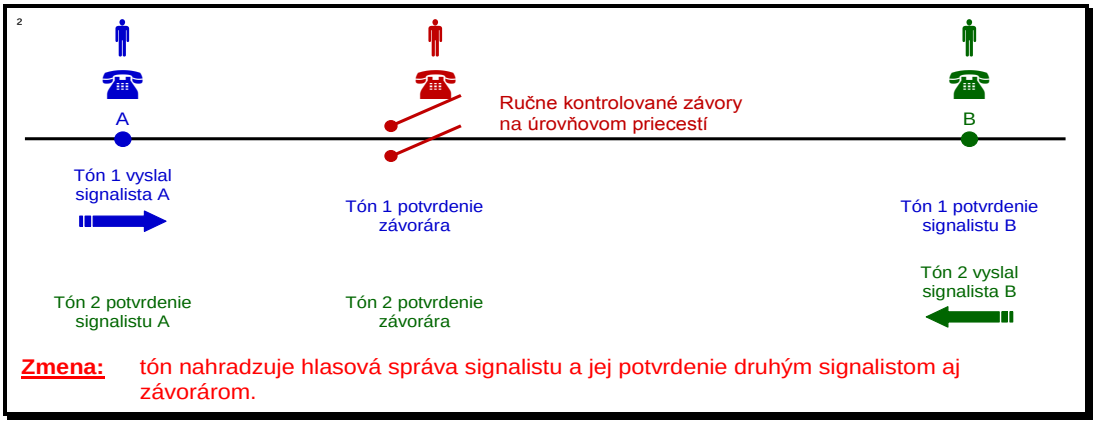
a) príklady s odkazom na ich pôvod, prevzaté od odborníkov pracovnej skupiny pre CSM,
b) ďalšie príklady prevzaté od odborníkov pracovnej skupiny pre CSM, úmyselne uvedené bez odkazu na ich pôvod. Príslušní odborníci žiadali, aby pôvod zostal dôverný;
c) príklady, ktorých pôvod nie je uvedený a ktoré poskytli zamestnanci agentúry na základe svojej predchádzajúcej odbornej praxe.

Pri každom príklade je možné sledovať vývoj medzi uplatneným procesom a postupom vyžadovaným v nariadení o CSM, ako aj zdôvodnenie a pridaná hodnota vykonania (prípadných) ďalších krokov, ktoré vyžaduje CSM.

C.2. Príklady uplatnenia kritérií významnej zmeny podľa Článok 4 ods. 2

C.2.1. Agentúra pracuje na vymedzení pojmu „významnej zmeny“. V tejto časti je z tejto práce uvedený príklad uplatnenia kritérií podľa Článok 4 ods. 2.

C.2.2. Zmena spočíva v úprave spôsobu, akým signalisti informujú závorára o smerovaní vlaku prichádzajúceho na ručne riadenú úrovňovú križovatku. Zmena je znázornená na Obr. 15.



Obr. 15: Príklad nevýznamnej zmeny: telefonická správa pre riadenie úrovňovej križovatky.

C.2.3. Existujúci systém: pred zavedením zamýšľanej zmeny dostával závorár informáciu o smerovaní vlaku prichádzajúceho na ručne riadenú úrovňovú križovatku automaticky zvonením telefónu. Tón zvonenia sa líšil podľa toho, odkiaľ prichádzal hovor.

C.2.4. Zamýšľaná zmena: keďže pôvodný telefonický systém zastaral a musí sa nahradiť novým, digitálnym, príslušnú informáciu už technicky nie je možné vložiť do tónu zvonenia. Tón je

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

úplne rovnaký bez ohľadu na to, od ktorého signalistu prichádza. Preto bolo rozhodnuté dosiahnuť rovnakú funkciu prevádzkovým postupom:

a) po odchode vlaku signalista verbálne informuje závorára o smere prichádzajúceho vlaku;
b) informácia sa kontroluje podľa cestovného poriadku a potvrdzujú ju obaja, závorár aj druhý signalista, aby sa vylúčilo nesprávne pochopenie na strane závorára.

Zamýšľanú zmenu a s ňou spojený prevádzkový postup ilustruje Obr. 15.

C.2.5. Hoci zmena zdanlivo bude mať potenciál vplyvu na bezpečnosť (riziko nespustenia závor včas), iné kritériá uvedené v Článok 4 ods. 2 ako:

a) nízka zložitosť;
b) chýbajúca inovácia;
c) ľahké monitorovanie;

pravdepodobne nasvedčujú, že zamýšľaná zmena nie je významná.

C.2.6. V tomto príklade je v každom prípade potrebná istá analýza bezpečnosti alebo argument, ktorými sa preukáže, že táto z hľadiska bezpečnosti rozhodujúca úloha nahradenia starého technického systému prevádzkovým postupom (vzájomnej krížovej kontroly zamestnancov) bude mať podobnú úroveň bezpečnosti. Otázkou zostáva, či na to bude žiaduce uplatnenie procesu CSM v plnom rozsahu, so záznamom o nebezpečenstve, nezávislým posúdením orgánu pre posudzovanie atď. V tomto prípade je otázne, či to prinesie nejakú pridanú hodnotu za predpokladu, že takáto zmena by nemohla byť potom kvalifikovaná ako významná.

C.3. Príklady rozhraní medzi aktérmi železničného sektora

C.3.1. Toto sú niektoré príklady rozhraní a dôvodov spolupráce medzi dvoma aktérmi železničného sektora:

a) MI – MI: napr. na oboch infraštruktúrach treba navrhnúť bezpečnostné opatrenia na zaistenie bezpečného prechodu vlaku z jednej infraštruktúry na druhú;
b) MI – ŽP: napr. môžu existovať konkrétne prevádzkové predpisy podmienené infraštruktúrou, ktoré musí dodržiavať vodič;
c) MI – výrobca: napr. subsystémy výrobcu by mohli mať obmedzenia používania, ktoré musí dodržiavať MI;
d) MI – poskytovateľ služieb: napr. konkrétne obmedzenia týkajúce sa údržby infraštruktúry, ktoré musí dodržiavať subdodávateľ činností údržby;
e) ŽP – výrobca: napr. subsystémy výrobcu by mohli mať obmedzenia používania, ktoré musí dodržiavať ŽP;
f) ŽP – poskytovateľ služieb: napr. keď konkrétne obmedzenia týkajúce sa údržby infraštruktúry musí dodržiavať subdodávateľ činností údržby;
g) ŽP – držitelia: napr. keď konkrétne obmedzenia používania vozidiel musí dodržiavať železničný podnik, ktorý ich prevádzkuje;
h) výrobca – výrobca: napr. riadenie technických rozhraní súvisiacich s bezpečnosťou medzi subsystémami dvoch rôznych výrobcov;
i) výrobca – poskytovateľ služieb: napr. vedenie záznamu o nebezpečenstve výrobcom, keď určité práce objednáva v subdodávke od podniku, ktorý je príliš malý na to, aby mohol organizovať bezpečnosť posudzovaného projektu;
j) poskytovateľ služieb – poskytovateľ služieb: podobný príklad ako v písmene j).

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

C.3.2. Poskytovatelia služieb vykonávajú všetky činnosti, napr. údržby, predaja cestovných lístkov, inžinierskych služieb, v subdodávkach buď pre MI alebo ŽP, alebo výrobcu.

C.3.3. Riadenie rozhraní a identifikáciu súvisiacich nebezpečenstiev ilustruje tento príklad: Predpokladá sa rozhranie medzi výrobcom vlakov a navrhovateľom (ŽP). Opisuje potom spôsob splnenia kritérií uvedených v odseku [G 3] v časti 1.2.1:

a) vedenie: navrhovateľ (ŽP),

b) vstupy:

(1) zoznam(y) príslušných nebezpečenstiev prevzaté z podobných projektov,
(2) opis všetkých vstupov a výstupov (I/O) rozhrania vrátane charakteristík výkonnosti;

c) metódy: pozri dodatok A.2 k usmerneniu EN 50 126-2 {Ref. 9};

d) požadovaní účastníci:

(1) manažér zaisťovania bezpečnosti navrhovateľa (ŽP),
(1) manažér zaisťovania bezpečnosti výrobcu vlakov,
(2) projektový orgán navrhovateľa,
(3) vývojový ústav výrobcu vlakov,
(4) personál údržby navrhovateľa (čiastočne v závislosti od analyzovaných I/O),
(5) vodiči (čiastočne v závislosti od analyzovaných I/O);

e) výstupy:

(1) spoločne dohodnutá správa o identifikácii nebezpečenstiev,
(2) bezpečnostné opatrenia pre záznam o nebezpečenstve s jednoznačným opisom zodpovednosti.

C.4. Príklady metód určovania všeobecne prijateľných rizík

C.4.1. Úvod

C.4.1.1. Všeobecne prijateľné riziká sú v nariadení o CSM definované ako riziká, ktoré sú *„také malé, že nie je dôvod implementovať akékoľvek dodatočné bezpečnostné opatrenie (na ďalšie zníženie rizika)“*. Pri identifikácii nebezpečenstiev, klasifikovanie niektorých nebezpečenstiev ako spojených so všeobecne prijateľnými rizikami umožňuje upustiť od ďalšieho analyzovania týchto nebezpečenstiev v procese posudzovania rizík. Citované vymedzenie všeobecne prijateľných rizík ponecháva určitý priestor na výklad. Preto je v nariadení uvedené, že rozhodnutie o klasifikovaní nebezpečenstiev so všeobecne prijateľným rizikom sa ponecháva na odborný posudok.

C.4.1.2. V skutočnosti je ťažké vymedziť zvyčajne explicitnejšie kritérium všeobecne prijateľného rizika, ktoré by platilo pre všetky rôzne možné systémové úrovne, na ktorých sa pravdepodobne takéto nebezpečenstvá zistia a ktoré pravdepodobne vyvolajú rôzne faktory neochoty prijať riziko v rôznych aplikáciách. Keďže však je dôležité zaistiť, aby posudky odborníkov boli správne pochopené a reprodukovateľné, je užitočné určité usmernenie týkajúce sa vymedzovania rizík ako všeobecne prijateľných. Kritériá na vymedzenie všeobecne prijateľných rizík môžu byť kvantitatívne, kvalitatívne a semikvalitatívne. Niekoľko príkladov odvodenia kritérií, ktoré umožnia kvantitatívne alebo semikvantitatívne vyhodnotenie všeobecne prijateľných rizík, je uvedených ďalej.

C.4.1.3. Túto zásadu ilustrujú ďalej uvedené príklady. Sú prevzaté z článku: *„Die Gefährdungseinstufung im ERA-Risikomanagementprozess“, Kurz, Milius, Signal + Draht (100) 9/2008.*

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

C.4.2. Odvodenie kvantitatívneho kritéria

C.4.2.1. Všeobecne prijateľné riziká je možné vymedziť ako riziká, ktoré sú oveľa menšie než prijateľné riziko danej triedy nebezpečenstva. S využitím štatistických údajov je pravdepodobne možné vypočítať súčasnú úroveň rizika železničných systémov, a potom vyhlásiť vypočítanú úroveň za prijateľnú. Vydelením úrovne rizika počtom nebezpečenstiev (N) (napr. je v železničnom systéme možné zvoliť N = 100 hlavných kategórií nebezpečenstiev), dostaneme prijateľnú úroveň rizika pripadajúcu na jednu kategóriu nebezpečenstva. Potom je možné konštatovať, že nebezpečenstvo s rizikom, ktoré je rádovo dvojnásobne nižšie ako prijateľná úroveň rizika na jedno nebezpečenstvo (je to parameter x % uvedený v odseku [G 1] v časti 2.2.3), sa dá považovať za všeobecne prijateľné riziko.

C.4.2.2. Preveriť však treba, či príspevok všetkých nebezpečenstiev spojených so všeobecne prijateľným rizikom neprevyšuje daný podiel (napr. y %) na celkovom riziku na úrovni systému: pozri časť 2.2.3 a vysvetlenie v odseku [G 2] v časti 2.2.3.

C.4.3. Hodnotenie všeobecne prijateľných rizík

C.4.3.1. Medzné hodnoty všeobecne prijateľných rizík, odvodené v uvedených príkladoch, je potom možné použiť na kalibrovanie kvalitatívnych nástrojov, ako sú matica rizík, graf rizík alebo čísla priority rizík, ktoré odborníkom pomôžu pri rozhodovaní o klasifikácii rizika ako všeobecne prijateľného. Dôležité je zdôrazniť, že kvantitatívne hodnoty ako kritériá na hodnotenie všeobecne prijateľných rizík ešte neznamenajú potrebu presného odhadu rizík alebo analýzy, ktorej cieľom je rozhodnúť o všeobecnej prijateľnosti daného rizika. Tu je rozhodujúci posudok odborníka, ktorý vo fáze identifikácie nebezpečenstiev robí približný (hrubý) odhad.

C.4.3.2. Je tiež dôležité preveriť, či príspevok všetkých nebezpečenstiev spojených so všeobecne prijateľným rizikom neprevyšuje daný podiel (napr. y %) na celkovom riziku na úrovni systému: pozri časť 2.2.3 a vysvetlenie v odseku [G 2] v časti 2.2.3.

C.5. Príklad posúdenia rizík významnej organizačnej zmeny

C.5.1. **Poznámka:** Tento príklad nie je uvedený ako výsledok uplatňovania procesu CSM; realizoval sa pred existenciou CSM. Účelom tohto príkladu je:

a) zistiť podobnosť medzi existujúcimi metódami posudzovania rizík a procesom CSM;
b) ilustrovať sledovateľnosť medzi krokmi existujúceho procesu a procesu, ktorý si vyžaduje CSM;
c) zdôvodniť pridanú hodnotu prípadných ďalších krokov, ktoré si vyžaduje CSM.

Zdôrazňujeme, že tento príklad je uvedený len na informáciu. Jeho účelom je pomôcť čitateľovi pochopiť proces CSM. Príklad sám sa však nesmie transponovať ani použiť ako referenčný systém pre inú významnú zmenu. Posúdenie rizík sa pre každú významnú zmenu musí robiť v súlade s nariadením o CSM.

C.5.2. Tento príklad sa týka organizačnej zmeny. Príslušný navrhovateľ ju považoval za významnú. Na hodnotenie zmeny bol použitý prístup vychádzajúci z posúdenia rizík.

C.5.3. Pobočka organizácie manažéra infraštruktúry, ktorá do zmeny vykonávala niektoré činnosti údržby (iné ako signalizačné a telematické), musela vstúpiť do súťaže s inými podnikmi pôsobiacimi v tejto oblasti. Priamym dôsledkom bola potreba znížiť počet pracovníkov a

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

prerozdeliť pracovníkov a úlohy samostatnej pobočky v organizácii MI, ktorá vstúpila do súťaže.

