



Evropska železniška agencija

**Zbirka primerov ocen tveganja in nekaterih možnih
orodij za podporo Uredbe o skupni varnostni
metodi**

Referenca v ERA:	ERA/GUI/02-2008/SAF
Različica v ERA:	1.1
Datum:	6. januar 2009

Dokument pripravila:	Evropska železniška agencija 160, Boulevard Harpignies BP 20392 F-59307 Valenciennes Cedex Francija
Vrsta dokumenta:	Priročnik
Status dokumenta:	Javni dokument

	Ime in priimek	Funkcija
Objavil:	Marcel VERSLYPE	izvršni direktor
Pregledala:	Anders LUNDSTRÖM Thierry BREYNE	vodja enote za varnost vodja sektorja za oceno varnosti
Napisal: (Avtor)	Dragan JOVIČIĆ	enota za varnost – vodja projekta



INFORMACIJE O DOKUMENTU

Podatki o spremembah

Tabela 1: Status dokumenta

Različica Datum	Avtor(-ji)	Številka oddelka	Opis spremembe
Star naslov in struktura dokumenta: „Navodila za uporabo priporočila o prvi skupini skupnih varnostnih metod“			
Različica navodil 0.1 15. 2. 2007	Dragan JOVIČIĆ	Vse	Prva različica „navodil za uporabo“, povezana z različico 1.0 „priporočil o prvi skupini skupnih varnostnih metod“. To je tudi prva različica dokumenta, predložena v uradni pregled delovni skupini za skupno varnostno metodo.
Različica navodil 0.2 7. 6. 2007	Dragan JOVIČIĆ	Vse	Preureditev dokumenta, da bi ustrežal strukturi različice 4.0 priporočila o skupni varnostni metodi. Posodobitev glede na <u>postopek uradne revizije</u> različice 1.0 priporočila, ki jo je izvedla delovna skupina za skupno varnostno metodo.
		Vse	Posodobitev dokumenta z dodatnimi informacijami, zbranimi na internih srečanjih ERA, ter zahtevami projektne in delovne skupine za skupno varnostno metodo glede oblikovanja novih točk.
		Slika 12	Sprememba slike, ki predstavlja „okvir obvladovanja tveganja za prvo skupino skupnih varnostnih metod“, v skladu s pripombami, podanimi v okviru revizije in terminologijo ISO.
Različica navodil 0.3 20. 7. 2007	Dragan JOVIČIĆ	Dodatki	Preureditev obstoječih dodatkov in oblikovanje novih. Nov dodatek za združitev vseh diagramov, ki prikazujejo in omogočajo branje ter razumevanje Priročnika.
		Vsi oddelki	Dokument je bil posodobljen, da: <ul style="list-style-type: none"> • se čim bolj razvijejo obstoječi oddelki x; • se podrobneje opredeli, kaj pomeni „dokazovanje skladnosti sistema z varnostnimi zahtevami“; • se vzpostavi povezava s ciklom V CENELEC (tj. sliki 8 in 10 iz standarda EN 50126); • se nadalje razvije potreba po sodelovanju in usklajevanju med različnimi udeleženci železniškega sektorja, katerih dejavnosti lahko vplivajo na varnost železniškega sistema; • se pojasnijo dokazila (npr. dnevnik nevarnosti in varnostna analiza), ki naj bi ocenjevalnim organom prikazala pravilno uporabo postopka ocene tveganja skupne varnostne metode. Dokument je bil posodobljen tudi v skladu s prvim notranjim pregledom Agencije.
Različica navodil 0.4 16. 11. 2007	Dragan JOVIČIĆ	Vsi oddelki	Dokument je bil posodobljen po <u>postopku uradne revizije</u> v skladu s pripombami, ki so jih v zvezi z različico 0.3 predložili in se o njih prek telefona sporazumeli naslednji člani delovne skupine za skupno varnostno metodo ali organizacije: <ul style="list-style-type: none"> • belgijski, španski, finski, norveški, francoski in danski nacionalni varnostni organi; • SIEMENS (član združenja UNIFE); • norveški upravljavec železniške infrastrukture (Jernbaneverket – član Evropskega združenja upravljavcev železniške infrastrukture).
Različica navodil 0.5 27. 2. 2008	Dragan JOVIČIĆ	Vsi oddelki	Dokument je bil posodobljen v skladu s pripombami, ki so jih v zvezi z različico 0.3 predložili in se o njih prek telefona sporazumeli naslednji člani delovne skupine za skupno varnostno metodo ali organizacije: <ul style="list-style-type: none"> • Skupnost evropskih železnic, • nizozemski nacionalni varnostni organ.
		Vsi oddelki	Dokument je bil posodobljen v skladu s podpisano različico priporočila o skupni varnostni metodi.

Tabela 1: Status dokumenta

Različica Datum	Avtor(-ji)	Številka oddelka	Opis spremembe
			Dokument je bil posodobljen v skladu s pripombami, ki sta jih v okviru notranjega pregleda Agencije predložila Christophe CASSIR in Marcus ANDERSSON.
		Vsi oddelki Dodatki	Popolno preštevilčenje odstavkov v dokumentu glede na priporočilo. Vključeni so primeri uporabe priporočila o skupni varnostni metodi.
Nov naslov in struktura dokumenta: „Zbirka primerov ocen tveganja in nekaterih možnih orodij za podporo Uredbe o skupni varnostni metodi“			
Različica priročnika 0.1 23. 5. 2008	Dragan JOVIČIĆ	Vse	Prva različica dokumenta je nastala zaradi razdelitve različice 0.5 „navodil za uporabo“ na dva dopolnjujoča se dokumenta.
Različica priročnika 0.2 3. 9. 2008	Dragan JOVIČIĆ	Vse	Posodobitev dokumenta v skladu z: <ul style="list-style-type: none"> • Uredbo Evropske komisije o skupni varnostni metodi {Ref. 3}; • pripombami z delavnice 1. julija 2008, na kateri so sodelovali člani Odbora za varnost in interoperabilnost železniškega prometa (RISC); • pripombami članov delovne skupine za skupno varnostno metodo (norveški in finski nacionalni varnostni organ, nacionalni varnostni organ Združenega kraljestva, francoski nacionalni varnostni organ, Skupnost evropskih železnic, Evropsko združenje upravljavcev železniške infrastrukture, Jens BRABAND [UNIFE] ter Stéphane ROMEI [UNIFE]).
Različica priročnika 1.0 10. 12. 2008	Dragan JOVIČIĆ	Vse	Posodobitev dokumenta v skladu z Uredbo Evropske komisije o skupni varnostni metodi za ovrednotenje in oceno tveganja {Ref. 3}, ki jo je sprejel Odbor za varnost in interoperabilnost železniškega prometa na plenarnem zasedanju 25. novembra 2008.
Različica priročnika 1.1 6. januar 2009	Dragan JOVIČIĆ	Vse	Posodobitev dokumenta v skladu s pripombami v zvezi z Uredbo o skupni varnostni metodi, ki sta jih predložili pravna in jezikovna služba Evropske komisije.

Kazalo

INFORMACIJE O DOKUMENTU	2
Podatki o spremembah	2
Kazalo 4	
Seznam slik	5
Seznam tabel.....	6
0. UVOD.....	7
0.1. Področje uporabe.....	7
0.2. Zunaj področja uporabe	7
0.3. Načelo tega dokumenta	8
0.4. Opis dokumenta	8
0.5. Referenčni dokumenti	9
0.6. Standardne opredelitve pojmov, izrazi in kratice	10
0.7. Posebne opredelitve pojmov.....	10
0.8. Posebni izrazi in kratice	10
OBRAZLOŽITEV ČLENOV UREDBE O SKUPNI VARNOSTNI METODI.....	12
Člen 1. Namen.....	12
Člen 2. Področje uporabe.....	12
Člen 3. Opredelitve pojmov	14
Člen 4. Pomembne spremembe.....	16
Člen 4(1).....	16
Člen 4(2).....	16
Člen 5. Postopek upravljanja s tveganji	17
Člen 6. Neodvisno ocenjevanje	18
Člen 7. Poročila o varnostni oceni.....	19
Člen 8. Upravljanje nadzora tveganja/notranje in zunanje revizije.....	20
Člen 9. Povratne informacije in tehnični napredek.....	21
Člen 10. Začetek veljavnosti.....	22
PRILOGA I – OBRAZLOŽITEV POSTOPKA IZ UREDBE O SKUPNI VARNOSTNI METODI.....	23
1. SPLOŠNA NAČELA, KI SE UPORABLJAJO V POSTOPKU UPRAVLJANJA S TVEGANJI.....	23
1.1. Splošna načela in obveznosti	23
1.2. Upravljanje vmesnikov	30
2. OPIS POSTOPKA OCENJEVANJA TVEGANJA.....	33
2.1. Splošni opis – ujemanje med postopkom ocenjevanja tveganja po skupni varnostni metodi in ciklom V CENELEC.....	33
2.2. Določanje nevarnosti.....	40
2.3. Uporaba kodeksov ravnanja in ovrednotenje tveganj.....	43
2.4. Uporaba referenčnih sistemov in ovrednotenje tveganja	44
2.5. Eksplicitna ocena in ovrednotenje tveganja.....	45
3. DOKAZOVANJE SKLADNOSTI Z VARNOSTNIMI ZAHTEVAMI.....	49
4. UPRAVLJANJE Z NEVARNOSTMI	52

4.1.	Postopek upravljanja z nevarnostmi	52
4.2.	Izmenjava informacij	53
5.	DOKAZILA O UPORABI POSTOPKA UPRAVLJANJA S TVEGANJI	56
	PRILOGA II K UREDBI O SKUPNI VARNOSTNI METODI	59
	Merila, ki jih morajo izpolnjevati ocenjevalni organi	59
	DODATEK A: DODATNA POJASNILA	60
A.1.	Uvod	60
A.2.	Razvrstitev nevarnosti	60
A.3.	Merilo za sprejemljivost tveganja za tehnične sisteme (MST-TS)	60
A.4.	Dokazi v zvezi z oceno varnosti	70
	DODATEK B: PRIMERI TEHNIK IN ORODIJ ZA PODPORO POSTOPKA OCENJEVANJA TVEGANJA	73
	DODATEK C: PRIMERI	74
C.1.	Uvod	74
C.2.	Primeri uporabe meril za pomembno spremembo iz člena 4(2)	74
C.3.	Primeri vmesnikov med udeleženci v železniškem sektorju	75
C.4.	Primeri metod za določitev splošno sprejemljivih tveganj	76
C.5.	Primer ocene tveganja pomembne organizacijske spremembe	77
C.6.	Primer ocene tveganja pomembne operativne spremembe – sprememba ur vožnje	79
C.7.	Primer ocene tveganja pomembne tehnične spremembe (UVS)	81
C.8.	Primer švedske smernice BVH 585.30 za oceno tveganja železniških predorov	84
C.9.	Primer ocene tveganja na ravni sistema za podzemno železnico v Københavnu	86
C.10.	Primer smernice Medvladne organizacije za mednarodni železniški promet (OTIF) za izračun tveganja zaradi prevoza nevarnega blaga po železnici	89
C.11.	Primer ocene tveganja v zvezi odobritvijo nove vrste tirnih vozil	91
C.12.	Primer ocene tveganja pomembne operativne spremembe – vlak upravlja le strojevodja	93
C.13.	Primer uporabe referenčnega sistema za izpeljavo varnostnih zahtev za nove sisteme elektronskih zapornic v Nemčiji	96
C.14.	Primer eksplicitnega merila za sprejemljivost tveganja za radijsko upravljanje vlaka (FFB) v Nemčiji	97
C.15.	Primer preskusa uporabe merila za sprejemljivost tveganja za tehnične sisteme	98
C.16.	Primeri mogočih struktur evidence nevarnosti	99
C.17.	Primer splošnega seznama nevarnosti za delovanje železnice	107

Seznam slik

Slika 1 :	Okvir obvladovanja tveganja iz Uredbe o skupni varnostni metodi {Ref. 2}	24
Slika 2 :	Usklajen sistem varnega upravljanja in skupna varnostna metoda	26
Slika 3 :	Primeri odvisnosti med varnostnimi analizami (oblikovani na podlagi slike 9 iz standarda EN 50129)	28
Slika 4 :	Poenostavljen cikel V s slike 10 standarda EN 50126	33
Slika 5 :	Slika 10 cikla V standarda EN 50126 (življenjski cikel sistema iz standarda CENELEC)	34
Slika 6 :	Izbor ustreznih varnostnih ukrepov za nadzor tveganj	39
Slika 7 :	Splošno sprejemljiva tveganja	41
Slika 8 :	Filtriranje nevarnosti, povezanih s splošno sprejemljivim tveganjem	41
Slika 9 :	Piramida meril za sprejemljivost tveganja	47

Slika 10 : Slika A.4 iz EN 50129: opredelitev nevarnosti glede na mejo sistema	49
Slika 11 : Izpeljava varnostnih zahtev za faze nižje stopnje	50
Slika 12 : Strukturirana dokumentacijska hierarhija	56
Slika 13 : Redundantna arhitektura za tehnični sistem	62
Slika 14 : Shematski prikaz preskusa uporabe merila za sprejemljivost tveganja za tehnične sisteme	64
Slika 15 : Primer nepomembne spremembe – telefonsko sporočilo za nadzorovanje nivojskega prehoda ...	74
Slika 16 : Sprememba zanke ob progi s podsistemom s signalom radio in-fill	82

Seznam tabel

Tabela 1: Status dokumenta.....	2
Tabela 2: Tabela referenčnih dokumentov.....	9
Tabela 3: Tabela izrazov	10
Tabela 4: Tabela kratic	10
Tabela 1: Značilen primer kalibrirane matrike tveganja	68
Tabela 2: Primer evidence nevarnosti za organizacijsko spremembo iz oddelka C.5. Dodatka C.....	101
Tabela 7: Primer evidence nevarnosti proizvajalca za podsistem upravljanja - vodenja na vlaku	102
Tabela 3: Primer evidence nevarnosti za prenos informacij v zvezi z varnostjo drugim udeležencem	105

0. UVOD

0.1. Področje uporabe

0.1.1. Cilj tega dokumenta je zagotoviti dodatna pojasnila v zvezi z „Uredbo Komisije o sprejetju skupne varnostne metode za ovrednotenje in oceno tveganja iz člena 6(3)(a) Direktive 2004/49/ES Evropskega parlamenta in Sveta“ {Ref. 3}. Uredba se bo v tem dokumentu imenovala „Uredba o skupni varnostni metodi“.

0.1.2. Ta dokument ni pravno zavezujoč in njegova vsebina se ne sme razlagati kot edini način za izpolnjevanje zahtev iz skupne varnostne metode. Cilj tega dokumenta je dopolniti priročnik za uporabo Uredbe o skupni varnostni metodi {Ref. 4} v zvezi s tem, kako se lahko uporabi in izvaja postopek iz Uredbe o skupni varnostni metodi. Zagotavlja dodatne praktične informacije, pri čemer na noben način ne narekuje obveznih postopkov, ki bi jih bilo treba spoštovati, in ne vzpostavlja pravno zavezujoče prakse. Te informacije so lahko uporabne za vse udeležence⁽¹⁾, katerih dejavnosti lahko vplivajo na varnost železniških sistemov in ki morajo neposredno ali posredno uporabljati skupno varnostno metodo. Dokument navaja primere ocen tveganja in nekatera možna orodja, ki podpirajo uporabo skupne varnostne metode. Ti primeri so predloženi le kot nasvet in pomoč. Udeleženci lahko uporabijo nadomestne metode ali še naprej uporabljajo svoje obstoječe metode in orodja za skladnost s skupno varnostno metodo, če menijo, da so primernejši. Poleg tega primeri in dodatne informacije, ki so navedeni v tem dokumentu, niso izčrpani in ne zajemajo vseh možnih razmer, v katerih se predlagajo pomembne spremembe, zato je lahko dokument izključno informativen.

0.1.3. Ta informativni dokument se bere le kot dodatna pomoč pri uporabi Uredbe o skupni varnostni metodi. Kadar se ta dokument uporablja, se mora brati skupaj z Uredbo o skupni varnostni metodi {Ref. 3} in z njo povezanim priročnikom {Ref. 4}, da se dodatno olajša uporaba skupne varnostne metode, vendar Uredbe o skupni varnostni metodi ne nadomešča.

0.1.4. Dokument je pripravila Evropska železniška agencija (ERA) s pomočjo železniškega združenja in strokovnjakov nacionalnih varnostnih organov iz delovne skupine za skupno varnostno metodo. Predstavlja dobro zasnovano zbirko zamisli in informacij, ki jih je Agencija zbrala na internih sestankih ter srečanjih z delovno skupino in projektnimi skupinami za skupno varnostno metodo. Evropska železniška agencija bo dokument po potrebi pregledala in posodobila, da bo izražal napredek na področju evropskih standardov, spremembe Uredbe o skupni varnostni metodi za oceno tveganja in morebitne nove izkušnje v zvezi z uporabo Uredbe o skupni varnostni metodi. Ker v času pisanja ni mogoče določiti časovnega okvira tega postopka revizije, se mora bralec glede informacij o najnovejši izdaji tega dokumenta, ki je na voljo, obrniti na Evropsko železniško agencijo.

0.2. Zunaj področja uporabe

0.2.1. Ta dokument ne zagotavlja navodil, kako organizirati, upravljati ali načrtovati (in izdelati) železniški sistem ali njegove sestavne dele. Prav tako ne opredeljuje pogodbenih sporazumov in dogovorov o uporabi postopka obvladovanja tveganja, ki lahko obstajajo med

⁽¹⁾ Zadevni udeleženci so naročniki iz člena 2(r) Direktive 2008/57/ES o interoperabilnosti železniškega sistema v Skupnosti ali proizvajalci, oboji v Uredbi imenovani „predlagatelji“, ali njihovi dobavitelji in izvajalci storitev.

nekaterimi udeleženci. Pogodbeni dogovori pri posameznih projektih ne spadajo niti v področje uporabe Uredbe o skupni varnostni metodi niti na področje z njo povezanega priročnika in tega dokumenta.

0.2.2. Kljub temu so lahko dogovori, ki ne spadajo v področje uporabe tega dokumenta in o katerih se sporazumejo ustrezni udeleženci, zapisani v ustreznih pogodbah na začetku projekta, vendar brez poseganja v določbe skupne varnostne metode. To lahko na primer zajema:

- (a) stroške, povezane z obvladovanjem tveganj v zvezi z varnostjo na vmesnikih med udeleženci;
- (b) stroške, povezane s prenosom nevarnosti in z njimi povezanih varnostnih ukrepov na udeležence, ki na začetku projekta še niso znani;
- (c) način obvladovanja sporov, ki lahko nastanejo med projektom;
- (d) itd.

Če med razvojem projekta nastanejo nesoglasja ali spor med predlagateljem in njegovimi podizvajalci, se je pri reševanju kakršnega koli spora mogoče sklicevati na ustrezne pogodbe.

0.3. Načelo tega dokumenta

0.3.1. Čeprav se morda zdi, da je ta dokument namenjen samostojnemu branju, je treba poudariti, da ne nadomešča Uredbe o skupni varnostni metodi {Ref. 3}. Za lažje sklicevanje je v dokumentu citiran vsak člen Uredbe o skupni varnostni metodi. Ustrezen člen je po potrebi predhodno obrazložen v priročniku za uporabo Uredbe o skupni varnostni metodi {Ref. 4}. Kadar se to zdi potrebno, so v odstavkih, ki sledijo, navedene dodatne informacije, ki pomagajo pri nadaljnem razumevanju Uredbe o skupni varnostni metodi.

0.3.2. The articles and their underlying paragraphs from the CSM Regulation are copied in a text box in the present document using the "Bookman Old Style" Italic Font, the same as the present text. That formatting enables to easily distinguish the original text of the CSM Regulation {Ref. 3} from the additional explanations provided in this document. The text from the guide for the application of the CSM Regulation {Ref. 4} is not copied in the present document.

0.3.3. V pomoč bralcu je struktura tega dokumenta določena glede na strukturo Uredbe o skupni varnostni metodi in z njo povezanega priročnika.

0.4. Opis dokumenta

0.4.1. Dokument je razdeljen na naslednje dele:

- (a) poglavje 0. ki določa področje uporabe dokumenta in vsebuje seznam referenčnih dokumentov;
- (b) prilogi I in II zagotavljata dodatne informacije za ustrezne oddelke Uredbe o skupni varnostni metodi {Ref. 3} in z njo povezanega priročnika {Ref. 4};
- (c) novi dodatki podrobneje predstavljajo nekatere posebne vidike in ponazarjajo primere.

0.5. Referenčni dokumenti

Tabela 2: Tabela referenčnih dokumentov

{Ref. št.}	Naslov	Referenca	Različica
{Ref. 1}	Direktiva 2004/49/ES Evropskega parlamenta in Sveta z dne 29. aprila 2004 o varnosti na železnicah Skupnosti ter o spremembi Direktive Sveta 95/18/ES o izdaji licence prevoznikom v železniškem prometu in Direktive 2001/14/ES o dodeljevanju železniških infrastrukturnih zmogljivosti, naložitvi uporabnin za uporabo železniške infrastrukture in podeljevanju varnostnega spričevala (Direktiva o varnosti na železnici)	2004/49/ES UL L 164, 30.4.2004, str. 44, kakor je bila popravljen v UL L 220, 21.6.2004, str. 16.	–
{Ref. 2}	Direktiva 2008/57/ES Evropskega parlamenta in Sveta z dne 17. junija 2008 o interoperabilnosti železniškega sistema v Skupnosti	2008/57/ES UL L 191, 18.7.2008, str. 1.	–
{Ref. 3}	Uredba Komisije (ES) št. .../.. z dne [...] o sprejetju skupne varnostne metode za ovrednotenje in oceno tveganja iz člena 6(3)(a) Direktive 2004/49/ES Evropskega parlamenta in Sveta	xxxx/yy/ES	glasoval Odbor za varnost in interoperabilnost železniškega prometa 25. novembra 2008
{Ref. 4}	Priročnik za uporabo Uredbe Komisije o sprejetju skupne varnostne metode za ovrednotenje in oceno tveganja iz člena 6(3)(a) Direktive o varnosti na železnici	ERA/GUI/01-2008/SAF	1.0
{Ref. 5}	Direktiva 2008/57/ES Evropskega parlamenta in Sveta z dne 17. junija 2008 o interoperabilnosti železniškega sistema v Skupnosti	2008/57/ES UL L 191, 18.7.2008, str. 1.	–
{Ref. 6}	Sistem varnega upravljanja – Merila za oceno za prevoznike v železniškem prometu in upravljavce železniške infrastrukture	Merila za oceno sistemov varnega upravljanja Del A Varnostna spričevala in pooblastila	31. 5. 2007
{Ref. 7}	Železniške aplikacije – Sistemi komunikacije, signalizacije in obdelave – Varnost v zvezi z elektronskimi sistemi signalizacije	EN 50129	februar 2003
{Ref. 8}	Železniške aplikacije – Specifikacije in prikaz zanesljivosti, razpoložljivosti, vzdrževalnosti in varnosti – Del 1: sam standard	EN 50126-1	september 2006
{Ref. 9}	Železniške aplikacije – Specifikacije in prikaz zanesljivosti, razpoložljivosti, vzdrževalnosti in varnosti – Del 2: Priročnik za uporabo standarda EN 50126-1 za varnost	EN 50126-2 (smernica)	končni osnutek (avgust 2006)
{Ref. 10}	Splošna smernica za izračun tveganja, povezanega z železniškim prevozom nevarnega blaga	Smernica Medvladne organizacije za mednarodni železniški promet, ki jo je odobril odbor strokovnjakov za Pravilnik o mednarodnem železniškem prevozu nevarnega blaga	24. november 2005
{Ref. 11}	Merilo za sprejemljivost tveganja za tehnične sisteme	Obvestilo 01/08	1.1 (25. 1. 2008)

Tabela 2: Tabela referenčnih dokumentov

{Ref. št.°} Naslov	Referenca	Različica
{Ref. 12} Enota za varnost ERA: Študija izvedljivosti – „Porazdelitev varnostnih ciljev (na podsisteme tehničnih specifikacij za interoperabilnost) in uskladitev tehničnih specifikacij za interoperabilnost z vidika varnosti“ WP1.1 – Ocena izvedljivosti za porazdelitev skupnih varnostnih ciljev	WP1.1	1.0
{Ref. 13} „Železniške aplikacije – Sistem za razvrščanje železniških vozil – Del 4: EN 0015380, del 4: Funkcionalne skupine“	EN 0015380, del 4	

0.6. Standardne opredelitve pojmov, izrazi in kratice

- 0.6.1. Splošne opredelitve pojmov, izraze in kratice, ki se uporabljajo v tem dokumentu, je mogoče poiskati v klasičnem slovarju.
- 0.6.2. Novi pojmi, izrazi in kratice v tem priročniku so opredeljeni v razdelkih spodaj.

0.7. Posebne opredelitve pojmov

- 0.7.1. Glej Člen 3.

0.8. Posebni izrazi in kratice

- 0.8.1. Ta razdelek opredeljuje nove posebne izraze in kratice, ki se v tem dokumentu pogosto uporabljajo.

Tabela 3: Tabela izrazov

Izraz	Opredelitev
Agencija	Evropska železniška agencija (ERA)
priročnik	„priročnik za uporabo Uredbe Komisije (ES) št.°.../.. z dne [...] o sprejetju skupne varnostne metode za ovrednotenje in oceno tveganja iz člena 6(3)(a) Direktive 2004/49/ES Evropskega parlamenta in Sveta“
Uredba o skupni varnostni metodi	„Uredba Komisije (ES) št.°.../.. z dne [...] o sprejetju skupne varnostne metode za ovrednotenje in oceno tveganja iz člena 6(3)(a) Direktive 2004/49/ES Evropskega parlamenta in Sveta“ {Ref. 3}

Tabela 4: Tabela kratic

Kratice	Pomen
UVS	upravljanje - vodenje in signalizacija
SVM	skupna(-e) varnostna(-e) metoda(-e)
SVC	skupni varnostni cilji
EK	Evropska komisija
ERA	Evropska železniška agencija
UŽI	upravljavce(-vci) železniške infrastrukture

Tabela 4: Tabela kratic

Kratica	Pomen
NOV	neodvisni ocenjevalec varnosti
OTIF	Medvladna organizacija za mednarodni železniški promet
DČ	država članica
PO	priglašeni organ
NVO	nacionalni varnostni organ
PVK	postopek vodenja kakovosti
SVK	sistem vodenja kakovosti
RISC	Odbor za varnost in interoperabilnost železniškega prometa
PŽP	prevoznik(i) v železniškem prometu
PVU	postopek varnega upravljanja
SVU	sistem varnega upravljanja
VŽP	varnost v železniških predorih
SD	se dopolni
TSI	tehnične specifikacije za interoperabilnost

OBRAZLOŽITEV ČLENOV UREDBE O SKUPNI VARNOSTNI METODI

Člen 1. Namen

Člen 1(1)

This Regulation establishes a common safety method on risk evaluation and assessment (CSM) as referred to in Article 6(3)(a) of Directive 2004/49/EC.

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

Člen 1(2)

The purpose of the CSM on risk evaluation and assessment is to maintain or to improve the level of safety on the Community's railways, when and where necessary and reasonably practicable. The CSM shall facilitate the access to the market for rail transport services through harmonisation of:

- (a) the risk management processes used to assess the safety levels and the compliance with safety requirements;*
- (b) the exchange of safety-relevant information between different actors within the rail sector in order to manage safety across the different interfaces which may exist within this sector;*
- (c) the evidence resulting from the application of a risk management process.*

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

Člen 2. Področje uporabe

Člen 2(1)

The CSM on risk evaluation and assessment shall apply to any change of the railway system in a Member State, as referred to in point (2) (d) of Annex III to Directive 2004/49/EC, which is considered to be significant within the meaning of Article 4 of this Regulation. Those changes may be of a technical, operational or organisational nature. As regards organisational changes, only those changes which could impact the operating conditions shall be considered.

[G 1] Skupna varnostna metoda se uporablja za celoten železniški sistem in zajema oceno naslednjih sprememb železniškega sistema, če so z uporabo Člen 4 ovrednotene kot pomembne:

- (a) izgradnje novih prog ali spremembe obstoječih prog;
- (b) uvedbe novih in/ali preoblikovanih tehničnih sistemov;
- (c) operativnih sprememb (kot so nova ali spremenjena operativna pravila in postopki vzdrževanja);

- (d) sprememb v okviru organizacij prevoznika v železniškem prometu/upravljavca železniške infrastrukture.

Izraz „sistem“ se v okviru skupne varnostne metode nanaša na vse vidike sistema, ki med drugim vključujejo njegov razvoj, delovanje, vzdrževanje itd. do umika iz obratovanja ali odstranitve.

[G 2] Skupna varnostna metoda zajema pomembne spremembe:

- (a) „majhnih in preprostih“ sistemov, ki so lahko sestavljeni iz nekaj tehničnih podsistemov ali elementov, ter
(b) „velikih in kompleksnejših“ sistemov (ki lahko na primer vključujejo postaje in predore).

Člen 2(2)

Where the significant changes concern structural sub-systems to which Directive 2008/57/EC applies, the CSM on risk evaluation and assessment shall apply:

- (a) *if a risk assessment is required by the relevant technical specification for interoperability (TSI). In this case the TSI shall, where appropriate, specify which parts of the CSM apply;*
(b) *to ensure safe integration of the structural subsystems to which the TSIs apply into an existing system, by virtue of Article 15(1) of Directive 2008/57/EC.*

However, application of the CSM in the case referred to in point (b) of the first subparagraph must not lead to requirements contradictory to those laid down in the relevant TSIs which are mandatory.

Nevertheless if the application of the CSM leads to a requirement that is contradictory to that laid down in the relevant TSI, the proposer shall inform the Member State concerned which may decide to ask for a revision of the TSI in accordance with Article 6(2) or Article 7 of Directive 2008/57/EC or a derogation in accordance with Article 9 of that Directive.

- [G 1] V skladu z Direktivo o varnosti na železnici {Ref. 1} in Direktivo o interoperabilnosti železniškega sistema {Ref. 2} mora biti na primer nova vrsta tirnega vozila za progo za visoke hitrosti skladna s tehničnimi specifikacijami za interoperabilnost tirnega vozila za visoke hitrosti. Čeprav tehnične specifikacije za interoperabilnost zajemajo večino ocenjevanega sistema, ključno vprašanje človeškega dejavnika v zvezi s kabino strojevodje v tehnične specifikacije za interoperabilnost ni vključeno. Zato se za zagotovitev, da so vse smiselno predvidljive nevarnosti, povezane z vprašanji človeškega dejavnika (tj. vmesniki med strojevodjo, tirnim vozilom in ostalim železniškim sistemom), opredeljene in ustrezno nadzorovane, uporabi postopek skupne varnostne metode.

Člen 2(3)

This Regulation shall not apply to:

- (a) metros, trams and other light rail systems;*
- (b) networks that are functionally separate from the rest of the railway system and intended only for the operation of local, urban or suburban passenger services, as well as railway undertakings operating solely on these networks;*
- (c) privately owned railway infrastructure that exists solely for use by the infrastructure owner for its own freight operations;*
- (d) heritage vehicles that run on national networks providing that they comply with national safety rules and regulations with a view to ensuring safe circulation of such vehicles;*
- (e) heritage, museum and tourist railways that operate on their own network, including workshops, vehicles and staff.*

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

Člen 2(4)

This Regulation shall not apply to systems and changes, which, on the date of entry into force of this Regulation, are projects at an advanced stage of development within the meaning of Article 2 (t) of Directive 2008/57/EC.

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

Člen 3. Opredelitve pojmov

For the purpose of this Regulation the definitions in Article 3 of Directive 2004/49/EC shall apply.

The following definitions shall also apply:

- (1) 'risk' means the rate of occurrence of accidents and incidents resulting in harm (caused by a hazard) and the degree of severity of that harm (EN 50126-2);*
- (2) 'risk analysis' means systematic use of all available information to identify hazards and to estimate the risk (ISO/IEC 73);*
- (3) 'risk evaluation' means a procedure based on the risk analysis to determine whether the acceptable risk has been achieved (ISO/IEC 73);*
- (4) 'risk assessment' means the overall process comprising a risk analysis and a risk evaluation (ISO/IEC 73);*
- (5) 'safety' means freedom from unacceptable risk of harm (EN 50126-1);*
- (6) 'risk management' means the systematic application of management policies, procedures and practices to the tasks of analysing, evaluating and controlling risks (ISO/IEC 73);*
- (7) 'interfaces' means all points of interaction during a system or subsystem life cycle, including operation and maintenance where different actors of the rail sector will work together in order to manage the risks;*
- (8) 'actors' means all parties which are, directly or through contractual arrangements, involved in the application of this Regulation pursuant to Člen 5(2);*
- (9) 'safety requirements' means the safety characteristics (qualitative or quantitative) of a system and its operation (including operational rules) necessary in order to meet legal or company safety targets;*

- (10) 'safety measures' means a set of actions either reducing the rate of occurrence of a hazard or mitigating its consequences in order to achieve and/or maintain an acceptable level of risk;
- (11) 'proposer' means the railway undertakings or the infrastructure managers in the framework of the risk control measures they have to implement in accordance with Article 4 of Directive 2004/49/EC, the contracting entities or the manufacturers when they invite a notified body to apply the "EC" verification procedure in accordance with Article 18(1) of Directive 2008/57/EC or the applicant of an authorisation for placing in service of vehicles;
- (12) 'safety assessment report' means the document containing the conclusions of the assessment performed by an assessment body on the system under assessment;
- (13) 'hazard' means a condition that could lead to an accident (EN 50126-2);
- (14) 'assessment body' means the independent and competent person, organisation or entity which undertakes investigation to arrive at a judgment, based on evidence, of the suitability of a system to fulfil its safety requirements;
- (15) 'risk acceptance criteria' means the terms of reference by which the acceptability of a specific risk is assessed; these criteria are used to determine that the level of a risk is sufficiently low that it is not necessary to take any immediate action to reduce it further;
- (16) 'hazard record' means the document in which identified hazards, their related measures, their origin and the reference to the organisation which has to manage them are recorded and referenced;
- (17) 'hazard identification' means the process of finding, listing and characterising hazards (ISO/IEC Guide 73);
- (18) 'risk acceptance principle' means the rules used in order to arrive at the conclusion whether or not the risk related to one or more specific hazards is acceptable;
- (19) 'code of practice' means a written set of rules that, when correctly applied, can be used to control one or more specific hazards;
- (20) 'reference system' means a system proven in use to have an acceptable safety level and against which the acceptability of the risks from a system under assessment can be evaluated by comparison;
- (21) 'risk estimation' means the process used to produce a measure of the level of risks being analysed, consisting of the following steps: estimation of frequency, consequence analysis and their integration (ISO/IEC 73);
- (22) 'technical system' means a product or an assembly of products including the design, implementation and support documentation; the development of a technical system starts with its requirements specification and ends with its acceptance; although the design of relevant interfaces with human behaviour is considered, human operators and their actions are not included in a technical system; the maintenance process is described in the maintenance manuals but is not itself part of the technical system;
- (23) 'catastrophic consequence' means fatalities and/or multiple severe injuries and/or major damages to the environment resulting from an accident (Table 3 from EN 50126);
- (24) 'safety acceptance' means status given to the change by the proposer based on the safety assessment report provided by the assessment body;
- (25) 'system' means any part of the railway system which is subject to a change;
- (26) 'notified national rule' means any national rule notified by Member States under Council Directive 96/48/EC⁽²⁾, Directive 2001/16/EC of the European Parliament and the Council⁽³⁾ and Directives 2004/49/EC and 2008/57/EC.

(2) UL L 235, 17.09.1996, str. 6.

(3) UL L 110, 20.04.2001, str. 1.

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

Člen 4. Pomembne spremembe

Člen 4(1)

If there is no notified national rule for defining whether a change is significant or not in a Member State, the proposer shall consider the potential impact of the change in question on the safety of the railway system.

When the proposed change has no impact on safety, the risk management process described in Article 5 does not need to be applied.

[G 1] Če ni priglašenega nacionalnega predpisa, je za odločitev odgovoren predlagatelj. Pomembnost spremembe temelji na strokovni presoji. Če je na primer predvidena sprememba v obstoječem sistemu kompleksna, se lahko ovrednoti kot pomembna, če je tveganje vpliva na obstoječe funkcije sistema⁽⁴⁾ visoko, čeprav sama sprememba ni nujno tesno povezana z varnostjo.

Člen 4(2)

When the proposed change has an impact on safety, the proposer shall decide, by expert judgement, the significance of the change based on the following criteria:

- (a) failure consequence: credible worst-case scenario in the event of failure of the system under assessment, taking into account the existence of safety barriers outside the system;*
- (b) novelty used in implementing the change: this concerns both what is innovative in the railway sector, and what is new just for the organisation implementing the change;*
- (c) complexity of the change;*
- (d) monitoring: the inability to monitor the implemented change throughout the system life-cycle and take appropriate interventions;*
- (e) reversibility: the inability to revert to the system before the change;*
- (f) additionality: assessment of the significance of the change taking into account all recent safety-related modifications to the system under assessment and which were not judged as significant.*

The proposer shall keep adequate documentation to justify his decision.

[G 1] **Primer majhnih sprememb:** po začetku obratovanja sistema je lahko enkratno povečanje najvišje hitrosti proge za 5 km/h nepomembno. Če se najvišja hitrost proge še naprej povečuje v korakih po 5 km/h, lahko seštevek zaporednih sprememb (ovrednotenih posamezno kot nepomembne spremembe) glede na prvotne varnostne zahteve sistema kljub temu postane pomembna sprememba.

⁽⁴⁾ Ker funkcije v sistemu niso vedno neodvisne, lahko spremembe nekaterih funkcij vplivajo tudi na druge funkcije sistema, čeprav se lahko zdi, da jih spremembe ne zadevajo neposredno.

- *****
- [G 2] Da se ovrednoti, ali je skupina več zaporednih (nepomembnih) sprememb pomembna, kadar se štejejo kot celota, je treba oceniti vse nevarnosti in z njimi povezana tveganja pri vseh spremembah. Skupina zadevnih sprememb se lahko šteje za nepomembno, če je nastalo tveganje splošno sprejemljivo.
- [G 3] Delo Agencije v zvezi s pomembnimi spremembami je pokazalo, da:
- (a) ni mogoče opredeliti usklajenih pragov ali pravil, na podlagi katerih se lahko za zadevno spremembo sprejme odločitev o njeni pomembnosti in
 - (b) ni mogoče zagotoviti izčrpnega seznama pomembnih sprememb;
 - (c) odločitev ne more veljati za vse predlagatelje ter vse tehnične, operativne, organizacijske in okoljske pogoje.
- Zato je bistveno, da so za odločitev še naprej odgovorni predlagatelji, ki so v skladu s členom 4(3) Direktive o varnosti na železnici {Ref. 1} odgovorni za varno delovanje in nadzor tveganj, povezanih z njihovim delom sistema.
- [G 4] Kot pomoč predlagatelju je v oddelku C.2. Dodatka C naveden en primer „ovrednotenja in uporabe meril“.
- [G 5] Skupna varnostna metoda se ne sme uporabiti, če se sprememba v zvezi z varnostjo ne šteje za pomembno. Vendar to ne pomeni, da ni treba narediti ničesar. Predlagatelj izvede neke vrste (predhodne) analize tveganja, da določi, ali je sprememba pomembna. Te analize tveganja ter kakršne koli utemeljitve in trditve je treba dokumentirati, da se nacionalnemu varnostnemu organu omogočijo revizije. Ocenjevalni organ ne sme neodvisno oceniti ovrednotenja pomembnosti spremembe in odločitve, da sprememba ni pomembna.

Člen 5. Postopek upravljanja s tveganji

Člen 5(1)

The risk management process described in the Annex I shall apply:

- (c) for a significant change as specified in Article 4, including the placing in service of structural sub-systems as referred to in Article 2(2)(b);*
- (d) where a TSI as referred to in Article 2 (2)(a) refers to this Regulation in order to prescribe the risk management process described in Annex I.*

- [G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

Člen 5(2)

The risk management process described in Annex I shall be applied by the proposer.

- [G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

Člen 5(3)

The proposer shall ensure that risks introduced by suppliers and service providers, including their subcontractors, are managed. To this end, the proposer may request that suppliers and service providers, including their subcontractors, participate in the risk management process described in Annex I.