C.5.4. Problémy dotknutého manažéra infraštruktúry:

a) zamestnanci MI, ktorých sa zmena dotkla, vykonávali núdzovú údržbu a núdzové opravy, ktorými sa odstraňovali nepredvídateľné poruchy infraštruktúry. Títo zamestnanci vykonávali aj niektoré plánované alebo projektom stanovené činnosti údržby, napr. podbíjanie trate, čistenie koľajového ložiska, úprava vegetácie;
b) tieto úlohy sa považovali za rozhodujúce z hľadiska bezpečnosti a presnosti prevádzky. Museli sa preto analyzovať s cieľom nájsť správne opatrenia, ktoré zaistia, aby sa situácia nezhoršila, keď organizáciu MI opustí veľa osôb zodpovedajúcich za záležitosti bezpečnosti.
c) potrebné bolo zachovať rovnakú úroveň bezpečnosti a presnosť vlakov počas zmeny organizácie aj po nej.

C.5.5. V porovnaní s procesom CSM sa uplatnili tieto kroky (pozri aj Obr. 1):

a) opis systému [časť 2.1.2]:

(1) opis úloh, ktoré plnila existujúca organizácia (t. j. organizácia MI pred zmenou),
(2) opis zmien plánovaných v organizácii MI,
(3) rozhrania „pobočky, ktorá sa mala osamostatniť“ s ostatnými okolitými organizáciami alebo s fyzickým prostredím bolo možné opísať len stručne. Hranice nebolo možné vyjadriť s presnosťou 100 %;

b) identifikácia nebezpečenstiev [časť 2.2]:

(1) brainstormig skupiny odborníkov na:

(i) zistenie všetkých nebezpečenstiev s príslušným vplyvom na riziko, ktoré prinesie zamýšľaná organizačná zmena,
(ii) určenie možných opatrení na zníženie rizika;

(2) klasifikácia nebezpečenstiev:

(i) ako funkcie závažnosti súvisiaceho rizika: vysoké, stredné, nízke riziko;
(ii) ako funkcie vplyvu zmeny: zvýšené, nezmenené, znížené riziko;

c) použitie referenčného systému [časť 2.4]:

Systém pred zmenou bol posudzovaný ako systém s prijateľnou úrovňou bezpečnosti. Použil sa preto ako „referenčný systém“ na odvodenie kritérií akceptovania rizika (RAC) organizačnej zmeny;

d) explicitný odhad a hodnotenie rizika [časť 2.5]:

Pre každé nebezpečenstvo so zvýšeným rizikom z dôvodu organizačnej zmeny sú určené opatrenia na zníženie rizika. Zostatkové riziko sa porovnáva s RAC referenčného systému na kontrolu, či je potrebné identifikovať ďalšie opatrenia;

e) preukázanie súladu systému s požiadavkami na bezpečnosť [časť 3]:

(1) analýza rizík a záznamy o nebezpečenstve ukázali, že nebezpečenstvá nie je možné kontrolovať, pokiaľ sa neoveria a nepreukáže sa, že požiadavky na bezpečnosť (resp. vybrané bezpečnostné opatrenia) boli splnené;
(2) analýza rizík a záznamy o nebezpečenstve boli živými dokumentmi. Účinnosť opatrení, o ktorých sa rozhodlo, sa sledovala v pravidelných intervaloch, aby sa zistilo, či sa zmenili podmienky a či nie je potrebné aktualizovať analýzu a hodnotenie rizík;
(3) ak by zavedené opatrenia neboli dosť účinné, aktualizovala by sa analýza rizík, hodnotenie rizík a záznam o nebezpečenstve a znovu by sa sledovali účinky;

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

f) riadenie nebezpečenstiev [časť 4.1]:

Zistené nebezpečenstvá a bezpečnostné opatrenia boli zapísané a vedené v zázname o nebezpečenstve. Jedným zo záverov príkladu bola priebežná aktualizácia analýzy rizík a záznamu o nebezpečenstve s prijímaním rozhodnutí a opatrení počas zmeny organizácie. Analýza rizík sa v tomto príklade vzťahovala aj na riziká na rozhraniach so subdodávateľmi a podnikateľmi.

Štruktúra a polia použitého záznamu o nebezpečenstve, ako aj výňatok niektorých položiek sú uvedené v časti C.16.2. dodatku C.

g) nezávislé posúdenie [Článok 6]:

Tretia strana vykonala aj nezávislé posúdenie, ktorého cieľom bolo:

(1) preskúmať správnosť riadenia rizík a posúdenia rizík,
(2) preskúmať, či je organizačná zmena vhodná a či umožní zachovať rovnakú úroveň bezpečnosti ako pred zmenou.

C.5.6. Na príklade vidieť, že zásady, ktoré vyžaduje spoločná bezpečnostná metóda, sú existujúce metódy, ktoré sa v železničnom sektore už uplatňujú na posudzovanie rizík organizačných zmien. Posúdenie rizík v tomto príklade spĺňa všetky požiadavky CSM. Využíva dve zo zásad akceptovania rizika, ktoré sú umožnené harmonizovaným prístupom CSM:

a) „referenčný systém“ sa uplatňuje na určenie kritérií akceptovania rizika potrebných na vyhodnotenie akceptovania rizika organizačnej zmeny;
b) „explicitný odhad a hodnotenie rizík“:

(1) na analýzu odchýlok zmeny od referenčného systému,
(2) na určenie opatrení, ktorými sa zníži riziko zvýšené v dôsledku zmeny,
(3) na vyhodnotenie či sa dosiahla prijateľná úroveň.

C.6. Príklad posúdenia rizík významnej prevádzkovej zmeny – zmeny pracovného času vodičov

C.6.1. **Poznámka:** Tento príklad nie je uvedený ako výsledok uplatňovania procesu CSM; realizoval sa pred existenciou CSM. Účelom tohto príkladu je:

c) a) zistiť podobnosť medzi existujúcimi metódami posudzovania rizík a procesom CSM;
d) b) ilustrovať sledovateľnosť medzi krokmi existujúceho procesu a procesu, ktorý si vyžaduje CSM;
e) zdôvodniť pridanú hodnotu prípadných ďalších krokov, ktoré si vyžaduje CSM.

Zdôrazňujeme, že tento príklad je uvedený len na informáciu. Jeho účelom je pomôcť čitateľovi pochopiť proces CSM. Príklad sám sa však nesmie transponovať ani použiť ako referenčný systém pre inú významnú zmenu. Posúdenie rizík sa pre každú významnú zmenu musí robiť v súlade s nariadením o CSM.

C.6.2. Príklad je prevádzkovou zmenou, ktorou chcel železničný podnik prideliť vodičom nové trasy a potenciálne nový pracovný čas (vrátane rotácie a zmennosti).

C.6.3. V porovnaní s procesom CSM sa uplatnili tieto kroky (pozri aj Obr. 1):

a) významnosť zmeny [Článok 4]:

Železničný podnik vykonal predbežné posúdenie rizík, na základe ktorého dospel k záveru, že prevádzková zmena je významná. Keďže vodiči mali pracovať na nových

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

trasách a možno mimo svojho obvyklého pracovného času, nebolo možné zanedbať možnosť prehliadnutia signalizácie nebezpečenstva, prekročenia dovolenej rýchlosti alebo ignorovania dočasného obmedzenia rýchlosti.

Pri porovnaní tohto predbežného posúdenia rizík s kritériami podľa Článok 4 ods. 2 nariadenia o CSM, zmenu by bolo možné zaradiť ako významnú na základe týchto kritérií:

(1) význam z hľadiska bezpečnosti: zmena súvisí s bezpečnosťou, pretože vplyv zmeny spôsobu práce vodiča by mohol byť katastrofický;
(2) dôsledok poruchy: uvedené chyby vodiča majú potenciál viesť ku katastrofickým dôsledkom;
(3) inovatívnosť: potenciálne by ŽP mohol zaviesť nové spôsoby práce vodičov;
(4) zložitosť zmeny: zmena pracovného času vodičov by mohla byť zložitá, pretože by si mohla vyžiadať úplné posúdenie a zmenu existujúcich pracovných podmienok;

b) vymedzenie systému [časť 2.1.2]:

Vymedzenie systému opísané na začiatku:

(1) existujúce pracovné podmienky: pracovný čas, zmennosť atď;
(2) zmeny pracovného času;
(3) otázky rozhraní (napr. s manažérom infraštruktúry).

Rôznymi iteráciami sa vymedzenie systému aktualizovalo so zreteľom na požiadavky na bezpečnosť, ktoré vyplynuli s procesu posúdenia rizík. Do tohto iteratívneho procesu identifikácie nebezpečenstiev a aktualizácie vymedzenia systému boli zapojení kľúčoví predstavitelia zamestnancov.

c) identifikácia nebezpečenstiev [časť 2.2]:

Brainstormingom skupiny odborníkov, v ktorej boli aj predstavitelia vodičov, sa pre nové trasy a nový rozvrh zmien identifikovali nebezpečenstvá a možné bezpečnostné opatrenia. Preskúmali sa úlohy vodičov v nových podmienkach, aby sa dalo posúdiť, či ovplyvnia vodičov, ich pracovné zaťaženie, zemepisný rozsah pôsobnosti a čas systému pracovných zmien.
ŽP konzultoval aj s odborovou organizáciou, či nemôže poskytnúť ďalšie informácie a skúmal riziko únavy a úroveň chorobnosti, ktorú by mohol vyvolať možný nárast nadčasov z dôvodov predĺžených ciest po neznámych trasách.
Každému nebezpečenstvu bola priradená úroveň závažnosti rizika a dôsledkov (vysoká, stredná, nízka) a vplyv navrhovanej zmeny sa skúmal vzhľadom na ne (zvýšené, nezmenené, znížené riziko).

d) použitie kódexov postupov [časť 2.3]:

Na revíziu existujúcich pracovných podmienok a určenie nových požiadaviek na bezpečnosť sa použili kódexy postupov súvisiace s pracovným časom a ľudskou únavou. Podľa kódexov postupov sa napísali prevádzkové predpisy potrebné pre nový systém práce na zmeny. Na revízii prevádzkových postupov a dohode o pokračovaní na zmene sa zúčastnili všetky zainteresované strany.

e) preukázanie súladu systému s požiadavkami na bezpečnosť [časť 3]:

Do systému riadenia bezpečnosti ŽP sa zaviedli revidované prevádzkové postupy. Monitorovali sa a zaviedol sa proces kontroly, ktorým sa zaistilo správne kontrolovanie zistených nebezpečenstiev počas prevádzky železničného systému.

f) riadenie nebezpečenstiev [časť 4.1]:

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Pozri už uvedené o procese riadenia nebezpečenstiev v železničných podnikoch, ktorý môže byť časťou ich systému riadenia bezpečnosti na zaznamenávanie a riadenie rizík. Zistené nebezpečenstvá boli zapísané do záznamu o nebezpečenstve spolu s požiadavkami na bezpečnosť (t. j. s odkazom na revidované prevádzkové postupy) znižujúce súvisiace riziko.
Revidované postupy sa monitorovali a podľa potreby revidovali, aby sa zaistilo správne kontrolovanie zistených nebezpečenstiev počas prevádzky železničného systému.

g) nezávislé posúdenie [Článok 6]:

Posúdenie rizík a proces riadenia rizík posúdila odborne spôsobilá osoba v rámci železničného podniku, ktorá bola nezávislá od procesu posudzovania. Odborne spôsobilá osoba posúdila proces aj výsledky, t. j. zistené požiadavky na bezpečnosť.

ŽP založil svoje rozhodnutie o zavedení nového systému na správe o nezávislom posúdení, ktorú vypracovala táto odborne spôsobilá osoba.

C.6.4. Na príklade vidieť, že zásady a postupy uplatnené v železničnom podniku sú v súlade so spoločnou bezpečnostnou metódou. Riadenie rizík a proces posúdenia rizík splnil všetky požiadavky CSM.

C.7. Príklad posúdenia rizík významnej technickej zmeny (CCS)

C.7.1. **Poznámka:** Tento príklad nie je uvedený ako výsledok uplatňovania procesu CSM; realizoval sa pred existenciou CSM. Účelom tohto príkladu je:

h) a) zistiť podobnosť medzi existujúcimi metódami posudzovania rizík a procesom CSM;
i) b) ilustrovať sledovateľnosť medzi krokmi existujúceho procesu a procesu, ktorý si vyžaduje CSM;
j) c) zdôvodniť pridanú hodnotu prípadných ďalších krokov, ktoré si vyžaduje CSM.

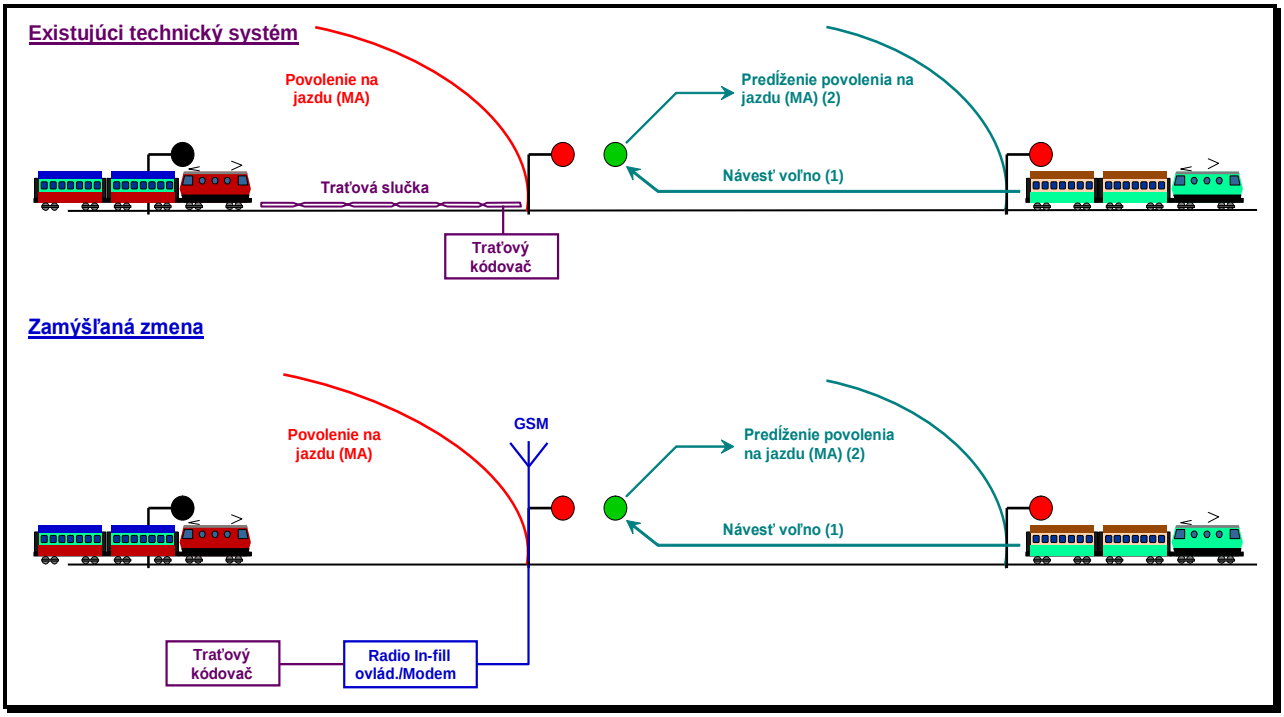
Zdôrazňujeme, že tento príklad je uvedený len na informáciu. Jeho účelom je pomôcť čitateľovi pochopiť proces CSM. Príklad sám sa však nesmie transponovať ani použiť ako referenčný systém pre inú významnú zmenu. Posúdenie rizík sa pre každú významnú zmenu musí robiť v súlade s nariadením o CSM.

C.7.2. Príklad sa týka technickej zmeny systému riadenia a zabezpečenia vlakov. Príslušný výrobca ju považoval za významnú. Na hodnotenie zmeny bol použitý prístup vychádzajúci z posúdenia rizík.

C.7.3. Opis zmeny: zmena pozostáva z nahradenia traťovej slučky umiestnenej pred návesťou subsystémom „radio in-fill + GSM“ (pozri Obr. 16).

C.7.4. Problém: zachovanie úrovne bezpečnosti systému po zmene.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu



Obr. 16: Výmena traťovej slučky za subsystém „radio in-fill“.

C.7.5. V porovnaní s procesom CSM sa uplatňujú tieto kroky (pozri aj Obr. 1):

a) posúdenie významnosti zmeny [Článok 4]:

Na posúdenie významnosti zmeny sa použijú kritériá uvedené v Článok 4 ods. 2. Pri rozhodovaní o významnosti zmeny sa prihliadalo hlavne na zložitosť a inovatívnosť.

b) opis systému [časť 2.1.2]:

(1) opis existujúceho systému: slučka a jej funkcie v systéme signalizácie, riadenia a zabezpečenia vlakov,
(2) opis zmeny, ktorú plánujú navrhovateľ a výrobca,
(3) opis funkčných a fyzických rozhraní medzi slučkou a ostatným systémom.

Funkcia „slučka+kódovacie zariadenie“ v existujúcom systéme slúži na vydanie signálu pre príjazd vlaku, keď úsek za návesťou (t. j. pred blížiacim sa vlakom) už nie je obsadený: pozri Obr. 16.

c) identifikácia nebezpečenstiev [časť 2.2]:

Na základe brainstormingu skupiny odborníkov sa uplatní iteratívny proces posudzovania rizík a identifikácie nebezpečenstiev (pozri časť 2.1.1), ktorého cieľom je:

(1) zistenie všetkých nebezpečenstiev s príslušným vplyvom na riziko, ktoré prinesie zamýšľaná zmena,
(2) určenie možných opatrení na kontrolovanie rizika.

Keď slučka, a teda rádio infill vydá signál, je riziko vydania nebezpečného povolenia jazdy blížiacemu sa vlaku, kým ešte predchádzajúci vlak stále obsadzuje úsek pred návesťou. Toto riziko sa musí znížiť na prijateľnú úroveň.

d) použitie referenčného systému [časť 2.4]:

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Systém pred zmenou (slučka) je posudzovaný ako systém s prijateľnou úrovňou bezpečnosti. Použije sa teda ako „referenčný systém“ na odvodenie požiadaviek na bezpečnosť pre subsystém rádio infill.

e) explicitný odhad a hodnotenie rizika [časť 2.5]:

(1) rozdiely medzi subsystémami „traťová slučka“ a „radio in-fill+GSM“ sa analyzujú na základe explicitného odhadu a hodnotenia rizík. Pri subsystéme „radio in-fill + GSM“ sa zistili tieto nové nebezpečenstvá:

(i) vyslanie nebezpečných informácií hackermi v prestávke prenosu, pretože „radio in-fill+GSM“ je otvorený prenosový subsystém,
(ii) oneskorený prenos alebo prenos zapamätaných paketov dát v prestávke prenosu,

(2) explicitný odhad rizík a použitie RAC-TS na časť ovládača Radio In-fill.

f) použitie kódexov postupov [časť 2.3]:

(1) v norme EN 50159-2 (*„Dráhové aplikácie. Komunikačné a signalizačné systémy a systémy na spracovanie údajov. Časť 2. Komunikácia súvisiaca s bezpečnosťou v otvorených prenosových systémoch“*) sú uvedené požiadavky na bezpečnosť na zníženie rizika nových nebezpečenstiev na prijateľnú úroveň, napr.:

(i) šifrovaním a ochranou údajov,
(ii) radením správ a časovými pečiatkami;

(2) použitie napr. normy EN 50 128 pri vývoji softvéru pre ovládač Radio Infill;

g) preukázanie súladu systému s požiadavkami na bezpečnosť [časť 3]:

(1) dosledovanie implementácie požiadaviek na bezpečnosť v procese vývoja subsystému „Radio In-fill + GSM“,
(2) overenie, že navrhnutý a nainštalovaný systém spĺňa požiadavky na bezpečnosť;

h) riadenie nebezpečenstiev [časť 4.1]:

Zistené nebezpečenstvá, bezpečnostné opatrenia a výsledné požiadavky na bezpečnosť, ktoré vyplynuli z posúdenia rizík a aplikácia troch zásad akceptovania rizika sú zapísané a evidované v zázname o nebezpečenstve.

i) nezávislé posúdenie [Článok 6]:

Tretia strana vykonala aj nezávislé posúdenie, ktorého cieľom je:

(1) preskúmať správnosť vykonaného riadenia rizík a posúdenia rizík,
(2) preskúmať, či je technická zmena vhodná a či umožňuje zachovať rovnakú úroveň bezpečnosti ako pred zmenou.

C.7.6. Na príklade vidieť, že tri zásady akceptovania rizika, ktoré vyžaduje spoločná bezpečnostná metóda, sú na vymedzenie požiadaviek na bezpečnosť, kladených na posudzovaný systém, použité komplementárne. Posúdenie rizík v tomto príklade spĺňa všetky požiadavky nariadenia o CSM zhrnuté na Obr. 1 vrátane vedenia záznamu o nebezpečenstve a nezávislého posúdenia bezpečnosti treťou stranou.

C.8. Príklad švédskeho usmernenia BVH 585.30 na posudzovanie rizík železničných tunelov

C.8.1. **Poznámka:** Tento príklad nie je uvedený ako výsledok uplatňovania procesu CSM; realizoval sa pred existenciou CSM. Účelom tohto príkladu je:

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

k) a) zistiť podobnosť medzi existujúcimi metódami posudzovania rizík a procesom CSM;
l) b) ilustrovať sledovateľnosť medzi krokmi existujúceho procesu a procesu, ktorý si vyžaduje CSM;
m) c) zdôvodniť pridanú hodnotu prípadných ďalších krokov, ktoré si vyžaduje CSM.

Zdôrazňujeme, že tento príklad je uvedený len na informáciu. Jeho účelom je pomôcť čitateľovi pochopiť proces CSM. Príklad sám sa však nesmie transponovať ani použiť ako referenčný systém pre inú významnú zmenu. Posúdenie rizík sa pre každú významnú zmenu musí robiť v súlade s nariadením o CSM.

C.8.2. Účelom tohto príkladu je porovnať proces podľa nariadenia o CSM s usmernením BVH 585.20, ktoré uplatňuje švédsky manažér infraštruktúry Banverket na návrh a overovanie dosiahnutej úrovne bezpečnosti pri projektovaní a výstavbe nových železničných tunelov. Spoločné znaky a rozdiely s metódou CSM sú uvedené ďalej; podrobné požiadavky na posúdenie rizík je možné nájsť v usmernení BVH 585.30.

C.8.3. V porovnaní s procesom CSM na Obr. 1:

a) Usmernenie BVH 585.30 má tieto spoločné znaky:

(1) opis systému [časť 2.1.2]:

Usmernenie vyžaduje podrobný opis systému, ktorý má obsahovať:

(i) opis tunela,
(ii) opis trate,
(iii) opis typu dráhových vozidiel (vrátane vlakového personálu),
(iv) opis premávky a plánovanej prevádzky,
(v) opis externej pomoci (vrátane záchranných služieb);

(2) identifikácia nebezpečenstiev [časť 2.2]:

Usmernenie výslovne nevyžaduje identifikáciu nebezpečenstiev. Vyžaduje identifikáciu rizík a „katalóg nehôd“ obsahujúci druhy zistených potenciálnych nehôd, ktoré sa považujú za významný vplyv na úroveň rizika tunela a ktoré sa nadväzne musia posúdiť. Príklady nehôd:

(i) „vykoľajenie osobného vlaku“,
(ii) „vykoľajenie nákladného vlaku“,
(iii) „nehoda súvisiaca s nebezpečným tovarom“,
(iv) „požiar vo vozidle“,
(v) „zrážka osobného vlaku s ľahkým/ťažkým objektom“,
(vi) atď;

(3) nie je ustanovené uplatnenie kódexov postupov ani podobných referenčných systémov. Predpokladá sa, že analýza rizík by sa mala vykonať v každom prípade;

(4) explicitný odhad a hodnotenie rizika [časť 2.5]:

(i) v usmernení sa všeobecne pre každý druh nehody odporúča vykonať úplnú analýzu možných porúch na základe kvantitatívnej analýzy rizík. Ale vzhľadom na to, že zámerom analýzy rizík je analýza celkovej úrovne bezpečnosti tunela a nie analýza bezpečnosti jednotlivo na podrobnejších úrovniach, výsledky všetkých scenárov sa pre tunel sčítajú do celkovej úrovne rizika;
(ii) prijateľnosť tejto celkovej úrovne rizika pre tunel sa musí porovnať s týmto explicitným kvantitatívnym kritériom akceptovania rizika: *„železničná premávka na kilometer tunela musí byť rovnako bezpečná ako železničná premávka na kilometer otvorenej trate s vylúčením úrovňových priecestí“.* Toto kritérium je transformované do krivky F-N vychádzajúcej z historických údajov

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

o železničných nehodách vo Švédsku a extrapolovanej tak, aby pokrývala dôsledky, o ktorých nie sú štatistické údaje;

(iii) popri tomto kritériu celkovej úrovne rizika tunela sú ešte ďalšie požiadavky, ktoré musia byť splnené najmä v súvislosti s evakuáciou tunela a možnosťami záchranných služieb:

- overenie, že v „najhoršom dôveryhodnom prípade“ požiaru vo vlaku (stanovené sú aj kritériá na jeho posúdenie) je možná sebazáchrana;
- tunel by mal byť vyprojektovaný tak, aby dovoľoval možné záchranné činnosti v danom súbore scenárov;

(5) výstup posúdenia rizík 2.1.6:

Výstupy posúdenia rizík sú:

(i) zoznam bezpečnostných opatrení minimálneho štandardu založeného na TSI–SRT a vnútroštátnych predpisoch uplatňovaných na návrh tunela a

(ii) všetky ďalšie bezpečnostné opatrenia, ktoré sa zistili pri analýze rizík ako potrebné aj s uvedením ich účelu. Je ustanovené, že o opatreniach by sa malo rozhodovať podľa tohto poradia dôležitosti:

- prevencia nehôd,
- zníženie dôsledkov nehôd,
- uľahčenie evakuácie,
- uľahčenie záchranných činností;

(6) riadenie nebezpečenstiev [časť 4.1]:

Usmernenie výslovne nevyžaduje vedenie záznamov o nebezpečenstve. Súvisí to so skutočnosťou, že úroveň posudzovania je všeobecná, a preto sa nebezpečenstvá jednotlivo nevyhodnocujú a nekontrolujú. Prijateľnosť celkového rizika tunela sa hodnotí, bez akéhokoľvek rozdeľovania kritéria akceptovania celkového rizika na rôzne druhy nehôd alebo nebezpečenstiev, ktoré sú ich príčinou.

Existuje však zoznam všetkých bezpečnostných opatrení, a to tak „minimálneho štandardu“, ako aj opatrení, ktoré boli pri analýze rizík identifikované ako potrebné: pozri pododsek a)(5)(ii). V zozname bezpečnostných opatrení by sa malo uvádzať, či sa týkajú tunelovej infraštruktúry, trate, prevádzky alebo dráhových vozidiel a tiež, aké sú ich zamýšľané účinky podľa výpočtu uvedeného v pododseku a)(5)(ii). Usmernenie ale nevyžaduje výslovne uviesť, ktoré nebezpečenstvá príslušné bezpečnostné opatrenie kontroluje ani kto zaň zodpovedá.

(7) nezávislé posúdenie [Článok 6]:

Nezávislé posúdenie treťou stranou je povinné a jeho cieľom je:

(i) preskúmať či bolo správne vykonané posúdenie rizík, odporúčané v usmernení BVH 585.30,

(ii) posúdiť prijateľnosť analýzy rizík,

(iii) preskúmať, či je v projekte zrozumiteľne uvedený spôsob, akým by sa malo vykonávať budúce riadenie bezpečnosti.

Záverečný dokument o analýze rizík podpisuje nezávislý posudzovateľ a koordinátor bezpečnosti daného projektu.

b) Usmernenie BVH 585.30 sa líši v týchto znakoch:

(1) preukázanie súladu systému s požiadavkami na bezpečnosť [časť 3]:

Usmernenie BVH 585.30 nevyžaduje sledovať implementáciu požiadaviek na bezpečnosť ani overovať, či konečný návrh tunela spĺňa stanovené požiadavky na

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

bezpečnosť. Iba opisuje, ako by sa táto požiadavka mala uplatniť, aby sa zaistila ich implementácia vo fáze výstavby.

V usmernení sú uvedené požiadavky na bezpečnosť, ktoré treba použiť na overenie, či analýza rizík bola vykonaná primeraným a transparentným spôsobom a či ju v projekte možno prijať.

C.8.4. Na záver, porovnanie s CSM ukazuje, že:

a) usmernenie BVH 585.30 spĺňa príslušné časti CSM, hoci ich rozsah pôsobnosti a účel nie sú zhodné;
b) usmernenie BVH 585.30 posudzuje celkovú úroveň rizika železničného tunela;
c) nebezpečenstvá nie sú kontrolované samostatne, a preto je menšie zameranie na riadenie nebezpečenstiev;
d) nie je výslovne ustanovené preukazovanie splnenia všetkých bezpečnostných opatrení a overovanie ich správnej implementácie. Usmernenie však ustanovuje, že úlohou bezpečnostného koordinátora projektu (BVH 585.30 stanovuje úlohu aj odbornú spôsobilosť) je overiť, že závery analýzy rizík sú zapracované v dokumentoch a výkresoch projektu a tiež kontrolovať, aby boli správne realizované vo fáze výstavby.

C.8.5. CSM je všeobecnejšia ako usmernenie BVH 585.30 v tom zmysle, že ponúka tri rôzne zásady akceptovania rizika. Uplatnenie BVH 585.30 však v rámci CSM nie je žiadnym problémom, pretože je zlučiteľné s použitím tretej zásady explicitného odhadovania rizík.