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

Člen 6. Neodvisno ocenjevanje

Člen 6(1)

An independent assessment of the correct application of the risk management process described in Annex I and of the results of this application shall be carried out by a body which shall meet the criteria listed in Annex II. Where the assessment body is not already identified by Community or national legislation, the proposer shall appoint its own assessment body which may be another organisation or an internal department.

[G 1] Zahtevana stopnja neodvisnosti, ki jo mora imeti ocenjevalni organ, je odvisna od stopnje varnosti, ki se zahteva za ocenjevani sistem. Med čakanjem na uskladitev te teme je najboljša praksa v zvezi s to zadevo na voljo v klavzuli 8 standarda IEC61508-1:2001 ali v oddelku 5.3.9. standarda EN 50129 {Ref. 7}. Stopnja neodvisnosti je odvisna od resnosti posledic nevarnosti, povezane z opremo, in njene novosti. Oddelek 9.7.2. standarda EN 50126-2 in standard EN 50129 določata stopnjo neodvisnosti za sisteme signalizacije. Načeloma bi se lahko to uporabilo tudi za druge sisteme.

[G 2] Agencija trenutno še vedno obravnava opredelitev vlog in odgovornosti različnih ocenjevalnih organov (nacionalni varnostni organ, priglasi organi in neodvisni ocenjevalci varnosti) ter potrebne vmesnike med njimi. S tem se bo opredelilo, kdo (če je mogoče) od teh ocenjevalnih organov bo opravil posamezne naloge in na kakšen način. Na koncu bo to omogočilo določitev, kako:

- (a) na podlagi dokazov preveriti, ali se postopka obvladovanja in ocenjevanja tveganja, ki ju zajema skupna varnostna metoda, uporabljata pravilno, in
- (b) pomagati predlagatelju pri odločitvi, da sprejme pomembno spremembo v okviru ocenjevanega sistema.

Člen 6(2)

Duplication of work between the conformity assessment of the safety management system as required by Directive 2004/49/EC, the conformity assessment carried out by a notified body or a national body as required by Directive 2008/57/EC and any independent safety assessment carried out by the assessment body in accordance with this Regulation, shall be avoided.

[G 1] Dodatne informacije se bodo zagotovile z delom Agencije v zvezi z vlogami in odgovornostmi ocenjevalnih organov.

Člen 6(3)

The safety authority may act as the assessment body where the significant changes concern the following cases:

- (a) where a vehicle needs an authorisation for placing in service, as referred to in Articles 22(2) and 24(2) of Directive 2008/57/EC;*
- (b) where a vehicle needs an additional authorisation for placing in service, as referred to in Articles 23(5) and 25(4) of Directive 2008/57/EC;*
- (c) where the safety certificate has to be updated due to an alteration of the type or extent of the operation, as referred to in Article 10(5) of Directive 2004/49/EC;*
- (d) where the safety certificate has to be revised due to substantial changes to the safety regulatory framework, as referred to in Article 10(5) of Directive 2004/49/EC;*
- (e) where the safety authorisation has to be updated due to substantial changes to the infrastructure, signalling or energy supply, or to the principles of its operation and maintenance, as referred to in Article 11(2) of Directive 2004/49/EC;*
- (f) where the safety authorisation has to be revised due to substantial changes to the safety regulatory framework, as referred to in Article 11(2) of Directive 2004/49/EC.*

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

Člen 6(4)

Where the significant changes concern a structural subsystem that needs an authorisation for placing in service as referred to in Article 15(1) or Article 20 of Directive 2008/57/EC, the safety authority may act as the assessment body unless the proposer already gave that task to a notified body in accordance with Article 18(2) of that Directive.

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

Člen 7. Poročila o varnostni oceni

Člen 7(1)

The assessment body shall provide the proposer with a safety assessment report.

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

Člen 7(2)

In the case referred to in point (a) of Article 5(1), the safety assessment report shall be taken into account by the national safety authority in its decision to authorise the placing in service of subsystems and vehicles.

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

Člen 7(3)

In the case referred to in point (b) of Article 5(1), the independent assessment shall be part of the task of the notified body, unless otherwise prescribed by the TSI.

If the independent assessment is not part of the task of the notified body, the safety assessment report shall be taken into account by the notified body in charge of delivering the conformity certificate or by the contracting entity in charge of drawing up the EC declaration of verification.

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

Člen 7(4)

When a system or part of a system has already been accepted following the risk management process specified in this Regulation, the resulting safety assessment report shall not be called into question by any other assessment body in charge of performing a new assessment for the same system. The recognition shall be conditional on demonstration that the system will be used under the same functional, operational and environmental conditions as the already accepted system, and that equivalent risk acceptance criteria have been applied.

[G 1] To načelo vzajemnega priznavanja je že sprejeto v standardih CENELEC: glej oddelek 5.5.2. standarda EN 50129 in oddelek 5.9. standarda EN 50126-2. V standardu CENELEC načelo vzajemne odobritve ali vzajemnega priznavanja predlagatelji ali neodvisni ocenjevalci varnosti uporabljajo za generične proizvode in generične aplikacije⁽⁵⁾, če se ocenjevanje varnosti in dokazovanje varnosti izvajata v skladu z zahtevami standarda CENELEC.

[G 2] Vzajemno priznavanje je treba uporabiti tudi za sprejetje novih ali preoblikovanih sistemov, če sta njihova ocena tveganja in dokazovanje skladnosti sistema z varnostnimi zahtevami izvedena v skladu z določbami Uredbe o skupni varnostni metodi {Ref. 3}.

Člen 8. Upravljanje nadzorovanja tveganja/notranje in zunanje revizije

Člen 8(1)

The railway undertakings and infrastructure managers shall include audits of application of the CSM on risk evaluation and assessment in their recurrent auditing scheme of the safety management system as referred to in Article 9 of Directive 2004/49/EC.

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

Člen 8(2)

Within the framework of the tasks defined in Article 16(2)(e) of Directive 2004/49/EC, the

(5) Za dodatno obrazložitev v zvezi z izrazoma „generični proizvod in generična aplikacija“ ter s tem povezanimi načeli glej točko [G 5] oddelka 1.1.5, opombi (7) in (8) na strani 28 ter Slika 3 tega dokumenta.

national safety authority shall monitor the application of the CSM on risk evaluation and assessment.

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

Člen 9. Povratne informacije in tehnični napredek

Člen 9(1)

Each infrastructure manager and each railway undertaking shall, in its annual safety report referred to in Article 9(4) of Directive 2004/49/EC, report briefly on its experience with the application of the CSM on risk evaluation and assessment. The report shall also include a synthesis of the decisions related to the level of significance of the changes.

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

Člen 9(2)

Each national safety authority shall, in its annual safety report referred to in Article 18 of Directive 2004/49/EC, report on the experience of the proposers with the application of the CSM on risk evaluation and assessment, and, where appropriate, its own experience.

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

Člen 9(3)

The European Railway Agency shall monitor and collect feedback on the application of the CSM on risk evaluation and assessment and, where applicable, shall make recommendations to the Commission with a view to improving it.

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

Člen 9(4)

The European Railway Agency shall submit to the Commission by 31 December 2011 at the latest, a report which shall include:

- (a) an analysis of the experience with the application of the CSM on risk evaluation and assessment, including cases where the CSM has been applied by proposers on a voluntary basis before the relevant date of application provided for in Article 10;*
- (b) an analysis of the experience of the proposers concerning the decisions related to the level of significance of the changes;*
- (c) an analysis of the cases where codes of practice have been used as described in section 2.3.8 of Annex I;*
- (d) an analysis of overall effectiveness of the CSM on risk evaluation and assessment.*

The safety authorities shall assist the Agency by identifying cases of application of the CSM on risk evaluation and assessment.

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

Člen 10. Začetek veljavnosti

Člen 10(1)

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

Člen 10(2)

This Regulation shall apply from 1 July 2012.

However, it shall apply from 19 July 2010:

- (a) to all significant technical changes affecting vehicles as defined in Article 2 (c) of Directive 2008/57/EC;*
- (b) to all significant changes concerning structural sub-systems, where required by Article 15(1) of Directive 2008/57/EC or by a TSI.*

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

PRILOGA I – OBRAZLOŽITEV POSTOPKA IZ UREDBE O SKUPNI VARNOSTNI METODI

1. SPLOŠNA NAČELA, KI SE UPORABLJAJO V POSTOPKU UPRAVLJANJA S TVEGANJI

1.1. Splošna načela in obveznosti

1.1.1. The risk management process covered by this Regulation shall start from a definition of the system under assessment and comprise the following activities:

- (a) the risk assessment process, which shall identify the hazards, the risks, the associated safety measures and the resulting safety requirements to be fulfilled by the system under assessment;*
- (b) demonstration of the compliance of the system with the identified safety requirements and;*
- (c) management of all identified hazards and the associated safety measures.*

This risk management process is iterative and is depicted in the diagram of the Appendix (of the CSM Regulation). The process ends when the compliance of the system with all safety requirements necessary to accept the risks linked to the identified hazards is demonstrated.

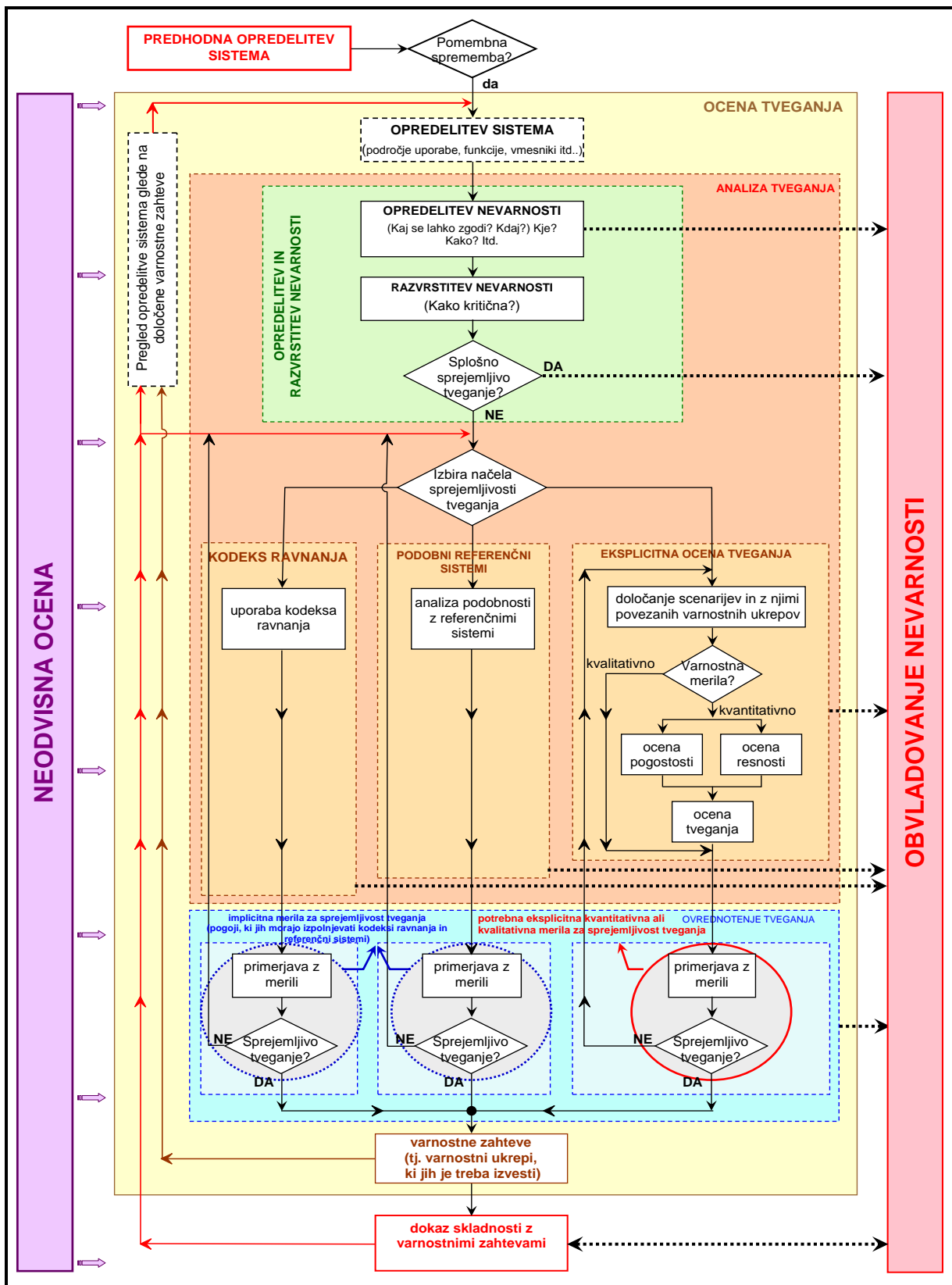
[G 1] Okvir obvladovanja tveganja za skupno varnostno metodo in s tem povezan postopek ocenjevanja tveganja sta prikazana na Slika 1. Po potrebi se vsako polje/dejavnost na tej sliki podrobneje opiše v posebnem razdelku tega dokumenta.

[G 2] Standard CENELEC priporoča, da se postopka obvladovanja in ocene tveganja opišeta v varnostnem načrtu. Če pa to za projekt ni primerno, se lahko s tem povezan opis vključi v kateri koli drug ustrezen dokument. Glej oddelek 1.1.6.

[G 3] Postopek ocene tveganja se začne s predhodno opredelitvijo sistema. Med razvojem projekta se predhodna opredelitev sistema postopno posodobi in nadomesti z opredelitvijo sistema. Če predhodne opredelitve sistema ni, se za izvedbo ocene tveganja uporabi uradna opredelitev sistema. Vendar je v tem primeru koristno, da se na začetku projekta sestanejo vsi udeleženci, ki jih pomembna sprememba zadeva, da:

- (a) se sporazumejo o splošnih načelih sistema, funkcijah sistema itd. Načeloma se lahko to opiše v predhodni opredelitvi sistema;
- (b) se sporazumejo o organizaciji projekta;
- (c) se sporazumejo o delitvi vlog in odgovornosti med različnimi že vključenimi udeleženci, vključno z nacionalnim varnostnim organom, priglašnim organom in neodvisnim ocenjevalcem varnosti, kadar je primerno.

Takšno sodelovanje med na primer predhodno opredelitvijo sistema predlagatelju, podizvajalcem, nacionalnemu varnostnemu organu, priglašenemu organu in neodvisnemu ocenjevalcu varnosti, če je primerno, zagotavlja priložnost, da se zgodaj sporazumejo o kodeksih ravnanja ali referenčnih sistemih, ki so sprejemljivi za uporabo v okviru projekta.



Slika 1 : Okvir obvladovanja tveganja iz Uredbe o skupni varnostni metodi [Ref. 2]

1.1.2. This iterative risk management process:

- (a) shall include appropriate quality assurance activities and be carried out by competent staff;*
- (b) shall be independently assessed by one or more assessment bodies.*

- [G 1] Sistem varnega upravljanja prevoznika v železniškem prometu in upravljavca železniške infrastrukture določa postopek in procese, ki:
- (a) spremljajo, ali je sistem še naprej varen v celotnem življenjskem ciklu (tj. med delovanjem in vzdrževanjem);
 - (b) zagotavljajo varno odpravo ali zamenjavo zadevnega sistema.
- Ta postopek ni del skupne varnostne metode za oceno tveganja.
- [G 2] Za izvajanje skupne varnostne metode morajo biti vse vključene stranke usposobljene (tj. imajo ustrezne spretnosti, znanje in izkušnje). Obstaja stalna potreba po upravljanju usposobljenosti v okviru organizacij udeležencev železniškega sektorja:
- (a) za upravljavce železniške infrastrukture in prevoznike v železniškem prometu to zajema njihov sistem varnega upravljanja v skladu s Prilogo III(2)(e) k Direktivi o varnosti na železnici {Ref. 1};
 - (b) drugi udeleženci, katerih dejavnosti lahko vplivajo na varnost železniškega sistema, imajo na splošno vsaj na ravni projekta (glej točko [G 1] oddelka 5.1.) postopek vodenja kakovosti in/ali postopek varnega upravljanja, ki zajema to zahtevo, čeprav sistem varnega upravljanja ni obvezen.
- [G 3] Naslednji oddelki standarda CENELEC EN 50126-1 {Ref. 8} določajo navodila v zvezi z usposobljenostjo:
- (a) na podlagi oddelka 5.3.5.(b): „vse osebe z odgovornostmi v okviru postopka obvladovanja“ tveganja mora biti „usposobljeno za izvajanje teh odgovornosti“;
 - (b) oddelek 5.3.5.(d): zahteve obvladovanja in ocene tveganja je treba „izvajati v okviru poslovnih postopkov, ki jih podpira sistem vodenja kakovosti, skladen z zahtevami iz standardov EN ISO 9001, EN ISO 9002 ali EN ISO 9003, ki so primerne za“ ocenjevani sistem. Primer vidikov, ki se nadzorujejo s sistemom vodenja kakovosti, je naveden v oddelku 5.2. standarda EN 50129 {Ref. 7}.
- Ti zajemajo dejavnosti zagotavljanja kakovosti, usposobljenost in izobraževanje osebja/oseb, ki se zahtevajo za podporo postopka v okviru skupne varnostne metode.
- [G 4] Postopek ocenjevanja tveganja zelo pogosto od samega začetka projekta spremlja ocenjevalni organ, vendar tako zgodnja vključitev ocenjevalnega organa ni obvezna, če tega ne zahteva nacionalna zakonodaja v državi članici, čeprav je priporočena. Mnenje neodvisnega ocenjevalnega organa je lahko koristno pred prehodom z enega koraka ocenjevanja tveganja k naslednjemu. Za nadaljnje podrobnosti o neodvisnem ocenjevanju glej Člen 6.

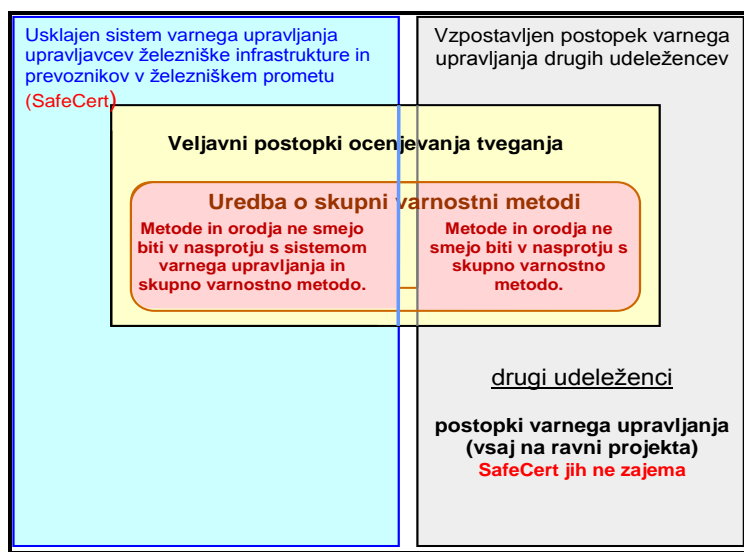
1.1.3. The proposer in charge of the risk management process required by this Regulation shall maintain a hazard record according to section 4.

- [G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

1.1.4. *The actors who already have in place methods or tools for risk assessment may continue to apply them as far as they are compatible with the provisions of this Regulation and subject to the following conditions:*

- (a) *the risk assessment methods or tools are described in a safety management system which has been accepted by a national safety authority in accordance with Article 10(2)(a) or Article 11(1)(a) of Directive 2004/49/EC, or;*
- (b) *the risk assessment methods or tools are required by a TSI or comply with publicly available recognised standards specified in notified national rules.*

[G 1] Slika 2 predstavlja povezavo med skupno varnostno metodo ter „sistemi varnega upravljanja in postopki ocenjevanja tveganja“.



Slika 2 : Usklajen sistem varnega upravljanja in skupna varnostna metoda

1.1.5. *Without prejudice to civil liability in accordance with the legal requirements of the Member States, the risk assessment process shall fall within the responsibility of the proposer. In particular the proposer shall decide, with agreement of the actors concerned, who will be in charge of fulfilling the safety requirements resulting from the risk assessment. This decision shall depend on the type of safety measures selected to control the risks to an acceptable level. The demonstration of compliance with the safety requirements shall be conducted according to section 3.*

[G 1] Če je predlagatelj upravljavec železniške infrastrukture ali prevoznik v železniškem prometu, je včasih treba v postopek vključiti druge udeležence⁽⁶⁾ (glej oddelek 1.2.1.). V nekaterih primerih lahko upravljavec železniške infrastrukture ali prevoznik v železniškem prometu delno ali v celoti odda dejavnosti ocene tveganja pogodbeniku. O vlogah in odgovornostih vsakega udeleženca se zadevni udeleženci običajno sporazumejo v zgodnji fazi projekta.

⁽⁶⁾ To je v skladu z Dodatkom A.4 k standardu CENELEC 50 129 {Ref. 7}.

[G 2] Pomembno je opozoriti, da predlagatelj vedno ostane odgovoren za uporabo skupne varnostne metode, za sprejemljivost tveganja in s tem za varnost sistema. To bo vključevalo zagotovitev, da:

- (a) vključeni udeleženci v celoti sodelujejo, zato da se zagotovijo vse potrebne informacije, in
- (b) je jasno, kdo mora izpolniti posebne zahteve v zvezi s skupno varnostno metodo (na primer prevzeti analizo tveganja ali upravljanje evidence nevarnosti).

V primeru nesporazuma med udeleženci glede varnostnih zahtev, ki jih morajo izpolniti, se je mogoče posvetovati z nacionalnim varnostnim organom. Vendar za iskanje rešitve ostaja odgovoren predlagatelj, pri čemer te odgovornosti ni mogoče prenesti na nacionalni varnostni organ: glej tudi oddelek 0.2.2.

[G 3] Če nalogo opravlja podizvajalec, ta ni zavezan k temu, da ima lastno varnostno organizacijo, če ni upravljavec železniške infrastrukture ali prevoznik v železniškem prometu ali zlasti če je struktura/velikost podizvajalca majhna ali če je njegov prispevek k celotnemu sistemu majhen. Za obvladovanje tveganja, vključno z dejavnostmi ocene tveganja in obvladovanja nevarnosti, lahko ostane odgovorna organizacija na višji ravni (tj. stranka podizvajalca). Vendar je podizvajalec vedno odgovoren za zagotovitev pravih informacij, ki so povezane z njegovimi dejavnostmi in jih organizacija na višji ravni potrebuje za pripravo dokumentacije v zvezi z obvladovanjem tveganja.

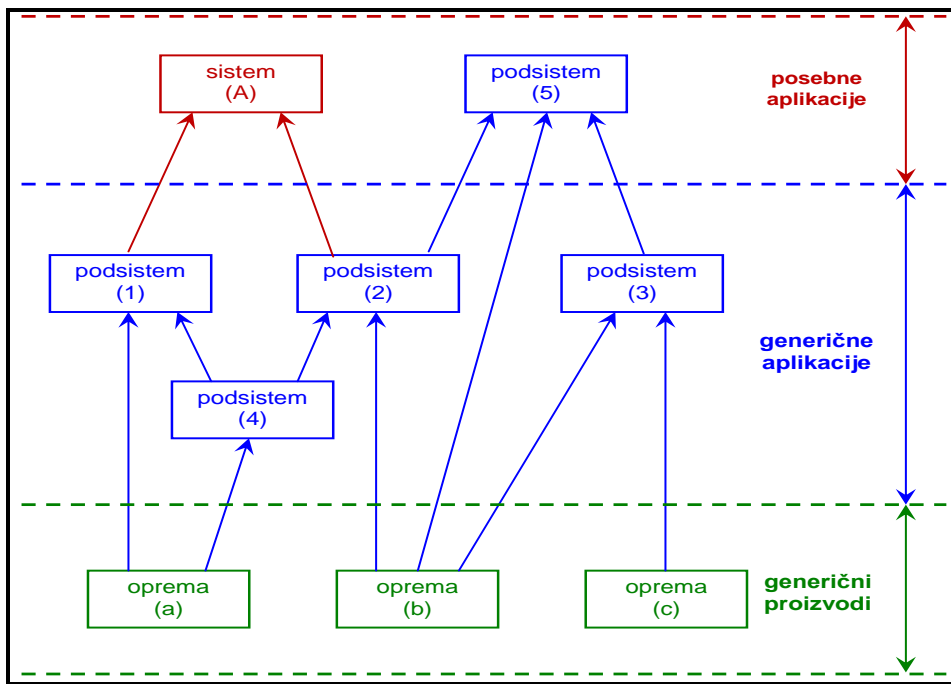
Sodelujoče organizacije se lahko sporazumejo na primer tudi o ustanovitvi skupne varnostne organizacije, da racionalizirajo stroške. V tem primeru bo dejavnosti vseh vključenih organizacij v zvezi z varnostjo upravljala le ena organizacija. Za točnost informacij (tj. o nevarnostih, tveganjih in varnostnih ukrepih) ter upravljanje izvajanja varnostnih ukrepov ostaja odgovorna organizacija, ki je pristojna za nadzorovanje nevarnosti, s katerimi so ti varnostni ukrepi povezani.

[G 4] Predlagatelj „stopnje varnosti“ in „varnostne zahteve“, ki so dodeljene udeležencem, vključenim v projekt, ter različnim podsistemom in opreми teh udeležencev, običajno določi:

- (a) v pogodbah med predlagateljem in zadevnimi udeleženci (podizvajalci);
- (b) v varnostnem načrtu ali katerem koli drugem ustreznem dokumentu z istim namenom, z opisom celotne organizacije projekta in odgovornosti vsakega udeleženca, vključno z odgovornostmi predlagatelja: glej oddelek 1.1.6.;
- (c) v evidenci(-ah) nevarnosti predlagatelja: glej oddelek 4.1.1.

xxsx Ta dodelitev „stopenj varnosti“ in „varnostnih zahtev“ sistema temeljnimi podsistemom in opreми ter s tem zadevnim udeležencem, vključno s samim predlagateljem, se lahko izboljša/razširi med „fazo dokazovanja skladnosti sistema z varnostnimi zahtevami“: Glej Slika 1. V primerjavi s ciklom V CENELEC (glej oddelek 2.1.1. in Slika 5 na strani 34) ta dejavnost ustreza fazi 5, ki obravnava „porazdelitev zahtev sistema“ na različne podsisteme in komponente.

[G 5] Člen 5(2) omogoča, da drugi udeleženci, razen prevoznika v železniškem prometu in upravljavca železniške infrastrukture, prevzamejo splošno odgovornost za skladnost s skupno varnostno metodo glede na lastne potrebe. Na primer za generične proizvode ali generične aplikacije⁽⁷⁾ lahko proizvajalec izvede oceno tveganja na podlagi „opredelitve generičnega sistema“, da se določijo stopnje varnosti in varnostne zahteve, ki jih morajo generični proizvodi in generične aplikacije izpolnjevati.



Slika 3 : Primeri odvisnosti med varnostnimi analizami (oblikovani na podlagi slike 9 iz standarda EN 50129).

[G 6] Standard CENELEC priporoča, da proizvajalec zagotovi dokumentiran dokaz iz ocene tveganja v zvezi z varnostnimi analizami za generični proizvod (generično aplikacijo⁽⁷⁾) in evidenc nevarnosti. Te varnostne analize in evidence nevarnosti vključujejo vse predpostavke⁽⁸⁾ in opredeljene „omejitve uporabe“ (tj. pogoje uporabe v zvezi z varnostjo), ki

(7) Izraza „varnostna analiza za generično aplikacijo“ in „generični proizvod“ sta že uporabljena v standardu CENELEC, v okviru katerega se lahko obravnavajo tri različne kategorije varnostne analize (glej Slika 3):

- (a) **varnostna analiza za generični proizvod** (neodvisno od aplikacije). Generični proizvod se lahko ponovno uporabi za različne neodvisne aplikacije;
- (b) **varnostna analiza za generično aplikacijo** (za razred aplikacij). Generična aplikacija se lahko ponovno uporabi za razred/vrsto aplikacije s skupnimi funkcijami;
- (c) **varnostna analiza za posebno aplikacijo** (za posebno aplikacijo). Posebna aplikacija se uporablja le za eno posebno postavitev.

Za več informacij o njihovi medsebojni odvisnosti glej oddelek 9.4. in sliko 9.1. smernice CENELEC 50 126-2 {Ref. 9}

(8) Te predpostavke in omejitve uporabe določajo omejitve in veljavnost „ocen varnosti“ in „analiz varnosti“, povezanih z zadevnimi varnostnimi analizami za generični proizvod in generično aplikacijo. Če jih zadevna posebna aplikacija ne izpolni, je treba ustrezne „ocene varnosti“ in „analize varnosti“ (npr. vzročne analize) posodobiti ali nadomestiti z novimi.

To je v skladu z naslednjim splošnim varnostnim načelom: „Kadar koli projektiranje posameznega (pod)sistema temelji na generičnih aplikacijah in generičnih proizvodih, je treba dokazati, da je posamezen (pod)sistem skladen z vsemi predpostavkami in omejitvami uporabe (v standardu CENELEC imenovanimi pogoji uporabe v zvezi z varnostjo), ki se prenesejo na ustrezne varnostne analize za generično aplikacijo in generični proizvod (glej Slika 3).“

veljajo za zadevne generične proizvode (generično aplikacijo). Kadar koli se generični proizvod in generična aplikacija uporabljata za delovanje pri posebni aplikaciji, je zato treba za vsako posebno aplikacijo dokazati skladnost z vsemi temi predpostavkami⁽⁷⁾ in „omejitvami uporabe“ (ali pogoji uporabe v zvezi z varnostjo).

1.1.6. The first step of the risk management process shall be to identify in a document, to be drawn up by the proposer, the different actors' tasks, as well as their risk management activities. The proposer shall coordinate close collaboration between the different actors involved, according to their respective tasks, in order to manage the hazards and their associated safety measures.

- [G 1] Zelo pogosto ima vsak projekt dokument, ki opisuje dejavnosti obvladovanja tveganja, razen če se na začetku projekta v pogodbah dogovori drugače. Ustrezen dokument se posodobi in pregleda, kadar koli se izvirni sistem pomembno spremeni.
- [G 2] Takšen dokument določa organizacijsko strukturo, dodeljene odgovornosti osebja, postopke, procese in dejavnosti, ki skupaj zagotavljajo, da ocenjevani sistem izpolnjuje določene stopnje varnosti in varnostne zahteve. Dokument mora biti skladen s skupno varnostno metodo, ker je v pomoč ocenjevalnemu organu in mu zagotavlja potrebna navodila. Standardi CENELEC priporočajo, da se takšne informacije vključijo v varnostni načrt ali drug dokument s tematskim sklopom, namenjenim tem temam.
- [G 3] Celotna organizacija projekta je predstavljena zlasti v predlagateljevem varnostnem načrtu ali kateri koli drugem ustreznem dokumentu. Opisuje, kako so vloge in odgovornosti razdeljene med vključene udeležence. Podrobne informacije so na voljo v varnostnih načrtih ali varnostnih organizacijah različnih vključenih udeležencev. Običajno se o delitvi odgovornosti med različnimi udeleženci razpravlja in dogovori v okviru predhodne opredelitve sistema (tj. na začetku projekta), če ta obstaja.
- [G 4] Varnostni načrt je dokument v razvoju, ki se v življenjskem obdobju projekta po potrebi posodobi.
- [G 5] Več podrobnosti je na voljo v standardu EN 50126-1 {Ref. 8} in z njim povezani smernici 50126-2 {Ref. 9} o vsebini varnostnega načrta.

1.1.7. Evaluation of the correct application of the risk management process described in this Regulation falls within the responsibility of the assessment body.

- [G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

Continuation of the footnote

Če za posebno aplikacijo ni mogoče doseči skladnosti z nekaterimi predpostavkami in omejitvami uporabe na ravni podsistema (npr. v primeru zahtev v zvezi z varnostjo delovanja), se lahko ustrezne predpostavke in omejitve uporabe prenesejo na višjo raven (tj. običajno na raven sistema). Te predpostavke in omejitve uporabe se nato jasno opredelijo v „varnostni analizi za posebno aplikacijo“ zadevnega podsistema. Bistveno je, da se v takšnih primerih odvisnosti zagotovi, da so pogoji uporabe v zvezi z varnostjo vsake varnostne analize izpolnjeni v varnostni analizi na višji ravni ali pa se prenesejo naprej na pogoje uporabe v zvezi z varnostjo varnostne analize na najvišji ravni (tj. varnostna analiza za sistem).

1.2. Upravljanje vmesnikov

1.2.1. For each interface relevant to the system under assessment and without prejudice to specifications of interfaces defined in relevant TSIs, the rail-sector actors concerned shall cooperate in order to identify and manage jointly the hazards and related safety measures that need to be handled at these interfaces. The management of shared risks at the interfaces shall be co-ordinated by the proposer.

- [G 1] Če na primer zaradi operativnih vzrokov prevoznik v železniškem prometu potrebuje upravljavca železniške infrastrukture, da ta izvede opredeljene spremembe infrastrukture na podlagi zahtev iz Priloge III(2)(g) k Direktivi o varnosti na železnici {Ref. 1}, prevoznik v železniškem prometu spremlja tudi splošno delo za zagotovitev pravilne izvedbe predvidenih sprememb. Vendar vodstvo prevoznika v železniškem prometu zadevnemu upravljavcu železniške infrastrukture ne odvzame odgovornosti, da obvesti ostale prevoznike v železniškem prometu, če zadevna sprememba infrastrukture vpliva tudi nanje. Upravljavec železniške infrastrukture bo morda moral izvesti celo oceno tveganja v skladu s skupno varnostno metodo, če je zadevna sprememba z njegovega vidika pomembna.
- [G 2] Prenosi odgovornosti med različnimi udeleženci so mogoči in v nekaterih okoliščinah celo potrebni. Kadar je v sistem vključenih več udeležencev, je kljub temu zelo pogosto en udeleženec določen kot odgovoren za sistem v celoti. Vedno obstajajo odvisnosti med podsistemi in delovanji, za opredelitev katerih je potrebno posebno prizadevanje. Zato mora nekdo prevzeti splošno odgovornost za analize varnosti in imeti popoln dostop do vse ustrezne dokumentacije. Razumljivo je, da je za popolnost in sistematičnost ocene tveganja na splošno odgovoren predlagatelj, ki namerava uvesti pomembno spremembo.
- [G 3] Glavna merila, o katerih se je treba sporazumeti v zvezi z upravljanjem vmesnikov med zadevnimi udeleženci, so:
- (a) vodstvo, ki ga običajno zagotovi predlagatelj, ki namerava uvesti pomembno spremembo;
 - (b) zahtevani vnosi;
 - (c) metode za opredelitev nevarnosti in oceno tveganja;
 - (d) zahtevani udeleženci s potrebno usposobljenostjo (tj. kombinacijo znanja, spretnosti in praktičnih izkušenj na tem področju – glej tudi opredelitev „usposobljenosti osebja“ iz točke [G 2](b) člena 3 {Ref. 4});
 - (e) pričakovani rezultati.
- Ta merila so opisana v varnostnih načrtih (ali v katerih koli drugih ustreznih dokumentih) podjetij, ki obravnavajo zadevne vmesnike.
- [G 4] V oddelku C.3. Dodatka C so navedeni primeri vmesnikov in primer uporabe navedenih glavnih meril za upravljanje vmesnikov med proizvajalcem vlakov in upravljavcem železniške infrastrukture ali prevoznikom v železniškem prometu.
- [G 5] Pri upravljanju vmesnikov je treba upoštevati tudi tveganja, ki bi lahko izhajala iz vmesnikov s človeškimi izvajalci (med delovanjem in vzdrževanjem) za načrtovanje teh vmesnikov.

1.2.2. *When, in order to fulfil a safety requirement, an actor identifies the need for a safety measure that it cannot implement itself, it shall, after agreement with another actor, transfer the management of the related hazard to the latter using the process described in section 4.*

- [G 1] Postopek prenosa nevarnosti in z njimi povezanih varnostnih ukrepov med udeleženci se uporablja tudi na nižjih stopnjah cikla V CENELEC na Slika 5 na strani 34. Uporabi se lahko, kadar koli morajo takšne informacije izmenjati na primer udeleženec in njegovi podizvajalci. Razlika v primerjavi z enakim postopkom na ravni sistema je, da predlagatelja ni treba obvestiti o vseh prenosih nevarnosti in z njimi povezanih varnostnih ukrepov na ravni podsistema. Predlagatelj je o tem obveščen le, kadar so prenesene nevarnosti in z njimi povezani varnostni ukrepi povezani z vmesniki na visoki ravni (tj. kadar vplivajo na vmesnike s predlagateljem).

1.2.3. *For the system under assessment, any actor who discovers that a safety measure is non-compliant or inadequate is responsible for notifying it to the proposer, who shall in turn inform the actor implementing the safety measure.*

- [G 1] Sistem varnega upravljanja prevoznika v železniškem prometu in upravljavca železniške infrastrukture zajema ureditve in postopke za zagotovitev, da se neskladnosti ali neustreznosti varnostnih ukrepov upravljajo pravilno. Zato te ureditve in postopki niso del skupne varnostne metode.
- [G 2] Podobno se o ureditvah in postopkih⁽⁹⁾, ki jih morajo vzpostaviti drugi udeleženci⁽¹⁰⁾ za zagotovitev, da se neskladnosti ali neustreznosti varnostnih ukrepov upravljajo pravilno in se varnostni ukrepi po potrebi prenesejo na vse ustrezne udeležence, zadevni udeleženci dogovorijo na začetku projekta, pri čemer se podrobnosti navedejo v njihovem varnostnem načrtu: glej oddelek 0.2.

1.2.4. *The actor implementing the safety measure shall then inform all the actors affected by the problem either within the system under assessment or, as far as known by the actor, within other existing systems using the same safety measure.*

- [G 1] To bo tako omogočilo upravljanje morebitne neskladnosti ali neustreznosti varnostnega ukrepa v okviru ocenjevanega sistema ali v okviru podobnih sistemov, ki uporabljajo enak ukrep.

⁽⁹⁾ Načeloma so te ureditve in postopki zajeti v postopku vodenja kakovosti in/ali varnega upravljanja teh udeležencev, ki je vzpostavljen vsaj na ravni projekta (glej tudi Slika 2).

⁽¹⁰⁾ Izraz „drugi udeleženci“ predstavlja vse zadevne udeležence, razen upravljavcev železniške infrastrukture in prevoznikov v železniškem prometu.