C.9. Príklad posúdenia rizika kodanského metra na úrovni systému

C.9.1. **Poznámka:** Tento príklad nie je uvedený ako výsledok uplatňovania procesu CSM; realizoval sa pred existenciou CSM. Účelom tohto príkladu je:

e) a) zistiť podobnosť medzi existujúcimi metódami posudzovania rizík a procesom CSM;
f) b) ilustrovať sledovateľnosť medzi krokmi existujúceho procesu a procesu, ktorý si vyžaduje CSM;
g) c) zdôvodniť pridanú hodnotu prípadných ďalších krokov, ktoré si vyžaduje CSM.

Zdôrazňujeme, že tento príklad je uvedený len na informáciu. Jeho účelom je pomôcť čitateľovi pochopiť proces CSM. Príklad sám sa však nesmie transponovať ani použiť ako referenčný systém pre inú významnú zmenu. Posúdenie rizík sa pre každú významnú zmenu musí robiť v súlade s nariadením o CSM.

C.9.2. Tento príklad sa týka úplného a komplexného automatizovaného systému metra vrátane technických subsystémov, z ktorých pozostáva (napr. automatického zabezpečenia vlaku a dráhových vozidiel), ako aj systému jeho prevádzky a údržby. Na vyhodnotenie systému a jeho základných subsystémov sa uplatnil prístup založený na posudzovaní rizík. Súčasťou projektu bolo aj osvedčovanie SMS podniku, ktorý mal systém prevádzkovať. Vzťahuje sa na schopnosť ŽP a MI bezpečne prevádzkovať a udržiavať systém počas celej životnosti systému.

C.9.3. V porovnaní s procesom CSM sa uplatnili tieto kroky (pozri aj Obr. 1):

a) opis systému [časť 2.1.2]:

(1) opis požiadaviek na výkonnosť systému,
(2) opis prevádzkových predpisov,
(3) zrozumiteľný opis rozhraní a zodpovednosti rôznych aktérov, najmä rozhraní medzi technickými subsystémami,

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(4) vymedzenie systémových požiadaviek vysokej úrovne (najmä pokiaľ ide o prijateľnú početnosť nehôd a vymedzenie oblasti ALARP),

b) identifikácia nebezpečenstiev [časť 2.2]:

(1) predbežná analýza systémovej úrovne nebezpečenstiev,
(2) funkčná analýza na úrovni systému so zvýraznením všetkých subsystémov, a nielen subsystémov zrejme rozhodujúcich z hľadiska bezpečnosti (napr. automatického zabezpečenia vlaku a dráhových vozidiel), ktoré sa zúčastňujú na bezpečnostných funkciách a majú aktívnu úlohu na zaisťovaní bezpečnosti cestujúcich a personálu;
(3) intenzívna koordinácia medzi aktérmi (zhotoviteľmi, dodávateľmi technických subsystémov a stavebných objektov) s cieľom:

(i) systematicky zisťovať všetky odôvodnene predvídateľné nebezpečenstvá,
(ii) zisťovať možné opatrenia na zníženie všetkých rizík spojených so zistenými nebezpečenstvami na prijateľnú úroveň;

c) použitie kódexov postupov [časť 2.3]:

Použili sa rôzne kódexy postupov, normy a predpisy, napr.:

(1) nariadenie BOStrab o stavbe a prevádzke vozidiel pouličných dráh (nemecký predpis uplatňovaný na mestské koľajové systémy) a o prevádzke bez vodiča,
(2) publikácie VDV (nemecké kódexy postupov) súvisiace s požiadavkami na zariadenia na zaistenie bezpečnosti cestujúcich na staniciach dopravných systémov bez vodiča,
(3) normy CENELEC pre dráhové systémy (EN 50 126, 50 128 a 50 129). Tieto normy sa zaoberajú najmä technickými železničnými systémami. Obsahujú však aj metodický prístup, ktorý má všeobecnú platnosť, a preto sa všeobecne uplatňovali na kodanskom metre:

(i) EN 50126 bola použitá pri činnostiach riadenia bezpečnosti a posudzovania rizík celého koľajového systému,
(ii) EN 50 129 bola použitá na celom signalizačnom systéme,
(iii) EN 50 128 bola použitá pri vývoji softvéru technických subsystémov (vrátane verifikácie a validácie),

(4) požiarne normy pre tunely (NEPA 130);
(5) normy o navrhovaní konštrukcií a realizovaní stavieb (eurokódy);

d) použitie referenčného systému [časť 2.4]:

Pri tomto metre sa musela dosiahnuť úroveň bezpečnosti zodpovedajúca moderným zariadeniam v Nemecku, vo Francúzsku a Veľkej Británii. Tieto existujúce systémy sa použili ako podobné referenčné systémy na odvodenie kritérií akceptovania rizika, pokiaľ išlo o prijateľné početnosti nehôd v kodanskom metre;

e) explicitný odhad a hodnotenie rizika [časť 2.5]:

(1) na odhad rizík spojených s konkrétnymi nebezpečenstvami,
(2) na ovládanie núdzového vetrania tunela (vrátane ľudských činiteľov zúčastnených hasičských útvarov),
(3) na určenie opatrení, ktorými sa znížia riziká,
(4) na vyhodnotenie, či sa v celom systéme dosiahla prijateľná úroveň rizika;

f) preukázanie súladu systému s požiadavkami na bezpečnosť [časť 3]:

(1) manažérske a technické činnosti na preukazovanie bezpečnosti systému v súlade so zložitosťou systému,
(2) rozdelenie požiadaviek na bezpečnosť systému na technické subsystémy a stavebné objekty, ako aj na všetky funkcie metra súvisiace s bezpečnosťou,

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(3) preukázanie, že každý subsystém, tak ako je zhotovený, spĺňa požiadavky na bezpečnosť,
(4) pri bezpečnostných funkciách, ktoré plní viac subsystémov, by sa súlad s požiadavkami na bezpečnosť nedal preukázať na úrovni subsystému. Preukazoval sa na úrovni systému integrovaním rôznych subsystémov, nástrojov a postupov;
(5) preukázanie, že celý systém spĺňa požiadavky na bezpečnosť na vysokej úrovni.

g) riadenie nebezpečenstiev [časť 4.1]:

Zistené nebezpečenstvá, s nimi súvisiace bezpečnostné opatrenia a výsledné požiadavky na bezpečnosť boli zapísané do centrálneho záznamu o nebezpečenstve a riadené prostredníctvom neho. Za tento záznam o nebezpečenstve zodpovedal hlavný manažér bezpečnosti projektu. Prevádzkové nebezpečenstvá, ktoré sa zistili počas projektovania a realizácie, ako aj nebezpečenstvá súvisiace s prevádzkou a údržbou za zapisovali do záznamu o nebezpečenstve;

h) doklady o riadení a posudzovaní rizík [časť 5]:

Výsledky posudzovania rizík sa formálne dokumentovali a dokladovali v bezpečnostnej dokumentácii v súlade s požiadavkami noriem CENELEC:

(1) v súhrnnej bezpečnostnej dokumentácii systému,
(2) v bezpečnostnej dokumentácii každého technického subsystému (vrátane signalizačných subsystémov a stavebných objektov),
(3) v bezpečnostnej dokumentácii stavebných objektov (staníc, tunelov, viaduktov, násypov),
(4) v bezpečnostnej dokumentácii zariadení,
(5) v bezpečnostnej dokumentácii vozidiel,
(6) v bezpečnostnej dokumentácii prevádzkovateľov (na pomoc pri osvedčovaní SMS ŽP a MI, t. j. pri preukazovaní schopnosti navrhovateľa prevádzkovať a udržiavať systém v bezpečnom stave);

i) nezávislé posúdenie [Článok 6]:

Celý proces sledoval a posudzoval nezávislý posudzovateľ bezpečnosti, ktorého na to poveril orgán technického dozoru (t. j. dánske ministerstvo dopravy). Úlohy nezávislého posudzovateľa bezpečnosti sú uvedené v príslušnom kódexe postupov. Ich súčasťou bola:

(1) kontrola správnosti riadenia rizík a posúdenia rizík,
(2) kontrola vhodnosti posudzovaného systému na daný účel a možnosti prevádzkovať a udržiavať ho v bezpečnom stave po celý čas životného cyklu,
(3) odporúčanie, aby orgán technického dozoru projekt schválil.

C.9.4. Celý projekt bol podporovaný vhodným procesom riadenia kvality.

C.9.5. Dodávatelia predkladali manažérovi bezpečnosti navrhovateľa dôkazy projektu (t. j. bezpečnostné preukazy a podrobnú doplňujúcu dokumentáciu technických subsystémov a stavebných objektov). Tieto dôkazy potom skontrolovala organizácia riadenia bezpečnosti, ako aj nezávislý posudzovateľ bezpečnosti, ktorého závery boli uvedené v správe o posúdení.
Správu o nezávislom posúdení bezpečnosti preskúmal manažment bezpečnosti navrhovateľa a predložil ju navrhovateľovi, ktorý všetku spisovú dokumentáciu postúpil na konečné schválenie orgánu technického dozoru (t. j. dánskemu ministerstvu dopravy).

C.9.6. Na príklade vidieť, že zásady, ktoré vyžaduje spoločná bezpečnostná metóda, sú existujúce metódy, ktoré sa v železničnom sektore uplatňujú. Posúdenie rizík v tomto príklade spĺňa

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

všetky požiadavky CSM. Využíva všetky tri zásady akceptovania rizika, s ktorými sa uvažuje pri harmonizovanom prístupe k CSM.

C.10. Príklad usmernenia OTIF na výpočet rizika zapríčineného prepravou nebezpečného tovaru po železnici

C.10.1. **Poznámka:** Tento príklad nie je uvedený ako výsledok uplatňovania procesu CSM; realizoval sa pred existenciou CSM. Účelom tohto príkladu je:

j) a) zistiť podobnosť medzi existujúcimi metódami posudzovania rizík a procesom CSM;
k) b) ilustrovať sledovateľnosť medzi krokmi existujúceho procesu a procesu, ktorý si vyžaduje CSM;
l) c) zdôvodniť pridanú hodnotu prípadných ďalších krokov, ktoré si vyžaduje CSM.

Zdôrazňujeme, že tento príklad je uvedený len na informáciu. Jeho účelom je pomôcť čitateľovi pochopiť proces CSM. Príklad sám sa však nesmie transponovať ani použiť ako referenčný systém pre inú významnú zmenu. Posúdenie rizík sa pre každú významnú zmenu musí robiť v súlade s nariadením o CSM.

C.10.2. Celková filozofia usmernenia OTIF je v súlade s účelom CSM, ale usmernenie má zúžený rozsah pôsobnosti. Cieľom usmernenia OTIF je *„zabezpečiť jednotnejší prístup k posudzovaniu rizík dopravy nebezpečného tovaru v členských štátoch COTIF, a tým porovnateľnosť jednotlivých posúdení rizík“*. Podporuje tak vzájomné uznávanie posúdení rizika dopravy nebezpečného tovaru po železnici medzi členskými štátmi dohovoru COTIF.

C.10.3. Pri porovnaní CSM s vývojovým diagramom na Obr. 1:

a) Usmernenie OTIF má tieto spoločné znaky:

(1) spoločný prístup k posudzovaniu rizík, viac-menej len na základe explicitného odhadu rizík (t. j. tretej zásady akceptovania rizika CSM),
(2) posudzovanie rizík OTIF pozostáva z:

(i) fázy analýzy rizík, ktorá má

- fázu identifikácie nebezpečenstiev a
- fázu odhadu rizík,

(ii) fázy hodnotenia rizík založenej na kritériách (akceptovania) rizík, ktoré zatiaľ nie sú harmonizované. Tieto kritériá môžu byť v skutočnosti ovplyvnené množstvom vnútroštátnych špecifík.

b) Usmernenie OTIF sa líši v týchto znakoch:

(1) odlišný je rozsah uplatňovania. Kým CSM sa má uplatňovať len na významné zmeny železničného systému, usmernenie OTIF by sa malo uplatňovať na posudzovanie rizík prepravy nebezpečného tovaru po železnici bez ohľadu na to, či ide o významnú zmenu železničného systému;
(2) na kontrolovanie rizika/rizík neexistuje možnosť voľby medzi troma zásadami akceptovania rizika. Tretia zásada, t. j. explicitný odhad rizík, je jedinou možnosťou. Okrem toho sa musí zakladať výhradne na kvantitatívnom odhade. Kvalitatívna analýza rizík môže byť vhodná len na porovnanie možností uplatnenia (bezpečnostných) opatrení na zníženie rizík;
(3) na určenie, či sa ďalším bezpečnostnými opatreniami nemôže ďalej znížiť posudzované riziko za rozumnú cenu, sa vyžaduje uplatnenie zásady ALARP (*As Low As Reasonably Practicable*);

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(4) neexistuje pojem „nebezpečenstiev spojených so všeobecne prijateľným“, ktoré umožňuje zamerať posudzovanie rizika na nebezpečenstvá s najväčším podielom. Napriek tomu odporúča znížiť počet potenciálnych scenárov nehody na rozumný počet základných scenárov (pozri v časti § 3.2 usmernenia OTIF {Ref. 10});
(5) proces sa sústreďuje na posudzovanie rizík, ale neobsahuje:

(i) proces na výber a implementáciu (bezpečnostných) opatrení na úpravu rizika,
(ii) proces na prijatie rizika,
(iii) proces na preukazovanie súladu systému s požiadavkami na bezpečnosť,
(iv) proces na oznamovanie rizika iným príslušným aktérom (pozri nasledujúci bod);

(6) nemá usmernenie o dôkaze, ktorý má zabezpečiť proces posudzovania rizík;
(7) nevyžaduje sa riadenie nebezpečenstiev;
(8) nevyžaduje sa žiadne nezávislé posúdenie správnosti uplatnenia spoločného prístupu treťou stranou.

C.10.4. Z porovnania medzi usmernením OTIF a CSM vidieť, že obe sú zlučiteľné napriek tomu, že ich rozsah pôsobnosti a účel sa presne nezhodujú. CSM je všeobecnejšia než usmernenie OTIF, v tomto zmysle je pružnejšia. Na druhej strane CSM pokrýva aj viac činností riadenia rizík:

a) umožňuje použiť zásady akceptovania rizika, ktoré sa zakladajú na existujúcich postupoch železníc: pozri časť 2.1.4;
b) jej uplatňovanie sa vyžaduje len na významné zmeny a ďalšia analýza rizík sa vyžaduje len pri nebezpečenstvách, ktoré nie sú spojené so všeobecne prijateľným rizikom;
c) obsahuje výber a implementáciu bezpečnostných opatrení, od ktorých sa očakáva kontrolovanie zistených nebezpečenstiev a s nimi súvisiacich rizík;
d) harmonizuje proces riadenia rizík, vrátane:

(1) harmonizácie kritérií akceptovania rizika, ktorými sa zaoberá agentúra v rámci prác na všeobecne prijateľných rizikách a kritériách akceptovania rizika,
(2) preukazovania súladu systému s požiadavkami na bezpečnosť,
(3) výsledkov a dôkazov procesu posúdenia rizík,
(4) výmeny informácií súvisiacich s bezpečnosťou medzi aktérmi na rozhraniach,
(5) vedenia záznamov o nebezpečenstve o všetkých zistených nebezpečenstvách a s nimi súvisiacich bezpečnostných opatreniach,
(6) nezávislého posúdenia správnosti uplatnenia CSM treťou stranou.

C.10.5. Uplatnenie usmernenia OTIF v rámci CSM (v prípade dopravy nebezpečného tovaru predstavuje pre MI alebo ŽP významnú zmenu) však nie je žiadnym problémom, pretože je zlučiteľné s použitím tretej zásady explicitného odhadovania rizík.

C.11. Príklad posúdenia rizika pri žiadosti o schválenie nového typu dráhového vozidla

C.11.1. **Poznámka:** Tento príklad nie je uvedený ako výsledok uplatňovania procesu CSM; realizoval sa pred existenciou CSM. Účelom tohto príkladu je:

e) a) zistiť podobnosť medzi existujúcimi metódami posudzovania rizík a procesom CSM;
f) b) ilustrovať sledovateľnosť medzi krokmi existujúceho procesu a procesu, ktorý si vyžaduje CSM;
g) c) zdôvodniť pridanú hodnotu prípadných ďalších krokov, ktoré si vyžaduje CSM.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Zdôrazňujeme, že tento príklad je uvedený len na informáciu. Jeho účelom je pomôcť čitateľovi pochopiť proces CSM. Príklad sám sa však nesmie transponovať ani použiť ako referenčný systém pre inú významnú zmenu. Posúdenie rizík sa pre každú významnú zmenu musí robiť v súlade s nariadením o CSM.

C.11.2. Tento príklad posúdenia rizika sa týka žiadosti o schválenie nového typu dráhového vozidla. Analýza rizík bola vykonaná na vyhodnotenie rizík spojených so zavedením nového nákladného vozňa.

C.11.3. Účelom zmeny bolo zvýšenie účinnosti, kapacity, výkonu a bezporuchovosti dopravy hromadného tovaru na konkrétnej trati pre nákladnú dopravu. Keďže vozne boli určené na cezhraničnú dopravu, bolo potrebné aj schválenie dvoch rôznych NBO. Navrhovateľom bol dopravca, ktorý vlastnil aj podnik vyrábajúci tovar určený na prepravu.

C.11.4. Súčasťou projektu bola konštrukcia, výroba, montáž, uvedenie do prevádzky a overenie nového dráhového vozidla. Bola vykonaná analýza rizík na overenie, že nový dizajn spĺňa požiadavky na bezpečnosť pre každý subsystém, ako aj pre celý systém.

C.11.5. V analýze rizík boli odkazy na postupy a definície uvedené v norme CENELEC EN 50 126 a hodnotenie rizík bolo vykonané podľa tejto normy.

C.11.6. V porovnaní s procesom CSM sa uplatnili tieto kroky:

a) opis systému [časť 2.1.2]:

V každej fáze návrhu boli tieto požiadavky na dokumentáciu o overení bezpečnosti a na opis návrhu systému:

(1) vo fáze koncepčného návrhu: predbežný opis prevádzkových požiadaviek prevádzkovateľa,
(2) vo fáze špecifikácií: funkčná špecifikácia, uplatniteľné technické normy, plán skúšok a overovania. Zahrnuté boli aj požiadavky prevádzkovateľa na používanie a údržbu vozňa,
(3) vo fáze výroby: technická dokumentácia výrobcu vrátane výkresov, noriem, výpočtov, analýzy atď. Hĺbková analýza rizík nových alebo inovačných dizajnov alebo nových oblastí použitia;
(4) vo fáze overovania:

(i) overovanie technickej výkonnosti vozňa výrobcom (správy o skúškach, výpočty, overovanie súladu s normami a funkčnými požiadavkami);
(ii) dokumentácia opatrení na zníženie rizík a správy o skúškach potvrdzujúce zlučiteľnosť vozňov so železničnou infraštruktúrou;
(iii) dokumentácia údržby a odbornej prípravy, používateľské návody atď.

(5) vo fáze schvaľovania:

(i) bezpečnostné vyhlásenie a dôkaz o bezpečnosti (bezpečnostný preukaz) výrobcu;
(ii) schválenie nákladného vozňa a jeho dokumentácie prevádzkovateľom;

b) identifikácia nebezpečenstiev [časť 2.2]:

nebezpečenstvá sa identifikovali priebežne vo všetkých fázach návrhu. Najprv sa použil prístup „zdola nahor“, pričom rôzni výrobcovia hodnotili postupnosti rizík vznikajúcich následkom porúch komponentov svojho subsystému. Rozdelenie na subsystémy bolo takéto:

(1) podvozok,
(2) brzdový systém,

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(3) centrálne spriahlo,
(4) atď.

Potom sa použil doplnkový prístup „zhora nadol“ na zistenie medzier alebo chýbajúcich informácií. Riziká, ktoré sa nepodarilo bezprostredne prijať, sa zapísali do záznamu o nebezpečenstve na ďalšie spracovanie a klasifikáciu.

c) použitie zásad akceptovania rizika [časť 2.1.4]:

Explicitný odhad rizík sa vykonal na systéme ako celku. Na posúdenie jednotlivých nebezpečenstiev sa však dali použiť kódexy postupov alebo podobné referenčné systémy. Uplatnenie zásady, aby každý nový subsystém bol aspoň taký bezpečný ako subsystém, ktorý nahrádza, tak povedie k novému kompletnému systému s vyššou úrovňou bezpečnosti, ako mal predchádzajúci systém. Na zobrazenie zistených nebezpečenstiev bola použitá matica rizík podľa EN 50 126. Uplatnili sa aj rôzne ďalšie kritériá akceptovania rizika, okrem iných tieto:

(1) jednoduchá porucha by nemala viesť k situácii, ktorá by mohla vážne ohroziť ľudí, materiál alebo životné prostredie;
(2) ak tomu nemožno zabrániť prostriedkami technickej konštrukcie, mali by tomu zabrániť prevádzkové predpisy alebo požiadavky na údržbu. Toto sa dalo uplatniť len na nebezpečenstvá, pri ktorých bolo možné zistiť poruchu ešte pred vznikom nebezpečnej situácie;
(3) pri komponentoch s vysokou pravdepodobnosťou poruchy, alebo pri ktorých nebolo možné poruchy zistiť vopred ani im predísť dodržaním prevádzkových predpisov, by sa mali uvážiť ďalšie bezpečnostné funkcie a zábrany;
(4) redundantné systémy s komponentmi, ktoré môžu mať počas prevádzky nezistiteľné poruchy, by mali byť chránené opatreniami údržby, ktoré zabránia zníženej redundantnosti;
(5) o výslednej konečnej úrovni bezpečnosti rozhodol manažment, ktorého rozhodnutie sa zakladalo na kvantitatívnej a kvalitatívnej analýze rizík;

d) preukázanie súladu systému s požiadavkami na bezpečnosť [časť 3]:

Všetky zistené riziká a nebezpečenstvá sa zapisovali a ich zoznam sa priebežne konzultoval a aktualizoval. Zostávajúce nebezpečenstvá sa zapisovali do záznamu o nebezpečenstve spolu so zodpovedajúcim zoznamom opatrení znižujúcich riziká, ktoré sa mali prevziať do konštrukcie, prevádzky a údržby. Na tomto základe bola vypracovaná záverečná bezpečnostná správa ktorou sa overilo, že všetky požiadavky na bezpečnosť sú splnené;

e) riadenie nebezpečenstiev [časť 4.1]:

Ako už bolo uvedené, zistené nebezpečenstvá a s nimi súvisiace bezpečnostné opatrenia sa zapisovali do záznamu o nebezpečenstve, v ktorej sa sledoval vývoj všetkých zistených nebezpečenstiev a bezpečnostných opatrení. Nebezpečenstvá spojené s rizikami, ktoré boli prijateľné bez opatrení, sa však do záznamu o nebezpečenstve nezapisovali;

f) nezávislé posúdenie [Článok 6]:

V prijatej dokumentácii nebola žiadna zmienka o nezávislom posúdení v súvislosti s touto významnou zmenou.

C.11.7. Príklad posúdenia rizík vychádza z normy CENELEC EN 50 126, a teda dobre zodpovedá procesu CSM. Posúdenie rizík v príklade spĺňa požiadavky CSM s výnimkou požiadavky na nezávislé posúdenie, ktorá v prijatej dokumentácii nebola výslovne objasnená. Boli použité explicitné kritériá akceptovania rizika a boli zrozumiteľne uvedené.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

C.12. Príklad posúdenia rizík významnej prevádzkovej zmeny – jednočlennej obsluhy vlaku

C.12.1. **Poznámka:** Tento príklad nie je uvedený ako výsledok uplatňovania procesu CSM; realizoval sa pred existenciou CSM. Účelom tohto príkladu je:

g) a) zistiť podobnosť medzi existujúcimi metódami posudzovania rizík a procesom CSM;
h) b) ilustrovať sledovateľnosť medzi krokmi existujúceho procesu a procesu, ktorý si vyžaduje CSM;
i) c) zdôvodniť pridanú hodnotu prípadných ďalších krokov, ktoré si vyžaduje CSM.

Zdôrazňujeme, že tento príklad je uvedený len na informáciu. Jeho účelom je pomôcť čitateľovi pochopiť proces CSM. Príklad sám sa však nesmie transponovať ani použiť ako referenčný systém pre inú významnú zmenu. Posúdenie rizík sa pre každú významnú zmenu musí robiť v súlade s nariadením o CSM.

C.12.2. Príkladom je prevádzková zmena, v rámci ktorej sa železničný podnik rozhodol, že na trase, na ktorej predtým býval vo vlaku sprievodca, ktorý pomáhal rušňovodičovi pri vypravovaní vlaku, bude vlak viesť len vodič (Driver Only Operated; DOO).

C.12.3. V porovnaní s procesom CSM sa uplatnili tieto kroky (pozri aj Obr. 1):

a) významnosť zmeny [Článok 4:

Železničný podnik vykonal predbežné posúdenie rizík, na základe ktorého dospel k záveru, že prevádzková zmena je významná. Keďže vodič má vlak obsluhovať sám, bez pomoci, nie je možné zanedbať možnosť, že cestujúcich zachytia dvere alebo že vypadnú na trať (napr. ak sa dvere otvoria na nesprávnej strane).

Pri porovnaní tohto predbežného posúdenia rizík s kritériami podľa Článok 4 nariadenia o CSM, zmenu by bolo možné zaradiť ako významnú na základe týchto kritérií:

(1) význam z hľadiska bezpečnosti: zmena súvisí s bezpečnosťou lebo vplyv požiadavky na úplne iný spôsob riadenia prevádzky vlakovej služby by mohol byť katastrofický;
(2) dôsledok poruchy: potenciálny účinok činnosti vodiča by mohol mať katastrofické dôsledky, ak by prevádzka nebola riadená účinne;
(3) inovatívnosť: prevádzka s jednočlennou obsluhou by si mohla vyžadovať inovačné spôsoby prevádzkovania vlakov, ktorých riziká sa musia posúdiť;

b) vymedzenie systému [časť 2.1.2]:

Vymedzenie systému opísalo:
(1) existujúci systém, zrozumiteľne vysvetliac, ktoré úlohy plnil vodič, a ktoré ostatná obsluha vlaku (alebo sprievodca), aby pomohli vodičovi;
(2) zmenu povinností vodiča vzhľadom na vylúčenie pomocného personálu vlaku;
(3) technické požiadavky systému na zvládnutie zmien v prevádzke;
(4) existujúce rozhrania medzi pomocnou obsluhou vlaku, vodičom a traťovými zamestnancami manažéra infraštruktúry;

Rôznymi iteráciami sa vymedzenie systému aktualizovalo so zreteľom na požiadavky na bezpečnosť, ktoré vyplynuli z procesu posúdenia rizík. Do tohto iteratívneho procesu identifikácie nebezpečenstiev a aktualizácie vymedzenia systému boli zapojené kľúčové osoby (vrátane vodičov, predstaviteľov zamestnancov a manažéra infraštruktúry).

c) identifikácia nebezpečenstiev [časť 2.2]:

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Nebezpečenstvá a možné bezpečnostné opatrenia sa zisťovali brainstormingom skupiny odborníkov, v ktorej boli okrem iných aj:

(1) zástupcovia vodičov a zamestnancov kvôli svojim prevádzkovým skúsenostiam,
(2) predstavitelia MI, pretože zmena by za predpokladu napr. zmien na staniciach (napr. namontovaním zrkadiel, a priemyselnej televízie (CCTV) na nástupištiach) mohla ovplyvniť aj infraštruktúru.

Skúmali sa aj ďalšie úlohy, ktoré mal vodič plniť, aby sa zistili všetky predvídateľné nebezpečenstvá, ktoré by sa pravdepodobne objavili po zrušení pomocnej obsluhy vlaku. Pri identifikácii nebezpečenstiev sa hľadali najmä kľúčové prevádzkové nebezpečenstvá, ktoré by sa mohli vyskytnúť na staniciach na existujúcich trasách, keď tam bola pomoc vlakového alebo traťového personálu vrátane bezpečného vypravovania vlakov, konkrétnych otázok súvisiacich s vodičom, vozovým parkom (napr. kontrolou otvárania a zatvárania dverí), požiadavkami údržby atď.

Každému zistenému nebezpečenstvu bola priradená úroveň závažnosti rizika a dôsledkov (vysoká, stredná, nízka) a vplyv navrhovanej zmeny sa skúmal vzhľadom na ne (zvýšené, nezmenené, znížené riziko).

d) použitie kódexov postupov [časť 2.3] a použitie podobných referenčných systémov [časť 2.4]:

Na vymedzenie požiadaviek na bezpečnosť vzhľadom na zistené nebezpečenstvá sa použili kódexy postupov (t. j. súbor noriem pre jednočlennú obsluhu vlaku) aj podobné referenčné systémy. Tieto požiadavky na bezpečnosť obsahovali:

(1) revidované prevádzkové postupy pre vodiča, ktoré vyžadovali bezpečné prevádzkovanie vlakov bez pomoci vo vlaku;
(2) akékoľvek ďalšie vybavenie potrebné vo vlaku alebo na trati na zaistenie bezpečných a bezporuchových prostriedkov na vypravenie vlaku;
(3) kontrolný zoznam na zaistenie vhodnosti kabíny vodiča, s prihliadnutím na rozhranie medzi železničným systémom (vlakovým aj traťovým) a vodičom;

Potrebné prevádzkové predpisy sa revidovali v súlade s požiadavkami platných kódexov postupov a príslušných referenčných systémov. Na revízii prevádzkových postupov a dohode o pokračovaní na zmene sa zúčastnili všetky zainteresované strany.

e) preukázanie súladu systému s požiadavkami na bezpečnosť [časť 3]:

Systém sa implementoval v súlade so zistenými požiadavkami na bezpečnosť (ďalším vybavením a revidovanými postupmi). Tieto sa overili ako vhodné prostriedky na zaistenie dostatočnej úrovne bezpečnosti posudzovaného systému.