1.2.5. *When agreement cannot be found between two or more actors it is the responsibility of the proposer to find an adequate solution.*

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

1.2.6. *When a requirement in a notified national rule cannot be fulfilled by an actor, the proposer shall seek advice from the relevant competent authority.*

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

1.2.7. *Independently from the definition of the system under assessment, the proposer is responsible for ensuring that the risk management covers the system itself and the integration into the railway system as a whole.*

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

2. OPIS POSTOPKA OCENJEVANJA TVEGANJA

2.1. Splošni opis – ujemanje med postopkom ocenjevanja tveganja po skupni varnostni metodi in ciklom V CENELEC

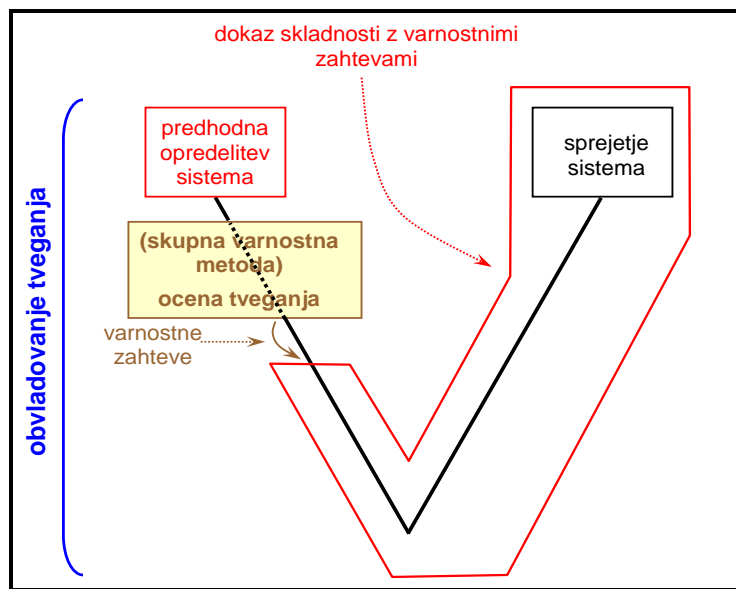
2.1.1. *The risk assessment process is the overall iterative process that comprises:*

- (a) the system definition;*
- (b) the risk analysis including the hazard identification;*
- (c) the risk evaluation.*

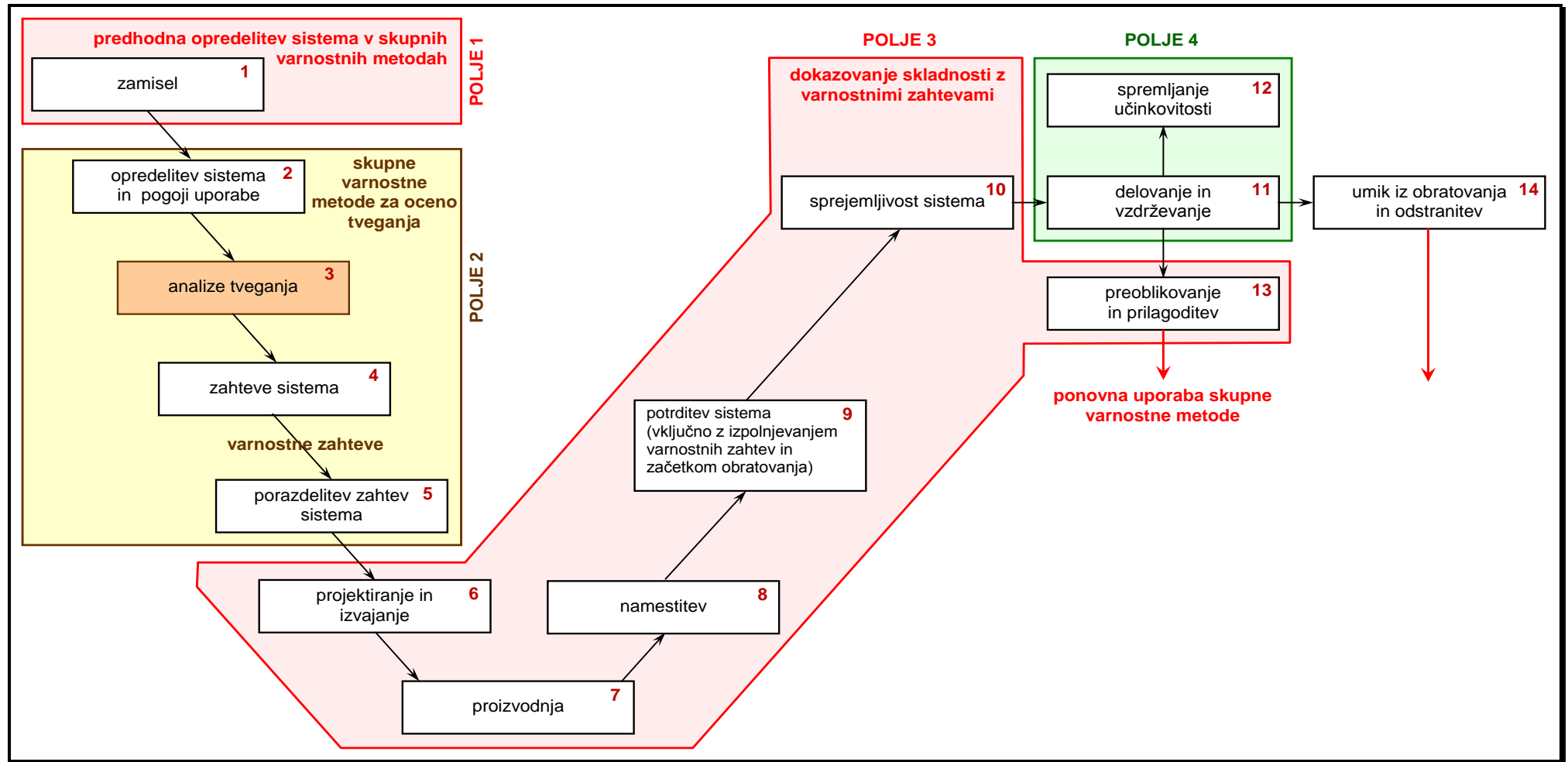
The risk assessment process shall interact with the hazard management according to section 4.1..

[G 1] Postopek obvladovanja tveganja, ki ga zajema skupna varnostna metoda, se lahko predstavi v okviru cikla V, ki se začne s (predhodno) opredelitvijo sistema in konča s sprejetjem sistema: glej Slika 4. Ta poenostavljeni cikel V se lahko nato prikaže v klasičnem ciklu V na sliki 10 standarda EN 50126-1 {Ref. 8}. Za dokaz ujemanja postopka obvladovanja tveganja po skupni varnostni metodi na Slika 1 je cikel V CENELEC s slike 10 predstavljen na Slika 5:

- (a) „predhodna opredelitev sistema“ iz skupne varnostne metode na Slika 1 ustreza fazi 1 v ciklu V CENELEC, tj. opredelitvi „zamisli“ sistema (glej polje 1 na Slika 5);
- (b) „ocena tveganja“ iz skupne varnostne metode na Slika 1 vključuje naslednje faze cikla V CENELEC (glej polje 2 na Slika 5):
 - (1) fazo 2 na Slika 5: „opredelitev sistema in pogoji uporabe“;
 - (2) fazo 3 na Slika 5: „analiza tveganja“;
 - (3) fazo 4 na Slika 5: „zahteve sistema“;
 - (4) fazo 5 na Slika 5: „porazdelitev zahtev sistema“ na različne podsisteme in komponente.



Slika 4 : Poenostavljen cikel V s slike 10 standarda EN 50126



Slika 5 : Slika 10 cikla V standarda EN 50126 (življenjski cikel sistema iz standarda CENELEC)

- [G 2] Rezultati postopka ocenjevanja tveganja v okviru skupne varnostne metode (po ponovitvah – glej Slika 1) so:
- (a) „opredelitev sistema“, posodobljena z „varnostnimi zahtevami“, ki izhajajo iz dejavnosti „analize tveganja“ in „ovrednotenja tveganja“ (glej oddelek 2.1.6.);
 - (b) „porazdelitev zahtev sistema“ na različne podsisteme in komponente (faza 5 na Slika 5);
 - (c) „evidenca nevarnosti“, v kateri se evidentirajo:
 - (1) vse opredeljene nevarnosti in z njimi povezani varnostni ukrepi;
 - (2) iz tega izhajajoče varnostne zahteve;
 - (3) predpostavke, ki se upoštevajo pri sistemu ter ki določajo omejitve in veljavnost ocene tveganja (glej točko (g) oddelka 2.1.2.);
 - (d) ter na splošno vsi dokazi, ki izhajajo iz uporabe skupne varnostne metode: glej oddelek 5.

Rezultati ocene tveganja iz skupne varnostne metode ustrezajo rezultatom v zvezi z varnostjo iz faze 4 v ciklu V CENELEC, tj. podrobnem opisu zahteve sistema na Slika 5 : Slika 10 cikla V standarda EN 50126 (življenjski cikel sistema iz standarda CENELEC)

- [G 3] Opredelitev sistema, posodobljena z rezultati ocene tveganja, in evidenca nevarnosti predstavljata vhodne elemente, na podlagi katerih je sistem projektiran in sprejet. „Dokazovanje skladnosti sistema z varnostnimi zahtevami“ iz skupne varnostne metode ustreza naslednjim fazam cikla V CENELEC (glej polje 3 na Slika 5):
- (a) fazi 6 na Slika 5: „projektiranje in izvajanje“;
 - (b) fazi 7 na Slika 5: „proizvodnja“;
 - (c) fazi 8 na Slika 5: „namestitve“;
 - (d) fazi 9 na Slika 5: „potrditev sistema (vključno z izpolnjevanjem varnostnih zahtev in začetkom obratovanja)“;
 - (e) fazi 10 na Slika 5: „sprejetje sistema“.
- [G 4] Dokazovanje skladnosti sistema z varnostnimi zahtevami je odvisno od tega, ali je pomembna sprememba tehnična, operativna ali organizacijska. Zato različni koraki v ciklu V CENELEC na Slika 5 morda niso ustrezni za vse pomembne spremembe zadevne vrste. Cikel V na Slika 5 je treba ustrezno obravnavati in uporabljati na podlagi ustrezne ocene, kaj je primerno za posamezno aplikacijo (npr. pri operativnih in organizacijskih spremembah ni faze proizvodnje).
- [G 5] To pomeni, da „dokazovanje skladnosti sistema z varnostnimi zahtevami“ iz skupne varnostne metode ne vključuje le dejavnosti „preverjanja in potrditve“ s testi ali simulacijo. V praksi zajema vse faze od 6 do 10 (glej seznam zgoraj in Slika 5) v ciklu V CENELEC. Te vključujejo dejavnosti projektiranja, proizvodnje, namestitve, preverjanja in potrditve, s tem povezane dejavnosti zanesljivosti, razpoložljivosti, vzdrževalnosti in varnosti ter sprejetje sistema.
- [G 6] Splošno načelo med „dokazovanjem skladnosti sistema z varnostnimi zahtevami“ je, da se ocena tveganja osredotoča le na funkcije in vmesnike sistema, povezane z varnostjo. To pomeni, da se dejavnosti ocenjevanja tveganja in varnosti, kadar so potrebne v okviru ene od faz cikla V CENELEC na Slika 5, osredotočajo na:
- (a) funkcije in vmesnike, povezane z varnostjo;



- (b) podsisteme in/ali komponente, vključene v uresničevanje funkcij in/ali vmesnikov, povezanih z varnostjo, ki se ocenjujejo v okviru dejavnosti ocenjevanja tveganja na višji ravni.

[G 7] Iz primerjave s klasičnim ciklom V CENELEC na Slika 5 izhaja, da:

- (a) skupna varnostna metoda zajema faze od 1 do 10 in fazo 13 tega cikla V. Te vključujejo vrsto dejavnosti, ki so potrebne za sprejetje ocenjevanega sistema;
- (b) skupna varnostna metoda ne zajema faz 11, 12 in 14 življenjskega cikla sistema:
 - (1) fazi 11 in 12 sta povezani z „delovanjem in vzdrževanjem“ ter „spremljanjem učinkovitosti“ sistema po njegovem sprejetju na podlagi skupne varnostne metode. Ti dve fazi sta zajeti v sistemu varnega upravljanja prevoznika v železniškem prometu in upravljavca železniške infrastrukture (glej polje 4 na Slika 5). Vendar če se med delovanjem, vzdrževanjem ali spremljanjem učinkovitosti sistema zdi, da je sistem treba preoblikovati in prilagoditi (faza 13 na Slika 5), medtem ko že deluje, se v skladu s Člen 2 za nove potrebne spremembe ponovno uporabi skupna varnostna metoda. Če je sprememba torej pomembna:
 - (i) se za te nove spremembe uporabita postopka obvladovanja in ocenjevanja tveganja iz skupne varnostne metode;
 - (ii) je v skladu s Člen 6 za te nove spremembe potrebno sprejetje;
 - (2) tudi „umik iz obratovanja in odstranitev“ sistema, ki že deluje (faza 14), se lahko obravnava kot pomembna sprememba, zato se lahko v skladu s Člen 2 za fazo 14 na Slika 5 ponovno uporabi skupna varnostna metoda.

Za več informacij o obsegu vsake faze ali dejavnosti v ciklu V CENELEC, opisanem na Slika 5, glej oddelek 6 standarda EN 50126-1 {Ref. 8}.

2.1.2. The system definition should address at least the following issues:

- (a) system objective, e.g. intended purpose;*
- (b) system functions and elements, where relevant (including e.g. human, technical and operational elements);*
- (c) system boundary including other interacting systems;*
- (d) physical (i.e. interacting systems) and functional (i.e. functional input and output) interfaces;*
- (e) system environment (e.g. energy and thermal flow, shocks, vibrations, electromagnetic interference, operational use);*
- (f) existing safety measures and, after iterations, definition of the safety requirements identified by the risk assessment process;*
- (g) assumptions which shall determine the limits for the risk assessment.*

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

2.1.3. A hazard identification shall be carried out on the defined system, according to section 2.2.

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

2.1.4. The risk acceptability of the system under assessment shall be evaluated by using one



or more of the following risk acceptance principles:

- (a) the application of codes of practice (section 2.3);*
- (b) a comparison with similar systems (section 2.4);*
- (c) an explicit risk estimation (section 2.5).*

In accordance with the general principle referred to in section 1.1.5, the assessment body shall refrain from imposing the risk acceptance principle to be used by the proposer.

- [G 1] Na splošno se bo predlagatelj odločil, katero načelo sprejemljivosti tveganja je najustreznejše za nadzorovanje opredeljenih nevarnosti, na podlagi posebnih zahtev projekta in svojih izkušenj z vsemi tremi načeli.
- [G 2] Sprejemljivosti tveganja na ravni sistema ni vedno mogoče ovrednotiti z uporabo le enega od treh načel sprejemljivosti tveganja. Sprejemljivost tveganja bo pogosto temeljila na mešanici teh načel. Če je treba pri pomembni nevarnosti uporabiti več kot eno načelo sprejemljivosti tveganja za nadzorovanje s tem povezanega tveganja, je treba zadevno nevarnost razdeliti na podnevarnosti, tako da se vsaka posamezna podnevarnost ustrezno nadzoruje z enim od načel sprejemljivosti tveganja.
- [G 3] Odločitev za nadzorovanje nevarnosti z načelom sprejemljivosti tveganja mora upoštevati nevarnost in vzroke nevarnosti, ki so bili v fazi opredelitve nevarnosti že opredeljeni. Če sta torej z isto nevarnostjo povezana dva različna in neodvisna vzroka, je treba nevarnost razdeliti v dve različni podnevarnosti. Tako bo vsaka podnevarnost nadzorovana z enim načelom sprejemljivosti tveganja. Ti podnevarnosti je treba evidentirati in upravljati v evidenci nevarnosti. Če je na primer nevarnost posledica napake v projektiranju, se ta lahko upravlja z uporabo kodeksa ravnanja, medtem ko ta sam morda ne bo dovolj, če je vzrok za nevarnost napaka v vzdrževanju; v tem primeru je treba uporabiti drugo načelo sprejemljivosti tveganja.
- [G 4] Za zmanjšanje tveganja na sprejemljivo raven je morda potrebnih več ponovitev med fazami analize in ovrednotenja tveganja, dokler se ne opredelijo ustrezni varnostni ukrepi.
- [G 5] Preostalo tveganje, ugotovljeno na podlagi izkušenj iz prakse za obstoječe sisteme in sisteme na podlagi uporabe kodeksov ravnanja, se šteje za sprejemljivo. Tveganje, ki izhaja iz eksplicitne ocene tveganja, temelji na presoji strokovnjaka in različnih predpostavkah, ki jih je sprejel strokovnjak, ali na zbirkah podatkov, povezanih z izkušnjami iz nesreč in delovanja. Zato preostalo tveganje iz eksplicitne ocene tveganja ne more biti potrjeno takoj na podlagi izkušenj iz prakse. Za tak dokaz je potreben čas za delovanje, spremljanje in pridobitev reprezentativnih izkušenj za zadeven(-vne) sistem(-e). Na splošno je prednost uporabe kodeksa ravnanja in primerjave s podobnimi referenčnimi sistemi preprečitev preveč podrobne določitve nepotrebno strogih varnostnih zahtev, ki so lahko posledica preveč konservativnih (varnostnih) predpostavk v eksplicitnih ocenah tveganja. Kljub temu se lahko zgodi, da nekaterih varnostnih zahtev iz kodeksa ravnanja ali podobnih referenčnih sistemov za ocenjevanje sistema ni treba izpolniti. V tem primeru bi bila prednost uporabe eksplicitne ocene tveganja preprečitev nepotrebne pretiranega projektiranja ocenjevanega sistema in bi omogočila stroškovno učinkovitejše projektiranje, kakršnega še ni bilo.
- [G 6] Če se opredeljene nevarnosti in z njimi povezano(-a) tveganje(-a) ocenjevanega sistema ne morejo nadzorovati z uporabo kodeksov ravnanja ali podobnih referenčnih sistemov, se izvede eksplicitna ocena tveganja na podlagi kvantitativnih ali kvalitativnih analiz nevarnih dogodkov. Takšne razmere se običajno pojavijo, kadar je ocenjevanje sistema popolnoma nov (ali projektiranje inovativno) ali kadar sistem odstopa od kodeksa ravnanja ali referenčnega sistema. V tem primeru se bo v eksplicitni oceni tveganja ovrednotilo, ali je tveganje

sprejemljivo (tj. nadaljnja analiza ni potrebna) oziroma ali so potrebni dodatni varnostni ukrepi za dodatno zmanjšanje tveganja.

- [G 7] Navodila za zmanjšanje in sprejemljivost tveganja so na voljo tudi v oddelku 8 smernice EN 50126-2 {Ref. 9}.
- [G 8] Uporabljeno načelo sprejemljivosti tveganja in njegovo uporabo mora ovrednotiti ocenjevalni organ.

2.1.5. The proposer shall demonstrate in the risk evaluation that the selected risk acceptance principle is adequately applied. The proposer shall also check that the selected risk acceptance principles are used consistently.

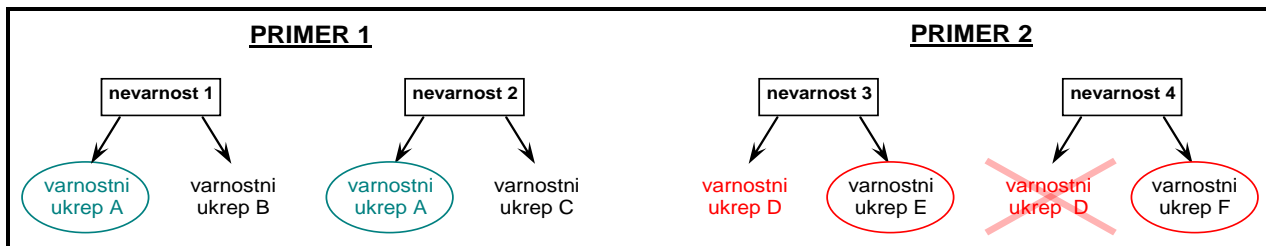
- [G 1] Če je na primer za programsko opremo komponente kot varnostna zahteva določena uporaba razvojnega postopka stopnje 4 varnostne integritete (SIL 4) standarda EN 50128, bo treba z dokazili potrditi, da je postopek, ki ga priporoča standard, izpolnjen. To na primer vključuje dokazila, da:
- (a) so izpolnjene zahteve glede neodvisnosti pri organizaciji projektiranja, preverjanju in potrjevanju programske opreme;
 - (c) so uporabljene pravilne metode standarda EN 50128 za stopnjo 4 varnostne integritete (SIL 4);
 - (d) itd.
- [G 2] Če se bo na primer za izdelavo električnih ventilov za zasilne zavore uporabil poseben kodeks ravnanja, bo treba z dokazili potrditi, da so bile pri postopku izdelave izpolnjene vse zahteve kodeksa ravnanja.

2.1.6. The application of these risk acceptance principles shall identify possible safety measures which make the risk(s) of the system under assessment acceptable. Among these safety measures, the ones selected to control the risk(s) shall become the safety requirements to be fulfilled by the system. Compliance with these safety requirements shall be demonstrated in accordance with section 3.

- [G 1] Opredeliti je mogoče dve vrsti varnostnih ukrepov:
- (a) „preventivne varnostne ukrepe“, ki preprečujejo nastanek nevarnosti ali njihovih vzrokov, in
 - (b) „varnostne ukrepe za ublažitev“, ki preprečujejo, da bi se nevarnosti razvile v nesreče, ali zmanjšujejo posledice nesreč po njihovem nastanku (zaščitni ukrepi).
- Za zagotavljanje nemotenega obratovanja je preprečevanje vzrokov na splošno učinkovitejše.
- [G 2] Predlagatelj bo za najustreznejše štel tiste varnostne ukrepe, ki zagotavljajo najboljši kompromis med stroški za doseg zmanjšanja tveganja in stopnjo preostalega tveganja. Izbrani varnostni ukrepi postanejo varnostne zahteve za ocenjevani sistem.

[G 3] Pomembno je preveriti, da izbrani varnostni ukrepi za nadzor ene nevarnosti niso v nasprotju z drugimi nevarnostmi. Kot je prikazano na Slika 6, se lahko na primer zgodita naslednja primera⁽¹¹⁾:

- (a) PRIMER 1: če se lahko z istim varnostnim ukrepom (ukrep A na Slika 6) nadzirajo različne nevarnosti, ne da bi se ustvarjala nasprotja med njimi, in če je to ekonomsko upravičeno, se lahko kot s tem povezana „varnostna zahteva“ izbere samo zadeven varnostni ukrep. Skupno število varnostnih zahtev, ki jih je treba izpolniti, je manjše kot pri izvajanju ukrepov B in C;



Slika 6 : Izbor ustreznih varnostnih ukrepov za nadzor tveganj

- (b) PRIMER 2: obratno pa varnostni ukrep, ki lahko nadzira eno nevarnost, vendar ustvarja nasprotje z drugo nevarnostjo (ukrep D na Slika 6), ne more biti izbran kot „varnostna zahteva“. Za zadevno nevarnost morajo biti uporabljeni drugi varnostni ukrepi (ukrepa E in F na Slika 6):

- (1) značilen primer v sistemu upravljanja - vodenja je uporaba lokacije vlaka na tirih za nadzorovanje uporabe zavor ali odobritev pospeševanja vlaka. Uporaba sprednjega dela vlaka kot njegove lokacije (glede na zadnji del vlaka) v vseh razmerah ni varna:
 - (i) ko mora sistem upravljanja - vodenja ETCS varno uporabiti zasilne zavore, uporabi NAJBOLJ VAREN SPREDNJI DEL za zagotovitev, da se bo sprednji del vlaka dejansko ustavil pred nevarnim mestom;
 - (ii) obratno, kadar se vlaku odobri pospeševanje na primer po omejitvi hitrosti, sistem upravljanja - vodenja ETCS uporabi NAJMANJ VAREN ZADNJI DEL;
- (2) drug primer je varnostni ukrep, ki bi lahko bil veljaven za zaustavitev vlaka v vseh okoliščinah, v katerih mora biti varen, razen v predoru ali na mostu. V tem zadnjem primeru se ukrep D v PRIMERU 2 na Slika 6 ne sprejme.

2.1.7. The iterative risk assessment process can be considered as completed when it is demonstrated that all safety requirements are fulfilled and no additional reasonably foreseeable hazards have to be considered.

[G 1] Glede na tehnične odločitve pri projektiranju sistema, njegovih podsistemov in opreme na primer se lahko med „dokazovanjem skladnosti z varnostnimi zahtevami“ opredelijo nove nevarnosti (npr. uporaba nekaterih barv lahko v primeru požara povzroči strupene pline). Te nove nevarnosti in z njimi povezana tveganja je treba šteti za nove vhodne elemente za nov

⁽¹¹⁾ Opozoriti je treba, da priročnik ne navaja vseh razmer, v katerih bi lahko bili varnostni ukrepi v nasprotju z drugimi opredeljenimi nevarnostmi. Navedenih je le nekaj ponazoritvenih zgledov.

krog v ponovnem postopku ocenjevanja tveganja. Dodatek A.4.3. k standardu EN 50129 vsebuje druge primere, v katerih lahko nastanejo nove nevarnosti, ki jih je treba nadzirati.

2.2. Določanje nevarnosti

2.2.1. The proposer shall systematically identify, using wide-ranging expertise from a competent team, all reasonably foreseeable hazards for the whole system under assessment, its functions where appropriate and its interfaces.

All identified hazards shall be registered in the hazard record according to section 4.

- [G 1] Nevarnosti so izražene na enaki stopnji podrobnosti, kolikor je to mogoče. Med predhodno analizo nevarnosti se lahko zgodi, da so opredeljene nevarnosti na različnih stopnjah podrobnosti (npr. ker med analizo HAZOP sodelujejo ljudje z različnimi izkušnjami). Stopnja podrobnosti je odvisna tudi od načela sprejemljivosti tveganja, ki je izbrano za nadzor opredeljene(-ih) nevarnosti. Na primer, če se nevarnost v celoti nadzoruje s kodeksom ravnanja ali podobnim referenčnim sistemom, podrobnejša opredelitev nevarnosti ne bo potrebna.
- [G 2] V evidenci nevarnosti je treba evidentirati vse nevarnosti, ki so opredeljene v postopku ocenjevanja tveganja (vključno s tistimi, ki so povezane s splošno sprejemljivimi tveganji), ter z njimi povezane varnostne ukrepe in tveganja.
- [G 3] Glede na naravo sistema, ki bo analiziran, se lahko za opredelitev nevarnosti uporabijo različne metode:
- (a) empirična opredelitev nevarnosti z uporabo preteklih izkušenj (npr. uporaba kontrolnih seznamov ali splošnih seznamov nevarnosti);
 - (b) ustvarjalna opredelitev nevarnosti za nova zaskrbjujoča področja (proaktivno napovedovanje, npr. študije vrste „kaj če“ (WHAT-IF), kot so FMEA ali HAZOP).
- [G 4] Empirična in ustvarjalna metoda za opredelitev nevarnosti se lahko uporabljata skupaj in se dopolnjujeta, da se zagotovi izčrpnost seznama morebitnih nevarnosti in varnostnih ukrepov, kadar se ta uporablja.
- [G 5] Kot predhodni korak se lahko opredelitev nevarnosti začne s skupino za zbiranje zamisli, v kateri so strokovnjaki z različnih področij, ki zajemajo vse bistvene vidike pomembne spremembe. Kadar zbor strokovnjakov presodi, da je to potrebno, se lahko uporabijo empirične metode za analizo posameznih funkcij ali načinov delovanja.
- [G 6] Metode, ki se uporabijo za opredelitev nevarnosti, so odvisne od opredelitve sistema. Nekaj primerov je navedenih v Dodatku B.
- [G 7] Več informacij o tehnikah in metodah za opredelitev nevarnosti je na voljo v prilogah A.2. in E k smernici EN 50126-2 {Ref. 9}.
- [G 8] Primer seznama splošnih nevarnosti je naveden v oddelku C.17. Dodatka C.

2.2.2. *To focus the risk assessment efforts upon the most important risks, the hazards shall be classified according to the estimated risk arising from them. Based on expert judgement, hazards associated with a broadly acceptable risk need not be analysed further but shall be registered in the hazard record. Their classification shall be justified in order to allow independent assessment by an assessment body.*

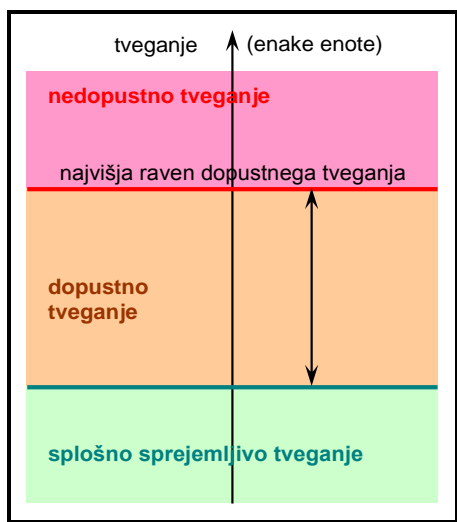
[G 1] Za pomoč pri postopku ocene tveganja se lahko pomembne nevarnosti nadalje razvrstijo v različne kategorije. Pomembne nevarnosti so lahko na primer razvrščene ali uvrščene glede na pričakovano resnost tveganja in pogostost pojavljanja. Navodila za tako dejavnost so v standardih CENELEC: glej oddelek A.2. Dodatka A.

[G 2] Analiza in ovrednotenje tveganja, opisana v oddelku 2.1.4., se uporablja zlasti tako, da začneta z najvišje uvrščeno nevarnostjo.

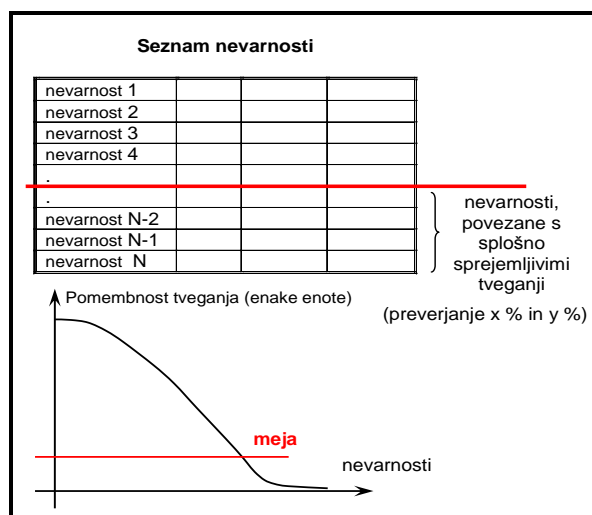
2.2.3. *As a criterion, risks resulting from hazards may be classified as broadly acceptable when the risk is so small that it is not reasonable to implement any additional safety measure. The expert judgement shall take into account that the contribution of all the broadly acceptable risks does not exceed a defined proportion of the overall risk.*

[G 1] Na primer, tveganje, povezano z nevarnostjo, se lahko šteje za splošno sprejemljivo:

- (a) če tveganje predstavlja manj kot določeni odstotek (npr. x %) najvišjega dopustnega tveganja za to vrsto nevarnosti. Vrednost x % lahko temelji na najboljši praksi in izkušnjah različnih pristopov analize tveganja, npr. razmerje med razvrstitvami splošno sprejemljivega tveganja in nedopustnega tveganja na krivuljah F-N ali v matrikah tveganja. To se lahko predstavi, kot je prikazano na sliki 7;
- (b) ali če je izguba, povezana s tveganjem, tako majhna, da izvajanje kakršnih koli varnostnih protiukrepov ni razumno.



Slika 7 : Splošno sprejemljiva tveganja



Slika 8 : Filtriranje nevarnosti, povezanih s splošno sprejemljivim tveganjem

[G 2] Poleg tega je treba, če se opredelijo nevarnosti z različnimi stopnjami podrobnosti (tj. nevarnosti visoke stopnje na eni strani in podrobne podnevarnosti na drugi strani), sprejeti

previdnostne ukrepe za preprečitev napačne razvrstitve med nevarnosti, povezane s splošno sprejemljivim(-i) tveganjem(-i). Prispevek vseh nevarnosti, povezanih s splošno sprejemljivim(-i) tveganjem(-ji), ne sme presegati določenega deleža (npr. y %) celotnega tveganja na ravni sistema. To preverjanje je potrebno, da se prepreči, da bi z razdelitvijo nevarnosti na številne podnevarnosti nizke stopnje izničili temeljne predpostavke. Če je ena nevarnost izražena kot mnoge „manjše“ podnevarnosti, se lahko vsaka od teh razvrsti kot nevarnost, povezana s splošno sprejemljivim(-i) tveganjem(-ji), če se vrednotijo samostojno, ampak kot nevarnost, povezana s pomembnim tveganjem, kadar se vrednotijo skupaj (tj. kot ena nevarnost visoke stopnje). Vrednost deleža (npr. y %) je odvisna od meril za sprejemljivost tveganja, ki se uporabljajo na ravni sistema. Lahko temelji na operativnih izkušnjah podobnih referenčnih sistemov in se v okviru teh vrednoti.

- [G 3] Preverjanji zgoraj (tj. glede na x % in y %) omogočata osredotočenje ocene tveganja na najpomembnejše nevarnosti in zagotavljata nadzor vseh pomembnih tveganj (glej Slika 8). Brez poseganja v pravne zahteve v državi članici mora predlagatelj na podlagi strokovne presoje določiti vrednosti x % in y % ter zagotoviti, da ju neodvisno oceni ocenjevalni organ. Primera vrednosti sta lahko x = 1 % in y = 10 %, če se to zdi sprejemljivo na podlagi strokovne presoje.
- [G 4] V oddelku 2.2.2. je določeno, da razvrstitev med „splošno sprejemljiva tveganja“ neodvisno oceni ocenjevalni organ.

2.2.4. During the hazard identification, safety measures may be identified. They shall be registered in the hazard record according to section 4.

- [G 1] Glavni namen dejavnosti je opredelitev nevarnosti, ki so povezane s spremembo. Če so varnostni ukrepi že opredeljeni, jih je treba evidentirati v evidenci nevarnosti. Narava ukrepov je odvisna od spremembe; lahko so postopkovni, tehnični, operativni ali organizacijski.

2.2.5. The hazard identification only needs to be carried out at a level of detail necessary to identify where safety measures are expected to control the risks in accordance with one of the risk acceptance principles mentioned in point 2.1.4. Iteration may thus be necessary between the risk analysis and the risk evaluation phases until a sufficient level of detail is reached for the identification of hazards.

- [G 1] Čeprav se tveganje nadzoruje na sprejemljivi ravni, se lahko predlagatelj odloči, da je potrebna podrobnejša opredelitev nevarnosti. Eden od razlogov za to je lahko, da se verjetno lahko določi stroškovno učinkovitejše varnostne ukrepe za nadzor tveganja, če je opredelitev nevarnosti podrobnejša.

2.2.6. Whenever a code of practices or a reference system is used to control the risk, the hazard identification can be limited to:

- (a) The verification of the relevance of the code of practices or of the reference system.*
(b) The identification of the deviations from the code of practices or from the reference system.

- [G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

2.3. Uporaba kodeksov ravnanja in ovrednotenje tveganj

2.3.1. *The proposer, with the support of other involved actors and based on the requirements listed in point 2.3.2, shall analyse whether one or several hazards are appropriately covered by the application of relevant codes of practice.*

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

2.3.2. *The codes of practice shall satisfy at least the following requirements:*

- (a) be widely acknowledged in the railway domain. If this is not the case, the codes of practice will have to be justified and be acceptable to the assessment body;*
- (b) be relevant for the control of the considered hazards in the system under assessment;*
- (c) be publicly available for all actors who want to use them.*

[G 2] Ocenjuje se, da dodatna obrazložitev ni potrebna.

2.3.3. *Where compliance with TSIs is required by Directive 2008/57/EC and the relevant TSI does not impose the risk management process established by this Regulation, the TSIs may be considered as codes of practice for controlling hazards, provided requirement (c) of point 2.3.2 is fulfilled.*

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

2.3.4. *National rules notified in accordance with Article 8 of Directive 2004/49/EC and Article 17(3) of Directive 2008/57/EC may be considered as codes of practice provided the requirements of point 2.3.2 are fulfilled.*

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

2.3.5. *If one or more hazards are controlled by codes of practice fulfilling the requirements of point 2.3.2, then the risks associated with these hazards shall be considered as acceptable. This means that:*

- (a) these risks need not be analysed further;*
- (b) the use of the codes of practice shall be registered in the hazard record as safety requirements for the relevant hazards.*

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

2.3.6. *Where an alternative approach is not fully compliant with a code of practice, the proposer shall demonstrate that the alternative approach taken leads to at least the same level of safety.*

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

2.3.7. *If the risk for a particular hazard cannot be made acceptable by the application of codes of practice, additional safety measures shall be identified applying one of the two other risk acceptance principles.*

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

2.3.8. *When all hazards are controlled by codes of practice, the risk management process may be limited to:*

- (a) The hazard identification in accordance with section 2.2.6;*
- (b) The registration of the use of the codes of practice in the hazard record in accordance with section 2.3.5;*
- (c) The documentation of the application of the risk management process in accordance with section 5;*
- (d) An independent assessment in accordance with Article 6.*

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

2.4. Uporaba referenčnih sistemov in ovrednotenje tveganja

2.4.1. *The proposer, with the support of other involved actors, shall analyse whether one or more hazards are covered by a similar system that could be taken as a reference system.*

[G 1] Več informacij o teh načelih je na voljo v oddelku 8 smernice EN 50126-2 {Ref. 9}.

2.4.2. *A reference system shall satisfy at least the following requirements:*

- (a) it has already been proven in-use to have an acceptable safety level and would still qualify for acceptance in the Member State where the change is to be introduced;*
- (b) it has similar functions and interfaces as the system under assessment;*
- (c) it is used under similar operational conditions as the system under assessment;*
- (d) it is used under similar environmental conditions as the system under assessment.*

[G 2] Na primer, star sistem upravljanja-vodenja, za katerega se pokaže, da ima sprejemljivo stopnjo varnosti, se lahko nadomesti z drugim sistemom z novejšo tehnologijo in večjo varnostno učinkovitostjo. Zato je treba vsakič, ko se uporablja referenčni sistem, preveriti, ali ima še vedno sprejemljivo stopnjo varnosti.

[G 2] Ker so lahko na primer nekateri vidiki varnosti v predorih ali pri prevozu nevarnega blaga posebni ter odvisni od operativnih in okoljskih pogojev, je treba za vsak projekt preveriti, ali se bo sistem uporabljal pod enakimi pogoji.

2.4.3. If a reference system fulfils the requirements listed in point 2.4.2, then for the system under assessment:

- (a) the risks associated with the hazards covered by the reference system shall be considered as acceptable;*
- (b) the safety requirements for the hazards covered by the reference system may be derived from the safety analyses or from an evaluation of safety records of the reference system;*
- (c) these safety requirements shall be registered in the hazard record as safety requirements for the relevant hazards.*

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

2.4.4. If the system under assessment deviates from the reference system, the risk evaluation shall demonstrate that the system under assessment reaches at least the same safety level as the reference system. The risks associated with the hazards covered by the reference system shall, in that case, be considered as acceptable.

[G 1] Več informacij o analizah podobnosti je na voljo v oddelku 8.1.3. smernice EN 50126-2 {Ref. 9}.

2.4.5. If the same safety level as the reference system cannot be demonstrated, additional safety measures shall be identified for the deviations, applying one of the two other risk acceptance principles.

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

2.5. Eksplicitna ocena in ovrednotenje tveganja

2.5.1. When the hazards are not covered by one of the two risk acceptance principles described in sections 2.3 and 2.4, the demonstration of the risk acceptability shall be performed by explicit risk estimation and evaluation. Risks resulting from these hazards shall be estimated either quantitatively or qualitatively, taking existing safety measures into account.

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

2.5.2. *The acceptability of the estimated risks shall be evaluated using risk acceptance criteria either derived from or based on legal requirements stated in Community legislation or in notified national rules. Depending on the risk acceptance criteria, the acceptability of the risk may be evaluated either individually for each associated hazard or globally for the combination of all hazards considered in the explicit risk estimation.*

If the estimated risk is not acceptable, additional safety measures shall be identified and implemented in order to reduce the risk to an acceptable level.

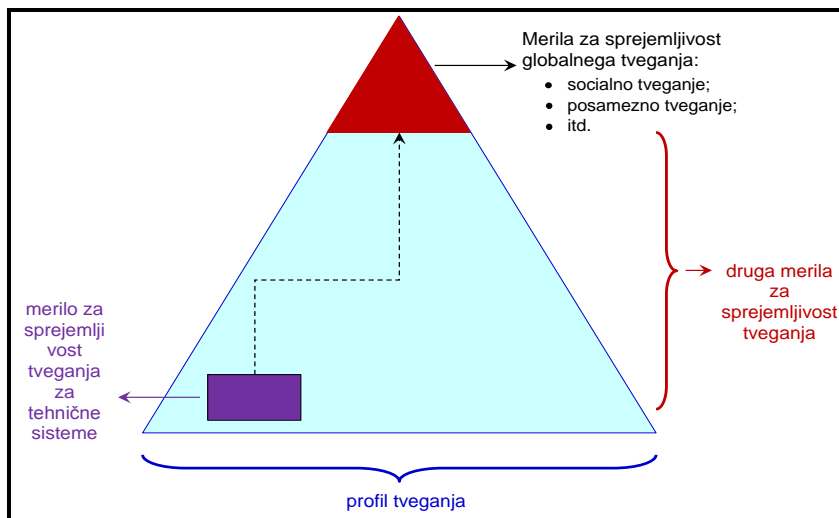
[G 1] Za ovrednotenje, ali so tveganja iz ocenjevanega sistema sprejemljiva ali ne, so potrebna merila za sprejemljivost tveganja (glej polja „ovrednotenje tveganja“ na Slika 1). Merila za sprejemljivost tveganja so lahko implicitna ali eksplicitna:

(a) implicitna merila za sprejemljivost tveganja: v skladu z oddelkoma 2.3.5. in 2.4.3. se tveganja, ki jih zajema uporaba kodeksov ravnanja in primerjava z referenčnimi sistemi, implicitno štejejo za sprejemljiva, če (glej pikčast krog na sliki 1):

- (1) so izpolnjeni pogoji uporabe kodeksov ravnanja iz oddelka 2.3.2.;
- (2) so izpolnjeni pogoji uporabe referenčnega sistema iz oddelka 2.4.2.;

(b) eksplicitna merila za sprejemljivost tveganja: Za ovrednotenje, ali je (so) tveganje(-a), ki se nadzoruje(-jo) z uporabo eksplicitne ocene tveganja, sprejemljivo(-a) ali ne, so potrebna eksplicitna merila za sprejemljivost tveganja (glej krog s polno črto na Slika 1 za tretje načelo). Ta so lahko opredeljena na različnih ravneh železniškega sistema. Lahko se obravnavajo kot „piramida meril“ (glej Slika 9), ki se začne z merili za sprejemljivost tveganja na visoki ravni (ki so izražena na primer kot družbeno ali posamezno tveganje) ter nadaljuje s podsistemi in komponentami (da se zajamejo tehnični sistemi), pri čemer so med dejavnostmi delovanja in vzdrževanja sistema in podsistemov vključeni človeški izvajalci. Čeprav merila za sprejemljivost tveganja prispevajo k doseganju varnostne učinkovitosti sistema in so zato povezana s SVC in NRV, je zelo težko oblikovati matematični model: za več podrobnosti o tem glej {Ref. 12}.