Do systému riadenia bezpečnosti ŽP sa zaviedli revidované prevádzkové postupy. Postupy sa monitorovali a podľa potreby revidovali, aby sa zaistilo správne kontrolovanie zistených nebezpečenstiev počas prevádzky železničného systému.

f) riadenie nebezpečenstiev [časť 4.1]:

Pozri už uvedené o procese riadenia nebezpečenstiev v železničných podnikoch, ktorý môže byť časťou ich systému riadenia bezpečnosti na zaznamenávanie a riadenie rizík. Zistené nebezpečenstvá boli zapísané do záznamu o nebezpečenstve spolu s požiadavkami na bezpečnosť, t. j. s odkazom na ďalšie vlakové a traťové vybavenie, ako aj revidované prevádzkové postupy znižujúce súvisiace riziko.
Revidované postupy sa sledovali a podľa potreby ďalej revidovali, aby sa zaistilo správne kontrolovanie zistených nebezpečenstiev počas prevádzky železničného systému.

g) nezávislé posúdenie [Článok 6]:

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Posúdenie rizík a proces riadenia rizík posúdila príslušná odborne spôsobilá osoba v rámci železničného podniku, ktorá bola nezávislá od procesu posúdenia. Táto osoba posúdila proces aj výsledky, t. j. zistené požiadavky na bezpečnosť.

ŽP založil svoje rozhodnutie o zavedení nového systému na správe o nezávislom posúdení, ktorú vypracovala táto odborne spôsobilá osoba.

C.12.4. Na príklade vidieť, že zásady a postupy uplatnené v železničnom podniku sú v súlade so spoločnou bezpečnostnou metódou. Riadenie rizík a proces posúdenia rizík splnil všetky požiadavky CSM.

C.13. Príklad použitia referenčného systému na odvodenie požiadaviek na bezpečnosť na nové elektronické stavadlové systémy v Nemecku

C.13.1. **Poznámka:** Tento príklad nie je uvedený ako výsledok uplatňovania procesu CSM; realizoval sa pred existenciou CSM. Účelom tohto príkladu je:

h) a) zistiť podobnosť medzi existujúcimi metódami posudzovania rizík a procesom CSM;
i) b) ilustrovať sledovateľnosť medzi krokmi existujúceho procesu a procesu, ktorý si vyžaduje CSM;
j) c) zdôvodniť pridanú hodnotu prípadných ďalších krokov, ktoré si vyžaduje CSM.

Zdôrazňujeme, že tento príklad je uvedený len na informáciu. Jeho účelom je pomôcť čitateľovi pochopiť proces CSM. Príklad sám sa však nesmie transponovať ani použiť ako referenčný systém pre inú významnú zmenu. Posúdenie rizík sa pre každú významnú zmenu musí robiť v súlade s nariadením o CSM.

C.13.2. Na účel odvodenia štandardných požiadaviek na bezpečnosť na budúce elektronické zabezpečovacie systémy vykonali Nemecké železnice (Deutsche Bahn) analýzu rizík na už schválenom systéme elektronického zabezpečovacieho zariadenia. Systém bol pôvodne schválený podľa nemeckých kódexov postupov (Mü 8004).

C.13.3. Analýza rizík bola vykonaná v súlade s normami CENELEC (EN 50 126 a EN 50 129) a pozostávala z týchto krokov:

a) vymedzenie systému,
b) identifikácia nebezpečenstiev,
c) analýza a kvantifikácia nebezpečenstiev.

C.13.4. Pri vymedzovaní systému boli starostlivo vymedzené hranice systému, jeho funkcie a rozhrania. Hlavným problémom pritom bolo vymedzenie systému tak, aby nezáviselo od vnútornej architektúry stavadlového systému a aby zároveň ostalo kompatibilné s existujúcimi stavadlovými systémami. Osobitná pozornosť sa preto venovala veľmi jasnému vymedzeniu rozhraní s vonkajšími systémami spolupracujúcimi so stavadlom, bez podrobností vnútorných funkcií stavadla.

C.13.5. Preto sa potom identifikovali len nebezpečenstvá na rozhraniach s cieľom zachovať podobnosť (t. j. vyhnúť sa závislosti od určitých architektúr). Do úvahy sa brali iba nebezpečenstvá zapríčinené technickými poruchami. Pri každom rozhraní tak boli identifikované dve všeobecné a spoločné nebezpečenstvá:

a) nesprávny výstup stavadla vyslaný rozhraniu,
b) (správny) vstup je poškodený na rozhraní.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

C.13.6. Pre každé rozhranie boli potom tieto generické nebezpečenstvá charakterizované konkrétnejšie.

C.13.7. V nasledujúcej fáze sa analyzovali príspevky komponentov existujúceho systému ku každému zistenému nebezpečenstvu a zostavili sa do stromu porúch. Na základe odhadu početnosti porúch komponentov potom bolo možné vypočítať početnosť výskytu každého nebezpečenstva a tieto početnosti potom použiť ako tolerovateľné intenzity nebezpečenstva (*THR*) pre budúce generácie elektronických zabezpečovacích zariadení.

C.13.8. Analýzu rizík sledoval a posudzoval národný bezpečnostný orgán (*Eisenbahn-Bundesamt, EBA*).

C.13.9. Súčasťou analýzy rizík bola aj analýza ovládania a zobrazovania funkcií elektronického systému. Znovu bol za referenčný systém vzatý existujúci schválený elektronický stavadlový systém s cieľom odvodiť požiadavky na bezpečnosť funkcií rozhrania človek-stroj (*Machine-Man-Interface; MMI*) na kontrolovanie náhodných porúch a chýb a na kontrolovanie systematických chýb. Napokon boli stanovené úrovne integrity bezpečnosti (SIL) pre rôzne funkcie: pre funkcie MMI v normálnej prevádzke, funkcie MMI v prevádzke Command-Release (poruchový režim) a funkčnosť zobrazovania.

C.13.10. Aj túto analýzu rizík sledoval a posudzoval národný bezpečnostný orgán (EBA).

C.13.11. Uvedené príklady posudzovania rizík ozrejmujú využitie druhej zásady akceptovania rizika (referenčný systém) CSM na odvodenie požiadaviek na bezpečnosť pre nové systémy. Navyše vychádzali z noriem CENELEC, a teda dobre zodpovedajú procesu CSM. Posudzovanie rizík v príkladoch spĺňa požiadavky nariadenia o CSM, ktoré sa týkajú jednotlivých fáz procesu. Keďže ich súčasťou nie je projektová činnosť, nie je tu odkaz na vedenie záznamu o nebezpečenstve ani na preukazovanie súladu posudzovaného systému s identifikovanými požiadavkami na bezpečnosť.

C.13.12. Ďalšie informácie o týchto analýzach rizík je možné nájsť v:

a) Ziegler, P., Kupfer, L., Wunder, H.: *Erfahrungen mit der Risikoanalyse ESTW (DB AG)*, Signal+Draht, 10, 2003, 10-15;

b) Bock, H., Braband, J., a 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, 234-253.

C.14. Príklad explicitného kritéria akceptovania rizika pre rádiom riadenú prevádzku vlakov v Nemecku

C.14.1. **Poznámka:** Tento príklad nie je uvedený ako výsledok uplatňovania procesu CSM; realizoval sa pred existenciou CSM. Účelom tohto príkladu je:

c) a) zistiť podobnosť medzi existujúcimi metódami posudzovania rizík a procesom CSM;
d) b) ilustrovať sledovateľnosť medzi krokmi existujúceho procesu a procesu, ktorý si vyžaduje CSM;
e) zdôvodniť pridanú hodnotu prípadných ďalších krokov, ktoré si vyžaduje CSM.

Zdôrazňujeme, že tento príklad je uvedený len na informáciu. Jeho účelom je pomôcť čitateľovi pochopiť proces CSM. Príklad sám sa však nesmie transponovať ani použiť ako

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

referenčný systém pre inú významnú zmenu. Posúdenie rizík sa pre každú významnú zmenu musí robiť v súlade s nariadením o CSM.

C.14.2. Analýza rizík podľa noriem CENELEC bola vykonaná pre úplne nový prevádzkový postup, ktorý bol navrhovaný (ale sa nikdy nezaviedol) v Nemecku pre konvenčné železničné trate. Koncepcia spočívala v bezpečnom prevádzkovaní vlakov len ovládaním (trasy a vlaku) na báze rádiokomunikácie. Vzhľadom na to, že neexistovali kódexy postupov (schválené technické predpisy) ani referenčné systémy pre takýto nový systém, vykonal sa explicitný odhad rizík, ktorého cieľom bolo preukázanie bezpečnosti nového postupu. Potrebné bolo preukázať, že úroveň rizika pre cestujúcich pri novom systéme neprevýši hodnotu prijateľného rizika (explicitné kritérium akceptovania rizika).

C.14.3. Toto explicitné kritérium akceptovania rizika bolo odhadnuté na základe štatistických údajov o nehodách v Nemecku, ktorých príčinou mohli byť signalizačné, a riadiace a zabezpečovacie systémy a jeho hodnovernosť sa preverovala aj porovnaním s kritériom MEM. Takéto preukázanie bezpečnosti sa zhoduje s požiadavkou nemeckého železničného stavebného a prevádzkového poriadku (*Eisenbahn-Bau und Betriebsordnung; EBO*) na „rovnakú úroveň bezpečnosti“ v prípade odchýlok od technických predpisov. Aj túto analýzu rizík sledoval a posudzoval národný bezpečnostný orgán (EBA).

C.14.4. Tento príklad posúdenia rizík ukazuje možný spôsob odvodenia globálneho explicitného kritéria (ako tretej zásady akceptovania rizika v CSM), keď pre nové systémy neexistujú platné kódexy postupov ani referenčný systém. Analýza rizík, ktorá bola pre nový systém nadväzne vykonaná, vychádzala z noriem CENELEC, a teda dobre zodpovedá procesu CSM. Posúdenie rizík v tomto príklade spĺňa požiadavky nariadenia o CSM, ale nie je v ňom odkaz na vedenie záznamu o nebezpečenstve, ani na preukazovanie súladu posudzovaného systému s identifikovanými požiadavkami na bezpečnosť.

C.14.5. Ďalšie informácie o tejto analýze rizík je možné nájsť v článku: Braband, J., Günther, J., Lennartz, K., Reuter, D.: *Risikoakzeptanzkriterien für den FunkFahrBetrieb (FFB)*, Signal + Draht, Nr. 5, 2001, 10-15.

C.15. Príklad testu uplatniteľnosti RAC-TS

C.15.1. Účelom tohto dodatku je, na príklade funkcie vozidlového subsystému ETCS ukázať použitie kritéria podľa časti 2.5.4 a určenie uplatniteľnosti kritéria RAC-TS.

C.15.2. Vozidlový subsystém ETCS je technický systém. Posudzovala sa táto funkcia: *„poskytnúť vodičovi údaje, ktoré mu umožňujú viesť vlak bezpečne a zapnúť brzdy v prípade prekročenia dovolenej rýchlosti“*.

Opis funkcie: na základe informácií (o dovolenej rýchlosti) prijatých z traťového subsystému a výpočtu rýchlosti vlaku palubným subsystémom ETCS:

a) vodič vedie vlak a zaisťuje, aby rýchlosť vlaku neprevýšila dovolenú rýchlosť,
b) súčasne palubný subsystém ETCS dohliada, aby vlak nikdy neprekročil najvyššiu dovolenú rýchlosť. Pri prekročení dovolenej rýchlosti automaticky zapína brzdy.

vodič aj vozidlový subsystém ETCS využívajú vyhodnocovanie rýchlosti vlaku, ktoré počíta vozidlový subsystém ETCS.

C.15.3. Otázka: „uplatňuje sa kritérium RAC-TS na hodnotenie rýchlosti vlaku vozidlovým subsystémom?“

C.15.4. Aplikácia vývojového diagramu na Obr. 14 a odpovede na rôzne otázky:

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

a) Posudzované nebezpečenstvo pre technický systém:

„Prekročenie bezpečnej rýchlosti, na ktoré bol upozornený systém ETCS“ (pozri UNISIG SUBSET 091).

b) Je možné kontrolovať nebezpečenstvo podľa kódexu postupov alebo referenčného systému?

NIE. Predpokladá sa, že systém ETCS je nový a inovačný projekt. Preto neexistuje žiadny kódex postupov ani referenčný systém, ktorý by umožňoval obmedziť nebezpečenstvo na prijateľnú úroveň rizika.

c) Je pravdepodobné, že by nebezpečenstvo mohlo viesť ku katastrofickým dôsledkom?

ÁNO, pretože *„prekročenie bezpečnej rýchlosti, na ktoré bol upozornený systém ETCS,“* môže mať za následok vykoľajenie vlaku s možnými *„smrteľnými a/alebo viacnásobnými ťažkým zraneniami a/alebo veľkými škodami na životnom prostredí*“.

d) Sú katastrofické dôsledky priamym dôsledkom poruchy technického systému?

ÁNO, ak nie sú ďalšie bezpečnostné zábrany. Totožné vyhodnotenie rýchlosti vlaku, ktoré vypočítal vozidlový subsystém ETCS, dostane vodič aj funkcia ovládania bŕzd vozidlového subsystému ETCS. Preto za predpokladu, že vodič (z dôvodov využitia výkonu) vedie vlak maximálnou rýchlosťou povolenou traťovým vybavením, potom ani vodič, ani vozidlový subsystém ETCS nezistia, že vlak prekročil rýchlosť, ak bola rýchlosť vlaku podhodnotená. To je potenciál, ktorý povedie k vykoľajeniu vlaku s katastrofickými dôsledkami.

e) Závery:

(1) o kvantitatívnych požiadavkách: uplatniť THR $10^{-9}\,h^{-1}$ na náhodné poruchy hardvéru vozidlového subsystému ETCS, čím sa zaistí, aby:

(i) vyhodnotenie tohto kvantitatívneho cieľa zohľadnilo pri redundantných systémoch spoločné prvky (napr. jediný alebo spoločný vstup do všetkých kanálov, spoločné pripojenie na zdroj energie, komparátory, rozhodovacie členy atď.),
(ii) boli pokryté časy detekcie „spiacich“ alebo latentných porúch,
(iii) bola vykonaná analýza porúch so spoločnou príčinou (CCF/CMF),
(iv) sa vykonalo nezávislé posúdenie;

(2) o požiadavkách na proces: na riadenie systematických porúch/chýb vozidlového subsystému ETCS uplatniť proces SIL 4. To si vyžaduje uplatňovať:

(i) proces riadenia kvality v súlade so SIL 4,
(ii) proces riadenia bezpečnosti v súlade so SIL 4,
(iii) príslušné normy, napr.:

- pri vývoji softvéru používať normu EN 50 128,
- pri vývoji hardvéru používať 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 atď.

(3) proces(y) nezávislého posúdenia.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

C.16. Príklady možných štruktúr záznamov o nebezpečenstve

C.16.1. Úvod

C.16.1.1. Minimálne požiadavky, ktoré sa musia zapisovať do záznamu o nebezpečenstve, sú uvedené v časti 4.1.2 nariadenia o CSM. V príkladoch záznamov o nebezpečenstve uvedených ďalej sú zvýraznené tónovaným pozadím.

C.16.1.2. Môžu existovať rôzne spôsoby štruktúrovania záznamu o nebezpečenstve, ako aj akýchkoľvek ďalších informácií, ktoré by mohli charakterizovať nebezpečenstvá a s nimi súvisiace bezpečnostné opatrenia. Napríklad každá informácia o nebezpečenstve a súvisiacich bezpečnostných opatreniach sa môže vyplniť do jedného poľa. Nech sa však použije akákoľvek štruktúra, je dôležité, aby záznam o nebezpečenstve zrozumiteľne vyjadroval vzťahy medzi nebezpečenstvami a s nimi súvisiacimi bezpečnostnými opatreniami. Možným riešením je záznam o nebezpečenstve, ktorý obsahuje pre každé nebezpečenstvo a pre každé bezpečnostné opatrenie aspoň jedno pole obsahujúce:

a) zrozumiteľný opis vrátane odkazov na svoj pôvod a zásadu akceptovania rizika vybranú na obmedzenie súvisiaceho rizika. Toto pole umožní pochopiť nebezpečenstvo a s ním súvisiace bezpečnostné opatrenia, ako aj to, akou bezpečnostnou analýzou boli zistené.

   Vzhľadom na to, že sa záznam o nebezpečenstve používa a udržiava počas celého životného cyklu systému (t. j. počas prevádzky a údržby systému), je užitočná ľahká sledovateľnosť alebo prepojenie medzi každým nebezpečenstvom a:

   (1) súvisiacim rizikom,
   (2) príčinami nebezpečenstva, keď sú už zistené,
   (3) súvisiacimi bezpečnostnými opatreniami, ako aj predpokladmi vymedzenia hraníc posudzovaného systému,
   (4) súvisiacimi bezpečnostnými analýzami, ktorými sa nebezpečenstvo zistilo.

   Formulácia bezpečnostných opatrení (najmä opatrení prevádzaných na iných aktérov než navrhovateľa) a znenie opisov súvisiacich nebezpečenstiev a rizík musí byť navyše zrozumiteľné a dostatočné. „Zrozumiteľné a dostatočné“ znamená, že vzťahy medzi bezpečnostnými opatreniami, rizikami, ktoré sa majú kontrolovať, a súvisiacimi nebezpečenstvami je možné pochopiť bez toho, aby bolo potrebné vrátiť sa k príslušným bezpečnostným analýzam.

b) zásadu akceptovania rizika použitú na kontrolovanie nebezpečenstva v záujme podpory vzájomného uznávania a pomoci orgánu pre posudzovanie posúdiť správnosť uplatňovania CSM;

c) zrozumiteľné informácie o jeho stave: v tomto poli sa uvedie, či je príslušné nebezpečenstvo/bezpečnostné opatrenie stále otvorené, alebo kontrolované/potvrdené.

   (1) Otvorené nebezpečenstvo/bezpečnostné opatrenie sa sleduje, kým nie je kontrolované/potvrdené;
   (2) Naopak, kontrolované/potvrdené nebezpečenstvo sa už nesleduje, pokiaľ sa v prevádzke alebo údržbe systému nevyskytnú významné zmeny: pozri písmeno b) odseku [G 6] v časti 2.1.1. Ak sa to stane:

      (i) znovu sa uplatní CSM na požadované zmeny v súlade s Článok 2. Pozri tiež odsek 2.1.1.[G 7]b)(1) v časti 2.1.1;
      (ii) všetky kontrolované nebezpečenstvá a bezpečnostné opatrenia sa posudzujú znovu, aby sa overilo, či nie sú ovplyvnené zmenami. Ak sú, príslušné nebezpečenstvá a s nimi súvisiace bezpečnostné opatrenia sa znovu otvoria a znovu budú viesť v zázname o nebezpečenstve;

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Mohlo by sa stať, že namiesto opatrení zapísaných v zázname o nebezpečenstve sa (napr. z dôvodu nákladov) implementujú rôzne iné bezpečnostné opatrenia. Implementované bezpečnostné opatrenia sa potom zapíšu do záznamu o nebezpečenstve s dôkazom/odôvodnením vhodnosti a s preukázaním, že s týmito bezpečnostnými opatreniami systém spĺňa požiadavky na bezpečnosť.

d) odkaz na súvisiaci dôkaz o kontrolovaní nebezpečenstva alebo potvrdení bezpečnostného opatrenia. Toto pole neskôr umožní nájsť dôkaz, ktorý umožnil kontrolovať nebezpečenstvo a potvrdiť s ním spojené bezpečnostné opatrenia;

Nebezpečenstvo môže byť v zázname o nebezpečenstve označené ako kontrolované, len keď sa vopred potvrdili všetky bezpečnostné opatrenia spojené s týmto nebezpečenstvom;

e) organizácie alebo subjekty zodpovedné za jeho riadenie.

C.16.1.3. Iný príklad možného obsahu záznamu o nebezpečenstve je uvedený v dodatku A.3. k usmerneniu EN 50 126-2 {Ref. 9}.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

C.16.2. Príklad záznamu o nebezpečenstve organizačnej zmeny v časti C.5. dodatku C

Tab. 6: Príklad záznamu o nebezpečenstve organizačnej zmeny v časti C.5. dodatku C.

Opis nebezpečenstva	**Bezpečnostné opatrenie**	**Priorita bezpečnosti/ presnosť**	**Implementácia[18]**	**Poznámky**	**Zodpovednosť[18]**	**Pôvod**	**Použitá zásada akceptovania rizika**	**Za overenie zodpovedá**	**Spôsob overenia**	**Stav xx.xx.xx**
Znížená motivácia zamestnancov, ktorí ostávajú v podniku. Preto personál ďalej odchádza. Znechutení/vyčerpaní manažéri.	Nové kolo motivačnej práce pre personál realizovať v menších skupinách. Prerozdelenie prostriedkov tak, aby podnik dostával na plnenie zmysluplné úlohy. Častejšia kontrola manažérom trate. Rozdeliť prostriedky tak, aby sa zaistilo, že kľúčový personál zotrvá počas celého procesu. Osobitnú pozornosť venovať zaisteniu prenosu informácií a poznatkov od odchádzajúcich zamestnancov k tým, ktorí prevezmú úlohy atď.	Vysoká/ vysoká	Koordinuje XYZ. Regióny sa musia postarať o opatrenia na zvýšenie kontroly tratí, zastupiteľnosť zamestnancov a sledovanie manažérom trate.	Častejšiu kontrolu je potrebné zahrnúť do zmlúv atď.	Riaditeľ podniku	Brainstorming Správa HAZID Rx	N/A			Zmena podmienok okolností významne znížila toto riziko. Vykonaná analýza pracovného prostredia a istá odborná príprava personálu.
Neskúsení a nespôsobilí subdodávatelia podnikateľov, bez kontroly kvality.	Zvýšená potreba dokladov o spôsobilosti. Systematická kontrola plnenia úloh.	Vysoká/ stredná	MI musí koordinovať. Regióny musia zaviesť opatrenia vyžadujúce pracovnú spôsobilosť a kontrolu práce	Implementované sledovaním zmluvy. Vstup pre plánovanie preskúmania.	Manažér infraštruktúry	Brainstorming Správa HAZID Rx	N/A	Manažér bezpečnosti		Zvýšené zameranie na bežné postupy kontroly (2 operatívne kontroly mesačne v každej prevádzkovej oblasti)
Neurčitosť úloh a povinností na rozhraní medzi podnikom a manažérom	Vymedziť úlohy a povinnosti. Zmapovať všetky rozhrania a vymedziť, kto je zodpovedný za každé rozhranie.	Stredná/ stredná	V každom regióne samostatne	Implementované zmluvou o údržbe a strategickom pláne	Regionálni riaditelia	Brainstorming Správa HAZID	N/A	Manažér bezpečnosti		Regióny predložili svoju stratégiu.

(18) *Tieto dva stĺpce sa vzťahujú na informácie/pole o aktéroch zodpovedných za kontrolovanie zistených nebezpečenstiev.*

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Tab. 6: Príklad záznamu o nebezpečenstve organizačnej zmeny v časti C.5. dodatku C.

Opis nebezpečenstva	Bezpečnostné opatrenie	Priorita bezpečnosti/ presnosť	Implemen-tácia[18]	Poznámky	Zodpoved-nosť[18]	Pôvod	Použitá zásada akceptovania rizika	Za overenie zodpovedá	Spôsob overenia	Stav xx.xx.xx
infraštruktúry (manažérom trate).				reorganizácie.		Rx				

C.16.3. Príklad úplného záznamu o nebezpečenstve pre palubný systém riadenia vlaku.

C.16.3.1. V tejto časti je uvedený príklad jediného záznamu o nebezpečenstve (pozri odsek [G 3] v časti 4.1.1) o:

a) všetkých vnútorných požiadavkách na bezpečnosť uplatniteľných na subsystém, za ktorý aktér zodpovedá a

b) všetkých zistených nebezpečenstvách a s nimi súvisiacich bezpečnostných opatreniach, ktoré aktér nemôže implementovať a ktoré musí previesť na iných aktérov.

Tab. 7: Príklad záznamu o nebezpečenstve výrobcu palubného systému riadenia vlaku.

Čís. nebezp.	Pôvod	Opis nebezpečenstva	Doplňujúce informácie	Zodpovedný aktér	Bezpečnostné opatrenie	Použitá zásada akceptovania rizika	Exporto-vané	Stav
1	Správa HAZOP R_X	Maximálna rýchlosť vlaku (Vmax) nastavená príliš vysoko.	Nesprávna špecifická konfigurácia systému riadenia vlaku (personál údržby). Zavedenie nesprávnych údajov vo vlaku (vodič).	Železničný podnik	• Vymedziť postup schvaľovania konfigurácie údajov systému riadenia vlaku. • Vymedziť prevádzkový postup procesu vkladania údajov vodičom.	Explicitný odhad rizík	Áno	Kontroluje sa (exportované ŽP) Pozri aj časť C.16.4.2 v dodatku C.
2	Správa HAZOP R_X	Brzdné krivky (t. j. povolenie na jazdu) v údajoch konfigurácie systému riadenia vlaku sú málo prísne.	Postup pre určitú konfiguráciu systému riadenia vlaku závisí: • od bezpečnostných rozpätí zvolených pre brzdový systém vlaku; • od oneskorenia reakcie brzdového systému vlaku (toto priamo závisí od dĺžky vlaku, najmä	Železničný podnik	• Vo vymedzení systému správne stanoviť požiadavky na systém. • Zvoliť dostatočné bezpečnostné rozpätia pre brzdový systém konkrétneho vlaku.	Explicitný odhad rizík	Áno	Kontroluje sa (exportované ŽP) Pozri aj časť C.16.4.2 v dodatku C.

Tab. 7: Príklad záznamu o nebezpečenstve výrobcu palubného systému riadenia vlaku.

Čís. nebezp.	Pôvod	Opis nebezpečenstva	Doplňujúce informácie	Zodpovedný aktér	Bezpečnostné opatrenie	Použitá zásada akceptovania rizika	Exportované	Stav
			nákladného).					
3	Správa HAZOP R_X	• Maximálna rýchlosť vlaku (Vmax) nastavená príliš vysoko. • Brzdné krivky (t. j. povolenie na jazdu) v údajoch konfigurácie systému riadenia vlaku sú príliš benevolentné.	Neaktualizovanie priemeru kolesa vlaku v špecifickej konfigurácii systému riadenia vlaku (personál údržby).	Železničný podnik	• Vymedziť postup merania priemeru kolesa vlaku personálom údržby. • Vymedziť postup pravidelnej aktualizácie priemeru kolesa vlaku v systéme riadenia vlaku.	Explicitný odhad rizík	Áno	Kontroluje sa (exportované ŽP) Pozri aj časť C.16.4.2 v dodatku C.
			Chybný postup výrobcu v príprave a ukladaní údajov konfigurácie do systému riadenia vlaku.	Výrobca	Vymedziť postup vkladania priemeru kolesa vlaku do údajov konfigurácie systému riadenia vlaku.	Explicitný odhad rizík	Áno	Kontroluje sa postupom Px
4	Správa HAZOP R_X	Vjazd vlaku vysokou rýchlosťou (160 km/h, ak traťová návesť signalizuje voľno) na trať bez aktívneho subsystému zabezpečenia vlaku a bez signalizácie traťového návestného zariadenia.	Mohlo by sa kontrolovať len vodičovou bdelosťou. Vjazd do traťovej oblasti vybavenej ATP závisí od vodičovho potvrdenia pred miestom prechodu. Ak potvrdenie chýba, zabezpečovacie zariadenie vlaku automaticky zapne brzdy vlaku.	Manažér infraštruktúry	Manažér infraštruktúry musí zaistiť, aby vlaky, ktoré nie sú vybavené aktívnym subsystémom zabezpečenia vlaku, nemohli vojsť na príslušnú trať. Vymedziť postup riadenia premávky.	Explicitný odhad rizík	Áno	Kontroluje sa (exportované MI) Pozri aj časť C.16.4.2 v dodatku C.
				Železničný podnik	Zabezpečiť školenie vodičov o vstupovaní na úsek trate vybavený ATP.	Explicitný odhad rizík	Áno	Kontroluje sa (exportované ŽP) Pozri aj časť C.16.4.2 v dodatku C.
5	Správa HAZOP R_X	Vodičovi sa zobrazuje príliš vysoká nastavená maximálna rýchlosť vlaku (Vmax).	Informácie zobrazené na rozhraní vodiča sleduje palubný systém riadenia vlaku SIL 4, ktorý v prípade nezrovnalostí medzi zobrazenou a očakávanou hodnotou zapne núdzovú brzdu. V prípade nesúladu systému riadenia vlaku s povolením na jazdu zapne systém núdzovú brzdu.	Výrobca	Vyvinúť palubný subsystém zabezpečenia vlaku na úrovni SIL 4	Explicitný odhad rizík	Áno	Bezpečnostný preukaz preukazuje, že SIL 4 subsystému posúdil nezávislý posudzovateľ bezpečnosti
6	Správa	Vlak odchádza bez	Strata redundantnej architektúry palubného	Výrobca	Vyvinúť palubný subsystém	Explicitný	Áno	Bezpečnostný

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Tab. 7: Príklad záznamu o nebezpečenstve výrobcu palubného systému riadenia vlaku.

Čís. nebezp.	Pôvod	Opis nebezpečenstva	Doplňujúce informácie	Zodpovedný aktér	Bezpečnostné opatrenie	Použitá zásada akceptovania rizika	Exportované	Stav
	HAZOP R_X	rozhrania vodič - stroj	subsystému signalizácie, riadenia a zabezpečenia vlaku.		zabezpečenia vlaku na úrovni SIL 4	odhad rizík		preukaz preukazuje, že SIL 4 subsystém posúdil nezávislý posudzovateľ bezpečnosti
atď.								