Stopnja, na kateri so opredeljena eksplicitna merila za sprejemljivost tveganja, mora ustrezati pomembnosti in kompleksnosti pomembne spremembe. Ni treba na primer ovrednotiti splošnega tveganja železniškega sistema, kadar se spreminja vrsta osi na tirnih vozilih. Opredelitev meril za sprejemljivost tveganja se lahko osredotoči na varnost tirnih vozil. Obratno se velike spremembe ali dodatki k obstoječemu železniškemu sistemu ne smejo vrednotiti le na podlagi varnostne učinkovitosti posameznih funkcij ali sprememb, ki so dodane. Tudi na ravni železniškega sistema je treba preveriti, ali je sprememba sprejemljiva kot celota.



Slika 9 : Piramida meril za sprejemljivost tveganja

- [G 2] Eksplicitna merila za sprejemljivost tveganja, ki so potrebna za podporo vzajemnega priznavanja, se bodo med državami članicami uskladila v okviru rednega dela Agencije v zvezi z merili za sprejemljivost tveganja. Dodatne informacije bodo vključene v ta dokument, ko bodo na voljo.
- [G 3] Medtem se lahko tveganja ovrednotijo na primer z uporabo matrice tveganja, ki je na voljo v oddelku 4.6. smernice EN 50126-1 {Ref. 8}. Uporabijo se lahko tudi druge vrste ustreznih meril, če se šteje, da ta merila zagotavljajo sprejemljivo stopnjo varnosti v zadevnem primeru.

2.5.3. When the risk associated with one or a combination of several hazards is considered as acceptable, the identified safety measures shall be registered in the hazard record.

- [G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

2.5.4. Where hazards arise from failures of technical systems not covered by codes of practice or the use of a reference system, the following risk acceptance criterion shall apply for the design of the technical system:

For technical systems where a functional failure has credible direct potential for a catastrophic consequence, the associated risk does not have to be reduced further if the rate of that failure is less than or equal to 10^{-9} per operating hour.

- [G 1] Nadaljnje podrobnosti o merilu za sprejemljivost tveganja za tehnične sisteme ter o tem, za katere vidike in funkcije tehničnega sistema se uporablja, so na voljo v obvestilu Agencije, ki je priloženo temu dokumentu: glej oddelek A.3. Dodatka A in referenčni dokument {Ref. 11}.

2.5.5. *Without prejudice to the procedure specified in Article 8 of Directive 2004/49/EC, a more demanding criterion may be requested, through a national rule, in order to maintain a national safety level. However, in the case of additional authorisations for placing in service of vehicles, the procedures of Articles 23 and 25 of Directive 2008/57/EC shall apply.*

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

2.5.6. *If a technical system is developed by applying the 10^{-9} criterion defined in point 2.5.4, the principle of mutual recognition is applicable in accordance with Article 7(4) of this Regulation.*

Nevertheless, if the proposer can demonstrate that the national safety level in the Member State of application can be maintained with a rate of failure higher than 10^{-9} per operating hour, this criterion can be used by the proposer in that Member State.

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

2.5.7. *The explicit risk estimation and evaluation shall satisfy at least the following requirements:*

- (a) the methods used for explicit risk estimation shall reflect correctly the system under assessment and its parameters (including all operational modes);*
- (b) the results shall be sufficiently accurate to serve as robust decision support, i.e. minor changes in input assumptions or prerequisites shall not result in significantly different requirements.*

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

3. DOKAZOVANJE SKLADNOSTI Z VARNOSTNIMI ZAHTEVAMI

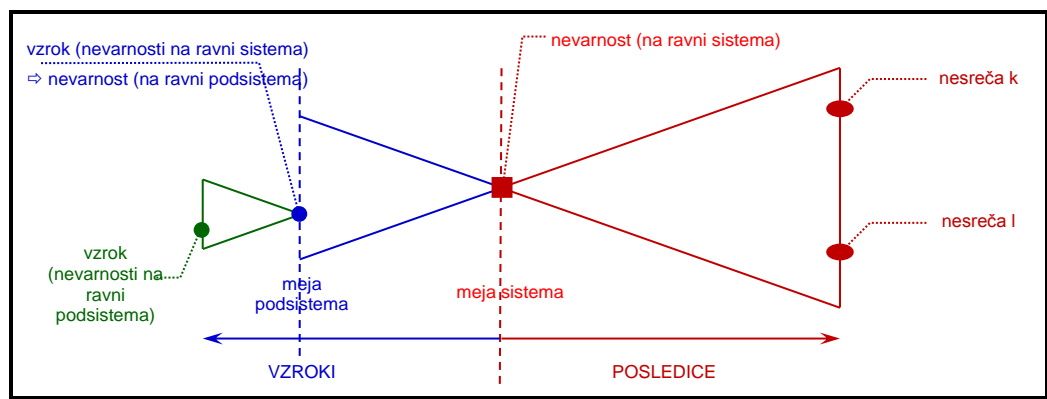
3.1. *Prior to the safety acceptance of the change, fulfilment of the safety requirements resulting from the risk assessment phase shall be demonstrated under the supervision of the proposer.*

[G 1] Kot je obrazloženo v točkah [G 3] do [G 6] oddelka 2.1.1., „dokazovanje skladnosti sistema z varnostnimi zahtevami“ vključuje faze 6 do 10 cikla V CENELEC (glej polje 3 na Slika 10). Glej točko [G 3] oddelka 2.1.1.

[G 2] Glej tudi točko [G 4] oddelka 2.1.1. tega dokumenta.

3.2. *This demonstration shall be carried out by each of the actors responsible for fulfilling the safety requirements, as decided in accordance with point 1.1.5.*

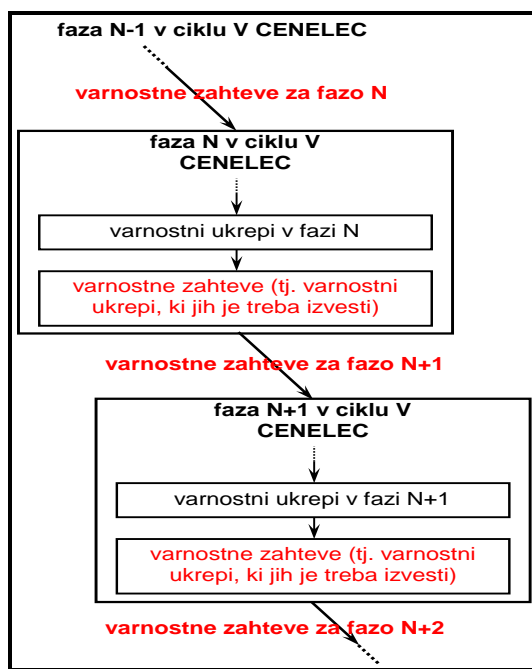
[G 1] Primer ocen in analiz varnosti, ki se lahko izvedejo na ravni podsistema, so vzročne analize: glej Slika 10. Vendar se lahko za dokazovanje skladnosti podsistema z vhodnimi varnostnimi zahtevami uporabi katera koli druga metoda.



Slika 10 : Slika A.4 iz EN 50129: opredelitev nevarnosti glede na mejo sistema

[G 2] Hierarhično strukturiranje nevarnosti in vzrokov v zvezi s sistemi in podsistemi se lahko ponovi za vsako fazo nižje stopnje cikla V CENELEC na Slika 10. Prav tako se lahko za vsako fazo cikla razvoja sistema ponovijo tudi dejavnosti glede opredelitve nevarnosti in vzročne analize (ali katere koli ustrezne metode) ter uporaba kodeksov ravnanja, podobnih referenčnih sistemov, eksplicitnih analiz in ovrednotenij, da se iz varnostnih ukrepov, opredeljenih na ravni podsistema, izpeljejo varnostne zahteve, ki morajo biti izpolnjene v naslednji fazi. To je prikazano na Slika 11.

[G 3] Glej tudi točko [G 4] oddelka 2.1.1. tega dokumenta.



Slika 11 : Izpeljava varnostnih zahtev za faze nižje stopnje

3.3. *The approach chosen for demonstrating compliance with the safety requirements as well as the demonstration itself shall be independently assessed by an assessment body.*

[G 1] Zato so neodvisno ocenjene tudi vse dejavnosti, predstavljene v polju 3⁽¹²⁾ cikla V CENELEC na Slika 10.

[G 2] Vrsta in stopnja podrobnosti za neodvisno oceno, ki jo izvedejo ocenjevalni organi (tj. podrobna ali makroskopska ocena), se obravnavata v obrazložitvah Člen 6.

3.4. *Any inadequacy of safety measures expected to fulfil the safety requirements or any hazards discovered during the demonstration of compliance with the safety requirements shall lead to reassessment and evaluation of the associated risks by the proposer according to section 2. The new hazards shall be registered in the hazard record according to section 4.*

[G 1] Na primer, način gašenja požara lahko povzroči novo nevarnost (zadušitev), zaradi katere bodo potrebne nove varnostne zahteve (npr. poseben postopek evakuacije potnikov). Drug primer je uporaba ojačanega stekla za preprečitev, da se okna v nesrečah razbijejo in steklo poškoduje potnike ali jih celo vrže skozi okno. Pri tem je povzročena nova nevarnost, da je

(12) Povezava na področju dejavnosti med skupno varnostno metodo in Slika 10 (tj. slika 10 cikla V CENELEC 50126) je opisana v oddelku 2.1.1. Zlasti točka [G 3] oddelka 2.1.1. navaja, katere dejavnosti CENELEC so vključene v fazo „dokazovanja skladnosti sistema z varnostnimi zahtevami“ iz skupne varnostne metode.

- evakuacija vagonov v sili skozi okna veliko težja, posledica česar so lahko varnostne zahteve, da morajo biti nekatera okna posebej izdelana za omogočanje evakuacije.
- [G 2] Primer operative spremembe: zahteva se, da se prepovejo vsi prevozi nevarnega blaga po progah skozi gosto poseljena območja. Namesto tega mora tak prevoz potekati po drugi poti s predori, kar ustvarja različne vrste nevarnosti.
- [G 3] Drugi primeri novih nevarnosti, ki se lahko opredelijo med dokazovanjem skladnosti sistema z varnostnimi zahtevami, so navedeni v Dodatku A.4.3. k standardu EN 50129.

4. UPRAVLJANJE Z NEVARNOSTMI

4.1. Postopek upravljanja z nevarnostmi

4.1.1. Hazard record(s) shall be created or updated (where they already exist) by the proposer during the design and the implementation and till the acceptance of the change or the delivery of the safety assessment report. The hazard record shall track the progress in monitoring risks associated with the identified hazards. In accordance with point 2(g) of Annex III to Directive 2004/49/EC, once the system has been accepted and is operated, the hazard record shall be further maintained by the infrastructure manager or the railway undertaking in charge with the operation of the system under assessment as an integrated part of its safety management system.

- [G 1] Uporabo evidence nevarnosti za evidentiranje, obvladovanje in nadzorovanje informacij, povezanih z varnostjo, priporočata tudi standarda CENELEC 50126-1 {Ref. 8} in 50129 {Ref. 7}.
- [G 2] Udeleženec ima lahko glede na kompleksnost sistema na primer eno ali več evidenc nevarnosti. V obeh primerih evidenco(-e) nevarnosti neodvisno oceni(-jo) ocenjevalni organ(-i). Možna rešitev je na primer:
- (a) ena „notranja evidenca nevarnosti“ za upravljanje vseh notranjih varnostnih zahtev, ki veljajo za podsistem, za katerega je udeleženec odgovoren. Njen obseg in količina dela, povezanega z njenim upravljanjem, sta odvisna od njene strukture in seveda kompleksnosti podsistema. Vendar evidence nevarnosti ni treba predložiti drugim udeležencem, ker se uporablja za namene notranjega upravljanja. Notranja evidenca nevarnosti vsebuje vse opredeljene nevarnosti, ki se nadzirajo, in z njimi povezane varnostne ukrepe, ki so potrjeni;
 - (b) ena „zunanja evidenca nevarnosti“, da se v skladu z oddelkom 1.2.2. nevarnosti in z njimi povezani varnostni ukrepi (ki jih udeleženec sam ne more v celoti izvajati) prenesejo na druge udeležence. Običajno je ta druga evidenca nevarnosti manjša in je zanjo potrebnega manj dela, povezanega z upravljanjem (glej primer v oddelku C.16.4. Dodatka C).
- [G 3] Če se zdi upravljanje več evidenc nevarnosti zapleteno, je druga možna rešitev, da se vse nevarnosti in z njimi povezani varnostni ukrepi, ki jih zajemajo točke (a) do (b), upravljajo v eni sami evidenci nevarnosti, vendar z možnostjo dveh poročil o evidenci nevarnosti (glej primer v oddelku C.16.3. Dodatka C):
- (a) eno poročilo o notranji evidenci nevarnosti, ki niti ne bi bilo potrebno, če bi bila evidenca nevarnosti strukturirana tako dobro, da omogoči neodvisno oceno;
 - (b) eno poročilo o zunanji evidenci nevarnosti za prenos nevarnosti in z njimi povezanih varnostnih ukrepov na druge udeležence.
- [G 4] Kot je obrazloženo v oddelku 4.2., se na koncu projekta, ko je sistem sprejet:
- (a) vse nevarnosti, ki so prenesene na druge udeležence, nadzirajo v zunanji evidenci nevarnosti udeleženca, ki jih je prenesel. Ker so uvožene v notranje evidence nevarnosti drugih udeležencev in se v njih upravljajo, ni treba, da jih zadeven udeleženec nadalje upravlja med življenjskim ciklom (pod)sistema;
 - (b) se vsi z njimi povezani varnostni ukrepi kljub temu ne smejo potrditi v evidenci nevarnosti iz razlogov, ki so obrazloženi v točki [G 9] oddelka 4.2. Koristno je, da organizacija, ki izvaža omejitve uporabe, v svoji evidenci nevarnosti jasno navede, da z njimi povezani varnostni ukrepi, niso bili potrjeni.

- [G 5] Obratno se vse notranje evidence nevarnosti vodijo v celotnem življenjskem ciklu (pod)sistema. To omogoča opazovanje napredka pri spremljanju tveganj, povezanih z opredeljenimi nevarnostmi, med delovanjem in vzdrževanjem (pod)sistema, tj. celo po začetku njegovega obratovanja: glej polje 4 cikla V CENELEC na Slika 5.

4.1.2. The hazard record shall include all hazards, together with all related safety measures and system assumptions identified during the risk assessment process. In particular, it shall contain a clear reference to the origin and to the selected risk acceptance principles and shall clearly identify the actor(s) in charge of controlling each hazard.

- [G 1] Informacije o nevarnostih in z njimi povezanih varnostnih ukrepov, ki jih sporočijo drugi udeleženci (glej oddelek 1.2.2.), vključujejo tudi vse predpostavke⁽¹³⁾ in omejitve uporabe⁽¹³⁾ (imenovane tudi pogoji uporabe v zvezi z varnostjo), ki veljajo za različne podsisteme, varnostne analize za generični proizvod in generične aplikacije, ki jih pripravijo proizvajalci, kadar je primerno.
- [G 2] Možen primer strukture evidence nevarnosti je opisan v oddelku C.16.. Dodatka C.

4.2. Izmenjava informacij

All hazards and related safety requirements which cannot be controlled by one actor alone shall be communicated to another relevant actor in order to find jointly an adequate solution. The hazards registered in the hazard record of the actor who transfers them shall only be "controlled" when the evaluation of the risks associated with these hazards is made by the other actor and the solution is agreed by all concerned.

- [G 1] Na primer, proizvajalec lahko za podsistem opreme ETCS na vozilu za meritev poti in hitrosti v laboratoriju potrdi algoritme s simulacijo teoretičnih signalov, ki bi jih lahko sprožile s tem povezane odometrične naprave za zaznavanje. Vendar je za potrditev podsistema meritve poti in hitrosti v celoti potrebna pomoč prevoznika v železniškem prometu in upravljavca železniške infrastrukture, da se potrditev izvede z uporabo dejanskih vlakov in dejanskega stika koles vlaka s tračnicami.
- [G 2] Drugi primeri bi lahko bili prenosi varnostnih ukrepov v zvezi z delovanjem ali vzdrževanjem za tehnično opremo od proizvajalcev na prevoznike v železniškem prometu. Te varnostne ukrepe bodo morali izvajati prevozniki v železniškem prometu.
- [G 3] Da lahko vključene organizacije ponovno ocenijo te nevarnosti ter z njimi povezane varnostne ukrepe in tveganja, je koristno, da organizacija, ki jih je opredelila, zagotovi vse obrazložitve, potrebne za dobro razumevanje problema. Lahko se zgodi, da je treba prvotno besedilo v zvezi z nevarnostmi, varnostnimi ukrepi in tveganji spremeniti, da se omogoči njihova razumljivost, brez da bi bilo treba o njih ponovno skupaj razpravljati. Posledica ponovne skupne ocene nevarnosti je lahko opredelitev novih varnostnih ukrepov.

⁽¹³⁾ Za dodatno obrazložitev v zvezi z izrazi varnostne analize za „generični proizvod in generično aplikacijo“ ter „predpostavke in omejitve uporabe“ glej točko [G 5] oddelka 1.1.5. ter opombi (7) in (8) na strani 28 tega dokumenta.

- *****
- [G 4] Udeleženec prejemnik, ki je odgovoren za izvajanje, preverjanje in potrjevanje prejetih ali novih varnostnih ukrepov, v svoji evidenci nevarnosti evidentira vse zadevne nevarnosti in z njimi povezane varnostne ukrepe (uvožene in skupno opredeljene).
- [G 5] Kadar varnostni ukrep ni v celoti potrjen, je treba pripraviti jasno omejitev uporabe (npr. operativni ukrepi za ublažitev) in jo evidentirati v evidenci nevarnosti. Možno je, da se tehnični varnostni ukrepi/varnostni ukrepi glede projektiranja:
- (a) ne izvajajo pravilno;
 - (b) ne izvajajo v celoti ali;
 - (c) namerno ne izvajajo, ker se na primer namesto tistih, ki so evidentirani v evidenci nevarnosti, izvajajo drugačni varnostni ukrepi (npr. zaradi stroškov). Ker taki varnostni ukrepi niso potrjeni, morajo biti v evidenci nevarnosti jasno opredeljeni. Predložen mora biti tudi dokaz/utemeljitev, zakaj so varnostni ukrepi, ki se izvajajo namesto tistih, evidentiranih v evidenci nevarnosti⁽¹⁴⁾, ustrezni, ter dokaz, da je z nadomestnimi varnostnimi ukrepi sistem usklajen z varnostnimi zahtevami;
 - (d) itd.
- V teh primerih se zadevni tehnični varnostni ukrepi/varnostni ukrepi glede projektiranja ne morejo preverjati in potrditi med obvladovanjem nevarnosti. Zadevna(-e) nevarnost(-i) in varnostni ukrepi morajo v evidenci nevarnosti ostati odprti, da se prepreči napačna uporaba varnostnih ukrepov za druge sisteme z uporabo načela sprejemljivosti tveganja, in sicer „podobnega referenčnega sistema“.
- [G 6] Običajno se varnostni ukrepi, ki se izvajajo „nepravilno“ in/ali ki se „ne izvajajo v celoti“, odkrijejo na začetku življenjskega cikla sistema in so popravljeni pred sprejetjem sistema. Če so kljub temu odkriti prepozno za pravilno in popolno izvajanje tehničnega varnostnega ukrepa, mora organizacija, ki je odgovorna za izvajanje in upravljanje, v evidenci nevarnosti opredeliti in evidentirati jasne omejitve uporabe za ocenjevani sistem. Te omejitve uporabe so pogosto omejitve operativne uporabe za ocenjevani sistem.
- [G 7] Koristno je lahko tudi, da se v evidenci nevarnosti evidentira, ali se bodo s tem povezani varnostni ukrepi pravilno izvajali na poznejši stopnji življenjskega cikla sistema ali se bo sistem še naprej uporabljal z opredeljenimi omejitvami uporabe. Prav tako bi lahko bilo koristno, da se v evidenci nevarnosti utemelji, zakaj se s tem povezani tehnični varnostni ukrepi ne izvajajo pravilno/v celoti.
- [G 8] Udeleženec, ki prejme omejitve uporabe:
- (a) vse uvozi v svojo evidenco nevarnosti;
 - (b) zagotovi, da so pogoji uporabe ocenjevanega sistema skladni z vsemi prejetimi omejitvami uporabe;
 - (c) preveri in potrdi, ali je ocenjevani sistem skladen s temi omejitvami uporabe.
- [G 9] Glede na odločitve, o katerih so se sporazumele vključene organizacije:
- (a) se zadevni tehnični varnostni ukrepi pravilno izvajajo pri projektiranju na poznejši stopnji. Organizacija, ki izvaža omejitve uporabe, še naprej spremlja pravilno tehnično izvajanje s tem povezanih varnostnih ukrepov. Zato zadevni varnostni ukrepi ne morejo biti potrjeni in nevarnosti, ki so z njimi povezane, nadzorovane v evidenci nevarnosti te

(14) Če se namesto prvotno določenih varnostnih ukrepov izvajajo drugi varnostni ukrepi, jih je treba prav tako evidentirati v evidenci nevarnosti.

organizacije, dokler se ustrezni tehnični varnostni ukrepi ne izvajajo v celoti. To je treba zagotoviti, čeprav so v vmesnem času vzpostavljene izvožene omejitve uporabe;

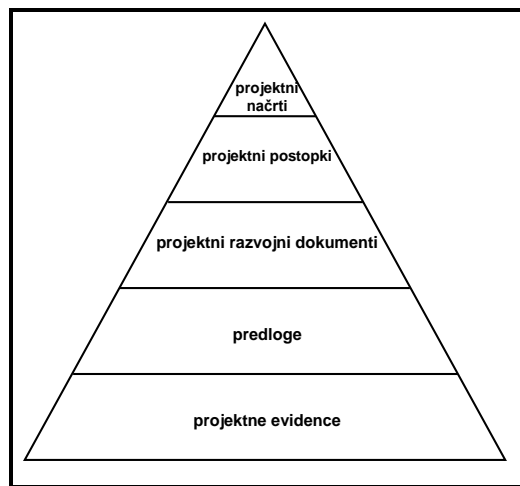
- (b) ali pa se zadevni tehnični varnostni ukrepi ne bodo izvajali pri projektiranju na poznejši stopnji. Tako se bo sistem še naprej uporabljal v svojem celotnem življenjskem ciklu s povezanimi omejitvami uporabe. V tem primeru se lahko stori naslednje:
- (1) organizacija, ki izvaža omejitve uporabe, s tem povezanih varnostnih ukrepov v svoji evidenci nevarnosti ne evidentira kot „potrjenih“. Na ta način ustrezni varnostni ukrepi pri uporabi zadevnega sistema kot referenčnega sistema v drugih projektih ne bodo spregledani. Tudi če se drug udeleženec odloči, da bo s tem povezana tveganja obvladoval drugače, je koristno, da organizacija, ki izvaža omejitve uporabe, v svoji evidenci nevarnosti jasno poudari, da s tem povezani varnostni ukrepi niso bili potrjeni;
 - (2) opis sistema se lahko spremeni, da se omejitve uporabe vključijo v okvir uporabe sistema (tj. predpostavke za sistem) in v varnostne zahteve. To bo omogočilo nadzor nevarnosti. Če se bo sistem uporabljal kot referenčni sistem v drugi aplikaciji:
 - (i) se bo moral nov sistem uporabljati pod enakimi pogoji (tj. za izpolnjevanje omejitev uporabe, povezanih s temi predpostavkami), ali
 - (ii) bo predlagatelj izvedel dodatno oceno tveganja za odstopanja od teh predpostavk.

5. DOKAZILA O UPORABI POSTOPKA UPRAVLJANJA S TVEGANJI

5.1. *The risk management process used to assess the safety levels and compliance with safety requirements shall be documented by the proposer in such a way that all the necessary evidence showing the correct application of the risk management process is accessible to an assessment body. The assessment body shall establish its conclusion in a safety assessment report.*

[G 1] Te zahteve obravnava že sistem varnega upravljanja upravljavca železniške infrastrukture in prevoznika v železniškem prometu. Drugi udeleženci v železniškem sektorju, ki so vključeni v pomembno spremembo, imajo na splošno vsaj na ravni projekta postopek vodenja kakovosti in/ali varnega upravljanja, čeprav sistem varnega upravljanja ni obvezen. Oba postopka temeljita na strukturirani dokumentacijski hierarhiji v podjetju ali vsaj v okviru projekta. Obravnavata tudi dokumentacijske potrebe glede upravljanja zanesljivosti, razpoložljivosti, vzdrževalnosti in varnosti. Taka strukturirana dokumentacija je lahko v glavnem sestavljena iz naslednjega (glej sliko 12):

- (a) **Projektne načrti** zajemajo opis organizacije, ki jo je treba vzpostaviti za upravljanje dejavnosti v okviru projekta.
- (b) **Projektne postopki** zajemajo podroben opis načina za opravljanje posebne naloge. Postopki in navodila običajno že obstajajo v podjetju ter se kot taki uporabljajo. Novi projektne postopki se pripravijo le, če je treba opisati posebno nalogo v okviru projekta.
- (c) **Projektne razvojni dokumenti** se pripravijo v okviru življenjskega cikla sistema, predstavljenega na Slika 5.
- (d) **Predloge podjetja ali vsaj projekta** so namenjene pripravi različnih vrst dokumentov, ki jih je treba izdelati.
- (e) **Projektne evidence** se pripravijo v okviru projekta in so potrebne za dokazovanje skladnosti s postopkoma vodenja kakovosti in/ali varnega upravljanja podjetja.



Slika 12 : Strukturirana dokumentacijska hierarhija

To je eden od načinov za izpolnjevanje potreb po dokumentiranih dokazih. Mogoči so tudi drugi načini, dokler so izpolnjena merila skupne varnostne metode.

[G 2] Standardi CENELEC priporočajo, da se skladnost sistema s funkcionalnimi in varnostnimi zahtevami dokaže v dokumentu o varnostni analizi (ali v poročilu o varnosti). Čeprav uporaba varnostne analize ni obvezna, v dokumentu o strukturirani utemeljitvi varnosti zagotavlja:

- (a) dokaze o vodenju kakovosti;
- (b) dokaze o varnem upravljanju;
- (c) dokaze o funkcionalni in tehnični varnosti.

Hkrati ima prednost, da podpira in usmerja ocenjevalni(-e) organ(-e) pri neodvisni oceni pravilne uporabe skupne varnostne metode.

[G 3] Varnostna analiza opisuje in povzema, kako so v okviru postopka razvoja sistema med seboj povezani dokumenti projekta, ki izhajajo iz uporabe postopka podjetja ali projekta za vodenje kakovosti in/ali varno upravljanje, da se prikaže varnost sistema. Običajno varnostna analiza ne vključuje velike količine podrobnih dokazov in podporne dokumentacije, ampak zagotavlja natančne reference takšnih dokumentov.

[G 4] **Varnostna analiza za tehnične sisteme:** Standardi CENELEC se lahko uporabljajo kot smernice za pisanje in/ali strukturo varnostnih analiz:

- (a) glej standard EN 50129 {Ref. 7} za „Železniške aplikacije – Sistemi komunikacije, signalizacije in obdelave – Varnost v zvezi z elektronskimi sistemi signalizacije“; Dodatek H.2. k smernici EN 50126-2 {Ref. 9} prav tako predlaga strukturo varnostne analize za sisteme signalizacije;
- (b) glej Dodatek H.1. k smernici EN 50126-2 {Ref. 9} za strukturo varnostne analize za tirno vozilo;
- (c) glej Dodatek H.3. k smernici EN 50126-2 {Ref. 9} za strukturo varnostne analize za infrastrukturo.

Kot je razvidno iz teh referenc, sta struktura varnostne analize za tehnične sisteme in njena vsebina odvisni od sistema, za katerega je treba zagotoviti dokaz skladnosti z varnostnimi zahtevami.

Varnostna analiza, določena v Dodatku H k smernici EN 50126-2 {Ref. 9}, zagotavlja le primere in morda ni primerna za vse sisteme zadevne vrste. Zato je treba pri uporabi predloge ustrezno presoditi, kaj je primerno za posamezno aplikacijo.

[G 5] **Varnostna analiza za organizacijske in operativne vidike železniških sistemov**

Zaenkrat ni posebnega standarda, ki bi določal strukturo, vsebino in smernice za pisanje varnostne analize za organizacijske in operativne vidike železniškega sistema. Kljub temu je cilj varnostne analize na strukturiran način dokazati skladnost sistema z njegovimi varnostnimi zahtevami, zato se lahko uporabi enaka struktura varnostne analize, kot se uporablja za tehnične sisteme. Reference iz točke [G 4] oddelka 5.1. vsebujejo nasvete in kontrolni seznam točk, ki jih je treba obravnavati ne glede na vrsto ocenjevanega sistema. Za upravljanje organizacijskih in operativnih sprememb se zahtevata enaka postopka vodenja kakovosti in varnega upravljanja kot pri tehničnih spremembah z dokazom skladnosti sistema z določenimi varnostnimi zahtevami. Za organizacijske in operativne spremembe ne veljajo zahteve iz standardov CENELEC, ki so povezane izključno z obrati za projektiranje tehničnega sistema, kot so na primer načela „varnosti vgrajene strojne opreme“, elektromagnetna združljivost, itd.

5.2. *The document produced by the proposer under point 5.1. shall at least include:*

- (a) description of the organisation and the experts appointed to carry out the risk assessment process,*
- (b) results of the different phases of the risk assessment and a list of all the necessary safety requirements to be fulfilled in order to control the risk to an acceptable level.*

[G 1] Glede na kompleksnost sistema se lahko dokazi zberejo v eni ali več varnostnih analizah. Glej točki [G 4] in 5.1.[G 5] oddelka 5.1. za strukturo varnostne analize za tehnične sisteme ter operativne in organizacijske vidike.

[G 2] Glej tudi oddelek A.4. Dodatka A za morebitne primere dokazov.

- *****
- [G 3] Na splošno se pričakuje, da je življenjska doba tehničnih sistemov in podsistemov v železniškem sektorju približno 30 let. V tako dolgem obdobju se verjetno lahko pričakuje tudi več pomembnih sprememb teh sistemov. Zato se lahko izvedejo dodatne ocene tveganja za te sisteme in njihove vmesnike s spremljajočo dokumentacijo, ki jo bo treba pregledati, dopolniti in prenesti na različne udeležence in organizacije, ki uporabljajo evidence nevarnosti. Za to so potrebne precej stroge zahteve glede nadzora dokumentacije in upravljanja konfiguracije.
- [G 4] Zato je koristno, da podjetje, ki arhivira vse informacije v zvezi z oceno in obvladovanjem tveganja, zagotavlja, da so rezultati/informacije shranjeni na fizičnem nosilcu, ki se lahko bere/dostopa celotno življenje (življenjski cikel) sistema (npr. 30 let).
- [G 5] Glavni razlogi za to zahtevo so med drugim:
- (a) zagotavljanje, da so vse analize varnosti in evidence o varnosti ocenjevanega sistema dostopne celoten življenjski cikel sistema. Zato je:
 - (1) v primeru nadaljnjih pomembnih sprememb istega sistema na voljo najnovejša dokumentacija o sistemu;
 - (2) v primeru kakršnih koli težav v življenjskem ciklu sistema možnost vpogleda v s tem povezane analize varnosti in evidence o varnosti koristna;
 - (b) zagotavljanje, da so dostopne vse analize varnosti in evidence o varnosti ocenjevanega sistema, če se ta uporabi v drugi aplikaciji kot podoben referenčni sistem.

PRILOGA II K UREDBI O SKUPNI VARNOSTNI METODI

Merila, ki jih morajo izpolnjevati ocenjevalni organi

1. *The assessment body may not become involved either directly or as authorised representatives in the design, manufacture, construction, marketing, operation or maintenance of the system under assessment. This does not exclude the possibility of an exchange of technical information between that body and all the involved actors.*
2. *The assessment body must carry out the assessment with the greatest possible professional integrity and the greatest possible technical competence and must be free of any pressure and incentive, in particular of a financial type, which could affect their judgement or the results of their assessments, in particular from persons or groups of persons affected by the assessments.*
3. *The assessment body must possess the means required to perform adequately the technical and administrative tasks linked with the assessments; it shall also have access to the equipment needed for exceptional assessments.*
4. *The staff responsible for the assessments must possess:*
 - *proper technical and vocational training,*
 - *a satisfactory knowledge of the requirements relating to the assessments that they carry out and sufficient practice in those assessments,*
 - *the ability to draw up the safety assessment reports which constitute the formal conclusions of the assessments conducted.*
5. *The independence of the staff responsible for the independent assessments must be guaranteed. No official must be remunerated either on the basis of the number of assessments performed or of the results of those assessments.*
6. *Where the assessment body is external to the proposer's organisation must have its civil liability ensured unless that liability is covered by the State under national law or unless the assessments are carried out directly by that Member State.*
7. *Where the assessment body is external to the proposer's organisation its staff are bound by professional secrecy with regard to everything they learn in the performance of their duties (with the exception of the competent administrative authorities in the State where they perform those activities) in pursuance of this Regulation.*

[G 1] Ocenjuje se, da dodatna obrazložitev ni potrebna.

DODATEK A: DODATNA POJASNILA

A.1. Uvod

- A.1.1. Namen tega dodatka je olajšati branje tega dokumenta. Namesto velike količine informacij v okviru samega dokumenta so v tem dodatku podrobneje razložene bolj zapletene teme.

A.2. Razvrstitev nevarnosti

- A.2.1. Oddelek 4.6.3. standarda EN 50126-1 {Ref. 8} in Dodatek B.2. k smernici EN 50126-2 {Ref. 9} vsebujeta smernico za razvrstitev/uvrstitev nevarnosti.

A.3. Merilo za sprejemljivost tveganja za tehnične sisteme (MST-TS)

A.3.1. Zgornja meja sprejemljivosti tveganja za tehnične sisteme

- A.3.1.1. Merilo za sprejemljivost tveganja za tehnične sisteme je opisano v oddelku 2.5.4. {Ref. 4}.
- A.3.1.2. Namen merila za sprejemljivost tveganja za tehnične sisteme je določiti zgornjo mejo sprejemljivosti tveganja za tehnične sisteme, za katere ni mogoče izpeljati varnostnih zahtev z uporabo kodeksov ravnanja niti s primerjavo s podobnimi referenčnimi sistemi. Zato določa referenčno točko, na podlagi katere je mogoče kalibrirati metode za analizo tveganja za tehnične sisteme. Kot je opisano v oddelku A.3.6. Dodatka A k temu dokumentu, se lahko ta referenčna točka ali zgornja meja sprejemljivosti tveganja uporabi tudi za določitev merila za sprejemljivost tveganja za druge napake v delovanju tehničnih sistemov, pri katerih ni verjetne neposredne možnosti za katastrofalno posledico (tj. za druge stopnje resnosti). Vendar merilo za sprejemljivost tveganja za tehnične sisteme ni metoda za analizo tveganja.
- A.3.1.3. Merilo za sprejemljivost tveganja za tehnične sisteme je delno kvantitativno merilo. Uporablja se za naključne okvare strojne opreme in sistematične okvare/napake tehničnega sistema. Zajete so torej tudi sistematične okvare/napake tehničnega sistema, ki bi lahko bile posledica človeške napake pri razvojnem postopku tehničnega sistema (tj. podroben opis, projektiranje, izvajanje in potrjevanje). Vendar merilo za sprejemljivost tveganja za tehnične sisteme ne vključuje človeških napak med delovanjem in vzdrževanjem tehničnih sistemov.
- A.3.1.4. V skladu z dodatkom A.3. in A.4. k standardu CENELEC 50129 sistematične okvare/napake niso kvantitativno opredeljive, zato je treba kvantitativni cilj prikazati le za naključne okvare strojne opreme, medtem ko se sistematične okvare/napake obravnavajo s kvalitativnimi metodami⁽¹⁵⁾. „*Ker integritete sistematične okvare ni mogoče oceniti s kvantitativnimi metodami, se uporabijo stopnje varnostne integritete za združitev metod, orodij in tehnik, za katere se šteje, da ob učinkoviti uporabi zagotavljajo ustrezno stopnjo zaupanja pri izvedbi sistema na navedeni stopnji integritete.*“

⁽¹⁵⁾ V skladu s standardi CENELEC 50126, 50128 in 50129 mora biti kvantitativna vrednost, ki obravnava naključne okvare strojne opreme, vedno povezana s stopnjo varnostne integritete za obvladovanje sistematičnih okvar/napak. Zato vrednost $10^{-9} h^{-1}$ merila za sprejemljivost tveganja za tehnične sisteme zahteva tudi vzpostavitev ustreznega postopka za pravilno obvladovanje sistematičnih okvar/napak. Vendar se za lažje branje opombe pogosto nanaša le na naključne okvare strojne opreme tehničnega sistema.

- *****
- A.3.1.5. Podobno v skladu s standardi CENELEC tudi integriteta programske opreme tehničnih sistemov ni kvantitativno opredeljiva. Standard CENELEC 50128 vsebuje navodila za razvojni postopek programske opreme, povezane z varnostjo, glede na zahtevano stopnjo varnostne integritete. To vključuje postopke projektiranja, preverjanja, potrjevanja in zagotavljanja kakovosti programske opreme.
V skladu s standardom CENELEC 50128 je za programirljive elektronske nadzorne sisteme izvajanje varnostnih funkcij najvišja možna stopnja varnostne integritete za proces razvoja programske opreme SIL 4, ki ustreza kvantitativni dopustni stopnji nevarnosti $10^{-9} h^{-1}$.
- A.3.1.6. Ker sistematične okvare/napake ne morejo biti kvantitativno opredeljene, jih je treba upravljati kvalitativno z vzpostavitvijo postopka kakovosti in postopka varnosti, ki sta združljiva s stopnjo varnostne integritete, zahtevane za ocenjevani sistem:
- (a) namen postopka kakovosti je „*čim bolj zmanjšati pojavnost človeških napak na vseh stopnjah življenjskega cikla in s tem zmanjšati tveganje sistematičnih napak v sistemu*“;
 - (b) namen postopka varnosti je „*dodatno zmanjšati pojavnost človeških napak, povezanih z varnostjo, skozi celoten življenjski cikel in s tem zmanjšati preostalo tveganje sistematičnih napak, povezanih z varnostjo*“.
- A.3.1.7. Navodila za obvladovanje pojavnosti sistematičnih okvar/napak ter navodila za morebitne ukrepe v zvezi s projektiranjem za zaščito pred okvarami s skupnim vzrokom/načinom in za zagotovitev, da je tehnični sistem varen v primeru takšnih okvar/napak, so na voljo v naslednjih standardih:
- (a) standard CENELEC 50126-1 {Ref. 8} in njegov priročnik 50126-2 {Ref. 9} navajata klavzule CENELEC 50129 in njihovo uporabo za dokumentirane dokaze za sisteme, ki niso sistemi signalizacije: glej tabelo 9.1. v priročniku 50126-2 {Ref. 9}. Ta seznam vsebuje sklicevanje na navodila, kako obravnavati napake, ki izhajajo iz samega sistema, in učinek okolja na ocenjevani sistem.

Na primer tehnike/ukrepi za konstrukcijske posebnosti so navedeni v „*tabeli E.5.: konstrukcijske posebnosti (iz 5.4.)*“ standarda CENELEC 50129 {Ref. 7} „*za preprečitev in nadzor napak, ki jih povzročijo*:
 - (1) *kakršne koli preostale napake pri projektiranju;*
 - (2) *okoljski pogoji;*
 - (3) *napačna uporaba ali napake pri delovanju;*
 - (4) *kakršne koli preostale napake v programski opremi;*
 - (5) *človeški dejavniki*“.
Dodatka D in E k standardu CENELEC 50129 {Ref. 7} zagotavljata tehnike in ukrepe za preprečevanje sistematičnih napak ter nadzor naključnih okvar strojne opreme in sistematičnih okvar/napak za elektronske sisteme, povezane z varnostjo, na področju signalizacije. Veliko se jih lahko razširi na sisteme, ki niso sistemi signalizacije, prek sklicevanja na te smernice v tabeli 9.1. iz priročnika 50126-2 {Ref. 9};
 - (b) standard CENELEC 50128 vsebuje navodila za razvojni postopek programske opreme, povezane z varnostjo, glede na stopnjo varnostne integritete (SIL 0 do SIL 4), ki se zahteva za programsko opremo ocenjevanega sistema.
- A.3.1.8. Merilo za sprejemljivost tveganja za tehnične sisteme predstavlja tudi najvišjo stopnjo integritete, ki se lahko zahteva v skladu s standardi CENELEC in IEC. Za lažje sklicevanje so citirane zahteve iz standardov IEC 61508-1 in CENELEC 50129:
- (a) IEC 61508-1: „*Ta standard pri nevarni okvari določa nižjo mejo ciljnih ravni okvare, kot se lahko zahteva. Te so določene kot nižje meje za stopnjo 4 varnostne integritete.*“

Mogoča so projektiranja sistemov, povezanih z varnostjo, z nižjimi vrednostmi za ciljne ravni okvare za nekompleksne sisteme, vendar se šteje, da vrednosti v tabeli predstavljajo meje, ki se lahko zaenkrat dosežejo za razmeroma kompleksne sisteme (na primer programirljive elektronske sisteme, povezane z varnostjo)."

- (b) EN 50129: „Funkcija, ki ima kvantitativne zahteve, strožje od $10^{-9} h^{-1}$, se obravnava na enega od naslednjih načinov:
- (1) če je mogoče funkcijo razdeliti na funkcionalno neodvisne podfunkcije, se lahko dopustna stopnja nevarnosti razdeli med te podfunkcije in se vsaki podfunkciji dodeli stopnja varnostne integritete;
 - (2) če funkcije ni mogoče razdeliti, se izpolnijo vsaj ukrepi in metode, zahtevani za stopnjo 4 varnostne integritete, pri čemer se funkcija uporabi v kombinaciji z drugimi tehničnimi in operativnimi ukrepi, da se doseže potrebna dopustna stopnja nevarnosti.“

A.3.1.9. Vsi tehnični sistemi morajo nato kvantitativno varnostno zahtevo omejiti na to vrednost. Če je potrebna višja stopnja zaščite, je ni mogoče doseči le z enim sistemom. Spremeniti je treba arhitekturo sistema, na primer z vzporedno uporabo dveh neodvisnih sistemov, ki se med seboj navzkrižno preverjata za ustvarjanje varnih rezultatov. Vendar to nedvomno povečuje stroške razvoja tehničnega sistema.

Opomba: če obstajajo funkcije, npr. popolnoma mehanski sistemi, ki lahko na podlagi operativnih izkušenj dosežejo višjo stopnjo integritete, se lahko stopnja varnosti opiše s posebnim kodeksom ravnanja ali pa se lahko varnostne zahteve določijo z analizo podobnosti z obstoječim sistemom. V okviru skupne varnostne metode se mora merilo za sprejemljivost tveganja za tehnične sisteme uporabljati le, če ni nobenega kodeksa ravnanja ali referenčnega sistema.

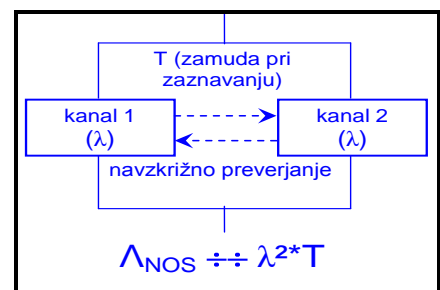
A.3.1.10. Lahko se torej povzame naslednje:

- (a) v skladu s standardi CENELEC 50126, 50128 in 50129 sistematične okvare/napake v razvoju niso kvantitativno opredeljive;
- (b) pojav sistematičnih okvar/napak in njihovega preostalega tveganja je treba nadzorovati in obvladovati z uporabo ustreznih postopkov kakovosti in varnosti, združiljivih s stopnjo varnostne integritete, ki je zahtevana za ocenjevani sistem;
- (c) najvišja dosegljiva stopnja varnostne integritete za naključne okvare strojne opreme in sistematične okvare/napake tehničnih sistemov je SIL 4;
- (d) ta omejitev stopnje varnostne integritete na SIL 4 pomeni, da je treba tudi najvišjo dopustno stopnjo nevarnosti (THR) (tj. najvišjo stopnjo okvar) za tehnične sisteme omejiti na $10^{-9} h^{-1}$.

A.3.1.11. Dopustno stopnjo nevarnosti $10^{-9} h^{-1}$ lahko tehnični sistem doseže z „varno arhitekturo“ (ki sama po sebi izpolnjuje takšno varnostno učinkovitost) ali „redundančno arhitekturo“ (npr. dva neodvisna kanala za obdelavo se navzkrižno preverjata).

Za redundančno arhitekturo je razvidno, da je splošna napaka pri oddajanju signala (Λ_{NOS}) tehničnega sistema sorazmerna z $\lambda^2 \cdot T$, kadar:

- (a) λ^2 predstavlja kvadrat stopnje napake pri oddajanju signala enega kanala;



Slika 13 : Redundančna arhitektura za tehnični sistem

- (b) T predstavlja čas, ki je potreben, da en kanal zazna napako(-e) pri oddajanju signala drugega kanala. To je običajno večkratnik časa/cikla za obdelavo kanala. T je običajno manj kot ena sekunda.

A.3.1.12. Na podlagi te formule ($\lambda^2 \cdot T$) se lahko teoretično prikaže (pri čemer se upoštevajo le naključne okvare strojne opreme tehničnega sistema – glej tudi točko A.3.1.13. Dodatka A), da se lahko kvantitativna zahteva 10^{-9} h^{-1} za merilo za sprejemljivost tveganja za tehnične sisteme doseže. Sistematične okvare/napake je treba upravljati s postopkom: glej točko A.3.1.6. Dodatka A. Na primer:

- (a) če je povprečni čas med okvarami 10 000 ur za vrednost zanesljivosti kanala in konservativna predpostavka, da ni nobena okvara kanala varna, je napaka pri oddajanju signala 10^{-4} h^{-1} ;

- (b) tudi pri času deset minut (tj. $\approx 2 \cdot 10^{-3}$ ur) za zaznavo napak(-e) pri oddajanju signala drugega kanala, kar je prav tako konservativna predpostavka;

je splošna napaka pri oddajanju signala $\Lambda_{\text{NOS}} \approx 2 \cdot 10^{-10} \text{ h}^{-1}$.

A.3.1.13. V praksi je treba za takšno redundančno arhitekturo pri ovrednotenju splošnih kvantitativnih napak strojne opreme pri oddajanju signala upoštevati ukrepe v zvezi s projektiranjem za zaščito pred okvarami s skupnim vzrokom/načinom in zagotovitev, da je tehnični sistem v primeru okvare/napake s skupnim vzrokom/načinom varen. Pri tem ovrednotenju splošne napake pri oddajanju signala (Λ_{NOS}) je zato treba upoštevati tudi:

- (a) komponente, skupne vsem kanalom, npr. posamezne ali skupne vhodne elemente v vse kanale, skupno napajanje, komparatorje, naprave za izbiranje itd.;
- (b) čas, potreben za zaznavo skritih ali neodkritih okvar. Pri kompleksnih tehničnih sistemih je lahko ta čas za več redov velikosti daljši od 1 sekunde;
- (c) vpliv okvar s skupnim vzrokom/načinom okvar.

Navodila o teh temah so na voljo v standardih, ki so navedeni v točki A.3.1.7. Dodatka A k temu dokumentu.

A.3.2. Shematski prikaz preskusa uporabe merila za sprejemljivost tveganja za tehnične sisteme

A.3.2.1. Način uporabe merila za sprejemljivost tveganja za tehnične sisteme za nevarnosti, ki izhajajo iz okvar tehničnih sistemov, se lahko predstavi, kot je prikazano na Slika 14

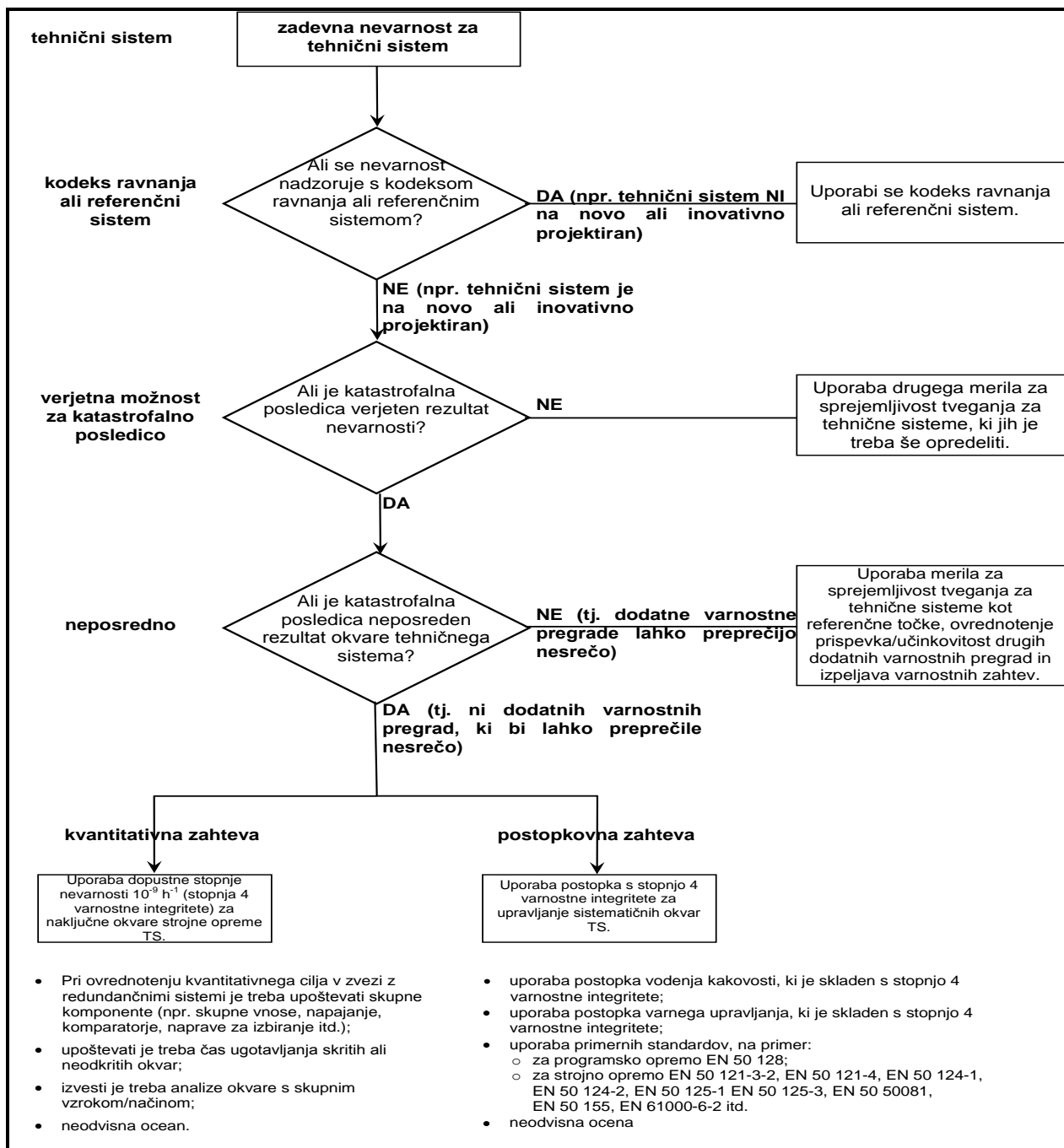
A.3.2.2. Uporaba tega shematskega prikaza na primeru je predstavljena v oddelku C.15. Dodatka C.

A.3.3. Opredelitev tehničnega sistema iz skupne varnostne metode

A.3.3.1. Merilo za sprejemljivost tveganja za tehnične sisteme se uporablja le za tehnične sisteme. V Člen 3(22)Uredbe o skupni varnostni metodi je določena naslednja opredelitev „tehničnega sistema“:

„tehnični sistem“ pomeni proizvod ali skupino proizvodov, vključno z zasnovano, uvedbo in podporno dokumentacijo; razvoj tehničnega sistema se prične z določitvijo zahtev, konča

pa z njegovo odobritvijo; čeprav se upošteva zasnova ustreznih vmesnikov s človeškim vedenjem, človeški izvajalci in njihova dejanja niso vključeni v tehnični sistem; postopek vzdrževanja je opisan v priročnikih za vzdrževanje, vendar ni del tehničnega sistema.



Slika 14 : Shematski prikaz preskusa uporabe merila za sprejemljivost tveganja za tehnične sisteme

A.3.4. Obrazložitev opredelitve „tehničnega sistema“

A.3.4.1. Ta opredelitev tehničnega sistema opisuje področje uporabe tehničnega sistema: „*tehnični sistem je proizvod ali skupina proizvodov, vključno z zasnovo, uvedbo in podporno dokumentacijo*“. Zato obsega in vključuje:

- (a) fizične elemente, ki sestavljajo tehnični sistem;
- (b) s tem povezano programsko opremo (če obstaja);
- (c) projektiranje in izvajanje tehničnega sistema, vključno s konfiguracijo ali parametrizacijo generičnega proizvoda v skladu s posebnimi zahtevami specifične aplikacije, če je primerno;
- (d) podporno dokumentacijo, potrebno za:
 - (1) razvoj tehničnega sistema;
 - (2) delovanje in vzdrževanje tehničnega sistema.

A.3.4.2. Opombe, povezane s to opredelitvijo, natančneje določajo področje uporabe tehničnega sistema:

- (a) „*Razvoj tehničnega sistema se prične z določitvijo zahtev, konča pa z varnostnim pooblastilom*“. Vključuje faze od 1 do 10 cikla V, predstavljenega na sliki 10 standarda CENELEC 50 126-1 {Ref. 8};
- (b) „*Upošteva zasnovo ustreznih vmesnikov s človeškim vedenjem. Vendar človeški izvajalci in njihova dejanja niso vključeni v tehnični sistem*“. Čeprav napake zaradi človeškega dejavnika med delovanjem in vzdrževanjem tehničnega sistema niso del tehničnega sistema samega, jih je treba pri projektiranju vmesnikov za človeške izvajalce upoštevati. Namen tega je čim bolj zmanjšati verjetnost človeških napak zaradi slabega projektiranja ustreznih vmesnikov za človeške izvajalce;
- (c) „*Opredelitev pojma ne zajema postopka vzdrževanja, slednji je opisan v priročnikih za vzdrževanje*“. To pomeni, da merila za sprejemljivost tveganja za tehnične sisteme ni treba uporabljati za delovanje in vzdrževanje tehničnega sistema; slednja sta odvisna zlasti od postopkov in ukrepov, ki jih izvaja človeško osebje.
Vendar mora opredelitev tehničnega sistema vključevati vse ustrezne zahteve (npr. redno preventivno vzdrževanje ali korektivno vzdrževanje v primeru okvar) na dovolj podrobni ravni, da se podpre vzdrževanje tehničnih sistemov. Vendar način organizacije in izvajanja vzdrževanja zadevnega tehničnega sistema ni del opredelitve tehničnega sistema, ampak del ustreznih priročnikov o vzdrževanju.

A.3.4.3. Glej tudi oddelek A.3.1. Dodatka A.

A.3.5. Funkcije tehničnih sistemov, za katere se uporablja merilo za sprejemljivost tveganja za tehnične sisteme

A.3.5.1. Merilo za sprejemljivost tveganja za tehnične sisteme se v skladu z opredelitvijo uporablja za napake pri oddajanju signala pri funkcijah, ki jih mora izpolniti tehnični sistem, če obstaja „**neposredna** možnost za katastrofalne posledice“: glej oddelek 2.5.4. {Ref. 4}.

A.3.5.2. Merilo za sprejemljivost tveganja za tehnične sisteme se lahko uporabi tudi za funkcije, ki vključujejo tehnične sisteme, vendar v zvezi z njihovimi napakami ne obstaja „**neposredna** možnost za katastrofalne posledice“. V tem primeru se mora merilo za sprejemljivost tveganja za tehnične sisteme uporabljati kot splošen cilj sklopa dogodkov, ki privede do katastrofalnih posledic. Na podlagi tega splošnega cilja je treba dejanski prispevek vsakega



dogodka in s tem napak v delovanju tehničnega sistema, ki je vključen v zadevno možnost, izpeljati v skladu z oddelkom A.3.6. Dodataka A.

Takšno uporabo merila za sprejemljivost tveganja za tehnične sisteme mora nato obravnavati in se o njej dogovoriti še delovna skupina za skupno varnostno metodo.

A.3.5.3. Za katere funkcije tehničnega sistema se uporablja merilo za sprejemljivost tveganja za tehnične sisteme? V skladu s standardom IEC 61226:2005 velja:

- (a) funkcija je v tem smislu opredeljena kot „poseben namen ali cilj, ki ga je treba izpolniti in se lahko določi ali opiše neodvisno od fizičnih sredstev za njegovo doseganje“;
- (b) funkcija (obravnavana kot črna skrinjica) prenese vhodne parametre (npr. snov, energijo, informacije) k izhodnim parametrom, ki so povezani s ciljem (npr. snov, energija, informacije);
- (c) analiza funkcije ni odvisna od njenega tehničnega uresničevanja.

A.3.5.4. Merilo za sprejemljivost tveganja za tehnične sisteme se uporablja za naslednje vrste funkcij:

- (a) primeri za podsistem ETCS na vlaku:
 - (1) „strojevodji se zagotovijo informacije, ki mu omogočajo varno upravljanje vlaka, v primeru prevelike hitrosti pa se uporabijo zavore“. Na podlagi informacij, ki jih zagotovi ETCS na vlaku z izračunom hitrosti ob progi (dovoljena hitrost) in na vlaku, lahko strojevodja in ETCS na vlaku nadzorujeta, da vlak ne preseže omejitve hitrosti. Merilo za sprejemljivost tveganja za tehnične sisteme se uporablja za oceno hitrosti vlaka na vlaku, ker:
 - (i) ni dodatne pregrade (neposredne), ker so informacije, predložene strojevodji, prav tako slabo ocenjene;
 - (ii) bi lahko prevelika hitrost vlaka povzročila iztirjenje, kar je nesreča z možnostjo za katastrofalne posledice;
 - (2) „strojevodji se zagotovijo informacije, ki mu omogočajo varno upravljanje vlaka, v primeru kršitve dovoljenja za vožnjo pa se uporabijo zavore“;
- (b) primer za tirni tokokrog: „zaznava zasedenosti dela tira“. Merilo za sprejemljivost tveganja za tehnične sisteme se bo za to funkcijo uporabilo kot takšno le, če v zapornice ni vgrajena funkcija „spremljanja zaporedja“;
- (c) primer za kretnico: „nadzor nad položajem kretnice“.

A.3.5.5. Tudi nekateri standardi opredeljujejo funkcije, za katere bi se lahko uporabljalo merilo za sprejemljivost tveganja za tehnične sisteme. Na primer:

- (a) v normativnem delu standarda prEN 0015380-4 {Ref. 13} (ModTrain Work) so opredeljene tri hierarhične ravni funkcij (v informativnih prilogah so razširjene na do pet ravni). Standard prEN 0015380-4 skupaj opredeljuje več sto funkcij, povezanih z vlaki;
- (b) na splošno je priporočeno izbrati funkcije s prvih treh ravni iz standarda prEN 0015380-4 (vendar ne nižje), pri čemer se upošteva tudi razčlemba konstrukcije izdelka;
- (c) za funkcije, ki ne spadajo v področje uporabe standarda prEN 0015380-4, je treba s primerjavo določiti ustrezno raven delovanja, in sicer s strokovno presojo.

Te primere funkcij iz standarda prEN 0015380-4 mora v okviru dela v zvezi z splošno sprejemljivimi tveganji in merili za sprejemljivost tveganja obravnavati še Agencija.

A.3.5.6. Merilo za sprejemljivost tveganja za tehnične sisteme se uporablja na primer tudi za naslednjo funkcijo iz standarda prEN 0015380-4: „nadzor nad nagibanjem“ (oznaka = CLB). Funkcija se lahko na ravni sistema uporabi na naslednja načina:

- (a) prvi primer: vlak se v ovinkih nagiba zaradi udobja potnikov, pri čemer je treba spremljati skladnost širine vlaka z infrastrukturo ob progi;



- (b) drugi primer: vlak se v ovinkih nagiba le zaradi udobja potnikov, vendar spremljanje skladnosti širine vlaka z infrastrukturo ob progi ni potrebno.

V prvem primeru se bo merilo za sprejemljivost tveganja za tehnične sisteme uporabljalo, v drugem primeru pa ne, ker okvara funkcije nagiba nima katastrofalnih posledic.

A.3.5.7. Primer (b) iz točke A.3.5.4. in primera iz točke A:3.5.6. Dodatka A jasno kažejo, da ne bo mogoče oblikovati vnaprej opredeljenega seznama funkcij, za katere se merilo za sprejemljivost tveganja za tehnične sisteme uporablja v vseh primerih. To bo vedno odvisno od tega, kako bo sistem uporabil te funkcije podsistema.

A.3.5.8. Primer uporabe merila za sprejemljivost tveganja za tehnične sisteme je naveden v oddelku C.15. Dodataka C.

A.3.6. Primeri uporabe merila za sprejemljivost tveganja za tehnične sisteme

A.3.6.1. Uvod

- (a) To poglavje prikazuje primere, kako določiti stopnjo okvare za druge stopnje resnosti nevarnosti in kako je mogoče izpeljati varnostne zahteve, ki so nižje od $10^{-9} h^{-1}$. Ta dokument ne priporoča oziroma ne zahteva nobene posebne metode. Daje le napotke, kako se lahko merilo za sprejemljivost tveganja za tehnične sisteme uporabi za kalibriranje nekaterih pogosto uporabljenih metod. Agencija ga mora v okviru svojega dela v zvezi s splošno sprejemljivimi tveganji in merili za sprejemljivost tveganja dopolniti.
- (b) Dejansko se lahko merilo za sprejemljivost tveganja za tehnične sisteme neposredno uporabi le za majhno število primerov, ker v praksi malo napak v delovanju tehničnih sistemov neposredno povzroči nesreče z morebitnimi katastrofalnimi posledicami. Zato je mogoče poiskati kompromise (npr. s kalibriranjem matrike tveganja po tem merilu) med različnimi parametri, npr. resnostjo v primerjavi s pogostostjo, da se merilo uporabi za nevarnosti s posledicami, ki niso katastrofalne, in se določi mejna stopnja okvare.

A.3.6.2. Primer 1: kompromis glede neposrednega tveganja

- (a) Merilo za sprejemljivost tveganja za tehnične sisteme se lahko preprosto uporabi za možnosti, ki se od referenčnih pogojev, opredeljenih v merilu za sprejemljivost tveganja za tehnične sisteme v oddelku 2.5.4. Uredbe o skupni varnostni metodi {Ref. 3}, razlikujejo le po nekaj neodvisnih parametrih.
- (b) Predvidevamo, da je za posamezen parameter p odnos do tveganja multiplikativen. Predvidevamo, da je p^* v referenčnem pogoju prisoten, medtem ko se v drugi možnosti uporablja p' . V tem primeru je pomembno le razmerje med parametroma p^*/p' , pri čemer se lahko stopnja pojavnosti zmanjša. Ta postopek se lahko ponovi, če so parametri neodvisni.
- (c) Primer:
- (1) predvidevamo, da je dejanska možnost za katastrofalno posledico, ki je bila ocenjena s strokovno presojo, desetkrat manjša od možnosti v okviru referenčnih pogojev iz oddelka 2.5.4 Uredbe o skupni varnostni metodi {Ref. 3}. V tem primeru bi bila zahteva $10^{-8} h^{-1}$ namesto $10^{-9} h^{-1}$;
 - (2) predvidevamo, da se opredeli dodatna varnostna pregrada drugega tehničnega sistema (neodvisnega od posledic), ki učinkuje v 50 % primerov;
 - (3) v tem primeru bi bila varnostna zahteva $5 \cdot 10^{-7} h^{-1}$ (tj. $0,5 \cdot 10^{-8} h^{-1}$) namesto $10^{-9} h^{-1}$.

A.3.6.3. Primer 2: kalibracija matrike tveganja

- (a) Za pravilno uporabo merila za sprejemljivost tveganja za tehnične sisteme v matriki tveganja mora biti matrika povezana s pravilno ravno sistema (primerljivo z ravno, določeno v oddelku A.3.5. Dodatka A);
- (b) merilo za sprejemljivost tveganja za tehnične sisteme eno polje v matriki tveganja določa kot dopustno, kar ustreza koordinati (resnost katastrofe; pogostost pojavljanja $10^{-9} h^{-1}$): glej rdeče polje v tabeli 5. Vsa polja, ki so povezana z večjo pogostostjo, je treba označiti kot „nedopustna“. Opozoriti je treba, da je pogostost nesreč enaka kot pogostost napak v delovanju le v primeru verjetne neposredne možnosti za katastrofalno posledico;
- (c) nato se lahko izpolnijo ostala polja v matriki, vendar je treba upoštevati učinke, kot sta strah pred tveganjem ali naraščanje kategorij. V najpreprostejšem primeru linearnega desetinskega naraščanja (kot je v Tabela 1 prikazano s puščico) se polje, ki je z merilom za sprejemljivost tveganja za tehnične sisteme tako označeno kot „sprejemljivo“, linearno ekstrapolira na preostalo matriko. To pomeni, da so vsa polja na isti diagonali (ali pod diagonalo) prav tako označena kot „sprejemljiva“. Tudi polja pod njo se lahko označijo kot „sprejemljiva“;

Tabela 1: Značilen primer kalibrirane matrike tveganja

Pogostost pojavljanja nesreče (zaradi nevarnosti)	Stopnje tveganja			
	pogosto (10^{-4} na uro)	nedopustno	nedopustno	nedopustno
verjetno (10^{-5} na uro)	nedopustno	nedopustno	nedopustno	nedopustno
občasno (10^{-6} na uro)	sprejemljivo	nedopustno	nedopustno	nedopustno
redko (10^{-7} na uro)	sprejemljivo	sprejemljivo	nedopustno	nedopustno
malo verjetno (10^{-8} na uro)	sprejemljivo	sprejemljivo	sprejemljivo	nedopustno
neverjetno (10^{-9} na uro)	sprejemljivo	sprejemljivo	sprejemljivo	sprejemljivo
	nebitveno	manj pomembno	kritično	katastrofalno
	Stopnje resnosti posledic nevarnosti (npr. nesreče)			
Ovrednotenje tveganja	Nadzor/zmanjševanje tveganja			
Nedopustno	Tveganje je treba odpraviti.			
Sprejemljivo	Tveganje je sprejemljivo. Potrebna je neodvisna ocena.			

- (d) ko je matrika izpolnjena, se lahko uporabi tudi za nevarnosti, ki niso katastrofalne. Če je na primer resnost druge napake v delovanju razvrščena kot „kritična“, dopustna pogostost nesreč po kalibrirani matriki tveganja ne sme biti več kot „malo verjetna“ (ali celo manj);
- (e) pripomniti je treba, da je lahko uporaba matrike tveganja vzrok za preveč konservativne rezultate, kadar se uporablja za pogostosti napak v delovanju (tj. za napake v delovanju, ki neposredno ne povzročijo nesreč).

A.3.6.4. Načelo za kalibriranje drugih metod za analizo tveganja

Druge metode za analizo tveganja, na primer predlagana shema števil prioritete tveganj ali graf tveganja iz VDV 331 ali IEC 61508, se prav tako lahko kalibrirajo po podobnem postopku, kot je določen za matriko tveganja:

- (a) prvi korak: referenčna točka iz merila za sprejemljivost tveganja za tehnične sisteme se razvrsti kot dopustna, točke z večjo pogostostjo ali večjo resnostjo pa kot nedopustno merilo za sprejemljivost tveganja za tehnične sisteme;
- (b) drugi korak: mehanizmi za sklepanje kompromisov posebne metode se uporabijo za ekstrapolacijo dopustnosti tveganja na nevarnosti, ki niso katastrofalne (z uporabo linearnega kompromisa v zvezi s tveganjem kot začetne točke);
- (c) tretji korak: za nevarnosti, ki niso katastrofalne, se lahko merilo za sprejemljivost tveganja za tehnične sisteme nato izpelje iz kalibrirane metode za analizo tveganja s primerjavo koordinate (pogostosti; resnosti) s tako pridobljeno krivuljo F-N.

A.3.7. Sklepi v zvezi z merilom za sprejemljivost tveganja za tehnične sisteme

- A.3.7.1. V splošnem okviru ocene tveganja, ki ga predlaga skupna varnostna metoda, so merila za sprejemljivost tveganja potrebna, da se določi, kdaj je preostala stopnja tveganja (tveganj) sprejemljiva in s tem kdaj končati eksplicitno oceno tveganja.
- A.3.7.2. Merilo za sprejemljivost tveganja za tehnične sisteme je cilj projektiranja ($10^{-9} h^{-1}$) za tehnične sisteme.
- A.3.7.3. Glavni nameni merila za sprejemljivost tveganja za tehnične sisteme so:
 - (a) določiti zgornjo mejo sprejemljivosti tveganja in s tem referenčno točko, na podlagi katere je mogoče kalibrirati metode za analizo tveganja za tehnične sisteme;
 - (b) omogočiti vzajemno priznavanje tehničnih sistemov, ker se bodo s tem povezane ocene tveganja in varnosti ovrednotile glede na enako merilo za sprejemljivost tveganja v vseh državah članicah;
 - (c) zmanjšati stroške, saj ne zahteva nepotrebno visokih kvantitativnih varnostnih zahtev;
 - (d) spodbuditi konkurenco med proizvajalci. Zaradi uporabe različnih meril za sprejemljivost tveganja, ki jih uporablja predlagatelj ali država članica, bi industrija izvedla veliko različnih dokazovanj v zvezi z enakimi tehničnimi sistemi. To bi lahko ogrozilo konkurenčnost proizvajalcev in po nepotrebem podražilo proizvode.
- A.3.7.4. Delno kvantitativne zahteve iz merila za sprejemljivost tveganja za tehnične sisteme ni treba vedno dokazati za tehnične sisteme. Dejansko se mora v okviru skupne varnostne metode merilo za sprejemljivost tveganja za tehnične sisteme uporabljati le za tehnične sisteme, pri katerih opredeljenih nevarnosti ni mogoče ustrezno nadzorovati niti z uporabo kodeksov ravnanja niti s primerjavo s podobnimi referenčnimi sistemi. To omogoča določitev manjših varnostnih zahtev, če se lahko ohrani globalna stopnja varnosti.
- A.3.7.5. Usklajeno delno kvantitativno merilo za sprejemljivost tveganja za tehnične sisteme je potrebno le, če ne obstajata noben kodeks ravnanja in noben referenčni sistem.
- A.3.7.6. Ker je stopnja varnostne integritete za sistematične okvare/napake omejena na SIL 4, mora biti stopnja varnostne integritete za naključne okvare strojne opreme tehničnih sistemov prav tako omejena na SIL 4. To ustreza najvišji dopustni stopnji nevarnosti (THR) $10^{-9} h^{-1}$ (tj. najvišja stopnja okvare). Če se zahtevajo strožje varnostne zahteve, tega v skladu s standardom CENELEC 50 129 ni mogoče doseči le z enim sistemom; spremeniti je treba arhitekturo sistema, na primer z uporabo dveh sistemov, kar neizogibno bistveno poveča stroške tehničnega sistema. Za več podrobnosti glej oddelek A.3.1. Dodatka A.
- A.3.7.7. Oddelek A.3.6. Dodatka A določa, kako se lahko merilo za sprejemljivost tveganja za tehnične sisteme uporabi kot referenčna točka za kalibriranje posebnih metod za analizo

tveganja, kadar obstaja pri tehničnih sistemih možnost za manj resne posledice od katastrofalnih.

A.4. Dokazi v zvezi z oceno varnosti

A.4.1. Ta oddelek zagotavlja navodila v zvezi z dokazi, ki se običajno predložijo ocenjevalnemu organu, da se omogoči neodvisna ocena in izpolnijo varnostne zahteve brez poseganja v nacionalne zahteve v državi članici. To se lahko uporabi kot kontrolni seznam za preverjanje, ali so med uporabo skupne varnostne metode zajeti in dokumentirani vsi s tem povezani vidiki, kadar je primerno.

A.4.2. Varnostni načrt: v standardu CENELEC je priporočeno, da se varnostni načrt izdela na začetku projekta ali da se s tem povezan opis vključi v kateri koli drug ustrezen dokument, če to za projekt ni primerno. Če so ocenjevalni organi imenovani na začetku projekta, se lahko varnostni načrt predloži tudi njim, da izrazijo svoje mnenje. Načeloma varnostni načrt opisuje:

- (a) vzpostavljeno organizacijo in usposobljenost ljudi, vključenih v razvoj in oceno tveganja;
- (b) vse dejavnosti v zvezi z varnostjo, ki se načrtujejo v različnih fazah projekta, in pričakovane rezultate.

A.4.3. Dokazi, ki se zahtevajo v zvezi s fazo opredelitve sistema:

- (a) opis sistema:
 - (1) opredelitev področja uporabe/mej sistema;
 - (2) opis funkcij;
 - (3) opis strukture sistema;
 - (4) opis operativnih in okoljskih pogojev;
- (b) opis zunanjih vmesnikov;
- (c) opis notranjih vmesnikov;
- (d) opis faz življenjskega cikla;
- (e) opis varnostnih načel;
- (f) opis predpostavk, ki določajo omejitve ocene tveganja.

A.4.4. Da se omogoči izvedba ocene tveganja, se v opredelitvi sistema upošteva okvir predvidene spremembe:

- (a) če je predvidena sprememba preoblikovanje obstoječega sistema, morata biti v opredelitvi sistema opisana sistem pred spremembo in tudi predvidena sprememba;
- (b) če je predvidena sprememba izgradnja novega sistema, je opis omejen na opredelitev sistema, ker opis obstoječega sistema ni.

A.4.5. Dokazi, ki se zahtevajo v zvezi s fazo opredelitve nevarnosti:

- (a) opis in utemeljitev (vključno z omejitvami) metod in orodij za opredelitev nevarnosti (metoda od zgoraj navzdol, od spodaj navzgor, HAZOP itd.);
- (b) rezultati:
 - (1) sezname nevarnosti;
 - (2) nevarnosti v zvezi s sistemom (mejami);
 - (3) nevarnosti v zvezi s podsistemom;
 - (4) nevarnosti v zvezi z vmesniki;
 - (5) varnostni ukrepi, ki se lahko opredelijo med to fazo.

A.4.6. Potrebni so tudi naslednji dokazi iz faze analize tveganja:



- (a) kadar se za nadzorovanje nevarnosti uporabljajo kodeksi ravnanja, dokaz, da so za ocenjevani sistem izpolnjene vse ustrezne zahteve iz kodeksov ravnanja. To vključuje tudi dokaz pravilne uporabe ustreznih kodeksov ravnanja;
- (b) kadar se za nadzorovanje nevarnosti uporabljajo podobni referenčni sistemi:
 - (1) opredelitev varnostnih zahtev za ocenjevani sistem iz ustreznih referenčnih sistemov;
 - (2) dokaz, da se ocenjevani sistem uporablja pod podobnimi operativnimi in okoljskimi pogoji kot ustrezen referenčni sistem. Če to ni mogoče, pa dokaz, da so odstopanja od referenčnega sistema pravilno ocenjena;
 - (3) dokaz, da se v ocenjevanem sistemu varnostne zahteve iz referenčnih sistemov uporabljajo pravilno;
- (c) kadar se za nadzorovanje nevarnosti uporablja eksplicitna ocena tveganja:
 - (1) opis in utemeljitev (vključno z omejitvami) metode in orodij za analizo tveganja (kvalitativno, kvantitativno, delno kvantitativno, neregresijsko analizo ...);
 - (2) opredelitev veljavnih varnostnih ukrepov in dejavnikov za zmanjšanje tveganja za vsako nevarnost (vključno z vidiki človeškega dejavnika);
 - (3) ovrednotenje in razvrstitev tveganja za vsako nevarnost:
 - (i) ocena posledic nevarnosti in utemeljitev (s predpostavko in pogoji);
 - (ii) ocena pogostosti nevarnosti in utemeljitve (s predpostavko in pogoji);
 - (iii) razvrstitev nevarnosti v skladu z njihovo kritičnostjo in pogostostjo pojavljanja;
 - (4) opredelitev dodatnih primernih varnostnih ukrepov za sprejemljiva tveganja za vsako nevarnost (ponovitev postopka po fazi ovrednotenja tveganja).

A.4.7. Dokazi, ki se zahtevajo v zvezi z ovrednotenjem tveganja:

- (a) kadar se izvaja eksplicitna ocena tveganja:
 - (1) opredelitev in utemeljitev meril za ovrednotenje tveganja za vsako nevarnost;
 - (2) dokaz/utemeljitev, da varnostni ukrepi in varnostne zahteve zajemajo vsako nevarnost na sprejemljivi ravni (glede na navedeno merilo za ovrednotenje tveganja);
- (b) na podlagi oddelkov 2.3.5 and 2.4.3. Uredbe o skupni varnostni metodi se tveganja, ki jih zajemata uporaba kodeksov ravnanja in primerjava z referenčnimi sistemi, implicitno štejejo za sprejemljive, če (glej pikčast krog na Slika 1):
 - (1) so izpolnjeni pogoji uporabe kodeksov ravnanja iz oddelka 2.3.2.;
 - (2) so izpolnjeni pogoji uporabe referenčnega sistema iz oddelka 2.4.2.

Merila za sprejemljivost tveganja so za ti dve načeli sprejemljivosti tveganja implicitna.

A.4.8. Dokazi v zvezi z obvladovanjem nevarnosti:

- (a) evidentiranje vseh nevarnosti v evidenci nevarnosti, ki vključuje naslednje elemente:
 - (1) opredeljeno nevarnost;
 - (2) varnostne ukrepe, ki preprečujejo pojav nevarnosti ali blažijo njene posledice;
 - (3) varnostne zahteve v zvezi z ukrepi;
 - (4) ustrezen del sistema;
 - (5) udeleženca, odgovornega za varnostne ukrepe;
 - (6) status nevarnosti (npr. odprta, rešena, odpravljena, prenesena, pod nadzorom itd.);
 - (7) datum evidentiranja, pregleda in nadzora vsake nevarnosti;
- (b) opis, kako se bodo nevarnosti učinkovito obvladovale v celotnem življenjskem ciklu;



- (c) opis izmenjave informacij med strankami v zvezi z nevarnostmi na vmesnikih in dodelitvijo odgovornosti.
- A.4.9. Dokazi v zvezi s kakovostjo postopka ovrednotenja in ocene tveganja:
- (a) opis oseb, ki so vključene v postopek, in njihove usposobljenosti;
 - (b) za eksplicitne ocene tveganja opis informacij, podatkov in drugih statistik, ki se uporabijo v postopku, ter utemeljitev njihove ustreznosti (npr. študija občutljivosti za uporabljene podatke).
- A.4.10. Dokazi skladnosti z varnostnimi zahtevami:
- (a) seznam uporabljenih standardov;
 - (b) opis projektiranja in operativnih načel;
 - (c) dokazi o uporabi dobrega sistema vodenja kakovosti in sistema varnega upravljanja za projekt: glej točko [G 3] oddelka 1.1.2.;
 - (d) povzetek poročil o analizi varnosti (npr. analiza vzroka nevarnosti), ki dokazuje izpolnjevanje varnostnih zahtev;
 - (e) opis in utemeljitev metod ter orodij (FMECA, drevo napak ...), ki se uporabljajo za analizo vzroka nevarnosti;
 - (f) povzetek preskusov preverjanja in potrditve varnosti.
- A.4.11. Varnostna analiza: v standardu CENELEC je priporočeno, da se vsi zgoraj navedeni dokazi prerazvrstijo in povzamejo v enem dokumentu, ki se predloži ocenjevalnemu organu: glej točki [G 4] in [G 5] oddelka 5.1.

**DODATEK B: PRIMERI TEHNIK IN ORODIJ ZA PODORO
POSTOPKA OCENJEVANJA TVEGANJA**

- B.1. Primeri tehnik in orodij za izvajanje dejavnosti ocenjevanja tveganja, ki jih zajema skupna varnostna metoda, so na voljo v Prilogi E priročnika o standardu EN 50126-2 {Ref. 9}. Povzetek tehnik in orodij je v tabeli E.1. Opisana je vsaka tehnika, pri čemer je za več informacij po potrebi zagotovljeno sklicevanje na druge standarde.

DODATEK C: PRIMERI

C.1. Uvod

C.1.1. Namen tega dodatka je olajšati branje tega dokumenta. Združuje vse zbrane primere, katerih cilj je olajšati uporabo skupne varnostne metode.

C.1.2. Primeri ocen tveganja ali varnosti, ki so navedeni v tem dodatku, ne izhajajo iz uporabe postopka skupne varnostne metode, ker so bili izvedeni pred obstojem Uredbe o skupni varnostni metodi. Primeri se lahko razvrstijo v:

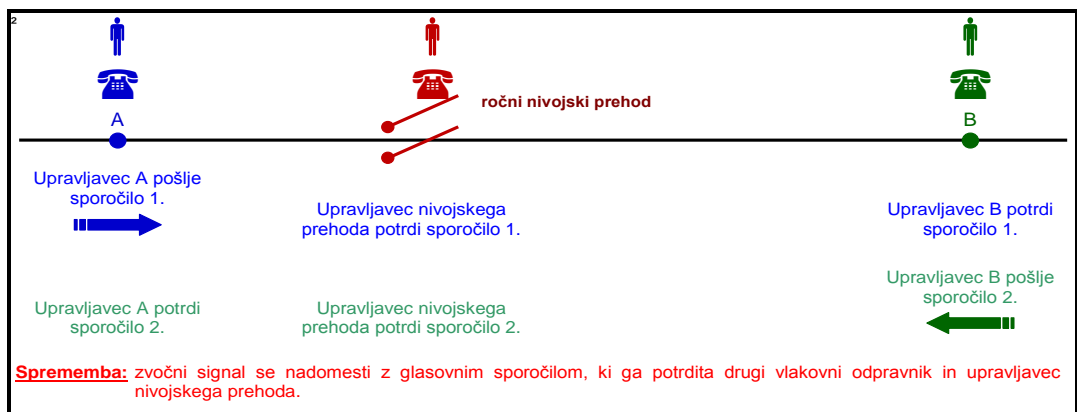
- primere z navedbo njihovega izvora, ki so jih predložili strokovnjaki iz delovne skupine za skupno varnostno metodo;
- primere brez namerne navedbe njihovega izvora, ki so jih prav tako predložili strokovnjaki iz delovne skupine za skupno varnostno metodo. Zadevni strokovnjaki so zahtevali, da izvor ostane zaupen;
- primere, katerih izvor ni naveden in ki so jih pripravili člani osebja Agencije na podlagi svojih prejšnjih strokovnih izkušenj.

Za vsak primer so navedene sledljivost med uporabljenim postopkom in postopkom, ki se zahteva v skupni varnostni metodi, utemeljitev ter dodana vrednost za izvedbo dodatnih korakov (če obstajajo), ki se zahtevajo v skupni varnostni metodi.

C.2. Primeri uporabe meril za pomembno spremembo iz člena 4(2)

C.2.1. Agencija si prizadeva izdelati opredelitev tega, kar se lahko šteje za „pomembno spremembo“. Primer teh prizadevanj je naveden v tem oddelku, in sicer kako uporabiti merila iz Člen 4(2).

C.2.2. Sprememba predstavlja spremembo načina, na katerega na ročno upravljanim nivojskem prehodu prometni odpravnik sporoča informacije o smeri prihajajočega vlaka upravljavcu nivojskega prehoda. Sprememba je predstavljena na Slika 15.



Slika 15 : Primer nepomembne spremembe – telefonsko sporočilo za nadzorovanje nivojskega prehoda

C.2.3. Obstoječ sistem: pred uvedbo predvidene spremembe so se informacije o smeri prihajajočega vlaka z zvonjenjem telefona samodejno sporočile upravljavcu nivojskega prehoda. Ton zvonjenja se je razlikoval glede na to, od kod je klic prihajal.

C.2.4. Predvidena sprememba: ker star telefonski sistem postaja zastarel in ga je treba nadomestiti z novim, digitalnim, v zvonjenje tehnično ni več mogoče vključiti ustreznih informacij. Ton zvonjenja je povsem enak, ne glede na to, od katerega prometnega odpravnika prihaja. Zato je bilo odločeno, da se ista funkcija doseže z operativnim postopkom:

- (a) ob odhodu vlaka prometni odpravnik ustno obvesti upravljavca nivojskega prehoda o smeri prihajajočega vlaka;
- (b) informacija se primerja z voznim redom, pri čemer jo potrdira upravljavec nivojskega prehoda in drugi prometni odpravnik, da je upravljavec ne razume napačno.

Predvidena sprememba in z njo povezan operativni postopek sta prikazana na Slika 15

C.2.5. Čeprav se zdi, da sprememba morda vpliva na varnost (tveganje, da se zapornica nivojskega prehoda ne zapre pravočasno), lahko druga merila iz Člen 4(2), kot so:

- (a) nizka stopnja kompleksnosti;
- (b) odsotnost novosti in
- (c) enostavno spremljanje;

pomenijo, da predvidena sprememba ni pomembna.

C.2.6. V tem primeru je kljub temu potrebna nekakšna analiza varnosti ali dokaz, da se pokaže, da bi pri tej nalogi, pomembni za varnost, nadomestitev starega tehničnega sistema z operativnim postopkom (osebje se medsebojno preverja) vodila do podobne stopnje varnosti. Vprašanje je, ali je zato potrebna uporaba celotnega postopka skupne varnostne metode z evidenco nevarnosti, neodvisno oceno, ki jo izvede ocenjevalni organ, itd. V tem primeru je vprašljivo, ali ima to kakršno koli dodano vrednost, kar pomeni, da se takšna sprememba zato ne bi mogla šteti za pomembno.

C.3. Primeri vmesnikov med udeleženci v železniškem sektorju

C.3.1. Navedenih je nekaj primerov vmesnikov in vzrokov za sodelovanje med udeleženci v železniškem sektorju:

- (a) upravljavec železniške infrastrukture – upravljavec železniške infrastrukture: za obe infrastrukturi se na primer predvidijo varnostni ukrepi za zagotovitev varnega prehoda vlakov iz ene infrastrukture v drugo;
- (b) upravljavec železniške infrastrukture – prevoznik v železniškem prometu: obstajajo lahko na primer posebna operativna pravila, odvisna od infrastrukture, ki jih mora strojevodja vlaka upoštevati;
- (c) upravljavec železniške infrastrukture – proizvajalec: podsistemi proizvajalca lahko imajo na primer omejitve uporabe, ki jih mora upravljavec železniške infrastrukture izpolnjevati;
- (d) upravljavec železniške infrastrukture – izvajalec storitev: obstajajo lahko na primer posebne omejitve glede vzdrževanja infrastrukture, ki jih mora podizvajalec dejavnosti vzdrževanja izpolnjevati;
- (e) prevoznik v železniškem prometu – proizvajalec: podsistemi proizvajalca lahko imajo na primer omejitve uporabe, ki jih mora prevoznik v železniškem prometu izpolnjevati;
- (f) prevoznik v železniškem prometu – izvajalec storitev: obstajajo lahko na primer posebne omejitve glede vzdrževanja infrastrukture, ki jih mora podizvajalec dejavnosti vzdrževanja izpolnjevati;
- (g) prevoznik v železniškem prometu – upravitelji: obstajajo lahko na primer omejitve uporabe za posamezna vozila, ki jih mora prevoznik v železniškem prometu, ki upravlja ta vozila, izpolnjevati;
- (h) proizvajalec – proizvajalec: na primer upravljanje tehničnih vmesnikov v zvezi z varnostjo med podsistemi dveh različnih proizvajalcev;

- *****
- (i) proizvajalec – izvajalec storitev: na primer upravljanje evidence nevarnosti s strani proizvajalca, kadar se nekatera dela oddajo pogodbeniku, ki je premajhen, da bi imel varnostno organizacijo za zadevni projekt;
 - (j) izvajalec storitev – izvajalec storitev: podoben primer kot v točki (i) zgoraj.
- C.3.2. Izvajalci storitev zajemajo vse dejavnosti, ki jih upravljavec železniške infrastrukture ali prevoznik v železniškem prometu ali proizvajalec odda pogodbeniku, kot so vzdrževanje, prodaja vozovnic, inženirske storitve itd.
- C.3.3. Za prikaz upravljanja vmesnikov in s tem povezane opredelitve nevarnosti je naveden naslednji primer. Obravnava vmesnik med proizvajalcem vlakov in predlagateljem (prevoznikom v železniškem prometu). Nato opisuje, kako se lahko izpolnijo glavna merila iz točke [G 1] oddelka 1.2.1.:
- (a) vodstvo: predlagatelj (prevoznik v železniškem prometu);
 - (b) vnosi:
 - (1) seznam(-i) ustreznih nevarnosti iz podobnih projektov;
 - (2) opis vseh vnosov in rezultatov v zvezi z vmesnikom, vključno z učinkovitostjo;
 - (c) metode: glej Dodatek A.2. smernice EN 50126-2 {Ref. 9};
 - (d) zahtevani udeleženci:
 - (1) predlagatelj upravljavca zagotavljanja varnosti (prevoznika v železniškem prometu);
 - (2) proizvajalčev upravljavec zagotavljanja varnosti vlakov;
 - (3) predlagatelj organ za projektiranje vlaka;
 - (4) predlagateljevo osebje za vzdrževanje vlaka (delno odvisno od analiziranega vnosa/rezultatov);
 - (5) strojevodje vlakov (delno odvisno od analiziranega vnosa/rezultatov);
 - (e) rezultati:
 - (1) poročilo o skupno dogovorjeni opredelitvi nevarnosti;
 - (2) varnostni ukrepi za evidenco nevarnosti z jasnim opisom odgovornosti.

C.4. Primeri metod za določitev splošno sprejemljivih tveganj

C.4.1. Uvod

- C.4.1.1. Splošno sprejemljiva tveganja so v Uredbi o skupni varnostni metodi opredeljena kot „*tako majhna, da izvajanje dodatnih varnostnih ukrepov ni smiselno (za nadaljnje zmanjšanje tveganja)*“. Pri opredelitvi nevarnosti razvrščanje nekaterih nevarnosti kot povezanih s splošno sprejemljivimi tveganji omogoča, da se te nevarnosti ne analizirajo nadalje v postopku ocenjevanja tveganja. Zgoraj navedena opredelitev splošno sprejemljivih tveganj dopušča nekaj svobode pri razlagi. Zato je v Uredbi navedeno, da je odločitev o razvrstitvi nevarnosti s splošno sprejemljivimi tveganji prepuščena strokovni presoji.
- C.4.1.2. Dejansko je težko skupaj opredeliti bolj eksplicitno merilo za splošno sprejemljiva tveganja, ki bi se uporabljalo na vseh mogočih različnih ravneh sistema, na katerih se lahko takšne nevarnosti opredelijo, kar se prav tako upošteva kot različni dejavniki strahu pred tveganjem, ki lahko prevladajo pri različnih aplikacijah. Vendar ker je pomembno zagotoviti, da so presoje strokovnjakov preproste za razumevanje in sledljive, so nekatera navodila za

opredelitev tveganj kot splošno sprejemljivih koristna. Merila za opredelitev splošno sprejemljivih tveganj so lahko kvantitativna, kvalitativna ali delno kvalitativna. Spodaj je navedenih nekaj primerov, kako izpeljati merila, ki omogočajo kvantitativno ali delno kvantitativno ovrednotenje splošno sprejemljivih tveganj.

- C.4.1.3. Spodaj navedeni primeri prikazujejo navedeno načelo. Povzeti so iz članka: „Die Gefährdungseinstufung im ERA-Risikomanagementprozess“, Kurz, Milius, Signal + Draht (100), september 2008.

C.4.2. Izpeljava kvantitativnega merila

- C.4.2.1. Splošno sprejemljiva tveganja je mogoče opredeliti kot tveganja, ki so veliko manjša od sprejemljivega tveganja za zadeven razred nevarnosti. Z uporabo statističnih podatkov bi lahko bilo mogoče izračunati, kakšna je sedanja stopnja tveganja za železniške sisteme, in izračunano stopnjo tako razglasiti kot sprejemljivo. Če to stopnjo tveganja delimo s številom (N) nevarnosti (poljubno lahko na primer domnevamo, da obstaja približno $N = 100$ glavnih kategorij nevarnosti v železniškem sistemu), dobimo sprejemljivo stopnjo tveganja na kategorijo nevarnosti. Nato je mogoče navesti, da bi se nevarnost s tveganjem, ki je za dva reda velikosti nižje od sprejemljive stopnje tveganja na nevarnost (to je parameter x % iz točke [G 1] oddelka 2.2.3.), štela za splošno sprejemljivo tveganje.

- C.4.2.2. Vendar je treba preveriti, ali prispevek vseh nevarnosti, povezanih s splošno sprejemljivim(-i) tveganjem(-ji), presega določen delež (npr. y %) celotnega tveganja na ravni sistema: glej oddelek 2.2.3. in obrazložitev v točki [G 2] oddelka 2.2.3.

C.4.3. Ovrednotenje splošno sprejemljivih tveganj

- C.4.3.1. Mejne vrednosti za splošno sprejemljiva tveganja, kot so izpeljane v zgornjih primerih, se lahko nato uporabijo za kalibriranje kvalitativnih orodij, kot so matrika tveganja, graf tveganja ali števila prioritete tveganj, da strokovnjaku pomagajo sprejeti odločitev o razvrstitvi tveganja kot splošno sprejemljivega. Pomembno je poudariti, da kvantitativne vrednosti kot merila za splošno sprejemljiva tveganja ne pomenijo, da je treba za sprejetje odločitve o splošni sprejemljivosti tveganja izvesti natančno presojo ali analizo tveganja. Tukaj se za izvedbo te grobe presoje v fazi opredelitve nevarnosti uporablja presoja strokovnjaka.

- C.4.3.2. Treba je tudi preveriti, ali prispevek vseh nevarnosti, povezanih s splošno sprejemljivim(-i) tveganjem(-ji), presega določen delež (npr. y %) celotnega tveganja na ravni sistema: glej oddelek 2.2.3. in obrazložitev v točki [G 2] oddelka 2.2.3.

C.5. Primer ocene tveganja pomembne organizacijske spremembe

- C.5.1. **Opomba:** ta primer ocene tveganja ne izhaja iz uporabe postopka skupne varnostne metode; izveden je bil pred obstojem skupne varnostne metode. Namen primera je:

- opredeliti podobnosti med veljavnimi metodami ocenjevanja tveganja in postopkom skupne varnostne metode;
- zagotoviti sledljivost med veljavnim postopkom in postopkom, ki ga zahteva skupna varnostna metoda;
- zagotoviti utemeljitev dodane vrednosti izvedbe dodatnih korakov (če obstajajo), ki se zahtevajo v skupni varnostni metodi.

- Poudariti je treba, da je ta primer le informativen. Njegov namen je pomagati bralcu pri razumevanju postopka skupne varnostne metode. Vendar se sam primer ne sme prenesti na drugo pomembno spremembo ali se uporabiti kot referenčen sistem zanjo. Ocena tveganja se v skladu z Uredbo o skupni varnostni metodi izvede za vsako pomembno spremembo.
- C.5.2. Primer je povezan z organizacijsko spremembo. Zadevni predlagatelj jo je obravnaval kot pomembno. Za ovrednotenje spremembe je bil uporabljen pristop na podlagi ocene tveganja.
- C.5.3. Veja organizacije upravljavca železniške infrastrukture, ki je do spremembe opravljala nekatere dejavnosti vzdrževanja (razen dejavnosti v zvezi s signalizacijo in telematskih dejavnosti), je morala postati konkurenčnejša glede na druga podjetja z istega področja. Neposreden vpliv je bila potreba po zmanjšanju in prerazporeditvi osebja ter nalog v okviru ločene veje organizacije upravljavca železniške infrastrukture.
- C.5.4. Težave zadevnega upravljavca železniške infrastrukture:
- (a) osebje upravljavca železniške infrastrukture, na katero je sprememba vplivala, je bilo odgovorno za nujno vzdrževanje in popravila zaradi nenadnih napak na infrastrukturi. Osebje je izvajalo tudi nekatere načrtovane ali na projektu temelječe dejavnosti vzdrževanja, kot so ohranjanje višine tira, čiščenje gramozne grede, nadzor vegetacije;
 - (b) te naloge so se obravnavale kot pomembne za varno in točno delovanje. Zato jih je bilo treba analizirati, da se ugotovijo pravi ukrepi, ki bodo zagotovili, da se razmere ne poslabšajo, ker veliko oseb, odgovornih za varnost, odhaja iz organizacije upravljavca železniške infrastrukture;
 - (c) med spremembo organizacije in po njej je treba ohraniti enako stopnjo varnosti in točnosti vlakov.
- C.5.5. V primerjavi s postopkom skupne varnostne metode so bili uporabljeni naslednji koraki (glej tudi Slika 1):
- (a) opis sistema [oddelek 2.1.2.]:
 - (1) opis nalog, ki jih je izvedla obstoječa organizacija (tj. organizacija upravljavca železniške infrastrukture pred spremembo);
 - (2) opis načrtovanih sprememb v organizaciji upravljavca železniške infrastrukture;
 - (3) vmesniki med „vejo, ki bo ločena,“ in drugimi organizacijami, ki jo obkrožajo, ali fizičnim okoljem so se lahko opisali le na kratko. Meji ni bilo mogoče določiti popolnoma jasno;
 - (b) opredelitev nevarnosti [oddelek 2.2.]:
 - (1) skupina strokovnjakov zbira zamisli:
 - (i) da se ugotovijo vse nevarnosti s pomembnim vplivom na tveganje zaradi predvidene organizacijske spremembe;
 - (ii) da se opredelijo mogoči ukrepi za nadzor tveganja;
 - (2) razvrstitev nevarnosti:
 - (i) glede na resnost z njimi povezanega tveganja: visoko, srednje, nizko tveganje;
 - (ii) glede na vpliv spremembe: večje, nespremenjeno, manjše tveganje;
 - (c) uporaba referenčnega sistema [oddelek 2.4.]:

stopnja varnosti sistema pred spremembo je bila ocenjena kot sprejemljiva. Zato se je ta uporabljal kot „referenčni sistem“ za izpeljavo meril za sprejemljivost tveganja pri spremembi organizacije;
 - (d) eksplicitna ocena in ovrednotenje tveganja [oddelek 2.5.]:

za vsako nevarnost z večjim tveganjem zaradi spremembe organizacije se opredelijo ukrepi za zmanjšanje tveganja. Preostalo tveganje se primerja z merili za sprejemljivost tveganja iz referenčnega sistema, da se preveri, ali je treba opredeliti dodatne ukrepe;

(e) dokazovanje skladnosti sistema z varnostnimi zahtevami [oddelek 3]:

- (1) analiza tveganja in evidenca nevarnosti kažeta, da nevarnosti ni mogoče nadzorovati, dokler se te ne preverijo in dokler se ne dokaže, da se varnostne zahteve (tj. izbrani varnostni ukrepi) izvajajo;
- (2) analiza tveganja in evidenca nevarnosti sta bila stalno posodabljaljoča se dokumenta. Učinkovitost določenih ukrepov se je redno spremljala, da se je preverilo, ali so se pogoji spremenili ter ali je treba analizo tveganja in ovrednotenje tveganja posodobiti;
- (3) če izvedeni ukrepi niso bili dovolj učinkoviti, so se analiza tveganja, ovrednotenje tveganja in evidenca nevarnosti posodobili in ponovno spremljali;

(f) obvladovanje nevarnosti [oddelek 4.1.]:

opredeljene nevarnosti in varnostni ukrepi so bili evidentirani ter so se upravljali v evidenci nevarnosti. Eden od sklepov v zvezi s primerom je bilo stalno posodabljanje analize tveganja in evidence nevarnosti, ker so se odločitve in ukrepi sprejemali med spremembo organizacije. Tveganja na vmesnikih z na primer pogodbeniki in podjetniki, so bila prav tako zajeta v analizi tveganja.

Struktura in polja, uporabljeni za evidenco nevarnosti, ter povzetek nekaterih vrstic so navedeni v oddelku C.16.2. Dodatka C;

(g) neodvisna ocena [Člen 6]:

neodvisno oceno je izvedla tudi tretja stranka, in sicer:

- (1) da se preveri, ali sta bila obvladovanje in ocena tveganja izvedena pravilno;
- (2) da se preveri, ali je organizacijska sprememba ustrezna in bo omogočila vzdrževanje enake stopnje varnosti kot pred spremembo.

C.5.6. Primer kaže, da so načela, ki jih zahteva skupna varnostna metoda, veljavne metode v železniškem sektorju, ki se že uporabljajo za oceno tveganj za organizacijske spremembe. Ocena tveganja v navedenem primeru izpolnjuje vse zahteve iz skupne varnostne metode. Uporablja dve od treh načel sprejemljivosti tveganja, ki jih dovoljuje usklajen pristop skupne varnostne metode:

- (a) "referenčni sistem" se uporablja za določitev meril za sprejemljivost tveganja, ki so potrebna za ovrednotenje sprejemljivosti tveganja organizacijske spremembe;
- (b) "eksplicitna ocena in ovrednotenje tveganja":
 - (1) analiza odstopanj spremembe od referenčnega sistema;
 - (2) opredelitev ukrepov za zmanjšanje tveganja za večje tveganje, ki izhaja iz spremembe;
 - (3) ovrednotenje, ali je dosežena sprejemljiva stopnja tveganja.

C.6. Primer ocene tveganja pomembne operativne spremembe – sprememba ur vožnje

C.6.1. **Opomba:** ta primer ocene tveganja ne izhaja iz uporabe postopka skupne varnostne metode; izveden je bil pred obstojem skupne varnostne metode. Namen primera je:

- (a) opredeliti podobnosti med veljavnimi metodami ocene tveganja in postopkom skupne varnostne metode;



- (b) zagotoviti sledljivost med veljavnim postopkom in postopkom, ki ga zahteva skupna varnostna metoda;
- (c) zagotoviti utemeljitev dodane vrednosti izvedbe dodatnih korakov (če obstajajo), ki se zahtevajo v skupni varnostni metodi.

Poudariti je treba, da je ta primer le informativen. Njegov namen je pomagati bralcu pri razumevanju postopka skupne varnostne metode. Vendar se sam primer ne sme prenesti na drugo pomembno spremembo ali se uporabiti kot referenčni sistem zanjo. Ocena tveganja se v skladu z Uredbo o skupni varnostni metodi izvede za vsako pomembno spremembo.

C.6.2. Primer je operativna sprememba, s katero je prevoznik v železniškem prometu želel uvesti nove proge in morda nov delovni čas (vključno z izmenami in vzorcem izmeničnih delovnih dni) za strojevodje.

C.6.3. V primerjavi s postopkom skupne varnostne metode so bili uporabljeni naslednji koraki (glej tudi sliko 1):

- (a) pomembnost spremembe [Člen 4]:

prevoznik v železniškem prometu je izvedel predhodno oceno tveganja, v kateri je bilo ugotovljeno, da je bila operativna sprememba pomembna. Ker so strojevodje vozili na novih progah in po možnosti izven svojega običajnega delovnega časa, ni bilo mogoče zanemariti možnosti, da spregledajo signale ob nevarnosti, vozijo prehitro ali ne upoštevajo začasnih omejitev hitrosti.

Pri primerjavi te predhodne ocene tveganja z merili iz Člen 4(2) Uredbe o skupni varnostni metodi bi se lahko sprememba opredelila kot pomembna tudi glede na naslednja merila:

- (1) pomembnost za varnost: sprememba je povezana z varnostjo, ker bi lahko bil vpliv spremembe načina dela strojevodij katastrofalen;
- (2) posledica odpovedi: zgoraj navedene napake strojevodij bi lahko imele katastrofalne posledice;
- (3) novosti: prevoznik v železniškem prometu bi morda lahko uvedel nove načine dela za strojevodje;
- (4) kompleksnost spremembe: spreminjanje ur vožnje bi lahko bilo zapleteno, ker bi lahko bila potrebna popolna ocena in prilagoditev obstoječih delovnih pogojev;

- (b) opredelitev sistema [oddelek 2.1.2.]:

opredelitev sistema je prvotno opisovala:

- (1) obstoječe delovne pogoje: delovni čas, vzorce izmeničnih delovnih dni itd.;
- (2) spremembe delovnega časa;
- (3) vprašanja v zvezi z vmesniki (npr. z upravljavcem železniške infrastrukture).

Med različnimi ponovitvami se je opredelitev sistema posodobila z varnostnimi zahtevami, ki izhajajo iz postopka ocene tveganja. Ključni predstavniki osebja so bili vključeni v ta ponoven postopek opredelitve nevarnosti in posodobitev opredelitve sistema;

- (c) opredelitev nevarnosti [oddelek 2.2.]:

nevarnosti in potencialne varnostne ukrepe za nove proge in vzorce izmeničnih delovnih dni je z zbiranjem zamisli opredelila skupina strokovnjakov, vključno s predstavniki strojevodij. Obravnavale so se naloge strojevodij v zvezi z novimi razmerami, da se oceni, ali vplivajo na strojevodje, njihovo delovno obremenitev, geografski obseg in čas sistema delovne izmene.



Prevoznik v železniškem prometu se je posvetoval tudi s sindikati delavcev, da je ugotovil, ali bi lahko zagotovili dodatne informacije, ter pregledal tveganje glede stopenj izčrpanosti in bolezni, ki bi ga lahko povzročilo morebitno povečanje nadur zaradi daljših poti na neznanih progah.

Vsaki nevarnosti se je pripisala stopnja resnosti tveganja in posledic (visoka, srednja, nizka), v primerjavi z njimi pa se je pregledal tudi vpliv predlagane spremembe (večje, nespremenjeno, manjše tveganje);

- (d) uporaba kodeksov ravnanja [oddelek 2.3.]:

za pregled obstoječih delovnih pogojev in določitev novih varnostnih zahtev so se uporabili kodeksi ravnanja v zvezi z delovnim časom in tveganji glede izčrpanosti ljudi. Potrebna operativna pravila so bila napisana v skladu s kodeksi ravnanja za nov sistem delovnih izmen. Vse potrebne stranke so bile vključene v pregledane operativne postopke in dogovor o nadaljnjem izvajanju spremembe;

- (e) dokazovanje skladnosti sistema z varnostnimi zahtevami [oddelek 3]:

pregledani operativni postopki so se uvedli v sistem varnega upravljanja prevoznika v železniškem prometu. Ti postopki so se spremljali in vzpostavljen je bil postopek pregleda za zagotovitev, da se zagotovi nadaljnji pravilni nadzor opredeljenih nevarnosti med delovanjem železniškega sistema;

- (f) obvladovanje nevarnosti [oddelek 4.1.]:

glej točko zgoraj, ker je lahko za prevoznike v železniškem prometu postopek obvladovanja nevarnosti del njihovega sistema varnega upravljanja za evidentiranje in obvladovanje tveganj. Opredeljene nevarnosti so bile evidentirane v evidenci nevarnosti z varnostnimi zahtevami (tj. sklicevanje na pregledane operativne postopke), ki nadzorujejo s tem povezano tveganje.

Pregledani postopki so se spremljali in po potrebi pregledali, da se zagotovi nadaljnji pravilni nadzor opredeljenih nevarnosti med delovanjem železniškega sistema;

- (g) neodvisna ocena [Člen 6]:

postopka ocenjevanja in obvladovanja tveganja je ocenila pristojna oseba v okviru družbe prevoznika v železniškem prometu, ki je bila neodvisna od postopka ocenjevanja. Pristojna oseba je ocenila postopek in rezultate, tj. opredeljene varnostne zahteve.

Prevoznik v železniškem prometu se je za začetek izvajanja novega sistema odločil na podlagi poročila o neodvisni oceni, ki ga je pripravila pristojna oseba.

- C.6.4. Primer kaže, da so načela in postopek, ki jih je uporabil prevoznik v železniškem prometu, v skladu s skupno varnostno metodo. Postopka obvladovanja in ocenjevanja tveganja sta izpolnila vse zahteve iz skupne varnostne metode.

C.7. Primer ocene tveganja pomembne tehnične spremembe (UVS)

- C.7.1. **Opomba:** ta primer ocene tveganja ne izhaja iz uporabe postopka skupne varnostne metode; izveden je bil pred obstojem skupne varnostne metode. Namen primera je:

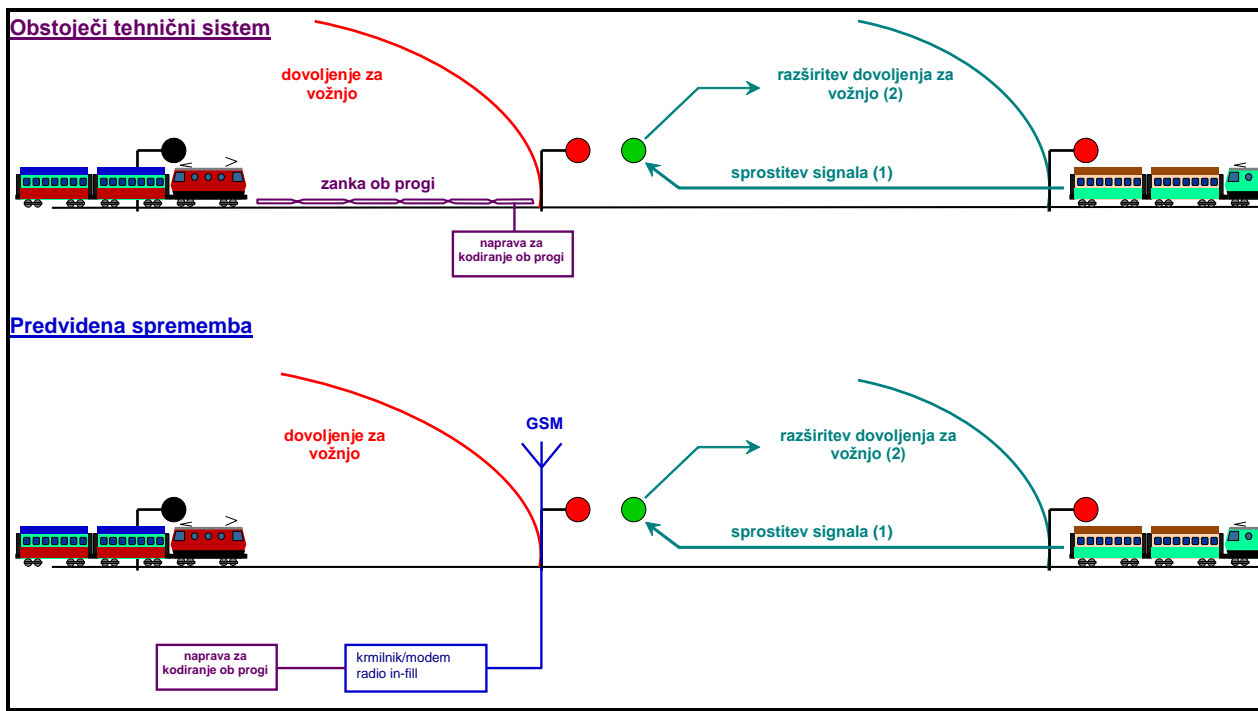
- (a) opredeliti podobnosti med veljavnimi metodami ocenjevanja tveganja in postopkom skupne varnostne metode;
- (b) zagotoviti sledljivost med veljavnim postopkom in postopkom, ki ga zahteva skupna varnostna metoda;



- (c) zagotoviti utemeljitev dodane vrednosti izvedbe dodatnih korakov (če obstajajo), ki se zahtevajo v skupni varnostni metodi.

Poudariti je treba, da je ta primer le informativen. Njegov namen je pomagati bralcu pri razumevanju postopka skupne varnostne metode. Vendar se sam primer ne sme prenesti na drugo pomembno spremembo ali se uporabiti kot referenčen sistem zanjo. Ocena tveganja se v skladu z Uredbo o skupni varnostni metodi izvede za vsako pomembno spremembo.

- C.7.2. Primer je povezan s tehnično spremembo sistema upravljanja - vodenja. Zadevni proizvajalec jo je obravnaval kot pomembno. Za ovrednotenje spremembe se je uporabil pristop na podlagi ocene tveganja.
- C.7.3. Opis spremembe: spremembo predstavlja nadomestitev zanke ob progi pred podsistemom s signalom „radio in-fill + GSM“ (glej Slika 16).
- C.7.4. Težava: ohraniti stopnjo varnosti sistema po spremembi.



Slika 16 : Sprememba zanke ob progi s podsistemom s signalom radio in-fill

- C.7.5. V primerjavi s postopkom skupne varnostne metode se uporabljajo naslednji koraki (glej tudi Slika 1):
- (a) ocena pomembnosti spremembe [Člen 4]:
- merila iz Člen 4(2) se uporabljajo za oceno pomembnosti spremembe. Za odločitev, da je sprememba pomembna, sta se uporabili zlasti stopnji kompleksnosti in novosti;
- (b) opis sistema [oddelek 2.1.2.]:
- (1) opis obstoječega sistema: zanka in njene funkcije v sistemu upravljanja - vodenja;
 - (2) opis spremembe, ki jo načrtujeta predlagatelj in proizvajalec;
 - (3) opis funkcionalne in fizične povezanosti zanke z ostalim sistemom.



Funkcija „zanka + naprave za kodiranje“ v obstoječem sistemu je sprostiti signal ob približevanju vlaka, kadar odsek za signalom (tj. pred približujočim se vlakom) ni zaseden: glej Slika 16;

(c) opredelitev nevarnosti [oddelek 2.2.]:

na podlagi zbiranja zamisli skupine strokovnjakov se uporabi ponoven postopek ocenjevanja tveganja in opredelitve nevarnosti (glej oddelek 2.1.1.), in sicer:

- (1) da se opredelijo nevarnosti s pomembnim vplivom na tveganje zaradi predvidene spremembe;
- (2) da se opredelijo mogoči ukrepi za nadzor tveganja.

Ker zanka, in s tem radio infill, sprosti signal, obstaja tveganje, da se približujočemu vlakom zagotovi nevarno dovoljenje za vožnjo, medtem ko je vlak pred njim še vedno na odseku pred signalom. Tveganje je treba nadzorovati na sprejemljivi ravni;

(d) uporaba referenčnega sistema [oddelek 2.4.]:

stopnja varnosti systema pred spremembo (zanka) je bila ocenjena kot sprejemljiva. Zato se uporablja kot „referenčni sistem“ za izpeljavo varnostnih zahtev za podsistem s signalom radio infill;

(e) eksplicitna ocena in ovrednotenje tveganja [oddelek 2.5.]:

- (1) razlike med „zanko“ in podsistemi „radio infill + GSM“ se analizirajo z eksplicitno oceno in ovrednotenjem tveganja. Za podsistem „radio infill + GSM“ se opredelijo naslednje nove nevarnosti:

- (i) hekerji lahko prenesejo nevarne informacije v zračnih režah, ker je podsistem „radio infill + GSM“ podsistem z odprtim prenosom;
- (ii) zapoznel prenos ali prenos evidentiranih podatkovnih paketov v zračni reži;

- (2) eksplicitna ocena tveganja in uporaba merila za sprejemljivost tveganja za tehnične sisteme za del s krmilnikom radio infill;

(f) uporaba kodeksov ravnanja [oddelek 2.3.]:

- (1) standard EN 50159-2 („*Železniške aplikacije: 2. del: Varnost v zvezi s komunikacijami v odprtih prenosnih (transmisijskih) sistemih*“) zagotavlja varnostne zahteve za nadzorovanje novih nevarnosti na sprejemljivi ravni, npr.:

- (i) kodiranje in zaščita podatkov;
- (ii) določanje zaporedja sporočil in časovno označevanje sporočil;

- (2) na primer uporaba standarda EN 50128 za razvoj programske opreme krmilnika radio infill;

(g) dokazovanje skladnosti sistema z varnostnimi zahtevami [oddelek 3]:

- (1) spremljanje izvajanja varnostnih zahtev prek postopka razvoja podsistema „radio infill + GSM“;
- (2) preverjanje, ali je sistem, kot je projektiran in nameščen, skladen z varnostnimi zahtevami;

(h) obvladovanje nevarnosti [oddelek 4.]:

opredeljene nevarnosti, varnostni ukrepi in nastale varnostne zahteve, ki izhajajo iz ocene tveganja in uporabe treh načel sprejemljivosti tveganja, se evidentirajo in upravljajo v evidenci nevarnosti;

(i) neodvisna ocena [Člen 6]:

neodvisno oceno izvede tudi tretja stranka, in sicer:

- (1) da se preveri, ali se obvladovanje in ocena tveganja izvajata pravilno;
- (2) da se preveri, ali je tehnična sprememba primerna in bo ohranila enake stopnje varnosti kot pred spremembo.

C.7.6. Primer kaže, da se tri načela sprejemljivosti tveganja, ki jih zahteva skupna varnostna metoda, uporabljajo kot dopolnilen način za opredelitev varnostnih zahtev za ocenjevani sistem. Ocena tveganja v primeru izpolnjuje vse zahteve iz skupne varnostne metode, povzete na Slika 1, vključno z upravljanjem evidence nevarnosti in neodvisno oceno varnosti, ki jo izvede tretja stranka.

C.8. Primer švedske smernice BVH 585.30 za oceno tveganja železniških predorov

C.8.1. **Opomba:** ta primer ocene tveganja ne izhaja iz uporabe postopka skupne varnostne metode; izveden je bil pred obstojem skupne varnostne metode. Namen primera je:

- (a) opredeliti podobnosti med veljavnimi metodami ocene tveganja in postopkom skupne varnostne metode;
- (b) zagotoviti sledljivost med veljavnim postopkom in postopkom, ki ga zahteva skupna varnostna metoda;
- (c) zagotoviti utemeljitev dodane vrednosti izvedbe dodatnih korakov (če obstajajo), ki se zahtevajo v skupni varnostni metodi.

Poudariti je treba, da je ta primer le informativen. Njegov namen je pomagati bralcu pri razumevanju postopka skupne varnostne metode. Vendar se sam primer ne sme prenesti na drugo pomembno spremembo ali se uporabiti kot referenčen sistem zanjo. Ocena tveganja se v skladu z Uredbo o skupni varnostni metodi izvede za vsako pomembno spremembo.

C.8.2. Namen primera je primerjati postopek iz skupne varnostne metode s smernico BVH 585.30, ki jo uporablja švedski upravljavec železniške infrastrukture Banverket za projektiranje in preverjanje izpolnjevanja ustrezne stopnje varnosti pri načrtovanju in izgradnji novih železniških predorov. Skupne točke smernice in skupne varnostne metode ter razlike med njima so navedene v nadaljevanju; podrobne zahteve v zvezi z oceno tveganja so navedene v smernici BVH 585.30.

C.8.3. V primerjavi s postopkom skupne varnostne metode na Slika 1 velja naslednje:

(a) smernica BVH 585.30 predstavlja naslednje skupne točke:

(1) opis sistema [oddelek 2.1.2.]:

v smernici se zahteva podroben opis sistema, ki vključuje:

- (i) opis predora;
- (ii) opis proge;
- (iii) opis vrste tirnega vozila (vključno z vlakovnim osebjem);
- (iv) opis prometa in predvidenih delovanj;
- (v) opis zunanje pomoči (vključno z reševalnimi službami);

(2) opredelitev nevarnosti [oddelek 2.2.]:

v smernici se opredelitev nevarnosti ne zahteva izrecno. Zahtevata se opredelitev tveganja ter „katalog nesreč“, ki vključuje vrste opredeljenih morebitnih nesreč, za katere se predvideva, da bi pomembno vplivale na stopnjo tveganja za predor, in jih mora zajeti naknadna ocena. Primeri nesreč:

- (i) „iztirjenje potniškega vlaka“;

- (ii) „iztirjenje tovornega vlaka“;
 - (iii) „nesreča, ki vključuje nevarno blago“;
 - (iv) „požar v vozilu“;
 - (v) „trčenje potniškega vlaka in lahkega/težkega predmeta“
 - (vi) itd.;
- (3) določba o uporabi kodeksov ravnanja ali podobnih referenčnih sistemov ne obstaja. Šteje se, da se mora analiza tveganja izvesti v vsakem primeru;
- (4) eksplicitno oceno in ovrednotenje tveganja [oddelek 2.5.]:
- (i) na splošno se v smernici za vsako vrsto nesreče priporoča izvedba celotnega drevesa dogodkov na podlagi kvantitativne analize tveganja. Vendar ker je namen analize tveganja analizirati globalno stopnjo varnosti predora in ne analizirati varnost posamezno na podrobnejših ravneh, se povzamejo posledice vseh mogočih možnosti, da se ugotovi splošna stopnja tveganja za predor;
 - (ii) sprejemljivost te globalne stopnje tveganja za predor je treba primerjati z naslednjim eksplicitnim kvantitativnim merilom za sprejemljivost tveganja: *„železniški promet na kilometer v predorih je tako varen kot železniški promet na kilometer na tirih na prostem, razen na nivojskih prehodih“*. Merilo je na podlagi zgodovinskih podatkov o železniških nesrečah na Švedskem preneseno na krivuljo F-N in ekstrapolirano, da zajema tudi posledice, ki jih v statističnih podatkih ni;
 - (iii) poleg merila za globalno stopnjo tveganja predora obstajajo tudi dodatne zahteve v zvezi z evakuacijo v predorih in možnostmi za reševalne službe, ki jih je treba izrecno izpolniti:
 - ↳ preveriti je treba, ali je v primeru požara na vlaku v „najslabšem verjetnem primeru“ mogoče samoreševanje (navedena so tudi merila za to oceno);
 - ↳ predor mora biti načrtovan tako, da omogoča reševanje za zadevno število možnosti;
- (5) rezultat ocene tveganja [oddelek 2.1.6.]:
- rezultati ocene tveganja so:
- (i) seznam varnostnih ukrepov, ki izhajajo iz minimalnega standarda na podlagi tehničnih specifikacij za interoperabilnost – varnost v železniških predorih, in nacionalna pravila, ki jih je treba uporabiti pri projektiranju predora, ter
 - (ii) vsi dodatni varnostni ukrepi, ki so bili z analizo tveganja opredeljeni kot potrebni, z navedbo njihovega imena. Navedeno je, da se je treba o ukrepih odločati v skladu z naslednjim prednostnim vrstnim redom:
 - ↳ preprečevanje nesreč;
 - ↳ zmanjšanje posledic nesreč;
 - ↳ omogočanje evakuacije;
 - ↳ omogočanje reševanja;
- (6) obvladovanje nevarnosti [oddelek 4.]:
- smernica vodenje evidence nevarnosti ne zahteva izrecno. To je povezano z dejstvom, da je stopnja ocene globalna, zaradi česar se nevarnosti ne ovrednotijo in nadzorujejo posamezno. Sprejemljivost globalnega tveganja v zvezi s predorom se ovrednoti brez kakršne koli porazdelitve merila za sprejemljivost globalnega tveganja na različne vrste nesreč ali temeljnih nevarnosti.
- Vendar obstaja seznam vseh varnostnih ukrepov, in sicer tistih, ki izhajajo iz „minimalnega standarda“, ter tistih, ki so bili z analizo tveganja opredeljeni kot potrebni: glej točko 0 zgoraj. Na seznamu varnostnih ukrepov je treba navesti, ali ti zadevajo infrastrukturo predora, tire, delovanje ali tirna vozila in tudi kakšen je

njihov predvideni učinek v skladu z oštevilčenim seznamom iz točke 0. Vendar smernica ne zahteva, da se izrecno navede, katere nevarnosti varnostni ukrepi nadzorujejo in kdo je odgovoren za katere ukrepe;

(7) neodvisno oceno [Člen 6]:

neodvisna ocena, ki jo izvede tretja stranka, je obvezna, da:

- (i) se preveri, ali je postopek ocene tveganja, ki je priporočen v smernici BVH 585.30, pravilno izveden;
- (ii) se analiza tveganja šteje za sprejemljivo;
- (iii) se preveri, ali je jasno navedeno, kako je treba izvajati prihodnje varno upravljanje pri projektu.

Končen dokument analize tveganja podpišeta neodvisni ocenjevalec in tudi koordinator za varnost v okviru projekta;

(b) smernica BVH 585.30 se razlikuje v naslednjih vidikih:

(1) dokazovanju skladnosti sistema z varnostnimi zahtevami [oddelek 3]:

smernica BVH 585.30 ne zahteva, da je treba spremljati, kako se opredeljene varnostne zahteve izvajajo, ali preveriti, ali končni načrt predora izpolnjuje navedene varnostne zahteve. Opisuje le, kako je treba to zahtevo prenesti, da se zagotovi njihovo izvajanje v fazi gradnje.

Smernica zagotavlja varnostne zahteve, ki jih je treba uporabiti za preverjanje, ali se analiza tveganja izvaja primerno in pregledno ter ali je lahko sprejeta v okviru projekta.

C.8.4. Primerjava s skupno varnostno metodo torej kaže, da:

- (a) je smernica BVH 585.30 v skladu z ustreznimi deli skupne varnostne metode, čeprav njuna področje uporabe in namen nista popolnoma enaka;
- (b) smernica BVH 585.30 ocenjuje splošno stopnjo tveganja železniškega predora;
- (c) se nevarnosti ne nadzorujejo posamezno, zaradi česar je manj poudarka na obvladovanju nevarnosti;
- (d) dokazovanje skladnosti in preverjanje pravilnega izvajanja vseh varnostnih ukrepov nista izrecno navedena. Vendar je v smernici navedeno, da je vloga koordinatorja za varnost v okviru projekta (vloga in pristojnost, ki se zahtevata v BVH 585.30) preveriti, ali so sklepi analize tveganja uporabljeni v projektnih dokumentih in slikah, ter tudi nadzorovati, da se pravilno uporabijo v fazi gradnje.

C.8.5. Skupna varnostna metoda je splošnejša od smernice BVH 585.30 v tem smislu, da omogoča uporabo treh različnih načel sprejemljivosti tveganja. Vendar uporaba smernice BVH 585.30 v okviru skupne varnostne metode ne povzroča težav, ker je združljiva z uporabo tretjega načela, tj. eksplicitne ocene tveganja.

C.9. Primer ocene tveganja na ravni sistema za podzemno železnico v Københavnu

C.9.1. **Opomba:** ta primer ocene tveganja ne izhaja iz uporabe postopka skupne varnostne metode; izveden je bil pred obstojem skupne varnostne metode. Namen primera je:

- (a) opredeliti podobnosti med veljavnimi metodami ocenjevanja tveganja in postopkom skupne varnostne metode;
- (b) zagotoviti sledljivost med veljavnim postopkom in postopkom, ki ga zahteva skupna varnostna metoda;



- (c) zagotoviti utemeljitev dodane vrednosti izvedbe dodatnih korakov (če obstajajo), ki se zahtevajo v skupni varnostni metodi.

Poudariti je treba, da je ta primer le informativen. Njegov namen je pomagati bralcu pri razumevanju postopka skupne varnostne metode. Vendar se sam primer ne sme prenesti na drugo pomembno spremembo ali se uporabiti kot referenčen sistem zanjo. Ocena tveganja se v skladu z Uredbo o skupni varnostni metodi izvede za vsako pomembno spremembo.

C.9.2. Primer je povezan s celovitim in kompleksnim sistemom podzemne železnice brez strojevodje, vključno s temeljnimi tehničnimi podsistemi (npr. avtomatska zaščita vlakov in tirna vozila) ter delovanjem in vzdrževanjem sistema. Za ovrednotenje sistema in temeljnih podsistemov se je uporabil pristop na podlagi ocene tveganja. Projekt je zajemal tudi izdajo spričeval za sistem varnega upravljanja družbe, ki je morala upravljati sistem. To je povezano z zmožnostjo prevoznika v železniškem prometu in upravljavca železniške infrastrukture, da varno upravljata in vzdržujeta celoten sistem v njegovem celotnem življenjskem ciklu.

C.9.3. V primerjavi s postopkom skupne varnostne metode so se uporabili naslednji koraki (glej tudi Slika 1):

- (a) opis sistema [oddelek 2.1.2.]:
- (1) opis zahtev glede učinkovitosti sistema;
 - (2) opis operativnih pravil;
 - (3) jasen opis vmesnikov in odgovornosti med različnimi udeleženci, zlasti med tehničnimi podsistemi;
 - (4) opis zahtev sistema na visoki ravni (v smislu sprejemljive pogostosti nesreč in opredelitve območja, v katerem je tveganje zmanjšano na najnižjo praktično, še sprejemljivo raven);
- (b) opredelitev nevarnosti [oddelek 2.2.]:
- (1) predhodna analiza nevarnosti na ravni sistema;
 - (2) funkcionalna analiza na ravni sistema, ki poudarja vse podsisteme in ne le očitno pomembnih za varnost (npr. avtomatska zaščita vlaka in tirna vozila), ki sodelujejo pri varnostnih funkcijah ter so dejavni pri zagotavljanju varnosti potnikov in osebja;
 - (3) temeljito usklajevanje med udeleženci (pogodbeniki, podsistemski dobavitelji za tehnične podsisteme in objekte nizke gradnje):
 - (i) da se sistematično opredelijo vse smiselno predvidljive nevarnosti;
 - (ii) da se opredelijo mogoči ukrepi za nadzor vseh tveganj, povezanih z opredeljenimi nevarnostmi, na sprejemljivi ravni;
- (c) uporaba kodeksov ravnanja [oddelek 2.3.]:
- uporabili so se različni kodeksi ravnanja, standardi in uredbe, npr.:
- (1) uredba BOStrab o gradnji in delovanju tramvajev (nemška uredba, ki se uporablja za mestne železniške sisteme) ter o upravljanju brez strojevodje;
 - (2) dokumenti VDV (nemški kodeksi ravnanja) v zvezi z zahtevami glede opreme za zagotavljanje varnosti potnikov na postajah pri upravljanju brez strojevodje;
 - (3) standardi CENELEC za železniške sisteme (EN 50126, 50128 in 50129). Ti standardi obravnavajo zlasti tehnične železniške sisteme. Vendar so bili v veliki meri sprejeti za podzemno železnico v Københavnu, ker vključujejo splošno veljaven metodološki pristop:
 - (i) standard EN 50126 se je uporabil za dejavnosti v zvezi z varnim upravljanjem in oceno tveganja celotnega železniškega sistema;
 - (ii) standard EN 50129 se je uporabil za celoten sistem signalizacije;





- (iii) standard EN 50128 se je uporabil za razvoj programske opreme (vključno z njenim preverjanjem in potrditvijo) za tehnične podsisteme;
- (4) standardi za požarno varnost predorov (NEPA 130);
- (5) standardi za gradbeništvo in objekte nizke gradnje (standardi Eurocode);
- (d) uporaba referenčnega sistema [oddelek 2.4.]:

podzemna železnica je morala doseči stopnjo varnosti ustreznih sodobnih infrastruktur v Nemčiji, Franciji ali Združenem kraljestvu. Ti obstoječi sistemi so se uporabili kot podobni referenčni sistemi za izpeljavo meril za sprejemljivost tveganja v smislu sprejemljivih pogostosti nesreč na podzemni železnici v Københavnu;
- (e) eksplicitna ocena in ovrednotenje tveganja [oddelek 2.5.]:
 - (1) za oceno tveganj, povezanih s posebnimi nevarnostmi;
 - (2) za nadzor prezračevanja predora (vključno s človeškimi dejavniki v gasilskih brigadah) v primeru nevarnosti;
 - (3) za opredelitev ukrepov za zmanjšanje tveganja;
 - (4) za ovrednotenje, ali je za celoten sistem dosežena sprejemljiva stopnja tveganja;
- (f) dokazovanje skladnosti sistema z varnostnimi zahtevami [oddelek 3]:
 - (1) vodstveno in tehnično prizadevanje, skladno s kompleksnostjo sistema, za dokaz varnosti sistema;
 - (2) porazdelitev varnostnih zahtev sistema na tehnične podsisteme in objekte nizke gradnje ter vse funkcije podzemne železnice v zvezi z varnostjo;
 - (3) dokaz, da vsak podsistem, kot je bil zgrajen, izpolnjuje svoje varnostne zahteve;
 - (4) za varnostne funkcije, ki jih izvaja več kot en podsistem, dokazovanja skladnosti z varnostnimi zahtevami ni bilo mogoče končati na ravni podsistema. Izvedlo se je na ravni sistema z združevanjem različnih podsistemov, orodij in postopkov;
 - (5) dokaz, da je celoten sistem skladen z varnostnimi zahtevami na visoki ravni;
- (g) obvladovanje nevarnosti [oddelek 4.]:

opredeljene nevarnosti, z njimi povezani varnostni ukrepi in nastale varnostne zahteve so se evidentirale in upravljale prek centralne evidence nevarnosti. Za to evidenco nevarnosti je bila odgovorna oseba, pristojna za varnost projekta. Operativne nevarnosti, ki so nastale med projektiranjem in namestitvijo, ter nevarnosti v zvezi z delovanjem in vzdrževanjem so bile vključene v evidenco nevarnosti;
- (h) dokazila o uporabi postopkov upravljanja s tveganji in ocenjevanja tveganj [oddelek 5]

rezultati ocene tveganja so bili v skladu z zahtevami iz standardov CENELEC uradno dokumentirani in podprti z varnostno analizo:

 - (1) varnostna analiza za celotni sistem;
 - (2) varnostna analiza za vsak tehnični podsistem (vključno s podsistemom signalizacije in objekti nizke gradnje);
 - (3) varnostna analiza za objekte nizke gradnje (postaje, predore, viadukte, nasipe);
 - (4) varnostna analiza za infrastrukturo;
 - (5) varnostna analiza za vozila;
 - (6) varnostna analiza izvajalca (pomoč pri izdaji spričevala za sistem varnega upravljanja prevoznika v železniškem prometu in upravljavca železniške infrastrukture, tj. dokazilo o zmožnosti predlagatelja, da sistem varno upravlja in vzdržuje);
- (i) neodvisna ocena [Člen 6]:

celoten postopek je spremljal in ocenil neodvisni ocenjevalec varnosti, ki je deloval s pooblastilom tehničnega nadzornega organa (tj. danskega ministrstva za promet). Vloge

neodvisnega ocenjevalca varnosti so določene v ustreznem kodeksu ravnanja. To je vključevalo:

- (1) preverjanje pravilnega obvladovanja tveganja in ocene tveganja;
- (2) preverjanje, ali sistem ustreza namenu in ali se bo v celotnem življenjskem ciklu varno upravljal in vzdrževal;
- (3) priporočilo za sprejetje tehničnemu nadzornemu organu.

C.9.4. Celoten projekt je bil podprt s primernim postopkom vodenja kakovosti.

C.9.5. Pri projektu so bili dokazi dobaviteljev (tj. varnostne analize in podrobna podpora dokumentacija za tehnične podsisteme in nizko gradnjo) predloženi osebi, pristojni za varnost predlagatelja. Te dokaze sta nato pregledala organizacija za varno upravljanje in tudi neodvisni ocenjevalec varnosti, katerih sklepi so bili navedeni v poročilu o oceni. Poročilo o neodvisni oceni varnosti je pregledal upravljavec varnosti predlagatelja, nato pa je bilo predloženo predlagatelju, ki je vso dokumentacijo posredoval tehničnemu nadzornemu organu (tj. danskemu ministrstvu za promet) za končno odobritev.

C.9.6. Primer kaže, da so načela, ki jih zahteva skupna varnostna metoda, veljavne metode v železniškem sektorju. Ocena tveganja iz opisanega primera izpolnjuje vse zahteve iz skupne varnostne metode. Zlasti uporablja vsa tri načela sprejemljivosti tveganja, ki jih dovoljuje usklajen pristop skupne varnostne metode.

C.10. Primer smernice Medvladne organizacije za mednarodni železniški promet (OTIF) za izračun tveganja zaradi prevoza nevarnega blaga po železnici

C.10.1. **Opomba:** ta primer ocene tveganja ne izhaja iz uporabe postopka skupne varnostne metode; izveden je bil pred obstojem skupne varnostne metode. Namen primera je:

- (a) opredeliti podobnosti med veljavnimi metodami ocenjevanja tveganja in postopkom skupne varnostne metode;
- (b) zagotoviti sledljivost med veljavnim postopkom in postopkom, ki ga zahteva skupna varnostna metoda;
- (c) zagotoviti utemeljitev dodane vrednosti izvedbe dodatnih korakov (če obstajajo), ki se zahtevajo v skupni varnostni metodi.

Poudariti je treba, da je ta primer le informativen. Njegov namen je pomagati bralcu pri razumevanju postopka skupne varnostne metode. Vendar se sam primer ne sme prenesti na drugo pomembno spremembo ali se uporabiti kot referenčen sistem zanjo. Ocena tveganja se v skladu z Uredbo o skupni varnostni metodi izvede za vsako pomembno spremembo.

C.10.2. Celotna filozofija smernice OTIF je v skladu z namenom skupne varnostne metode, vendar je področje uporabe smernice manjše. Cilj smernice OTIF „je pridobiti enotnejši pristop za oceno tveganja prevoza nevarnega blaga v državah članicah Konvencije o mednarodnih železniških prevozih (COTIF) in s tem narediti posamezne ocene tveganja primerljive“. Tako podpira vzajemno odobritev ocen tveganja prevoza nevarnega blaga po železnici med državami članicami COTIF.

C.10.3. V primerjavi s skupno varnostno metodo in prikazom postopkov na Slika 1:

- (a) smernica OTIF predstavlja naslednje skupne točke:



- (1) je skupen pristop za ocenjevanje tveganja, čeprav temelji le na eksplicitni oceni tveganja (tj. na tretjem načelu sprejemljivosti tveganja iz skupne varnostne metode);
- (2) ocena tveganja OTIF je sestavljena iz:
 - (i) faze analize tveganja, ki vključuje:
 - ↪ fazo opredelitve nevarnosti;
 - ↪ fazo ocene tveganja;
 - (ii) faze ovrednotenja tveganja, ki temelji na merilih za (sprejemljivost) tveganje(-a), ki še niso usklajena. Dejansko lahko na navedena merila vpliva veliko nacionalnih posebnosti;
- (b) smernica OTIF se razlikuje v naslednjih vidikih:
 - (1) področje uporabe je drugačno. Medtem ko je treba skupno varnostno metodo uporabljati le za pomembne spremembe železniškega sistema, je treba smernico OTIF uporabljati za oceno tveganj prevoza nevarnega blaga po železnici ne glede na to, ali je to pomembna sprememba železniškega sistema ali ne;
 - (2) izbira med tremi načeli sprejemljivosti tveganja za nadzor tveganja (tveganj) ni mogoča. Dovoljeno je le tretje načelo, tj. eksplicitna ocena tveganja. Poleg tega mora temeljiti izključno na kvantitativni presoji in ne kvalitativni. Kvalitativna analiza tveganja je lahko ustrezna le za primerjanje različnih (varnostnih) ukrepov za zmanjšanje tveganja;
 - (3) zahteva se uporaba načela ALARP (tveganje je zmanjšano na najnižjo praktično, še sprejemljivo raven) za določitev, ali bi se lahko ocenjeno tveganje z dodatnimi varnostnimi ukrepi nadalje zmanjšalo pri razumni ceni;
 - (4) pojem „nevarnosti, povezane s splošno sprejemljivim tveganjem“, ki bi omogočal, da se prizadevanje v zvezi z oceno tveganja osredotoči na nevarnosti z največjim prispevkom, ne obstaja. Kljub temu se v njej priporoča, da se število mogočih možnosti v zvezi z nesrečami zmanjša na razumno število temeljnih možnosti (glej oddelek 3.2. {Ref. 10});
 - (5) postopek se osredotoča na oceno tveganja, vendar ne vključuje:
 - (i) postopka za izbiro in izvajanje (varnostnih) ukrepov za preoblikovanje tveganja;
 - (ii) postopka za sprejemljivost tveganja;
 - (iii) postopka za dokazovanje skladnosti sistema z varnostnimi zahtevami;
 - (iv) postopka za sporočanje tveganja drugim zadevnim udeležencem (glej točko v nadaljevanju);
 - (6) v njej ni navodil v zvezi z dokazi, ki jih je treba predložiti v okviru postopka ocenjevanja tveganja;
 - (7) ni zahteve za obvladovanje nevarnosti;
 - (8) ni zahteve za neodvisno oceno pravilne uporabe skupnega pristopa, ki jo izvede tretja stranka.

C.10.4. Primerjava med smernico OTIF in skupno varnostno metodo kaže, da sta združljivi, čeprav njuna področje uporabe in namen nista popolnoma enaka. Skupna varnostna metoda je splošnejša od smernice OTIF in je v tem smislu prožnejša. Po drugi strani skupna varnostna metoda zajema tudi več dejavnosti obvladovanja tveganja:

- (a) omogoča uporabo treh načel sprejemljivosti tveganja, ki temeljijo na obstoječih praksah v zvezi z železnicami: glej oddelek 2.1.4.;





- (b) njena uporaba se zahteva le za pomembne spremembe, pri čemer se nadaljnja analiza tveganja zahteva le za nevarnosti, ki niso povezane s splošno sprejemljivim tveganjem;
- (c) vključuje izbiro in izvajanje varnostnih ukrepov, za katere se pričakuje, da bodo nadzorovali opredeljene nevarnosti in z njimi povezana tveganja;
- (d) usklajuje postopek obvladovanja tveganja, vključno z:
 - (1) usklajevanjem meril za sprejemljivost tveganja, ki se obravnava v okviru dela Agencije v zvezi s splošno sprejemljivimi tveganji in merili za sprejemljivost tveganja;
 - (2) dokazovanjem skladnosti sistema z varnostnimi zahtevami;
 - (3) rezultati in dokazi iz postopka ocene tveganja;
 - (4) izmenjavo informacij v zvezi z varnostjo med udeleženci, ki so vključeni prek vmesnikov;
 - (5) upravljanjem vseh opredeljenih nevarnosti in z njimi povezanih varnostnih ukrepov v evidenci nevarnosti;
 - (6) neodvisno oceno pravilne uporabe skupne varnostne metode, ki jo izvede tretja stranka.

C.10.5. Uporaba smernice OTIF v okviru skupne varnostne metode (če prevoz nevarnega blaga pomeni pomembno spremembo za upravljavca železniške infrastrukture ali prevoznika v železniškem prometu) kljub temu ne povzroča težav, ker je združljiva z uporabo tretjega načela, tj. eksplicitne ocene tveganja.

C.11. Primer ocene tveganja v zvezi odobritvijo nove vrste tirnih vozil

C.11.1. **Opomba:** ta primer ocene tveganja ne izhaja iz uporabe postopka skupne varnostne metode; izveden je bil pred obstojem skupne varnostne metode. Namen primera je:

- (a) opredeliti podobnosti med veljavnimi metodami ocenjevanja tveganja in postopkom skupne varnostne metode;
- (b) zagotoviti sledljivost med veljavnim postopkom in postopkom, ki ga zahteva skupna varnostna metoda;
- (c) zagotoviti utemeljitev dodane vrednosti izvedbe dodatnih korakov (če obstajajo), ki se zahtevajo v skupni varnostni metodi.

Poudariti je treba, da je ta primer le informativen. Njegov namen je pomagati bralcu pri razumevanju postopka skupne varnostne metode. Vendar se sam primer ne sme prenesti na drugo pomembno spremembo ali se uporabiti kot referenčen sistem zanjo. Ocena tveganja se v skladu z Uredbo o skupni varnostni metodi izvede za vsako pomembno spremembo.

C.11.2. Ta primer ocene tveganja je povezan z odobritvijo nove vrste tirnih vozil. Analiza tveganja se je izvedla, da se ovrednotijo tveganja v zvezi z uvedbo novega tovornega vagona.

C.11.3. Namen spremembe je bil povečati učinkovitost, zmogljivost, uspešnost in zanesljivost v zvezi s prevozom blaga v razsutem stanju na posebni tovorni progi. Ker so bili vagoni predvideni za čezmejni promet, je bila potrebna tudi odobritev dveh različnih nacionalnih varnostnih organov. Predlagatelj je bil prevoznik tovora, ki je v lasti družbe, ki proizvaja blago za prevoz.

C.11.4. Razvoj projekta je zajemal načrtovanje, proizvodnjo, sestavljanje, začetek uporabe in preverjanje novega tirnega vozila. Analiza tveganja se je izvedla za preverjanje, ali je novo projektiranje izpolnilo varnostne zahteve za vsak podsistem in sistem v celoti.

C.11.5. V analizi tveganja je naveden sklic na postopke in opredelitve iz standarda CENELEC EN 50126, v skladu s katerim se izvede ovrednotenje tveganja.



C.11.6. V primerjavi s postopkom skupne varnostne metode so se uporabili naslednji koraki:

(a) opis sistema [oddelek 2.1.2.]:

za vsako fazo projektiranja so obstajale zahteve v zvezi z dokumentacijo o preverjanju varnosti in opisom projektiranja sistema:

- (1) faza zasnove: predhoden opis operativnih zahtev izvajalca;
- (2) faza podrobnega opisa: funkcionalna specifikacija, veljavni tehnični standardi, načrt za preskušanje in preverjanje. Vključene so bile tudi zahteve izvajalca v zvezi z uporabo in vzdrževanjem vagona;
- (3) faza proizvodnje: tehnična dokumentacija proizvajalca, vključno s skicami, standardi, izračuni, analizami itd. Poglobljena analiza tveganja za nova ali inovativna projektiranja ali nova področja uporabe;
- (4) faza preverjanja:
 - (i) proizvajalec preverja tehnično učinkovitost vagona (poročila o preskusih, izračuni, preverjanja v skladu s standardi in funkcionalnimi zahtevami);
 - (ii) dokumentiranje ukrepov za zmanjševanje tveganja in poročila o preskusih za dokaz združljivosti vagonov z železniško infrastrukturo;
 - (iii) dokumenti o vzdrževanju in usposabljanju, priročniki za uporabo itd.;
- (5) faza sprejetja:
 - (i) izjava o varnosti in dokaz o varnosti (varnostna analiza), ki ju predloži proizvajalec;
 - (ii) izvajalec sprejme tovorni vagon in z njim povezano dokumentacijo;

(b) opredelitev nevarnosti [oddelek 2.2.]:

to se je stalno izvajalo v vseh fazah projektiranja. Najprej se uporabi pristop „od spodaj navzgor“, po katerem so različni proizvajalci ovrednotili zaporedja tveganja, ki izhajajo iz okvare komponent v okviru njihovega podsistema. Razdelitev na podсистeme je bila naslednja:

- (1) šasija;
- (2) zavorni sistem;
- (3) središčna naprava za spenjanje vagonov;
- (4) itd.

Nato se je za iskanje vrzeli ali manjkajočih informacij uporabil pristop „od zgoraj navzdol“. Tveganja, ki jih ni bilo mogoče takoj sprejeti, so se prenesla v evidenco nevarnosti za nadaljnjo obravnavo in razvrstitev;

(c) uporaba načel sprejemljivosti tveganja [oddelek 2.1.4.]:

eksplicitna ocena tveganja se je izvedla na sistemu kot celoti. Vendar bi se lahko za oceno posameznih nevarnosti uporabili kodeksi ravnanja ali podobni referenčni sistemi. Velja načelo, da mora biti vsak nov podsystem vsaj tako varen kot podsystem, ki ga nadomešča, zaradi česar je stopnja varnosti celotnega novega sistema višja od stopnje prejšnjega sistema. Matrika tveganja iz standarda EN50126 se je uporabila za grafični prikaz opredeljenih nevarnosti. Uporabila so se tudi različna dodatna merila za sprejemljivost tveganja, med drugim:

- (1) posamezna okvara ne sme povzročiti razmer, v katerih bi lahko bili ljudje, oprema ali okolje resno prizadeti;
- (2) če se temu ni mogoče izogniti s tehničnimi konstrukcijskimi sredstvi, je treba to preprečiti z operativnimi pravili ali zahtevami v zvezi z vzdrževanjem. To je veljalo le za nevarnosti, v zvezi s katerimi je bilo mogoče ugotoviti nastalo okvaro, preden je povzročila nevarne razmere;



- (3) za komponente z veliko možnostmi za okvaro ali kadar okvar ni mogoče odkriti vnaprej ali jih preprečiti z izpolnjevanjem operativnih pravil, je treba obravnavati dodatne varnostne funkcije in pregrade;
 - (4) redundantne sisteme s komponentami, na katerih lahko med delovanjem nastanejo okvare, ki jih ni mogoče odkriti, je treba zaščititi z ukrepi v zvezi z vzdrževanjem, da se prepreči manjša redundančnost;
 - (5) iz tega izhajajoča končna stopnja varnosti je bila odločitev o upravljanju, ki je temeljila na kvantitativni in kvalitativni analizi tveganja;
- (d) dokazovanje skladnosti sistema z varnostnimi zahtevami [oddelek 3]:
- vsa opredeljena tveganja in nevarnosti so se evidentirali, v zvezi s seznamom so potekala stalna posvetovanja, seznam pa se je stalno posodabljal. Preostale nevarnosti so se evidentirale v evidenci nevarnosti skupaj z ustreznim seznamom ukrepov za zmanjševanje tveganja, ki jih je treba sprejeti pri načrtovanju, delovanju in vzdrževanju. Na podlagi tega je bilo s preverjanjem, ali so se varnostne zahteve izvedle, pripravljeno končno poročilo o varnosti;
- (e) obvladovanje nevarnosti [oddelek 4.]:
- kot je navedeno zgoraj, so se nevarnosti in z njimi povezani varnostni ukrepi evidentirali v evidenci nevarnosti, v kateri se spremljajo vse opredeljene nevarnosti in varnostni ukrepi. Vendar nevarnosti, povezane s tveganji, ki so bila sprejemljiva brez ukrepov, niso bile vključene v evidenco nevarnosti;
- (f) neodvisna ocena [Člen 6]:
- v predloženih dokumentih v zvezi s to pomembno spremembo neodvisna ocena ni bila navedena.

C.11.7. Primer ocene tveganja temelji na standardu CENELEC EN 50126 in zato dobro ustreza postopku skupne varnostne metode. Ocena tveganja iz primera izpolnjuje vse zahteve iz skupne varnostne metode, razen zahteve za neodvisno oceno, ki v predloženih dokumentih ni bila izrecno pojasnjena. Uporabljena so bila eksplicitna merila za sprejemljivost tveganja, ki so bila jasno navedena.

C.12. Primer ocene tveganja pomembne operativne spremembe – vlak upravlja le strojevodja

C.12.1. **Opomba:** ta primer ocene tveganja ne izhaja iz uporabe postopka skupne varnostne metode; izveden je bil pred obstojem skupne varnostne metode. Namen primera je:

- (a) opredeliti podobnosti med veljavnimi metodami ocenjevanja tveganja in postopkom skupne varnostne metode;
- (b) zagotoviti sledljivost med veljavnim postopkom in postopkom, ki ga zahteva skupna varnostna metoda;
- (c) zagotoviti utemeljitev dodane vrednosti izvedbe dodatnih korakov (če obstajajo), ki se zahtevajo v skupni varnostni metodi.

Poudariti je treba, da je ta primer le informativen. Njegov namen je pomagati bralcu pri razumevanju postopka skupne varnostne metode. Vendar se sam primer ne sme prenesti na drugo pomembno spremembo ali se uporabiti kot referenčen sistem zanjo. Ocena tveganja se v skladu z Uredbo o skupni varnostni metodi izvede za vsako pomembno spremembo.



C.12.2. Primer je operativna sprememba, pri kateri se je prevoznik v železniškem prometu odločil, da mora vlak na progi, na kateri je prej pri odpravi vlaka strojevodja pomagal sprevodnik, upravljati le strojevodja.

C.12.3. V primerjavi s postopkom skupne varnostne metode so se uporabili naslednji koraki (glej tudi Slika 1):

(a) pomembnost spremembe [Člen 4]:

prevoznik v železniškem prometu je izvedel predhodno oceno tveganja, v kateri se je ugotovilo, da je bila operativna sprememba pomembna. Ker je moral strojevodja vlak upravljati sam, brez pomoči, ni bilo mogoče zanemariti možnosti, da bi se lahko potniki ujeli med vrata ali padli na tire (npr. če se vrata odprejo na napačni strani).

Pri primerjavi te predhodne ocene tveganja z merili iz Člen 4 Uredbe o skupni varnostni metodi, bi se lahko sprememba opredelila kot pomembna tudi glede na naslednja merila:

- (1) pomembnost za varnost: sprememba je povezana z varnostjo, ker bi lahko bil vpliv zahteve za popolnoma drugačen način upravljanja storitev železniškega prevoza katastrofalen;
- (2) posledica okvare: možen učinek učinkovitosti strojevodje lahko povzroči katastrofalne posledice, če se delovanje ne nadzoruje učinkovito;
- (3) novost: če vlak upravlja le strojevodja, so lahko potrebni novi načini upravljanja vlakov, katerih tveganja je treba oceniti;

(b) opredelitev sistema [oddelek 2.1.2.]:

opredelitev sistema je opisovala:

- (1) obstoječ sistem, pri čemer je bilo jasno obrazloženo, katere naloge je opravljal strojevodja in katere je v pomoč strojevodji izvajalo osebje na vozilu (ali sprevodnik);
- (2) spremembo odgovornosti strojevodje zaradi odprave pomožnega osebja na vlaku;
- (3) tehnične zahteve sistema, da se zajamejo spremembe pri delovanju;
- (4) obstoječi vmesniki med pomožnim osebjem na vozilu, strojevodjo in osebjem upravljalca železniške infrastrukture ob progi.

Med različnimi ponovitvami se je opredelitev sistema posodobila z varnostnimi zahtevami, ki izhajajo iz postopka ocene tveganja. Ključne osebe (vključno s strojevodji, predstavniki osebja in upravljalcem železniške infrastrukture) so bile vključene v ta ponoven postopek opredelitve nevarnosti in posodobitev opredelitve sistema;

(c) opredelitev nevarnosti [oddelek 2.2.]:

nevarnosti in mogoče varnostne ukrepe je z zbiranjem zamisli opredelila skupina strokovnjakov, med drugim vključno s:

- (1) strojevodji in predstavniki osebja zaradi njihovih izkušenj v zvezi z upravljanjem;
- (2) predstavniki upravljalca železniške infrastrukture, ker bi sprememba lahko vplivala tudi na infrastrukturo, kar na primer pomeni spremembe v zvezi s postajami (npr. namestitve ogledal/video nadzora na peronih).

Dodatne naloge, ki jih mora opravljati strojevodja, so bile pregledane, da se opredelijo vse predvidljive nevarnosti, ki bi lahko nastale zaradi odprave pomožnega osebja na vlaku. Opredelitev nevarnosti je obravnavala zlasti, kaj bi lahko bile ključne operativne nevarnosti na postajah in na obstoječih poteh, kjer je pomagalo osebje na vozilu ali ob

progi, vključno z varno odpravo vlakov, posebnimi zadevami v zvezi s strojevodjo, tirnimi vozili (npr. preverjanje odpiranja/zapiranja vrat), zahtevami v zvezi z vzdrževanjem itd.

Vsaki opredeljeni nevarnosti se je pripisala stopnja resnosti tveganja in posledic (visoka, srednja, nizka), na podlagi tega pa se je pregledal tudi vpliv predlagane spremembe (večje, nespremenjeno, manjše tveganje);

- (d) uporaba kodeksov ravnanja [oddelek 2.3.] in uporaba podobnih referenčnih sistemov [oddelek 2.4.]:

tako kodeksi ravnanja (tj. sklop standardov za vlak, ki ga upravlja le strojevodja) kot podobni referenčni sistemi so se uporabili za opredelitev varnostnih zahtev za opredeljene nevarnosti. Te varnostne zahteve so vključevale:

- (1) pregledane operativne postopke za strojevodjo, ki se zahtevajo za varno upravljanje vlakov brez pomoči na vozilu;
- (2) kakršno koli dodatno opremo, ki se potrebuje na vozilu ali na progi, da se zagotovijo varna in zanesljiva sredstva za odpravo vlakov;
- (3) kontrolni seznam za zagotovitev, da je bila kabina strojevodje primerna, pri čemer se upošteva vmesnik med železniškim sistemom (na vozilu in ob progi) ter strojevodjo.

Potrebna operativna pravila so se pregledala v skladu z zahtevami iz veljavnih kodeksov ravnanja in ustreznih referenčnih sistemov. Vse potrebne stranke so bile vključene v pregledane operativne postopke in dogovor o nadaljnjem izvajanju spremembe;

- (e) dokazovanje skladnosti sistema z varnostnimi zahtevami [oddelek 3]:

sistem se je izvedel v skladu z opredeljenimi varnostnimi zahtevami (dodatna oprema in pregledani postopki). Te so bile preverjene kot primerna sredstva za zagotovitev ustrezne stopnje varnosti za ocenjevani sistem.

Pregledani operativni postopki so bili uvedeni v sistem varnega upravljanja prevoznika v železniškem prometu. Spremljali so se in po potrebi pregledali, da se zagotovi nadaljnji pravilni nadzor opredeljenih nevarnosti med delovanjem železniškega sistema;

- (f) obvladovanje nevarnosti [oddelek 4.]:

glej točko zgoraj, ker je lahko za prevoznike v železniškem prometu postopek obvladovanja nevarnosti del njihovega sistema varnega upravljanja za evidentiranje in obvladovanje tveganj. Opredeljene nevarnosti so se v evidenci nevarnosti evidentirale z varnostnimi zahtevami, ki nadzorujejo s tem povezano tveganje, tj. sklicevanjem na dodatno opremo na vozilu in ob progi ter pregledane operativne postopke.

Pregledani postopki so se spremljali in po potrebi pregledali, da se zagotovi nadaljnji pravilni nadzor opredeljenih nevarnosti med delovanjem železniškega sistema;

- (g) neodvisna ocena [Člen 6]:

postopka ocene in obvladovanja tveganja je ocenila pristojna oseba v okviru družbe prevoznika v železniškem prometu, ki je bila neodvisna od postopka ocene. Pristojna oseba je ocenila postopek in rezultate, tj. opredeljene varnostne zahteve.

Prevoznik v železniškem prometu se je za začetek izvajanja novega sistema odločil na podlagi poročila o neodvisni oceni, ki ga je pripravila pristojna oseba.

- C.12.4. Primer kaže, da so načela in postopek, ki jih je uporabil prevoznik v železniškem prometu, v skladu s skupno varnostno metodo. Postopka obvladovanja in ocenjevanja tveganja sta izpolnila vse zahteve iz skupne varnostne metode.

C.13. Primer uporabe referenčnega sistema za izpeljavo varnostnih zahtev za nove sisteme elektronskih zapornic v Nemčiji

C.13.1. **Opomba:** ta primer ocene tveganja ne izhaja iz uporabe postopka skupne varnostne metode; izveden je bil pred obstojem skupne varnostne metode. Namen primera je:

- (a) opredeliti podobnosti med veljavnimi metodami ocenjevanja tveganja in postopkom skupne varnostne metode;
- (b) zagotoviti sledljivost med veljavnim postopkom in postopkom, ki ga zahteva skupna varnostna metoda;
- (c) zagotoviti utemeljitev dodane vrednosti izvedbe dodatnih korakov (če obstajajo), ki se zahtevajo v skupni varnostni metodi.

Poudariti je treba, da je ta primer le informativen. Njegov namen je pomagati bralcu pri razumevanju postopka skupne varnostne metode. Vendar se sam primer ne sme prenesti na drugo pomembno spremembo ali se uporabiti kot referenčen sistem zanjo. Ocena tveganja se v skladu z Uredbo o skupni varnostni metodi izvede za vsako pomembno spremembo.

C.13.2. Za izpeljavo standardnih varnostnih zahtev za prihodnje sisteme elektronskih zapornic je morala družba Deutsche Bahn opraviti analizo tveganja že odobrenega elektronskega sistema. Ta sistem je bil predhodno odobren v skladu z nemškim kodeksom ravnanja (Mü 8004).

C.13.3. Analiza tveganja se je izvedla v skladu s standardoma CENELEC (EN 50126 in EN 50129) in je vključevala naslednje korake:

- (a) opredelitev sistema;
- (b) opredelitev nevarnosti;
- (c) analizo in kvantitativno opredelitev nevarnosti.

C.13.4. Pri opredelitvi sistema so se opredelili meje sistema, njegove funkcije in vmesniki. Pri tem je bil največji izziv sistem opredeliti tako, da je neodvisen od notranje arhitekture sistema zapornic, medtem ko ostane združljiv z obstoječimi sistemi zapornic. Zato je bila posebna pozornost namenjena zelo jasni opredelitvi vmesnikov z zunanjimi sistemi, ki vzajemno delujejo z zapornicami, brez podrobnega opisa notranjih funkcij zapornic.

C.13.5. Nevarnosti so se nato opredelile le pri vmesnikih, da so ostale splošne (tj. da so se izognile vsaki odvisnosti od posebnih arhitektur). Obravnavale so se le nevarnosti, ki izhajajo iz tehničnih napak. Za vsak vmesnik sta se torej opredelili dve splošni nevarnosti:

- (a) vmesniku se prenese napačen izhodni element iz zapornice
- (b) (pravilen) vhodni element je na vmesniku pokvarjen

C.13.6. Nato so se za te splošne nevarnosti pri vsakem vmesniku navedle posebne značilnosti.

C.13.7. V naslednji fazi so se analizirali prispevki komponent obstoječega sistema k vsaki opredeljeni nevarnosti ter zbrali na drevesu napak. Na podlagi ocenjenih stopenj okvar komponent je bilo mogoče izračunati stopnjo pojavljanja za vsako nevarnost ter te stopnje uporabiti kot dopustno stopnjo nevarnosti (THR) za prihodnje generacije elektronskih zapornic.

C.13.8. Analizo tveganja je spremljal in ocenil nacionalni varnostni organ (EBA).

C.13.9. Kot del analize tveganja se je opravila tudi analiza funkcij za nadzor in prikaz v elektronskem sistemu. Obstoječ odobren sistem elektronskih zapornic se je ponovno uporabil kot referenca za izpeljavo varnostnih zahtev funkcij vmesnika človek-stroj za nadzorovanje

naključnih okvar in napak ter nadzorovanje sistematičnih napak. Kot rezultat so se določile stopnje varnostne integritete (SIL) za različne funkcije: za funkcije vmesnika človek-stroj pri običajnem delovanju, za funkcije vmesnika človek-stroj pri delovanju ukaz - izklop (poslabšan način delovanja) in za funkcionalnost prikaza.

C.13.10. Tudi to analizo tveganja je spremljal in ocenil nacionalni varnostni organ (EBA).

C.13.11. Ti primeri ocene tveganja prikazujejo, kako se lahko drugo načelo sprejemljivosti tveganja (referenčni sistem) iz skupne varnostne metode uporabi za izpeljavo varnostnih zahtev za nove sisteme. Poleg tega so temeljili na standardih CENELEC in zato dobro ustrezajo postopku skupne varnostne metode. Ocena tveganja v primerih izpolnjuje zahteve iz skupne varnostne metode v zvezi z zajetimi fazami. Vendar ker ni vključena nobena dejavnost projektiranja, ni niti sklicevanja na upravljanje evidence nevarnosti niti na dokazovanje skladnosti ocenjevanega sistema z opredeljenimi varnostnimi zahtevami.

C.13.12. Več informacij o teh analizah tveganja je na voljo v:

- (a) Ziegler, P., Kupfer, L., Wunder, H.: „*Erfahrungen mit der Risikoanalyse ESTW (DB AG)*“, Signal + Draht, 10, 2003, 10–15 in
- (b) Bock, H., Braband, J., in 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. Primer eksplicitnega merila za sprejemljivost tveganja za radijsko upravljanje vlaka (FFB) v Nemčiji

C.14.1. **Opomba:** ta primer ocene tveganja ne izhaja iz uporabe postopka skupne varnostne metode; izveden je bil pred obstojem skupne varnostne metode. Namen primera je:

- (a) opredeliti podobnosti med veljavnimi metodami ocenjevanja tveganja in postopkom skupne varnostne metode;
- (b) zagotoviti sledljivost med veljavnim postopkom in postopkom, ki ga zahteva skupna varnostna metoda;
- (c) zagotoviti utemeljitev dodane vrednosti izvedbe dodatnih korakov (če obstajajo), ki se zahtevajo v skupni varnostni metodi.

Poudariti je treba, da je ta primer le informativen. Njegov namen je pomagati bralcu pri razumevanju postopka skupne varnostne metode. Vendar se sam primer ne sme prenesti na drugo pomembno spremembo ali se uporabiti kot referenčen sistem zanjo. Ocena tveganja se v skladu z Uredbo o skupni varnostni metodi izvede za vsako pomembno spremembo.

C.14.2. Za popolnoma nov operativen postopek, ki je bil predviden (vendar nikoli uveden) v Nemčiji za železniške proge za konvencionalne hitrosti, je bila v skladu s standardi CENELEC izvedena analiza tveganja. Zamišljena je vključevala varno upravljanje vlakov le prek radijskega nadzora (proge in vlaka). Ker kodeksi ravnanja (priznani tehnično-tehnološki predpisi) in referenčni sistemi za takšen nov sistem niso obstajali, se je izvedla eksplicitna ocena tveganja, da se prikaže varnost novega postopka. Pokazati je bilo treba, da stopnja tveganja za potnika zaradi novega sistema ne bi preseгла sprejemljive vrednosti tveganja (eksplicitno merilo za sprejemljivost tveganja).

C.14.3. To eksplicitno merilo za sprejemljivost tveganja se je ocenilo na podlagi statističnih podatkov o nesrečah v Nemčiji, ki jih je bilo mogoče pripisati sistemom signalizacije in nadzora,

preverila pa se je tudi njegova verodostojnost po merilu MEM (najmanjša endogena smrtnost). Takšen dokaz varnosti je v skladu z zahtevo iz nemške uredbe EBO (Eisenbahn-Bau- und Betriebsordnung), da je treba v primeru odstopanj od tehnično-tehnoloških predpisov dosegati „enako stopnjo varnosti“. Analizo tveganja je prav tako spremljal in ocenil nacionalni varnostni organ (EBA).

- C.14.4. Ta primer ocene tveganja kaže, kako se lahko globalno eksplicitno merilo (za tretje načelo sprejemljivosti tveganja iz skupne varnostne metode) izpelje za nove sisteme brez veljavnih kodeksov ravnanja ali kakršnega koli referenčnega sistema. Analiza tveganja, ki se je nato izvedla za nov sistem, temelji na standardih CENELEC in zato dobro ustreza postopku skupne varnostne metode. Ocena tveganja v primeru izpolnjuje zahteve iz skupne varnostne metode, vendar ne omenja upravljanja evidence nevarnosti ali dokazovanja skladnosti ocenjevanega sistema z opredeljenimi varnostnimi zahtevami.
- C.14.5. Več informacij o tej analizi tveganja je na voljo v: Braband, J., Günther, J., Lennartz, K., Reuter, D.: „*Risikoakzeptanzkriterien für den FunkFahrBetrieb (FFB)*“, Signal + Draht, št. 5, 2001, 10–15.

C.15. Primer preskusa uporabe merila za sprejemljivost tveganja za tehnične sisteme

C.15.1. Namen tega dodatka je na primeru funkcije podsistema ETCS na vlaku pokazati, kako uporabiti merilo iz oddelka 2.5.4. in kako določiti, ali se lahko merilo za sprejemljivost tveganja za tehnične sisteme uporabi.

C.15.2. Podsystem ETCS na vlaku je tehnični sistem. Upošteva se naslednja funkcija: „*strojevodji se zagotovijo informacije, ki mu omogočajo varno upravljanje vlaka, v primeru prevelike hitrosti pa se uporabijo zavore*“.

Opis funkcije: na podlagi informacij s proge (dovoljena hitrost) in hitrosti na vlaku, ki jo izračuna podsystem ETCS na vlaku:

- (a) strojevodja upravlja vlak in zagotavlja, da hitrost vlaka ne presega dovoljene hitrosti;
- (b) hkrati podsystem ETCS na vlaku nadzoruje vlak, da nikoli ne preseže omejitve hitrosti. Če je hitrost prevelika, samodejno zavira.

Strojevodja in podsystem ETCS na vlaku uporabljata oceno hitrosti vlaka, ki jo izračuna podsystem ETCS na vlaku.

C.15.3. Vprašanje: „Ali se merilo za sprejemljivost tveganja za tehnične sisteme uporablja za oceno hitrosti vlaka, ki jo izvede podsystem na vlaku?“

C.15.4. Uporaba shematskega prikaza na Slika 14 in odgovori na različna vprašanja:

(a) zadevna nevarnost za tehnični sistem:

„*prekoračitev varne hitrosti, kot se priporoča za ETCS*“ (glej UNISIG SUBSET 091);

(b) ali se nevarnost lahko nadzoruje s kodeksom ravnanja ali referenčnim sistemom?

NE. Predpostavlja se, da je sistem ETCS novo in inovativno projektiranje. Zato ne obstajajo kodeksi ravnanja ali referenčni sistemi, ki lahko omogočijo nadzor nevarnosti na sprejemljivi stopnji tveganja;

(c) ali je katastrofalna posledica verjeten rezultat nevarnosti?

DA, ker lahko „prekoračitev varne hitrosti, kot se priporoča za ETCS,“ povzroči iztirjenje vlaka, ki bi lahko imelo za posledico „smrtne žrtve in/ali več resnih poškodb in/ali veliko škodo za okolje“;

(d) ali je katastrofalna posledica neposreden rezultat okvare tehničnega sistema?

DA, če ni dodatnih varnostnih pregrad. Enaka ocena hitrosti vlaka, kot jo izračuna podsistem ETCS na vlaku, se zagotovi strojevodji in funkciji za nadzor nad zavorami podsistema ETCS na vlaku. Če torej predpostavljamo, da strojevodja upravlja vlak (zaradi učinkovitosti) pri najvišji hitrosti, ki je dovoljena ob progih, niti strojevodja niti podsistem ETCS na vlaku ne bosta zaznala, da je vlak prekoračil hitrost v primeru prenizko ocenjene hitrosti vlaka. To lahko povzroči iztirjenje vlaka s katastrofalnimi posledicami;

(e) sklepi:

(1) v zvezi s kvantitativnimi zahtevami: uporabi se dopustna stopnja nevarnosti 10^{-9} h^{-1} za naključne okvare strojne opreme podsistema ETCS na vlaku, kar zagotavlja, da:

- (i) se pri ovrednotenju tega kvantitativnega cilja za redundančne sisteme upoštevajo skupne komponente (npr. posamezni ali skupni vnosi za vse kanale, skupno napajanje, komparatorji, naprave za izbiranje itd.);
- (ii) se zajame čas zaznavanja skritih ali neodkritih okvar;
- (iii) se opravi analiza okvare s skupnim vzrokom/načinom;
- (iv) se izvede neodvisna ocena;

(2) v zvezi z zahtevami postopka: za upravljanje sistematičnih okvar/napak podsistema ETCS na vlaku se uporabi postopek stopnje 4 varnostne integritete. To zahteva uporabo:

- (i) postopka vodenja kakovosti, ki je skladen s stopnjo 4 varnostne integritete;
- (ii) postopka varnega upravljanja, ki je skladen s stopnjo 4 varnostne integritete;
- (iii) ustreznih standardov, npr.:

- ↪ uporabo standarda EN 50128 za razvoj programske opreme;
- ↪ uporabo standardov EN 50121-3-2, EN 50121-4, EN 50124-1, EN 50124-2, EN 50125-1 EN 50125-3, EN 5050081, EN 50155, EN 61000-6-2 itd. za razvoj strojne opreme;

(3) neodvisna ocena postopka(-ov).

C.16. Primeri mogočih struktur evidence nevarnosti

C.16.1. Uvod

C.16.1.1. Minimalne zahteve, ki jih je treba evidentirati v evidenci nevarnosti, so opredeljene v oddelku 4.1.2. Uredbe o skupni varnostni metodi. Te so v primerih evidenc nevarnosti v nadaljevanju navedene v obarvanih poljih.

C.16.1.2. Obstajajo lahko različni načini strukturiranja evidence nevarnosti ter kakršnih koli dodatnih informacij, ki bi lahko opredelile nevarnosti in z njimi povezane varnostne ukrepe. V zvezi z nevarnostmi in z njimi povezanimi varnostnimi ukrepi se lahko na primer za posamezno informacijo izpolni eno polje. Vendar je za vse uporabljene strukture pomembno, da evidenca nevarnosti zagotavlja jasne povezave med nevarnostmi in z njimi povezanimi varnostnimi ukrepi. Ena od mogočih rešitev je, da evidenca nevarnosti za vsako nevarnost in za vsak varnostni ukrep vsebuje vsaj polje z:



- (a) jasnim opisom, vključno z navedbo izvora in načela sprejemljivosti tveganja, ki se izbere za nadzor s tem povezane nevarnosti. To polje omogoča razumevanje nevarnosti in z njo povezanih varnostnih ukrepov ter poznavanje, v katerih analizah varnosti so opredeljeni.

Ker se evidenca nevarnosti uporablja in vzdržuje v celotnem življenjskem ciklu sistema (tj. med delovanjem in vzdrževanjem sistema), je koristna jasna sledljivost ali povezava med vsako nevarnostjo in:

- (1) z njo povezanim tveganjem;
- (2) vzroki nevarnosti, kadar so že opredeljeni;
- (3) z njo povezanimi varnostnimi ukrepi in predpostavkami, ki opredeljujejo meje ocenjevanega sistema;
- (4) z njo povezanimi analizami varnosti, kadar je nevarnost opredeljena.

Poleg tega mora biti besedilo v zvezi z varnostnimi ukrepi (zlasti za tiste, ki se prenesejo na druge udeležence, kot je predlagatelj) ter s tem povezanimi nevarnostmi in tveganji jasno ter zadostno. „Jasno in zadostno“ pomeni, da se lahko razume, katera tveganja morajo varnostni ukrepi in z njimi povezane nevarnosti nadzorovati, brez da bi bilo treba ponovno uporabiti s tem povezane analize varnosti.

- (b) načelom sprejemljivosti tveganja, ki se uporablja za nadzor nevarnosti, da se podpre vzajemno priznavanje in se ocenjevalnemu organu pomaga oceniti pravilno uporabo skupne varnostne metode;

- (c) jasnimi informacijami o njegovem stanju: v tem polju je navedeno, ali je zadevna nevarnost/varnostni ukrep še vedno odprt ali pod nadzorom/potrjen;

- (1) odprta nevarnost/varnostni ukrep se spremlja, dokler ni pod nadzorom/potrjen(-a);
- (2) obratno se nadzorovane/potrjene nevarnosti/varnostni ukrepi ne spremljajo več, razen če se pojavijo pomembne spremembe pri delovanju ali vzdrževanju sistema: glej točko [G 6](b) oddelka 2.1.1. V tem primeru:
 - (i) se v skladu s Člen 2 za zahtevane spremembe ponovno uporabi skupna varnostna metoda. Glej tudi točko [G 6](b)(1) oddelka 2.1.1.;
 - (ii) se vse nadzorovane nevarnosti in varnostni ukrepi ponovno preučijo, da se preveri, ali spremembe ne vplivajo nanje. Če nanje vplivajo, se zadevne nevarnosti in z njimi povezani varnostni ukrepi v evidenci nevarnosti ponovno odprejo in upravljajo.

Lahko se zgodi, da se namesto varnostnih ukrepov, ki so evidentirani v evidenci nevarnosti, izvajajo drugačni varnostni ukrepi (npr. zaradi stroškov). Varnostni ukrepi, ki se izvajajo, se nato evidentirajo v evidenci nevarnosti z dokazom/utemeljitvijo, zakaj so ustrezni, ter dokazom, da je sistem s temi ukrepi skladen z varnostnimi zahtevami;

- (d) sklicem na s tem povezane dokaze, ki nadzorujejo nevarnost ali potrjujejo varnostni ukrep. To polje omogoča, da se pozneje lahko poiščejo dokazi, ki so omogočili nadzorovanje nevarnosti in potrditev s tem povezanega(-ih) varnostnega(-ih) ukrepa(-ov).

Nevarnost se lahko nadzoruje v evidenci nevarnosti le, kadar se vsi s tem povezani varnostni ukrepi v zvezi z nevarnostjo predhodno potrdijo;

- (e) organizacijo(-ami) ali podjetjem(-i), ki je (so) pristojno(-a) za njegovo upravljanje.

C.16.1.3. Drug primer mogoče vsebine evidence nevarnosti je naveden v Dodatku A.3. smernice EN 50126-2 {Ref. 9}.



C.16.2. Primer evidence nevarnosti za organizacijsko spremembo iz oddelka C.5. Dodatka C
Tabela 2: Primer evidence nevarnosti za organizacijsko spremembo iz oddelka C.5. Dodatka C.

Opis nevarnosti	Varnostni ukrepi	Prednost/nat ančnost varnosti	Izvajanje ⁽¹⁶⁾	Opombe	Odgovornost ¹⁸	Izvor	Uporabljeno načelo sprejemljivo sti tveganja	Odgovorno st za preverjanje	Način preverjanja	Status xx.xx.xx
Manjša motiviranost zaposlenih, ki ostanejo v družbi. Osebe zato še naprej zapuščajo družbo. Nemotivirani/izčrpani vodilni delavci	Nov krog motiviranja osebja, ki se izvaja v manjših skupinah. Prerazporeditev sredstev, da lahko družba izvaja pomembne naloge. Upravljalavec tirov pogosteje izvaja inšpekcijske preglede. Razporeditev sredstev za zagotovitev, da ključno osebje ostane do konca postopka. Posebna pozornost se nameni zagotovitvi, da se informacije in znanje prenesejo z odhajajočih zaposlenih na tiste, ki bodo prevzeli naloge. ltd.	Visoka/visoka	Usklajuje XYZ. Regije morajo obravnavati ukrepe, da se poveča nadzor nad tiri, prekrivanje zaposlenih in spremljanje s strani upravljalavca tirov.	Povečanje inšpekcijskih pregledov je treba vključiti v pogodbe. ltd.	Direktor družbe	Zbiranje zamisli. Poročilo o opredelitvi nevarnosti R _x .	Ni podatkov			Sprememba pogojev v zvezi z razmerami je pomembno zmanjšala to tveganje. Izvedba analize delovnega okolja in nekaj usposabljanja osebja.
Podizvajalci podjetnikov imajo premalo znanja, so premalo usposobljeni in slabo nadzirajo kakovost.	Večje povpraševanje po dokumentirani usposobljenosti. Sistematičen nadzor nad izvedenimi nalogami.	Visoka/srednja	Usklajevati mora upravljalavec železniške infrastrukture. Regije morajo izvajati ukrepe, s katerimi se zahtevata usposobljenost in nadzor dela.	Izvaja se s spremljanjem pogodbe. Vnos v načrtovanje pregleda.	Upravljalavec železniške infrastrukture	Zbiranje zamisli. Poročilo o opredelitvi nevarnosti R _x .	Ni podatkov	Oseba, pristojna za varnost		Večja osredotočenost na dejavnosti za nadzor (dva operativna nadzora na mesec in operativno področje).
Negotovost v zvezi	Opredelitev vlog in odgovornosti.	Srednja/sredn	V vsaki regiji	Izvajanje s	Regionalni	Zbiranje	Ni podatkov	Upravljalavec		Regije so

(16) Ta dva stolpca sta povezana z informacijami/poljem o udeležencih, ki so pristojni za nadzorovanje opredeljenih nevarnosti.

Tabela 2: Primer evidence nevarnosti za organizacijsko spremembo iz oddelka C.5. Dodatka C.

Opis nevarnosti	Varnostni ukrepi	Prednost/nat ančnost varnosti	Izvajanje ⁽¹⁶⁾	Opombe	Odgovorn ost ¹⁸	Izvor	Uporabljeno načelo sprejemljivo sti tveganja	Odgovorno st za preverjanje	Način preverja nja	Status xx.xx.xx
z vlogami in odgovornostmi pri vmesniku med družbo in upravljavcem železniške infrastrukture (upravljavcem tirov).	Določitev vseh vmesnikov in opredelitev tistih, ki so zanje odgovorni.	ja	posebej.	pogodbo o vzdrževanju in strateškem načrtom za preoblikovanje.	direktorji.	zamisli. Poročilo o opredelitvi nevarnosti R _x .		varnosti		predstavile svojo strategijo.

C.16.3. Primer popolne evidence nevarnosti za podsistem upravljanja - vodenja na vozilu

C.16.3.1. V tem oddelku je v primeru navedena ena evidenca nevarnosti (glej točko [G 3] oddelka 4.1.1.) za upravljanje:

- vseh notranjih varnostnih zahtev, ki veljajo za podsistem, za katerega je odgovoren udeleženec, in
- vseh opredeljenih nevarnosti ter z njimi povezanih varnostnih ukrepov, ki jih udeleženec ne more izvajati in jih je treba prenesti na druge udeležence.

Tabela 7: Primer evidence nevarnosti proizvajalca za podsistem upravljanja - vodenja na vlaku

Št. nevarnosti	Izvor	Opis nevarnosti	Dodatne informacije	Pristojni udeleženec	Varnostni ukrep	Uporabljeno načelo sprejemljivo sti tveganja	Izvožena	Status
1	Poročilo HAZOP R _x	Najvišja hitrost vlaka je previsoka (V _{max}).	Napačna posebna konfiguracija podsistema na vlaku (osebje za vzdrževanje). Napačen vnos podatkov na vlaku (strojevodja).	Prevoznik v železniškem prometu	<ul style="list-style-type: none"> Opredelitev postopka za odobritev podatkov za konfiguracijo podsistema na vlaku; opredelitev operativnega postopka za postopek vnosa podatkov, ki ga izvede 	Eksplisitna ocena tveganja	Da	Pod nadzorom (izvožena k prevozniku v železniškem prometu). Glej tudi oddelek C.16.4.2.

Tabela 7: Primer evidence nevarnosti proizvajalca za podsistem upravljanja - vodenja na vlaku

Št. nevarnosti	Izvor	Opis nevarnosti	Dodatne informacije	Pristojni udeleženeec	Varnostni ukrep	Uporabljeno načelo sprejemljivo sti tveganja	Izvožena	Status
					strojevodja.			Dodatka C.
2	Poročilo HAZOP R _x	Zavorne krivulje (tj. dovoljenje za vožnjo) v podatkih za konfiguracijo podsistema na vlaku so premalo stroge.	Postopek za posebno konfiguracijo podsistema na vlaku je odvisen od: <ul style="list-style-type: none"> • mej varnosti za zavorni sistem vlaka; • zamude pri odzivu zavornega sistema vlaka (to je neposredno odvisno od dolžine vlaka, zlasti pri tovornih vlakih). 	Prevoznik v železniškem prometu	<ul style="list-style-type: none"> • Pravilna določitev zahtev sistema v opredelitvi sistema; • določitev zadostnih mej varnosti za zavorni sistem posameznega vlaka. 	Eksplicitna ocena tveganja	Da	Pod nadzorom (izvožena k prevozniku v železniškem prometu). Glej tudi oddelek C.16.4.2. Dodatka C.
3	Poročilo HAZOP R _x	<ul style="list-style-type: none"> • Najvišja hitrost vlaka je previsoka (V_{max}). • Zavorne krivulje (tj. dovoljenje za vožnjo) v podatkih za konfiguracijo podsistema na vlaku so premalo stroge. 	Posodobitev premera koles vlaka v posebni konfiguraciji podsistema na vlaku ni uspešna (osebje za vzdrževanje).	Prevoznik v železniškem prometu	<ul style="list-style-type: none"> • Opredelitev postopka za izmero premera kolesa vlaka, ki jo izvede osebje za vzdrževanje; • Opredelitev postopka za redno posodabljanje premera kolesa vlaka v podsistemu na vlaku. 	Eksplicitna ocena tveganja	Da	Pod nadzorom (izvožena k prevozniku v železniškem prometu). Glej tudi oddelek C.16.4.2. Dodatka C.
			Postopek proizvajalca za pripravo in prenos podatkov za konfiguracijo v podsistem na vlaku ni uspešen.	Proizvajalec	Opredelitev postopka za posodabljanje premera kolesa vlaka v podatkih za konfiguracijo na vlaku.	Eksplicitna ocena tveganja	Da	Pod nadzorom s postopkom P _x
4	Poročilo HAZOP R _x	Vlak pri visoki hitrosti (160 km/h, če je ob progi signal za prosto) zapelje na tire brez aktivnega podsistema na vlaku in brez signalizacije ob progi.	Nadzoruje se lahko le s pozornostjo strojevodje. Prihod na območje ob progi, ki je opremljeno z ATP, je odvisen od postopka potrditve strojevodje pred menjavo lokacije. Če potrditve ni, podsistem upravljanja - vodenja na vlaku samodejno zavira.	Upravljavac železniške infrastrukture	Upravljavac železniške infrastrukture zagotovi, da vlaki, ki niso opremljeni s podsistemom aktivnega upravljanja - vodenja na vlaku, ne zapeljejo na zadeven tir.	Eksplicitna ocena tveganja	Da	Pod nadzorom (izvožena k upravljavcu železniške infrastrukture). Glej tudi oddelek C.16.4.2. Dodatka C.
				Prevoznik v železniškem prometu	Zagotovitev usposabljanja strojevodje za vstop na območje ob progi, ki je opremljeno z ATP.	Eksplicitna ocena tveganja	Da	Pod nadzorom (izvožena k prevozniku v železniškem prometu). Glej tudi oddelek C.16.4.2. Dodatka C.
5	Poročilo	Najvišja hitrost vlaka,	Informacije, prikazane na vmesniku strojevodja, se	Proizvajalec	Razvoj podsistema upravljanja -	Eksplicitna	Da	Varnostna analiza

Tabela 7: Primer evidence nevarnosti proizvajalca za podsistem upravljanja - vodenja na vlaku

Št. nevarnosti	Izvor	Opis nevarnosti	Dodatne informacije	Pristojni udeleženeec	Varnostni ukrep	Uporabljeno načelo sprejemljivo sti tveganja	Izvožena	Status
	HAZOP R _x	dokazana strojevodji, je previsoka (V _{max}).	spremljajo s podsistemom upravljanja - vodenja s stopnjo 4 varnostne integritete, ki v primeru neskladnosti med ugotovljeno in pričakovano vrednostjo uporabi zasilne zavore. V primeru neskladnosti z dovoljenjem za vožnjo podsistem upravljanja - vodenja na vlaku uporabi zasilne zavore.		vodenja na vlaku s stopnjo 4 varnostne integritete.	ocena tveganja		prikazuje podsistem s stopnjo 4 varnostne integritete, ki ga oceni neodvisni ocenjevalec varnosti.
6	Poročilo HAZOP R _x	Vlak se odpelje brez vmesnika strojevodja-stroj.	Izguba redundančne arhitekture podsistema na vlaku.	Proizvajalec	Razvoj podsistema upravljanja - vodenja na vlaku s stopnjo 4 varnostne integritete.	Eksplicitna ocena tveganja	Da	Varnostna analiza prikazuje podsistem s stopnjo 4 varnostne integritete, ki ga oceni neodvisni ocenjevalec varnosti.
ltd.								

C.16.4. Primer evidence nevarnosti za prenos informacij drugim udeležencem

C.16.4.1. V tem oddelku je v primeru navedena evidenca nevarnosti za prenos opredeljenih nevarnosti in z njimi povezanih varnostnih ukrepov, ki jih zadevni udeleženeec ne more izvajati, drugim udeležencem. Glej točko [G 1] oddelka 4.1.1.

Ta primer je enak kot primer v oddelku C.16.3. Dodatka C. Edina razlika je, da so izločene vse notranje nevarnosti in varnostni ukrepi, ki bi jih lahko nadzoroval zadevni udeleženeec.

C.16.4.2. Zadnji stolpec Tabela 3 se uporabi za izpolnjevanje zahteve iz oddelka 4.2. Uredbe o skupni varnostni metodi. Za to obstajajo različne rešitve. En način je sklicevanje na dokaz, ki ga uporabi udeleženeec, ki prejme izvožene varnostne informacije. Drug način je lahko sestanek dveh udeležencev, da skupaj poiščeta primerno rešitev za nadzorovanje s tem povezanega(-nih) tveganja (tveganj). Rezultati takšnega sestanka se lahko sporočijo v dogovorjenem dokumentu (na primer zapisniku sestanka), na katerega se lahko sklicuje udeleženeec, ki izvažata informacije v zvezi z varnostjo, da zapre s tem povezane nevarnosti v evidenci nevarnosti.

Tabela 3: Primer evidence nevarnosti za prenos informacij v zvezi z varnostjo drugim udeležencem

Št. nevarnosti	Izvor nevarnosti		Opis nevarnosti	Dodatne informacije	Pristojni udeleženec	Varnostni ukrep	Pripomba prejemnika
	Št. v tabeli 7)	Drugo					
1	Št.°1	Poročilo HAZOP R _x	Najvišja hitrost vlaka je previsoka (V _{max}).	Napačna posebna konfiguracija podsistema na vlaku (osebje za vzdrževanje). Napačen vnos podatkov na vlaku (strojevodja).	Prevoznik v železniškem prometu	<ul style="list-style-type: none"> Opredelitev postopka za odobritev podatkov za konfiguracijo podsistema na vlaku; opredelitev operativnega postopka za postopek vnosa podatkov, ki ga izvede strojevodja. 	<ul style="list-style-type: none"> Podatki za konfiguracijo podsistema upravljanja - vodenja na vlaku so odvisni od fizičnih lastnosti tirnega vozila. Meje varnosti se nato uporabijo za te podatke pri usklajevanju upravljavca železniške infrastrukture in prevoznika v železniškem prometu. Podatki se nato prenesejo v podsistem na vlaku v skladu s primernim postopkom proizvajalca med namestitvijo, vključitvijo v tirno vozilo in sprejetjem podsistema upravljanja - vodenja. Strojvodje se usposobijo in ocenijo po postopku D_p. Strojvodje oceni tudi upravitelj železniške infrastrukture, in sicer po pravilih, ki veljajo za infrastrukturo upravljavca železniške infrastrukture.
2	Št.°2	Poročilo HAZOP R _x	Zavorne krivulje (tj. dovoljenje za vožnjo) v podatkih za konfiguracijo podsistema na vlaku so premalo stroge.	Postopek za posebno konfiguracijo podsistema na vlaku je odvisen od: <ul style="list-style-type: none"> mej varnosti za zavorni sistem vlaka; zamude pri odzivu zavornega sistema vlaka (to je neposredno odvisno od dolžine vlaka, zlasti pri tovornih vlakih). 	Prevoznik v železniškem prometu	<ul style="list-style-type: none"> Pravilna določitev zahtev sistema v opredelitvi sistema; določitev zadostnih mej varnosti za zavorni sistem posameznega vlaka. 	Glej pripombo v vrstici 1 zgoraj.
3	Št.°3	Poročilo HAZOP R _x	<ul style="list-style-type: none"> Najvišja hitrost vlaka je previsoka (V_{max}). Zavorne krivulje (tj. dovoljenje za vožnjo) v podatkih za konfiguracijo podsistema na vlaku so premalo stroge. 	Posodobitev premera koles vlaka v posebni konfiguraciji podsistema na vlaku ni uspešna (osebje za vzdrževanje).	Prevoznik v železniškem prometu	<ul style="list-style-type: none"> Opredelitev postopka za izmero premera kolesa vlaka, ki jo izvede osebje za vzdrževanje; Opredelitev postopka za redno posodabljanje premera kolesa vlaka v podsistemu na vlaku. 	<ul style="list-style-type: none"> Vzdrževanje podsistema upravljanja - vodenja na vlaku se izvaja v skladu s „postopkom vzdrževanja MP_Z“. Premer kolesa vlaka se posodablja v določenih intervalih v skladu s postopkom P_W. Strojvodje se za postopek vnosa podatkov usposablja in ocenijo po „postopku P_{DE}“.
4	Št.°4	Poročilo HAZOP R _x	Vlak pri visoki hitrosti (160 km/h, če je ob progi signal za prosto) zapelje na tire brez aktivnega podsistema na vlaku	Nadzoruje se lahko le s pozornostjo strojevodje. Prihod na območje ob progi, ki je opremljeno z ATP, je odvisen od postopka potrditve strojevodje pred menjavo lokacije. Če	Upravitelj železniške infrastrukture	Upravitelj železniške infrastrukture zagotovi, da vlaki, ki niso opremljeni s podsistemom aktivnega upravljanja - vodenja na vlaku, ne zapeljejo na zadeven tir.	Promet na infrastrukturi upravljavca železniške infrastrukture se upravlja na podlagi sklopa pravil R _{TM} .

Tabela 3: Primer evidence nevarnosti za prenos informacij v zvezi z varnostjo drugim udeležencem

Št. nevarnosti	Izvor nevarnosti		Opis nevarnosti	Dodatne informacije	Pristojni udeleženec	Varnostni ukrep	Pripomba prejemnika
	Št. v tabeli 7).	Drugo					
			in brez signalizacije ob progi.	potrditve ni, podsistem upravljanja - vodenja na vlaku samodejno zavira.		Opredelitev postopka za upravljanje prometa.	
					Prevoznik v železniškem prometu	Zagotovitev usposabljanja strojevodje za vstop na območje ob progi, ki je opremljeno z ATP.	<ul style="list-style-type: none"> • Strojvodje se redno usposabljuje v skladu s postopkom upravljavca železniške infrastrukture P_{IM_DP}. • Strojvodje oceni tudi upravljavec železniške infrastrukture, in sicer v skladu s pravili (S_R), ki veljajo za infrastrukturo upravljavca železniške infrastrukture.
itd.							

C.17. Primer splošnega seznama nevarnosti za delovanje železnice

C.17.1. ROSA (analiza varnosti za optimizacijo železnice) je projekt v okviru DEUFRAKO (francosko-nemškega sodelovanja), ki je poskušal sestaviti splošen in celovit seznam nevarnosti, ki bi zajemal standardno delovanje železnice. Cilj in izziv je bil te nevarnosti čim podrobneje opredeliti, medtem ko ne bi izražale posebnosti francoskih in nemških železnic. Seznam je bil sestavljen z uporabo takrat veljavnih seznamov nevarnosti iz obeh držav (SNCF in DB), navzkrižno pa se je preverjal s seznamami nevarnosti iz drugih držav. Kljub izraženemu cilju glede celovitosti in splošnosti seznama je ta tukaj naveden le kot okvirni primer, ki je lahko v pomoč udeležencem, kadar morajo opredeliti nevarnosti za poseben projekt. Pričakuje se, da bo nevarnosti, navedene na tem seznamu, verjetno treba izboljšati ali dopolniti, da bodo izražale vse posebnosti projekta.

C.17.2. Nevarnosti v osnutku seznama spodaj so „začetne nevarnosti“ (starting point hazards – SPH), tj. nevarnosti, iz katerih je mogoče izpeljati analizo posledic in vzročno analizo, da se določijo varnostni ukrepi/pregrade ter varnostne zahteve za nadzorovanje nevarnosti.

C.17.3. Seznam nevarnosti iz projekta ROSA:

SPH 01	Začetna napačna določitev omejitve hitrosti (v zvezi z infrastrukturo)
SPH 02	Napačna določitev omejitve hitrosti (v zvezi z vlakom)
SPH 03	Napačna določena zavorna razdalja/napačen profil hitrosti/napačne zavorne krivulje
SPH 04	Nezadostno zmanjševanje hitrosti (fizični vzroki)
SPH 05	Napačna/neprimerna hitrost/zavorni ukaz
SPH 06	Napačna evidentirana hitrost (napačna hitrost vlaka)
SPH 07	Napaka pri sporočanju omejitve hitrosti
SPH 08	Nehoteno premikanje vlaka
SPH 09	Napačna smer vožnje/hoteno vzvratno premikanje – (kombinacija začetnih nevarnosti SPH 08 in SPH 14)
SPH 10	Napačen evidentiran absoluten/relativen položaj
SPH 11	Napaka pri zaznavanju vlakov
SPH 12	Vlak ni celovit
SPH 13	Morebitna napačna proga za vlak
SPH 14	Napaka pri prenosu/sporočanju voznega reda/dovoljenja za vožnjo
SPH 15	Strukturna okvara vozne poti
SPH 16	Okvara komponente kretnic
SPH 17	Napačen ukaz v zvezi s kretnico
SPH 18	Napačno stanje kretnice
SPH 19	Predmet sistema na vozni poti/v ovojnici prostega prostora (razen v gramozni gredi)
SPH 20	Tuj predmet na vozni poti/v ovojnici prostega prostora

SPH 21	Udeleženelec v cestnem prometu na nivojskem prehodu
SPH 22	Učinki upora zraka na gramozno gred
SPH 23	Vpliv aerodinamičnih sil na vlak
SPH 24	Oprema vlaka/element/obremenitev presega ovojnico prostega prostora vlaka
SPH 25	Nepriprava velikost ovojnice prostega prostora vlaka (ob progi)
SPH 26	Napačna porazdelitev obremenitve
SPH 27	Okvara kolesa, okvara osi
SPH 28	Vročni osni/kolesni ležaji
SPH 29	Okvara podstavnega vozička/vzmetenja, dušenje
SPH 30	Okvara okvirja vozila/nadgradnje
SPH 31	Nepooblaščen prehod (z vidika varnosti)
SPH 32	Tire prečka pooblaščen osebje
SPH 33	Osebe dela na progi
SPH 34	Poseganje nepooblaščen osebje na tire (malomarnost)
SPH 35	Padec osebe z roba perona na tir
SPH 36	Upor zraka/osebje preblizu roba perona
SPH 37	Osebe dela blizu tira, npr. na sosednjem tiru
SPH 38	Oseba namerno zapusti vlak (razen pri izmenjavi potnikov)
SPH 39	Oseba pade skozi vrata (na strani)
SPH 40	Oseba pade skozi vrata v končni steni
SPH 41	Vlak se odpelje/nehoteno premakne z odprtimi vrati (ni kršenja ovojnice prostega prostora)
SPH 42	Padec osebe v prehodu med dva vagona
SPH 43	Potnik se nagne skozi vrata
SPH 44	Potnik se nagne skozi okno
SPH 45	Osebe/sprevodnik se nagne skozi vrata
SPH 46	Osebe/sprevodnik se nagne skozi okno
SPH 47	Ranžirno osebje na vozilu se nagne s stopnice
SPH 48	Oseba pade/spleza s perona na vrzel med vozilom in peronom
SPH 49	Oseba pade z vlaka/zapusti vlak, kjer ni perona
SPH 50	Padec osebe na območju vrat pri izmenjavi potnikov
SPH 51	Vrata vlaka se zaprejo, medtem ko je oseba na območju vrat
SPH 52	Vlak se premakne med izmenjavo potnikov
SPH 53	Možnost, da se oseba na vlaku poškoduje
SPH 54	Nevarnost požara/eksplozije (na/ob vlaku) – razred nesreč, posledica začetnih nevarnosti SPH 55, SPH 56)
SPH 55	Nepriprava temperatura (na vlaku)
SPH 56	Zastrupitev/zadušitev (na/ob vlaku)
SPH 57	Smrt zaradi električnega toka (na/ob vlaku)
SPH 58	Padec osebe na peron (razen pri izmenjavi potnikov)
SPH 59	Nepriprava temperatura (na peronu)
SPH 60	Zastrupitev/zadušitev (na peronu)
SPH 61	Smrt zaradi električnega toka (na peronu)