C.16.4. Príklad záznamu o nebezpečenstve prenosu informácií iným aktérom

C.16.4.1 V tejto časti je uvedený príklad záznamu o nebezpečenstve určenému na prevod zistených nebezpečenstiev a súvisiacich bezpečnostných opatrení, ktoré posudzovaný aktér nedokáže implementovať, na ďalších aktérov. Pozri odsek [G 1] v časti 4.1.1.
Tento príklad je zhodný s príkladom v časti C.16.3. dodatku C. Jediný rozdiel je v tom, že všetky interné nebezpečenstvá a bezpečnostné opatrenia, ktoré by mohol posudzovaný aktér kontrolovať, sú odstránené.

C.16.4.2. Posledný stĺpec Tab. 8 je použitý na splnenie požiadavky v časti 4.2 prílohy I k nariadeniu o CSM. Existujú rôzne riešenia tejto úlohy. Jedným môže byť odkaz na dôkaz, ktorý použil aktér prijímajúci exportované bezpečnostné informácie. Iným by mohlo byť rokovanie dvoch aktérov, ktorého cieľom je spoločne nájsť vhodné riešenie obmedzenie súvisiacich rizík. Výsledky z takéhoto rokovania by sa dali uviesť v spoločnom dokumente (napr. v zápisnici z rokovania), v ktorej by aktér exportujúci informácie súvisiace s bezpečnosťou mohol poukázať na uzavretie súvisiacich nebezpečenstiev v tomto zázname o nebezpečenstve.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Tab. 8: Príklad záznamu o nebezpečenstve určenom na prevod informácií súvisiacich s bezpečnosťou iným aktérom.

Čís. neb.	Pôvod nebezpečenstva		Opis nebezpečenstva	Doplňujúce informácie	Zodpovedný aktér	Bezpečnostné opatrenie	Komentár príjemcu
	Č. v Tab. 7	Iné					
1	č. 1	Správa HAZOP R_X	Maximálna rýchlosť vlaku (Vmax) nastavená príliš vysoko.	Nesprávna špecifická konfigurácia vlakového subsystému (personál údržby). Nesprávne údaje vo vlaku (vodič).	Železničný podnik	• Vymedziť postup schvaľovania konfigurácie údajov systému riadenia vlaku. • Vymedziť prevádzkový postup procesu vkladania údajov vodičom.	• Konfigurácia údajov subsystému signalizačného, riadiaceho a zabezpečovacieho subsystému závisí od fyzikálnych charakteristík vozidiel. • Bezpečnostné rozpätia sa potom uplatnia koordinovane na tieto údaje medzi manažérom infraštruktúry a železničným podnikom. • Tieto údaje sa potom do subsystému načítajú v súlade s príslušnými postupmi výrobcu počas inštalácie, integrácie do vozidla a preberania signalizačného, riadiaceho a zabezpečovacieho subsystému. • Vodiči sú školení a vyhodnocovaní postupom D_P. • Vodičov hodnotí aj MI podľa predpisov o infraštruktúre MI.
2	č. 2	Správa HAZOP R_X	Brzdné krivky (t. j. povolenie na jazdu) v údajoch konfigurácie systému riadenia vlaku sú málo prísne.	Postup pre určitú konfiguráciu systému riadenia vlaku závisí: • od bezpečnostných rozpätí zvolených pre brzdový systém vlaku; • od oneskorenia reakcie brzdového systému vlaku (toto priamo závisí od dĺžky vlaku, najmä nákladného).	Železničný podnik	• Vo vymedzení systému správne stanoviť požiadavky na systém. • Zvoliť dostatočné bezpečnostné rozpätia pre brzdový systém konkrétneho vlaku.	Pozri komentár k trati 1.
3	č. 3	Správa HAZOP R_X	• Maximálna rýchlosť vlaku (Vmax) nastavená príliš vysoko. • Brzdné krivky (t. j. povolenie na jazdu) v údajoch konfigurácie systému riadenia vlaku sú málo prísne.	Neaktualizovanie priemeru kolesa vlaku v špecifickej konfigurácii systému riadenia vlaku (personál údržby).	Železničný podnik	• Vymedziť postup merania priemeru kolesa vlaku personálom údržby. • Vymedziť postup pravidelnej aktualizácie priemeru kolesa vlaku v subsystéme zabezpečenia vlaku.	• Údržba subsystému signalizácie, riadenia a zabezpečenia vlaku sa vykonáva v súlade s „postupom údržby MP_Z“. • Priemer kolesa vlaku sa načítava postupom P_W vo vymedzených intervaloch. • Školenia o procese vkladaní údajov a hodnotenia vodičov sa uskutočňujú „postupom P_{DE}“.
4	č. 4	Správa HAZOP R_X	Vjazd vlaku vysokou rýchlosťou (160 km/h, ak traťová návesť signalizuje voľno) na trať bez aktívneho systému	Mohlo by sa kontrolovať len vodičovou bdelosťou. Vjazd do traťovej oblasti vybavenej ATP závisí od vodičovho potvrdenia pred miestom prechodu. Ak potvrdenie	Manažér infraštruktúry	Manažér infraštruktúry musí zaistiť, aby vlaky, ktoré nie sú vybavené aktívnym subsystémom zabezpečenia vlaku, nemohli vojsť na príslušnú trať.	Riadenie premávky na infraštruktúre MI sa riadi súborom predpisov R_{TM}.

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Tab. 8: Príklad záznamu o nebezpečenstve určenom na prevod informácií súvisiacich s bezpečnosťou iným aktérom.

Čís. neb.	Pôvod nebezpečenstva		Opis nebezpečenstva	Doplňujúce informácie	Zodpovedný aktér	Bezpečnostné opatrenie	Komentár príjemcu
	Č. v Tab. 7	Iné					
			riadenia vlaku a bez signalizácie traťového návestného zariadenia.	chýba, zabezpečovacie zariadenie vlaku automaticky zapne brzdy vlaku.		Vymedziť postup riadenia premávky.	
					Železničný podnik	Zabezpečiť školenie vodičov o vstupovaní na úsek trate vybavený ATP.	• Vodiči sú pravidelne školení postupom P_{IM_DP} manažéra infraštruktúry. • MI hodnotí vodičov aj podľa predpisov (S_R) platných pre infraštruktúru MI.
atď.							

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

C.17. Príklad zoznamu všeobecných a podobných nebezpečenstiev v prevádzke železníc

C.17.1. ROSA (*Rail Optimisation Safety Analysis*) je projekt v rámci francúzsko-nemeckej spolupráce DEUFRAKO, ktorý bol pokusom o zostavenie všeobecného a podobného komplexného zoznamu nebezpečenstiev v štandardnej železničnej prevádzke. Cieľom a výzvou bolo vymedzenie týchto nebezpečenstiev na maximálnej možnej úrovni podrobnosti, kým tieto nebudú vyjadrovať špecifiká francúzskych a nemeckých železníc. Zoznam bol zostavený s využitím zoznamov nebezpečenstiev existujúcich v súčasnosti v oboch krajinách (SNCF a DB) a krížovo sa kontroloval aj so zoznamami nebezpečenstiev z iných krajín. Napriek oznámenému cieľu, že bude komplexný, všeobecný a podobný, je tu uvedený zoznam len ako orientačný príklad, ktorý môže slúžiť ako pomôcka pre aktérov, keď budú musieť zistiť nebezpečenstvá pre určitý projekt. Predpokladá sa, že nebezpečenstvá uvedené v tomto zozname bude pravdepodobne potrebné spresniť alebo doplniť, aby vyjadrovali špecifiká daného projektu.

C.17.2. Nebezpečenstvá uvedené v nasledujúcom návrhu sa nazývajú východiskovými (*starting point hazards,* SPH) v tom zmysle, že z nich by mohla vychádzať analýza dôsledkov aj analýza príčin na účely určenia bezpečnostných opatrení/zábran a požiadaviek na bezpečnosť na kontrolovanie nebezpečenstiev.

C.17.3. Zoznam nebezpečenstiev v projekte ROSA

SPH 01	Initial wrong Determination of speed limit (related to infrastructure)	Vstupné nesprávne určenie obmedzenia rýchlosti (súvisiace s infraštruktúrou)
SPH 02	Wrong Determination of speed limit (train related)	Nesprávne určenie obmedzenia rýchlosti (súvisiace s vlakom)
SPH 03	Wrong braking distance determined /wrong speed profile / wrong braking curves	Nesprávne určená brzdná dráha /nesprávny rýchlostný profil/ nesprávne brzdné krivky
SPH 04	Insufficient deceleration (physical causes)	Nedostatočné spomaľovanie (fyzikálne príčiny)
SPH 05	Wrong/ inappropriate speed/ brake command	Nesprávna/ nevhodná rýchlosť/ príkaz na brzdenie
SPH 06	Wrong speed registered (wrong speed train)	Zaznamenaná nesprávna rýchlosť (nesprávna rýchlosť vlaku)
SPH 07	Failure of speed limit communication	Porucha pri oznamovaní obmedzenia rýchlosti
SPH 08	Train rolls away	Vlak odchádza
SPH 09	Wrong travel direction/ intentional backwards moving - (combination of SPH 08 and SPH 14)	Nesprávny smer jazdy/ úmyselné cúvanie + (kombinácia SPH 08 a SPH 14)
SPH 10	Wrong absolute/ relative position registered	Zaznamenaná absolútne/relatívne nesprávna poloha
SPH 11	Train detection failure	Porucha detekcie vlaku
SPH 12	Loss of train integrity	Strata integrity vlaku
SPH 13	Possible wrong route for train	Možná nesprávna trasa vlaku
SPH 14	Failure in transmission/communication of timetable/MA (movement authority)	Porucha prenosu/ oznamovania cestovného poriadku/ MA (povolenie na jazdu)
SPH 15	Guideway structural failure	Konštrukčná porucha vodiacej koľajnice
SPH 16	Broken switch component	Zlomená súčiastka výhybky
SPH 17	Wrong switch command	Nesprávny príkaz výhybky

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

SPH 18	Wrong switch status	Nesprávna poloha výhybky
SPH 19	System object on guideway/ within CE (clearance envelope) (excl. Ballast)	Objekt systému na vodiacej koľajnici/ v prejazdnom priereze (okrem koľajového lôžka)
SPH 20	Foreign object on guideway/ within CE	Cudzí objekt na vodiacej koľajnici/v prejazdnom priereze
SPH 21	Road traffic user on LC	Účastník cestnej premávky na úrovňovom priecestí
SPH 22	Slipstream effects on ballast	Účinky prúdu vzduchu na koľajové lôžko
SPH 23	Aerodynamic forces impact on train	Vplyv aerodynamických síl na vlak
SPH 24	Train equipment/ element/ loading infringes CE of train	Vybavenie/ časť/ náklad vlaku vyčnieva z prejazdného prierezu vlaku
SPH 25	Inappropriate CE dimension for train (wayside)	Nevhodný rozmer prejazdného prierezu pre vlak
SPH 26	Wrong distribution of loading	Nesprávne rozdelenie zaťaženia
SPH 27	Broken wheel, broken axle	Zlomené koleso, zlomená náprava
SPH 28	Hot axle/ wheel/ bearing	Horúca náprava/ horúce koleso/ ložisko
SPH 29	Failure of bogie/ suspension, damping	Porucha podvozka/ pruženia, tlmenia
SPH 30	Failure of vehicle frame/ car body	Porucha rámu/ karosérie vozňa
SPH 31	Trespassing (security-aspect)	Neoprávnený vstup (z bezpečnostného hľadiska)
SPH 32	Authorised person crosses track	Oprávnená osoba prechádza cez trať
SPH 33	Staff working on track	Personál pracujúci na trati
SPH 34	Unauthorised person intrudes track (negligence)	Neoprávnená osoba vstupuje na trať (nedbalosť)
SPH 35	Person falls from platform edge onto track	Osoba padá z okraja nástupišťa na trať
SPH 36	Slipstream/ person too close to platform edge	Prúd vzduchu/ osoba je príliš blízko hrany nástupišťa
SPH 37	Staff working near track e.g. neighbouring track	Personál pracujúci v blízkosti trate, napr. na susednej koľaji
SPH 38	Person leaves train intentionally (excl. passenger exchange)	Osoba úmyselne vystupuje z vlaku (okrem nastupovania a vystupovania cestujúcich)
SPH 39	Person falls out of (side) door	Osoba vypadáva z (bočných) dvier
SPH 40	Person falls out of door in end wall	Osoba vypadáva zo zadných čelných dvier
SPH 41	Train leaves/ rolls with open doors (uninfringed CE)	Vlak odchádza/ posunuje sa s otvorenými dverami (nenarušujúc prejazdový prierez)
SPH 42	Person falls in gangway area between two cars	Osoba padá v priechode medzi dvoma vozňami
SPH 43	Passenger leans out of door	Cestujúci sa vykláňa z dvier
SPH 44	Passenger leans out of window	Cestujúci sa vykláňa z okna
SPH 45	Staff/ train attendant leans out of door	Personál/ obsluha vlaku sa vykláňa z dvier
SPH 46	Staff/ train attendant leans out of window	Personál/ obsluha vlaku sa vykláňa z okna
SPH 47	Shunting staff on vehicle leaning out from step	Posunovač sa vykláňa zo schodíka vozidla
SPH 48	Person falls/climbs from platform into gap between vehicle and platform	Osoba padá/lezie z nástupišťa do medzery medzi vozidlom a nástupišťom
SPH 49	Person falls out of/ leaves train without presence of platform	Osoba vypadáva/vystupuje z vlaku mimo nástupišťa
SPH 50	Person falls in door area at passenger exchange	Osoba padá v priestore dverí pri nastupovaní a vystupovaní cestujúcich

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

SPH 51	Train doors close with person in door area	Dvere vlaku sa zatvárajú a v priestore dverí je osoba
SPH 52	Train moves during passenger exchange	Vlak sa pohybuje počas nastupovania/vystupovania cestujúcich
SPH 53	Possibility of person hurt in train	Možnosť zranenej osoby vo vlaku
SPH 54	Fire/ explosion hazard (in/ at train) - accident category, Consequence of SPH 55, SPH 56)	Nebezpečenstvo požiaru/výbuchu (vo/na vlaku) – kategória nehôd, následkom SPH 55, SPH 56
SPH 55	Inappropriate temperature (in train)	Nevhodná teplota (vo vlaku)
SPH 56	Intoxication/ asphyxiation (in/ at train)	Otrava/udusenie (vo/na vlaku)
SPH 57	Electrocution (in/ at train)	Ohrozenie elektrickým prúdom (vo/na vlaku)
SPH 58	Person falls on platform (excluding passenger exchange)	Osoba padá na nástupišti (okrem nastupovania/vystupovania cestujúcich)
SPH 59	Inappropriate temperature (on platform)	Nevhodná teplota (na nástupišti)
SPH 60	Intoxication/ asphyxiation (on platform)	Otrava/udusenie (na nástupišti)
SPH 61	Electrocution (on platform)	Ohrozenie elektrickým prúdom (na nástupišti)

Európska železničná agentúra ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● Francúzsko ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu