

Labāka dzelzceļa sistēma
sabiedrībai

Rokasgrāmata

Drošības pārvaldības sistēmas prasības drošības sertifikāta vai drošības atļaujas saņemšanai

	<i>Izstrādāja</i>	<i>Ratificēja</i>	<i>Apstiprināja</i>
<i>Vārds, uzvārds</i>	S. D'ALBERTANSON	M. SCHITTEKATTE	C. CARR
<i>Amats</i>	Projekta koordinators	Projekta vadītājs	Nodaļas vadītājs
<i>Datums</i>	4.9.2018.	4.9.2018.	4.9.2018.
<i>Paraksts</i>			

Dokumenta vēsture

<i>Versija</i>	<i>Datums</i>	<i>Piebildes</i>
1.0.	29.6.2018.	Galīgā versija publicēšanai
1.1.	10.7.2018.	Atjaunināts 2. attēls, pievienots paraksta teksts 3. attēlam
1.2.	4.9.2018.	Atjaunināts 2. attēls

Šis dokuments ir juridiski nesaistoša Eiropas Dzelzceļu aģentūras rokasgrāmata. Tas neskar lēmumu pieņemšanas procesu, ko paredz ar piemērojamiem ES tiesību aktiem. Turklāt ES tiesību aktu saistoša interpretācija ir tikai Eiropas Savienības Tiesas kompetencē.

0 Ievads

Pieteikuma iesniedzējs, kurš vēlas saņemt vienoto drošības sertifikātu vai drošības atļauju, parāda atbilstību attiecīgajām drošības pārvaldības sistēmas prasībām, kas ir izklāstītas Komisijas Deleģētajā regulā (ES) 2018/762. Šajā nolūkā pieteikuma iesniedzējs iesniedz valsts drošības iestādei (VDI) vai — attiecīgā gadījumā — Eiropas Savienības Dzelzceļu aģentūrai (turpmāk tekstā arī “Aģentūra”) dokumentārus pierādījumus savas drošības pārvaldības sistēmas (SMS) izveidei atbilstoši Direktīvas (ES) 2016/798 9. pantam.

Šī rokasgrāmata ir pastāvīgi papildināma un izstrādāta sadarbībā ar valstu drošības iestādēm un nozaru pārstāvjiem, un to ir paredzēts nemitīgi pilnveidot, pamatojoties uz lietotāju atsauksmēm un ņemot vērā Direktīvas (ES) 2016/798, attiecīgo kopīgo drošības metožu (CSM) un jebkuru citu attiecīgo ES regulu īstenošanā gūto pieredzi.

0.1 Rokasgrāmatas mērķis

Šīs rokasgrāmatas mērķis ir sniegt:

- informāciju par mērķi katrai no novērtēšanas prasībām, kas izklāstītas iepriekš minēto CSM I un II pielikumā, vajadzības gadījumā izklāstu papildinot ar paskaidrojumiem, kuros iekļauta īpaša informācija par konkrētiem prasībās lietotiem terminiem vai idejām;
- norādi par to, kādus pierādījumus organizācija var iesniegt, lai parādītu iepriekš minētajās CSM prasīto atbilstību;
- tādu pierādījumu piemēru ilustratīvu uzskaitījumu, ko var novērot vienotā drošības sertifikāta vai drošības atļaujas pieteikumos, kad tiek veikts novērtējums, vai o pieteikuma iesniedzējs var izmantot kā atsauces materiālu sava pieteikuma sagatavošanai;
- ilustratīvas atsauces un standartus, ko var izmantot, novērtējot, izstrādājot, īstenojot vai pastāvīgi uzlabojot drošības pārvaldības sistēmu, un
- dažas norādes par to, kādi jautājumi varētu būt jāapsver valsts drošības iestādei, kad tā veic dzelzceļa pārvadājumu uzņēmuma vai infrastruktūras pārvaldītāja uzraudzību.

Piezīme. Lai novērtētu pieteikumu vienotā drošības sertifikāta saņemšanai saistībā ar bīstamo kravu pārvadāšanu pa dzelzceļu, valsts drošības iestāde (VDI) var tieši darboties kā kompetentā iestāde attiecīgo pieteikuma daļu novērtēšanā. Vai arī tā var uzņemties koordinatora funkciju un pēc vajadzības sadarboties ar jebkuru citu kompetento iestādi bīstamo kravu pārvadājumu jomā un lūgt tās padomu par attiecīgajām novērtējuma daļām.

0.2 Rokasgrāmatas adresāti

Šis dokuments ir paredzēts:

- valstu drošības iestādēm un Eiropas Savienības Dzelzceļu aģentūrai, lai palīdzētu tām novērtēt dzelzceļa pārvadājumu uzņēmumu drošības pārvaldības sistēmas atbilstību attiecīgajām SMS prasībām un palīdzētu VDI veikt uzraudzību;
- valstu drošības iestādēm, lai palīdzētu tām novērtēt infrastruktūras pārvaldītāju drošības pārvaldības sistēmas atbilstību attiecīgajām SMS prasībām un veikt uzraudzību pēc sertifikāta vai atļaujas piešķiršanas, un
- dzelzceļa pārvadājumu uzņēmumiem un infrastruktūras pārvaldītājiem (turpmāk tekstā arī “pieteikuma iesniedzējs”), lai tiem palīdzētu to drošības pārvaldības sistēmas izstrādē, īstenošanā, uzturēšanā un pastāvīgā uzlabošanā atbilstoši attiecīgajām SMS prasībām (un citām piemērojamām drošības prasībām) un lai tie zinātu, ko gaidīt uzraudzības laikā.

0.3 Piemērošanas joma

Šī rokasgrāmata neparedz, kādi pierādījumi pieteikuma iesniedzējam ir jāuzrāda. Galvenais iemesls, kāpēc tas netiek noteikts, ir tas, ka ikvienas organizācijas SMS ir jābūt pielāgotai konkrētajiem riskiem, kas organizācijai jākontrolē. Tas nozīmē, ka ikviena SMS ir unikāla dokumentētas informācijas sistēma, kas sniedz norādi par īpašajiem riska kontroles pasākumiem un sistēmām, kuras ir ieviestas individuālā organizācijā, un mainās līdz ar organizāciju. Tāpēc nebūtu korekti preskriptīvi uzskaitīt informāciju, kas pieteikuma iesniedzējam ir jāsniedz. Tas padarītu novērtēšanas procesu bezjēdzīgu, jo visi pieteikumi būtu vienādi, bet attiecīgās SMS atšķirtos.

0.4 Rokasgrāmatas struktūra

Šis dokuments ir to Aģentūras rokasgrāmatu krājuma daļa, kas izstrādātas, lai palīdzētu dzelzceļa pārvaldījumu uzņēmumiem, infrastruktūras pārvaldītājiem, valstu drošības iestādēm un Aģentūrai pildīt to pienākumus un uzdevumus atbilstoši Direktīvai (ES) 2016/798.



1. attēls. Aģentūras rokasgrāmatu krājums

Šajā rokasgrāmatā sniegto informāciju papildina ar īpašu valstu drošības iestāžu rokasgrāmatu, kurā izklāstīti un izskaidroti paziņotie valsts noteikumi, kas ir spēkā attiecībā uz paredzēto darbības telpu, un dokumenti, ko iekļauj vienotā drošības sertifikāta pieteikumā, lai izpildītu Direktīvas (ES) 2016/798 10. panta 3. punkta b) apakšpunkta un 10. panta 8. punkta noteikumus (sk. arī Aģentūras pieteikumu iesniegšanas rokasgrāmatu vienoto drošības sertifikātu izdošanai). Attiecībā uz infrastruktūras pārvaldītājiem šī rokasgrāmata ir jāpapildina ar valstu drošības iestāžu sagatavotiem norādījumiem par prasībām, ko piemēro drošības atļaujām, kā paredzēts Direktīvas (ES) 2016/798 12. panta 1. punktā.

Paziņotie valsts noteikumi ir tikai tie noteikumi, ko dalībvalsts ir paziņojusi Komisijai. Atbilstoši Direktīvas (ES) 2016/798 12. apsvērumam ir paredzams, ka paziņoto valsts noteikumu skaits laika gaitā samazināsies. Tie tiks aizstāti ar pasākumiem, kas izklāstīti savstarpējās izmantojamības tehniskajās specifikācijās (SITS), citās ES regulās vai uzņēmumu noteikumos. Uzņēmumu noteikumi vai standarti attiecīgā gadījumā tiks novērtēti, izvērtējot atbilstību SITS, kas attiecas uz Eiropas Savienības dzelzceļu tīkla satiksmes nodrošināšanas un vadības apakšsistēmu (turpmāk tekstā arī "SITS OPE"), kā to atspoguļo šajā rokasgrāmatā izskaidrotās drošības pārvaldības sistēmai piemērotās prasības.

Šī rokasgrāmata ir strukturēta atbilstoši prasībām, kas noteiktas Komisijas Deleģētās regulas (ES) 2018/762 I un II pielikumā. Nākamajās sadaļās katras prasības izklāsts uzskatāmības labad ir sniegts dzeltenā ierāmētā lodziņā. Ja dzelzceļa pārvadājumu uzņēmumiem un infrastruktūras pārvaldītājiem piemērojamās prasības atšķiras, attiecīgais teksts, kas attiecas uz infrastruktūras pārvaldītājiem, ir norādīts iekavās **zilā krāsā**.

Šīs rokasgrāmatas 1. pielikums.. pielikumā ir sniegts blakus salīdzinājums vai korelācijas tabulas starp iepriekšējās regulās, proti, (ES) Nr. 1158/2010 un (ES) Nr. 1169/2010, paredzētajiem novērtēšanas kritērijiem un Komisijas Deleģētajā regulā (ES) 2018/762 noteiktajiem kritērijiem. Tabulās attiecīgā gadījumā ir arī sniegtas mīļnorādes uz ISO augsta līmeņa struktūras noteikumiem. Tās ir norādītas, lai palīdzētu pieteikuma iesniedzējiem parādīt to drošības pārvaldības sistēmas atbilstību jaunajām prasībām, jo īpaši gadījumos, kad pieteikuma iesniedzējam jau ir piešķirts drošības sertifikāts vai drošības atļauja un/vai pieteikuma iesniedzējam jau ir ieviesta cita ISO pārvaldības sistēma (piemēram, ISO 9001, 14001 vai 45001) (lai tās var integrēt kopā) vai ir plāni izstrādāt sistēmu, izmantojot attiecīgo modeli. Šīs tabulas izmantošana nav uzskatāma par sistemātisku pieņemumu, ka ir nodrošināta atbilstība prasībām, kas Komisijas Deleģētajā regulā (ES) 2018/762 [CSM *attiecībā uz SMS*] noteiktas organizācijām, kurām ir ISO sertifikāts.

0.5 ISO/IEC direktīvu 1. daļa un konsolidēts ISO papildinājums

ISO ir izstrādājusi oficiālas procedūras, kas jāievēro, izstrādājot un uzturot spēkā starptautisku standartu. [ISO/IEC direktīvu 1. daļā un konsolidētā ISO papildinājuma](#) SL pielikuma 2. papildinājumā ir pieņemta augsta līmeņa struktūra (HLS) pamatteksa izmantošanai katrā pārvaldības sistēmas standartā.

Komisijas Deleģētās regulas (ES) 2018/762 I un II pielikums nodrošina struktūru, kas atbilst ISO HLS, attiecīgā gadījumā atvieglojot tādu dažādu pārvaldības sistēmu integrāciju, kurām ir vienādi organizatoriskie pamatprincipi un prasības, bet atbilstība tiesību aktiem un riska jomas ir specifiskas katrai disciplīnai (piemēram, drošība, vide, kvalitāte).

ISO standarti un attiecīgās rokasgrāmatas var noderēt dzelzceļa pārvadājumu uzņēmumiem un infrastruktūras pārvaldītājiem to SMS izstrādē (piemēram, ISO 31000 ir vispārīgs dokuments, ko var izmantot, lai labāk izprastu riska pārvaldību, ISO 31010 sniedz informāciju par riska novērtēšanas metožu, piemēram, FMECA, FTA, ETA, HAZOP, atlasī un piemērošanu, ISO 55000 nosaka prasības attiecībā uz aktīvu pārvaldību). Tomēr reālu ieguvumu no minētajiem standartiem un rokasgrāmatām var gūt tikai tad, ja ir ļoti labas zināšanas par kontekstu, kādā rodas ar dzelzceļu saistītie riski.

Ja HLS izmantošana nodrošina saskaņotību ar ISO pārvaldības sistēmu standartiem, ir jāuzsver, ka iepriekš minētās CSM ir noteikumi, kas galvenokārt paredzēti, lai valstu drošības iestādes vai Aģentūra tos izmantotu, novērtējot pieteikumus drošības sertifikātu vai drošības atļauju piešķiršanai. Principā novērtējumus par vienotajiem drošības sertifikātiem vai drošības atļaujām veic, pamatojoties uz prasībām, kas attiecas uz SMS, nevis ISO HLS. Proti, ISO standartu pamatā ir brīvprātīga sertifikācija, bet daži tiesiskie regulējumi nosaka, ka tiem jārada pieņemums par atbilstību piemērojamiem noteikumiem, kas reglamentē konkrētu jomu. Nav noteikuma, ar ko paredz, ka ISO standartiem ir jārada pieņemums par atbilstību prasībām, kas ietvertas Direktīvā (ES) 2016/798, vai Komisijas Deleģētajai regulai (ES) 2018/762.

4.–10.2. noteikumi, kas ņemti no ISO/IEC direktīvu 1. daļas un 2016. gada konsolidētā papildinājuma SL pielikuma 2. papildinājuma, ir reproducēti vai pielāgoti ar Starptautiskās Standartizācijas organizācijas

(ISO) atļauju. Oriģinālo tekstu skatīt avota dokumentā. Dokuments ir pieejams [ISO Centrālā sekretariāta tīmekļa vietnē](#). Autortiesības pieder ISO.

0.6 Drošības pārvaldības sistēmas mērķis

SMS mērķis ir nodrošināt, ka organizācija droši kontrolē riskus, kas izriet no tās darbības mērķiem, un izpilda visus tai piemērojamos pienākumus drošības jomā.

Strukturētas pieejas pieņemšana sniedz iespēju apzināt apdraudējumus un pastāvīgi pārvaldīt riskus saistībā ar organizācijas darbībām, lai novērstu negadījumus. Šajā pieejā ņem vērā riska dalīšanu jomās, kur notiek mijiedarbība ar citiem dzelzceļa sistēmas dalībniekiem (galvenokārt dzelzceļa pārvadājumu uzņēmumiem, infrastruktūras pārvaldītājiem un par tehnisko apkopi atbildīgajām struktūrām, kā arī jebkuriem citiem dalībniekiem, kuri var ietekmēt dzelzceļa sistēmas ekspluatācijas drošību, piemēram, ražotājiem, remonta uzņēmumiem, vagonu turētājiem, pakalpojumu sniedzējiem, darbuzņēmējiem, pārvadātājiem, nosūtītājiem, saņēmējiem, iekrāvējiem, izkrāvējiem, mācību centriem, kā arī pasažieriem un citām personām, kuras mijiedarbojas ar dzelzceļa sistēmu, u. tml.). Visu SMS attiecīgo elementu pienācīga īstenošana var nodrošināt organizācijai vajadzīgo pārliecību, ka tā kontrolē un turpinās kontrolēt visus ar tās darbībām saistītos riskus jebkuros apstākļos.

Nobriedušas organizācijas atzīst, ka efektīvu riska kontroli var panākt tikai ar procesu, kurā ir apvienotas trīs kritiskas dimensijas, proti, tehniskais komponents ar izmantotajiem instrumentiem un aprīkojumu, cilvēka komponents, ko veido vadošie cilvēki ar savām prasmēm, apmācību un motivāciju, un organizatoriskais komponents, kas sastāv no procedūrām un metodēm, kuras nosaka uzdevumu savstarpējo saistību.

Attiecīgi pienācīga SMS var sekmīgi pārraudzīt un uzlabot visas trīs tās riska kontroles pasākumu dimensijas. Daudzas dzelzceļa SMS iezīmes ir ļoti līdzīgas pārvaldības praksei, ko atbalsta kvalitātes, darba aizsardzības, vides aizsardzības un uzņēmējdarbības izcilības veicinātāji. Tāpēc labas pārvaldības principus var vieglāk integrēt, kā minēts iepriekš, izmantojot CSM, kuras pamatā ir ISO HLS, un tādējādi ir iespējams izvairīties no vajadzības pilnīgi pārstrukturēt organizācijas, kas jau ir ieviesušas minētās sistēmas.

Ir atzīts, ka strukturētas pārvaldības sistēmas piešķir uzņēmējdarbībai pievienoto vērtību, ko panāk, efektīvi pārvaldot saskarnes. Tas palīdz uzlabot vispārējos rezultātus, panākt darbības efektivitātes uzlabojumus, uzlabot attiecības ar darbuzņēmējiem un apakšuzņēmējiem, klientiem un regulatīvajām iestādēm, kā arī palīdz veidot pozitīvu drošības kultūru.

Pieteikuma iesniedzējam sava SMS jāizstrādā tā, lai tā atbilstu Direktīvas (ES) 2016/798 9. pantā noteiktajām prasībām un nodrošinātu tā darbību drošu pārvaldību. Šajā nolūkā pieteikuma iesniedzējam jāparāda atbilstība CSM attiecībā uz SMS I un II pielikuma prasībām. Šīs prasības ir strukturētas tā, lai sniegtu pilnīgu priekšstatu par organizācijas drošības pārvaldības sistēmu atbilstoši ciklam “plāno–dari–pārbaudi–rīkojies” (PDPR). Pieteikuma iesniedzējam ir jāapsver katra atsevišķa prasība, kā arī tas, kā prasības sader kopā, veidojot saskaņotu SMS, kas kontrolē attiecīgos riskus.

0.7 Drošības pārvaldības sistēma un procesa pieeja

SMS ir rīks to dažādo dalībnieku sapulcināšanai, kuriem jāsadarbojas, lai tie spētu vadīt drošu un veiksmīgu organizāciju. Šie elementi ietver mehānismus, kas ir izveidoti, lai izpildītu starptautiskos un valsts noteikumus un standartus, nozaru un uzņēmumu līmeņa prasības, riska novērtējumu rezultātus un paraugpraksi visās uzņēmuma darbībās. Tāpēc SMS ir jābūt integrētai organizācijas uzņēmējdarbības procesos, turklāt tā nedrīkstētu kļūt par sistēmu “uz papīra”, kas speciāli izstrādāta, lai pierādītu atbilstību tiesiskajam regulējumam. SMS ir jābūt mainīgam pasākumu kopumam, kas pilnveidojas un attīstās līdz ar organizāciju, kura to izmanto. Lai izveidotu SMS, organizācijai ir jāsaprot kontrolējamie riski, tiesiskais regulējums, kurā tā darbojas un tai ir jābūt skaidram priekšstatam, kas ir “labi” darbības rezultāti. Šajā rokasgrāmatā ir norādīti

SMS kritēriji, kuriem jābūt izpildītiem, lai vērtētājiestāde piešķirtu vienoto drošības sertifikātu. Tomēr ir jāatceras, ka SMS kvalitāti veido ne tikai SMS daļu summa. SMS ir arī jādarbojas kā vienotam veselumam — katras daļas izpildei ir jāpalīdz nodrošināt visas sistēmas pareizu darbību.

Prasības, kas būs SMS novērtējuma pamatā, var tikt izpildītas, īstenojot dokumentētu procesu (vai procedūru u. tml.), tomēr tam arī ir jābūt integrētam organizācijā un tās dažādajās uzņēmējdarbības jomās. Piemēram, VDI var pārbaudīt politikas paziņojuma esamību, taču tai ir jāpārbauda arī organizācijas apņēmība attiecīgo politiku piemērot. Praksē VDI to var izdarīt, pārbaudot, kā notiek SMS pārraudzība un pārskatīšana augstākajā vadības līmenī, kā šajā procesā tiek iesaistīti darbinieki un kā viņiem paziņo rezultātus. Organizācijai var arī nebūt īpašas procedūras drošībai būtiskas informācijas pārvaldībai, bet tai ir jāapraksta, kā attiecīgajās uzņēmējdarbības daļās tā tiek pienācīgi pārvaldīta (piemēram, drošībai būtiskas informācijas paziņošana vilciena vadītājam).

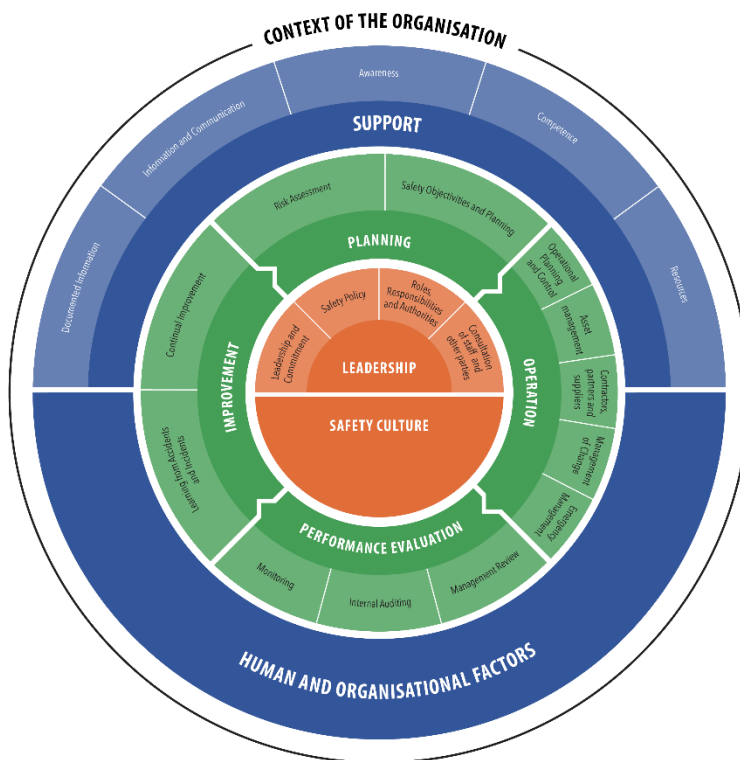
Svarīgs jauninājums Komisijas Deleģētās regulas (ES) 2018/762 [CSM attiecībā uz SMS] I un II pielikumā ir procesa pieejas ieviešana. Tā ir veicināta arīdzan ISO pārvaldības sistēmas standartos, kur dažādie pārvaldības sistēmas procesi ir cieši saistīti, un to konsekventa izmantošana palīdz sasniegt organizācijas mērķus. Komisijas Deleģētās regulas (ES) 2018/762 I un II pielikumā ir noteiktas dažas svarīgas saites starp procesiem, lai veicinātu izpratni par procesa pieeju, bet tas nenozīmē, ka šādas saites ir vienīgās, kādas pastāv, vai ka tās ir jāpierāda atbilstības nolūkos. Organizācijas spēja parādīt, kā tās pārvaldības sistēmas procesi ir savstarpēji saistīti, ir labs apliecinājums tam, ka organizācija saprot, kāda ir tās pārvaldības sistēmas efektīva darbība.

SMS elementus var ievērot, piemērojot ciklu “plānot–darīt–pārbaudīt–rīkoties” (PDPR) (sk. 2. attēls. attēlu). PDPR koncepcija atspoguļo SMS pamatelementu funkcionālo saistību:

- **plānošana** — noskaidro riskus un iespējas, izvirza drošības mērķus un nosaka procesus un pasākumus, kas vajadzīgi, lai gūtu rezultātus atbilstoši organizācijas drošības politikai;
- **darbība** — izstrādā, īsteno un piemēro plānotos procesus un pasākumus;
- **izpildes izvērtēšana** — pārbauda un izvērtē īstenoto procesu un pasākumu praktisko izpildi attiecībā pret mērķiem un plānu un ziņo par rezultātiem;
- **uzlabošana** — veic darbības, lai pastāvīgi uzlabotu drošības pārvaldības sistēmu un drošības rādītāju nolūkā sasniegt paredzētos rezultātus.

Šo PDPR pamatprocesu papildina citi SMS elementi:

- **“organizācijas konteksts”**, kas nodrošina ievaddatus plānošanas posmam;
- **“līderība”** kā PDPR cikla virzītājspēks;
- dažādas **“atbalsta”** funkcijas, kas atbalsta visus SMS elementus.



2. attēls. Dzelzceļa drošības pārvaldības sistēma

CONTEXT OF THE ORGANISATION	ORGANIZĀCIJAS KONTEKSTS
Awareness	Apzināšanās
Competence	Kompetence
Resources	Resursi
Information and Communication	Informācija un saziņa
Document Information	Dokumentu informācija
SUPPORT	ATBALSTS
Continual improvement	Pastāvīgi uzlabojumi
Risk assessment	Riska novērtējums
Safely Objectivities and Planning	Drošības mērķi un plānošana
Operational Planning and Control	Ekspluatācijas plānošana un kontrole
Asset management	Aktīvu pārvaldība
Contractors, partners and supplies	Darbuzņēmēji, partneri un piegādātāji
Management of change	Izmaiņu pārvaldība
Emergency management	Ārkārtas situāciju pārvaldība
Management review	Vadības veikta pārskatīšana

Internal Auditing	Iekšējā revīzija
Monitoring	Uzraudzība
Learning from Accidents and Incidents	No negadījumiem un starpgadījumiem gūtā mācība
PLANNING	PLĀNOŠANA
OPERATION	EKSPLUATĀCIJA
PERFORMANCE EVALUATION	VEIKTSPĒJAS IZVĒRTĒŠANA
IMPROVEMENT	UZLABOJUMI
LEADERSHIP	LĪDERĪBA
SAFETY CULTURE	DROŠĪBAS KULTŪRA
Leadership and Commitment	Līderība un apņemšanās
Safety Policy	Drošības politika
Consultation of staff and other parties	Apspriešanās ar personālu un citām pusēm

0.8 Drošības pārvaldības sistēma un drošības kultūra

Drošības kultūra ir uzvedības un domāšanas veidu kopums, ko organizācijā lielākoties ievēro attiecībā uz būtisku ar tās darbībām saistītu risku pārvaldību. Tas, protams, nozīmē, ka organizācijā var pastāvēt vairākas kultūras, kuru pamatā ir amata pienākumi, ģeogrāfiskā atrašanās vieta vai citas kopīgas vērtības. Drošības kultūra kā tāda veidojas diendienā, mijiedarbojoties dalībniekiem, tādas organizācijas kontekstā, kurai ir gan jāpielāgojas tās videi, gan jānodrošina visu tās locekļu integrācija.

Tiešs veids, kā raksturot drošības kultūru, ir aplūkot faktoros, kas veicina uzvedību. SMS nodrošina pamatu — nosakot potenciālos darba apstākļus un paredzamo rezultātu, organizācija nosaka vēlamu darbības veidu un tehniskos līdzekļus darbības atbalstam. Lai varētu darboties droši, organizācija vislabākajā iespējamā veidā paredz nevēlamas situācijas un īsteno to pārvaldības noteikumus un līdzekļus. Turklāt pastāv arī organizācijas “uzvedības pasaule”, proti, īpašības, sajūtas, nozīmes un attiecības, kas nosaka mijiedarbības veidus starp indivīdiem organizācijā tā, ka tiek ietekmēts domāšanas un rīcības veids. Šis kultūras aspekts galvenokārt attiecas uz “nerakstītajiem noteikumiem, kas nosaka cilvēku grupas uzvedību un lēmumus.” Organizācijas strukturālā un kultūras daļa kopā veicina (vai kavē) organizācijas veikspēju.

Tomēr pastāv augsts risks, ka pārāk birokrātiska pieeja drošības pārvaldībai varētu nonākt pretrunā darbības realitātei, kā rezultātā drošības pārvaldības sistēma “dzīvotu savu dzīvi”, respektīvi, visi pūliņi tiktu ieguldīti dokumentētas sistēmas izstrādē, uzturēšanā un pat tās esamības pierādīšanā, ignorējot darbu, kas jāiegulda, lai sistēma faktiski varētu darboties, kā iecerēts, un radot plaisu starp “iedomāto darbu” un “izdarīto darbu”.

Tomēr ir iespējams drošības pārvaldības sistēmu izmantot kā instrumentu, lai pozitīvi ietekmētu organizācijas drošības kultūru un fizisko vidi, kā arī darbinieku uzvedību drošību atbalstošā un veicinošā veidā. Tieši organizācijas strukturālās un kultūras daļas saskaņotība ir tā, kas galu galā palielina drošību. Lai palīdzētu cilvēkiem veikt viņu uzdevumu, organizācijai jāsaprot, kā cilvēki (ar savām spējām un ierobežojumiem) izmanto specifiskājas, lai atrisinātu problēmas, un šīs zināšanas jāņem vērā, veidojot viņu darba vidi. Tas pats attiecas uz noteikumiem un regulām — kamēr vien darbinieki, kuri tās īsteno, netiek ņemti vērā darba procedūru izstrādē, viņi ir spiesti pārkāpt noteikumus, lai izdarītu darbu, ikreiz, kad rodas pretrunas vai konflikti.

Visā šajā dokumentā ir uzsvērtas pamatīpašības, kas, cik zināms, veicina pozitīvu drošības kultūru. Turklāt 4. pielikums.. pielikumā lasītājam ir sniegta pamatinformācija par drošības kultūru un cita informācija, kas organizācijai noderēs tās stratēģijas izstrādē.

0.9 Pamatojoši pierādījumi un dokumentēta informācija

Šajā dokumentā ir sniegti daži norādījumi par pierādījumiem, kas pieteikuma iesniedzējam (t. i., dzelzceļa pārvadājumu uzņēmumam vai infrastruktūras pārvaldītājam) ir jāiesniedz, piesakoties drošības sertifikāta vai drošības atļaujas saņemšanai, bet iepriekš minēto iemeslu dēļ nav konkrēti noteikts, kas ir jāuzrāda. Attiecībā uz katru prasību ir sniegta norāde par pierādījumiem, kas pieteikuma iesniedzējam ir jāiesniedz, kopā ar attiecīgu norādi uz konkrēto prasību. Turpmāk ir doti daži piemēri, kā pierādījumi varētu izskatīties praksē. Jāatzīst, ka piemēri ir doti tikai izpratnes atvieglošanas nolūkā; tie nav vienīgais veids, kā parādīt atbilstību, un tie arī nav pilnīgs iespējamo alternatīvu uzskaitījums. Turklāt ir jāsaprot arī dzin tas, ka pieteikuma iesniedzējam, iesniedzot pieteikumu, ir jāapraksta, kā tas izpilda katru prasību. Vērtētājs var pieprasīt un pieteikuma iesniedzējs var uzrādīt kā pierādījumu ieteikto informāciju, lai paskaidrotu vai pamatotu, kā prasība tiek izpildīta. Gan pieteikuma iesniedzējam, gan vērtētājam vissvarīgāk attiecībā uz katru prasību ir pārliecināties, ka apgalvojumi par atbilstību ir piesaistīti atsaucēm, kurās izskaidrots, kur ir atrodami papildu pierādījumi, kas pamato izteiktos apgalvojumus. Piemēru sadaļa attiecībā uz katru prasību ir paredzēta, lai parādītu, kā šāds atsauces materiāls varētu izskatīties.

Atsauces, kam vajadzētu palīdzēt pieteikumu iesniedzējiem sagatavot pieteikumus, ir uzskaitītas pēc minētās sadaļas. Visbeidzot, pēdējā sadaļā zem katra elementa ir norādīta vajadzīgā saite uz uzraudzību. Tajā ir arī sniegta norāde par jautājumiem, uz kuriem vērtētājs var īpaši vērst VDI uzraudzības grupu uzmanību kā uz interešu jomām, ko var izmantot, lai pārbaudītu SMS vispusīgumu.

Arī pieeja, kas ir paredzēta ISO pārvaldības sistēmu standartos, un Komisijas Deleģētās regulas (ES) 2018/762 I un II pielikums nav preskriptīvi (izņemot īpašus gadījumus) attiecībā uz pierādījumu veidu (piemēram procedūru), kāds tiek gaidīts no pieteikuma iesniedzēja. Pieteikuma iesniedzējam ir atvēlēta zināma rīcības brīvība, lai organizācija varētu aprakstīt savu drošības pārvaldības sistēmu, atspoguļojot tās uzņēmējdarbības veidu, un darīt to samērīgi tās apjomam. Tas arī palīdzēs pārorientēties no atbilstības pārbaudes “uz papīra” uz pastāvīgi mainīgas sistēmas novērtējumu, kas pienācīgi atspoguļo uzņēmuma drošības pārvaldības pasākumus tādos, kādi tie ir praksē.

Termins “dokumentēta informācija” tika ieviests kā daļa no ISO HLS un pārvaldības sistēmu standartu kopējiem terminiem. “Dokumentētas informācijas” definīcija ir atrodama *ISO 9000 standarta 3.8. noteikumā*. Dokumentētu informāciju var izmantot, lai paziņotu kādu vēstījumu, sniegtu pierādījumus par to, kas bijis ieplānots, kas ir faktiski izdarīts, vai lai dalītos ar zināšanām. Tā ietver dokumentus un ierakstus, piemēram, procedūras, sanāksmju protokolus, ziņojumus, oficiālus paziņojumus par mērķiem, rezultātus, vienošanās, līgumus u. tml., bet neaprobežojas tikai ar tiem. Plašāks skaidrojums ir atrodams Rokasgrāmatā par ISO 9001:2015 prasībām dokumentētai informācijai, kas pieejama ISO tīmekļa vietnē

https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/documented_information.pdf.

Jēdziens “procedūra” nav jāsaprot kā tāds, kas attiecas uz esošu atsevišķu dokumentu, kurā plaši aplūkots tikai katrs atsevišķs SMS elements, vai kas nosaka, ka ir jābūt izstrādātam īpašam jaunu dokumentu kopumam. Ja šajā dokumentā ir atsauce uz procedūru, tā jāsaprot kā atsauce uz dokumentētu informāciju (piemēram, dokumentiem papīra formātā), kurā ir izklāstītas secīgi veicamās darbības. Ja ir atsauce uz procesu, tā jāsaprot kā atsauce uz līdzekļiem, ko izmanto, lai sasniegtu konkrētu uzdevumu vai mērķi, un kas var būt un var nebūt izklāstīti procedūrā.

0.10 Mijņorādes uz citām ES regulām un piemērojamām tiesību aktu prasībām

Atsauces uz citām ES regulām palielina dažādo tiesību aktu saskaņotību, vienlaikus atzīstot to savstarpējo saikni. SMS pasākumiem vienmēr ir jāatbilst spēkā esošajiem tiesību aktiem, ja vien nav norādīts citādi

(piemēram, īpaši pārejas noteikumi, atlikta piemērošana). Ja ES regula ir atcelta, visas atsauces parasti uzskata par atsaucēm uz jauno regulu (ja tā ir norādīta).

Visiem dzelzceļa pārvadājumu uzņēmumiem un infrastruktūras pārvaldītājiem ir jāizpilda dažādi juridiskie pienākumi, kuri aptver arī citus jautājumus, ne tikai ar drošību saistītos. Daži no šādiem citiem pienākumiem tieši vai netieši ietekmēs to, kā organizācija pilda savus uzdevumus drošības jomā ar savas SMS starpniecību, piemēram, panāk atbilstību tiesību aktiem, kas izriet no Savstarpējās izmantojamības direktīvas (ES) 2016/797, vai gādā par to pakalpojumu drošību, ko infrastruktūras pārvaldītāji sniedz dzelzceļa pārvadājumu uzņēmumiem atbilstoši Direktīvai (ES) 2012/34. Tāpēc SMS, ko dzelzceļa pārvadājumu uzņēmumi un infrastruktūras pārvaldītāji izmanto drošības apdraudējumu risināšanai, jābūt organizētai tā, lai attiecīgā gadījumā nodrošinātu atbilstību šādiem citiem juridiskiem pienākumiem.

Labāka dzelzceļa sistēma
sabiedrībai

Saturs

0	Ievads	2
0.1	Rokasgrāmatas mērķis	2
0.2	Rokasgrāmatas adresāti	2
0.3	Piemērošanas joma	3
0.4	Rokasgrāmatas struktūra	3
0.5	ISO/IEC direktīvu 1. daļa un konsolidēts ISO papildinājums	4
0.6	Drošības pārvaldības sistēmas mērķis	5
0.7	Drošības pārvaldības sistēma un procesa pieeja	5
0.8	Drošības pārvaldības sistēma un drošības kultūra	8
0.9	Pamatojoši pierādījumi un dokumentēta informācija	9
0.10	Mijņorādes uz citām ES regulām un piemērojamām tiesību aktu prasībām	9
1	Organizācijas konteksts	16
1.1	Normatīvā prasība	16
1.2	Mērķis	16
1.3	Paskaidrojumi	17
1.4	Pierādījumi	18
1.5	Pierādījumu piemēri	18
1.6	Atsauces un standarti	19
1.7	Uzraudzības jautājumi	19
2	Līderība	20
2.1	Līderība un apņemšanās	20
2.1.1	Normatīvā prasība	20
2.1.2	Mērķis	20
2.1.3	Paskaidrojumi	21
2.1.4	Pierādījumi	21
2.1.5	Pierādījumu piemēri	22
2.1.6	Atsauces un standarti	22
2.1.7	Uzraudzības jautājumi	22
2.2	Drošības politika	24
2.2.1	Normatīvā prasība	24
2.2.2	Mērķis	24
2.2.3	Paskaidrojumi	24
2.2.4	Pierādījumi	24
2.2.5	Pierādījumu piemēri	25
2.2.6	Uzraudzības jautājumi	25
2.3	Organizatoriskās funkcijas, pienākumi, pārskatatbildība un pilnvaras	26

2.3.1	Normatīvā prasība	26
2.3.2	Mērķis	26
2.3.3	Paskaidrojumi	26
2.3.4	Pierādījumi	27
2.3.5	Pierādījumu piemēri	27
2.3.6	Atsauces un standarti	28
2.3.7	Uzraudzības jautājumi	28
2.4	Apspriešanās ar personālu un citām pusēm	29
2.4.1	Normatīvā prasība	29
2.4.2	Mērķis	29
2.4.3	Paskaidrojumi	29
2.4.4	Pierādījumi	29
2.4.5	Pierādījumu piemēri	30
2.4.6	Uzraudzības jautājumi	30
3	Plānošana	31
3.1	Rīcība riska novēršanai	31
3.1.1	Normatīvā prasība	31
3.1.2	Mērķis	31
3.1.3	Paskaidrojumi	32
3.1.4	Pierādījumi	33
3.1.5	Pierādījumu piemēri	34
3.1.6	Atsauces un standarti	35
3.1.7	Uzraudzības jautājumi	35
3.2	Drošības mērķi un plānošana	36
3.2.1	Normatīvā prasība	36
3.2.2	Mērķis	36
3.2.3	Paskaidrojumi	36
3.2.4	Pierādījumi	37
3.2.5	Pierādījumu piemēri	37
3.2.6	Uzraudzības jautājumi	37
4	Atbalsts	38
4.1	Resursi	38
4.1.1	Normatīvā prasība	38
4.1.2	Mērķis	38
4.1.3	Paskaidrojumi	38
4.1.4	Pierādījumi	38
4.1.5	Pierādījumu piemēri	38
4.1.6	Uzraudzības jautājumi	39
4.2	Kompetence	40
4.2.1	Normatīvā prasība	40
4.2.2	Mērķis	40
4.2.3	Paskaidrojumi	41
4.2.4	Pierādījumi	41
4.2.5	Pierādījumu piemēri	42

4.2.6	Atsauces un standarti	43
4.2.7	Uzraudzības jautājumi	43
4.3	Apzināšanās	44
4.3.1	Normatīvā prasība	44
4.3.2	Mērķis	44
4.3.3	Pierādījumi	44
4.3.4	Pierādījumu piemēri	44
4.3.5	Uzraudzības jautājumi	45
4.4	Informācija un saziņa	46
4.4.1	Normatīvā prasība	46
4.4.2	Mērķis	46
4.4.3	Paskaidrojumi	46
4.4.4	Pierādījumi	47
4.4.5	Pierādījumu piemēri	47
4.4.6	Uzraudzības jautājumi	48
4.5	Dokumentēta informācija	49
4.5.1	Normatīvā prasība	49
4.5.2	Mērķis	50
4.5.3	Paskaidrojumi	50
4.5.4	Pierādījumi	51
4.5.5	Pierādījumu piemēri	52
4.5.6	Atsauces un standarti	52
4.5.7	Uzraudzības jautājumi	52
4.6	Cilvēkfaktoru un organizatorisko faktoru integrācija	54
4.6.1	Normatīvā prasība	54
4.6.2	Mērķis	54
4.6.3	Paskaidrojumi	54
4.6.4	Pierādījumi	54
4.6.5	Pierādījumu piemēri	55
4.6.6	Atsauces un standarti	56
4.6.7	Uzraudzības jautājumi	56
5	Ekspluatācija	57
5.1	Ekspluatācijas plānošana un kontrole	57
5.1.1	Normatīvā prasība	57
5.1.2	Mērķis	58
5.1.3	Paskaidrojumi	59
5.1.4	Pierādījumi	60
5.1.5	Pierādījumu piemēri	61
5.1.6	Atsauces un standarti	62
5.1.7	Uzraudzības jautājumi	63
5.2	Aktīvu pārvaldība	64
5.2.1	Normatīvā prasība	64
5.2.2	Mērķis	65
5.2.3	Paskaidrojumi	65

5.2.4	Pierādījumi.....	66
5.2.5	Pierādījumu piemēri	68
5.2.6	Atsauces un standarti	72
5.2.7	Uzraudzības jautājumi	72
5.3	Darbuzņēmēji, partneri un piegādātāji	73
5.3.1	Normatīvā prasība	73
5.3.2	Mērķis.....	73
5.3.3	Paskaidrojumi	74
5.3.4	Pierādījumi.....	74
5.3.5	Pierādījumu piemēri	74
5.3.6	Uzraudzības jautājumi	75
5.4	Izmaiņu pārvaldība	76
5.4.1	Normatīvā prasība	76
5.4.2	Mērķis.....	76
5.4.3	Paskaidrojumi	76
5.4.4	Pierādījumi.....	77
5.4.5	Pierādījumu piemēri	77
5.4.6	Uzraudzības jautājumi	77
5.5	Ārkārtas situāciju pārvaldība	78
5.5.1	Normatīvā prasība	78
5.5.2	Mērķis.....	78
5.5.3	Paskaidrojumi	79
5.5.4	Pierādījumi.....	79
5.5.5	Pierādījumu piemēri	79
5.5.6	Uzraudzības jautājumi	80
6	Veiktspējas izvērtēšana	81
6.1	Uzraudzība	81
6.1.1	Normatīvā prasība	81
6.1.2	Mērķis.....	81
6.1.3	Paskaidrojumi	81
6.1.4	Pierādījumi.....	82
6.1.5	Pierādījumu piemēri	82
6.1.6	Uzraudzības jautājumi	82
6.2	Iekšējā revīzija	83
6.2.1	Normatīvā prasība	83
6.2.2	Mērķis.....	83
6.2.3	Paskaidrojumi	83
6.2.4	Pierādījumi.....	83
6.2.5	Pierādījumu piemēri	84
6.2.6	Atsauces un standarti	84
6.2.7	Uzraudzības jautājumi	84
6.3	Vadības veikta pārskatīšana	85
6.3.1	Normatīvā prasība	85
6.3.2	Mērķis.....	85

6.3.3	Pierādījumi.....	85
6.3.4	Pierādījumu piemēri	86
6.3.5	Uzraudzības jautājumi	86
7	Uzlabojumi	87
7.1	No negadījumiem un starpgadījumiem gūtā mācība.....	87
7.1.1	Normatīvā prasība	87
7.1.2	Mērķis.....	87
7.1.3	Paskaidrojumi	88
7.1.4	Pierādījumi.....	88
7.1.5	Pierādījumu piemēri	88
7.1.6	Atsauces un standarti	89
7.1.7	Uzraudzības jautājumi	89
7.2	Pastāvīgi uzlabojumi.....	90
7.2.1	Normatīvā prasība	90
7.2.2	Mērķis.....	90
7.2.3	Paskaidrojumi	90
7.2.4	Pierādījumi.....	92
7.2.5	Pierādījumu piemēri	93
7.2.6	Uzraudzības jautājumi	93
1.	pielikums. Korelācijas tabulas.....	94
2.	pielikums. Atbilstoši Savienības tiesību aktiem piešķirtu produktu vai pakalpojumu atļauju, atzišanas dokumentu vai sertifikātu savstarpējā atzišana	102
3.	pielikums. Darbības uz pievedceļiem, līgumsaistības un partnerības	106
4.	pielikums. Drošības kultūra	110
5.	pielikums. Cilvēkfaktori un organizatoriskie faktori	115
6.	pielikums. Definīcijas	118

Labāka dzelzceļa sistēma
sabiedrībai

1 Organizācijas konteksts

1.1 Normatīvā prasība

1.1 Organizācija:

- (a) apraksta savu darbību veidu, **iezīmes**, apjomu un jomu;
- (b) apzina nopietnus drošības apdraudējumus, ko rada dzelzceļa darbības, kuras veiks pati organizācija vai tās kontrolē esoši darbuzņēmēji, partneri un piegādātāji;
- (c) apzina ieinteresētās personas (piemēram, regulatīvās struktūras, iestādes, **dzelzceļa pārvadājumu uzņēmumus**, infrastruktūras pārvaldītājus, darbuzņēmējus, piegādātājus, partnerus), tostarp personas ārpus dzelzceļa sistēmas, kas ir svarīgas drošības pārvaldības sistēmas kontekstā;
- (d) apzina un saglabā c) apakšpunktā minēto ieinteresēto personu juridiskās un cita veida prasības saistībā ar drošību;
- (e) nodrošina, ka d) apakšpunktā minētās prasības ir ņemtas vērā drošības pārvaldības sistēmas izstrādē, ieviešanā un uzturēšanā;
- (f) apraksta drošības pārvaldības sistēmas tvērumu, norādot, kuras uzņēmējdarbības daļas ir vai nav iekļautas tās tvērumā, un ņemot vērā d) apakšpunktā minētās prasības.

1.2 Šajā pielikumā piemēro šādas definīcijas:

- (a) “**iezīmes**” attiecībā uz infrastruktūras pārvaldītāju veiktajām dzelzceļa darbībām ir darbības raksturojums, ņemot vērā tās jomu, ietverot infrastruktūras projektēšanu un būvniecību, infrastruktūras tehnisko apkopi, satiksmes plānošanu, satiksmes pārvaldību un vadību, un ņemot vērā dzelzceļa infrastruktūras izmantojumu, ietverot parastās un/vai ātrgaitas dzelzceļa līnijas, pasažieru un/vai kravu pārvadājumus;
- (b) “**apjoms**” attiecībā uz infrastruktūras pārvaldītāju veiktajām dzelzceļa darbībām ir apjoms, ko raksturo dzelzceļa sliežu ceļa garums un aplēstais infrastruktūras pārvaldītāja lielums, ko izsaka kā dzelzceļa nozarē strādājošo darba ņēmēju skaitu.

1.2 Mērķis

Pieteikuma iesniedzējam ir pēc iespējas precīzāk jāparāda iestādei, ka tā SMS aptver visu tā darbību. Vērtētājiestādei ir jāspēj skaidri saprast, kāds ir darbības veids un kā notiek darbības pārvaldība ar SMS starpniecību. Pieteikuma iesniedzējam ir jāparāda, ka tam ir skaidra izpratne par tā attiecībām ar ieinteresētajām personām un nopietnajiem riskiem, ar ko tas saskaras, kā arī par to, kurš tiek ietekmēts un kā šie jautājumi tiek pārvaldīti SMS.

1.3 Paskaidrojumi

Iepriekš minētā tiesību akta 1.1. punktā, kur šī prasība attiecas uz infrastruktūras pārvaldītājiem, “veids” ir aizstāts ar “iezīmēm”, un “lauks” ir svītrots.

Prasības par organizāciju, tās kontekstu un drošības pārvaldības sistēmas tvērumu (**1.1. punkts**) mērķis ir panākt vērtētāju labāku izpratni par organizācijas uzņēmējdarbību, ieinteresēto personu prasībām un vidi, kurā organizācija darbojas. Organizācijas veids ir novērtējuma sākumpunkts. Ja šī informācija ir zināma jau pieteikuma sagatavošanas sākumā, pieteikuma iesniedzējs var aprakstīt, ko tas dara un kā ir strukturēta tā organizācija, un tas savukārt ļauj vērtētājam pieņemt lēmumus par to, kā plānot novērtējumu. Piemēram, ja organizācija ir centralizēta vai īsteno būtiski atšķirīgas darbības ar plašu vietējo rīcības brīvību savu darbību plānošanā un organizēšanā vai ja organizācija nodarbina vairāk vai mazāk darbuzņēmēju, attiecīgi tiks gaidīts, ka pieteikuma iesniedzēja organizācija un tās SMS būs strukturētas tā, lai risinātu radītās problēmas. Organizācijas vispārējā konteksta skaidrojums var arī norādīt, kā notiek cilvēkfaktoru un organizatorisko faktoru pārvaldība. Struktūra, kas ir izklāstīta ISO HLS 4. noteikumā, var palīdzēt saprast, kāds ir vajadzīgais sagatavošanās darbs pirms SMS izveides. Lai vērtētājs varētu veikt pienācīgu novērtējumu, viņam ir būtiski saprast darbības tvērumu.

Darbību veids (**1.1. punkta a) apakšpunkts**) pēc definīcijas ietver pasažieru pārvadājumus (ietverot vai neietverot ātrgaitas pārvadājumu pakalpojumus), kravu pārvadājumus (ietverot vai neietverot bīstamas kravas) un manevru pakalpojumus. Tas var ietvert arī citus īpašus darbības veidus, piemēram, ritekļu testēšanu, to ekspluatāciju dzelzceļa infrastruktūras uzturēšanai, darbības uz privātiem pievedceļiem. Vairāk informācijas par darbības veidu, apjomu un telpu ir atrodams Aģentūras pieteikumu iesniegšanas rokasgrāmatā vienotā drošības sertifikāta izdošanai. Plašāka informācija par darbībām uz pievedceļiem ir atrodama 3. pielikums.. pielikumā.

Attiecībā uz infrastruktūras pārvaldītājiem “iezīmes” un “apjoms” (1.2. punkts) nozīmē uzņēmuma veidu un tā ģeogrāfisko lielumu un sarežģītību. “Iezīmes” atspoguļo izmantotās infrastruktūras veidu, to, cik mūsdienīga tā ir, vai tā ir ātrgaitas vai tradicionālā infrastruktūra, vai abējādi, savukārt “apjoms” attiecas uz vadītā uzņēmuma veidu.

Nopietnu risku apzināšana šajā gadījumā nozīmē, ka pieteikuma iesniedzējam ir jāpierāda, ka tas, pamatojoties uz savu analīzi, apzinās savus visbūtiskākos riskus. . Nopietna riska apzināšana nozīmē arī to, ka pieteikuma iesniedzējs ir izveidojis riska pārvaldības sistēmu (vai gatavojas to izveidot), un, pamatojoties uz to, viņš var:

- *analizēt bīstamus notikumus un novērtēt riskus,*
- *uzzināt par visbūtiskākajiem riskiem (to seku un biežuma ziņā) un*
- *noteikt to pasākumu prioritātes, kuru mērķis ir novērst negadījumus (1.1. punkta b) apakšpunkts).*

Tas palīdz noteikt organizācijas kontekstu un parāda vērtētājiestādei, ka organizācija izprot vidi, kurā tā darbojas. Darbību drošību var ietekmēt darbības, ko veic citas personas ārpus dzelzceļa sistēmas (**1.1. punkta c) apakšpunkts**), tāpēc arī tās ir jāņem vērā, novērtējot risku. Plašāka informācija par līgumsaistībām un partnerību ir atrodama 3. pielikums.. pielikumā.

Ar drošību saistīto piemērojamo prasību (**1.1. punkta d) apakšpunkts**) apzināšana ietver prasības, sākot no piemērojamo ES regulu noteikumiem (piemēram, attiecīgā CSM par drošības pārvaldības sistēmām un jo īpaši tās I un II pielikums, CSM riska noteikšanai un novērtēšanai, CSM pārraudzībai, attiecīgās SITS, Īstenošanas akts par drošības sertifikācijas praktisko kārtību un, ja piemērojams, Īstenošanas akts par ritekļu atļauju izsniegšanas praktisko kārtību un ECM regula) un valsts tiesību aktiem (paziņotie valsts noteikumi, vietējie tiesību akti) un beidzot ar jebkādām citām prasībām, kuras organizācija apņemas izpildīt (piemēram, sektora vai nozares līmeņa noteikumi vilcienu ekspluatācijas vai pārvaldības sistēmai un tehniskie standarti — ISO, CEN/CENELEC, UIC). Šajā sadaļā organizācija nosaka tiesību aktu noteikumus, kas tai jāizpilda, kā arī tās nozaru un citas prasības, kas tai būs jāievēro, lai varētu droši ekspluatēt vilcienus.

Šajā dokumentā termini “personāls”, “darbinieki” un “darba ņēmēji” ir sinonīmi, proti, ar tiem apzīmē personas, kuras strādā pieteikuma iesniedzēja organizācijas tiešā kontrolē.

1.4 Pierādījumi

- *Dzelzceļa pārvadājumu uzņēmumiem: informācija par darbības veidu, piemēram, pasažieru un/vai kravu pārvadājumi, bīstamo kravu pārvadājumi, ģeogrāfiskais aptvērums (iekļaujot karti vai maršrutu plānu) un darbības apjoms (norādot ritošā sastāva veidus, darbinieku skaitu), un to jauninājumi un izmaiņas kopš pēdējā novērtējuma (1.1. punkta a) apakšpunkts).*
- *Infrastrukturā pārvaldītājiem: informācija par to darbību veidu, par kurām tie gādā, piemēram, kravu un/vai pasažieru pārvadājumi, manevru pakalpojumi vai citi apkalpes vietu pakalpojumi (kā minēts Direktīvas 2012/34/ES II pielikumā), kas ietekmē dzelzceļa drošību, kā arī par ģeogrāfisko aptvērumu (iekļaujot karti vai maršrutu plānu) un tīklā notiekošo dzelzceļa pārvadājumu uzņēmumu darbību apjomu. Infrastruktūras pārvaldītājam arī ir jāiekļauj informācija par jebkuru ritošo sastāvu (tostarp iekārtu infrastruktūras uzturēšanai vai mērījumu veikšanai), ko tas ekspluatē, un jānorāda nodarbināto darbinieku skaits, kā arī jauninājumi un izmaiņas kopš pēdējā novērtējuma (1.1. punkta a) apakšpunkts).*
- *Drošības sertifikāta vai drošības atļaujas pieteikuma iesniedzējam jāparāda, kā tas ir identificējis attiecīgās normatīvās prasības, piemēram, CSM novērtēšanas prasības, savstarpējās izmantojamības tehniskās specifikācijas, jo īpaši specifikācijas par satiksmes nodrošināšanas un vadības apakšsistēmu (SITS OPE), un piemērojamos valsts noteikumus, un kā tas uztur atbilstību minētajām prasībām (SMS procesi, kas atbalsta atbilstību) (1.1. punkta c) un d) apakšpunkts).*
- *Pieteikuma iesniedzējam jānorāda ieinteresētās personas (piemēram, darbuzņēmēji vai partneri), kuriem ir svarīga nozīme tā SMS sekmīgā īstenošanā (t. i., kuru darbībai ir ietekme vai potenciāla ietekme uz SMS), norādot arī, kāpēc tās ir vajadzīgas SMS sekmīgai darbībai (1.1. punkta c) un d) apakšpunkts).*
- *Abiem: pieteikuma iesniedzējam ir jānorāda, kur tā drošības pārvaldības sistēmas dokumentācijā tiek izpildīta katra no SMS prasībām, tostarp piemērojamo savstarpējās izmantojamības tehnisko specifikāciju, jo īpaši SITS OPE, attiecīgās prasības un attiecīgie paziņotie valsts noteikumi (1.1. punkta e) apakšpunkts).*
- *Pieteikuma iesniedzējam jānorāda, kādi ir visnopietnākie drošības apdraudējumi, kas ietekmē tā uzņēmējdarbību (1.1. punkta b) apakšpunkts).*
- *Pieteikuma iesniedzējam jāsniedz informācija par SMS tvērumu (tostarp par tās robežām ar citām uzņēmuma daļām) (1.1. punkta f) apakšpunkts).*

1.5 Pierādījumu piemēri

Karte, kurā ir attēlota darbības ģeogrāfiskā teritorija. Informācija par ritošo sastāvu, ko atļauts ekspluatēt (tostarp — attiecīgā gadījumā — jebkurš iespējamais ritošais sastāvs, ko ierosināts ekspluatēt sertifikāta vai atļaujas derīguma termiņa laikā, un jebkuri izmantošanas teritorijas ierobežojumi). Tiek iekļauta informācija par to pakalpojumu veidiem, ko pieteikuma iesniedzējs plāno sniegt (pasažieru un/vai kravu pārvadājumi).

Ja pieteikuma iesniedzējs ir infrastruktūras pārvaldītājs, šo informāciju var sniegt, atsaucoties, piemēram, uz:

- *informāciju, kas ir iekļauta Dzelzceļa infrastruktūras reģistrā, kurš izveidots atbilstoši Savstarpējās izmantojamības direktīvai (49. pants);*
- *tīkla pārskatu (jo īpaši I sadaļu), kas izveidots atbilstoši Direktīvai 2012/34/ES, un*
- *maršrutu grāmatu (SITS OPE).*

Informācija, ko sniedz nolūkā saņemt drošības atļauju vai drošības sertifikātu, ir pienācīgi papildināta ar atsaucēm un pietiekami dokumentēta, lai pierādītu attiecīgo ES tiesību aktu ievērošanu.

Norāde par pašreizējo un ierosināto personāla sastāvu vienotā drošības sertifikāta derīguma termiņa laikā, ciktāl šāds sastāvs ir zināms.

Dzelzceļa pārvadājumu uzņēmums sniedz informāciju par savām darbības saskarnēm, tostarp saskarnēm ar infrastruktūras pārvaldītāju(-iem), citiem dzelzceļa pārvadājumu uzņēmumiem, darbuzņēmējiem un neatliekamās palīdzības dienestiem. Šī informācija ietver jebkādas infrastruktūras pārvaldītāja īpašas prasības, kas ietekmē dzelzceļa pārvadājumu uzņēmuma SMS.

Dzelzceļa pārvadājumu uzņēmumi, lai izskaidrotu, kā tiek ievēroti noteikumi un citas attiecīgas prasības, ar vienas pieturas aģentūras starpniecību var iesniegt atbilstības tabulu kā daļu no pieteikuma dokumentācijas drošības sertifikāta saņemšanai.

Savukārt infrastruktūras pārvaldītājam ir jāiesniedz līdzīgs to personu uzskaitījums, ar kurām tam ir darbības saskarnes, piemēram, dzelzceļa pārvadājumu uzņēmumu, kas darbojas kontrolētajā infrastruktūrā, darbuzņēmēju, kaimiņvalstu infrastruktūras pārvaldītāju, būvlaukumu, vietējo iestāžu (attiecībā uz ceļa saskarnēm) un neatliekamās palīdzības dienestu saraksts.

Informācija par tiesību aktu (gan vietējo, gan Eiropas) noteikumiem, k tas ievēros.

Apraksts (arī organigramma), kurā ir izklāstīts, kā SMS ir strukturēta un tiek pārvaldīta organizācijā, un kurā ir iekļautas arī saites uz dažādajām SMS sadaļām, kas sniedz sīkāku informāciju par darbības noteikumiem.

Jaunākā gada pārskata kopija, kurā ir sīki izklāstīti visnopietnākie riski, ko organizācija pārvalda, un to kontroles mērķi, izmantotā novērtēšanas metodika un to prioritāšu noteikšana.

.

1.6 Atsauces un standarti

- *SITS OPE piemērošanas rokasgrāmatas*

1.7 Uzraudzības jautājumi

Pārbaudīt sniegtās informācijas precizitāti, to salīdzinot ar zināmu informāciju par esošām darbībām, ja pieteikumu iesniedz par sertifikāta atjaunošanu, vai citu pieejamu informāciju, ja pieteikuma iesniedzējs ir jaunpienācējs.

Pārbaudīt, vai aprakstītā SMS nodrošina pasākumus drošības pārvaldībai praksē.

Pārbaudīt, vai visas organizācijas saskarnes ar citiem dalībniekiem ir atspoguļotas SMS pasākumos riska kontrolēšanai.

2 Līderība

2.1 Līderība un apņemšanās

2.1.1 Normatīvā prasība

- 2.1.1. Augstākā līmeņa vadība demonstrē līderību un apņemšanos izstrādāt, ieviest, uzturēt un pastāvīgi uzlabot drošības pārvaldības sistēmu, tālab:
- (a) uzņemties vispārēju pārskatatbildību un atbildību par drošību;
 - (b) nodrošinot, ka organizācijas dažādu līmeņu vadība apņemas gādāt par drošību ar savu darbību un attiecībās ar personālu un darbuzņēmējiem;
 - (c) nodrošinot, ka drošības politika un drošības mērķi ir izveidoti, izprasti un saderīgi ar organizācijas stratēģisko virzību;
 - (d) nodrošinot, ka prasības drošības pārvaldības sistēmai ir integrētas organizācijas uzņēmējdarbības procesos;
 - (e) nodrošinot, ka ir pieejami drošības pārvaldības sistēmai vajadzīgie resursi;
 - (f) nodrošinot, ka drošības pārvaldības sistēma efektīvi kontrolē organizācijas radītos drošības apdraudējumus;
 - (g) mudinot personālu atbalstīt drošības pārvaldības sistēmai noteikto prasību izpildi;
 - (h) veicinot drošības pārvaldības sistēmas pastāvīgu uzlabošanu;
 - (i) nodrošinot, ka organizācijas uzņēmējdarbības risku apzināšanā un pārvaldībā ir ņemti vērā drošības apsvērumi, un paskaidrojot, kā tiks atpazīts un atrisināts drošības mērķu un citu mērķu konflikts;
 - (j) sekmējot pozitīvu drošības kultūru.

2.1.2 Mērķis

. Skaidra un pozitīva drošības pārvaldības virziena noteikšana būtiski ietekmēs to, kā tiek pārvaldīts risks. Vērtētājiestādei jābūt pārliecinātai, ka pieteikuma iesniedzējs ir apņēmis atvēlēt resursus, lai organizācija varētu darboties droši un pārvaldīt riskus efektīvi un lai pieteikuma iesniedzēja organizācijā ir vadītāji, kuri nodrošina to praksē. Vadības apņemšanos attiecībā uz cilvēkfaktoriem un organizatoriskajiem faktoriem parāda ar politiku un mērķiem, kā arī ar vadības un vadītāju uzvedību. Turklāt vadītāju īstenota uz cilvēkfaktoriem un organizatoriskajiem faktoriem vērsta pieeja arī nodrošinās to, ka apmācības un procedūru izstrādes pamatā ir veicamais uzdevums tā dabiskajā vidē — tas palīdzēs optimizēt gan riska kontroli, gan rezultātus.

Drošības politikā ir noteikts drošības nozīmīgums un prioritātes, tostarp cilvēkfaktoru un organizatorisko faktoru integrēšana un drošības kultūras veicināšana.

Organizācija veicina pastāvīgu un kolektīvu modrību, vēršoties pret bezrūpību (“viss tiek kontrolēts”) un pārlietu vienkāršošanu (“drošībai pietiek ar procedūru ievērošanu”) un attīstot izzinošu attieksmi. Turklāt visi organizācijas dalībnieki zina, ka neatkarīgi no plānošanas un organizācijas kvalitātes, tehniskajiem šķēršļiem un procedūrām vienmēr var būt atšķirība starp gaidīto un reālo. Tiek izmantoti visi iespējamie avoti, lai atklātu un kopīgi analizētu situācijas, ko nav izdevies precīzi paredzēt.

Turklāt organizācijas saziņa par drošību atbilst vadības lēmumu realitātei.

Lai SMS darbotos efektīvi un nākotnē pilnveidotos, ir svarīgi, lai vadītāji parādītu saviem darbiniekiem un ieinteresētajām personām, ka viņi nosaka pozitīvu darba kārtību, pēc kuras var pārvaldīt drošību. Tiem darbiniekiem, kuri ieņem vadošus amatus, ir vislielākā ietekme uz organizācijas kultūru, un tāpēc ir būtiski, lai viņi varētu nodot pareizo vēstījumu tiem, kuri strādā viņu atbildībā. Vadītāju uzvedība visos organizācijas līmeņos un tas, cik lielu nozīmi viņi piešķir drošībai savos ikdienas lēmumos, būtiski ietekmē citu dalībnieku uzvedību viņu uzdevumu drošā izpildē. Vadītājiem arī ir jārada fiziskā un sociālā darba vide, kurā tiek droši veikts vadošais darbs.

2.1.3 Paskaidrojumi

“Augstākā līmeņa vadība” (**2.1.1. punkts**) šajā kontekstā ir personas, kuras pieņem lēmumus kā organizācijas “vadošais prāts”. Parasti šīs personas ir izpilddirektors, augstākā līmeņa vadības grupas locekļi, priekšsēdētājs un valdes locekļi. “Augstākā līmeņa vadībai” gan kā grupai, gan kā indivīdiem ir jāparāda līderība un apņēmība ievērot un īstenot drošības pārvaldības sistēmu.

Pietiekama uzmanība ir jāvelta drošības apdraudējumu (**2.1.1. punkta i) apakšpunkts**) līdzsvarošanai ar citiem uzņēmējdarbības riskiem, lai izvairītos no situācijas, ka vadība nosaka uzņēmējdarbības vajadzību prioritātes tā, ka pasliktinās drošības rādītāji. Augstākā līmeņa vadībai jānodrošina, ka mērķu sasniegšanā tiek uzturēti drošības rādītāji un tiek pārvaldīti riski, ciktāl tas ir praktiski iespējams. Pretrunīgi mērķi nedrīkstētu būt iemesls pretrunīgu uzdevumu noteikšanai indivīdiem, tādējādi radot drošības problēmas.

Integrēta cilvēkfaktoru un organizatorisko faktoru pieeja līderībā un vadībā nozīmē mērķu, prognožu un atbildības noteikšanu attiecībā uz drošības uzvedību visos organizācijas līmeņos un savlaicīgas atgriezeniskās saites un saziņas nodrošināšanu.

2.1.4 Pierādījumi

- Pastāv drošības politika un mērķi, un pastāv pierādījumi, ka šāda politika un mērķi ir pieejami un saprotami visiem darbiniekiem, un ir paskaidrots, kā tie iekļaujas citos uzņēmējdarbības procesos (**2.1.1. punkta a), b), g) un e) apakšpunkts**).
- Drošības politikā ir noteikts, ka ir svarīgi piemērot cilvēkfaktoru un organizatorisko faktoru pieeju visos ar drošību saistītajos procesos, lai organizācijā sasniegtu augstu drošības līmeni. Organizācija parāda, kā tiek pārvaldīti cilvēkfaktori un organizatoriskie faktori organizācijas procesos (**2.1.1. punkta c) apakšpunkts**).
- SMS un citu uzņēmējdarbības aktivitāšu saistība ir skaidri noteikta procedūrā vai organigrammā (**2.1.1. punkta e) un i) apakšpunkts**).
- Drošības politikā vai citos procesos ir pieejama informācija, kas apliecina, ka vadība ir apņēmusies nodrošināt un uzturēt pietiekamus resursus, lai SMS varētu darboties efektīvi (**2.1.1. punkta e) apakšpunkts**).
- Ir pierādījumi, ka vadītāji veicina pozitīvu drošības kultūru (**2.1.1. punkta j) apakšpunkts**).
- Ir pierādījumi, kas parāda, kā tiek nodrošināts, ka darbinieki saprot savus darba uzdevumus un pienākumus attiecībā uz drošību, un kā tas, ko viņi dara, ietekmē organizācijas spēju kontrolēt risku ar SMS starpniecību (**2.1.1. punkta d), f) un i) apakšpunkts**).
- Drošības politikā vai citā dokumentācijā ir pierādījumi, ka organizācija informē savus darbiniekus par to, cik svarīga ir viņu loma SMS praktiskās darbības nodrošināšanā, lai būtu iespējams jēgpilni kontrolēt riskus (**2.1.1. punkta e) apakšpunkts**).
- Pastāv procesi, kuros noteikts, kā ir jāpievēršas cilvēkfaktoriem un organizatoriskajiem faktoriem un kā tie ir jāpaziņo organizācijas iekšienē saistībā ar organizācijas uzņēmējdarbības mērķiem un organizatoriskiem procesiem, piemēram, projektiem, starpgadījumu un negadījumu izmeklēšanu,

riska analīzēm un citām ar drošību saistītām darbībām organizācijas personālam, darbuņēmējiem, partneriem un piegādātājiem (2.2.1. punkta c), d) un e) apakšpunkts).

- *Pastāv pierādījumi, ka vadība ir ieviesusi procesus, lai nodrošinātu, ka organizācijas darbuņēmēji pienācīgi ņem vērā cilvēkfaktorus un organizatoriskos faktorus (2.2.1. punkta c), d) un e) apakšpunkts).*

2.1.5 Pierādījumu piemēri

Ir iesniegta izpilddirektora parakstīta un datēta drošības politika, kurā ir skaidri norādīta vadības apņemšanās attiecībā uz drošību un drošības uzlabojumiem un tas, kā darbinieki ir iesaistīti drošības apdraudējuma pārvaldībā. Drošības politikā ir arī norādīts, kā tā tiks pārskatīta.

Organizācijai ir noteikts skaidrs tādu drošības mērķu kopums, kuri ir būtiski (Significant), izmērāmi (Measurable), sasniedzami (Achievable), reālistiski (Realistic) un ar noteiktu termiņu (Time bound) (SMART), un atsevišķā procedūrā ir izklāstīta skaidra metodika šo mērķu noteikšanai un to sasniegšanas vai nesasnēgšanas analīzei.

Skaidrs vadītāju paziņojums par to, kā tie sekmē pozitīvu drošības kultūru un kā personāls tiek iesaistīts un iesaistās šajā procesā.

Pārskats par sanāksmēm, ko organizē augstākā līmeņa vadība un kurās viens no darba kārtības standarta jautājumiem ir drošība, un šādu sanāksmju biežums.

Skaidrs paziņojums par organizācijas apņemšanos nodrošināt pietiekamus resursus, lai SMS varētu efektīvi darboties risku kontrolēšanai.

Organigrammā ir skaidri izklāstīts, kā darbojas SMS un kurš par ko atbild.

Jauna aprīkojuma, piemēram, jaunu vilcienu, izstrādē izmanto cilvēkfaktoru un organizatorisko faktoru pieeju. Tas nozīmē, ka, nosakot izstrādes prasības, tiek izmantota pašreizējo lietotāju pieredze, tiek analizēti uzdevumi, lai apzinātu kognitīvas un fizioloģiskas problēmas, tiek samazinātas iespējamās darbības kļūdas, izstrādē piemērojot pamatnostādnes par cilvēkfaktoriem, piemēram, dažādus ISO vai UIC standartus, tiek veikta darba slodzes un noguruma pārvaldības analīze, lai nodrošinātu, ka personāls spēj pildīt uzdevumus, tiek veikta riska analīze, lai apzinātu iespējamās problēmas, un tiek noteiktas problēmu novēršanas darbības. Tiek ņemti vērā vides faktori, piemēram, sniegs, karstums, lietus u. tml., kā arī sociālekonomiski faktori, piemēram, organizatoriskās prioritātes, iepirkums un valsts kultūra.

Vadība savās atskaitēs par braucieniem vai apmeklējumiem uz vietas, kuri saistīti ar drošību, parāda savu apņemšanos sekmēt pozitīvu drošības kultūru un vēlmi vadīt, rādot priekšzīmi.

2.1.6 Atsauces un standarti

- [Drošības kultūra](#) (SKYbrary)

2.1.7 Uzraudzības jautājumi

Nozīmīgi uzraudzības aspekti ir atšķirības apmērs starp jebkādiem politikas virzieniem un procedūrām, kas iesniegtas kā daļa no iepriekš minētajiem pierādījumiem, un uzraudzības laikā novēroto realitāti un tas, ciklāl organizācija ir informēta par šādu atšķirību.

Vadītāju patiesu apņemšanos veicināt SMS un drošības kultūru, kā arī darbinieku uzticību organizācijai uzraudzības laikā pārbauda, izvērtējot, kādi ir organizācijas ieviestie mehānismi, lai izprastu un attīstītu šādu kultūru un SMS.

Pārbaudīt, vai organizācija var parādīt, ka tā atvēl pietiekamus resursus drošības pārvaldības sistēmas izstrādei, īstenošanai, uzturēšanai un nepārtrauktai uzlabošanai.

Intervējot augstākā līmeņa vadību un citu personālu, pārbaudīt, kā vadība pauž apņemšanos uzlabot drošību. Noskaidro, cik bieži un kā augstākā līmeņa vadība sazinās ar personālu drošības jautājumos un/vai sekmē drošības kultūru (darbsemināri, forumi, specializētas drošības jautājumiem veltītas dienas u. tml.).

Pārbaudīt, vai augstākā līmeņa vadība sniedz kādus paziņojumus par mērķiem, proti, aicinājumus visiem darbiniekiem sniegt ieguldījumu mērķu sasniegšanā vai pateicības visiem darbiniekiem par darbības rādītāju uzlabošanu.

2.2 Drošības politika

2.2.1 Normatīvā prasība

2.2.1.	Augstākā līmeņa vadība izstrādā dokumentu, kurā aprakstīta organizācijas drošības politika un kas ir: <ul style="list-style-type: none">a) atbilstošs organizācijas dzelzceļa darbību veidam, iezīmēm un apjomam;b) organizācijas izpilddirektora (vai augstākā līmeņa vadības pārstāvja(-ju)) apstiprināts;c) aktīvi īstenots, paziņots un darīts pieejams visam personālam.
2.2.2.	Drošības politika: <ul style="list-style-type: none">a) ietver apņemšanos pakļauties visām juridiskajām un cita veida prasībām saistībā ar drošību;b) nodrošina sistēmu drošības mērķu izvirzīšanai un organizācijas drošības rādītāju izvērtēšanai salīdzinājumā ar šiem mērķiem;c) ietver apņemšanos kontrolēt no pašas organizācijas darbības izrietošos un citu radītos drošības apdraudējumus;d) ietver apņemšanos pastāvīgi uzlabot drošības pārvaldības sistēmu;e) tiek uzturēta saskaņā ar organizācijas uzņēmējdarbības stratēģiju un drošības rādītāju izvērtējumu.

2.2.2 Mērķis

Drošības politika ir svarīgs dokuments, kas parāda, kā organizācija pārvalda savus pienākumus drošības jomā, kā arī līderību un ieguldījumu pienācīgā drošības pārvaldībā. Pieteikuma iesniedzējam ir jāspēj parādīt, ka tam ir drošības politika, kas atbilst iepriekš izklāstītajām prasībām un īsumā apraksta riska kontroles pamatstruktūru.

2.2.3 Paskaidrojumi

Drošības politika ir vadības filozofijas formulējums, tāpēc šī sadaļa ir cieši saistīta ar 3.1. sadaļu. Piemēram, iepriekš minētajā normatīvajā prasībā nav tieši minēti cilvēkfaktori un organizatoriskie faktori.

Iepriekš minētā tiesību akta 2.2.1. punkta a) apakšpunktā, kur šī prasība attiecas uz infrastruktūras pārvaldītājiem, “veids” ir aizstāts ar “iezīmēm”.

2.2.4 Pierādījumi

- Dzelzceļa pārvadājumu uzņēmumam: izpilddirektora parakstīta rakstiska drošības politika, kurā ir atspoguļots darbības veids un apjoms, pierādīta atbilstība tiesību aktu prasībām un citām prasībām, paredzēti nepārtraukti uzlabojumi drošības jomā, kā arī paredzēta sistēma drošības mērķu noteikšanai (2.2.1. punkta a) un b) apakšpunkts), (2.2.2. punkta a)–c) apakšpunkts).*
- Infrastruktūras pārvaldītājam: izpilddirektora parakstīta rakstiska drošības politika, kurā ir atspoguļotas dzelzceļa pārvadājumu un infrastruktūras attīstības iezīmes un apjoms, pierādīta atbilstība tiesību aktu prasībām un citām prasībām, paredzēti nepārtraukti uzlabojumi drošības jomā un kura tiek izmantota drošības mērķu noteikšanai (2.2.2. punkta a)–c) apakšpunkts).*
- Abiem: informācija, kas pierāda, ka drošības politika ir paziņota visiem darbiniekiem (2.2.1. punkta c) apakšpunkts).*

- Informācija, kas apliecina, ka drošības politika tiek uzturēta tā, ka tā vienmēr ir saskaņota ar organizācijas uzņēmējdarbības stratēģiju **(2.2.2. punkta d) apakšpunkts)**.
- Pierādījumi, ka drošības politikā ir izteikta apņemšanās pārraudzīt drošības rādītājus un ka politika tiek *periodiski pārskatīta pēc drošības rādītāju analīzes*, grozīta pēc organizācijas drošības rādītāju pārskatīšanas, veicot salīdzināšanu attiecībā pret izvirzītajiem mērķiem **(2.2.2. punkta b) un d) apakšpunkts)**.

2.2.5 Pierādījumu piemēri

Izpilddirektora parakstīta un datēta drošības politika, kas precīzi atspoguļo darbības veidu, apjomu un iezīmes. Dokumentā ir izteikta apņemšanās pastāvīgi uzlabot SMS.

Drošības politika ir aktuāla, un ir noteikts tās pārskatīšanas cikls, kas atbilst uzņēmējdarbības stratēģijai.

Drošības mērķi ir saskaņoti ar drošības politikā izklāstīto misiju un redzējumu, un ir redzams, ka darbinieki apzinās to vērtību un tas pastiprina viņu apņemšanos tos sasniegt.

Drošības politikā ir informācija vai atsauces, kurās izklāstīts process politikas pārskatīšanai, lai noteiktu, vai tā ir jāgroza pēc organizācijas drošības rādītāju pārskatīšanas, tos salīdzinot attiecībā pret izvirzītajiem mērķiem.

Ir ieviests process drošības politikas paziņošanai ar organizācijas iekštīkla starpniecību un tās izvietojumam stratēģiski/funkcionāli svarīgās vietās.

2.2.6 Uzraudzības jautājumi

Uzraudzības laikā būs svarīgi pārbaudīt, cik efektīvi drošības politika ir paziņota visiem darbiniekiem, kā viņi ir to sapratuši un kāda realitātē ir tās loma organizācijas ievērotā drošības sistēmas noteikšanā. Galvenais jautājums ir, vai drošības politikas dokuments palīdz noteikt darba kārtību vai pastāv tikai tāpēc, ka to pieprasa tiesību akti.

Pārbaudīt, vai pēc izmaiņām organizācijas drošības rādītājos ir veikta drošības politikas pārskatīšana.

Pārbaudīt, vai drošības politika atspoguļo reālo situāciju organizācijā.

2.3 Organizatoriskās funkcijas, pienākumi, pārskatatbildība un pilnvaras

2.3.1 Normatīvā prasība

2.3.1.	Personālam, kura funkcijas ietekmē drošību (tostarp vadībai un citam personālam, kas pilda ar drošību saistītus uzdevumus), visos organizācijas līmeņos nosaka, dokumentē, piešķir un paziņo tā pienākumus, pārskatatbildību un pilnvaras.
2.3.2.	Organizācija nodrošina, ka personālam, kam deleģēti pienākumi ar drošību saistītu uzdevumu izpildē, ir pilnvaras, kompetence un attiecīgi resursi, kas ļauj pildīt uzdevumus, izvairoties no nelabvēlīgas ietekmes, kādu rada ar citām uzņēmējdarbības funkcijām saistīta darbība.
2.3.3.	Pienākumu deleģēšana ar drošību saistītu uzdevumu izpildē tiek dokumentēta un paziņota attiecīgajam personālam, akceptēta un izprasta.
2.3.4.	Organizācija apraksta 2.3.1. punktā minēto funkciju sadalījumu pa uzņēmējdarbības funkcijām organizācijā un attiecīgā gadījumā ārpus tās (sk. 5.3. Darbuzņēmēji, partneri un piegādātāji).

2.3.2 Mērķis

Šīs prasības mērķis ir nodrošināt, lai pieteikuma iesniedzējs radītu skaidru priekšstatu par organizācijas struktūru, kā arī par funkciju un pienākumu sadalījumu un uzturēšanu laika gaitā dažādos organizācijas līmeņos no vadošajiem darbiniekiem līdz augstākā līmeņa vadībai. Tas ir būtiski, lai varētu saprast, cik efektīvi organizācijas drošības pārvaldības sistēma kontrolē risku. Pieteikuma iesniedzējam ir jāparāda, kā notiek kompetentu darbinieku norīkošana darbību veikšanai, kā tiek nodrošināts, ka darbiniekiem ir skaidra izpratne par viņu funkcijām un pienākumiem, un kā darbiniekiem liek atskaitīties par viņu darbību.

2.3.3 Paskaidrojumi

Var būt atšķirīga izpratne par drošības pārvaldības noteikumiem ekspluatācijas līmenī un pārvaldības procesiem, kuriem būtu jāvirza drošības pārvaldības sistēma (piemēram, riska novērtēšanu, pārraudzību). To funkciju izklāsts, kas ir būtiskas drošības pārvaldības sistēmā (**2.3.1. punkts**), aptver ne tikai darbiniekus, kuri atbild par drošības procesu pārvaldību, piemēram, drošības vadītāju vai drošības darbinieku grupu, bet arī jebkuru darbinieku, kura darba uzdevumi ir saistīti ar drošību, piemēram, ekspluatācijas personālu, neatkarīgi no tā, vai šādi darbinieki ieņem vai neieņem vadības līmeņa amatus organizācijā (t. i., augstākā līmeņa vadītājus, tiešos vadītājus, citu personālu/darbiniekus/strādājošos).

Funkciju, pienākumu, pārskatatbildības un pilnvaru izklāstā (**2.3.1. punkts**) ir jābūt iekļautai ar drošību saistītas informācijas apmaiņai. Piemēram, ir jābūt norādītam, kurš atbild par novēlotas maiņas paziņojuma sniegšanu vilcienā vadītājiem (**sk. arī 4.4.1. un 4.4.2. punktu**).

SMS ir jāatbilst CSM SMS prasībām (1.1.1. punkta d) apakšpunkts), un augstākā līmeņa vadības pienākums ir nodrošināt SMS atbilstību minētajām prasībām. Augstākā līmeņa vadība var deleģēt dažus no saviem pienākumiem attiecīgiem darbiniekiem. Par darbības rezultātiem tiek ziņots saskaņā ar prasībām par vadības veiktu pārskatīšanu (6.3. punkts), ja attiecīgajiem darbiniekiem ir pienākums ziņot augstākā līmeņa vadībai par drošības pārvaldības sistēmas darbību.

“Ar drošību saistīti uzdevumi” (**2.3.1. punkts**) ir ne tikai uzdevumi, kas ietver tiešu drošības pārvaldību (t. i., drošībai kritiski uzdevumi, ko veic darbinieki, kad viņi kontrolē vai ietekmē vilciena kustību, kas var ietekmēt cilvēku veselību un drošību, kā noteikts SITS OPE). Tie ietver arī ar ekspluatāciju nesaistītus uzdevumus, kas ietekmē drošību.

“Deleģēšana” (**2.3.3. punkts**) ir pienākumu nodošana no augstāka uz zemāku pilnvaru līmeni, parasti lai paātrinātu organizācijas reakciju uz problēmām, kas rodas. Ar drošību saistītus pienākumus var deleģēt, t. i.,

nodot zemākam līmenim noteikto darba pienākumu jomā ar nosacījumu, ka šāda deleģēšana tiek dokumentēta. Pārskatatbildību par drošību nevar deleģēt. Tā paredz pienākumu personai, no kuras prasa atbildību, parādīt, ka tā ir apmierinoši izpildījusi savus ar drošību saistītos pienākumus, ja kaut kas netiek izdarīts, nedarbojas vai nesasniedz mērķi. Uzdevumu paziņošana un akceptēšana (**2.3.3. punkts**), ietverot ar drošību saistītus uzdevumus, ir daļa no parastā uzņēmējdarbības procesa, kas nosaka, kā notiek darbinieku atlase funkciju veikšanai, un šim procesam ir jābūt revidējamam.

Funkciju sadalījumu (**2.3.4. punkts**) var apliecināt, iesniedzot attiecīgu organizācijas shēmu vai organigrammu.

Vadībai ir jābūt pietiekamām zināšanām un izpratnei par cilvēkfaktoru un organizatorisko faktoru jautājumiem, lai nodrošinātu, ka vajadzības gadījumā tiek iesaistīti speciālisti. Cilvēkfaktoru un organizatorisko faktoru speciālistu funkcijām, pienākumiem un pārskatatbildībai ir jābūt noteiktai atbilstoši veicamajiem uzdevumiem (**2.3.3. punkts**).

Ir jābūt ieviestam procesam, lai nodrošinātu, ka personas var ziņot par gandrīz notikušiem negadījumiem, starpgadījumiem un negadījumiem, nebaidoties par represijām. Politika atbalsta indivīdu tiesības un pienākumus ziņot par drošības problēmām un nepieļauj aizskaršanu, iebiedēšanu, represijas vai diskrimināciju ziņošanas gadījumā. Taisnīgas kultūras panākumu pamatā ir uzticēšanās un atklātība organizācijā. Tā veidojas laika gaitā un ir atkarīga no vadības vēlmes veikt vispusīgu analīzi, ja ir notikuši negadījumi un starpgadījumi, kā arī vēlmes uzklaut un uzzināt, pirms tā rīkojas. Taisnīgas kultūras izveidē svarīga nozīme ir drošības problēmu konsekventai risināšanai.

2.3.4 Pierādījumi

- *Organigramma un attiecīgs paskaidrojošs teksts, kurā atspoguļota organizācijas struktūra, attiecīgie ar drošību saistītie pienākumi un tas, kā ir veidota drošības pārvaldības sistēma un kā tā ir saistīta ar organizācijas kontekstu (**2.3.1. punkts**), (**2.3.4. punkts**).*
- *Citas informācijas uzskaitījums, kurā ir sīki izklāstīti ar drošību saistītie pienākumi organizācijas struktūrā (**2.3.1. punkts**), (**2.3.3. punkts**).*
- *Pierādījumi, ka attiecībā uz visiem darbiniekiem ir ieviesta un tiek uzturēta kompetences pārvaldības sistēma, kas novērtē uzdevumu atbilstību uzdotajiem darba pienākumiem, kompetencei un resursiem (**2.3.2. punkts**).*
- *Pierādījumi no kompetences pārvaldības sistēmas vai citām procedūrām, ka organizācija nodrošina, ka funkcijas un pienākumi tiek paziņoti darbiniekiem un viņi tos akceptē un skaidri saprot un ka no darbiniekiem tiek prasīta atbildība par pienākumu izpildi (**2.3.3. punkts**).*
- *Ekspluatācijas un tehniskās apkopes pienākumu apraksts, tostarp to prasību definīcija, kuras darbiniekiem un attiecīgā gadījumā darbuzņēmējiem ir jāizpilda (**2.3.4. punkts**).*
- *Cilvēkfaktoru un organizatorisko faktoru stratēģijā ir jābūt parādītām prasībām, kas nosaka, kad un kā tiek piesaistīti cilvēkfaktoru un organizatorisko faktoru speciālisti un kādi ir viņu uzdevumi un pienākumi (**2.3.1. punkts**), (sk. arī **4.6. punktu**).*

2.3.5 Pierādījumu piemēri

Organigramma, papildināta ar tekstu, lai vērtētājs var saprast, kā SMS ir strukturēta un kā tās dažādās daļas ir savstarpēji saistītas.

Process, kurā izklāstīts, kāds ir ar drošību saistīto pienākumu sadalījums un kur ir atļautas deleģēšanas pilnvaras, ar dažiem procesa darbības piemēriem.

Tādu amatu aprakstu piemēri, kas ietver ar drošību saistītus uzdevumus, tostarp apraksti par amatiem, kas nav tieši saistīti ar ekspluatāciju, taču netieši ietekmē ekspluatācijas norisi (t. i., darbu piešķiršana, ekspluatācijas plānošana un ar ekspluatāciju saistītas informācijas sniegšana darbiniekiem, ekspluatācijas uzraudzība).

Atsauce uz kompetences pārvaldības sistēmu (CMS), norādot informāciju par to, kā tā ir strukturēta, un saites, kur ir atrodama sīkāka informācija.

Ir norādīts atgriezeniskās saites process, ko izmanto, lai nodrošinātu, ka informācija, ko nodod no organizācijas augstākā līmeņa visiem zemākajiem līmeņiem, ir skaidri saprotama.

Procedūra(-as), ko izmanto, lai noteiktu, kāda kompetence un resursi ir vajadzīgi, lai atbalstītu ar drošību saistītu uzdevumu un pienākumu izpildi visos hierarhijas līmeņos.

Cilvēkfaktoru un organizatorisko faktoru stratēģija parāda, kā šie faktori tiek integrēti procesos un projektos. Kompetence un darbības saistībā ar cilvēkfaktoriem un organizatoriskajiem faktoriem ir atbilstošas organizatoriskā procesa vai projekta apmēram. Cilvēkfaktoru speciālistu funkcijas, pienākumi un pārskatatbildība, kā arī viņu iesaistīšanas posmi ir noteikti procesā vai projekta plānā.

2.3.6 Atsauces un standarti

- [Pārskatatbildība un pienākumi saistībā ar drošību](#) (SKYbrary)

2.3.7 Uzraudzības jautājumi

Uzraudzības jomā galvenā nozīme ir “pakāpei”. Jautājums, uz kuru jāatbild, ir “ciktāl sniegtā informācija atspoguļo reālo situāciju praksē?”

Lai atbildētu uz lielāko daļu šajā sadaļā uzdoto jautājumu, būs jāizvērtē kompetences pārvaldības sistēmas darbība.

2.4 Apspriešanās ar personālu un citām pusēm

2.4.1 Normatīvā prasība

- | |
|---|
| <p>2.4.1. Izstrādājot, uzturot un uzlabojot drošības pārvaldības sistēmu, ar personālu, tā pārstāvjiem un ieinteresētajām trešām personām attiecīgā gadījumā atbilstoši apspriežas par attiecīgajām daļām, kas ietilpst to atbildības jomā, tostarp ekspluatācijas procedūru drošības aspektiem.</p> <p>2.4.2. Organizācija veicina apspriešanos ar personālu, šādā nolūkā nodrošinot metodes un līdzekļus personāla iesaistei, reģistrējot personāla viedokli un sniedzot atbildi uz to.</p> |
|---|

2.4.2 Mērķis

Pieteikuma iesniedzējam ir jāiesniedz pierādījumi, ka tas aktīvi iesaista savu personālu (vai tā pārstāvjus), kā arī ārējās ieinteresētās personas drošības pārvaldības sistēmas izmantošanā un pilnveidošanā, lai kontrolētu riskus laika gaitā. Tas arī ļaus vērtētājiestādei spriest, kāda ir drošības kultūra organizācijā un cik aktīvi organizācija iesaista attiecīgās trešās personas drošības pārvaldībā jomās, kur notiek riska dalīšana.

Organizācija atzīst, ka nevienam atsevišķam indivīdam nav visas informācijas, kas vajadzīga drošības ilgtspējīgai pārvaldībai. Procesa eksperti, drošības eksperti, atbalsta dienesti, vadošie darbinieki, vadība un pārziņi, arodbiedrības, ārējie darbuzņēmēji pārzina un izmanto informāciju, kas ir būtiska drošībai. Ir jādod viņiem iespēja tikties, apspriesties un izteikt savu viedokli, lai gūtu maksimālu izpratni par reālo situāciju darbvietā. Īpaša uzmanība ir vajadzīga organizatoriskajās saskarnēs starp dienestiem, departamentiem un organizācijām. Ir jāveicina ideju un informācijas apmaiņa par riska, negadījumu un starpgadījumu analīzi un risināšanu.

Iesaistīšanos drošībai kritiskas informācijas paziņošanā un līdzdalību bīstamu situāciju un starpgadījumu analīzē veicina uzticību radoša vide. Turklāt riska novērtēšanā, tehnisku iekārtu projektēšanā un pārveidošanā, kā arī jaunu procedūru izstrādē jau agrīnā posmā jācenšas iesaistīt ekspluatācijas personālu.

2.4.3 Paskaidrojumi

Ar šādām ārējām personām (**2.4.1. punkts**) var apspriesties par jautājumiem saistībā ar pārvaldības sistēmu. Piemēram, darbuzņēmēji var būt atbildīgi par dažiem ar drošību saistītiem uzdevumiem, piemēram, vilcienu sagatavošanu vai infrastruktūras uzturēšanu. Kad veic riska novērtēšanu par vilcienu sagatavošanas procedūru vai infrastruktūras uzturēšanu, laba prakse ir iesaistīt procesā darbuzņēmējus.

“Ārējās personas” ir organizācijas, kam ir saskarsme ar pieteikuma iesniedzēju, piemēram, darbuzņēmēji, partneri, piegādātāji, attiecīgās valsts aģentūras, vietējās iestādes vai neatliekamās palīdzības dienesti.

Pozitīvas drošības kultūras attīstību veicina kvalitatīva un savlaicīga attiecīgās informācijas paziņošana tiem, kuriem tā ir jāsaņem.

2.4.4 Pierādījumi

- Pieteikuma iesniedzējam ir jāsniedz informācija par procesu, ko izmanto, lai apspriestos ar personālu (vai tā pārstāvjiem) un attiecīgajām ārējām ieinteresētajām personām, ietverot arī informāciju par to, kā šādu apspriežu rezultātā tiek ieviestas izmaiņas drošības pārvaldības sistēmā vai īpašās ekspluatācijas procedūrās (**2.4.1. punkts**), (**2.4.2. punkts**).
- Pieteikuma iesniedzējam ir jāsniedz informācija par ieviesto sistēmu, ko izmanto personāla informēšanai par apspriežu rezultātu (**2.4.2. punkts**).

2.4.5 Pierādījumu piemēri

Process vai procedūra, ko izmanto, lai apspriestos ar personālu (un — attiecīgā gadījumā — tā pārstāvjiem) un ieinteresētajām personām SMS izstrādē.

Tādu sanāksmju protokolu piemēri, ko rīko, lai apspriestos ar personālu (un/vai tā pārstāvjiem), protokolos norādot arī sanāksmju iznākumu.

Piemēri par to, kā notiek personāla viedokļu un ierosinājumu apkopošana izmaiņu pārvaldības procesā (t. i., par ekspluatācijas procedūras projektu, grozīšanu vai jaunu procedūru) un kā tos ņem vērā.

Ir sniegts dokuments/procedūra, kas apliecina, kā ekspluatācijas personāls, kura darbs būs saistīts ar jaunu vai uzlabotu tehnisko sistēmu, tiek iesaistīts darba agrīnā posmā (plānošanā un izstrādē), lai apkopotu viedokļus, piemēram, par cilvēka-mašīnas saskarni.

Pastāv procedūras, kurās noteikts, kā jāpievēršas cilvēkfaktoriem un organizatoriskajiem faktoriem un kā organizācijas iekšienē jāpaziņo rezultāti saistībā ar organizācijas uzņēmējdarbības mērķiem un organizatoriskiem procesiem, piemēram, projektiem, starpgadījumu un negadījumu izmeklēšanu, riska analīzēm un citām ar drošību saistītām darbībām personālam, darbuzņēmējiem, partneriem un piegādātājiem.

Organizācijai ir skaidri jāformulē, kas tiek gaidīts un kāda ir vajadzīgā rīcība attiecībā uz drošību. Organizācijas prioritātes ir saskaņotas, lai izvairītos no pretrunīgiem mērķiem. Ir aprakstīts process darbību plānošanai, risku novērtēšanai un kontrolēšanai, piemēram, izmantojot konservatīvu lēmumu pieņemšanu, lai nodrošinātu, ka drošību neapdraud citas uzņēmējdarbības intereses. Drošības mērķi ir saistīti ar drošības kultūru. Vadība uzņemas aktīvu lomu vajadzīgo drošības kultūras izmaiņu plānošanā un īstenošanā.

2.4.6 Uzraudzības jautājumi

Apspriedēm ar attiecīgo iekšējo un ārējo personālu un tā iesaistīšanai ir svarīga nozīme, lai varētu nodrošināt, ka personas, kurām ir attiecīga pieredze, spēj pozitīvi ietekmēt organizācijas drošības pārvaldības sistēmu.

Uzraudzībai šajā jomā ir jābūt vērstai uz ierakstiem, kā notiek apspriešanās ar personālu un ārējām personām un kā to viedokļi tiek ņemti vērā, pievēršoties arī ierakstiem par SMS izmaiņām, kas notikušas šajā jomā.

Īpaša uzmanība ir jāpievērš tam, kā tiek sniegta atgriezeniskā saite un kāda mācība tiek gūta.

Labāka dzelzceļa sistēma
sabiedrībai

3 Plānošana

3.1 Rīcība riska novēršanai

3.1.1 Normatīvā prasība

3.1.1. Riska novērtējums

3.1.1.1. Organizācija:

- (a) apzina un analizē visus ekspluatācijas (tostarp cilvēka veiktspējas), organizatoriskos un tehniskos riskus, kas attiecas uz organizācijas veikto darbību veidu ([iezīmēm](#)), apjomu un lauku. Šādi riski ietver vismaz riskus, kas izriet no cilvēkfaktoriem un organizatoriskajiem faktoriem, tādiem kā darba slodze, darba procesa plānošana, nogurums vai procedūru piemērotība, kā arī citu ieinteresēto personu darbības (sk. 1. Organizācijas konteksts);
- (b) izvērtē a) apakšpunktā minētos riskus, šādā nolūkā piemērojot attiecīgas riska novērtēšanas metodes;
- (c) izstrādā un ievieš drošības pasākumus un nosaka ar tiem saistītos pienākumus (sk. 2.3. Organizatoriskās funkcijas, pienākumi, pārskatatbildība un pilnvaras);
- (d) izstrādā drošības pasākumu efektivitātes uzraudzības sistēmu (sk. 6.1. Uzraudzība);
- (e) atzīst nepieciešamību attiecīgā gadījumā sadarboties ar citām ieinteresētajām personām (piemēram, dzelzceļa pārvadājumu uzņēmumiem, infrastruktūras pārvaldītājiem, ražotāju, tehniskās apkopes nodrošinātāju, par tehnisko apkopi atbildīgo struktūru, dzelzceļa ritekļa turētāju, pakalpojumu sniedzēju un iepirkuma struktūru) jautājumos par riska dalīšanu un pienācīgu drošības pasākumu ieviešanu;
- (f) par riskiem paziņo personālam un iesaistītajām trešām personām (sk. 4.4. Informācija un saziņa).

3.1.1.2 Novērtējot risku, organizācija ņem vērā nepieciešamību noteikt, nodrošināt un uzturēt drošu darba vidi, kas atbilst piemērojamajiem tiesību aktiem, jo īpaši Padomes Direktīvai 89/391/EEK.

3.1.2. Izmaiņu plānošana

3.1.2.1. Pirms izmaiņu ieviešanas (sk. 5.4. Izmaiņu pārvaldība) organizācija saskaņā ar Regulā (ES) Nr. 402/2013 noteikto riska pārvaldības procesu apzina iespējamās drošības apdraudējumus un attiecīgus drošības pasākumus (sk. 3.1.1. Riska novērtējums), tostarp ņem vērā no paša izmaiņu procesa izrietošos drošības apdraudējumus.

3.1.2 Mērķis

Šī prasība attiecas uz SMS būtību — tās mērķis ir panākt, lai pieteikuma iesniedzējs parāda, kā tā sistēmas identificē un kontrolē riskus, kas rodas. Tā arī nosaka, ka pieteikuma iesniedzējam ir jāparāda, kā tas riska novērtējuma rezultātus izmanto praksē riska kontroles uzlabošanai un kā tos pārbauda laika gaitā. Ir svarīgi atcerēties, ka šī prasība neattiecas tieši uz izmaiņu radīto risku pārvaldību (uz to attiecas cita prasība), bet ir saistīta ar to. Jānorāda, ka pastāv īpaša prasība risku novērtēšanas gaitā pievērsties ar cilvēka veiktspēju saistītiem jautājumiem, piemēram, darba uzdevuma izstrādei un noguruma riska pārvaldībai.

Tas, kā šī informācija tiek organizēta un paziņota kā daļa no SMS, pieteikuma iesniedzējam ir jāizklāsta pieteikumā, un saturam ir jāatspoguļo riski, kas rodas organizācijai, ņemot vērā tās darbības veidu, apjomu un jomu (sk. organizācijas kontekstu). Jāņem vērā gan riski, par kuriem atbildību uzņemas pieteikuma iesniedzējs, gan riski, kas izriet no trešo personu darbības.

Visā organizācijā vienotu izpratni, kā novērst būtiskus riskus, uzskata par prioritāti labai drošības pārvaldībai. Tas, ka kāds scenārijs īstenojas reti, nedrīkst būt iemesls to ignorēt. Turklāt, lai nodrošinātu riska novērtēšanai izvēlēta scenārija reālistiskumu salīdzinājumā ar reālām darbībām, ieguldījumu drošības analīzē un riska novērtēšanā sniedz gan drošības pārvaldības eksperti, gan operatori, kuru atbildībā ir vissarežģītākā uzņēmējdarbības daļa. Šādu novērtējumu rezultātus pieejamā un saprotamā formātā paziņo visiem dalībniekiem, kuri sniedz ieguldījumu drošībā. Direktori un vadība veicina apspriedes par būtiskajiem riskiem, kas jāpārvalda, lai nodrošinātu vienotu izpratni un informētību. Turklāt būtisku risku esamība tiek uzsvērtā visā sistēmas dzīves ciklā.

3.1.3 Paskaidrojumi

Pieteikuma novērtējuma nolūkos pieteikuma iesniedzējam ir jāpierāda, kā tas izpilda Padomes Direktīvu 89/391/EEK un ar to saistītos noteikumus. Novērtējums tiks vērst uz pierādījumiem par šo jautājumu pārvaldību, nevis uz šiem jautājumiem kā tādiem. Tādus jautājumus kā noguruma vai stresa pārvaldība, kā arī fiziskās un psiholoģiskās piemērotības pārbaude var aplūkot kā juridiskus jautājumus darba aizsardzības kontekstā, tomēr tie mijiedarbojas ar kompetences pārvaldības sistēmu (piemēram, attiecībā uz apmācību pēc ilgas prombūtnes) un darba uzdevumu piešķiršanu (darbinieki jānorīko konkrēta darba veikšanai, ja ir pārliecība par viņu piemērotību darbam), kā noteikts SITS OPE.

Iepriekš minētā tiesību akta 3.1.1.1. punkta a) apakšpunktā, kur šī prasība attiecas uz infrastruktūras pārvaldītājiem, attiecībā uz novērtējumu “veids” ir aizstāts ar “ieziņēm”.

“Darbības” (**3.1.1.1. punkta a) apakšpunkts**) šajā dokumentā nozīmē gan darbību, ko ieinteresētās personas (darbuuzņēmēji, piegādātāji un citas) veic pieteikuma iesniedzēja vārdā vai kopā ar to, gan arī aktīvus, ko izmanto šādu darbību atbalstam. Galvenais ir, lai pieteikuma iesniedzējs parādītu, ka tas ir ieviesis stabilu riska novērtēšanas procesu un ka tiek novērsti visi attiecīgie riski. Atbilstošā un pamatotā gadījumā organizācijai arī jāņem vērā daži citi riski (piemēram, hidroģeoloģiskie riski, riski uz pārbrauktuvēm, pa vilcieniem mesti akmeņi, piekļuves noteikumu pārkāpēji). Tomēr šie jautājumi ir saistīti ar ekspluatācijas riskiem (jo tie visi ietekmē vilcienu darbību), un ir iespējams, ka tie ir saistīti ne tikai ar cilvēku veikspēju.

“Citas ieinteresētās personas” ir gan organizācijas, gan indivīdi. Šādas personas var būt nesaistītas ar dzelzceļa sistēmu (**1.1.1. punkta c) apakšpunkts**).

Izmaiņas var būt un var nebūt saistītas ar drošību (**3.1.2.1. punkts**). Jebkuru ar drošību saistītu izmaiņu ietekme ir jānovērtē, un ir jānosaka atbilstoši drošības pasākumi, lai samazinātu saistītos riskus līdz pieņemamam līmenim. Arī izmaiņu pārvaldības procesa īstenošana var radīt drošības apdraudējumus, jo īpaši, ja tiek nolemts atlikt noteiktu izmaiņu īstenošanu, kad ir daļēji vai pilnīgi jāizvairās no cita drošības apdraudējuma rašanās. Tomēr riska pārvaldība (**3.1.1.1. punkts**) neattiecas tikai uz izmaiņu pārvaldību. Kopumā organizācijai ir jānodrošina pienācīga pārvaldība drošības apdraudējumiem saistībā ar tās darbību. Tāpēc vajadzība apzināt, pārvaldīt un kontrolēt šādus drošības apdraudējumus kā daļu no pieteikuma iesniedzēja SMSpārsniedz izmaiņu pārvaldības un CSM riska noteikšanai un novērtēšanai piemērošanas darbības jomu.

CSM riska noteikšanai un novērtēšanai ir piemērojama visu tehnisko, ekspluatācijas vai organizatorisko izmaiņu gadījumā (attiecībā uz organizatoriskām izmaiņām — ja tām ir sekas, kas skar ekspluatāciju vai tehnisko apkopi). Attiecībā uz katrām ar drošību saistītajām izmaiņām pieteikuma iesniedzējam/ierosinātājam vispirms ir jāizlemj, vai izmaiņas ir būtiskas (vai nav). Ja uzskata, ka izmaiņas ir būtiskas, tam jāparāda, ka ar izmaiņām saistītie riski ir pieņemami, izmantojot CSM izklāstītos principus, un

ka no šādas parādīšanas izrietošās prasības ir efektīvi īstenotas sistēmā, kurā tiek ieviestas izmaiņas. Tad veikto riska novērtējumu novērtē neatkarīgā novērtējumā vai arī to novērtē atzīta struktūra, kas sagatavo ziņojumu par analīzes pieņemamību vai nepieņemamību. VDI ņem vērā šādus ziņojumus savos uzraudzības pasākumos, bet tās nevar apstrīdēt ziņojuma rezultātus, ja vien tām nav iemesla uzskatīt, ka riska novērtēšanas process nav noritējis, kā pienākas. Ja izmaiņas ir saistītas ar drošību, bet nav būtiskas, pieteikuma iesniedzējam/ierosinātājam ir jādokumentē savs lēmums un tik un tā jāveic izmaiņu riska novērtēšana atbilstoši SMS riska pārvaldības procesam. Šādā gadījumā pieteikuma iesniedzējam ir pienākums izvēlēties atbilstošās riska novērtēšanas metodes, lai pamatotu, ka tā ieviestie riska kontroles pasākumi ir atbilstoši saistīto risku ierobežošanai līdz pieņemamam līmenim. Jānorāda, ka, lai gan CSM-REA piemērošana ir atkarīga no tā, vai izmaiņas ir būtiskas vai nav, organizācija varētu izvēlēties piemērot CSM attiecībā uz riska noteikšanu un novērtēšanu jebkurā gadījumā, piemēram, ja tai šķiet, ka komerciālu vai sociālu apsvērumu dēļ saistībā ar izmaiņām ir pamatoti veikt organizācijas paveiktā darba neatkarīgu novērtējumu.

CSM riska noteikšanai un novērtēšanai ietver sešus kritērijus, kas ir jāizvērtē, nosakot “būtiskumu”. Tie ir šādi:

- **atteices sekas** — *ticams sliktākā gadījuma scenārijs novērtējamās sistēmas atteices gadījumā, ņemot vērā drošības šķēršļu esamību ārpus sistēmas;*
- **izmaiņu īstenošanā izmantotie jauninājumi** — *šis kritērijs attiecas gan uz to, kas ir inovatīvs dzelzceļa nozarē, gan uz to, kas ir jauns tikai organizācijai, kura īsteno izmaiņas;*
- **izmaiņu sarežģītība;**
- **pārraudzība** — *nespēja pārraudzīt īstenotās izmaiņas visā sistēmas dzīves ciklā un veikt attiecīgus ieviešanas pasākumus;*
- **atgriezeniskums** — *nespēja atgriezties pie sistēmas, kāda tā bija pirms izmaiņām, un*
- **papildināmība** — *izmaiņu būtiskuma novērtējums, ņemot vērā visus nesenos ar drošību saistītos novērtējamās sistēmas pārveidojumus, kas nav atzīti par būtiskiem.*

Šie elementi ir jāizmanto, lai novērtētu, uz kāda pamata ir pieņemti organizāciju lēmumi par būtiskumu atbilstoši CSM-REA.

Lai gan riska pārvaldības process, kas noteikts CSM riska noteikšanai un novērtēšanai, ir piemērojams ar drošību saistītu būtisku izmaiņu gadījumā, minētajā noteikumā paredzētie principi, kas ir riska pārvaldības procesa pamatā, ir ierasta prakse attiecībā uz riska pārvaldību, tāpēc tos var piemērot visās citās situācijās, kad ir vajadzīga riska novērtēšana.

Pastāv sistemātiska pieeja drošībai kritisku darba uzdevumu un procesu identificēšanai, un drošībai kritisku darba uzdevumu analīzei izmanto metodes no cilvēkfaktoru un organizatorisko faktoru jomas, piemēram, uzdevumu analīzi, HUA (hierarhisko uzdevumu analīzi), TUA (tabulāro uzdevumu analīzi). Lai izvēlētos un piemērotu atbilstošās metodes, jāizmanto profesionālu cilvēkfaktoru un organizatorisko faktoru speciālistu zināšanas.

Riska novērtēšanas procesā ir jāapraksta cilvēkfaktoru un organizatorisko faktoru speciālistu iesaistīšana un attiecīgās lietotāju un citu ieinteresēto personu kompetences. Piemēram, tas varētu būt apraksts par to, ciktāl cilvēkfaktoru un organizatorisko faktoru speciālistiem ir jābūt iesaistītiem riska analīzē un kāds ir vajadzīgais cilvēkfaktoru un organizatorisko faktoru kompetences līmenis.

Ir aprakstītas atbilstošās metodes cilvēkfaktoru un organizatorisko faktoru integrēšanai riska novērtēšanā, piemēram, uzdevumu analīze, izmantojamības analīze, simulācija, bīstamības un operatīvās darbības analīze (HAZOP) attiecībā uz cilvēkiem, izvērstās diagrammas metode.

3.1.4 Pierādījumi

- *Pieteikuma iesniedzējam ir jāuzrāda pierādījumi, kas apliecina, ka tas ir ieviesis riska novērtēšanas procesu (arī izmantotās metodikas, iesaistītā personāla un jebkuras veiktās apstiprināšanas vai*

pārbaudes apraksts), aptverot gan riskus, kas identificēti kā būtiskas izmaiņas atbilstoši CSM riska noteikšanai un novērtēšanai (Komisijas Īstenošanas regula (ES) Nr. 402/2015), gan riskus, ko uzskata par nebūtiskiem, bet kas tik un tā jākontrolē, un ka process aptver visus ekspluatācijas, organizatoriskos un tehniskos riskus (3.1.1.1. punkta a) un b) apakšpunkts).

- Pierādījumi, ka riska novērtējumos ir ņemti vērā cilvēkfaktoru un organizatorisko faktoru jautājumi. Cilvēkfaktoru un organizatorisko faktoru stratēģijā ir jāparāda, kā un kad cilvēkfaktori un organizatoriskie faktori ir riska novērtēšanas procesā integrēta daļa, un jāpierāda atbilstošu metožu un kompetences izmantošana (3.1.1.1. punkta a) apakšpunkts).
- Pierādījumi par līdzekļiem, ko izmanto, lai vajadzības gadījumā riska novērtēšanas procesā iesaistītu attiecīgās trešās personas, un par to, kā tiek pārvaldīti no trešām personām izrietoši riski, kas skar dzelzceļa pārvaldījumu uzņēmuma vai infrastruktūras pārvaldītāja darbības (3.1.1.1. punkta a), e) un f) apakšpunkts).
- Pierādījumi, ka pieteikuma iesniedzējs ir ieviesis procesu riska kontroles pasākumu izstrādei un īstenošanai, norādot arī, kuram ir pienākums nodrošināt to izpildi (3.1.1.1. punkta c) apakšpunkts).
- Pieteikuma iesniedzējam ir jānorāda, kā tas iesaista attiecīgo personālu riska novērtēšanā un saistītajos kontroles pasākumos un kā personālam paziņo šādas novērtēšanas un pasākumu rezultātus (3.1.1.1. punkta f) apakšpunkts).
- Pieteikuma iesniedzējam ir jāparāda, kā tas pārrauga savu riska kontroles pasākumu efektivitāti un kā vajadzības gadījumā tiek atjaunināti procesi un procedūras (3.1.1.1. punkta d) apakšpunkts).
- Iesniegtajos pierādījumos pieteikuma iesniedzējam ir jānorāda, kā tas ņem vērā vajadzību ievērot citus piemērojamos tiesību aktus, piemēram, tos, kas pieņemti atbilstoši Padomes Direktīvai 89/391/EEK (3.1.1.2. punkts).
- Pieteikuma iesniedzējs iesniedz pierādījumus, lai saistībā ar savu izmaiņu pārvaldības procesu parādītu, ka jebkuru izmaiņu ietekme tiek sistemātiski izvērtēta. Tas nozīmē, ka tiek izmantota riska novērtēšana, izmantojot arī CSM riska noteikšanai un novērtēšanai, lai apzinātu riskus un vajadzīgos kontroles pasākumus. Pieteikuma iesniedzējs arī iesniedz pierādījumus, ka izmaiņu pārvaldības procesā noteiktie kontroles pasākumi ir īstenoti (3.1.2.1. punkts).

3.1.5 Pierādījumu piemēri

Riska novērtēšanas process vai procedūra, pēc vajadzības norādot, kā un kad tiek izmantota atteices režīmu un rezultātu analīze (FMEA), bīstamības un operatīvās darbības analīze (HAZOP) vai citas metodes, lai atbalstītu kontroles pasākumu īstenošanu riska novēršanai.

Tādi pierādījumi kā apdraudējumu reģistrs, kas apliecina, ka organizācijā ir ieviests process apdraudējumu sistemātiskai novērtēšanai, kas ir pirmais solis riska pārvaldībā, kurā ir iekļauti pārraudzības rezultāti un kurš tiek nekavējoties atjaunināts, kad konstatē jaunus riskus, papildināts ar attiecīgu informāciju par drošības pasākumiem, kas noteikti, lai kontrolētu risku (piemēram, tehnisko aprīkojumu, ekspluatācijas procedūrām, personāla apmācību).

Pārskats par procesa elementiem, kas nosaka, kā riska novērtēšanas procesā tiek ņemti vērā cilvēkfaktori un kā vajadzības gadījumā tiek iesaistītas trešās personas.

Procedūra riska novērtējuma rezultātu paziņošanai darbiniekiem, vajadzības gadījumā ar ilustratīviem piemēriem.

Procedūra, ko izmanto, lai izpildītu citus attiecīgus ES tiesību aktus, piemēram, Padomes Direktīvu 89/391/EEK, ciktāl uz riskiem saistībā ar personālu (nāve, īslaicīgi vai pastāvīgi savainojumi, gandrīz notikuši negadījumi) var attiecināt darba aizsardzības tiesisko regulējumu, tomēr kontroles pasākumiem ir jābūt iekļautiem ekspluatācijas noteikumos vai jāpapildina šādi noteikumi.

Norāde par procesu, ko izmanto, lai nodrošinātu, ka katrai personāla kategorijai deleģētie ar drošību saistītie uzdevumi ir izstrādāti tā, ka:

- *izpildāmo uzdevumu apjoms nav pārmērīgs laikā, kad tiek veikts ar drošību saistīts uzdevums;*
- *ja ar drošību saistītie uzdevumi tiek apvienoti, organizācija spēj pierādīt, ka tiek saglabāts drošības līmenis;*
- *nav pretrunu starp to uzdevumu izpildi, kas saistīti ar drošību, un citu personālam uzdotu mērķu izpildi (atbilstoši 2.1.1. punkta j) apakšpunktam).*

Pastāv cilvēkfaktoru un organizatorisko faktoru stratēģija, kas ir saistīta ar riska novērtēšanas procesiem. Tas parāda, ka tiek izmantoti riska analīzes rezultāti un ka tiek īstenoti un izvērtēti drošības uzlabošanas pasākumi.

3.1.6 Atsauces un standarti

- [Aģentūras rokasgrāmata par to, kā piemērot CSM riska noteikšanai](#)
- [Pielaujamā riska kritēriji tehniskām sistēmām un ekspluatācijas procedūrām, ko izmanto dažādās nozarēs](#)
- [Pamatnostādnes par to, kā īstenot Regulu \(ES\) 2015/1136 par saskaņotiem projektēšanas mērķiem \(CSM DT\) saistībā ar CSM riska noteikšanai](#)
- ISO 31000:2009 "Riska pārvaldība"
- ISO 31010:2009 "Riska pārvaldība. Riska novērtēšanas metodes"

3.1.7 Uzraudzības jautājumi

Veicot uzraudzību, ir jāpārlicinās, ka drošības pārvaldības sistēmas pamatā ir riska novērtēšanas process, tāpēc ir jābūt iespējai intervijās un dokumentācijas un procesu pārbaudēs noskaidrot, vai tā patiešām ir. Saistībā ar to svarīgi ir uzraudzības konstatējumi, kam būs būtiska nozīme, nākotnē atjaunojot vienoto drošības sertifikātu vai drošības atļauju. Turklāt jebkuri riska novērtēšanas procesu uzraudzībā gūtie konstatējumi vajadzības gadījumā ir jāizmanto kā ievaddati VDI uzraudzības stratēģijā.

Kā ievaddatus vēlākai uzraudzībai var izmantot šādu informāciju:

- *apdraudējumu uzskaitījums;*
- *riska analīzes rezultāti, tostarp — attiecīgā gadījumā — riska novērtēšanas struktūras vai struktūru ziņojumi;*
- *riska novērtēšanas metožu (piemēram, FMECA, FTA, ETA, HAZOP) izmantošanas pamatojums, tostarp tas, kā tiek noteikti riska novērtēšanas kritēriji un apdraudējuma smaguma pakāpe un iespējamība;*
- *attiecīgā gadījumā — bīstamo notikumu klasifikācija atbilstoši tēmai, sekām vai cēloņiem (piemēram, apdraudējumu pagaidu saraksts).*

Darbiniekiem, kuru pienākumi ir saistīti ar riska novērtēšanu, ir jāzina, kāda ir viņu funkcija un kāds ir procesa nozīmīgums, un ir jābūt kompetentiem īstenot procesu efektīvi.

Ir ļoti būtiski izskatīt vairākus riska novērtēšanas piemērus, jo tie ļaus secināt, vai riski tiek pienācīgi ņemti vērā, izmantojot attiecīgu metodiku. Tad apskatē uz vietas ir jāpārlicinās, vai identificētie kontroles pasākumi ir ieviesti praksē.

3.2 Drošības mērķi un plānošana

3.2.1 Normatīvā prasība

- 3.2.1. Lai uzturētu un iespēju robežās uzlabotu drošības rādītājus, organizācija izstrādā drošības mērķus attiecīgajām funkcijām attiecīgajos līmeņos.
- 3.2.2. Drošības mērķi:
- (a) ir saskanīgi ar drošības politiku un organizācijas stratēģiskajiem mērķiem (attiecīgā gadījumā);
 - (b) ir saistīti ar prioritārajiem riskiem, kuri ietekmē organizācijas drošības rādītājus;
 - (c) ir izmērāmi;
 - (d) ņem vērā piemērojamās juridiskās un cita veida prasības;
 - (e) tiek pārskatīti to sasniegšanas kontekstā un attiecīgi pārstrādāti;
 - (f) tiek paziņoti.
- 3.2.3. Organizācijai ir plāns(-i), kur aprakstīts, kā organizācija sasniegs drošības mērķus.
- 3.2.4. Organizācija apraksta drošības mērķu sasniegšanas uzraudzībai izmantoto stratēģiju un plānu(-us) (sk. Uzraudzība).

3.2.2 Mērķis

Mērķis ir nodrošināt, ka organizācija izpilda tiesību aktu prasības un gādā, lai pastāvīgas drošības uzlabošanas koncepcija tiktu darīta zināma personālam un vadība tai ticētu.

Pieteikuma iesniedzējam jāpierāda, ka tas ir izvirzījis jēgpilnus mērķus un procesu to īstenošanai un pārraudzībai visā to dzīves ciklā.

3.2.3 Paskaidrojumi

Šajā kontekstā drošības rādītāji nozīmē organizācijas darbības rādītājus salīdzinājumā ar tās drošības mērķiem un drošības pārvaldības sistēmas un visu tās atbalsta procesu un procedūru veikspēju.

Jēdzieni “drošības mērķi” un drošības “mērķrādītāji” ir savstarpēji aizstājami, lai gan pēdējam minētajam parasti ir skaitliska nozīme. Drošības mērķi jeb drošības mērķrādītāji atšķiras no dalībvalstu līmenī noteiktajiem kopīgajiem drošības mērķiem (CST), tomēr daži uzņēmumi kopīgos drošības mērķus var izmantot kā sasniedzamos mērķus, lai saglabātu vai uzlabotu savus drošības rādītājus.

Drošības mērķi ir saistīti ar riskiem, jo riski ietekmē organizācijas drošības rādītājus (t. i., paredzētos drošības pārvaldības sistēmas rezultātus un attiecīgi arī panākumus mērķu sasniegšanā). Drošības mērķi var būt kvantitatīvi, piemēram, notikumu skaita samazinājums absolūtā izteiksmē vai procentos. Drošības mērķi var būt arī kvalitatīvi, izteikti kā vispārīga vērtība, piemēram, “tiks uzlabota drošība uz pārbrauktuvēm” vai “tiks saglabāts pašreizējais drošības līmenis.”

Izmantojot pieeju “plānot–darīt–pārbaudīt–rīkoties”, mērķi ir regulāri jāpārskata, prioritāšu noteikšanā ņemot vērā riska novērtēšanas un līdzšinējās pārraudzības un negadījumu un starpgadījumu izmeklēšanas rezultātus, lai saglabātu un, ja tas ir praktiski iespējams, uzlabotu drošības rādītājus.

Tādu drošības rādītāju noteikšana un pārraudzība, kas atbalsta organizācijas lēmumu pieņemšanu par riska kontroli, un tas, vai šādi rādītāji ir efektīvi, ir pamatinformācija drošības mērķu noteikšanai un pārskatīšanai.

3.2.4 Pierādījumi

- Pastāv SMART — tādu drošības mērķu kopums, kas iekļaujas organizācijas plašākās uzņēmējdarbības vajadzībās **(3.2.1. punkts), (3.2.2. punkta a), b) un c) apakšpunkts)**.
- Paziņojums, kurā ir norādītas tiesību aktu prasības un tas, kā tās ir izpildītas **(3.2.2. punkta d) apakšpunkts)**.
- Apraksts par to, kā šos mērķus var sasniegt un kā tos paziņo attiecīgajiem darbiniekiem **(3.2.2. punkta f) apakšpunkts), (3.2.3. punkts)**.
- Pastāv mērķu pārraudzības process, kas atbilst prasībām, kuras noteiktas CSM pārraudzībai (Regula (ES) Nr. 1078/2012), lai nodrošinātu, ka mērķi vienmēr atbilst paredzētajam nolūkam un ka organizācija sasniedz savus mērķus **(3.2.2. punkta e) apakšpunkts), (3.2.4. punkts)**.

3.2.5 Pierādījumu piemēri

Process, saskaņā ar kuru izvirza un pārbauda drošības mērķus un nosaka to prioritātes un kurš nosaka, kā jāizvairās no konfliktiem ar citiem mērķiem vai kā šādi konflikti jārisina, ja no tiem nevar izvairīties. Procesā ir jābūt paredzētam, kādā līmenī nosaka mērķus un kā tie veicina citu mērķu sasniegšanu citos līmeņos, ja piemērojams. Tajā arī ir jābūt paredzētām saskarnēm, termiņiem un jebkādiem vajadzīgiem kvalitatīviem vai kvantitatīviem atbalsta datiem.

Drošības mērķi un to īstenošanas plāns, papildināts ar procesu, kas jāievēro, kad šķiet, ka drošības mērķi netiks sasniegti.

Process vai procedūra pārraudzības pasākumu rezultātu pārvēršanai drošības mērķos, darbību plānošana, lai mērķus sasniegtu, un saistītie sasniegšanas rādītāji.

3.2.6 Uzraudzības jautājumi

Galvenais jautājums attiecībā uz uzraudzību būs tas, cik sasniedzami ir noteiktie mērķi praksē un kas notiek realitātē, ja kļūst skaidrs, ka tie, visticamāk, netiks sasniegti.

Kā drošības mērķi tiek noteikti un pārskatīti — mērķi ir vērsti uz jutīgām vai kritiskām darbībām / kontroles pasākumiem un izmanto rezultātus un darbības rādītājus?

Kā organizācija parāda nepārtrauktus uzlabojumus riska kontrolē ar savu drošības mērķu starpniecību?

Izvērtēt, vai organizācija var efektīvi pārraudzīt savus drošības rādītājus un šim nolūkam izmanto CSM pārraudzībai, lai novērtētu darbību attiecībā pret drošības mērķiem un saistītajiem drošības rādītājiem.

Izskatīt kāda mērķa (piemēram, pirms dažiem gadiem noteikta) piemēru un secināt, vai un kā tam ir sekots līdz no tā noteikšanas līdz galīgajai īstenošanai (vai neīstenošanai).

Labāka dzelzceļa sistēma
sabiedrībai

4 Atbalsts

4.1 Resursi

4.1.1 Normatīvā prasība

4.1.1. Organizācija sagādā resursus, tostarp kompetentu personālu un efektīvu un lietojamu aprīkojumu, kas vajadzīgi, lai izstrādātu, ieviestu, uzturētu un pastāvīgi uzlabotu drošības pārvaldības sistēmu.

4.1.2 Mērķis

Šīs prasības mērķis ir pārliecināties, vai organizācija ir ieviesusi procesus pietiekamu resursu, piemēram, tehniskā aprīkojuma vai sistēmu, vai kompetentu darbinieku, nodrošināšanai, lai tās SMS varētu kontrolēt risku atbilstoši tās mērķiem.

4.1.3 Paskaidrojumi

Pietiekamu resursu atvēlēšana ir pienācīga drošības līmeņa sasniegšanas priekšnosacījums.

4.1.4 Pierādījumi

- Informācija par kompetences pārvaldības sistēmu (CMS) vai, ja CMS nav, pierādījumi par to, kā organizācija nodrošina pietiekamu kompetentu darbinieku skaitu (**4.1.1. punkts**).
- Informācija par to, kā organizācija nodrošina, ka tai ir pietiekams efektīvs un izmantojams aprīkojums, lai tā varētu izpildīt savus pakalpojumu sniegšanas pienākumus un uzturēt efektīvu drošības pārvaldības sistēmu, kas kontrolē risku (**4.1.1. punkts**).
- Informācija par tehniskās apkopes funkciju organizāciju un par to, kā tā ir saistīta ar pietiekamu resursu nodrošināšanu, lai organizācija varētu izpildīt savus pakalpojumu sniegšanas pienākumus (**4.1.1. punkts**).

4.1.5 Pierādījumu piemēri

Izklāsts par to, kā tiek pieņemti lēmumi par vajadzīgo personālu, lai SMS darbotos efektīvi, norādot arī ziņas par attiecīgām atsaucē procedūrām vai procesiem, kur ir atrodama plašāka informācija.

Kompetences pārvaldības procedūra vai ziņas par procesu, kura mērķis ir nodrošināt, ka organizācijai ir kompetenti darbinieki ar attiecīgajām funkcijām, attiecīgā gadījumā iesniedzot sīki izstrādātas mācību programmas (**sk. arī 4.2. punktu**).

Paziņojums, kurā ir izklāstīts process resursu piešķiršanai, lai izpildītu ekspluatācijas vajadzības, papildināts ar attiecīgām atsaucēm uz papilddokumentiem.

Dokuments, kurā ir izklāstīti piešķirtie resursi, kas nepieciešami plānotām un lielām organizācijas pārmaiņām (tostarp personāls un vajadzīgā aprīkojuma nodrošinājums).

4.1.6 Uzraudzības jautājumi

Pārbaudīt, vai kompetences un aprīkojuma prasības ir atgriezeniski saistītas ar riska novērtējuma rezultātiem.

Pārbaudot CMS, valsts drošības iestādei ir jāpārbauda, vai organizācijai ir līdzekļi, ar ko identificēt un paturēt darbiniekus ar atbilstošajām prasmēm, lai organizācija savus uzdevumus izpildītu droši. Īpaši svarīgi ir tas, kā notiek CMS aktualizēšana.

Izvērtējot ar šo kritēriju saistītās tehniskās apkopes darbības, uzraudzības veicējiem ir jānodrošina, ka tad, kad šādas darbības tiek uzdotas izpildei ārējiem darbuzņēmējiem, dzelzceļa pārvadājumu uzņēmums vai infrastruktūras pārvaldnieks īsteno savu uzraudzības funkciju, lai nodrošinātu, ka darbuzņēmēji piegādā attiecīgo droši lietojamo produktu.

Lai noskaidrotu cilvēkresursu pietiekamību vai nepietiekamību, kā rādītāju var izmantot neaizpildītās vakances SMS jomās.

Arī aprīkojuma izmantošanas veids, piemēram, uz darba vietu nogādāto rezerves detaļu skaits, var liecināt par nodrošinātā aprīkojuma kvalitāti un tādējādi arīdzan par resursu pietiekamību.

4.2 Kompetence

4.2.1 Normatīvā prasība

4.2.1.	Organizācijas kompetences pārvaldības sistēma nodrošina, ka personāls, kura funkcijas ietekmē drošību, ir kompetents pildīt ar drošību saistītus uzdevumus, kas ietilpst tā atbildības jomā (sk. 2.3. Organizatoriskās funkcijas, pienākumi, pārskatatbildība un pilnvaras); tostarp sistēma nodrošina vismaz: <ul style="list-style-type: none">(a) ar drošību saistītu uzdevumu pildīšanai vajadzīgās kompetences (tostarp zināšanu, prasmju, ar tehniskiem aspektiem nesaistītas uzvedības un attieksmes) noteikšanu;(b) atlases principus (vajadzīgais pamatzglītības līmenis, psiholoģiskā un fiziskā atbilstība);(c) sākotnējo apmācību, pieredzi un kvalifikāciju;(d) pastāvīgu apmācību un periodisku esošās kompetences pilnveidošanu;(e) periodisku kompetences novērtējumu un psiholoģiskās un fiziskās atbilstības pārbaudes nolūkā nodrošināt kvalifikācijas un prasmju uzturēšanu laika gaitā;(f) lai personāls spētu pildīt ar drošību saistītus uzdevumus — īpašu apmācību par attiecīgajām drošības pārvaldības sistēmas daļām.
4.2.2.	Organizācija personālam, kas pilda ar drošību saistītus uzdevumus, paredz mācību programmu atbilstoši 4.2.1. punkta c), d) un f) apakšpunktā minētajam un nodrošina, ka: <ul style="list-style-type: none">(a) mācību programma tiek izstrādāta atbilstoši noteiktajām kompetences prasībām un personāla individuālajām vajadzībām;(b) attiecīgā gadījumā apmācība nodrošina, ka personāls var darboties visos ekspluatācijas apstākļos (normālā, traucētā un avārijas režīmā);(c) apmācības ilgums un zināšanu atsvaidzināšanas apmācības biežums atbilst mācību mērķiem;(d) tiek reģistrēta informācija par visu personālu (sk. 4.5.3. Dokumentētas informācijas kontrole);(e) mācību programma tiek regulāri pārskatīta un revidēta (sk. 6.2. Iekšējā revīzija), un vajadzības gadījumā tiek veiktas izmaiņas (sk. 5.4. Izmaiņu pārvaldība).
4.2.3.	Ievieš pasākumus, kas atvieglo personāla atgriešanos darbā pēc negadījumiem/starpgadījumiem vai ilgas prombūtnes, tostarp nodrošina papildu apmācību, ja konstatēts, ka tā vajadzīga.

4.2.2 Mērķis

Šīs prasības mērķis ir nodrošināt, ka organizācijai ir attiecīgas struktūras un resursi tai radušos risku kontrolei un ka tā var izmantot personālu, kas ir kompetents pildīt savas drošības funkcijas un jo īpaši drošībai kritiskas funkcijas. Arī kompetences pārvaldības sistēma ļauj organizācijai uzturēt tās personāla prasmes, zināšanas un pieredzi laika gaitā.

Kompetencei ir izšķiroša nozīme darbību apmierinošas izpildes nodrošināšanā. Kompetents personāls ir vajadzīgs gan vadošajos amatos (tostarp darbuzņēmēji, konsultanti un ar drošību saistītu pakalpojumu sniedzēji), gan vadības amatos. Vadības amatu kompetences prasībām bieži vien nepievērš pienācīgu uzmanību, tomēr vadītāji pieņem svarīgus lēmumus, kam var būt būtiska un plaša ietekme uz veselību un drošību. Šādās prasībās ir jābūt ietvertiem noteikumiem par visu darbinieku apmācību atbilstoši vajadzīgajiem drošības standartiem, par kompetences uzturēšanu neatkarīgi no apstākļiem, ietverot tādus jautājumus kā personāla pieejamība, un par kompetences līmeņa pārraudzību attiecībā pret vajadzīgajiem standartiem.

Šajā kontekstā drošību uzskata par profesionālās uzvedības un profesionalitātes neatņemamu sastāvdaļu, nevis par profesionālo prasmju papildinājumu. Arī organizācijas spēja reāllaikā pārvaldīt neparedzētus notikumus ir ļoti atkarīga no vadošo darbinieku un viņu vadītāju kompetences. Šādas kompetences var attīstīt sarežģītu scenāriju simulācijās un regulārā apmācībā.

4.2.3 Paskaidrojumi

Mācību programmu (**4.2.2. punkts**) var nodrošināt ar trešās personas mācību centra starpniecību. Šādā gadījumā organizācijai ir jāpārlicinās, ka mācību centrs ir kompetents sniegt attiecīgos pakalpojumus, proti, tas ir sertificēts vai atzīts centrs atbilstoši valsts vai Eiropas shēmai, vai arī organizācijai tieši jāpārtrauga apmācība un tās rezultāti. Mācību centri var nodrošināt visu organizācijai vajadzīgo apmācību vai tikai tās daļu, pamatojoties uz personāla kompetencēm dažādajās jomās. Ja apmācību organizācijai nodrošina mācību centrs, kas ir trešā persona, organizācijai ir jāpārlicinās, vai apmācība ietver nepieciešamos elementus; ja nepieciešamie elementi nav ietverti, organizācijai šāda ārēja apmācība pēc vajadzības ir jāpapildina ar iekšējo apmācību.

Vārdu “attieksme” (**4.2.1. punkta a) apakšpunkts**) lieto, lai raksturotu cilvēku reakciju uz noteiktām situācijām un to, kā viņi parasti rīkojas (t. i., ir proaktīvi, spēj sadarboties ar citiem cilvēkiem). Tam ir ļoti svarīga nozīme savstarpēju saišu veidošanā SMS darbā.

Vajadzētu būt sistemātiskai pieejai, lai nodrošinātu, ka darbinieki ar kompetenci cilvēkfaktoru un organizatorisko faktoru jautājumos ir pieejami vai nu uz vajadzību analīzes pamata, vai pēc izsaukuma.

Darbinieki ar kompetenci cilvēkfaktoru un organizatorisko faktoru jautājumos ir jāizmanto, piemēram, projektos saistībā ar jauniem vai pārveidotiem risinājumiem, negadījumu analīzē, lai nodrošinātu netehnisku redzējumu, vai cilvēku veikspējas jautājumos.

4.2.4 Pierādījumi

- *Pieteikuma iesniedzējam ir jāsniedz informācija par tā kompetences pārvaldības sistēmu un par to, kā tā darbojas, lai izpildītu prasībās noteikto (**4.2.1. punkts**), (**4.2.2. punkta a)–e) apakšpunkts**).*
- *Pierādījumos ir iekļautas ziņas par ieviestajām darbinieku mācību programmām (tostarp — ja nepieciešams — informācija par organizācijas izvirzītajām pasniedzēju kompetences prasībām) un par to, kā šādas programmas tiek aktualizētas un pārskatītas (tostarp, ja nepieciešams — attiecībā uz drošības konsultanta amatu saskaņā ar RID) (**4.2.2. punkta a)–e) apakšpunkts**).*
- *Pierādījumos ir norādīti pasākumi, kas atvieglo personāla atgriešanos darbā pēc negadījumiem un starpgadījumiem vai ilgas prombūtnes, tostarp izklāstot, kā tiek noteiktas papildu apmācības vajadzības (**4.2.3. punkts**).*
- *Ja pieteikuma iesniedzējs izmanto atzītu mācību centru, kas sertificēts atbilstoši ES regulām, attiecīgā sertifikāta kopijā ir iekļauts pieņēmums par atbilstību iepriekš izklāstītajiem elementiem, ciktāl tiem piemēro konkrēto sertifikācijas procesu (**4.2.1. punkta a), c)–f) apakšpunkts**), (**4.2.2. punkts**).*
- *Pieteikuma iesniedzējam ir jānorāda, kā tas attiecībā uz vieniem un tiem pašiem uzdevumiem nodrošina, lai tā darbinieku un tā nolīgto darbuuzņēmēju, piegādātāju un konsultantu darbinieku kompetences neatšķirtos (**4.2.1. punkta a)–f) apakšpunkts**).*
- *Pieteikuma iesniedzējam ir jānorāda, kā tiek novērtētas cilvēkfaktoru un organizatorisko faktoru kompetences vajadzības, tostarp nosakot, kādu funkciju veikšanai un kādiem procesiem ir vajadzīga cilvēkfaktoru un organizatorisko faktoru kompetence un kāda līmeņa kompetence ir vajadzīga. Pieejamā cilvēkfaktoru spēja (piemēram, oficiālās cilvēkfaktoru kvalifikācijas, t. i., akadēmiskais*

grāds, iekšēji/ārēji atzītas kompetences un pieredze) ir pielāgota uzņēmuma briedumam un sarežģītībai un samērīga ar to (4.2.1. punkta a)–f) apakšpunkts).

- *Pieteikuma iesniedzējam ir jāsniedz informācija par procesu, saskaņā ar kuru personāls tiek pilnvarots veikt galvenos pienākumus, ietverot personāla kompetenču pastāvīgo pārvaldību (4.2.1. punkta a)–f) apakšpunkts, 4.2.2. punkta d) apakšpunkts).*

4.2.5 Pierādījumu piemēri

Kompetences pārvaldības sistēma, sniedzot arī skaidrojumu par to, kā tā darbojas laika gaitā, ja nepieciešams, arī attiecībā uz darbiniekiem, kuri nav vadošie darbinieki, kā arī ietverot saites uz apliecināšu dokumentāciju, tostarp dažādajām mācību programmām, un norādot, kā tiek pārvaldīti mācību centri, ar kuriem ir noslēgti apakšlīgumi.

Ir norādītas līgumsaistības (tostarp pilnvaras), kas noslēgtas ar jebkuriem sertificētiem mācību centriem, papildinātas ar pierādījumiem par centru sertifikāciju.

Personāla grupu mācību programmu piemēri.

Kvalifikācijas, tostarp psiholoģiskās vai fiziskās prasības, ko uzskata par vajadzīgām konkrētu ar drošību saistītu funkciju veikšanai.

Negadījumu un starpgadījumu izmeklēšanas procedūra, ciktāl tā ir saistīta ar mācību programmu pārveidošanu, ņemot vērā negadījumus un starpgadījumus, iepriekšējo uzraudzību u. tml.

Procedūra vai process, lai nodrošinātu personāla īpašu apmācību vai zināšanu atsvaidzināšanas apmācību par:

- *paredzamajām izmaiņām, kas skar iekšējos noteikumus, infrastruktūru, organizatorisko struktūru u. tml.;*
- *uzdoto uzdevumu aktualizāciju (piemēram, vilcienu vadītājiem — par jauniem maršrutiem, jauniem lokomotīvu veidiem, jaunu pakalpojuma veidu).*

Process, lai nodrošinātu, ka:

- *kompetence tiek uzturēta ar pietiekamu praksi reālajā vidē (piemēram, vilcienu vadītājiem — zināšanas par darbības apstākļiem, vilcienu kategorijām, vilces vienībām, līnijām un stacijām) un/vai plānojot īpašu apmācību, jo īpaši pēc ilgas prombūtnes (piemēram, slimības) vai negadījumiem/starpgadījumiem;*
- *tiek īstenota vajadzīgā rīcība, ja ir konstatētas neatbilstības vai neatbilstoša uzvedība, piemēram, persona vai aprīkojums tiek atsaukts no ekspluatācijas uz noteiktu laiku, piemēro ierobežojumus attiecībā uz atzītām prasmēm, ja tiek konstatēta neatbilstība, tiek organizēta īpaša apmācība u. tml.;*
- *tiek veikti atbilstoši pasākumi attiecībā uz personālu pēc negadījumiem un starpgadījumiem (piemēram, vilcienu vadītājiem, kuri pabrauc garām signālam, negadījumiem, kuros iesaistīts cilvēks, u. tml. Piemēram, organizācija nodrošina, ka vilciena vadītājs ir piemērots atsākt pakalpojuma sniegšanu vai tiek aizstāts ar citu vadītāju, kurš ir kompetents sniegt attiecīgo pakalpojumu);*
- *gūtā mācība pēc smagiem negadījumiem vai jebkura cita būtiska notikuma tiek kopīgota, jo īpaši ja tiek konstatēti jauni riski, kas ir jāpārvalda ekspluatācijas līmenī;*
- *pārraudzības process attiecībā uz kompetences pārvaldības sistēmu, norādot arī to, kā tiek novērtēta tās efektivitāte.*

Process, lai nodrošinātu, ka tiek noteiktas attiecīgās kompetences attiecībā uz cilvēkfaktoriem un organizatoriskajiem faktoriem un ka pastāv sistemātiska pieeja, lai nodrošinātu, ka tiek atvēlēts pietiekams laiks un resursi cilvēkfaktoriem un organizatoriskajiem faktoriem.

Drošības kultūras kompetences pamatā ir vajadzību analīze. Drošības kultūras kompetences vajadzības tiek novērtētas, un tiek parādītas stratēģijas pareizo kompetenču un resursu nodrošināšanai. Tiek parādīts, ka vadība veicina pamatzināšanas par drošības kultūru un tās nozīmīgumu.

4.2.6 Atsauces un standarti

- ISO 10015:1999 *“Kvalitātes pārvaldības pamatnostādnes apmācībai”*
- ISO 10018: *“Kvalitātes pārvaldība. Pamatnostādnes par cilvēkiem un kompetenci”*

4.2.7 Uzraudzības jautājumi

Kā riska novērtējuma rezultāti ir saistīti ar CMS pārskatīšanu?

Izvērtējot kompetences pārvaldības sistēmu, svarīgi ir atcerēties, ka būs kompetences prasības, kas pārsniedz organizācijas personāla kompetences un ietekmē arī darbuzņēmējus un citus dalībniekus.

CMS sistēma ir jāpārbauda, lai redzētu, cik tā atbilst faktiskajai situācijai un vai saskaņā ar to īstenotās apmācības darbības atspoguļo organizācijas pašreizējās vajadzības.

Organizācijas rīcībā ir jābūt dažiem līdzekļiem, kā nodrošināt, ka darbību veikšanai nolīgtais personāls ir kompetents to darīt. Tas ir īpaši svarīgi, kad piesaista darbuzņēmējus, kuri nodrošina tikai darbaspēku, jo šāda darbaspēka kompetences pārbaudes var nebūt tik pamatīgas.

Kompetences līmenim, kāds vajadzīgs līdzīgu darbību veikšanai tieši nodarbinātajiem darbiniekiem un darbuzņēmējiem, ir jābūt vienādam.

Ir ieviesta sistēma, kas nodrošina uzdevumu un amatu, tostarp drošībai kritisku uzdevumu ar drošības elementu identificēšanu.

Pastāv stabila un efektīva kompetences pārvaldības sistēma, kas ietver vajadzīgo zināšanu un prasmju, apmācības, uzturēšanas un kompetences resursu noteikšanu, kā arī procesi darbinieku pieņemšanai darbā, apmācībai, novērtēšanai, kompetences pārraudzībai un uzskaites veikšanai, norādot, kā visi šie aspekti veicina kompetences sasniegšanu un uzturēšanu.

Orientēšanās uz cilvēkfaktoriem — kā tiek novērtēta fiziskā un psiholoģiskā piemērotība (piemēram, vilcienu vadītājiem un citiem darbiniekiem, kuri veic drošībai kritiskus uzdevumus).

4.3 Apzināšanās

4.3.1 Normatīvā prasība

4.3.1. Augstākā līmeņa vadība nodrošina, ka tā un personāls, kura funkcijas ietekmē drošību, apzinās savu darbību būtiskumu, svarīgumu un sekas, kā arī savu devumu drošības pārvaldības sistēmas pareizā piemērošanā un efektivitātē, tostarp drošības mērķu sasniegšanā (sk. Drošības mērķi un plānošana).

4.3.2 Mērķis

Apzināšanās nozīmē darbinieku informēšanu un informētību par organizācijas drošības politiku un to, kā viņi veicina drošību organizācijā, par apdraudējumiem un riskiem, kas viņiem jāapzinās, kā arī negadījumu un starpgadījumu izmeklēšanas rezultātiem. Tā arī attiecas uz darbinieku informēšanu par sekām gan viņiem, gan organizācijai gadījumā, ja viņi nesniedz savu ieguldījumu SMS īstenošanā. Šīs prasības mērķis ir risināt drošības kultūras jautājumus organizācijā. Augstākā līmeņa vadībai ir jānosaka organizācijas darbības programma un virziens un jāizklāsta, kā notiek uzņēmējdarbība. Darbinieki, kuri strādā organizācijā, ievēro vadības norādījumus. Pieteikuma iesniedzējam ir jāparāda, kā tas risina šādus jautājumus savos procesos un procedūrās.

4.3.3 Pierādījumi

- *Pieteikuma iesniedzējam ir jānorāda, kur tā cilvēkresursu procesā vai citos procesos ir atspoguļota darbinieku būtiskā loma organizācijas mērķu īstenošanā, kā tas novērtē darbinieku sniegumu un kādus pasākumus tas veic, lai sniegumu saglabātu un uzlabotu (4.3.1. punkts) (sk. arī 2.3. punktu).*
- *Informācija par kompetences pārvaldības sistēmas darbību (4.3.1. punkts).*

4.3.4 Pierādījumu piemēri

Paziņojums drošības politikā vai citviet par organizācijas “vadošo prātu” apņemšanos veicināt organizācijas drošības kultūru, lai nodrošinātu risku kontroli, īstenojot pārvaldības sistēmas pieeju; šādā dokumentā jābūt norādītam arī visu darbinieku statusam drošības politikas veicināšanā, ko nodrošina viņu darbības un izvirzīto drošības mērķu īstenošana. Ir norādītas saites uz konkrētajām procedūrām, kuru mērķis ir popularizēt šīs idejas visā organizācijā.

Izklāstā ir norāde par to, kā organizācija popularizē savu drošības kultūras pieeju saviem darbuzņēmējiem, partneriem un piegādātājiem.

Attiecībā uz politiku kā tādu — augstākā līmeņa vadības paziņojumi par mērķiem, proti, aicinājumi visiem darbiniekiem sniegt ieguldījumu mērķu sasniegšanā vai, piemēram, pateicības paziņojumi par darbības rādītāju uzlabošanu.

Informācija, kas pierāda, ka vidējā līmeņa vadība un ekspluatācijas personāls ir iesaistīti vadošajās drošības iniciatīvās (semināros, forumos, speciālās drošībai veltītās dienās, mācību programmās, kas vērstas uz to, lai veicinātu informētību par viņu lomu SMS, u. tml.).

Saziņas kanālu un izmantoto kanālu apraksts.

4.3.5 Uzraudzības jautājumi

Iztaujājot darbiniekus par šo jautājumu, ir būtiski noskaidrot, kāda ir viņu izpratne par viņiem piemērojamām funkcijām un pienākumiem. Pēc tā var spriest, vai organizācija spēj saprast efektīvas organizatoriskās kultūras vai informētības nozīmīgumu drošības uzturēšanā ar SMS starpniecību.

Kas ir organizācijas pašreizējās kultūras pamatā un kādi pasākumi ir ieviesti tās uzlabošanai un attīstīšanai — tie ir uzraudzībai būtiski jautājumi.

Pārbaudīt, kā tiek pārraudzīta ar veselību un drošību saistīto pienākumu/mērķu izpilde, informēšana par riskiem, ziņošanas kultūra — vai tiek meklēti izlaidumi, kļūdas, pārkāpumi vai citas neatbilstības.

4.4 Informācija un saziņa

4.4.1 Normatīvā prasība

4.4.1.	Organizācija nosaka pienācīgus saziņas kanālus, nodrošinot ar drošību saistītas informācijas apmaiņu starp dažādiem organizācijas līmeņiem un ar ieinteresētajām trešām personām, tostarp ar darbuzņēmējiem, partneriem un piegādātājiem.
4.4.2.	Lai nodrošinātu, ka ar drošību saistīta informācija nonāk pie spriedējiem un lēmējiem, organizācija pārvalda ar drošību saistītas informācijas identificēšanu, saņemšanu, apstrādi, ģenerēšanu un izplatīšanu.
4.4.3.	Organizācija nodrošina, ka ar drošību saistīta informācija ir: <ul style="list-style-type: none">(a) būtiska, pilnīga un saprotama personām, kuras to izmantos;(b) derīga;(c) precīza;(d) konsekventa;(e) kontrolēta (sk. Dokumentētas informācijas kontrole);(f) paziņota pirms tās stāšanās spēkā;(g) saņemta un saprasta.

4.4.2 Mērķis

Šo prasību izpildes mērķis ir parādīt, ka pieteikuma iesniedzējs savā pieteikumā ir apliecinājis, ka tam ir attiecīgi līdzekļi ar drošību saistītas informācijas identificēšanai dažādos līmeņos un tās paziņošanai pareizajā laikā un pareizajām personām, ka tas veic potenciālo scenāriju analīzi, lai nodrošinātu, ka pašreizējie riska kontroles pasākumi joprojām ir nozīmīgi un aktuāli un var identificēt jaunus apdraudējumus un iespējas, ko rada ārēja ietekme (politiska, sociāla, ar vidi saistīta, tehnoloģiska, ekonomiska un juridiska). Pārbaudīt, vai viņi var pārliecināties, ka informācija ir sasniegusi to attiecīgo speciālistu (jo īpaši drošībai svarīgo personālu) organizācijā, kuram uz to ir jāreaģē. Minētais attiecas arī uz to, kā pieteikuma iesniedzējs sniedz attiecīgu ar drošību saistītu informāciju citām ieinteresētajām personām, ar kurām tas mijiedarbojas.

4.4.3 Paskaidrojumi

Organizācija norāda, kāda veida ar drošību saistīta informācija ir jāpaziņo, kā to paziņos (sk. arī 4.5. punktu), kam to paziņos un ar kādiem nosacījumiem šo informāciju sniegs un apstrādās (4.4.1. punkts). Apmaina ar informāciju par drošību notiek starp darbiniekiem, kuri organizācijā veic uzdevumus, ar darbuzņēmējiem/apakšuzņēmējiem, partneriem vai piegādātājiem, starp dzelzceļa pārvadājumu uzņēmumiem un infrastruktūras pārvaldītājiem un — attiecīgā gadījumā — starp infrastruktūras pārvaldītājiem.

Var izšķirt dažādu veidu informāciju:

- SMS dokumentācija (**sk. arī 4.5. punktu**);
- *statiskā informācija, kas jāsaņem no infrastruktūras pārvaldītāja, lai varētu projektēt dzelzceļa darbības, piemēram, ekspluatācijas noteikumi un dzelzceļa infrastruktūras raksturojums (piemēram, sliežu platums, vilcienu garums, slīpumi un asslodze);*
- *informācija, kas vajadzīga dzelzceļa darbību plānošanai, piemēram, staciju darba laika grafiki, maršrutu saraksti, pagaidu ātruma ierobežojumi, dzelzceļa infrastruktūras izmaiņas, uz sliedēm*

notiekoši darbi, sliežu platuma ierobežojumi, vilcieni, kas jānovirza no plānotā maršruta, līnijas sektori, kurā ir viensliežu dzelzceļš, vilcienu kustības prognozes (tostarp jebkuras vilcienu maršrutu un/vai svārstsatiksmes pakalpojumu izmaiņas);

- *informācija par vilcienu satiksmes pārvaldību (starp dzelzceļa pārvadājumu uzņēmumiem un infrastruktūras pārvaldītājiem un — attiecīgā gadījumā — starp infrastruktūras pārvaldītājiem), norādot kompetentos darbiniekus katrā organizācijā, ar kuriem var sazināties traucētas ekspluatācijas vai avārijas situācijās (sk. arī 5.5. punktu) parastajā darba laikā un ārpus tā.*

SITS OPE ir noteiktas pamatprasības informācijas apmaiņai (4.4.2. punkts) starp dzelzceļa pārvadājumu uzņēmumu un infrastruktūras pārvaldītāju, ECM regulā — starp dzelzceļa pārvadājumu uzņēmumu un ECM, CSM, kas attiecas uz prasībām drošības pārvaldības sistēmām — starp dzelzceļa pārvadājumu uzņēmumu / infrastruktūras pārvaldītāju un iestādēm (Aģentūru, VDI).

Ir ieviesta kārtība, kādā notiek informācijas apmaiņa ar attiecīgajām personām par drošības apdraudējumiem, kas saistīti ar tehnisko sistēmu, arī strukturālo apakšsistēmu, defektiem un konstrukcijas neatbilstībām vai darbības atteicēm, tostarp kārtība, kādā notiek informācijas apmaiņa par visām korektīvajām darbībām, kas veiktas, piemēram, pamatojoties uz SAIT (drošības brīdinājumu rīka) nolīgumu, ko Aģentūra ir veicinājusi dzelzceļa nozarē. Izmantojot SAIT, tiek izpildīts Direktīvā par dzelzceļa drošību (4. panta 5. punktā) noteiktais informācijas apmaiņas pienākums, kā arī prasība apmainīties ar šādu informāciju, kas noteikta CSM pārraudzībai (4. pantā) un Regulā par struktūrām, kas atbild par tehnisko apkopi (5. panta 5. punktā).

“Derīga” iepriekš minētajā kontekstā (4.4.3. punkta b) apakšpunkts) nozīmē “atbilstoša faktiskajai situācijai”.

“Konsekventa” iepriekš minētajā kontekstā **(4.4.3. punkta d) apakšpunkts)** nozīmē, ka informācija nav pretrunīga, ja tā ir iegūta no dažādiem avotiem.

“Saprasta” iepriekš minētajā kontekstā **(4.4.3. punkta g) apakšpunkts)** nozīmē, ka pieteikuma iesniedzējs apliecina, ka ir veicis pasākumus, lai nodrošinātu, ka drošībai kritisku informāciju ir saņēmuši tie, kuriem tā adresēta. To var nodrošināt, rīkojot ad-hoc apmācību, uzdodot jautājumus instruktāžās, lai pārbaudītu izpratni, vai drošībai kritiskā saziņā, pieņemot protokolus, kas paredz svarīgu ziņojumu atkārtošanu atpakaļ ziņotājam, piemēram, starp signalizētāju un vilciena vadītāju, lai apstiprinātu, ka tie ir saprasti pareizi, vai jebkādiem citiem līdzekļiem, kas atbilst šai prasībai.

4.4.4 Pierādījumi

- *Pieteikuma iesniedzējs norāda dažādos organizācijā pastāvošos saziņas kanālus un to mērķi **(4.4.1. punkts)**.*
- *Pieteikuma iesniedzējam jāiesniedz pierādījumi, piemēram, par jebkādu iekšējo drošības brīdinājumu sistēmu, jebkādu sistēmu, kas paredzēta, lai sniegtu personālam būtisku rutīnas informāciju, un jebkādu sistēmu, kas paredzēta, lai sniegtu personālam būtisku ad-hoc informāciju **(4.4.2. punkts)**.*
- *Pieteikuma iesniedzējs norāda, kā tas pārlicinās, vai tā izplatīto informāciju ir saņēmuši tās adresāti (jo īpaši tie, kuri veic drošībai kritiskas funkcijas) un ir to sapratuši. **(4.4.3. punkts)**.*

4.4.5 Pierādījumu piemēri

Skaidrs paziņojums par to, kā notiek augšupējā un lejupējā saziņa dažādu veidu un līmeņu informācijas nodošanai, ietverot saites uz konkrētajām drošības brīdinājumu un rutīnas saziņas procedūrām.

Paziņojumā ir norādīts, kādus pasākumus pieteikuma iesniedzējs veic attiecībā uz dažādu veidu saziņu, lai nodrošinātu, ka paziņotā informācija sasniedz darbiniekus, kuriem tā adresēta, un ka darbinieki saprot, kas tiek paziņots, piemēram, drošībai kritiska informācija.

Process vai procedūra, kas nodrošina, ka ikvienam ar drošību saistīta uzdevuma veikšanā iesaistītam darbiniekam tiek nodrošināta pareizā dokumentu versija pareizajā laikā.

Process vai procedūra ar drošību saistītu dokumentu piegādes apstiprināšanai.

Process/procedūra, lai nodrošinātu, ka ārējām personām, piemēram, infrastruktūras pārvaldītājam(-iem), (citiem) dzelzceļa pārvadājumu uzņēmumiem, iestādēm u. tml. tiek norādīta kontaktpersona, kura spēj sazināties ar tiem (piemēram, valodu prasmes) un kam ir piekļuve atbilstošā līmeņa informācijai.

Informētība par veidlapu grāmatiņu (sk. SITS OPE), kurā ir iekļauts saziņas protokolu vai līdzekļu kopums oficiālas ar ekspluatāciju saistītas informācijas skaidrai un ātrai apmaiņai (papīra vai citā formātā, piemēram, ierakstīšanas ierīces), jo īpaši par vilcienu kustību traucētas ekspluatācijas režīmā.

Drošības brīdinājumi, ar kuriem jāveic apmaiņa organizācijā vai ar citām ieinteresētajām personām. Daži tipiski piemēri:

- *dzelzceļa pārvadājumu uzņēmumi sniedz informāciju infrastruktūras pārvaldītājam par jebkurām neērtībām, kas var ietekmēt vilcienu kustību (ritošā sastāva bojājumi, piemēram, sakarsušas bukses), lai infrastruktūras pārvaldītājs varētu veikt riska kontroles pasākumus (piemēram, bloķēt satiksmi uz blakusesošajām sliežu ceļiem);*
- *infrastruktūras pārvaldītājs sniedz informāciju par infrastruktūras kļūmēm un iespējamiem pagaidu drošības pasākumiem, piemēram, ātruma ierobežojumiem, visiem dzelzceļa pārvadājumu uzņēmumiem, kas darbojas attiecīgajā telpā.*

Attiecībā uz darbiniekiem, kuriem ir uzticēta saskarņu pārvaldība — pierādījumi par to, kam tiek nosūtīts drošības brīdinājums atkarībā no darbības telpas (piemēram, tie ir iekļauti maršrutu grāmatā);

process vai procedūra informācijas izplatīšanai par organizācijas struktūras izmaiņām gan mikro, gan makro līmenī;

to norādījumu kopijas, kas sniegti darbiniekiem, kuri veic ar drošību saistītus uzdevumus, un kas saistīti ar tīkla(-u) ekspluatācijas noteikumiem, kuriem jābūt:

- *pilnīgiem — visi noteikumi un prasības, kas attiecas uz drošības jomā veicamiem uzdevumiem saistībā ar dzelzceļa pārvadājumu uzņēmuma darbību, ir identificēti un aprakstīti attiecīgajos dokumentos;*
- *precīziem — katrs noteikums un prasība ir pareizi formulēta bez kļūdām (piemēram, rīcība pirms signāla, ar drošību saistīta saziņa);*
- *konsekventiem — prasības, ko piemēro atsevišķai personai vai atsevišķai personu grupai un kas izriet no dažādiem avotiem, ir saderīgas un konsekventas un nav pretrunīgas.*

4.4.6 Uzraudzības jautājumi

Pārbaudīt, vai ir ieviestas metodes un process, ko izmanto, lai nodrošinātu aktualitāti riska kontrolē un potenciālo iespēju un draudu izpētē.

Pārbaudīt, vai ir ieviests process oficiālas informācijas izmantošanas pārraudzībai.

Uzraudzībā galvenie jautājumi ir par to, cik aktuāla ir informācija un vai tā savlaicīgi sasniedz visus attiecīgos darbiniekus, piemēram, tos, kuri strādā naktīs maiņās vai tālu no organizācijas galvenajām mītnēm.

4.5 Dokumentēta informācija

4.5.1 Normatīvā prasība

4.5.1. Drošības pārvaldības sistēmas dokumentācija

4.5.1.1. Ir izstrādāts drošības pārvaldības sistēmas apraksts, kurā ietverti šādi aspekti:

- (a) ar dzelzceļa darbību drošību saistīto procesu un darbības, tostarp ar drošību saistītu uzdevumu un attiecīgo pienākumu identifikācija un apraksts (sk. 2.3. Organizatoriskās funkcijas, pienākumi, pārskatatbildība un pilnvaras);
- (b) šo procesu mijiedarbība;
- (c) procedūras vai citi dokumenti, kur aprakstīts, kā šie procesi tiek īstenoti;
- (d) darbuzņēmēju, partneru un piegādātāju identifikācija un sniegto pakalpojumu veida un apjoma apraksts;
- (e) tādu līgumsaistību un citu uzņēmējdarbības līgumu identifikācija, kas noslēgti starp organizāciju un citām d) apakšpunktā norādītajām personām un vajadzīgi, lai kontrolētu organizācijai raksturīgos drošības apdraudējumus un drošības apdraudējumus saistībā ar darbuzņēmēju izmantošanu;
- (f) šajā regulā prasītā atsauce uz dokumentētu informāciju.

4.5.1.2. Organizācija nodrošina, ka saskaņā ar Direktīvas (ES) 2016/798 9. panta 6. punktu attiecīgajai valsts drošības iestādei (vai iestādēm) tiek iesniegts gada drošības pārskats, kas ietver:

- (a) kopsavilkumu par lēmumiem, kuri nosaka ar drošību saistītu izmaiņu nozīmīguma līmeni, tostarp pārskatu par nozīmīgām izmaiņām, saskaņā ar Regulas (ES) Nr. 402/2013 18. panta 1. punktu;
- (b) organizācijas drošības mērķus nākamajam gadam/turpmākajiem gadiem un to, kā nopietni drošības apdraudējumi ietekmē šo drošības mērķu noteikšanu;
- (c) negadījumu/starpgadījumu iekšējās izmeklēšanas (sk. 7.1. No negadījumiem un starpgadījumiem gūtā mācība) un citu uzraudzības darbību (sk. 6.1. Uzraudzība, 6.2. Iekšējā revīzija un 6.3. Vadības veikta pārskatīšana) rezultātus saskaņā ar Regulas (ES) Nr. 1078/5. panta 1. punktu;
- (d) sīku informāciju par to, kā norit neīstenoto valsts izmeklēšanas struktūru ieteikumu īstenošana (sk. 7.1. No negadījumiem un starpgadījumiem gūtā mācība);
- (e) organizācijas drošības raksturlielumus, kas noteikti organizācijas drošības rādītāju izvērtēšanas vajadzībām (sk. 6.1 Uzraudzība);
- (f) attiecīgā gadījumā — RID minētā drošības konsultanta gada ziņojuma secinājumus par organizācijas darbību saistībā ar bīstamo kravu pārvadājumiem.

4.5.2. Informācijas radīšana un atjaunināšana

4.5.2.1. Organizācija nodrošina, ka ar drošības pārvaldības sistēmu saistītas dokumentētas informācijas radīšanai un atjaunināšanai tiek izmantoti atbilstoši formāti un informācijas līdzekļi.

4.5.3. Dokumentētas informācijas kontrole

4.5.3.1. Organizācija ar drošības pārvaldības sistēmu saistītu dokumentētu informāciju, jo īpaši tās glabāšanu, izplatīšanu un izmaiņu vadību, kontrolē, lai attiecīgā gadījumā nodrošinātu tās pieejamību, piemērotību un aizsardzību.

4.5.2 Mērķis

Pieteikuma iesniedzējam ir jāparāda, ka vispārējā drošības pārvaldības sistēma ir atbilstoša sniegto pakalpojumu veidam un apjomam un spēj pārvaldīt radītos riskus. Šajā nolūkā ir vajadzīgs:

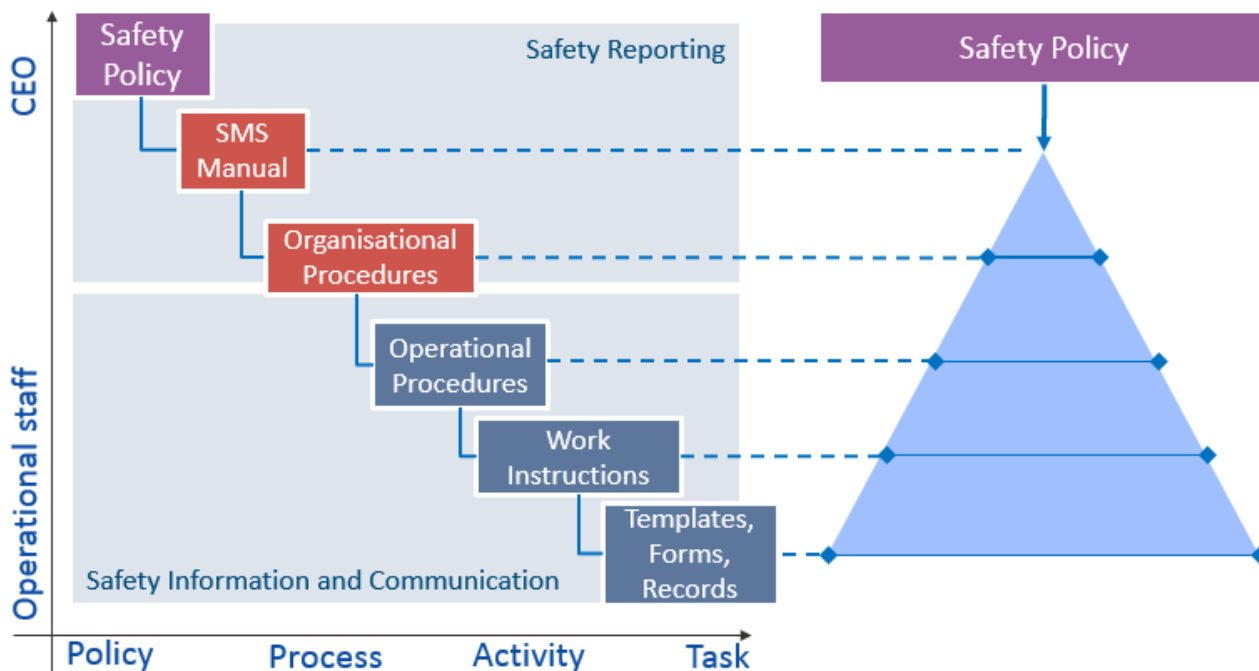
- skaidrojums par pieteikuma iesniedzēja drošības politiku, organizāciju un augsta līmeņa SMS pasākumiem un
- sīkāks izklāsts par pasākumiem, kas paredzēti iepriekš minētajās prasībās 4.5.1.1. punkta a)–f) apakšpunktā un 4.5.1.2. punkta a)–g) apakšpunktā.

Pieteikuma iesniedzējam ir arī jāparāda, kā tiek pārvaldīta tā SMS dokumentācija, t. i., kā notiek dokumentētas informācijas (t. i., dokumentu un ierakstu/datu) identificēšana, radīšana, uzturēšana, uzglabāšana un saglabāšana, lai nodrošinātu, ka tā ir aktuāla un ka darbiniekiem pēc vajadzības ir pieejamas pareizās versijas.

4.5.3 Paskaidrojumi

Jebkādi dokumenti, kuros pieteikuma iesniedzējs parāda tā SMS atbilstību piemērojamām prasībām (4.5.1.1. punkta f) apakšpunkts), ir daļa no SMS dokumentētās informācijas.

Turpmāk 3. attēls. attēlā ir norādīta tipiska dokumentācijas struktūra.



3. attēls. Tipiska dokumentācijas struktūra

Operational staff	Ekspluatācijas personāls
CEO	Izpilddirektors
Safety Policy	Drošības politika

Safety Reporting	Drošības pārskatu sniegšana
SMS Manual	SMS rokasgrāmata
Organisational Procedure	Organizatoriskā procedūra
Work instructions	Darba norādījumi
Template, Forms, Records	Veidne, veidlapas, ieraksti
Safety Information and Communication	Drošības informācija un saziņa
Policy	Politika
Process	Process
Activity	Darbība
Task	Uzdevums

Atkarībā no darbības telpas dzelzceļa pārvadājumu uzņēmumi var iesniegt dažādus ziņojumus **(4.5.1.2. punkts)** to dalībvalstu VDI, kurās tie veic darbības. Parasti ziņojuma joma attiecas tikai uz to darbības daļu, kas tiek veikta attiecīgajā dalībvalstī. Tomēr Aģentūra iesaka minētajā ziņojumā aptvert visu darbības telpu, jo tam ir jāatvieglo informācijas apmaiņa starp VDI, kas uzrauga vienu un to pašu dzelzceļa pārvadājumu uzņēmumu.

Drošības konsultanta gada ziņojums **(4.5.1.2. punkta f) apakšpunkts)** bīstamu kravu pārvadājumu gadījumā, kā to nosaka Direktīva 2008/68/EK ar grozījumiem un RID — bīstamo kravu drošības konsultanta gada ziņojums ir arī ievadinformācija gada drošības ziņojumam. Drošības konsultantam ir jāpilda noteiktas funkcijas, tostarp jākonsultē uzņēmums, kas viņu iecēlis, par veselības, drošības un vides jautājumiem saistībā ar bīstamo kravu pārvadājumiem un vajadzīgo ziņojumu sagatavošanu.

Dokumentētās informācijas identifikācija, formāts (piemēram, valoda, programmatūras versija un grafika) un informācijas nesējs (piemēram, papīra, elektronisks formāts) **(4.5.2.1. punkts)** ir organizācijas ziņā. Tai nav jābūt rakstiskā papīra rokasgrāmatas formātā.

Dokumentu kontrole **(4.5.3.1. punkts)** nosaka procesu (vai procedūru) iekšējai kontrolei, jo īpaši pārskatīšanai un atbilstības apstiprināšanai pirms dokumentu izdošanas un izmantošanas, kas jāņem vērā un jāīsteno attiecībā uz informāciju, kura jādokumentē. Tās mērķis ir noteikt dokumentu aktuālo pārskatīšanas statusu, lai nepieļautu nederīgu vai novecojušu dokumentu izmantošanu. Kontrole jo īpaši nodrošina, ka:

- *visās vietās, kur tiek veiktas drošības pārvaldības sistēmas efektīvai funkcionēšanai būtiskas darbības, ir pieejami vajadzīgie attiecīgo dokumentu izdevumi;*
- *nederīgi vai novecojuši dokumenti tiek nekavējoties izņemti no visām to izdošanas vai izmantošanas vietām vai kā citādi netiek pieļauta to izmantošana neparedzētiem mērķiem;*
- *jebkādi novecojuši dokumenti, ko patur juridiskiem vai informatīviem mērķiem, ir atbilstoši identificēti.*

4.5.4 Pierādījumi

- *Pieteikuma iesniedzējam ir jāiesniedz apraksts par drošības pārvaldības sistēmu un par to, kā tā darbojas, ar atbilstošām norādēm uz attiecīgām procedūrām, ja nepieciešams **(4.5.1.1. punkta a)–c) apakšpunkts)**.*

- *Pieteikuma iesniedzējam ir jānorāda funkcijas un pienākumi, kas ir noteikti ar drošību saistītu uzdevumu veikšanai, un tas, kā tiek pārvaldīti pieteikuma iesniedzēja un citu dalībnieku darbību radītie riski (4.5.1.1. punkta a) apakšpunkts).*
- *Pieteikuma iesniedzējam jāiesniedz pierādījumi, ka tas ir sagatavojis (vai ir ieviesis pasākumus, lai sagatavotu) gada drošības ziņojumu, aptverot 4.5.1.2. punktā minētos jautājumus (4.5.1.2. punkta a)-f) apakšpunkts).*
- *Pieteikuma iesniedzējam ir jānorāda, kā darbojas dokumentu pārvaldības sistēma, tostarp, kā tiek sniegta informācija un kā tā ir pieejama izmantošanai, kad tas ir vajadzīgs, kā notiek kontrolēta tās maiņa sistēmā un kā tā tiek uzglabāta un uzturēta, lai būtu ātri izgūstama, un dokumentu pārvaldības sistēmai ir jānodrošina iespēja informāciju glabāt vietās, kurās ir piemērota vide, lai līdz minimumam samazinātu tās kvalitātes pasliktināšanos vai sabojāšanu un novērstu tās zaudēšanu (4.5.2.1. punkts, 4.5.3.1. punkts).*

4.5.5 Pierādījumu piemēri

Apraksts par drošības pārvaldības sistēmu, tās vispārējo struktūru un saites uz dokumentiem, kas pamato tajā ietvertos procesus (piemēram, rokasgrāmatu, organizatoriskajām un ekspluatācijas procedūrām, darba norādījumiem). Neatkarīgi no dokumentētas informācijas jaunās koncepcijas, ko ievieša ISO, organizācija var saglabāt tradicionālo dokumentācijas struktūru, ja vien tā atbilst paredzētajam mērķim.

Izklāsts par to, kā dažādie dokumenti tiek strukturēti, publicēti, darīti pieejami, noformēti kā lietas, uzturēti/pārskatīti un atcelti, ar atsauci uz attiecīgajām dokumentu kontroles procedūrām.

Pieteikuma iesniedzēja gada pārskata sagatavošanas procedūra, ja pieteikums attiecas uz pirmo vienoto drošības sertifikātu. Procedūrā ir norādīts ieteicamais ziņojuma noformējums.

Dokumentu pārvaldības process vai procedūra, kurā jābūt izklāstītam, kā notiek dokumentu atjaunināšana pēc regulārās pārskatīšanas un pēc negadījumiem vai starpgadījumiem. Procesā vai procedūrā ir noteikts sūdzību risināšanas process gadījumos, kad saskaņotie atjauninājumi nav ieviesti vajadzīgajā termiņā vai ja nav panākta vienošanās par to, kā atjaunināt dokumentu.

Tiek lietota kontrolēta valoda (t. i., īsi, skaidri teikumi, izvairoties no žargona), lai veicinātu vienotu izpratni un datu labu kvalitāti.

Personāls, kas ir pilnvarots apstiprināt dokumentus izdošanai, nodrošina, ka to saturs ir precīzs un ir saprotams visiem tiešajiem lietotājiem (vai saņēmējiem), uz kuriem tas attiecas.

Ja praktiski iespējams, izmaiņu veidu norāda dokumentā vai attiecīgos pielikumos, lai atvieglotu to pārskatīšanu un apstiprināšanu.

Ir noteikti, dokumentēti un tiek ievēroti dokumentu un ierakstu saglabāšanas termiņi.

4.5.6 Atsauces un standarti

- *Pamatnostādnes par prasībām dokumentētai informācijai, ko paredz ISO 9001:2015, ISO/TC 176/SC2/N1286, ir pieejamas vietnē www.iso.org/tc176/sc02/public.*

4.5.7 Uzraudzības jautājumi

Pārbaudīt, vai līgumsaistības paredz risku efektīvu pārraudzību un kontroli organizācijā (t. i., kad pakalpojumu sniegšanai tiek nolīgti darbuzņēmēji).

Veicot uzraudzību, ir ļoti svarīgi noteikt, kādas praksē ir attiecības starp personām, kuras kontrolē dokumentu pārvaldības sistēmu, un personām, kuras atbild par informācijas atjaunināšanu un sadarbību ar pirmajām minētajām personām. Tieši šajā līmenī bieži var pastāvēt dokumentācijas kontroles iedalījums, jo ir iespējams, ka abas šā procesa daļas atrodas divās dažādās pārvaldības ķēdēs. Tas var radīt, piemēram, situāciju, ka dokumentācijas atjaunināšanas darba nozīmīgums tiek uztverts atšķirīgi, rezultātā radot laika nobīdes dokumentācijas izstrādē un atjaunināšanā un ar to saistītus riskus.

Personāla spēja piekļūt atjauninātai informācijai/dokumentācijai.

SMS struktūrai un darbības modelim ir jāatspoguļo reālais darba izpildes veids, nevis tikai mākslīgi jāpapildina ieražas un prakse.

4.6 Cilvēkfaktoru un organizatorisko faktoru integrācija

4.6.1 Normatīvā prasība

4.6.1. Organizācija demonstrē sistemātisku pieeju cilvēkfaktoru un organizatorisko faktoru integrēšanai drošības pārvaldības sistēmā. Šī pieeja:

- a) ietver stratēģijas izstrādi un cilvēkfaktoru un organizatorisko faktoru jomas īpašo zināšanu un atzīto metožu izmantošanu;
- b) pievēršas riskiem saistībā ar iekārtu konstrukciju un izmantošanu, uzdevumiem, darba apstākļiem un organizatoriskiem pasākumiem, ņemot vērā cilvēku spējas un to robežas, un ietekmi uz cilvēka veiktspēju.

4.6.2 Mērķis

Pieteikuma iesniedzējs parāda, ka cilvēkfaktoru un organizatorisko faktoru pieejas sistemātiska izmantošana riska identificēšanā ir SMS neatņemama daļa. Šo elementu izpilde ir būtiska, lai varētu parādīt, ka pieteikuma iesniedzējs ir kompetents veikt dzelzceļa darbību un ka tā SMS ir integrētas riska kontroles sistēmas, lai pārvaldītu riskus, kas tam rodas.

4.6.3 Paskaidrojumi

Cilvēkfaktori un organizatoriskie faktori ietver sistēmiskas perspektīvas izmantošanu, kad tiek apsvērta mijiedarbība starp cilvēkfaktoriem, tehnoloģiskajiem faktoriem un organizatoriskajiem faktoriem. Cilvēkfaktori un organizatoriskie faktori organizācijai ir jāņem vērā, īstenojot dzīves cikla pieeju. Tas nozīmē, ka tiek noteikti un izvērtēti cilvēkfaktori un organizatoriskie faktori drošības pārvaldības darbībās saistībā ar uzņēmējdarbības mērķiem, pārvaldību, darbībām, cilvēku veiktspēju, uzdevumiem un darbvietas iekārtojumu visā sistēmas dzīves ciklā, piemēram, no nodošanas ekspluatācijā līdz ekspluatācijas pārtraukšanai. Cilvēkfaktoru un organizatorisko faktoru stratēģijā ir norādīta sistemātiska pieeja cilvēkfaktoru un organizatorisko faktoru integrēšanai drošības pārvaldības darbībās.

Organizācijai ir jāpiesaista attiecīgi cilvēkfaktoru un organizatorisko faktoru speciālisti, kuri vajadzīgi tās uzņēmējdarbības atbalstam. "Cilvēkfaktoru un organizatorisko faktoru speciālisti" nozīmē, ka iesaistītajam personālam ir jābūt kvalificētam atbilstoši valsts un/vai starptautiskiem standartiem attiecīgajā jomā, piemēram, šādam personālam būtu jāatbilst dalības prasībām, ko noteicis Eiropas Ergonomistu reģistrācijas centrs vai citas tamlīdzīgas struktūras. Lielās organizācijās var būt cilvēkfaktoru nodaļas, kur strādā cilvēkfaktoru speciālisti, kuri atbalsta organizāciju. Mazas organizācijas var uzdot visu līmeņu vadītājiem pienākumu konstatēt vajadzību piesaistīt cilvēkfaktoru speciālistu, kad nepieciešams.

Vairāk informācijas par stratēģiju attiecībā uz cilvēkfaktoriem un organizatoriskajiem faktoriem ir atrodams 5. pielikumā.

4.6.4 Pierādījumi

- *Pieteikuma iesniedzējs stratēģijā ir izklāstījis, kā cilvēkfaktori un organizatoriskie faktori tiek integrēti, lai riskus, kas saistīti ar mijiedarbību starp cilvēku uzvedību, organizatoriskajiem apstākļiem un tehnoloģiju, pienācīgi ņemtu vērā attiecīgajos SMS procesos. Piemēram, tas varētu nozīmēt, ka ir plāns, kas nosaka, kā tiek ņemti vērā cilvēkfaktori un organizatoriskie faktori attiecībā*

uz jaunu signalizācijas sistēmu visos dzīves cikla posmos. Saistībā ar to pieteikuma iesniedzējam ir skaidri jānorāda, kur ir atrodama plašāka informācija par attiecīgajām procedūrām **(4.6.1. punkts)**.

- *Piemēram, attiecībā uz jauniem vai pārveidotiem projektiem, procedūrām, apmācību, darba slodzi un darba vidi, lai nodrošinātu sistēmas drošumu un efektivitāti visā tās dzīves laikā, tiek īstenots uz lietotāju vērsts projektēšanas process, kura pamatā ir cilvēciski un organizatoriski principi un metodes, kā arī lietotāju iesaistīšana.*
- *Tiek ievēroti pieejamie projektēšanas standarti, ar kuriem ņem vērā cilvēkfaktorus un organizatoriskos faktorus, kā arī paraugprakse. Attiecīgie standarti ir, piemēram, ISO sērija 11064 "Ergonomiska kontroles centru projektēšana" un ISO sērija 9241 "Cilvēka–sistēmas mijiedarbības ergonomika".*
- *Tiešos lietotājus iesaista projektēšanas procesā, piemēram, prasību definēšanā, vēlākā izstrādes un testēšanas procesā.*
- *Uz lietotāju vērsts projektēšanas process ir iteratīvs process, kam ir vairāki posmi. Tiek veiktas dažādas analīzes, lai saprastu un noteiktu lietošanas kontekstu (piemēram, personāla un kompetenču analīze, uzdevumu analīze un risku analīze). Lietotāju prasības nosaka, pamatojoties uz šiem analīzes veidiem. Projektu risinājumus, tostarp saskarņu, darba vietu, apmācības, procedūru un organizācijas projektus, izstrādā tā, lai tiktu izpildītas lietotāju prasības. Projektus izvērtē, izmantojot oficiālas metodes, piemēram, uzdevumu analīzi, simulāciju, riska novērtēšanu, speciālistu izvērtējumus, lietotāju izvērtējumus, pārbaudi un apstiprināšanu.*

4.6.5 Pierādījumu piemēri

Cilvēkfaktoru un organizatorisko faktoru stratēģijas kopija, kurā ir sīki izklāstīts, kā tiek ņemta vērā cilvēkfaktoru un organizatorisko faktoru speciālistu un metožu izmantošana.

Organizācija veic analīzi, izmantojot uz pierādījumiem balstītas ekspluatācijas un atbalsta procesu metodes visos dzīves cikla posmos, sākot no projektēšanas un beidzot ar likvidāciju. Analīzē ir jānosaka visi cilvēkfaktori un organizatoriskie faktori, kā arī veiktspēju ietekmējošie faktori, kas ietekmēs dzelzceļa drošību un drošības pārvaldības darbības, kuras vajadzīgas, lai kontrolētu risku.

Cilvēkfaktoru un organizatorisko faktoru stratēģijā ir jāparāda ieviestās drošības pārvaldības darbības, kā arī pieeja stratēģijas efektivitātes pārraudzībai un uzlabošanai. Stratēģijas pamatā ir jābūt proaktīvai pieejai, bet vajadzības gadījumā tajā ir jāparedz arī reaktīvas darbības.

Vajadzētu būt norādītām drošības pārvaldības darbībām, kas ir saistītas ar atbalsta funkcijām un sistēmām, uzdevumu izstrādi, personāla līmeņiem, apmācību, aprīkojuma projektēšanu un izmantošanu, procedūrām un saziņas protokoliem.

Šādā stratēģijā var būt norādīts, piemēram, kā cilvēkfaktori un organizatoriskie faktori tiek integrēti izmaiņu pārvaldības procesā. Cilvēkfaktoru integrēšana nozīmē procesu, kad cilvēkfaktori un ergonomika tiek integrēti sistēmtehnikas procesā. Cilvēkfaktoru integrēšanas plānā ir paredzēta sistemātiska pieeja saistības noteikšanai starp visām projekta darbībām un cilvēkfaktoru jomu. Cilvēkfaktoru projektēšana nozīmē cilvēka īpašību integrēšanu sistēmas definēšanā, izstrādē, pilnveidošanā un izvērtēšanā, lai optimizētu cilvēka–mašīnas veiktspēju atbilstoši ekspluatācijas nosacījumiem.

Ja ekspluatācijas procesi ietver kompleksus darba laika modeļus, cilvēkfaktoru un organizatorisko faktoru stratēģijā ir jāiekļauj noguruma riska pārvaldības programma.

4.6.6 Atsauces un standarti

- Wickens, C.D., Lee, J.D., Liu, Y & Gordon Becker, S.E (2004. gads). *An Introduction to Human Factors Engineering*. New Jersey: Pearson Education. ISBN-13: 978-0131837362
- ISO standartu sērijas, piemēram,
- ISO sērija 6385:2004 “Ergonomikas principi darba sistēmu izstrādē”
- ISO sērija 11064 “Ergonomiska kontroles centru projektēšana”
- ISO sērija 9241 “Cilvēka–sistēmas mijiedarbības ergonomika”
- ISO sērija 10075 “Ergonomikas principi saistībā ar garīgo darba slodzi”
- EEMUA 191. “Trauksmes sistēmas — izstrādes, pārvaldības un iepirkuma rokasgrāmata”
- UIC 651 “Vadītāja kabīņu iekārtojums lokomotīvēs, motorvagonos, motorvagonu vilcienos un piekabvagonos”
- Dzelzceļa drošības un standartu padome (2008. gads). “Saprast cilvēkfaktorus — rokasgrāmata dzelzceļa nozarei”

4.6.7 Uzraudzības jautājumi

Pārbaudīt, vai cilvēkfaktoru jautājumi tiek ņemti vērā lēmumu pieņemšanas procesos risku pārvaldībai, veicot riska novērtēšanu, izmaiņu pārvaldību un aktīvu pārvaldību.

Pārbaudīt, vai ekspluatācijas dokumentos ir atspoguļota apņemšanās pārvaldīt cilvēkfaktorus, īstenojot ergonomisku projektēšanu (piemēram, lietotājdraudzīgs projekts, vienkārša valoda, grafika kā norādījumu papildinājums, vienkārša atjauninājumu pārvaldība), lai atbalstītu risku pārvaldību.

Pārbaudīt, vai veikspējas pārraudzībā dzelzceļa pārvadājumu uzņēmums / infrastruktūras pārvaldītājs savu analīzi vērš uz cilvēkfaktoriem kā uz negadījumu, starpgadījumu vai bīstamu notikumu galvenajiem vai pakārtotajiem cēloņiem.

Pārbaudīt, vai ir dokumentēti tādu korektīvu pasākumu piemēri, kas veikti, lai likvidētu faktorus, kuri ietekmē cilvēku veikspēju un kaitē drošībai.

5 Eksploatācija

5.1 Eksploatācijas plānošana un kontrole

5.1.1 Normatīvā prasība

- 5.1.1. Kad organizācija plāno, izstrādā, īsteno un pārskata savus eksploatācijas procesus, tā nodrošina, ka eksploatācijas laikā tiek:
- (a) piemēroti pieļaujamā riska kritēriji un riska kontroles pasākumi (sk. 3.1.1. Riska novērtējums);
 - (b) izstrādāts(-i) drošības mērķu sasniegšanas plāns(-i) (sk. 3.2. Drošības mērķi un plānošana);
 - (c) vākta informācija eksploatācijas pasākumu piemērošanas pareizības un efektivitātes mērīšanas vajadzībām (sk. 6.1. Uzraudzība).
- 5.1.2. Organizācija nodrošina, ka eksploatācijas pasākumi atbilst ar drošību saistītajām prasībām, kas noteiktas piemērojamajās savstarpējas izmantojamības tehniskajās specifikācijās un attiecīgajos valstu noteikumos, un citām attiecīgajām prasībām (sk. 1. Organizācijas konteksts).
- 5.1.3. Lai kontrolētu riskus, kad tas ir būtiski eksploatācijas darbību drošībai (sk. 3.1.1. Riska novērtējums), ņem vērā vismaz šādus aspektus:
- (a) esošu vai jaunu vilcienu maršrutu un jaunu dzelzceļa pārvadājumu pakalpojumu plānošana, ietverot jaunu ritekļu veidu ieviešanu, nepieciešamību nomāt ritekļus un/vai pieņemt darbā personālu no trešām personām un informācijas par tehnisko apkopi eksploatācijas vajadzībām apmaiņu ar struktūrām, kas atbildīgas par tehnisko apkopi;
 - (b) vilcienu kustības grafiku izstrāde un ieviešana;
 - (c) vilcienu vai ritekļu sagatavošana pirms kustības uzsākšanas, ietverot pārbaudes pirms izbraukšanas un vilcienu sastāvu veidošanu;
 - (d) vilcienu kursēšana vai ritekļu kustība dažādos eksploatācijas apstākļos (normālā, traucētā un avārijas režīmā) ;
 - (e) eksploatācijas pielāgošana pieprasījumiem par izņemšanu no eksploatācijas un paziņojumiem par atgriešanu eksploatācijā, ko izdod par tehnisko apkopi atbildīgās struktūras;
 - (f) ritekļu kustības atļaujas;
 - (g) saskarņu izmantojamība vilcienu vadītāju kabīnēs un vilcienu kustības vadības centros un ar tehniskās apkopes personāla izmantotajām iekārtām.
- 5.1.3. Lai kontrolētu riskus, kad tas ir būtiski eksploatācijas darbību drošībai (sk. 3.1.1. Riska novērtējums), ņem vērā vismaz šādus aspektus:
- (c) drošu transporta robežu noteikšana satiksmes plānošanas un vadības vajadzībām, pamatojoties uz infrastruktūras konstrukcijas parametriem;
 - (d) satiksmes plānošana, tostarp kustības grafiks un vilcienu ceļu iedalīšana;

(e) satiksmes pārvaldība reāllaikā normālā ekspluatācijas režīmā un traucētos ekspluatācijas režīmos, piemērojot satiksmes izmantošanas ierobežojumus un īstenojot satiksmes traucējumu pārvaldību;

(f) īpašu sūtījumu pārvadāšanas nosacījumu noteikšana.

5.1.4. Lai pārvaldītu pienākumu sadalījumu, kad tas ir svarīgi ekspluatācijas darbību drošībai, organizācija apzina pienākumus, kas attiecas uz drošas vilcienu kursēšanas un ritekļu kustības koordināciju un pārvaldību, un nosaka, kā attiecīgie uzdevumi, kuri ietekmē visu pakalpojumu sniegšanas drošību, tiek iedalīti kompetentajam personālam organizācijā (sk. 2.3. Organizatoriskās funkcijas, pienākumi, pārskatbildība un pilnvaras) un attiecīgā gadījumā citām kvalificētām trešām personām (sk. 5.3. Darbuzņēmēji, partneri un piegādātāji).

5.1.4. Lai pārvaldītu pienākumu sadalījumu, kad tas ir svarīgi ekspluatācijas darbību drošībai, organizācija apzina pienākumus, kas attiecas uz dzelzceļu tīkla plānošanu un ekspluatāciju, un nosaka, kā attiecīgie uzdevumi, kuri ietekmē visu pakalpojumu sniegšanas drošību, tiek iedalīti kompetentajam personālam organizācijā (sk. 2.3. Organizatoriskās funkcijas, pienākumi, pārskatbildība un pilnvaras) un attiecīgā gadījumā citām kvalificētām trešām personām (sk. 5.3. Darbuzņēmēji, partneri un piegādātāji).

5.1.5. Lai pārvaldītu informāciju un saziņu, kad tas ir svarīgi ekspluatācijas darbību drošībai (sk. 4.4. Informācija un saziņa), attiecīgajam personālam (piemēram, vilcienu apkalpēm) sniedz sīku informāciju par visiem konkrētajiem brauciena apstākļiem, tostarp par attiecīgajām izmaiņām, kas var radīt briesmas, pagaidu vai pastāvīgiem ekspluatācijas ierobežojumiem (piemēram, konkrēta ritekļu veida vai konkrētu maršrutu dēļ) un nosacījumiem, kas attiecas uz īpašiem sūtījumiem, ja tie ir nepieciešami.

5.1.5. Lai pārvaldītu informāciju un saziņu, kad tas ir svarīgi ekspluatācijas darbību drošībai (sk. 4.4. Informācija un saziņa), attiecīgo personālu (piemēram, signalizētājus) informē par īpašām maršrutizācijas prasībām vilcieniem un ritekļu kustību, tostarp par attiecīgajām izmaiņām, kas var radīt briesmas, pagaidu vai pastāvīgiem ekspluatācijas ierobežojumiem (piemēram, sliežu ceļa tehniskās apkopes dēļ) un nosacījumiem, kas attiecas uz īpašiem sūtījumiem.

5.1.6. Lai pārvaldītu kompetenci, kad tas ir svarīgi ekspluatācijas darbību drošībai (sk. 4.2. Kompetence), organizācija saskaņā ar piemērojamajiem tiesību aktiem (sk. 1. Organizācijas konteksts), savam personālam nodrošina:

- (a) mācību un darba instrukciju ievērošanu un korektīvu pasākumu veikšanu vajadzības gadījumā;
- (b) īpašu apmācību gadījumā, ja gaidāmas izmaiņas, kas ietekmē ekspluatācijas norisi vai personālam uzticētos uzdevumus;
- (c) pienācīgu pasākumu veikšanu pēc negadījumiem un starpgadījumiem.

5.1.2 Mērķis

Pieteikuma iesniedzējam ir jāparāda, ka tas ir ieviesis attiecīgus procesus ekspluatācijas risku pārvaldībai ar SMS starpniecību, tostarp pārliecinoties, vai darbinieki saprot savas funkcijas, ekspluatācijas riskus, ar kuriem viņi saskaras, un to, kādi ir kontroles pasākumi, un vai darbinieki ir pietiekami kompetenti un atbilstoši apmācīti pārvaldīt šādus riskus atbilstoši drošības pārvaldības sistēmas dokumentācijai.

Pieteikuma iesniedzējam ir jānodrošina, ka ritekļi vai infrastruktūra tiek ekspluatēta droši saskaņā ar piemērojamām prasībām dažādos darbības apstākļos (t. i., normālas ekspluatācijas, traucētas ekspluatācijas vai avārijas režīmā), ietverot arī aktīvu izmantošanu testēšanas mērķiem (piemēram, ritekļu gaitas īpašību testēšana pirms atļaujas piešķiršanas) un izņēmuma apstākļos (piemēram, neierasti sūtījumi — tādu lielu

nedalāmu priekšmetu, ko nevar pārvest ar citiem transportlīdzekļiem, piemēram, betona siju / tilta kopņu u. tml., transportēšana).

5.1.3 Paskaidrojumi

Iepriekš minētā tiesību akta 5.1.3., 5.1.4. un 5.1.5. punktā, kur šī prasība attiecas uz infrastruktūras pārvaldītājiem, noteikumi, kas rakstīti ar melniem burtiem, ir aizstāti ar zilā krāsā rakstītiem noteikumiem.

Direktīvā (ES) 2016/798 ir noteikts, ka dzelzceļa pārvadājumu uzņēmumiem un infrastruktūras pārvaldītājiem ir jāizveido SMS, lai pārvaldītu drošības apdraudējumus, kas saistīti ar to dzelzceļa darbībām. Drošības pārvaldības jomā pastāv vienprātība, ka drošībai ir jābūt pēc iespējas integrētai parastajos uzņēmējdarbības procesos. Tas vajadzīgs tādēļ, lai uzņēmums pievērstos drošībai tikpat lielā mērā kā jebkuram citam uzņēmējdarbības procesam, tādējādi samazinot konfliktus starp dažādajiem procesiem.

ISO vadlīnijās (N360), kas ir SL pielikuma papilddokuments, ir noteikts, ka 8. noteikuma (Ekspluatācija) mērķis ir noteikt elementus, kas jāīsteno organizācijas darbībās, lai nodrošinātu pārvaldības sistēmas prasību izpildi, kā arī to, ka tiek ņemti vērā prioritārie riski un iespējas. Turklāt ir noteikts, ka var paredzēt arī papildu prasības (konkrētai disciplīnai) saistībā ar ekspluatācijas plānošanu un kontroli. Tās jo īpaši nedrīkst būt kaitējošas uzņēmuma uzņēmējdarbībai, bet tām ir jānodrošina pietiekama sistēma, lai kontrolētu galveno drošības jautājumu pārvaldību organizācijas uzņēmējdarbības procesos.

Papildus ir norādītas skaidras saites starp ekspluatācijas prasībām un citām pārvaldības sistēmas prasībām (līdzīgi ECM regulas III pielikumā noteiktajai pieejai), lai skaidri parādītu, ka saistībā ar konkrētajām pārvaldības sistēmas prasībām ir jāņem vērā īpašas ekspluatācijas prasības (piemēram, maršrutu plānošana dzelzceļa pārvadājumu uzņēmumiem ir darbība, par kuru jāveic riska novērtēšana). Šī pieeja nav paredzēta kā izsmeljoša, bet tās mērķis ir identificēt konkrētus jautājumus, kas, kā uzskata iestādes, ir būtiski (pamatojoties uz to pieredzi) un tāpēc ir jāpārbauda to novērtēšanas vai uzraudzības pasākumu laikā. Dzelzceļa pārvadājumu uzņēmumi un infrastruktūras pārvaldītāji nedrīkstētu koncentrēties tikai uz šīm konkrētajām prasībām, kad tie izstrādā savu drošības pārvaldības sistēmas kārtību (neņemot vērā, piemēram, citus drošības apdraudējumus). Jebkurā gadījumā dzelzceļa pārvadājumu uzņēmumiem un infrastruktūras pārvaldītājiem ir jāpiemēro drošības pārvaldības sistēmas prasības (piemēram, riska novērtēšana, pārraudzība, kompetence, informācija un paziņošana) visiem saviem attiecīgajiem uzņēmējdarbības procesiem, lai parādītu, ka drošības apdraudējumi tiek pienācīgi kontrolēti.

SMS integrēšanai uzņēmējdarbības/ekspluatācijas procesos ir ļoti svarīga nozīme, un, lai sasniegtu šo mērķi, organizācijai ir jāizpilda piemērojamās SITS (5.1.2. punkts), piemēram, SITS OPE, un paziņotie valsts noteikumi, ja saskarnes prasības nav pilnīgi atrunātas SITS. Dalībvalsts vai tās iestāde var arī publicēt pieņemamus atbilstības nodrošināšanas līdzekļus, lai veicinātu atbilstību to valsts noteikumiem. Attiecīgā gadījumā būtu jāapsver vismaz šādi ekspluatācijas procesi:

- *darbības infrastruktūra (infrastruktūras maršrutu un aprīkojuma kontrole, ritekļu kustības atļaušana visos apstākļos un infrastruktūras uzturēšanas nodrošināšana — vilcienu vadības un signalizācijas lauka iekārta(-s));*
- *vilcienu ekspluatācija (maršrutu un attiecīgu termiņu izstrāde, vilcienu sagatavošanas pārvaldība, vilcienu vadīšanas nodrošināšana, ritekļu apkalpes personāls, testēšana, uzturēšana un remonts);*
- *manevru pakalpojumi (ritekļu kustība, lai nokomplektētu vai izkomplektētu vilcienu).*

SITS OPE šajā ziņā ir būtiska, jo tajā ir izklāstīti darbības pamatprincipi (DPP), kuriem ir jābūt atspoguļotiem attiecīgajās SMS daļās, tāpēc atbilstību SITS OPE var izmantot, lai parādītu atbilstību attiecīgajām iepriekš minētajām SMS prasībām.

Informācijas apmaiņa ekspluatācijas mērķiem par ritekļu tehnisko apkopi (**5.1.3. punkta a) apakšpunkts**) ar ECM un turētājiem ir noteikta ECM regulas 5. panta 3. punktā. Tas attiecas arī uz tehniskās apkopes grafiku un ierobežojumiem, ko ECM ir noteikusi tehniskās apkopes laikā (īstermiņa plānošana).

Ja ir sniegta atsauce uz vilcienu grafiku izstrādi un īstenošanu (**5.1.3. punkta b) apakšpunkts**), tas nozīmē, ka pieteikuma iesniedzējam ir jāparāda, kā tas ar riska novērtēšanas starpniecību ir pārvaldījis darbības radīto risku tā organizācijā un saskarnē ar citiem dalībniekiem. Piemēram, pieteikuma iesniedzējam ir jāparāda, ka tas ir ņēmis vērā:

- *papildu darba slodzi signalizācijas darbiniekiem, kad noteiktos laikos tiek palielināts vilcienu skaits;*
- *atbilstošus ekspluatācijas līgumus ar attiecīgo(-ajiem) infrastruktūras pārvaldītāju(-iem) par satiksmes apturēšanu, atjaunošanu, informācijas apmaiņu un visiem citiem pakalpojumiem, ko uzskata par vajadzīgiem;*
- *ar sliežu ceļa tehnisko apkopi saistīto risku pārvaldību, kad vilcieni veic braucienus 24 stundas dienā.*

Jauns dzelzceļa pārvaldājumu pakalpojums (**5.1.3. punkta a) apakšpunkts**) var ietvert jaunu kravas veidu pārvaldījumus.

“Ritekļu kustībai” (**5.1.3. punkta d) apakšpunkts**) ir plašāka nozīme nekā “vilcienu kustībai” (t. i., plānotai ritekļu kustībai) un atļaujām, ko piešķir pirms vilciena izbraukšanas. Tā var ietvert arī salūzuša vilciena atjaunošanu, sliežu ceļa tehniskās apkopes mašīnu kustību vai neplānotu bojāta ritekļa aizstāšanu vilcienā pirms vilciena izbraukšanas.

Atbilstoši 1.1. pantam UIC brošūrā 502-1 ir ieteikta šāda termina “īpaši sūtījumi” (5.1.5. punkts) definīcija: *“Sūtījumu uzskata par īpašu, ja tā ārējie izmēri, svars vai īpašības attiecībā pret transportēšanā iesaistītā dzelzceļa pārvaldājumu uzņēmuma stacionāro iekārtu vai vagonu rada īpašas grūtības un tāpēc to var pieņemt tikai īpašos tehniskos vai ekspluatācijas apstākļos.”*

Infrastrukturā pārvaldītājam ir jānorāda un jānodrošina apstākļi un pasākumi ritekļa izmantošanai testiem tīklā attiecīgajā termiņā, kas noteikts Direktīvas (ES) 2016/797 21. panta 3. un 5. punktā (5.1.2. punkts).

Maršrutu saderības pārbaudi atskaitēs ir ietverts tā ritekļa/vilciena raksturojums, kas izvērtēts, ņemot vērā plānotos ekspluatācijas maršrutus, ietverot iespējamo(-os) novirzīšanas maršrutu(-us), ko norādījuši infrastruktūras pārvaldītāji (SITS OPE (ES) 2015/995, 4.2.2.5. punkts).

Ekspluatācijas maršruta raksturojuma pamatā ir infrastruktūras reģistrs (RINF) un/vai infrastruktūras pārvaldītāja sniegtā informācija.

Ja jebkura no pusēm konstatē problēmas, dzelzceļa pārvaldājumu uzņēmumam un infrastruktūras pārvaldītājam ir jārod kopīgs risinājums.

Cilvēkfaktori un organizatoriskie faktori ir jāņem vērā ekspluatācijas plānošanā saistībā ar, piemēram, darba grafikiem, noguruma pārvaldību, stresu, darba vidi (fizisko un psihosociālo), darba vietām un darba procesiem, u. tml.

Ekspluatācijas plānošanu un kontroli attīsta, lai pastāvīgi uzlabotu drošības kultūru. Drošības kultūra ir jāņem vērā saistībā ar, piemēram, darba slodzi, darba vidi (fizisko un psihosociālo), darba procesiem u. tml. Tas vajadzīgs, lai nodrošinātu, ka izmaiņām vai pasākumiem nav negatīvas ietekmes uz cilvēku veikspēju vai organizatorisko drošību.

5.1.4 Pierādījumi

- *Informācija, kas liecina, ka, plānojot, izstrādājot, īstenojot un pārskatot savus ekspluatācijas procesus, pieteikuma iesniedzējs plāno sasniegt drošības mērķus, piemēro riska novērtēšanas pasākumus un pārbauda rezultātus, norādot arī, kur ir atrodamā papildu informācija par procedūrām (**5.1.1. punkta a)–c) apakšpunkts**).*
- *Pierādījumi, ka organizācija pārzina un faktiski īsteno visas obligāto drošības prasību kategorijas, kas ir attiecināmas uz tās darbību, izklāstot arī to, kā SMS nodrošina atbilstību šādām prasībām.*

- Informācija, kas apliecina, ka pieteikuma iesniedzējs pārlicinās, vai tā ekspluatācijas pasākumi atbilst piemērojamām prasībām (tiesību aktiem, standartiem u. tml.) **(5.1.2. punkts)**.
- Saistībā ar ritekļu tipa atļauju un/vai atļauju ritekļa laišanai tirgū infrastruktūras pārvaldītājs spēj norādīt un nodrošināt **(5.1.2. punkts)**:
 - ekspluatācijas nosacījumus, kas piemērojami ritekļa izmantošanai testos tīklā, pamatojoties uz pieteikuma iesniedzēja sniegto informāciju atļaujas saņemšanai;
 - jebkādos vajadzīgos pasākumus, kas jāveic infrastruktūrā, lai nodrošinātu drošu un uzticamu ekspluatāciju testu laikā tīklā, un/vai
 - jebkādos vajadzīgos pasākumus infrastruktūras iekārtās testu veikšanai tīklā.
- Attiecībā uz pārbaudi pirms apstiprinātu ritekļu izmantošanas (pārstrādātās Savstarpējas izmantojamības direktīvas (IOD) 23. panta 1. punkts) un jo īpaši maršrutu saderības pārbaudi (pārstrādātās IOD 23. panta 1. punkta a) un b) apakšpunkts) dzelzceļa pārvaldītāju uzņēmums savā SMS var identificēt un iesniegt (CSM attiecībā uz SMS prasībām 5.1.3. punkta a) apakšpunkts) pierādījumus, procedūras un ierakstus, kas apliecina, ka ritekļi ir saderīgi ar maršrutu, kurā to ir plānots ekspluatēt, un ir pienācīgi integrēti vilciena sastāvā (sk. arī SITS OPE (2015/995, 4.2.2.5. punkts)).
- Pierādījumi par ekspluatācijas dokumentācijas atbilstību prasībām attiecībā uz ekspluatācijas (un tehniskās apkopes) pārvaldību organizatoriskajās un fiziskajās robežās, piemēram, organizatoriskās, tehniskās un ekspluatācijas saskarnes ar kaimiņvalstu infrastruktūru, robežstacijām, mijiedarbība ar citiem dzelzceļa pārvaldītāju uzņēmumiem vai infrastruktūras pārvaldītājiem u. tml. **(5.1.2. punkts)**.
- Informācija, kā notiek ekspluatācijas pasākumu risku pārvaldība ar riska novērtēšanas procesa starpniecību, aptverot iepriekš minētajās prasībās izklāstītos elementus **(5.1.3. punkta a) apakšpunkts un c)–f) apakšpunkts)**.
- Pierādījumi, ka par tehnisko apkopi atbildīgā struktūra ievēro Direktīvas (EK) 2016/798 14. panta 2. punktu **(5.1.3. punkta f) apakšpunkts)**.
- Informācija, kā tiek pārvaldīta atbildība, arī atbildība par noguruma riska pārvaldību, nolūkā garantēt ekspluatācijas pasākumu drošību **(5.1.4. punkts)**.
- Informācija, kā organizācija pārvalda informāciju un saziņu nolūkā garantēt ekspluatācijas pasākumu drošību **(5.1.5. punkts)**.
- Informācija par kompetences pārvaldības sistēmu un saistītajām procedūrām un par to, kāda ir to saistība ar konkrētiem darba vai uzdevumu norādījumiem, lai uzturētu ekspluatācijas pasākumu drošību **(5.1.6. punkts)**.
- Pierādījumi, ka ekspluatācijas dokumentācija (procedūras, darba norādījumi u. tml.) vajadzības gadījumā tiek atjaunināta (sk. arī 4.5.3. punktu).

5.1.5 Pierādījumu piemēri

Obligāto prasību (tostarp SITS) uzskaitījums un informācija par to, kā pieteikuma iesniedzējs tās izpilda (sk. arī 2. punktu).

Skaidrojums, kā tiek pārvaldīti ekspluatācijas riski ar riska novērtēšanas procesa starpniecību un kā tiek nodrošināta ekspluatācijas drošības mērķu sasniegšana. Ir norādītas saites uz attiecīgo procedūru atrašanās vietu.

Izklāsts, kā CMS veicina ekspluatācijas risku kontroli un kā tiek pārvaldīta informācijas aprīte un saziņa, lai nodrošinātu risku pienācīgu kontroli.

Informācija par pieteikuma iesniedzēja ritošā sastāva tehniskās apkopes sistēmu, norādot arī saites uz sīki izstrādātu dokumentāciju, kas to apliecina (ja nav ECM vai sertifikācijas shēmas).

Ziņas par procedūru pārbaudi veikšanai pirms izbraukšanas (SITS OPE), lai nodrošinātu atbilstības pārbaudi attiecībā uz:

- *bremzēšanu (bremzēšanas lapas sagatavošana);*
- *vilciena sastāvu;*
- *priekšējiem un aizmugurējiem signāliem;*
- *slodzes un vilkto ritekļu stāvokli.*

Neatbilstību konstatēšanai izmantotā procesa kopija un informācija par to, kā tiek nodrošināta vajadzīgo pasākumu veikšana, piemēram, ritekļa izņemšana no ekspluatācijas, salūzušas/bojātas sastāvdaļas/aprīkojuma/ritekļa nomaiņa vai ekspluatācijas ierobežojumu ieviešana.

Dokuments, kurā ir norādīti ritekļu veidi, kas izmantojami katrā konkrētajā maršrutā, veicamo darbību veidi un jo īpaši:

- *jebkuri ierobežojumi konkrētu ritekļu veidu ekspluatācijai;*
- *jebkuri ierobežojumi konkrētu ritekļu veidu ekspluatācijai konkrētos maršrutos;*
- *tehniskās apkopes papildu prasības attiecībā uz konkrētiem maršrutiem (sk. arī 5.2. punktu).*

Dokuments, kurā ir aprakstītas jebkuras papildu prasības attiecībā uz traucētas ekspluatācijas situāciju pārvaldību (piemēram, ja ir noticis starpgadījums ar ritekli) tīklā(-os), ko aptver darbības telpa.

Pastāv noguruma pārvaldības process, kas piemērojams darbiniekiem, kuriem ir neregulārs darba laiks. Procesā pamatā ir uz pierādījumiem balstītas metodes un profesionālā kompetence. Procesā ņem vērā, ka, īstenojot visaptverošu pieeju noguruma riska pārvaldībai, ir jāapsver vairāki faktori. Noguruma pārvaldības programmā ir jābūt iekļautai darba vides un darba uzdevumu plānošanai un kontrolei, lai, ciktāl tas ir praktiski iespējams, mazinātu noguruma ietekmi uz darbaspēka modrību un veikspēju atbilstoši riska līmenim un ekspluatācijas veidam.

Saistībā ar atbilstību DPP un SITS OPE ir iesniegti pierādījumi, kas apliecina, ka dzelzceļa pārvadājumu uzņēmums var nodrošināt, ka (tikai kā ilustratīvs piemērs):

- *vilcienu var ekspluatēt kādā līnijas daļā tikai tad, ja vilciena sastāvs ir saderīgs ar infrastruktūru (3. DPP).*

Minētais attiecas uz apstiprinājumu par vilciena saderību ar maršruta infrastruktūru, kurā to plānots ekspluatēt, pirms tiek atļauta tā kustība. Vilciena un infrastruktūras savstarpējo saderību ietekmē galvenokārt ritekļa izmēri un jebkura uz tā uzliktā slodze, atstatumi starp vilcienu un infrastruktūru vai vilcieniem, kas atrodas uz blakusesošām sliedēm (sliežu platums), minimālā vajadzīgā vilciena bremzēšanas jauda, vilciena svars un garums un infrastruktūras jauda un spēja.

Ir pierādījumi, ka:

- *tiek veiktas pārbaudes pirms izbraukšanas, lai nodrošinātu, ka pirms vilciena brauciena sākšanas vai brauciena laikā tā pasažieri, apkalpe un kravas tiek pārvadātas droši (4. DPP).*

Minētais attiecas uz vilcienu un tā gatavību kustībai. Tas ietver, piemēram, tādus drošības aspektus kā vilciena bremzēšanas jauda, ātrums, ar kādu vilcienam atļauts braukt, vilciena sastāva veidošana un sakabināšana, kravas identificēšana, iekraušana un nostiprināšana, pienācīgas informācijas sniegšana vilciena sagatavošanas un ekspluatācijas personālam. Mērķis ir novērst sadursmes un nobraukšanu no sliedēm, ko var izraisīt vairāki riski.

5.1.6 Atsauces un standarti

- ISO N360 JTCG konceptuāls SL pielikuma papilddokuments
- UIC brošūra Nr. 502-1

- [RID](#)
- *Rokasgrāmata par SITS OPE*

5.1.7 Uzraudzības jautājumi

Ekspluatācijas darbību uzraudzība ir jāveic, pievēršoties diskrētām jomām un izvērtējot tās sīkāk, lai redzētu, kā tās ir atspoguļotas uzraugāmās organizācijas drošības pārvaldības sistēmā un vai tajās strādā atbilstošie darbinieki atbilstošajā vietā un veic atbilstošo darbu. Tādējādi VDI varēs redzēt, vai SMS tiek attiecināta uz visām darbībām kā uz vienotu kopumu, vai arī tās tiek pārvaldītas atsevišķi un ir vāji saistītas ar drošības mērķiem un vispārējo stratēģiju.

Veicot uzraudzību, jo īpaši ir jāpārbauda:

- *tas, kā augstāka līmeņa SMS dokumenti tiek pārveidoti saskaņotos vietējos norādījumos, ko izmanto, lai pārvaldītu risku ekspluatācijas līmenī;*
- *avārijas apstākļu vai neplānotu situāciju pārvaldība;*
- *tas, kā tiek pārvaldītas darbības robežas, tostarp pasākumi mijiedarbībai ar citām personām;*
- *noguruma pārvaldības kārtība;*
- *bīstamu vielu pārvaldība;*
- *bīstamu kravu pārvadāšanas kārtība, tostarp organizācijas personāla apmācība, funkcijas un pienākumi, kā noteikts RID 1.3., 1.4. un 1.8. nodaļā, pēc vajadzības sadarbojoties ar jebkuru citu bīstamo kravu pārvadājumu kompetento iestādi;*
- *Compliance with the Fundamental Operating Principles set out in the TSI OPE.*

5.2 Aktīvu pārvaldība

5.2.1 Normatīvā prasība

5.2.1.	Organizācija pārvalda ar fiziskajiem aktīviem saistītos drošības apdraudējumus visā aktīvu dzīves ciklā (sk. 3.1.1. Riska novērtējums) no projekta līdz likvidācijai un izpilda ar cilvēkfaktoriem saistītās izmantošanas prasības.
5.2.2.	Organizācija: <ul style="list-style-type: none">(a) nodrošina, ka aktīvus izmanto paredzētajām vajadzībām, vienlaikus uzturot tos ekspluatācijai drošā stāvoklī, attiecīgā gadījumā saskaņā ar Direktīvas (ES) 2016/798 14. panta 2. punktu, un uzturot tiem paredzēto veiktspējas līmeni;(b) pārvalda aktīvus normālā un traucētā ekspluatācijas režīmā;(c) iespējami drīz pirms aktīva ekspluatācijas vai tās laikā konstatē neatbilstības ekspluatācijas prasībām, tostarp attiecīgi piemēro izmantošanas ierobežojumus, lai nodrošinātu aktīva uzturēšanu ekspluatācijai drošā stāvoklī (sk. 6.1. Uzraudzība).
5.2.3.	Organizācija nodrošina, ka aktīvu pārvaldības pasākumi attiecīgā gadījumā atbilst visām pamatprasībām, kas noteiktas attiecīgajās savstarpējas izmantojamības tehniskajās specifikācijās (sk. 1. Organizācijas konteksts).
5.2.4.	Lai kontrolētu riskus, kad tas ir būtiski tehniskās apkopes nodrošināšanai (sk. 3.1.1. Riska novērtējums), ņem vērā vismaz šādus aspektus: <ul style="list-style-type: none">(a) aktīva uzturēšanai ekspluatācijai drošā stāvoklī paredzētās tehniskās apkopes nepieciešamības konstatēšana, pamatojoties uz aktīva plānoto un faktisko izmantojumu un tā konstrukcijas parametriem;(b) pārvaldība, kas attiecas uz aktīva izņemšanu no ekspluatācijas tehniskās apkopes veikšanai, ja konstatēti bojājumi vai ja aktīva stāvoklis pasliktinājies, pārsniedzot a) apakšpunktā minētā ekspluatācijai drošā stāvokļa robežvērtības;(c) pārvaldība, kas attiecas uz aktīva atgriešanu ekspluatācijā ar iespējamiem izmantošanas ierobežojumiem pēc tam, kad veikta aktīva uzturēšanai ekspluatācijai drošā stāvoklī paredzētā tehniskā apkope;(d) monitoringa un mērīšanas iekārtu pārvaldība nolūkā nodrošināt to piemērotību paredzētajam mērķim.
5.2.5.	Lai pārvaldītu informāciju un saziņu, kad tas ir svarīgi drošai aktīvu pārvaldībai (sk. 4.4. Informācija un saziņa), organizācija ņem vērā: <ul style="list-style-type: none">(a) attiecīgās informācijas apmaiņu organizācijā vai ar trešām personām, kas atbildīgas par tehnisko apkopi (sk. 5.3. Darbuzņēmēji, partneri un piegādātāji), jo īpaši informācijas apmaiņu par nepareizām darbībām saistībā ar drošību, par negadījumiem un starpgadījumiem, kā arī par iespējamiem aktīva izmantošanas ierobežojumiem;(b) visas vajadzīgās informācijas, tostarp ar a) apakšpunktu saistītās informācijas, izsekojamību (sk. 4.4. Informācija un saziņa un 4.5.3. Dokumentētas informācijas kontrole);(c) reģistru izveidošanu un uzturēšanu par visiem aktīviem, ietverot tādu izmaiņu pārvaldību, kas ietekmē aktīvu drošību (sk. 5.4. Izmaiņu pārvaldība).

5.2.2 Mērķis

Pieteikuma iesniedzējam ir jāparāda, kā tas pārvalda savu aktīvu dzīves ciklu no projektēšanas līdz likvidācijai ar SMS noteikto procedūru un pasākumu starpniecību. Pieteikuma iesniedzējam ir jāparāda, ka tas ir piemērojis uz cilvēku vērstu pieeju katrā dzīves cikla posmā. Tam ir sīki jāizklāsta, kā tā aktīvu pārvaldība mijiedarbojas ar dažādiem tā drošības pārvaldības sistēmas elementiem, piemēram, kompetences pārvaldību, ekspluatācijas plānošanu un pārraudzību. Pieteikuma iesniedzēja mērķim ir jābūt šādam — parādīt, ka tas ir ieviesis stabilu aktīvu pārvaldības sistēmu, kurā ņem vērā tā darbību veida un apjoma radītos riskus.

5.2.3 Paskaidrojumi

“Aktīvs” (**5.2. punkts**) ir jebkurš aprīkojums (stacionārs vai pārvietojams), konstrukcija, programmatūra vai jebkurš cits komponents, kam laika gaitā ir vajadzīga tehniskā apkope, lai varētu veikt dzelzceļa darbību. Aktīvus iedala dzelzceļa pārvadājumu uzņēmuma pārvaldītos aktīvos (pārsvarā tie ir riteņli) un infrastruktūras pārvaldītāja pārvaldītos aktīvos (visi infrastruktūras komponenti, piemēram, sliežu ceļš, vadības/signalizācijas aprīkojums, aprīkojums vilcienu pārvirzīšanai no viena sliežu ceļa uz citu, strāvas avoti, pārbrauktuves, inženiertehniskās būves, piemēram, tilti, viadukti, tuneli, platformas, lifti, eskalatori u. tml. Pilnīgs uzskaitījums ir sniegts Direktīvas (ES) 2012/34 I pielikumā).

Aktīva dzīves ciklam ir šādi posmi:

- a) *projektēšana;*
- b) *īstenošana (būvniecība/ražošana, uzstādīšana, testēšana un nodošana ekspluatācijā);*
- c) *ekspluatācija un tehniskā apkope;*
- d) *remonts, pārveidojumi un modernizācija, tostarp izmaiņu pārvaldība;*
- e) *atjaunošana, ekspluatācijas pārtraukšana un likvidācija.*

Ir svarīgi, lai organizācija parādītu, kā tā nosaka un uztur spēkā (sistēmas un) drošības prasības aktīviem un kā notiks to pārbaude, apstiprināšana un uzraudzība.

Ja tehniskās apkopes veikšanai tiek nolīgta trešā persona, organizācijai ir pienākums noteikt un pārraudzīt, vai aktīva veikspēja atbilst organizācijas noteiktajiem standartiem.

Tiklīdz ir ieviesti procesi ar drošībai kritiskiem aktīviem saistītu risku pārvaldībai, organizācijai ir jāpārtrauga aktīvu veikspēja attiecībā pret šādiem riskiem un organizācijas prognozēm.

Ja pastāv aktīvu atjaunošanas, ekspluatācijas pārtraukšanas vai likvidācijas iespējamība, organizācija nosaka un dokumentē jebkuru ar šādām darbībām saistīto risku pārvaldības procesus.

Šādi procesi attiecas tikai uz organizācijām, kas veic vai varētu veikt šādas darbības.

Attiecībā uz tāda aktīva atjaunošanu, kam tuvojas dzīves cikla beigas, organizācija nodrošina, ka nomainās aktīvs atbilst noteiktajiem drošības rādītāju kritērijiem. Šajā procesā pārskata visas drošības analīzes darbības.

Prasības saistībā ar tehnisko apkopi (**5.2.4. punkts**) izriet no ECM regulas; kravas vagoni ir aktīvs, kas jāpārvalda dzelzceļa pārvadājumu uzņēmumam un, iespējams, infrastruktūras pārvaldītājam. Šīs ECM regulā noteiktās prasības ir konkrētākas un preskriptīvas, savukārt iepriekš minētās prasības attiecas galvenokārt uz saskarni starp dzelzceļa pārvadājumu uzņēmuma vai infrastruktūras pārvaldītāja SMS un ECM tehniskās apkopes sistēmu, lai nodrošinātu aktīvu drošu ekspluatāciju un tehnisko apkopi. Riska novērtēšanā ir jāapsver arī iespējamā jebkādas tehniskās apkopes (kas ir daļa no aktīva dzīves cikla) laikā veiktas komponentu nomainas ietekme uz drošību atbilstoši Direktīvas (ES) 2016/797 un attiecīgo SITS prasībām.

Ne visus aktīvus reglamentē SITS (**5.2.3. punkts**), un pat tad, ja ir piemērojamas SITS (piemēram, SITS INF), tās reglamentē tikai to, kas ir vajadzīgs savstarpējai izmantojamībai, kas nozīmē, ka tik un tā var būt

nepieciešams izpildīt vēl citas prasības. Atbilstība attiecīgo SITS būtiskajām prasībām (nevis tikai drošībai būtiskajām prasībām) ir jānodrošina, kad veic aizstāšanu, atjaunošanu vai modernizēšanu saskaņā ar Direktīvas (ES) 2016/797 noteikumiem.

Jēdziens “ekspluatācijai drošs stāvoklis” (5.2.4. punkta a) apakšpunkts) nozīmē, ka aktīvs ir ekspluatējams drošās tā ekspluatācijas robežās. Drošas ekspluatācijas robežas var veidoties visā sistēmas dzīves ciklā, tomēr tās ir jānosaka, paturot prātā savstarpējas izmantojamības parametrus. Var tikt identificēti bojājumi **(5.2.4. punkta b) apakšpunkts)**, un, pamatojoties uz pamatcēloņu analīzi, var attiecīgi pielāgot drošas ekspluatācijas robežas. Attiecībā uz riteklīm ekspluatācijai drošs stāvoklis nozīmē drošu ekspluatāciju atbilstoši Direktīvas (ES) 2016/798 14. panta 2. punktam.

Aktīvu konfigurācija **(5.2.5. punkta c) apakšpunkts)** ietver aktīvu unikālo identifikāciju, to atrašanās vietu, jebkuru veikto tehnisko apkopi u. tml. (ne tikai izmaiņu konfigurācijas pārvaldību). (Tehnisko) izmaiņu konfigurācijas pārvaldība attiecas uz aizstāšanu.

Ir jāieceļ ECM atbilstoši Direktīvas (ES) 2016/798 14. panta 1. punktam, lai nodrošinātu, ka riteklī, par kuru tehnisko apkopi tā atbild, ir ekspluatācijai drošā stāvoklī. Nav vajadzības sīki aprakstīt darbības, ko veic ECM, kura ir sertificēta saskaņā ar Regulu (ES) Nr. 445/2011. Turpretī ir jānorāda, uz kuriem elementiem un aspektiem attiecas ECM sertifikāts un kā tiek pārvaldīta saskarne ar ECM, jo īpaši — ar kādu informāciju notiek apmaiņa starp pieteikuma iesniedzēju un ECM un kā tā notiek.

Attiecībā uz riteklīm, kuru tehnisko apkopi veic nesertificētas ECM (t. i., ECM, kas nav sertificētas atbilstoši Regulai (ES) Nr. 445/2011), pieteikuma iesniedzējam ir pienākums nodrošināt, ka tā ekspluatētie riteklī ir ekspluatācijai drošā stāvoklī, pārtraugot, vai nesertificētās ECM ir izstrādājušas un efektīvi īstenojušas savu tehniskās apkopes sistēmu saskaņā ar Direktīvas (ES) 2016/798 14. panta 2. un 3. punktu un III pielikumu. Ja nesertificētās ECM nav daļa no pieteikuma iesniedzēja organizācijas, tiesību aktos noteikto pienākumu izpilde ir jānodrošina ar līgumsaistībām.

Dzelzceļa pārvadājumu uzņēmumu partnerību gadījumā katrs dzelzceļa pārvadājumu uzņēmums ir pilnīgi atbildīgs par ekspluatācijas drošību un attiecīgi arī par to risku kontroli, kuri ir saistīti ar tā darbību, tostarp par riteklju tehniskās apkopes funkciju nodrošināšanu. Nepietiek ar to, ka dzelzceļa pārvadājumu uzņēmums izmanto sava partnera dzelzceļa pārvadājumu uzņēmuma drošības sertifikātu kā līdzekli, lai kontrolētu ar tehniskās apkopes nodrošināšanu saistītos riskus, ja tas nav pamatots ar līgumsaistībām starp dzelzceļa pārvadājumu partneruzņēmumiem. Šādām līgumsaistībām jābūt kopīgi izstrādātām, un tās jāpārtrauga katram partnerim, turklāt tās ir daļa no katra partnera SMS, tāpēc uz tām attiecinā attiecīgo VDI veikto uzraudzību. Attiecīgajām VDI ir jāsadarbojas, lai risinātu jebkuras pārrobežu saskarņu problēmas, ko var būt radījušas līgumslēdzējas puses.

5.2.4 Pierādījumi

- *Informācija par aktīvu pārvaldības sistēmu organizācijas SMS, tostarp attiecīgas saites uz citām jomām, piemēram, riska novērtēšanu, ekspluatācijas plānošanu, izmaiņu pārvaldību u. tml. **(5.2.1. punkts), (5.2.2. punkts), (5.2.5. punkta a)–b) apakšpunkts).***

Projektēšanas posms:

- *pierādījumi par procesiem un apspriedēm, lai noteiktu prasības attiecībā uz aktīviem;*
- *pierādījumi par riska pārvaldības stratēģijām saistībā ar jaunu vai pārveidotu aktīvu iepirkumiem un laišanu ekspluatācijā;*
- *visu attiecīgo aktīvu projektēšanas un piegādes procesu dokumentēšana;*
- *procesi risku pārvaldībai projektēšanas posmā;*
- *pierādījumi par drošības nodrošināšanai izmantotajiem rīkiem;*
- *ziņas par standartiem vai citu drošības informāciju, uz ko paļaujas aktīva projektēšanā un tehniskajā apkopē, un jebkuri testi, ko izmanto atbilstības apstiprināšanai;*

- rokasgrāmatas vai cita tāda dokumenta esamība, kurā ir noteikti procesi aktīvu ekspluatācijai un tehniskajai apkopei un risku pārvaldībai ekspluatācijas un tehniskās apkopes posmā.

Īstenošanas posms:

- pierādījumi par drošības apdraudējumu pārvaldības, testēšanas un apstiprināšanas procesiem, kas attiecas uz aktīva būvniecību/ražošanu un laišanu ekspluatācijā un tā gatavību ekspluatācijai.

Ekspluatācijas un tehniskās apkopes posms:

- pierādījumi par pastāvīgu atbilstību standartiem un procesiem un apzināto risku pārvaldību;
- aktīvu tehniskās apkopes plāni un procedūras;
- pierādījumi par organizācijas darbībām saistībā ar risku apzināšanu un likvidēšanu;
- pierādījumi par procesiem, ko izmanto, lai ziņotu par jebkādam drošības rādītāju problēmām un korektīvām darbībām un tās pārvaldītu;
- pierādījumi par veikspējas tendenču salīdzināšanu ar prognozēto aktīva stratēģisko mūžu, lai sekotu līdzi veikspējas attīstībai un plānotu atjaunošanu;
- procesi kļūmju un atteicu konstatēšanai un korektīvas darbības veikšanai;
- tādu avārijas apstākļu vai neplānotu situāciju pārvaldība, kas var ietekmēt aktīvu drošību;
- pierādījumi, ka aktīvu pārvaldība tiek ņemta vērā attiecībā uz notikumiem, kas ir jāpaziņo, un par riska dalīšanas pārvaldību saskarnēs (sk. arī 3.1. punktu).

Atjaunošana, ekspluatācijas pārtraukšana un likvidācija:

- pierādījumi par procesiem ar aktīvu atjaunošanu, ekspluatācijas pārtraukšanu vai likvidāciju saistīto risku pārvaldībai atbilstoši organizācijas apjomam un veidam;
- pierādījumi par sistemātisku pieeju cilvēkfaktoru un organizatorisko faktoru ņemšanai vērā visos aktīvu pārvaldības dzīves cikla posmos (5.2.1. punkts);
- pierādījumi par ekspluatācijas dokumentācijas atbilstību prasībām attiecībā uz (ekspluatācijas) pārvaldību un uzturēšanu organizatoriskajās un fiziskajās robežās, piemēram, organizatoriskās, tehniskās un ekspluatācijas saskarnes ar kaimiņvalstu infrastruktūrām, robežstacijām, mijiedarbība ar citiem dzelzceļa pārvadājumu uzņēmumiem vai infrastruktūras pārvaldītājiem (5.2.3. punkts);
- informācija, kas apliecina, ka pieteikuma iesniedzējs parāda tā tehniskās apkopes pasākumu atbilstību attiecīgajām prasībām (tiesību aktiem, standartiem u. tml.) (5.2.3. punkts);
- ritekļu gadījumā — ECM sertifikāta kopija vai pierādījumi, ka par tehnisko apkopi atbildīgā struktūra izpilda Direktīvas (ES) 2016/798 14. panta 2. un 3. punkta un III pielikuma prasības (5.2.4. punkta a)–d) apakšpunkts).

Dzelzceļa pārvadājumu uzņēmumu partnerību gadījumā, ja ritekļa tehnisko apkopi veic partneris: pierādījumi, ka starp partneriem ir spēkā līgumsaistības, tostarp:

- informācijas apmaiņa, kā aprakstīts Regulas (ES) Nr. 445/2011 5. pantā;
- attiecīgā gadījumā — tehniskais atbalsts, jo īpaši attiecībā uz mantotajām vadības un signalizācijas sistēmām;
- kontrole attiecībā uz nolīgto tehniskās apkopes darbnīcu spēju veikt tehnisko apkopi;
- ritekļu pārraudzība un no šādas pārraudzības izrietošas attiecīgas informācijas apmaiņa (sk. arī 6.1. punktu);
- attiecībā uz aktīviem, par kuriem ir vajadzīgs atbilstības sertifikāts saskaņā ar ES tiesību aktiem vai valsts noteikumiem — šāda sertifikāta kopija kopā ar paskaidrojumu par to, ciktāl uz to paļaujas kā uz SMS daļu (5.2.4. punkta a)–d) apakšpunkts);
- informācija par to, kā darbojas SMS dokumentu pārvaldības daļa attiecībā uz aktīvu pārvaldību, tostarp pierādījumi, ka tehniskās apkopes dokumentācija (procedūras, darba norādījumi u. tml.) tiek vajadzības gadījumā atjaunināta (5.2.5. punkta a)–c) apakšpunkts);

- *pierādījumi par aktīvu konfigurācijas pārvaldību visā to dzīves ciklā, ietverot jebkādas izmaiņu pārvaldības procesus, kas ieviesti izmantošanai bāzes rekonfigurācijas gadījumos (5.2.5. punkta c) apakšpunkts).*

5.2.5 Pierādījumu piemēri

Projektēšanas posms

Organizācija dokumentē visus attiecīgos ar drošību saistītos procesus un informāciju saistībā ar aktīvu projektēšanu un piegādi, īstenojot konfigurācijas pārvaldības procesus (vai konfigurācijas pārvaldības sistēmu). Dokumentācijā izklāsta tehniskās un organizatoriskās darbības, ar kurām ievieš un uztur aktīva kontroli visā tā dzīves ciklā.

Organizācija nosaka un dokumentē procesu ar aktīva risinājuma izstrādi saistīto risku pārvaldībai,

- *nosakot prasības jebkuriem jauniem un/vai pārveidotiem aktīviem (sk. arī 1. punktu), un tā apspriežas par tiem ar attiecīgajām ieinteresētajām personām (sk. arī 2.4. punktu);*
- *pārvaldot ar šādu izmaiņu īstenošanu saistītos riskus (sk. arī 3.1. punktu) un*
- *pārvaldot ar aktīvu iepirkumu un līgumu pārvaldību saistītos riskus, ja piemērojams (sk. arī 3.1. un 5.3. punktu).*

Saistībā ar to jābūt veiktām apdraudējuma drošības analīzēm, lai apzinātu jomas, kurās ir vislielākais darbības traucējumu risks, tās pārskatot un salīdzinot ar organizācijas apdraudējumu žurnālu. To panāk, identificējot drošībai kritiskas sistēmas un nosakot veiktspējas pamatmērķus, šim nolūkam izmantojot attiecīgas riska apzināšanas metodes, piemēram,

- *aktīvu projekta uzticamības, pieejamības, uzturamības un drošības (RAMS) analīzi (kur galvenie drošības rādītāju kritēriji tiek paziņoti projektētājiem, lai nodrošinātu, ka aktīvs atbilst paredzētajam mērķim), un*
- *atteices režīmu, rezultātu un kritiskuma analīzi (FMECA) un/vai uz uzticamību vērstu tehnisko apkopi (RCM), lai pārvaldītu riskus projektēšanas posmā un atbalstītu tehniskās apkopes plāna izstrādi.*

Šīs prasības tiek pārvaldītas, salīdzinot tās ar konkrētajiem standartiem un procesiem, ko izmanto dzelzceļa infrastruktūras un ritošā sastāva projektēšanai, tehniskajai apkopei un ekspluatācijai, kā noteikusi organizācija. Organizācija parāda, ka:

- *drošībai kritiskas sistēmas tiek projektētas atbilstoši funkcionālajām specifikācijām;*
- *ir spēkā apstiprināšanas un laišanas ekspluatācijā testa plāns, lai apstiprinātu, ka aktīvs atbilst paredzētajam mērķim un ka tā ekspluatācija un tehniskā apkope ir droša, un*
- *ir sagatavota ekspluatācijas un tehniskās apkopes dokumentācija, kurā ir izklāstīti aktīvu atjaunināšanas, pārskatīšanas un tehniskās apkopes procesi (sk. arī 4.5. punktu).*

Organizācija parāda, ka tā savā sistēmu projektēšanas un iepirkuma pieejā izmanto attiecīgus sistēmtehnikas procesus un drošības nodrošināšanas procesus (piemēram, EN50126/8/9 attiecībā uz kompleksām sistēmām). To varētu panākt, izveidojot sistēmtehnikas pārvaldības plānu (SEMP), kurā norādītu procedūru ieinteresēto personu, sistēmas prasību un drošības vajadzību noteikšanai un reģistrēšanai.

Īstenošanas posms

Lai nodrošinātu sekmīgu un drošu aktīva īstenošanu, organizācija ievieš procesus ar aktīva būvniecību, testēšanu un laišanu ekspluatācijā saistīto risku pārvaldībai atbilstoši SMS procesiem.

Tā arī īsteno procesu, lai pārvaldītu:

- *aktīvu sistēmas un drošības prasību testēšanu, pārbaudi un apstiprināšanu, ko varētu nodrošināt, izmantojot testēšanas un laišanas ekspluatācijā pārvaldības plānu vai tam līdzvērtīgu dokumentu, un*

- *aktīva gatavību ekspluatācijai, ko var nodrošināt, izmantojot gatavības ekspluatācijai kontrolesarakstu.*

Ekspluatācijas un tehniskās apkopes posms

Organizācija ir izstrādājusi aktīvu ekspluatācijas un tehniskās apkopes dokumentāciju, kurā ir izklāstīti drošības pārvaldības procesi, ko tā izmanto, lai veiktu savu aktīvu atjaunināšanu, pārskatīšanu un tehnisko apkopi. Dokumentācijā tā izklāsta darbību tvērumu un, ja piemērojams, ieviestās riska pārvaldības stratēģijas, lai aptvertu visas attiecīgās darbības.

Minētā dokumentācija:

- *nodrošina, ka aktīva ekspluatācija un tehniskā apkope notiek atbilstoši aktīva projektam;*
- *tajā ir noteikti un ietverti visi ar drošību saistītie nosacījumi, kas paredz, kā aktīva izmantošana var būt ierobežota, un nosacījumi attiecībā uz aktīva izmantošanu, un*
- *tajā ir norādītas pastāvīgās pārbaudes, kas jāveic.*

Ierosināto aktīvu projekta un piegādes konfigurēšanas process (aprakstīts projektēšanas posmā) ir izvērts, aptverot visu tā dzīves ciklu, un tas tiek nodrošināts:

- *ieviešot un uzturot visu aktīvu uzskaiti izveidotā aktīvu reģistrā. Reģistrā iekļauj tādu informāciju kā aktīvu unikālā identifikācija, to atrašanās vieta, jebkāda veiktā tehniskā apkope u. tml.;*
- *pārvaldot dokumentus un informāciju par aktīviem saskaņā ar organizācijas SMS (sk. arī 4.4. un 4.5. punktu) un*
- *nosakot aktīvu kritiskumu, pamatojoties uz drošības apdraudējumu novērtējuma rezultātiem. Drošībai kritiskus aktīvus norāda aktīvu reģistrā.*

Organizācija pierāda, kā aktīvu informācija tiek izstrādāta, uzturēta un integrēta tās apdraudējumu žurnālā.

Organizācija pastāvīgi pārbauda atbilstību tās noteiktajiem standartiem un procesiem, lai nodrošinātu, ka dzelzceļa darbības vienmēr ir drošas un efektīvas. Šajā nolūkā organizācija ievieš procesus, lai nodrošinātu, ka:

- *aktīvu ekspluatācija un tehniskā apkope notiek atbilstoši attiecīgajām rokasgrāmatām;*
- *aktīvu stāvoklis tiek pārbaudīts;*
- *tiek veikta aktīvu testēšanai vai pārbaudei vajadzīgā aprīkojuma pienācīga kontrole, kalibrēšana un tehniskā apkope;*
- *visi riski, kas ir saistīti ar aktīvu ekspluatāciju un uzturēšanu, tiek pārvaldīti atbilstoši riska pārvaldības procesiem un visiem darba aizsardzības tiesību aktiem, un*
- *ir pieejamas rezerves daļas tehniskajai apkopei, jo īpaši drošībai kritiskiem aktīviem. To varētu nodrošināt, nosakot aktīvu rezerves detaļu vajadzības, pamatojoties uz aktīvu kritiskumu, ko nosaka, piemērojot "uz uzticamību vērstu tehnisko apkopi" (RCM).*

Organizācija parāda, ka tā veic aktīvu tehniskās apkopes plānošanu, lai:

- *ņemtu vērā kompetences, spējas un resursu prasības;*
- *izpildītu ar informācijas pārvaldību un uzskaiti saistītās vajadzības;*
- *īstenotu sīki izstrādātus plānus, kas sagatavoti uz risku balstītā procesā un kas nosaka dažādos tehniskās apkopes līmeņus un noteiktas organizatoriskās standarta struktūras, procedūras un atbildību par aktīvu tehnisko apkopi, un*
- *nodrošina to rīku un aprīkojuma kalibrēšanu, kas tiks izmantots tehniskajai apkopei.*

Minētais var jo īpaši ietvert:

- *tehniskās apkopes plānu (TMP) un*
- *darba norādījumus, ko izstrādā un revidē, pamatojoties uz TMP.*

Plānošana tiek dokumentēta un kontrolēta, izmantojot datorizētu tehniskās apkopes pārvaldības sistēmu (**sk. arī 4.5. punktu**).

Organizācija ir ieviesusi procesus, lai nodrošinātu, ka:

- *kad riteklis vai aprīkojums tiek piešķirts uzdevuma veikšanai:*
 - *komplektējot apkopi, un pirms izbraukšanas tiek pārbaudīta atbilstība veicamajam uzdevumam/misijai (piemēram, katra ritošā sastāva veida tehniskā piemērotība maršrutam);*
 - *drošībai kritisku komponentu tehniskā apkope notiek atbilstoši plānam (profilaktiskā tehniskā apkope atbilstoši noteiktajam biežumam un apkopes pasākuma veidam);*
 - *tehniskās apkopes pasākumi tiek noteikti, kad konstatē bojājumus vai kad bojājumi pārsniedz drošas ekspluatācijas robežas (korigējošā apkope), izņemot, ja tiek īstenoti ekspluatācijas ierobežojumi;*
 - *kad tiek konstatēta vajadzība veikt izmaiņas, iespējami drīz tiek veikti vajadzīgie pasākumi, piemēram, izņemšana no ekspluatācijas vai ekspluatācijas ierobežojumu noteikšana;*
- *par visām drošībai kritiskajām darbībām ir pieejami darba norādījumi;*
- *visu uzdevumu izpilde tiek oficiāli apstiprināta;*
- *dokumentācija par veikto tehnisko apkopi tiek kontrolēta (**sk. arī 4.5. punktu**), un*
- *ir pieejama uz kompetenci balstīta apmācība par visām drošībai kritiskām sistēmām (**sk. arī 4.1. punktu**).*

Ir izstrādāts process/procedūra, ko izmanto, lai nodrošinātu, ka ekspluatācijas ierobežojumi — pagaidu vai pastāvīgi (piemēram, konkrēta ritekļu veida vai konkrētu maršrutu dēļ) — tiek:

- *ņemti vērā, kad riteklis vai aprīkojums tiek piešķirts uzdevuma/misijas veikšanai;*
- *savlaicīgi paziņoti ritekļa vai aprīkojuma ekspluatācijas personālam (piemēram, vilciena vadītājam, vilciena priekšniekam).*

Organizācija parāda, ka tā:

- *izprot savu drošībai kritisko aktīvu veikspēju, nosakot, kas ir jāpārtrauc, jānovērtē un jāziņo;*
- *nosaka un reģistrē drošībai kritisku aktīvu veikspējas pārraudzības, novērtēšanas, analīzes un izvērtēšanas metodi un biežumu;*
- *pārtrauc veikspējas tendences attiecībā pret prognozēto aktīva stratēģisko mūžu (**sk. arī 6.1. punktu**);*
- *ziņo par veikspējas problēmām, pamatojoties uz drošības apdraudējuma līmeni, un par drošības rādītāju jautājumiem, lai tie tiktu pienācīgi atrisināti;*
- *izmanto pārraudzības rezultātus, lai vajadzības gadījumā pielāgotu tehniskās apkopes plānu;*
- *nosaka kanālus jebkādu rezultātu paziņošanai (**sk. arī 4.4. punktu**);*
- *uzlabo drošībai kritisko aktīvu atbilstību standartiem,*
 - *pārskatot ekspluatācijas un tehniskās apkopes kontroles pasākumus un novērtējot to aktīvu riskus, kuri neatbilst iepriekš noteiktajiem standartiem;*
 - *nosakot drošības rādītāju problēmu pamatcēloni(-ņus) un*
 - *nosakot darbības, kas var būt vajadzīgas, lai atjaunotu aktīvus ekspluatācijai drošā stāvoklī;*
- *pastāvīgi uzlabo SMS, apzinot iespējamus riskus un veicot korektīvus pasākumus (**sk. arī 7.2. punktu**), un*
- *dokumentē, kā ir izmantotas iespējas samazināt vai likvidēt risku un kā tas ir sasniegts.*

Organizācija ir ieviesusi procesus, lai konstatētu jebkuras kļūmes vai darbības traucējumus, kas var rasties aktīviem, un nodrošinātu attiecīgu korektīvu pasākumu veikšanu. Tie atbilst noteikumiem un tehniskās apkopes programmām vai plāniem un:

- *nodrošina atteīcu un rezultātā veikto korektīvo pasākumu attiecīgu reģistrēšanu;*
- *pievēršas drošībai kritiskiem darbības traucējumiem;*

- *nodrošina, ka par paziņojamiem notikumiem tiek attiecīgi ziņots, un*
- *koordinē neplānotos ar drošību saistītu aktīvu remontdarbus.*

Organizācija:

- *dokumentē darbības traucējumu pārvaldības procesu;*
- *izmanto atbilstošas analīzes metodes attiecībā uz drošībai kritiskām īpašībām, piemēram, pamatcēloņu analīzi (RCA);*
- *veic darbības traucējumu reģistrēšanu, norādot kļūmju kodus, darbības traucējumu režīmu, sekas, kritiskumu un korektīvos pasākumus;*
- *izstrādā procedūras parasto remontdarbu pārvaldībai un*
- *ievieš atgriezeniskās saites procesu inženiertehniskajām vai tehniskajām darbinieku grupām sistēmu pārskatīšanai un uzlabošanai un darbības traucējumu riska mazināšanai nākotnē.*

Tas tiek nodrošināts, izmantojot kļūmju ziņošanas, analīzes un korektīvo darbību metodi (FRACAS), kas:

- *reģistrē kļūmes, kas atklātas un reģistrētas, kad veic testēšanu un nodošanu ekspluatācijā, kā arī jebkuras kļūmes, kas rodas ekspluatācijas vai tehniskās apkopes laikā, un*
- *pārvalda turpmākos korektīvos pasākumus, ko veic, lai kļūmes novērstu.*

Organizācija dokumentē visas kļūmes un korektīvās darbības un pieprasa, lai tehniski kompetenta persona pārbaudītu visus neplānotos remontdarbus.

Ir ieviests process/procedūra, kas reglamentē aktīvu pārvaldību traucētas ekspluatācijas vai avārijas apstākļu gadījumā.

Organizācija ir ieviesusi procesus, lai pārvaldītu saskarņu riskus, kas rodas tās aktīvu ekspluatācijas un tehniskās apkopes laikā (sk. arī 3.1.1. punktu). Šādi procesi aptver saskarnes starp aktīviem un starp dalībniekiem, kuri tās izmanto.

Atjaunošanas, ekspluatācijas pārtraukšanas un likvidācijas posms

Organizācija saprot, kāds ir tās aktīvu stāvoklis, un, ja tas pasliktinās, attiecīgi reaģē, veicot aktīva nomaiņu vai tehnisko apkopi.

Organizācija ir izstrādājusi apstiprināšanas un laišanas ekspluatācijā testa plānu, lai apstiprinātu, ka jaunais aktīvs atbilst paredzētajam mērķim un ka tā ekspluatācija un tehniskā apkope ir droša. Ja organizācija paildzina esoša aktīva dzīves ciklu, tā meklē atbilstošu drošības informāciju, piemēram, vēsturiskus datus, lai nodrošinātu, ka aktīvs joprojām ir piemērots lietošanai.

Tiek veikta tendenču pārraudzība attiecībā pret prognozēto veiktspēju (sk. ekspluatācijas un tehniskās apkopes posmu).

Veicot jebkādas dzelzceļa infrastruktūras vai ritošā sastāva likvidāciju, organizācija pienācīgi pārvalda riskus saistībā ar aktīva izņemšanu no ekspluatācijas.

Drošībai kritisku aktīvu izmaiņu pārvaldība

Situācijās, kad organizācija vēlas mainīt drošībai kritisku aktīvu bāzes konfigurāciju, tā īsteno izmaiņu pārvaldības procesu, lai nodrošinātu drošības apdraudējumu efektīvu pārvaldību, nosakot konfigurācijas bāzes visiem drošībai kritiskajiem aktīviem ar saistīto programmatūru (neatkarīgi no tā, vai tās ir integrētas esošajās sistēmās vai ir atsevišķas programmas). Ja operators maina drošībai kritisku aktīvu konfigurācijas bāzi, tas, ja iespējams:

- *pārvalda no šādu aktīvu izmaiņām izrietošos riskus;*
- *pieraksta sērijas un modeļa numurus;*
- *apstiprina funkcionālās prasības attiecībā pret specifikācijām un riska kontroles pasākumiem;*
- *kontrolē konfigurācijas vienumu izlaides un*

- *nodrošina, ka ir aktualizēts jebkuru tādu aktīvu statuss, kuriem piemēro konfigurācijas pārvaldību.*

Noteikto bāzu, ekspluatācijas apstākļu vai drošībai kritisku aktīvu tehniskās apkopes grafiku izmaiņas, ko veikusi organizācija, nekādā veidā nemazina dzelzceļa darbību drošību.

Kopīgu drošības metožu piemērošana

Ir izstrādāts uzraudzības process/procedūra, ko par tehnisko apkopi atbildīgās struktūras (piemēram, ECM) izmanto, lai pārbaudītu, kā tiek piemērota CSM riska noteikšanai un CSM pārraudzībai (atkarībā no tā, kura CSM ir piemērojama) (t. i., CSM, ko nosaka tiesību akti un/vai līgumsaistības).

Cilvēkfaktoru integrācijas piemērošana

Ir ieviests sistemātisks process cilvēkfaktoru integrācijas piemērošanai visā sistēmas dzīves ciklā, piemēram, attiecībā uz aktīvu tiek apsvērts uzdevumu projekts, darba procedūras, darba vide un pietiekami resursi, tādējādi nodrošinot, ka cilvēkfaktori un organizatoriskie faktori tiek pienācīgi ņemti vērā.

Organizācijas programmā nosaka kārtību, kā tiks identificēti, pārskatīti un saskaņoti ar cilvēkfaktoriem un organizatoriskajiem faktoriem saistītie jautājumi un kā tie tiks virzīti, lai rastu risinājumus, visā projektēšanas vai izmaiņu pārvaldības procesā. Programma nosaka saistību ar citām personām, kuras saistītas ar projektēšanas vai izmaiņu ieviešanas darbību.

Ir sniegta informācija par drošības brīdinājumu informācijas rīka (SAIT) izmantošanu (sk. 5.4.3. punktu).

5.2.6 Atsauces un standarti

- [Pamatnostādnes par to, kā piemērot Drošības direktīvas 14. panta a\) punktu un Komisijas Regulu \(ES\) Nr. 445/2011, ar ko izveido sistēmu par kravas vagonu tehnisko apkopi atbildīgo struktūru sertifikācijai](#)
- CENELEC — EN50126 *Dzelzceļa aprīkojums — drošuma, darbīgas, uzturamības un drošības (RAMS) specificēšana un pierādīšana — 1. daļa: pamatprasības un vispārīgais process*
- *Valsts dzelzceļa drošības regulatora birojs — aktīvu pārvaldības pamatnostādnes (2015. gads)*

5.2.7 Uzraudzības jautājumi

Uzraudzības ziņā ir svarīgi pievērsties aktīva pārvaldībai visā tā dzīves ciklā, sākot no projektēšanas un beidzot ar likvidāciju, nevis individuāliem aktīva pārvaldības darbības traucējumiem, izņemot, ja tie ir tieši saistīti ar drošību.

Uzraudzībā ir jāņem vērā, kā tiek veikta to esošo aktīvu pārvaldība un tehniskā apkope, kuri datējami agrāk nekā spēkā esošie standarti.

Uzraudzībā ir jāņem vērā, vai un kā organizācija izmanto SAIT.

5.3 Darbuzņēmēji, partneri un piegādātāji

5.3.1 Normatīvā prasība

- 5.3.1. Organizācija apzina un kontrolē drošības apdraudējumus, kas izriet no ārpalpojumu sniedzējiem deleģētām darbībām, tostarp no ekspluatācijas sadarbībā ar darbuzņēmējiem, partneriem un piegādātājiem.
- 5.3.2. Lai kontrolētu 5.3.1. punktā minētos drošības apdraudējumus, organizācija nosaka darbuzņēmēju, partneru un piegādātāju atlases kritērijus un līguma prasības, kas tiem jāizpilda, aptverot:
- (a) juridiskās un cita veida prasības saistībā ar drošību (sk. 1. Organizācijas konteksts);
 - (b) līgumā noteikto uzdevumu izpildei vajadzīgo kompetences līmeni (sk. 4.2. Kompetence);
 - (c) atbildību par izpildāmajiem uzdevumiem;
 - (d) drošības rādītājus, ko paredzēts uzturēt līguma darbības laikā;
 - (e) saistības, kas attiecas uz tādas informācijas apmaiņu saistībā ar drošību (sk. 4.4. Informācija un saziņa);
 - (f) ar drošību saistītu dokumentu izsekojamību (sk. 4.5. Dokumentēta informācija).
- 5.3.3. Saskaņā ar procesu, kas noteikts Regulas (ES) Nr. 1078/2012 3. pantā, organizācija uzrauga:
- (a) visu darbuzņēmēju, partneru un piegādātāju darbību drošības rādītājus, lai nodrošinātu, ka tie izpilda līgumā noteiktās prasības;
 - (b) darbuzņēmēju, partneru un piegādātāju informētību par drošības apdraudējumiem, ko tie rada organizācijas darbībām.

5.3.2 Mērķis

Pieteikuma iesniedzējam jāparāda, ka tas spēj konstatēt, novērtēt un kontrolēt riskus, kas izriet no to darbuzņēmēju un citu piegādātāju darbībām, ar kuriem pieteikuma iesniedzējam ir darba attiecības. Mērķis nav panākt tikai riska novērtēšanu, un netiek arī prasīts visu risku vai attiecīgā riska kategoriju uzskaitījums, bet pieteikuma iesniedzējam ir jāparāda, kā tā sistēmas un procedūras kopumā ir izstrādātas un organizētas tā, lai atvieglotu šo risku identificēšanu, novērtēšanu un kontroli. Tas nozīmē, ka līgumā jābūt izklāstītam, kā notiek ar drošību saistītas informācijas apmaiņa. Vispārpieņemts risku pārvaldības veids ir labi formulētu līgumu izmantošana. Tomēr galvenā atbildība par darbuzņēmēju pārvaldību un to darbības rezultātu salīdzināšanu ar noteiktajām specifikācijām jāuzņemas organizācijai. Darbuzņēmēju vai apakšuzņēmēju piesaistīšana nenozīmē, ka dzelzceļa pārvadājumu uzņēmums / infrastruktūras pārvaldītājs deleģē kādu no saviem pienākumiem nodrošināt, ka nolīgtie pakalpojumi tiek sniegti atbilstoši pirms ekspluatācijas noteiktiem standartiem.

Pieteikuma iesniedzējam ir jāparāda, ka tam ir izstrādāti procesi, lai noteiktu darbuzņēmēju un citu piegādātāju kompetenci un novērtētu to drošības rādītājus iepirkuma procesā.

Katrai organizācijai ir pienākums īstenot pārraudzības procesu, kas noteikts CSM pārraudzībai, un nodrošināt, ka ar līgumsaistību starpniecību arī tās darbuzņēmēju īstenotie riska kontroles pasākumi tiek pārraudzīti atbilstoši CSM. Ja organizācijas konstatē jebkādu attiecīgu drošības apdraudējumu saistībā ar tehniskā aprīkojuma bojājumiem vai darbības traucējumiem, tām saskaņā ar CSM pārraudzībai ir jāziņo par šādiem apdraudējumiem pārējām iesaistītajām personām, lai tās varētu veikt visus vajadzīgos korektīvos pasākumus sistēmas drošības nodrošināšanai.

5.3.3 Paskaidrojumi

Plašāka informācija par līgumsaistībām un partnerībām ir atrodama 3. pielikums.. pielikumā.

5.3.4 Pierādījumi

- *Pierādījumi, kā organizācijas SMS mijiedarbojas ar darbuzņēmēju un piegādātāju pārvaldības sistēmām, lai kontrolētu riskus (5.3.1. punkts).*
- *Pierādījumi, ka līgumsaistības tiek veidotas, pamatojoties uz riska novērtējuma rezultātiem (5.3.1. punkts) (sk. arī 3.1. punktu).*
- *Pastāv procesi, kuros noteikts, kā jāpievēršas cilvēkfaktoriem un organizatoriskajiem faktoriem un kā tie jāpaziņo apakšuzņēmējiem un to vadībai (5.3.1. punkts).*
- *Pierādījumi, kā organizācija pārvalda dokumentāciju par darbuzņēmējiem un piegādātājiem (5.3.2. punkta a)–d) apakšpunkts).*
- *Pierādījumi, kā organizācija atlasa darbuzņēmējus un piegādātājus, lai nodrošinātu, ka tie ir kompetenti un ka drošības apdraudējumi tiek pienācīgi pārvaldīti (5.3.2. punkta a)–e) apakšpunkts).*
- *Ir ieviests process, lai nodrošinātu, ka svarīga drošības informācija tiek koplietota ar darbuzņēmējiem un piegādātājiem vai ka tie paziņo šādu informāciju (5.3.2. punkta d) apakšpunkts).*
- *Organizācija ir ieviesusi pārraudzības procesu vai procedūru, lai pārlicinātos, vai darbuzņēmēji, partneri un piegādātāji, ar kuriem tai ir darba attiecības, spēj pārvaldīt riskus, kas tiem rodas (5.3.3. punkta a) un b) apakšpunkts).*
- *Pierādījumi, ka darbuzņēmēji, partneri vai piegādātāji tiek regulāri pārraudzīti atbilstoši CSM pārraudzībai (Regula (ES) Nr. 1078/2012), lai nodrošinātu, ka produkts vai pakalpojums atbilst noteiktām prasībām un drošības mērķiem (5.3.3. punkta a) apakšpunkts) (sk. arī 6.1. punktu).*

5.3.5 Pierādījumu piemēri

Ir ieviesta darbuzņēmēju, partneru un piegādātāju atlases un pārraudzības procedūra. Procedūrā ir skaidri noteikts, ka standarti, kas darbuzņēmējiem jāpiemēro, ir tādi paši kā standarti, ko attiecinā uz tieši nodarbinātiem darbiniekiem, un ir noteiktas funkcijas un pienākumi. Procedūra dokumentē vajadzīgo informācijas apmaiņu starp pieteikuma iesniedzēja un darbuzņēmēju, partneru un piegādātāju SMS sistēmām.

Ir sniegti pierādījumi par drošības mērķiem, kas darbuzņēmējiem, partneriem un piegādātājiem ir jāsasniedz, un par rādītājiem, kas tiks izmantoti šo mērķu sasniegšanas novērtēšanai.

Cilvēkfaktoru un organizatorisko faktoru stratēģijā ir sīki izklāstīts, kā šie jautājumi tiek pārrunāti ar darbuzņēmējiem un apakšuzņēmējiem.

Dokumentu pārvaldības procedūra, kas attiecas uz organizācijas standartiem, kuri darbuzņēmējiem, partneriem un piegādātājiem ir jāpiemēro (sk. arī 4.5.1.1. punkta e) apakšpunktu "Dokumentu pārvaldība").

Pieteikuma iesniedzēja darbuzņēmēju, partneru un piegādātāju uzskaitījums/pārskats, kas paredzēts iekšējai vai ārējai izmantošanai, norādot to nodrošinātos produktus un/vai pakalpojumus (sk. arī 4.5.1.1. punkta d) un e) apakšpunktu) un to, kāda ir ietekme uz drošību, kā arī pasākumus konstatēto risku kontrolei (piemēram, informācijas apmaiņa, pienākumu skaidrošana, apmācība) (sk. arī 3.1.1.1. punkta a) apakšpunktu).

Kompetences pārvaldības sistēmas procedūra, kas ir sasaistīta ar darbuzņēmēju, partneru un piegādātāju procedūrām.

Darbuzņēmēju, partneru un piegādātāju pārvaldības process/procedūra nosaka to, kā tiek pārvaldīti no darbuzņēmēju, partneru vai piegādātāju darbībām izrietošie saskarņu riski un kā darbuzņēmēji, partneri vai

piegādātāji tiek informēti par šādiem riskiem, un, ja piemērojams, to, kā šādi riski tiek iekļauti līgumsaistībās un kā informācijas apmaiņa tiek integrēta SMS.

Atbilstošs revīziju/pārbaūžu plānošanas process attiecībā uz pieteikuma iesniedzēja darbuzņēmējiem, partneriem un piegādātājiem, norādot dažus šādu darbību uzskaites piemērus, piemēram, revīziju/pārbaūžu ziņojumus vai konstatējumus.

Process vai procedūra, ar ko nosaka darbuzņēmējiem, partneriem vai piegādātājiem piemērojamās attiecīgās prasības un dara tās viņiem zināmas, attiecīgā gadījumā norādot, kā tās tiek iekļautas līgumsaistībās, ar ko pienācīgi dokumentē dokumentu pārvaldības sistēmā, lai nodrošinātu informācijas izsekojamību.

Dokumentu pārvaldības sistēmas procedūra, ko izmanto, lai pārvaldītu sertifikātus, atļaujas, atzīšanu vai jebkāda cita veida pierādījumus, apliecinot atbilstību prasībām, ko piemēro darbuzņēmējiem, partneriem vai piegādātājiem, un lai kontrolētu šādu prasību derīgumu laika gaitā (piemēram, veicot pārraudzības pasākumus).

5.3.6 Uzraudzības jautājumi

Veicot organizācijas uzraudzību, lai gūtu pilnīgu priekšstatu par kontroles un pārraudzības apjomu, var būt jāveic uzraudzība kopā ar darbuzņēmēju vai piegādātāju, kurš strādā organizācijas labā. Var būt nepieciešams arī piekļūt dokumentācijai, ar ko strādā darbuzņēmējs vai piegādātājs, un izvērtēt, kā tā ir saistīta ar organizācijas SMS izklāstītajām procedūrām.

Ir ieviesta kārtība ar mērķi nodrošināt, ka darbuzņēmēju un piegādātāju drošības rādītāji un kompetence ir iepirkuma procesa neatņemama sastāvdaļa.

5.4 Izmaiņu pārvaldība

5.4.1 Normatīvā prasība

5.4.1. Organizācija īsteno un vada drošības pārvaldības sistēmas izmaiņas drošības rādītāju uzturēšanai vai uzlabošanai. Tas ietver lēmumu pieņemšanu dažādos izmaiņu pārvaldības posmos un turpmāk veiktu drošības apdraudējumu pārskatīšanu (sk. 3.1.1. Riska novērtējums).

5.4.2 Mērķis

Ir svarīgi, lai pieteikuma iesniedzējs spētu konstatēt jaunus riskus, kas var rasties tā darbībā, un uz tiem reaģēt, pēc vajadzības piemērojot prasības attiecībā uz to izmaiņu pārvaldību, kas noteiktas Direktīvā (ES) 2016/798 un CSM riska noteikšanai un novērtēšanai (Komisijas Īstenošanas regulā (ES) Nr. 402/2015). Būtu jāvar parādīt, ka SMS ietver procedūras šo risku izvērtēšanai un — attiecīgā gadījumā — jaunu riska kontroles pasākumu īstenošanai. Vajadzētu būt aptvertām visu veidu un līmeņu izmaiņām — būtiskām un nebūtiskām, pastāvīgām un īslaicīgām, tiešām un ilgtermiņa izmaiņām. Minētais attiecas uz:

- darbības veidu,
- aprīkojuma,
- procedūru,
- organizācijas,
- personāla vai
- saskarņu izmaiņām.

Procesam ir jābūt tādām, kas sniedz iespēju samērīgi un efektīvi novērtēt riskus, attiecīgā gadījumā iekļaujot ar cilvēkfaktoriem saistītus jautājumus, un pieņemt pamatotus kontroles pasākumus.

Funkciju, pienākumu, rīku un aprīkojuma, darba vides, procesu un procedūru izmaiņas papildina ar cilvēkfaktoriem un organizatoriskajiem faktoriem saistīto jautājumu analīzi, lai apzinātu ar izmaiņām saistītos iespējamās drošības apdraudējumus. Izmantotās metodes varētu būt, piemēram, uzdevumu analīze, izmantojamības analīze, simulācija, riska novērtēšana, HAZOP un aptauja par drošības jautājumiem. Ir sniegti piemēri, kas apliecina, ka pirms izmaiņu ieviešanas tiek veikts riska novērtējums, piemērojot cilvēkfaktoru un organizatorisko faktoru pieeju. Tas jo īpaši varētu attiekties uz darba procedūru izmaiņām, kuru iemesls ir aprīkojuma pārveidošana, darba grafiku izmaiņas vai pienākumu pārdale.

5.4.3 Paskaidrojumi

Ne visām izmaiņām piemēro riska novērtēšanu (**5.4.1. punkts**). Ja izmaiņas tiek aktīvi pārvaldītas, īstenojot citus SMS procesus, piemēram, ikdienas darbības, tās nav jāuzskata par izmaiņām, kas ir jāpārvalda oficiālajā izmaiņu procesā.

Funkcijas, pienākumi, pārskatatbildība un pilnvaras, kas jānosaka (sk. arī 2.3. punktu), ietver izmaiņu pārvaldību (5.4.1. punkts), piemēram, funkciju uzdošanu izmaiņu kontroles padomei.

Izmaiņu pārvaldības procesā ir jāapspriežas ar personālu (**sk. arī 2.4. punktu**).

Funkciju, pienākumu, rīku un procesu izmaiņas ievieš pēc tam, kad ir veikta drošības kultūras jautājumu analīze saistībā ar izmaiņām, lai apzinātu iespējamās drošības apdraudējumus. Drošības apdraudējumi, kas izriet no apjoma samazināšanas, pārvaldības izmaiņām vai darbību deleģēšanas ārpalpojumu sniedzējiem, tostarp darbībām vai sadarbības ar darbuzņēmējiem, partneriem un piegādātājiem, ir jāpārvalda kā līdzvērtīgi iekšējiem apdraudējumiem, un to prioritātes ir jānosaka tāpat kā iekšējiem apdraudējumiem.

5.4.4 Pierādījumi

- *Izmaiņu pārvaldības procesa apraksts (5.4.1. punkts).*
- *Apraksts par procedūrām un metodēm, ko izmanto jaunu vai mainītu risku izvērtēšanai un jauninājumu ieviešanai (5.4.1. punkts).*
- *Kontroles pasākumi, tostarp norādes uz to, kur atrodami sīki izstrādāti procesi (5.4.1. punkts).*
- *Informācija par to, kā organizācija konstatē būtiskas izmaiņas un pieņem lēmumus, kad piemērot procesus, kas paredzēti CSM riska noteikšanai un novērtēšanai, vai kad veikt riska novērtēšanu atbilstoši SMS procedūrām (5.4.1. punkts).*
- *Informācija par riska pārvaldības pasākumiem, ko organizācija ir ieviesusi, lai pārvaldītu ritekļu atļaujas un vienotā drošības sertifikāta vai drošības atļaujas izmaiņas (5.4.1. punkts).*
- *Informācija par procesu attiecīgās valsts drošības iestādes informēšanai par izmaiņām, pirms tiek sākta jauna dzelzceļa pārvadājumu darbība (5.4.1. punkts).*

5.4.5 Pierādījumu piemēri

Izmaiņu pārvaldības procedūras kopija kā daļa no pieteikuma. Šāds dokuments aptver vajadzību veikt visu izmaiņu riska novērtēšanu atbilstoši dažādajām tiesību aktu prasībām. Iesniegts tāda problēmu un pieņemumu žurnāla piemērs, kurš tiek regulāri pārskatīts līdz ar izmaiņu attīstību. Visbeidzot, procedūra aptver arī procesu attiecīgās(-o) VDI informēšanai par izmaiņām.

“Izmaiņu pārvaldības process” nozīmē riska novērtēšanas procesa izmantošanu, un rezultātus ņem vērā, izstrādājot, īstenojot un pārskatot ekspluatācijas procesus.

5.4.6 Uzraudzības jautājumi

Lai noteiktu, vai SMS paredzētie izmaiņu pārvaldības pasākumi ir pietiekami efektīvi, ir jāseko līdzi vairākām dažādu veidu izmaiņām ar noteiktā procesa starpniecību, lai secinātu, a) vai tās ir pārvaldītas pienācīgi un vai no izmaiņām izrietošie riski ir pienācīgi ņemti vērā, un b) vai jebkāda gūtā mācība ir integrēta SMS procedūru pārskatīšanā.

Tiek novērtēta izmaiņu pārvaldības pasākumu atbilstība CSM riska noteikšanai.

Organizācija ir ieviesusi procesus attiecīgo SITS, valsts noteikumu un citu standartu īstenošanai un pastāvīgai pārraudzībai, attiecīgā gadījumā parādot, kā tos piemēro visā jebkura aprīkojuma vai darbības dzīves ciklā.

5.5 Ārkārtas situāciju pārvaldība

5.5.1 Normatīvā prasība

- 5.5.1. Organizācija identificē ārkārtas situācijas un nosaka ar tām saistītus savlaicīgus pasākumus, kas jāveic ārkārtas situāciju pārvaldībai (sk. 3.1.1. Riska novērtējums) un normālu ekspluatācijas apstākļu atjaunošanai saskaņā ar Regulu (ES) 2015/995.
- 5.5.2. Organizācija nodrošina, ka jebkura identificētā veida ārkārtas situācijā:
- (a) ir iespējams nekavējoties sazināties ar neatliekamās palīdzības dienestiem;
 - (b) neatliekamās palīdzības dienestiem tiek sniegta visa būtiskā informācija gan iepriekš, lai sagatavotos reaģēšanai ārkārtas situācijā, gan ārkārtas situācijas laikā;
 - (c) pirmā palīdzība tiek sniegta pašu spēkiem.
- 5.5.3. Organizācija nosaka un dokumentē visu personu funkcijas un pienākumus saskaņā ar Regulu (ES) 2015/995.
- 5.5.4. Organizācijai ir rīcības, brīdināšanas un informēšanas plāni ārkārtas situācijām, kuros ietverti pasākumi nolūkā:
- (a) brīdināt visu personālu, kura atbildībā ir ārkārtas situāciju pārvaldība;
 - (b) paziņot informāciju visām personām (piemēram, infrastruktūras pārvaldītājam, [dzelzceļa pārvadājumu uzņēmumiem](#), darbuzņēmējiem, iestādēm, neatliekamās palīdzības dienestiem), tostarp ārkārtas situācijā dot norādījumus pasažieriem;
 - (c) pieņemt visus vajadzīgos lēmumus atbilstoši ārkārtas situācijas veidam.
- 5.5.5. Organizācija apraksta, kā ir iedalīti resursi un līdzekļi ārkārtas situāciju pārvaldībai (sk. 4.1. Resursi) un kā tiek apzinātas prasības, kas attiecas uz mācībām (sk. 4.2. Kompetence).
- 5.5.6. Ārkārtas situācijām paredzētos pasākumus regulāri izmēģina sadarbībā ar citām ieinteresētajām personām un vajadzības gadījumā atjaunina.
- 5.5.7. Organizācija nodrošina, ka infrastruktūras pārvaldītājs var vienkārši un bez kavēšanās sazināties ar kompetento atbildīgo personālu, kam ir pienācīgas valodu zināšanas, un ka infrastruktūras pārvaldītājam tiek sniegta informācija pietiekamā apjomā.
- 5.5.7. [Organizācija ārkārtas rīcības plānus koordinē ar visiem dzelzceļa pārvadājumu uzņēmumiem, kas darbojas organizācijas infrastruktūrā, ar neatliekamās palīdzības dienestiem nolūkā veicināt to ātru reaģēšanu un ar visām citām personām, kuras varētu tikt iesaistītas ārkārtas situācijā.](#)
- 5.5.8. Pastāv procedūra, lai avārijas gadījumos būtu sasniedzama par tehnisko apkopi atbildīgā struktūra vai dzelzceļa ritekļu turētājs.
- 5.5.8. [Organizācijai ir pasākumi, ar ko vajadzības gadījumā nekavējoties aptur darbības un dzelzceļa satiksmi un informē visas ieinteresētās personas.](#)
- 5.5.9. [Pārrobežu infrastruktūras gadījumā sadarbība starp attiecīgajiem infrastruktūras pārvaldītājiem veicina neatliekamās palīdzības dienestu vajadzīgo koordinēšanu un sagatavotību abpus robežas.](#)

5.5.2 Mērķis

Jebkuram pienākumu veicējam būtiskas ir stabilas ārkārtas situāciju plānošanas sistēmas, un tām ir jāaptver informācija, kas jāsniedz neatliekamās palīdzības dienestiem, lai tie varētu sagatavot plānus reaģēšanai uz būtiskiem starpgadījumiem. Svarīgi ir arī tie SMS aspekti, kas ir tieši saistīti ar reaģēšanu ārkārtas situācijā, piemēram, apmācība par ārkārtas situācijām un ārkārtas rīcības plānu izmēģināšana.

5.5.3 Paskaidrojumi

Ārkārtas situācijas (**5.5.1. punkts**) ir saistītas ar organizācijas riska novērtējuma rezultātiem, lai gan SITS OPE (sk. 4.2.3.7. punktu) ir paredzēts neierobežojošs ārkārtas situāciju uzskaitījums.

Ja novērtējums attiecas uz infrastruktūras pārvaldītāju, iepriekš minētā tiesību akta 5.5.7. un 5.5.8. punkts ir aizstāts ar tekstu zilā krāsā. Savukārt 5.5.9. punkta teksts zilā krāsā attiecas tikai uz infrastruktūras pārvaldītāju.

5.5.4 Pierādījumi

No pieteikuma iesniedzēja tiek gaidīts, ka tas iesniegs pārskatu par:

- *aptvertajiem ārkārtas situāciju veidiem, tostarp traucētas ekspluatācijas apstākļiem un to pārvaldības procedūrām (**5.5.1. punkts**);*
- *pieteikuma iesniedzēja sniegto informāciju, lai neatliekamās palīdzības dienesti varētu plānot pasākumus reaģēšanai uz būtiskiem starpgadījumiem uz dzelzceļa, attiecīgā gadījumā norādot atsauci uz pienākumiem, ko nosaka piemērojamie ES tiesību akti, un jebkuriem attiecīgiem pārrobežu pasākumiem (**5.5.2. punkta a) un b) apakšpunkts**);*
- *plāniem, funkcijām un pienākumiem (arī par izraudzītiem darbiniekiem ar noteiktām prasmēm, kuriem ir uzdots palīdzēt infrastruktūras pārvaldniekam, vai otrādi), apmācību un kompetences uzturēšanas pasākumiem, un pasākumiem, lai nodrošinātu efektīvu saziņu ar neatliekamās palīdzības dienestiem, attiecīgo personālu un saziņu ar tiem, kurus skar starpgadījumi, piemēram, pasažieriem vai skartajām trešām personām (tostarp dokumentam, kurā ir izklāstītas visu dalībnieku funkcijas un pienākumi, tas, kā ir piešķirti resursi un līdzekļi un kā ir noteiktas apmācības vajadzības); procedūrām parastās darbības atsākšanai pēc ārkārtas situācijas (**5.5.1. punkts**), (**5.5.3. punkts**), (**5.5.4. punkta a)–c) apakšpunkts**), (**5.5.5. punkts**), (**5.5.7. punkts**), (**5.5.8. punkts un 5.5.9. punkts tikai no infrastruktūras pārvaldītājam piemērojamām normatīvajām prasībām**);*
- *SMS īpašajiem aspektiem, kas ir tieši saistīti ar reaģēšanu ārkārtas situācijā, piemēram, apmācība par ārkārtas situācijām un ārkārtas rīcības plānu izmēģināšana, lai identificētu trūkumus (**5.5.6. punkts**);*
- *procedūru, lai sazinātos ar attiecīgo par tehnisko apkopi atbildīgo struktūru vai turētāju ārkārtas situācijā, kas saistīta ar kādu no tā rīcekļiem (**5.5.8. punkts tikai no infrastruktūras pārvaldītājam piemērojamām normatīvajām prasībām**).*

5.5.5 Pierādījumu piemēri

Ārkārtas situāciju pārvaldības procedūras(-u) un saistīto plānu (piemēram, atjaunošanas procedūru) kopija. Procedūra aptver visu ekspluatēto tīklu, pēc vajadzības paredzot īpašus pasākumus attiecībā uz tuneļiem un citām augsta riska vietām un pasākumus pārrobežu sadarbībai, personāla komplektēšanai un funkcijām un pienākumiem, un tā ietver norādes uz infrastruktūras pārvaldītāja ārkārtas situācijām paredzētajiem pasākumiem un uz to, kā vajadzības gadījumā sazināties ar citām attiecīgām personām, piemēram, ECM. Ja dzelzceļa pārvaldījumu uzņēmuma darbības telpa ietver vairākus infrastruktūras pārvaldītājus, dzelzceļa pārvaldījumu uzņēmumam ir jāņem vērā attiecīgo infrastruktūras pārvaldītāju ārkārtas situācijām paredzēto pasākumu (un ar lietotājiem noslēgto līgumu) atšķirības.

Procedūrā ir norāde uz CMS prasībām attiecībā uz personālu, kam jāreaģē uz ārkārtas situācijām, un tā paredz, kā pārliecināties, vai nolīgtais personāls atbilst tiem pašiem standartiem.

Ārkārtas situāciju pārvaldības procedūra ietver procesu norādījumu sniegšanai starpgadījumos cietušajiem un viņu ģimenēm par sūdzību iesniegšanas procedūrām.

Procedūra (attiecīgā gadījumā) ietver informāciju par to, kas notiek ārkārtas situācijā, kurā ir iesaistītas bīstamas kravas. Organizācijai (dzelzceļa pārvadājumu uzņēmumam) ir ieviests process, lai nodrošinātu, ka:

- *ir iespējams ātri sazināties ar iekrāvēju, cisternvagona īpašnieku, ja cisternvagonš pieder privātīpašniekam, cisternkonteīnera īpašnieku vai turētāju un operatoru, saņēmēju u. tml. personām;*
- *infrastrukturā pārvaldītājam pēc iespējas drīzāk tiek sniegta attiecīgā informācija (piemēram, vagonu reģistrācijas numuri, vagonu atrašanās vieta vilciena sastāvā, ANO numurs, RID klasifikācijas kods un bīstamās kravas bīstamības identifikācijas numurs atbilstoši RID noteikumiem);*
- *organizācijai (infrastrukturā pārvaldītājam) ir ieviests process, lai nodrošinātu, ka iestādēm (piemēram, glābšanas dienestiem, policijai, citiem neatliekamās palīdzības dienestiem un iestādēm) tiek sniegta attiecīgā informācija par bīstamām kravām (sk. piemērus iepriekš).*

5.5.6 Uzraudzības jautājumi

Lai pienācīgi novērtētu SMS procedūras ārkārtas situāciju pārvaldībai, var būt nepieciešams SMS procedūras savstarpēji salīdzināt ar attiecīgo saskarņu dalībnieku procedūrām (jo īpaši saistību starp galvenajiem dalībniekiem, piemēram, dzelzceļa pārvadājumu uzņēmumu, infrastruktūras pārvaldītāju un neatliekamās palīdzības dienestu), lai nodrošinātu, ka ieviestie šādu starpgadījumu pārvaldības procesi veido saskaņotu kopumu.

Pārbaudīt, vai ir plāni par visām paredzamajām ārkārtas situācijām.

Ir ieviesti pasākumi ārkārtas rīcības plānu izmēģināšanai un koordinēti pasākumi ar neatliekamās palīdzības dienestiem, kas neaprobežojas tikai ar teorētiskām apspriedēm par ārkārtas situācijām.

Ir ieviesti pasākumi mijiedarbībai ar citām ieinteresētajām personām, ietverot izmēģināšanu, kontroli, saziņu, koordināciju un kompetenci.

Labāka dzelzceļa sistēma
sabiedrībai

6 Veiktspējas izvērtēšana

6.1 Uzraudzība

6.1.1 Normatīvā prasība

6.1.1. Organizācija veic uzraudzību saskaņā ar Regulu (ES) Nr. 1078/2012 nolūkā:

- (a) pārbaudīt, vai visi drošības pārvaldības sistēmas procesi un procedūras, tostarp ekspluatācijas, organizatoriskie un tehniskie drošības pasākumi, tiek pareizi piemēroti un ir efektīvi;
- (b) pārbaudīt, vai drošības pārvaldības sistēma kopumā tiek pareizi piemērota un vai tā dod gaidītos rezultātus;
- (c) noskaidrot, vai drošības pārvaldības sistēma atbilst šajā regulā noteiktajām prasībām;
- (d) attiecīgi noteikt un īstenot korektīvus pasākumus un izvērtēt to efektivitāti (sk. 7.2. Pastāvīgi uzlabojumi), ja konstatēta neatbilstība a), b) vai c) apakšpunktam.

6.1.2. Organizācija visos organizācijas līmeņos regulāri uzrauga ar drošību saistītu uzdevumu izpildi un iejaucas gadījumā, ja šie uzdevumi netiek pienācīgi pildīti.

6.1.2 Mērķis

Organizācijai ir jāiesniedz pierādījumi, ka tā ir ieviesusi procesu drošības pārvaldības sistēmas piemērošanas un efektivitātes pārraudzībai un ka šāds process atbilst tās darbības apjomam un veidam. Organizācijai ir jāparāda, ka ar šo procesu var identificēt, novērtēt un izlabot jebkādas SMS darbības traucējumus.

6.1.3 Paskaidrojumi

Kontroles pasākumu efektivitāte nozīmē, ka organizācija ir ieviesusi procesu, lai pārbaudītu, ka pēc riska novērtēšanas un attiecīgu kontroles pasākumu piemērošanas šie pasākumi pēc noteikta laikposma tiek pārskatīti, lai nodrošinātu, ka ir sasniegts ar pasākumiem plānotais drošības apdraudējuma samazinājums (6.1.1. punkta d) apakšpunkts).

Veiktajā pārraudzībā ir jāiekļauj cilvēkfaktoru un organizatorisko faktoru jomā īstenojamās stratēģijas panākumu analīze.

Drošības rādītāji sistemātiski tiek vērtēti, ņemot vērā drošības kultūras uzlabošanas stratēģiju. Tas nozīmē, ka organizācijai ir jāizvērtē, kā drošības kultūras uzlabojumi iederas mērķī uzlabot drošību un veido daļu no šā mērķa.

Regulāri tiek veikti paškritiski un objektīvi organizācijas drošības kultūras programmu, prakses un rādītāju novērtējumi. Drošības informācija, piemēram, no korektīvo pasākumu programmas, cilvēku veiktspējas, starpgadījumu un negadījumu analīzes, apsekojumiem un attiecīgas iekšējās un ārējās ekspluatācijas pieredzes, tiek sistemātiski apkopota un izvērtēta, lai konstatētu tendences un izvairītos no organizatoriskas un individuālas pašplūsmas vai bezrūpības.

Sekmīgs novērtējums var nodrošināt resursu drošības rādītāju uzlabošanai, radot skaidru priekšstatu par to, kā organizācijas drošības kultūra ietekmē drošību. Novērtējuma mērķis ir apzināt drošības kultūras

priekšrocības un trūkumus, salīdzinot faktisko kultūru ar kultūru, kādai tai ir jābūt. Tas sniedz iespēju noteikt prioritātes attiecībā uz uzlabojumu jomām un ieviest izmaiņas, piemēram, procesā, apmācībā un uzvedībā. Drošības kultūras novērtējums ir proaktīvas darbības instruments, ar ko uzlabot drošības rādītājus un palielināt drošības rezerves. Ir ieteicams veikt neatkarīgus drošības kultūras novērtējumus ik pēc trīs–pieciem gadiem un organizatoriskus pašnovērtējumus reizi gadā vai divos gados.

6.1.4 Pierādījumi

- *Informācija par to, kā pieteikuma iesniedzējs ir īstenojis CSM pārraudzībai (6.1.1. punkta a) apakšpunkts).*
- *Informācija par to, kā pārraudzības procesā tiek konstatēti panākumi vai trūkumi paredzēto drošības rezultātu sasniegšanā (6.1.1. punkta b) apakšpunkts).*
- *Pierādījumi, ka SMS ir mainīta pārraudzības laikā konstatēto SMS procesu trūkumu izlabošanas rezultātā (6.1.1. punkta c) apakšpunkts).*
- *Organizācijā ir jābūt ieviestam veikspējas standartu un rādītāju noteikšanas procesam saistīto ekspluatācijas procesu, kā arī īstenoto izmaiņu pārraudzībai. Vajadzētu būt programmai, ko izmanto, lai pastāvīgi novērtētu ar cilvēkfaktoriem un organizatoriskajiem faktoriem saistīto procesu rādītājus, kā arī šo procesu rezultātu, piemēram, to, kā darbinieki izpilda īstenotās procedūras un kā tiek izmantots jauns aprīkojums (6.1.2. punkts).*

6.1.5 Pierādījumu piemēri

Paziņojums, ka tiek piemērota CSM pārraudzībai un ka ir ieviesta procedūra, kas attiecas uz šo darbību. Procedūrā ir izklāstīts, kā tiek novērtēti darbības rezultāti attiecībā pret izvirzītajiem drošības mērķiem un kā tie tiek koriģēti, īstenojot izmaiņu pārvaldības un riska novērtēšanas procesu, un kā tiks laboti SMS trūkumi.

Organizācija ir ieviesusi procesus un procedūras, lai sistemātiski izvērtētu, vai cilvēkfaktoru un organizatorisko faktoru integrēšanas pasākumi ir pietiekami un vai sasniegtie rezultāti atbilst veikspējas standartiem.

Organizācija ir ieviesusi procesus un procedūras, lai sistemātiski izvērtētu darbinieku veikspēju drošībai kritisku darba uzdevumu veikšanā. Šādu procesu pamatā ir proaktīva pieeja, nosakot veikspējas un sistemātiskas izvērtēšanas standartus. Izmanto uz pierādījumiem balstītas metodes, piemēram, apkalpes resursu pārvaldību.

6.1.6 Uzraudzības jautājumi

Pārraudzības procesa un no tā izrietošo konstatējumu un darbību izskatīšanai ir būtiska nozīme, lai varētu noteikt, vai SMS ir “dzīvs” un mainīgs dokuments, kas attīstās līdz ar pieredzē pamatotiem uzlabojumiem, vai arī tas ir dokuments, kas laika gaitā nemainās.

Lai VDI varētu konstatēt atbilstību CSM pārraudzībai, ir būtiski izskatīt vairākas riska pamatjomas un kontroles pasākumus un pārbaudīt, vai tie tiek piemēroti pareizi un ir efektīvi, izmantojot SMS.

6.2 Iekšējā revīzija

6.2.1 Normatīvā prasība

- 6.2.1. Organizācija neatkarīgi, objektīvi un pārredzami veic iekšējo revīziju nolūkā vākt un analizēt informāciju uzraudzības vajadzībām (sk. 6.1. Uzraudzība), ietverot:
- (a) plānoto iekšējo revīziju grafiku, ko var pārskatīt atkarībā no iepriekšējo revīziju un veikspējas uzraudzības rezultātiem;
 - (b) kompetento revidentu identifikāciju un atlasu (sk. 4.2. Kompetence);
 - (c) revīziju rezultātu analīzi un izvērtējumu;
 - (d) korektīvu vai uzlabojošu pasākumu nepieciešamības apzināšanu;
 - (e) pārliecināšanos par šo pasākumu pabeigtību un efektivitāti;
 - (f) dokumentāciju, kas attiecas uz revīziju veikšanu un rezultātiem;
 - (g) revīziju rezultātu paziņošanu augstākā līmeņa vadībai.

6.2.2 Mērķis

Pieteikuma iesniedzējam ir jāparāda, ka tam ir iekšējās revīzijas sistēma, kurā ir iesaistīti kompetenti darbinieki un kura sniedz jēgpilnus rezultātus, ko vadība ņem vērā, un kura nodrošina drošības pārvaldības sistēmas atbilstību tiesību aktu noteikumiem.

6.2.3 Paskaidrojumi

Iekšējās revīzijas pasākumi (**6.2.1. punkts**) ir pārraudzības rīki CSM pārraudzībai nozīmē. Lai gan tā ir atsevišķa prasība, tā ir paredzēta, lai palīdzētu sasniegt pārraudzības mērķus atbilstoši CSM pārraudzībai.

Iekšējās revīzijas pasākumu (6.2.1. punkts) mērķis ir sniegt informāciju par to, vai drošības pārvaldības sistēma atbilst piemērojamām prasībām (**6.1.1. punkta c) apakšpunkts**) un tiek efektīvi īstenota un uzturēta (**6.1.1. punkta a), b) un d) apakšpunkts**). Piemērojamās prasības ir prasības, kas noteiktas CSM par atbilstības novērtēšanu I un II pielikumā, un tādējādi arī jebkuras citas piemērojamās prasības, ko organizācija apņemas ievērot (**sk. arī 1.1. punktu**).

Revidentiem ir pienākums pārbaudīt to korektīvo vai uzlabojošo pasākumu izpildi un efektivitāti (**6.2.1. punkta c) apakšpunkts**), kuri jāveic, lai ņemtu vērā revīzijas secinājumus.

6.2.4 Pierādījumi

- Pierādījumi, ka ir ieviests iekšējās revīzijas process vai sistēma, paredzot plānotas revīzijas un mērķtiecīgas papildu revīzijas, ko veic, pamatojoties uz drošības rādītāju datiem (**6.2.1. punkta a) apakšpunkts**).
- Pierādījumi par kompetences pārvaldības sistēmu, kas ietver elementus, kuri attiecas uz iekšējo revidentu kompetenci (6.2.1. punkta b) apakšpunkts).
- Pierādījumi, ka gan iekšējās, gan ārējās revīzijās gūtie secinājumi ir ņemti vērā, attiecīgi rīkojoties (**6.2.1. punkta c), d), e) un f) apakšpunkts**).
- Pierādījumi, ka revīzijas rezultāti ir apsriesti augstākajā vadības līmenī un ka ir veikti attiecīgi pasākumi (6.2.1. punkta g) apakšpunkts).

6.2.5 Pierādījumu piemēri

Ir ieviesta iekšējās revīzijas procedūra plānotām un papildu revīzijām, kas ietver rezultātu apspriešanu augstākās vadības līmenī.

Revīzijas ziņojumu un iekšējās revīzijas secinājumu žurnālu piemēri, kas apliecina, kādi pasākumi ir veikti, lai tos ņemtu vērā.

Visā organizācijā veikto revīzijas pasākumu rezultāti tiek apkopoti un analizēti, sniedzot ieteikumus periodiskajai pārskatīšanai vadības līmenī.

Procedūrā ir atsauces uz kompetences pārvaldības sistēmu. CMS parāda, ka revidenti ir saņēmuši attiecīgu revidentu apmācību (piemēram, ISO).

6.2.6 Atsauces un standarti

- ISO 19011:2011 “Drošības pārvaldības sistēmu revīzijas pamatnostādnes”

6.2.7 Uzraudzības jautājumi

Uzraudzības sistēmā ir būtiski izvērtēt plānošanu un revīziju secinājumus. Tas ļaus pārliecināties, vai revīzijas tiek vērstas uz pareizajām jomām, vai rezultāti ir pamatoti un vai revīzijas veic kompetents un neatkarīgs personāls.

Būtu jāpārbauda, vai revīzijai atlasītās jomas ir pielāgotas organizācijas riska profilam.

Ir izveidots neplānotu revīziju veikšanas mehānisms, un to izmanto, pārskatot vairākus piemērus.

6.3 Vadības veikta pārskatīšana

6.3.1 Normatīvā prasība

6.3.1.	Augstākā līmeņa vadība regulāri pārskata drošības pārvaldības sistēmas pastāvīgo piemērotību un efektivitāti, ņemot vērā vismaz: <ul style="list-style-type: none">(a) sīku informāciju par to, kā norit pēc vadības iepriekš veiktās pārskatīšanas neīstenoto darbību īstenošana;(b) mainīgos iekšējos un ārējos apstākļus (sk. 1. Organizācijas konteksts);(c) organizācijas drošības rādītājus, kas saistīti ar:<ul style="list-style-type: none">(i.) tās drošības mērķu sasniegšanu;(ii.) tās veiktās uzraudzības rezultātiem, tostarp iekšējās revīzijas secinājumiem, negadījumu/starpgadījumu iekšējās izmeklēšanas rezultātiem un attiecīgo darbību statusu;(iii.) valsts drošības iestādes veiktās uzraudzības attiecīgo iznākumu;(d) ieteikumus par uzlabojumiem.
6.3.2.	Augstākā līmeņa vadība, pamatojoties uz tās veiktās pārskatīšanas iznākumu, uzņemas vispārēju atbildību par vajadzīgo drošības pārvaldības sistēmas izmaiņu plānošanu un īstenošanu.

6.3.2 Mērķis

Lai organizācijas drošības pārvaldības sistēma darbotos konstruktīvi un efektīvi, kā arī turpinātu attīstīties laika gaitā, ir nepieciešama spēcīga vadības līderība drošības jomā. Organizācijai ir jāparāda, ka vadība aktīvi iesaistās drošības pārvaldības sistēmas darbības pārskatīšanā un tās izstrādē nākotnei.

6.3.3 Pierādījumi

- *Procesi attiecībā uz vadības sanāksmēm, kurās pārskata drošības pārvaldības sistēmu un progresu revīzijās un pārskatīšanās sniegto iekšējo ieteikumu īstenošanā (6.3.1. punkta a)–d) apakšpunkts).*
- *Uzskaites dati par to, kādi ir bijuši organizācijas darbības rezultāti tās drošības mērķu sasniegšanā (6.3.1. punkta c) apakšpunkta i) daļa).*
- *Pierādījumi, ka attiecīgās VDI ieteikumi ir ņemti vērā drošības pārvaldības sistēmā (6.3.1. punkta c) apakšpunkta iii) daļa).*
- *Organizācija var parādīt, ka tai ir ieviesti procesi, lai noteiktu un izvirzītu mērķus atbilstoši tās darbības veidam, apjomam un attiecīgajiem riskiem, ka tā regulāri novērtē panākumus mērķu sasniegšanā, ievēro procedūras un izmanto drošības datus, lai pārraudzītu un pārskatītu ekspluatācijas pasākumus un ieviestu tajos izmaiņas (6.3.1. punkts).*
- *Pierādījumi, ka vadība uzņemas aktīvu lomu vajadzīgo drošības pārvaldības sistēmas izmaiņu plānošanā un īstenošanā (6.3.2. punkts).*

Ir ieviesti procesi un rīki sistemātiskai ziņošanai par visu veidu apzinātajiem riskiem, kļūdām, gandrīz notikušiem negadījumiem, trūkumiem un starpgadījumiem, kā arī paziņotās ar cilvēkfaktoriem un organizatoriskajiem faktoriem saistītās informācijas kategorizēšanai un analīzei, lai varētu noskaidrot pamatā esošos cēloņus un efektīvus pasākumus.

negadījumu izmeklēšanas procesā tiek piesaistīti cilvēkfaktoru un organizatorisko faktoru speciālisti.

Ir ieviesti sistemātiski procesi cilvēkfaktoru un organizatorisko faktoru jautājumos gūto atziņu novirzīšanai uz apmācību un izstrādi.

Negadījumu un starpgadījumu izmeklēšanā gūtās atziņas tiek darītas zināmas organizācijas darbiniekiem un novirzītas uz apmācību, izstrādi un citām jomām, lai mazinātu atkārtotās iespējamību.

Negadījumu izmeklēšanas rezultāti tiek publiskoti vadības sanāksmēs, un tos uzskata par svarīgu rīku mācības gūšanai un uzlabojumu veikšanai.

- *Ir ieviests kvalitātes nodrošināšanas process attiecībā uz negadījumu izmeklēšanu.*

6.3.4 Pierādījumu piemēri

Procedūra, ar kuru pārskata un izpilda iekšējos ieteikumus no revīzijām un pārskatīšanas, ko veikusi augstākā līmeņa vadība, un atlasītu sanāksmju protokoli.

Lietu žurnāls, kurā ir norādīti sniegtie ieteikumi un gūtie panākumi vadības novēroto trūkumu izlabošanā.

Procedūra, ko vadība izmanto, lai pārskatītu iekšējās starpgadījumu izmeklēšanas rezultātus un attiecīgos VDI veiktās uzraudzības iznākumus.

Ir sniegta informācija par to, kurus rādītājus vēlāk izvērtē augstākā līmeņa vadība un cik bieži.

6.3.5 Uzraudzības jautājumi

Uzraudzības laikā ir būtiski novērot, vai process, kura mērķis ir nodrošināt, ka vadība pārskata SMS efektivitāti, noved pie reālām izmaiņām ekspluatācijas līmenī.

Vadības informētība par mainīgiem iekšējiem un ārējiem apstākļiem. Vai vadība veic, piemēram, potenciālo iespēju izpēti vai izmanto citas metodes, piemēram, PESTLE (politisko, ekonomisko, sociāltehnisko, juridisko un vides) analīzi, lai tās rezultātus izmantotu savas SMS pilnveidošanā?

Saistība/saikne starp vadības veiktas pārskatīšanas rezultātiem un to, kā tie tiek izmantoti gada drošības ziņojumam.

7 Uzlabojumi

7.1 No negadījumiem un starpgadījumiem gūtā mācība

7.1.1 Normatīvā prasība

7.1.	No negadījumiem un starpgadījumiem gūtā mācība
7.1.1.	Par negadījumiem un starpgadījumiem, kas saistīti ar organizācijas dzelzceļa darbībām: <ul style="list-style-type: none">(a) ziņo, tos reģistrē, izmeklē un analizē, lai noteiktu to cēloņus;(b) pēc vajadzības ziņo valsts struktūrām.
7.1.2.	Organizācija nodrošina, ka: <ul style="list-style-type: none">(a) valsts drošības iestādes, valsts izmeklēšanas struktūras un nozares/iekšējās izmeklēšanas ieteikumi tiek izvērtēti un īstenoti, ja to īstenošana ir lietderīga vai obligāta;(b) būtiski citu ieinteresēto personu, piemēram, dzelzceļa pārvadājumu uzņēmumu, infrastruktūras pārvaldītāju, par tehnisko apkopi atbildīgo struktūru un dzelzceļa ritekļu turētāju, ziņojumi/informācija tiek izskatīti un ņemti vērā.
7.1.3.	Organizācija ar izmeklēšanu saistīto informāciju izmanto, lai pārskatītu riska analīzi un novērtējumu (sk. 3.1.1. Riska novērtējums), izdarītu secinājumus ar mērķi uzlabot drošību un attiecīgā gadījumā pieņemt korektīvus un/vai uzlabojošus pasākumus (sk. 5.4. Izmaiņu pārvaldība).

7.1.2 Mērķis

Organizācijai ir jāparāda, ka tā izmeklē negadījumus un starpgadījumus, lai gūtu mācību un uzlabotu riska kontroles pasākumus, ka izmeklēšanu, tostarp par cilvēkfaktoru un organizatorisko faktoru jautājumiem, veic kompetents personāls, ka par negadījumiem tiek ziņots attiecīgajām iestādēm un ka tiek sagatavoti ieteikumi un ziņojumi, pamatojoties uz kuriem vadība attiecīgi rīkojas.

Nevēlamo notikumu analīzē ir nevis jāmeklē vainīgais vai kādai nodaļai “jāuzvelj lielāka atbildība nekā citām”, bet gan jātiecas izprast un izlabot organizatoriskos trūkumus, kuru dēļ nevēlamie notikumi ir bijuši iespējami. Vissarežģītākais notikumu analīzē ir novērst arī “izrietošus” notikumus. Ja analīze beidzas ar tiešo cēloņu identificēšanu, tad ir iespējams novērst tikai nākamo līdzīgo notikumu. Turpretī, ja analīze sniedz iespēju identificēt tehniskos un organizatoriskos “pamatcēloņus”, uzlabojumu pasākumi ļaus novērst cita veida negadījumu, kam ir tādi paši mehānismi. Piemēram, ja analīzē kļūst skaidrs, ka kāda procedūra nebija atjaunināta un ka korektīvā pasākuma mērķis ir tikai labot attiecīgo procedūru, ietekme būs ierobežota. Ja analīzi veic plašāk, identificējot trūkumus procedūru atjaunināšanas procesā, uzlabojumu pasākuma pozitīvā ietekme var būt daudz plašāka.

Turklāt organizācija piemēro “dubultloka mācīšanās” pieeju, proti, mācīšanās ir vērsta ne tikai uz notikumu realitāti, bet arī uz organizācijas spēju veikt uzlabojumus, pievēršoties tiem elementiem, kas vai nu veicina, vai kavē zināšanu un informācijas nodošanu visā organizācijā.

Tiek veicināta un atvieglota ziņošana par bīstamām situācijām un “augstas iespējamības” starpgadījumiem. Vajadzības gadījumā ir mehānismi, kas nodrošina ziņošanas anonimitāti. Ja ziņošana notiek, norādot ziņotāja identitāti, darbinieki un grupas, kas nosūtījuši ziņojumus, palīdz veikt analīzi un noteikt īstermiņa reaģēšanas

pasākumus. Tiek organizētas grupu apspriedes, un veiktie pasākumi tiek darīti zināmi attiecīgajiem darbiniekiem un — atbilstošā gadījumā — visai organizācijai.

Turklāt bīstamu notikumu analīze tiek īstenota transversāli, izmantojot daudzveidīgu kompetenču kopumu un ņemot vērā visu attiecīgo personu (tostarp, ja nepieciešams, ārējo personu) viedokli.

Tiek veicināta “taisnīga kultūra”, atzīstot un nostiprinot pozitīvas drošības iniciatīvas (ziņošanu par starpgadījumiem, personāla iesaistīšanu analīzē un pastāvīgu uzlabojumu ieviešanā, atbalsta sniegšanā kolēģiem u. tml.). Šādā “taisnīgā kultūrā” nedrīkst būt baiļu par nosodīšanu — tas jāpanāk, nosakot vispāratzītu robežu starp to, kas ir un kas nav pieņemams. Tiek akceptētas tiesības kļūdīties.

7.1.3 Paskaidrojumi

Termini “gandrīz notikuši negadījumi” un “citi bīstami notikumi” ir ietverti “starpgadījuma” definīcijā atbilstoši Direktīvai (ES) 2016/798. Lai proaktīvi pārvaldītu drošību, ir vienlīdz svarīgi izmeklēt gandrīz notikušus negadījumus un citus bīstamus notikumus.

No negadījumiem un starpgadījumiem gūtajai mācībai ir jāatbalsta informācijas koplietošana ar citām ieinteresētajām personām (infrastruktūras pārvaldītājiem, citiem dzelzceļa pārvadājumu uzņēmumiem, ECM, lai attīstītu sadarbību un sekmētu SMS darbības vispārējo uzlabošanu).

Izmeklētājiem, kuri veic izmeklēšanu saistībā ar cilvēkfaktoriem un organizatoriskajiem faktoriem, ir jābūt īpaši apmācītiem vai arī viņiem ir jābūt pieejamām attiecīgām speciālām zināšanām, lai izskatītu attiecīgos jautājumus.

7.1.4 Pierādījumi

- *Informācija par negadījumu/starpgadījumu paziņošanas procesu, arī par to, kā tiek konstatēti un analizēti pamatcēloņi, tostarp par ziņošanu organizācijas iekšienē un ziņošanu citām kompetentām iestādēm un citām personām (7.1.1. punkts).*
- *Informācija par metodi, ko organizācija izmanto saistībā ar izmeklēšanu, tostarp cilvēkfaktoru un organizatorisko faktoru elementu izmeklēšanu, lai pārskatītu riska analīzes un izvērtēšanas procesu pēc notikuma (7.1.3. punkts).*
- *Pierādījumi, ka ir īstenoti kompetento iestāžu ieteikumi no ziņojumiem par negadījumiem un starpgadījumiem un ka ir ieviestas visas par vajadzīgām atzītās izmaiņas (7.1.2. punkta a) un b) apakšpunkts).*
- *Tiek izvērtēti iepriekšējie starpgadījumi, lai noteiktu attiecīgos faktorus, kas ir saistīti ar aktuālo(-ajiem) starpgadījumu(-iem). Ir pierādījumi par plašāku organizācijas izglītošanās sistēmu, lai mācītos no starpgadījumiem un pieredzes — gan valsts, gan starptautiskā mērogā (7.1.3. punkts).*
- *Pastāv metodika izmeklēšanas veikšanai, pamatojoties uz zināšanām par cilvēkfaktoriem un organizatoriskajiem faktoriem un mūsdienīgām metodēm.*
- *Ir izveidota mācību programma, kas paredzēta negadījumu un starpgadījumu izmeklētājiem un ietver cilvēkfaktoru un organizatorisko faktoru aspektu.*

7.1.5 Pierādījumu piemēri

Negadījumu izmeklēšanas procedūra, kurā ir izklāstītas izmeklēšanas metodes un iekļauta atsauce uz kompetences pārvaldības prasībām, ko piemēro negadījumu un starpgadījumu izmeklētājiem.

Dažādu veidu negadījumu un starpgadījumu ziņojumu paraugi, kuros ir norādīts, ka izmeklēšanu veikusi kompetenta persona, ka secinājumu pamatā ir pierādījumi un ka ieteikumi ir īstenoti.

Tādas procedūras/procesa kopija, kurā ir uzskaitīti korektīvie/ riska mazināšanas pasākumi, kas identificēti pēc negadījuma/starpgadījuma.

Ir sniegta informācija par drošības brīdinājumu informācijas rīka (SAIT) izmantošanu, lai sekotu līdzi jautājumiem, kas skar konkrētus aktīvus, un konsultētu citas organizācijas par šādiem jautājumiem.

Ir pieejami apmācīti izmeklētāji.

Ir izveidota mācību programma, kas paredzēta negadījumu un starpgadījumu izmeklētājiem.

Valdes sanāksmju protokoli, kas apliecina, ka negadījumu/starpgadījumu izmeklēšanas rezultāti un saistītie ieteikumi (t. i., korektīvie un/vai uzlabojošie pasākumi) tiek atgriezeniski paziņoti vadībai, un kā tos izmanto SMS pārskatīšanā (sk. arī 6.3. punktu).

Starpgadījumu un negadījumu izmeklēšanā izmanto cilvēkfaktoru un organizatorisko faktoru pieeju. Izmeklēšana ir vērsta uz sistemātisku perspektīvu, proti, tajā ne tikai aplūko cilvēkfaktorus, tehnoloģiskos un organizatoriskos faktorus kā tādus, bet arī pievērš īpašu uzmanību faktoru mijiedarbībai. Piemēram, ja vilciena vadītājs ir bijis iesaistīts SPAD starpgadījumā, faktori, ko ir ieteicams izpētīt, cita starpā ir, piemēram, nogurums, kognitīvā pārslodze, kompetence u. tml. (cilvēkfaktori), tehnoloģijas ietekme uz veiktspēju, piemēram, cilvēka–sistēmas saskarnes, iekārtojums, signālu izvietojums (tehnoloģiskie faktori), organizācijas ietekme uz veiktspēju, piemēram, apmācība, SMS, organizatoriskās prioritātes (organizatoriskie faktori), kā arī šo trīs jomu mijiedarbība, piemēram, iepirkuma ietekme uz projektu vai izmaiņu pārvaldību, ieviešot jaunu projektu.

7.1.6 Atsauces un standarti

- IAEA (2002) — *Drošības kultūra kodoliekārtu jomā: pamatnostādnes par izmantošanu drošības kultūras uzlabošanā. IAEA TECDOC-1529. Starptautiskā Atomenerģijas aģentūra, Vīne (2002. gads)*
- Mathis, T.L. & Galloway, S.M. (2013. gads) “Steps to safety culture excellence”
- Kecklund, L., Lavin, M. & Lindvall, J. (2016. gads) “Safety culture: A requirement for new business models. Lessons learned from other High-Risk Industries. In proceeding presented of The International Conference on Human and Organisational Aspects of Assuring Nuclear Safety – Exploring 30 Years of Safety Culture”, Vīne, 2016. gada 22.–26. februāris
- RSSB (2015. gads) “Safety Culture and behavioural development: Common factors for creating a culture of continuous development” (www.sparkrail.org)

7.1.7 Uzraudzības jautājumi

Negadījumu/starpgadījumu izmeklētāju kompetencei ir būtiska nozīme jēgpilnu ieteikumu izstrādē un atbilstošu profilaktisku pasākumu nodrošināšanā. Uzraudzības veicējiem ir jāizvērtē vadības iesaistīšanās negadījumu un starpgadījumu ziņojumu rezultātu īstenošanā, kas var ietekmēt ziņojuma kvalitāti, un jebkādu izrietošo rezultātu īstenošanā.

Iekšējās izmeklēšanas rezultāti ir noveduši pie organizācijas izglītošanās procesa, kas ir reģistrēts dokumentos, ziņojumos vai citos informācijas kanālos (t. i., iekšējā, uzņēmuma iekšējā žurnālā u. tml.).

Organizācijas kultūra saistībā ar starpgadījumu un gandrīz notikušu negadījumu ziņošanu.

7.2 Pastāvīgi uzlabojumi

7.2.1 Normatīvā prasība

7.2.1.	Organizācija pastāvīgi uzlabo drošības pārvaldības sistēmas piemērotību un efektivitāti, ņemot vērā sistēmu, kas noteikta Regulā (ES) Nr. 1078/2012, un vismaz šādu darbību iznākumu: <ul style="list-style-type: none">(a) uzraudzība (sk. 6.1. Uzraudzība);(b) iekšējā revīzija (sk. 6.2. Iekšējā revīzija);(c) vadības veikta pārskatīšana (sk. 6.3 Vadības veikta pārskatīšana);(d) no negadījumiem un starpgadījumiem gūtā mācība (sk. 7.1. No negadījumiem un starpgadījumiem gūtā mācība).
7.2.2.	Organizācija savā izglītošanās procesā nodrošina līdzekļus, kas motivē personālu un citas ieinteresētās personas aktīvi uzlabot drošību.
7.2.3.	Organizācija paredz stratēģiju drošības kultūras pastāvīgai uzlabošanai, kuras pamatā ir īpašo zināšanu un atzīto metožu izmantošana, lai apzinātu uzvedības problēmas, kas ietekmē dažādas drošības pārvaldības sistēmas daļas, un ieviestu pasākumus to novēršanai.

7.2.2 Mērķis

Pastāvīgi uzlabojumi ir efektīvas SMS nozīmīga daļa. Šīs prasības mērķis ir panākt, lai pieteikuma iesniedzējs parāda apņēmību veikt uzlabojumus un ka tā SMS to atbalsta.

Augstākā līmeņa vadība iesaistās **kolektīvās pārrunās**, lai pastāvīgi uzlabotu organizācijas drošības kultūru.

Šādas kolektīvas pārrunas ir iestrādātas stratēģijā ar orientāciju uz **kultūras iezīmēm**, kas būtiski ietekmē drošības rādītājus un kas būtu vairāk jānovērtē vai jāmaina.

7.2.3 Paskaidrojumi

Pastāvīgi uzlabojumi (**7.2.1. punkts**) ir vērsti uz SMS elementiem, kas izvērtē un noved pie uzlabojumu darbībām, bet ne elementiem, kas ir uzlabojami, jo tie jau ir daļa no pārraudzības pasākumu tvēruma.

Organizācijas izglītošanās process (**7.2.2. punkts**) ir darbību uzlabošanas process, uzlabojot zināšanas un izpratni.

Jēdzienam “drošības kultūra” (**7.2.3. punkts**) šajā dokumentā piemēro 2.1.1. punkta j) apakšpunktā un ar to saistītajā piezīmē minēto definīciju. Pozitīva drošības kultūra motivē organizācijas un individuus un sniedz tiem iespējas tiekties uz drošības un veikspējas uzlabošanu. Tā palielina apmierinātību ar darbu, veicina darbvietu saglabāšanu un sniedz ieguvumus izmaksu ziņā. Tā var arī palīdzēt sasniegt normatīvos mērķus, jo drošības iestādes un regulatori arvien biežāk atzīst drošības kultūras nozīmi efektīvā drošības pārvaldībā. Konkrētāk, pozitīvas drošības kultūras sniegtie ieguvumi var būt šādi:

- mazāks ekspluatācijas risks, pateicoties vispusīgākai riska novērtēšanai un uzlabotai darbaspēka izpratnei par risku;
- mazāk darbinieku savainošanas gadījumu, likvidējot apdraudējumus, kas apzināti, aktīvāk ziņojot par gandrīz notikušiem negadījumiem;
- mazāk nedrošu darbību un apstākļu, uzlabojot darbinieku iesaistišanu un līderības attīstību;
- mazākas ar darbinieku savainojumiem, nedrošām darbībām un apstākļiem saistītās izmaksas;
- labāka veikspēja, uzlabojot personāla apmācību un iesaistišanu un samazinot savainojumus, nedrošas darbības un apstākļus;

- *labāka un efektīvāka SMS, procedūras un noteikumus labāk pielāgojot realitātei.*

Nemot vērā pamatiezīmes, kas piemīt kultūrai, kura tiek radīta ikdienas mijiedarbībā un kuru ir grūti mainīt, augstākā līmeņa vadībai šī stratēģija ir jāskata ilgtermiņā, jāuztur un jāveicina.

Ir daudz veidu, kā uzlabot drošības kultūru, piemēram:

- *izstrādājot sistēmu informēšanai par problēmām. Tā var būt atkarīga no organizācijas brieduma, būt anonīma, bet vairojot uzticēšanos, būt atvērta un pieejama visiem. Ir svarīgi, lai sistēmā ir integrēta atgriezeniskā saite, kas rada darbiniekiem līdzdalības un piederības sajūtu;*
- *mainot iepirkuma un līgumu nosacījumus, lai mudinātu piegādātājus ievērot labu drošības kultūru. Drošības kultūra varētu būt piegādātāju atlases kritērijs;*
- *uzskatāmi atalgojot par drošu uzvedību. Atalgojums var izpausties vairākos veidos, piemēram, kā lielāka gada samaksa, piešķirot prēmijas, vai iknedēļas drošības balvas par izciliem darba rezultātiem;*
- *nosakot īpašus mērķus vadītājiem attiecībā uz līderību drošības jomā, piemēram, mudinot vadību uzņemties redzamāku lomu standartu noteikšanas jomā.*

Drošības kultūras novērtēšanai ir jāizmanto vairākmetožu pieeja. Datu vākšanas metožu pamatā ir jābūt sociālo zinātņu pētījumiem. Tas nozīmē, ka datus vāc uz vietas visā organizācijā, izmantojot tādas metodes kā novērošanu, dokumentu analīzi un intervijas.

Novērtējumu rezultāti ir jāpaziņo visos organizācijas līmeņos. Pamatojoties uz šādiem rezultātiem, ir attiecīgi jārikojas, lai veicinātu un uzturētu pozitīvu drošības kultūru, uzlabotu līderību drošības jomā un veicinātu mācīšanās attieksmi organizācijā.

Attiecīgu kultūras iezīmju apzināšana un atlase bieži ir sarežģīts uzdevums¹, kas ir jāveic rūpīgi.

Šā uzdevuma izpildē ir jāiesaista visu līmeņu darbinieki visā organizācijā un nereti arī ārpus tās (piemēram, darbuzņēmēji).

Lai gan darbinieku priekšstatus un viedokļus var noskaidrot, veicot aptauju, šādu metodi parasti uzskata par nepietiekamu, lai noteiktu kultūras iezīmes, kas ietekmē drošību. Ekspertiem — iespējams, atsaucei izmantojot aptaujas rezultātus — ir jāveic novērojumi, individuālas intervijas un jāizveido mērķa grupas, lai rezultāts būtu precīzāks.

Piezīme. Mērķa grupā apvieno nelielu cilvēku skaitu (parasti no 4 līdz 15) un moderatoru, lai pievērstos konkrētam jautājumam. Šādu grupu mērķis ir rīkot apsrieses, nevis saņemt individuālas atbildes uz formāliem jautājumiem, kā arī sagatavot kvalitatīvus datus.

Pamatojoties uz šo rezultātu, augstākā līmeņa vadība var izstrādāt un atbalstīt rīcības plānu, kura mērķis ir panākt, lai mainīgās kultūras iezīmes tiek vērtētas augstāk un tiek veicinātas. Augstākā līmeņa vadība seko līdzi noteikto darbību īstenošanai un to attiecīgi pārskata.

Lai nodrošinātu stratēģijas ilgtspēju, rezultāts ir jāpārskata reizi 2–5 gados, izmantojot tādu pašu pieeju. Biežums ir atkarīgs no sākotnējā pasākuma rezultātiem.

¹ Šā uzdevuma sarežģītību papildina tādi aspekti kā, piemēram, organizācijas darbību daudzveidība un tās lielums.

Vairākās augsta riska nozarēs šo rezultātu bieži iegūst, veicot *drošības kultūras novērtējumu*, uz kura pamata tiek izstrādāts rīcības plāns (sk. 2. attēls. Drošības kultūras novērtējumi. attēlu).

Drošības kultūras novērtējumu var veikt neatkarīgs vērtētājs, vai arī tas var būt pašnovērtējums. Neatkarīga novērtējuma priekšrocība ir tāda, ka organizācija gūst objektīvāku priekšstatu par drošības kultūru, taču pastāv risks, ka organizāciju varētu pārprast vai ka tai būs grūtības atzīt secinājumus. Pašnovērtējuma priekšrocība ir tāda, ka to veic uz vietas organizācijas personāls, kam ir padziļinātas zināšanas par organizāciju. Savukārt trūkums ir tas, ka statuss un hierarhija var traucēt šajā procesā. Dažas kultūras novērtējuma iezīmes:

- tas ietver 2–3 nedēļas ilgu novērtēšanas procesu un sagatavošanās posmu;
- tajā iesaistās daudzdisciplīnu pārskatīšanas grupa;
- datu vākšana notiek, izmantojot sociālo zinātņu metodes (tostarp intervijas, mērķa grupas, novērojumus);
- novērtējums aptver visu organizāciju un tās saskarnes;
- novērtējuma pamatā ir drošības kultūras modelis vai sistēma;
- augstākā līmeņa vadība izrāda iniciatīvu un uzskata novērtējumu par iespēju mācīties;
- rezultāti tiek izplatīti visā organizācijā;
- rezultāti tiek izmantoti par pamatu, lai izstrādātu/pārskatītu stratēģiju nolūkā pastāvīgi uzlabot drošības kultūras konkrētās iezīmes.

2. attēls. Drošības kultūras novērtējumi

Cilvēkfaktoru un organizatorisko faktoru stratēģijas un procesu uzlabošana ir SMS pastāvīgas uzlabošanas neatņemama daļa.

Sistemātiska pieeja ir noteikta kā pakāpenisks process ar drošības kultūru saistītu jautājumu risināšanai. Piemēram, ir jābūt procesam, kas nosaka, kā tiek veikta riska novērošana, ziņošana par negadījumiem un starpgadījumiem un kā tiek izmantota informācija un gūta mācība, lai ieviestu pastāvīgus uzlabojumus.

Plašāka informācija par drošības kultūru ir atrodama 4. pielikumā.

7.2.4 Pierādījumi

- *Informācija par pierādījumu salīdzināšanas procesu, lai pierādītu pastāvīgu SMS uzlabošanu (7.2.1. punkts).*
- *Procedūras, kurās ir izklāstīts, kā organizācija ņem vērā pārraudzības, iekšējās revīzijas, vadības sistēmas pārskatīšanas rezultātus un pēc negadījumiem un starpgadījumiem gūto mācību, lai uzlabotu SMS (7.2.1. punkts).*
- *Informācija par to, kā organizācija motivē personālu un citas personas uzlabot SMS (7.2.2. punkts).*
- *Pieteikuma iesniedzējam stratēģijā ir jāizklāsta, kā tiek attīstīta drošības kultūra, lai ar to saistītos riskus pienācīgi ņemtu vērā attiecīgajos SMS procesos. Saistībā ar to pieteikuma iesniedzējam ir skaidri jānorāda, kur ir atrodama plašāka informācija par attiecīgajām procedūrām (7.2.3. punkts).*
- *Drošības kultūru novērtē nepārtraukti, lai apzinātu uzlabojumu iespējas (7.2.3. punkts).*
- *Drošības kultūras uzlabojumus veic, izmantojot PDPR ciklu, lai nodrošinātu, ka darbībām ir ietekme. Gūto mācību īsteno un sistemātiski izvērtē tās ietekmi (7.2.3. punkts).*

7.2.5 Pierādījumu piemēri

Procedūras, kas attiecas uz pārraudzību, iekšējo revīziju, vadības sistēmas pārskatīšanu un negadījumu un starpgadījumu izmeklēšanu, jo īpaši sadaļas, kas vērstas uz gūstamo mācību drošības pārvaldības sistēmai.

Network Rail iniciatīva Close Call (www.safety.networkrail.co.uk/alerts-and-campaign/close-call), kas motivē personālu aktīvi ziņot organizācijai par trūkumiem/nepilnībām vai situācijām, kad pastāv risks drošībai vai veselībai.

Arodbiedrības/vadības periodisko sanāksmju, kas veltītas veselībai un drošībai, protokolu piemēri, apliecinot, ka ir pārrunātas situācijas, ko uzskata par neskaidrām/nedrošām vai kam jāpievērš lielāka uzmanība.

Negadījumu izmeklēšanas rezultāti tiek publiskoti vadības sanāksmēs, un tos uzskata par svarīgu rīku mācības gūšanai un uzlabojumu veikšanai.

Drošības kultūras uzlabošanas stratēģijas kopija un tas, kā stratēģija ir saistīta ar dažādajām SMS daļām.

Stratēģija sniedz pietiekamus pierādījumus, ka ir nodrošināta profesionālā kompetence un, ja nepieciešams, apmācība un speciālās zināšanas drošības kultūras jomā stratēģijas īstenošanai un pilnveidošanai.

Vajadzīgās apmācības un kompetences veids ir saistīts ar izpratni par drošības kultūras jēdzienu, kā arī līdzekļiem un veidiem, ko izmanto, lai novērtētu sasniegto un tiektos uz pastāvīgiem uzlabojumiem. Kritiskais aspekts ir izpratne par drošības struktūru kā visaptverošu jēdzienu, kas ietekmē visas SMS daļas, un par to, ka drošības kultūru nevar uzskatīt par atsevišķu nesaistītu elementu.

Ir ieviests process drošības uzlabošanas pasākumu pastāvīgai izvērtēšanai. Drošības uzlabošanas pasākumu ietekme tiek noteikta un īstenota praksē, lai to varētu izvērtēt.

7.2.6 Uzraudzības jautājumi

Uzraudzības laikā, veicot intervijas, kā arī dokumentācijas analīzi, ir jāpārbauda, kāda ir vadības iesaistīšanās SMS pastāvīgā uzlabošanā. Vai attiecībā uz uzlabojumiem izmanto uz risku balstītu pieeju, t. i., pieeju, kas saistīta ar sensitīviem un kritiskiem kontroles pasākumiem?

Būtu jāizvērtē, kā organizācija izmanto brieduma modeļus SMS darbības izvērtēšanai, ja tādi ir.

1. pielikums. Korelācijas tabulas

Turpmākajās tabulās ir sniegts blakus salīdzinājums par novērtējuma prasībām, kas ir noteiktas iepriekšējās Regulas (ES) Nr. 1158/2010 un Regulas (ES) Nr. 1169/2010 II pielikumā, un prasībām, kas ir noteiktas Komisijas Deleģētās regulas (ES) 2018/762 I un II pielikumā. Salīdzinājuma mērķis ir atvieglot pāreju no vecā drošības sertifikācijas režīma atbilstoši Direktīvai 2004/49/EK uz jauno režīmu, kas ieviests ar Direktīvu (ES) 2016/798.

Atbilstība Komisijas Deleģētajai regulai (ES) 2018/762 nav uzskatāma par pierādījumu, ka dzelzceļa pārvadājumu uzņēmumi vai infrastruktūras pārvaldītāji spēj izpildīt attiecīgās SMS prasības saskaņā ar Direktīvas (ES) 2016/798 9. pantu. Iepriekšējo un jauno novērtējuma prasību detalizācijas līmenis tik un tā var atšķirties, kaut arī tām piemēro zināmā mērā vienotus principus. Turklāt ne visas novērtējuma prasības, kas ir paredzētas Komisijas Deleģētās regulas (ES) 2018/762 I un II pielikumā, atbilst iepriekšējām regulām. Tādā gadījumā dzelzceļa pārvadājumu uzņēmumiem un infrastruktūras pārvaldītājiem jāiesniedz papildu pierādījumi, kas apliecina, ka tie izpilda jaunās novērtējuma prasības (vai to daļas).

Komisijas Deleģētajā regulā (ES) 2018/762 noteiktās SMS prasības, kas neatbilst prasībām Regulā (ES) Nr. 1158/2010 un/vai Regulā (ES) Nr. 1169/2010, ir jāuzskata par jaunām prasībām, un saistībā ar to pieteikuma iesniedzējam jāiesniedz papildu pierādījumi, lai parādītu atbilstību šādām prasībām. Vairumā gadījumu nav iespējama pilnīga atbilstība starp iepriekšējo regulu kritērijiem un jaunās CSM regulas prasībām. Tāpēc šādos apstākļos par salīdzinājuma pamatu ir izmantots prasību nolūks. Ir arī iespējams, ka Komisijas Deleģētajā regulā (ES) 2018/762 prasības ir definētas skaidrāk, lai gan tām ir vienāds nolūks. Šādā gadījumā minētajā regulā paredzētās prasības nav jāuzskata par jaunām, bet dažādās personas var tās izmantot, lai būtu vieglāk saprast, kādi pierādījumi tiek gaidīti no pieteikuma iesniedzēja.

Dzelzceļa pārvadājumu uzņēmumiem un infrastruktūras pārvaldītājiem, kas vēlas izstrādāt integrētu pārvaldības sistēmu, ir arī noteikta prasība nodrošināt atbilstību ISO augsta līmeņa struktūrai (HLS)². Arī dzelzceļa pārvaldības sistēma, kas ir sertificēta atbilstoši vienam vai vairākiem ISO pārvaldības sistēmu standartiem (piemēram, ISO 9001, ISO 14001 vai ISO 45001), nav uzskatāma par pierādījumu tam, ka dzelzceļa pārvadājumu uzņēmumi vai infrastruktūras pārvaldītāji spēj izpildīt attiecīgās SMS prasības saskaņā ar Direktīvas (ES) 2016/798 9. pantu.

1. tabula. Blakus salīdzinājums. Novērtēšanas kritēriji/prasības, ko piemēro gan dzelzceļa pārvadājumu uzņēmumiem, gan infrastruktūras pārvaldītājiem

<i>Regulas (ES) Nr. 1158/2010 un Regulas (ES) Nr. 1169/2010 kritērija identifikators</i>	<i>Regulas (ES) 2018/762 prasības identifikators</i>	<i>ISO HLS noteikuma Nr.</i>	<i>Komentārs</i>
A.1.	3.1.1.1.	6.1.	
A.2.	3.1.1.1.	6.1.	
A.3.	6.1.1.	9.1.	
A.4.	3.1.1.1. e)	N/P	
A.5.	4.4. 4.5.1.1.	7.4.	
A.6.	6.1.1. 5.4.1.	9.1. 8.1.	

² ISO/IEC direktīvas, 1. daļa, 2016. gada konsolidētais papildinājums, SL pielikums, 2. papildinājums.

<i>Regulas (ES) Nr. 1158/2010 un Regulas (ES) Nr. 1169/2010 kritērija identifikators</i>	<i>Regulas (ES) 2018/762 prasības identifikators</i>	<i>ISO HLS noteikuma Nr.</i>	<i>Komentārs</i>
B.1.	5.2.4.	N/P	Tehniskā apkope ir aktīva dzīves cikla posms.
B.2.	5.2.4.	N/P	Tehniskā apkope ir aktīva dzīves cikla posms.
B.3.	2.3.1. 4.2.1.	5.3. 7.2.	Tehniskās apkopes jomā veicamo pienākumu definīcija un sadalījums lielākoties ir norādīts 2.3.1. punktā. Tehniskās apkopes jomā vajadzīgo kompetenču identifikācija lielākoties ir norādīta 4.2.1. punktā.
B.4.	6.1.1. 5.2.5.	9.1. 7.4.	Datu vākšana (darbības traucējumi, bojājumi) un analīze ir pārraudzības procesa daļa. Datu apmaiņa starp darbiniekiem, kuri atbild par ekspluatāciju ikdienā, un darbiniekiem, kuri atbild par tehnisko apkopi, ir daļa no informācijas un saziņas procesa, ko piemēro aktīvu pārvaldībai.
B.5.	6.1.1.	N/P	Norādīts CSM pārraudzībai 4. panta 2. punktā.
B.6.	6.1.1.	9.1.	Tehniskās apkopes veikšanas un rezultātu izvērtēšana ir daļa no tehniskajai apkopei piemērotā pārraudzības procesa.
C.1.	5.3.2. a) 5.3.3. a)	8.1.	
C.2.	5.3.3. a)	8.1.	
C.3.	5.3.2. b)	N/P	
C.4.	5.2.5. b) 5.3.2. c)	N/P	
C.5.	5.3.2. c) 5.3.3. a)	N/P	
D.1.	3.1.1.1. a)	N/P	
D.2.	3.1.1.1. c)	N/P	
D.3.	6.1.1.	N/P	
E.1.	1.1.1. a) 1.1.1. b)	4.1.	
E.2.	4.5.1.1. a)	4.4.	
E.3.	4.5.1.1. c)	7.5.1.	
E.4.	4.5.1.1. a) 4.5.1.1. b)	7.5.1.	

<i>Regulas (ES) Nr. 1158/2010 un Regulas (ES) Nr. 1169/2010 kritērija identifikators</i>	<i>Regulas (ES) 2018/762 prasības identifikators</i>	<i>ISO HLS noteikuma Nr.</i>	<i>Komentārs</i>
F.1.	4.5.1.1. a)	4.4.	
F.2.	2.3. 4.5.1.1. a)	5.3. 4.4.	
F.3.	2.3.1. 2.3.4.	N/P	
F.4.	4.5.1.1. a) 4.2.1. 2.3.1. 2.3.2. 2.3.3.	4.4. 5.3.	Ar drošību saistītu uzdevumu definīcija ir drošības pārvaldības sistēmas apraksta daļa, kas ietver pienākumu sadalījumu. Ar katru attiecīgo funkciju saistītie pienākumi ir noteikti drošības pārvaldības sistēmā.
G.1.	4.5.1.1. a) 2.3.1.	4.4. 5.3.	Ar drošību saistītu uzdevumu definīcija ir drošības pārvaldības sistēmas apraksta daļa, kas ietver pienākumu sadalījumu. Ar katru attiecīgo funkciju saistītie pienākumi ir noteikti drošības pārvaldības sistēmā.
G.2.	6.1.1. 6.2.1.	9.1. 9.2.	Iekšējās revīzijas mērķis ir pārbaudīt, vai organizācija atbilst piemērojamām prasībām.
G.3.	2.1.1. d), i) 2.3.2.	N/P	
G.4.	2.3.1.	5.3.	
G.5.	4.1.1.	7.1.	Jāņem vērā, ka šeit pastāv saikne ar kritēriju, kas noteikts Regulas (ES) Nr. 1158/2010 N2. punkta d) apakšpunktā.
H.1.	2.4.1.	N/P	
H.2.	(izņemts)	N/P	Personāls, kas veic ar drošību saistītus uzdevumus, ir jāiesaista SMS izstrādē, uzturēšanā un uzlabošanā. Organizācijas ziņā ir īstenot 2.4.1. punkta prasības tā, lai atbilstība šim punktam būtu izsekojama.
I	7.2.1.	10.1. 10.2.	
J	2.2.1.	5.2.	
K.1.	3.2.1. 3.2.2. d)	6.2.	
K.2.	3.2.2. a)	6.2.	Drošības mērķiem ir jāatbilst drošības politikai, kurai ir jābūt samērīgai attiecībā pret dzelzeļa darbību veidu un apjomu.

<i>Regulas (ES) Nr. 1158/2010 un Regulas (ES) Nr. 1169/2010 kritērija identifikators</i>	<i>Regulas (ES) 2018/762 prasības identifikators</i>	<i>ISO HLS noteikuma Nr.</i>	<i>Komentārs</i>
K.3.	3.2.4.	6.2.	Drošības mērķi neaprobežojas ar dalībvalsts līmenī noteiktiem kopīgiem drošības mērķiem.
K.4.	6.1.1. 5.4.	9.1. 8.1.	
K.5.	3.2.4. (pielāgots)	9.1.	Atsauce uz pārraudzības stratēģiju un plānu(-iem) atbilstoši CSM pārraudzībai.
L.1.	6.1.1. 5.4.	9.1. 8.1.	
L.2.	4.2. 4.4. 4.5. 5.2.2. a)	N/P	Kompetenta personāla, procedūru, konkrētu dokumentu un ritošā sastāva izmantošana tiek attiecīgi pārvaldīta kompetences, informācijas un saziņas, kā arī dokumentētas informācijas un aktīvu pārvaldībā.
L.3.	1.1.1. e) 6.1.1. 6.1.2.	4.3. 9.2.	Atbilstība piemērojamām prasībām izriet galvenokārt no 3.1.2.2. punkta (neattiecas konkrēti uz tehnisko apkopi). Pārraudzība nodrošina procedūru pareizu piemērošanu. Iekšējā revīzija nodrošina procedūru atbilstību piemērojamām prasībām.
M.1.	3.1.2.1. 5.4.1.	6.1. 8.1.	Atbilstoši ISO vispirms notiek izmaiņu plānošana, kas ietver riska apzināšanu un novērtēšanu, un tad seko izmaiņu īstenošana.
M.2.	3.1.2.1.	N/P	
M.3.	5.4.1.	8.1.	
N.1.	4.2.1. 4.2.3.	7.2.	
N.2.	4.5.1.1. a) 2.3.1. 2.3.2. 2.3.4. 6.1.1.	N/P	
O.1.	4.4.1. 4.4.2. 4.4.3.	7.4.	
O.2.	4.4.3.	7.4.	
O.3.:	4.4.1.	N/P	
P.1.	4.4.3.	N/P	

<i>Regulas (ES) Nr. 1158/2010 un Regulas (ES) Nr. 1169/2010 kritērija identifikators</i>	<i>Regulas (ES) 2018/762 prasības identifikators</i>	<i>ISO HLS noteikuma Nr.</i>	<i>Komentārs</i>
P.2.	4.5.2. 4.5.3.	7.5.2. 7.5.3.	
P.3.	4.5.3.	7.5.3.	
Q.1.	7.1.1.	10.1.	
Q.2.	7.1.2.	N/P	
Q.3.	7.1.3.	10.2.	
R.1.	5.5.1.	N/P	
R.2.	5.5.2.	N/P	
R.3.	5.5.3.	N/P	
R.4.	5.5.4.	N/P	
R.5.	5.5.5.	N/P	
R.6.	5.5.1.	N/P	
R.7.	5.5.6.	N/P	
S.1.	6.2.1.	9.2.	
S.2.	6.2.1. a)	9.2.	
S.3.	6.2.1. b)	9.2.	
S.4.	6.2.1. c)–f)	9.2.	
S.5.	6.2.1. g) 6.3.1.	9.3.	
S.6.	6.2.1.	9.2.	

Turpmākajā tabulā ir blakus salīdzināti iepriekšējie novērtēšanas kritēriji un jaunās SMS prasības, kas piemērojamas tikai dzelzceļa pārvadājumu uzņēmumiem.

2. tabula. Blakus salīdzinājums. Novērtēšanas kritēriji/prasības, ko piemēro tikai dzelzceļa pārvadājumu uzņēmumiem

<i>Regulas (ES) Nr. 1158/2010 kritērija identifikators</i>	<i>Regulas (ES) Nr. 2018/762 I pielikums Prasības identifikators</i>	<i>ISO HLS Noteikuma Nr.</i>	<i>Komentārs</i>
R.8.	5.5.7.	N/P	

<i>Regulas (ES) Nr. 1158/2010 kritērija identifikators</i>	<i>Regulas (ES) Nr. 2018/762 I pielikums Prasības identifikators</i>	<i>ISO HLS Noteikuma Nr.</i>	<i>Komentārs</i>
R.9.	5.5.8.	N/P	

Turpmākajā tabulā ir blakus salīdzināti iepriekšējie novērtēšanas kritēriji un jaunās SMS prasības, kas piemērojamas tikai infrastruktūras pārvaldītājiem.

3. tabula. Blakus salīdzinājums. Novērtēšanas kritēriji/prasības, ko piemēro tikai infrastruktūras pārvaldītājiem

<i>Regulas (ES) Nr. 1169/2010 kritērija identifikators</i>	<i>Regulas (ES) Nr. 2018/762 II pielikums Prasības identifikators</i>	<i>ISO HLS Noteikuma Nr.</i>	<i>Komentārs</i>
R.8.	5.5.7.	N/P	
R.9.	5.5.8.	N/P	
T.1.	5.2.1.	N/P	Infrastruktūras droša projektēšana un ierīkošana ir aktīvu dzīves cikla daļa.
T.2.	3.1.2 5.4.1.	N/P	Infrastruktūras tehnisko izmaiņu identifikācija lielākoties ir izklāstīta 3.1.2. punktā. Infrastruktūras tehnisko izmaiņu pārvaldība lielākoties ir izklāstīta 5.4.1. punktā.
T.3.	3.1.2	N/P	Atbilstība piemērojamiem noteikumiem, kas attiecas uz infrastruktūras projektēšanu, lielākoties ir izklāstīta 3.1.2. punktā.
U.1.	5.1.1. 5.1.3.	N/P	Infrastruktūras drošības pārvaldība lielākoties ir izklāstīta 5.1.1. punktā.
U.2.	5.1.1.	N/P	Drošības pārvaldība uz infrastruktūras fiziskajām un/vai ekspluatācijas robežām lielākoties ir izklāstīta 5.1.1. punktā.
U.3.	5.1.3. c) 5.5.7.	N/P	Normālas un traucētas ekspluatācijas apstākļu pārvaldība lielākoties ir izklāstīta 5.1.3. punkta c) apakšpunktā.
U.4.	5.1.2. 5.2.3.	N/P	
V.1.	5.2.4. 6.1.1.	N/P	Infrastruktūras tehniskā apkope lielākoties ir izklāstīta 5.2.4. punktā. Revīzijas un pārbaudes (attiecīgā gadījumā) ir pārraudzības pasākumu daļa.
V.2.	5.2.4.	N/P	Infrastruktūras tehniskā apkope lielākoties ir izklāstīta 5.2.4. punktā.
V.3.	5.2.3.	N/P	
W.1.	5.1.3.	N/P	

<i>Regulas (ES) Nr. 1169/2010 kritērija identifikators</i>	<i>Regulas (ES) Nr. 2018/762 II pielikums Prasības identifikators</i>	<i>ISO HLS Noteikuma Nr.</i>	<i>Komentārs</i>
W.2.	5.1.1.	N/P	Drošības pārvaldība uz kustības vadības un signalizācijas sistēmas fiziskajām un/vai ekspluatācijas robežām lielākoties ir izklāstīta 5.1.1. punktā.
W.3.	5.1.2. 5.2.3.	N/P	

Turpmākajā tabulā ir blakus salīdzinātas ISO HLS un jaunās SMS prasības.

4. tabula. Blakus salīdzinājums. ISO augsta līmeņa struktūra

<i>ISO HLS Noteikuma Nr.</i>	<i>Regulas (ES) Nr. 2018/762 prasības identifikators</i>	<i>Komentārs</i>
4.1.	1.1.1. a) 1.1.1. b)	
4.2.	1.1.1. c) 1.1.1. d)	
4.3.	1.1.1. e) 1.1.1. f)	
4.4.	4.5.1.1. a)	
5.1	2.1.	
5.2.	2.2.	
5.3.	2.3.	
6.1.	3.1.1 3.1.2	Lai noteiktu, vai izmaiņas ir (vai nav) saistītas ar drošību un — attiecīgi — vai tās ir (vai nav) būtiskas, piemēro CSM riska noteikšanai. “Virtuālais” nošķirums ISO starp plānošanas stratēģisko līmeni (ISO HLS 6. noteikums) un taktisko līmeni (ISO HLS 8. noteikums) tiek izvērtēts atkārtoti, ņemot vērā ES tiesisko regulējumu un jo īpaši piemērojot iepriekš minēto CSM (neatkarīgi no izmaiņu veida).
6.2.	3.2.1. 3.2.2. a) 3.2.2. d) 3.2.4.	
7.1.	4.1.	
7.2.	4.2.	
7.3	4.3.	

ISO HLS Noteikuma Nr.	Regulas (ES) Nr. 2018/762 prasības identifikators	Komentārs
7.4.	4.4.	
7.5.1.	4.5.1	
7.5.2.	4.5.2.	
7.5.3.	4.5.3.	
8.1.	5.1 5.2. 5.3. 5.4. 5.5	Atbilstoši ISO vadlīnijām (N360) ISO HLS 8. noteikuma mērķis ir precizēt prasības, kas jāīsteno organizācijas darbībās, lai nodrošinātu pārvaldības sistēmas prasību izpildi, kā arī to, ka tiek ņemti vērā prioritārie riski un iespējas. Turklāt ir noteikts, ka var paredzēt arī papildu prasības (konkrētai disciplīnai) saistībā ar ekspluatācijas plānošanu un kontroli. Šajā ziņā 5.X prasības atbilst ISO pieejai. Konkrētāk, tās nekaitē uzņēmuma uzņēmējdarbībai, taču nodrošina pietiekamu sistēmu, lai kontrolētu galveno drošības jautājumu pārvaldību uzņēmuma uzņēmējdarbības procesos.
9.1.	6.1.	Jēdziens “pārraudzība” nozīmē pārraudzības sistēmu, kas definēta CSM pārraudzībai, tāpēc tam ir plašāka nozīme nekā ISO HLS 9.1. noteikumā definētajiem jēdzieniem “pārraudzība”, “novērtēšana”, “analīze” un “izvērtēšana”.
9.2.	6.2.	Iekšējās revīzijas pasākumi ir pārraudzības rīki CSM pārraudzībai nozīmē. Lai gan tā ir atsevišķa prasība, tā ir paredzēta, lai sasniegtu pārraudzības mērķus atbilstoši CSM pārraudzībai.
9.3.	6.3	
10.1.	7.1.	
10.2.	7.2.	

2. pielikums. Atbilstoši Savienības tiesību aktiem piešķirtu produktu vai pakalpojumu atļauju, atzīšanas dokumentu vai sertifikātu savstarpējā atzīšana

Vienotā drošības sertifikāta vai drošības atļaujas izdevēja iestāde var ņemt vērā citu struktūru, piemēram, ISO atbilstības novērtēšanas struktūru, piešķirtus sertifikātus, lai izvairītos no novērtējuma dublēšanās un papildu izmaksu rašanās pieteikuma iesniedzējam. Galīgais lēmums vienmēr jāpieņem izdevējai iestādei.

Tomēr saskaņā ar Īstenošanas regulas (ES) 2018/763 3. panta 12. punktu, novērtējot pieteikumus vienoto drošības sertifikātu saņemšanai, izdevēja iestāde izmanto atbilstoši attiecīgajiem Savienības tiesību aktiem izsniegtas dzelzceļa pārvadājumu uzņēmumu vai to darbuzņēmēju, partneru vai piegādātāju produktu vai pakalpojumu atļaujas, atzīšanas dokumentus vai sertifikātus kā pierādījumu par dzelzceļa pārvadājumu uzņēmumu spēju izpildīt attiecīgās drošības pārvaldības sistēmas prasības attiecībā uz konkrēto produkta vai pakalpojuma veidu. Lai gan ES tiesību aktos nav līdzvērtīga noteikuma par drošības atļauju pieteikumu novērtēšanu, arī valstu drošības iestādes tiek aicinātas piemērot tādu pašu principu.

Turpmākajā tabulā ir norādīti līdz šim ES tiesiskajā regulējumā aplūkoti dažādie gadījumi un sniegti ilustratīvi piemēri par produktu vai pakalpojumu veidiem, uz kuriem var attiecināt katru no gadījumiem.

5. tabula. Atbilstoši Savienības tiesību aktiem piešķirtas produktu vai pakalpojumu atļaujas, atzīšanas dokumenti vai sertifikāti

<i>Gadījums</i>	<i>Produktu vai pakalpojumu veids</i>	<i>Piemērojamie Savienības tiesību akti</i>	<i>Regulas (ES) Nr. 2018/762 prasības identifikators</i>	<i>Komentārs</i>
ECM sertifikāts	Ritekļu tehniskā apkope	Direktīvas (ES) 2016/798 14. panta 4. punkts	5.2. 5.3.	Gadījumos, kas paredzēti Direktīvas (ES) 2016/798 14. panta 4. punktā, par tehnisko apkopi atbildīgo struktūru un — attiecīgā gadījumā — tehniskās apkopes darbnīcu sertifikācija ir pietiekams pierādījums, ka dzelzceļa pārvadājumu uzņēmumi un infrastruktūras pārvaldītāji, īstenojot savu drošības pārvaldības sistēmu, spēj kontrolēt ar kravas vagonu tehnisko apkopi, tostarp darbuzņēmēju izmantošanu, saistītos riskus.

<i>Gadījums</i>	<i>Produktu vai pakalpojumu veids</i>	<i>Piemērojamie Savienības tiesību akti</i>	<i>Regulas (ES) Nr. 2018/762 prasības identifikators</i>	<i>Komentārs</i>
Atzīšanas dokuments	Vilcienu vadītāju apmācība	Direktīva 2007/59/EK Lēmums 2011/765/ES	4.2.2.	Mācību centriem ir jābūt kompetentās iestādes atzītiem mācību kursu nodrošināšanai vilcienu vadītājiem un vilcienu vadītāja kandidātiem atbilstoši Direktīvai 2007/59/EK. Mācību centriem ir būtiska nozīme, nodrošinot, ka vilcienu vadītāji ir kompetenti veikt viņiem uzdotos ar drošību saistītos uzdevumus. Saistībā ar to mācību centriem ir jābūt kompetentiem nodrošināt attiecīgo apmācību, un to atzīšana, ko veikusi kompetenta iestāde, attiecīgā gadījumā ir jāņem vērā drošības sertifikācijas struktūrai un valsts drošības iestādei, kad tās veic kompetences pārvaldības sistēmas novērtējumu.
Vilciena vadītāja apliecība un sertifikāts	Vilciena vadītāju kompetence un piemērotība	Direktīva 2007/59/EK	4.2.1.	Apliecības un sertifikāti, kas izsniegti atbilstoši Direktīvai 2007/59/EK, ir pietiekams vilciena vadītāju piemērotības un kompetences pierādījums. Minētais neliedz organizācijai parādīt, ka tās pasākumi attiecībā uz kompetenci un piemērotību ir atbilstoši.

<i>Gadījums</i>	<i>Produktu vai pakalpojumu veids</i>	<i>Piemērojamie Savienības tiesību akti</i>	<i>Regulas (ES) Nr. 2018/762 prasības identifikators</i>	<i>Komentārs</i>
Vienotais drošības sertifikāts	Infrastrukturā uzturēšana un pārbaude Manevrēšana Ritošā sastāva testēšana	Direktīvas (ES) 2016/798 10. pants	5.3.	Infrastrukturā pārvaldītāji savas infrastruktūras uzturēšanai vai pārbaudei var nolīgt uzņēmumus, kas uz sliedēm ekspluatē īpašus ritekļus. Tie arī var pieprasīt, lai operatoriem, kuri sniedz manevrēšanas vai testēšanas pakalpojumus, būtu drošības sertifikāts. Iepriekš minētajos gadījumos vienotais drošības sertifikāts ir pietiekams pierādījums, ka dzelzceļa pārvadājumu uzņēmumi un infrastruktūras pārvaldītāji, īstenojot savu drošības pārvaldības sistēmu, spēj kontrolēt ar darbuzņēmēju un piegādātāju izmantošanu saistītos riskus.
Atļauja laišanai tirgū / ritekļa tipa atļauja	Ritekļa (tipa) atļauja	Direktīva (ES) 2016/797	5.2.	Ritekļa (tipa) atļauja nodrošina, ka ar ritekļa projektēšanas, ražošanas, pārbaudes un apstiprināšanas procesa starpniecību ir panākta ritekļa atbilstība visu piemērojamo tiesību aktu (tostarp drošības jomā) būtiskajām prasībām, kas ļauj to droši izmantot dzelzceļa tīklos, kuriem tas ir paredzēts, ievērojot ritekļa/ ritekļa tipa tehniskajā dokumentācijā norādītos ierobežojumus un izmantošanas nosacījumus.

Īpašos gadījumos sertifikāta (vai līdzvērtīga dokumenta) piešķiršana saskaņā ar Savienības tiesību aktiem var nebūt pietiekams apstāklis, lai varētu kontrolēt visus drošības apdraudējumus saistībā ar dzelzceļa pārvadājumu uzņēmumiem un infrastruktūras pārvaldītājiem piegādātajiem produktiem vai to izmantotajiem pakalpojumiem.

Piemēram, dzelzceļa pārvadājumu uzņēmumi ir solidāri pilnīgi atbildīgi par ekspluatācijas drošību un attiecīgi arī par to risku kontroli, kas saistīti ar viņu darbībām, tostarp ritekļu tehnisko apkopi. Nepietiek ar to, ka dzelzceļa pārvadājumu uzņēmums izmanto sava partnera vienoto drošības sertifikātu kā līdzekli, lai kontrolētu ar tehniskās apkopes nodrošināšanu saistītos riskus, ja tas nav pamatots ar ciešām un faktiskām partneru līgumsaistībām. Šādām līgumsaistībām jābūt kopīgi izstrādātām un pārraudzītām katra partnera SMS procedūru piemērošanā, un tās ir arī daļa no katra partnera SMS, tāpēc uz tām attiecinā attiecīgo VDI veikto uzraudzību.

Tādējādi vienoto drošības sertifikātu var izmantot kā līdzekli ar tehniskās apkopes nodrošināšanu saistīto risku kontrolei un arī kā līdzekli, lai nodrošinātu atbilstību prasībām attiecībā uz to risku kontroli, kuri saistīti ar ritekļu tehnisko apkopi, ja ir izpildīti šādi trīs nosacījumi.

1. *Starp dzelzceļa pārvadājumu partneruzņēmumiem jābūt spēkā esošām līgumsaistībām, kas aptver ar ritekļu tehnisko apkopi saistītus aspektus, piemēram, šādus:*
 - a) *informācijas apmaiņa, kā aprakstīts Regulas (ES) Nr. 445/2011 5. pantā;*
 - b) *attiecīgā gadījumā — tehniskais atbalsts, jo īpaši attiecībā uz mantotajām vadības sistēmām;*
 - c) *kontrole attiecībā uz nolīgto tehniskās apkopes darbnīcu spēju veikt tehnisko apkopi;*
 - d) *ritekļu efektīva pārraudzība un no šādas pārraudzības izrietošas informācijas apmaiņa.*
2. *Šādas līgumsaistības ir izstrādātas riska novērtējuma rezultātā, un katram dzelzceļa pārvadājumu uzņēmumam tās ir regulāri jāpārbauda attiecībā pret CSM pārraudzībai (Regula (ES) Nr. 1078/2012). Tad abi dzelzceļa pārvadājumu partneruzņēmumi oficiāli apmainās ar šādas pārraudzības rezultātiem.*
3. *Abu partneru SMS ietver attiecīgus procesus un procedūras 1. un 2. punktā minēto nosacījumu izpildei.*

Citos gadījumos valsts tiesību aktos var būt noteikta prasība, ka attiecībā uz konkrētu produkta vai pakalpojuma veidu jābūt kompetentas struktūras (piemēram, valsts drošības iestādes) izdotam valsts sertifikātam (vai līdzvērtīgam dokumentam), ko arī varētu izmantot kā pierādījumu par dzelzceļa pārvadājumu uzņēmumu vai infrastruktūras pārvaldītāju spēju izpildīt attiecīgās prasības, kādas ir noteiktas Komisijas Deleģētajā regulā (ES) 2018/762. Piemēram, arī valsts sertifikāti, kas piešķirti ECM un/vai ritekļu (izņemot kravas vagonus) tehniskās apkopes darbnīcām, līdzīgi kā ECM sertifikāts, var sniegt pamatotu pārliecību, ka ritekļi, par kuru tehnisko apkopi ECM vai apkopes darbnīcas ir atbildīgas, ir ekspluatācijai drošā stāvoklī.

3. pielikums. Darbības uz pievedceļiem, līgumsaistības un partnerības

Darbības uz pievedceļiem

Šajā dokumentā “pievedceļi” ir dzelzceļa infrastruktūra, kas savienota ar dzelzceļa tīklu un par ko atbild infrastruktūras pārvaldītājs (t. i., dzelzceļa sistēmas infrastruktūras daļa, uz ko attiecas Direktīvas (ES) 2016/798 darbības joma). Atkarībā no minētās direktīvas transponēšanas katrā dalībvalstī pievedceļi var būt un var nebūt dzelzceļa tīkla daļa.

Darbības, ko veic uz pievedceļiem, piemēram, vagonu piekraušana, ir rūpnieciskas darbības, kas mijiedarbojas ar īpašām dzelzceļa darbībām, piemēram, ritekļu sastāvu — kas var būt vilcieni vai tiks izmantoti vilcienos — nokomplektēšanu, sagatavošanu un kustību. Minētais ietver dažādu ritekļu sakabināšanu, lai izveidotu ritekļu sastāvus vai vilcienus, un to pārvietošanu.

Pievedceļi var būt (uzskaitījums nav izsmeļošs):

- *infrastruktūra, ko izmanto, lai dzelzceļa ritekļus novietotu stāvēšanai to ekspluatācijas starplaikos;*
- *multimodālie termināļi;*
- *infrastruktūra, ko izmanto pasažieru ritekļu tehniskās apkopes darbībām, piemēram, tīrīšanai vai “vieglajai” apkopei;*
- *infrastruktūra, kas pieder dzelzceļa ritekļu tehniskās apkopes darbnīcai un ko šī darbnīca pārvalda;*
- *rūpnieciskas teritorijas vai ražotnes, kur notiek kravas vagonu rūpnieciskās piekraušanas/izkraušanas darbības.*

Darbības uz pievedceļiem veic “pievedceļu operators”. Pievedceļu operators var būt dzelzceļa pārvaldījumu uzņēmums, infrastruktūras pārvaldītājs, pakalpojumu sniedzējs (piemēram, pasažieru ritekļu tīrīšana), rūpnieciska organizācija (piemēram, ķīmiskā rūpnīca, kas piekrauj/izkrauj cisternvagonus) vai pat šādas rūpnieciskas organizācijas apakšuzņēmums. Pirmajā minētajā gadījumā organizācija ir pieņēmusi komerciālu lēmumu kļūt par dzelzceļa pārvaldījumu uzņēmumu vai ir dzelzceļa pārvaldījumu uzņēmums, kas plāno pārvaldīt pievedceļus papildus savām pašreizējām dzelzceļa darbībām. Pēdējā minētajā gadījumā infrastruktūras pārvaldītājs ir pievedceļu infrastruktūras pārvaldītājs vai darbojas kā dzelzceļa pārvaldījumu uzņēmums atbilstoši savai drošības atļaujai.

“Pievedceļu operators” kontrolē ar darba aizsardzību saistītos riskus, izmantojot savu veselības un drošības pārvaldības sistēmu atbilstoši starptautiskiem un vietējiem tiesību aktiem. Ja “pievedceļu operators” nav dzelzceļa pārvaldījumu uzņēmums, šādā pārvaldības sistēmā ņem vērā pienākumus veselības un drošības jomā saistībā ar ārējiem darbiniekiem un jo īpaši dzelzceļa pārvaldījumu uzņēmumu darbiniekiem, piemēram, kad vilcienu vadītāji uzbrauc uz pievedceļiem. Tajā pašā laikā dzelzceļa pārvaldījumu uzņēmums kontrolē ar darba aizsardzību saistītos riskus, izmantojot savu veselības un drošības pārvaldības sistēmu atbilstoši starptautiskiem un vietējiem tiesību aktiem.

1. gadījums. Pievedceļu operators ir dzelzceļa pārvaldījumu uzņēmums “Y”

Dzelzceļa pārvaldījumu uzņēmums ar savas SMS starpniecību kontrolē riskus saistībā ar tā dzelzceļa darbībām tā pievedceļu infrastruktūrā un dzelzceļa tīklā, par ko atbild infrastruktūras pārvaldītājs. Šāda risku kontrole aptver riskus saistībā ar ritekļu bojājumiem, ko izraisa visas uz pievedceļiem veiktās darbības, tostarp vilcienu sastāvu komplektēšana, sagatavošana un kustība.

Praksē dažreiz ir grūti noteikt atbildīgo dzelzceļa pārvaldījumu uzņēmumu. Piemēram, dzelzceļa pārvaldījumu uzņēmuma “X” vilciens uzbrauc uz pievedceļa (vadītājs un lokomotīve ir nolīgti), un dzelzceļa pārvaldījumu uzņēmums “Y”, kas ir pievedceļa operators, pārņem vilcienu kā jaunu vilcienu (vadītājs un lokomotīve ir nolīgti), un pa to laiku ir jāveic darbības uz pievedceļa. Šādā gadījumā piemēro iepriekš izklāstīto drošības principu. Ir kopēji saskarņu riski, kas ir jāņem vērā dzelzceļa pārvaldījumu uzņēmuma “Y” SMS (piemēram, ritekļu bojājums, ko izraisījušas darbības uz pievedceļa, piemēram, iekraušana). Turklāt ir jāapsver arī informācijas par ritekļiem nodošana no dzelzceļa pārvaldījumu uzņēmuma “X” dzelzceļa pārvaldījumu uzņēmumam “Y”. Minētais ietver apliecinājumu, ka riteklis ir ekspluatācijai drošā stāvoklī, kad dzelzceļa

pārvadājumu uzņēmums “X” to nodod pievedceļu operatoram, un — līdzīgi — arī tad, kad ritekli nodod tālāk ar dzelzceļa pārvadājumu uzņēmuma “Y” starpniecību. Dzelzceļa pārvadājumu uzņēmums “Y”, kas atbild par darbībām uz pievedceļiem, joprojām ir pilnīgi pārskatatbildīgs par risku kontroli saistībā ar tehniskās apkopes darbībām, ko veic uz pievedceļiem.

2. gadījums. Pievedceļu operators nav dzelzceļa pārvadājumu uzņēmums

Var apsvērt četrus apakšgadījumus:

- **2.1. apakšgadījums**, kad pievedceļu operators ir infrastruktūras pārvaldītājs;
- **2.2. un 2.3. apakšgadījums**, kad pievedceļu operators, kurš nav infrastruktūras pārvaldītājs, veic darbības tikai savā infrastruktūrā, bet ne dzelzceļa tīklā, par ko atbild infrastruktūras pārvaldītājs;
- **2.4. apakšgadījums** attiecas uz dzelzceļa darbībām, ko veic pievedceļu operators, kurš nav infrastruktūras pārvaldītājs, dzelzceļa tīklā, par ko atbild infrastruktūras pārvaldītājs.

2.1. apakšgadījums. Kad darbības uz pievedceļiem kopīgi veic dzelzceļa pārvadājumu uzņēmums(-i) un infrastruktūras pārvaldītājs (vai jebkura organizācija, kas rīkojas tā vārdā), katram dzelzceļa pārvadājumu uzņēmumam ar līgumsaistību starpniecību jābūt informētam par visiem ar drošību saistītajiem notikumiem, kas norisinājušies infrastruktūras pārvaldītāja darbību laikā. Minētais attiecas uz bojājumiem, negadījumiem un starpgadījumiem, kuros ir iesaistīti ritekļi.

Šādas līgumsaistības pārvalda attiecīgi ar katra dzelzceļa pārvadājumu uzņēmuma SMS un infrastruktūras pārvaldītāja SMS.

Dzelzceļa pārvadājumu uzņēmums ar savas SMS starpniecību kontrolē ar savām darbībām saistītos riskus, pamatojoties uz saņemto informāciju.

2.2. apakšgadījums. Vilciena sastāvu komplektēšanu un sagatavošanu veic dzelzceļa pārvadājumu uzņēmums (sakabināšana, sagatavošana) pievedceļu infrastruktūrā. Dzelzceļa pārvadājumu uzņēmumam ar līgumsaistību starpniecību jābūt informētam par visiem (ar drošību saistītiem) notikumiem, kas norisinājušies pievedceļu operatora veikto darbību (piemēram, iekraušanas vai tīrīšanas) laikā. Minētais attiecas uz bojājumiem, negadījumiem un starpgadījumiem, kuros ir iesaistīti ritekļi.

Šādas līgumsaistības pārvalda ar dzelzceļa pārvadājumu uzņēmuma SMS.

Dzelzceļa pārvadājumu uzņēmums ar savas SMS starpniecību kontrolē ar savām turpmākajām darbībām saistītos riskus, pamatojoties uz saņemto informāciju.

2.3. apakšgadījums. Vilciena sastāva nokomplektēšanu pilnīgi/daļēji veic pievedceļu operators vai organizācija, kas darbojas tā vārdā.

Pēc vilciena sastāva nokomplektēšanas tas tiek nodots vienam dzelzceļa pārvadājumu uzņēmumam.

Līdzīgi kā 2.2. apakšgadījumā dzelzceļa pārvadājumu uzņēmumam ar līgumsaistību starpniecību jābūt informētam par visiem notikumiem, kas norisinājušies pievedceļu operatora veikto darbību (piemēram, iekraušanas vai tīrīšanas) un vilciena sastāva nokomplektēšanas laikā. Šādi notikumi ietver bojājumus, negadījumus un starpgadījumus, kuros ir iesaistīti ritekļi.

Šādas līgumsaistības pārvalda ar dzelzceļa pārvadājumu uzņēmuma SMS.

Dzelzceļa pārvadājumu uzņēmums ar savas SMS starpniecību kontrolē ar savām darbībām saistītos riskus, pamatojoties uz saņemto informāciju.

2.4. apakšgadījums. Šis apakšgadījums papildina 2.3. apakšgadījumu, tāpēc turpmāk ir izklāstīts tikai dzelzceļa pārvadājumu uzņēmuma papildu pienākums.

Pievedceļu operators pārvieto vilcienus vai novirza ritekļu sastāvus no savas dzelzceļa infrastruktūras uz dzelzceļa tīklu, par ko atbild infrastruktūras pārvaldītājs.

Piemēram,

- *tas pārvieto vilcienus vai ritekļu sastāvus no tehniskās apkopes parka uz pasažieru stacijas platformām vai uz stāvvietu, kas savienota ar pasažieru staciju;*
- *tas pārvieto vilcienus vai ritekļu sastāvus no rūpnīcas uz apmaiņas vietu (apmaiņas pievedceļu), kas savienots ar kravas staciju.*

Pievedceļu operators nav ne dzelzceļa pārvadājumu uzņēmums, ne infrastruktūras pārvaldītājs, tomēr par darbībām, ko veic infrastruktūras pārvaldītāja tīklā, jābūt piešķirtam vienotam drošības sertifikātam vai drošības atļaujai.

Uz dzelzceļa darbībām, ko veic pievedceļu operators dzelzceļa tīklā, par kuru atbild infrastruktūras pārvaldītājs, attiecas dzelzceļa pārvadājumu uzņēmuma vienotais drošības sertifikāts vai infrastruktūras pārvaldītāja drošības atļauja. Tas nozīmē, ka dzelzceļa pārvadājumu uzņēmumam vai infrastruktūras pārvaldītājam ir jākontrolē riski, kas ir saistīti ar pievedceļu operatora veiktajām darbībām, īstenojot to SMS paredzētos apakšuzņēmēju pārvaldības pasākumus.

Visos gadījumos dzelzceļa pārvadājumu uzņēmumiem un infrastruktūras pārvaldītājam ir precīzi jāapraksta visu savu dzelzceļa darbību tvērums, kā arī to darbību tvērums, kas mijiedarbojas ar citām dzelzceļa darbībām, lai VDI īstenotā SMS uzraudzība būtu efektīva. Dzelzceļa pārvadājumu uzņēmumu un infrastruktūras pārvaldītāju spēja precīzi un pilnīgi aprakstīt savas darbības, kā arī citas darbības, kas mijiedarbojas ar dzelzceļa darbībām, ir būtiska SMS efektivitātes un VDI īstenotās uzraudzības efektivitātes nodrošināšanai.

Visos iepriekš izklāstītajos apakšgadījumos līgumsaistībās ir skaidri jānorāda (uzskaitījums nav izsmeljošs):

- *kas ir jādara katram līgumslēdzējam;*
- *kāda ir gaidītā rezultātu/pakalpojumu kvalitāte;*
- *funkciju un pienākumu sadalījums;*
- *ar kādu informāciju apmainīsies līgumslēdzēji, kad un kā tas notiks. Informācija ietver ziņošanu par notikumiem, kā aprakstīts visos iepriekš izklāstītajos apakšgadījumos, un par pievedceļu infrastruktūras īpašajām iezīmēm, piemēram, ātruma ierobežojumiem, svara ierobežojumiem vai slīpuma apstākļiem;*
- *kompetences prasības;*
- *veselības un drošības prasības (izriet no riska novērtēšanas, valsts prasībām u. tml.).*

Līgumsaistības un partnerības

Dzelzceļa pārvadājumu uzņēmumam ir pienākums nodrošināt vilciena drošu pārvietošanos, koordinējot un pārvaldot vilciena darbības. Līgumsaistības (kas parasti sastāv no pamatnolīgumiem, īpašiem nolīgumiem un pielikumiem) ir pamats efektīvai sadarbībai starp dažādiem dzelzceļa pārvadājumu uzņēmumiem — vai tie ir jaunpienācēji vai seni uzņēmumi —, un tām jāatbilst Eiropas un valsts tiesību aktu noteikumiem un jebkurām citām piemērojamām prasībām.

Tāpēc dzelzceļa pārvadājumu uzņēmumam ir jākontrolē savu darbību riski, tostarp tie, kas izriet no sadarbības ar partneriem un apakšuzņēmēju vai darbuzņēmēju izmantošanas. Tad VDI uzrauga, vai dzelzceļa pārvadājumu uzņēmums pārrēdzami un rūpīgi izpilda savus juridiskos pienākumus.

Dzelzceļa pārvadājumu uzņēmumi savu ar drošību saistīto atbildību par vilcieniem drošas ekspluatācijas koordinēšanu un pārvaldību nedrīkst uzticēt ārpuslīguma sniedzējiem. Tomēr tas nekaitē dažādiem dzelzceļa pārvadājumu uzņēmumu sadarbības režīmiem. Iepriekš izklāstītie pamatprincipi attiecas arī uz sadarbību starp dzelzceļa pārvadājumu uzņēmumiem. Dzelzceļa pārvadājumu uzņēmumam, kas atbild par vilcieniem drošu ekspluatāciju, jābūt skaidri norādītam visos nolīgumos, kas noslēgti starp iesaistītajām pusēm, un tam jābūt piešķirtam vienotajam drošības sertifikātam. Minētais dzelzceļa pārvadājumu uzņēmums vai nu tieši pārvalda resursus (personālu, ritekļus) ar savas SMS starpniecību, vai arī tas var nolemt, ka resursu izmantošana (piemēram, ritekļu noma, vilciena vadītāju nolīgšana) tiks (pilnīgi vai daļēji) uzticēta citai personai. Pēdējā minētajā gadījumā dzelzceļa pārvadājumu uzņēmumam joprojām ir pienākums kontrolēt

riskus saistībā ar darbuzņēmēju vai apakšuzņēmēju izmantošanu, ar savas SMS starpniecību pārtraugot līgumu izpildi saskaņā ar [Regulu \(ES\) Nr. 1078/2012](#), un tāpēc tam ir jāpārbauda, vai šādi resursi atbilst tiesību aktu prasībām un citām piemērojamām drošības prasībām (piemēram, par ritekļiem ekspluatācijai drošā stāvoklī, maršrutu saderību, personāla apmācību, vilciena vadītājiem ar derīgu apliecību un sertifikātu konkrētam maršrutam).

Vienotais drošības sertifikāts, ko drošības sertifikācijas struktūra piešķirusi (un ko attiecīgi uzrauga VDI) līgumslēdzējam (t. i., partnerim vai apakšuzņēmējam), var sniegt par ekspluatācijas drošību atbildīgajam dzelzceļa pārvadājumu uzņēmumam pietiekamu pārliecību, ka SMS pasākumi atbilst attiecīgajām prasībām. Līgumsaistības ietver ar drošību saistītas informācijas (piemēram, par vilciena vadītāju iepriekšējo atpūtas laiku) nodošanu starp līgumslēdzējiem.

Dzelzceļa pārvadājumu uzņēmumu sadarbības pamatā esošie principi joprojām ir tādi paši neatkarīgi no sadarbības režīmiem, t. i., partnerības vai dzelzceļa darbību (pilnīgas vai daļējas) uzticēšanas apakšuzņēmējiem vietējā vai pārrobežu ekspluatācijā. Tomēr to pasākumu veids un apjoms, kuri jāīsteno dzelzceļa pārvadājumu uzņēmumiem, un VDI īstenotās šādu sadarbības režīmu uzraudzības apjoms ir samērīgi attiecībā pret dzelzceļa pārvadājumu uzņēmumu sadarbības pakāpi.

Piemēram, attiecībā uz pārrobežu sadarbību starp dzelzceļa pārvadājumu uzņēmumiem (t. i., ārēju ritekļu un/vai personāla izmantošanu) varētu būt nepieciešams lielāks skaits kontroles pasākumu nekā attiecībā uz jebkuru citu sadarbības režīmu, jo ekspluatācija tiek nodota citam dzelzceļa pārvadājumu uzņēmumam, kura izmantotās valodas un ritošā sastāva ekspluatācijas noteikumi dažādās dalībvalstīs var atšķirties. Turpretī tikai ārēju vilciena vadītāju vai ritekļu nolīgšanas gadījumā acīmredzot būtu vajadzīga mazāka pārraudzība un attiecīgi arī mazāk VDI īstenoju uzraudzības pasākumu.

4. pielikums. Drošības kultūra

Ievads drošības kultūrā un drošības kultūras uzlabošanas stratēģijā

Kultūra rodas cilvēku mijiedarbībā viņu ikdienas dzīvē, un tā palīdz noteikt gaidāmos sabiedrības uzvedības veidus un normas. Kultūra ir komplekss jēdziens, kas ietver vairākus faktorus un kas laika gaitā attīstās atkarībā no apstākļiem, vides, kā arī tautas, valsts, sabiedrības un/vai organizācijas pieredzes.

Drošības kultūra ir tie kultūras elementi, kas īpaši attiecas uz drošību. Lai gan ir iespējams raksturot dažus drošības kultūru veicinošos faktorus, ir neiespējami apkopot visu informāciju, kas “iemieso” drošības kultūru. Nav vienota zinātniska un objektīva drošības kultūras kritērija, jo veicinošie faktori atšķiras — ne tikai starp organizācijām, bet arī to iekšienē. Dažādās nodaļās ir dažādas drošības prasības un vajadzības, piemēram, ar ekspluatāciju saistītas un finansiālas, un no tām izriet dominējošā drošības kultūra. Ieguldījumu organizācijas drošības kultūrā sniedz arī ārēji faktori, piemēram, normatīvās prasības, izglītības līmeņi, sociālās struktūras, kā arī tautas kultūra.

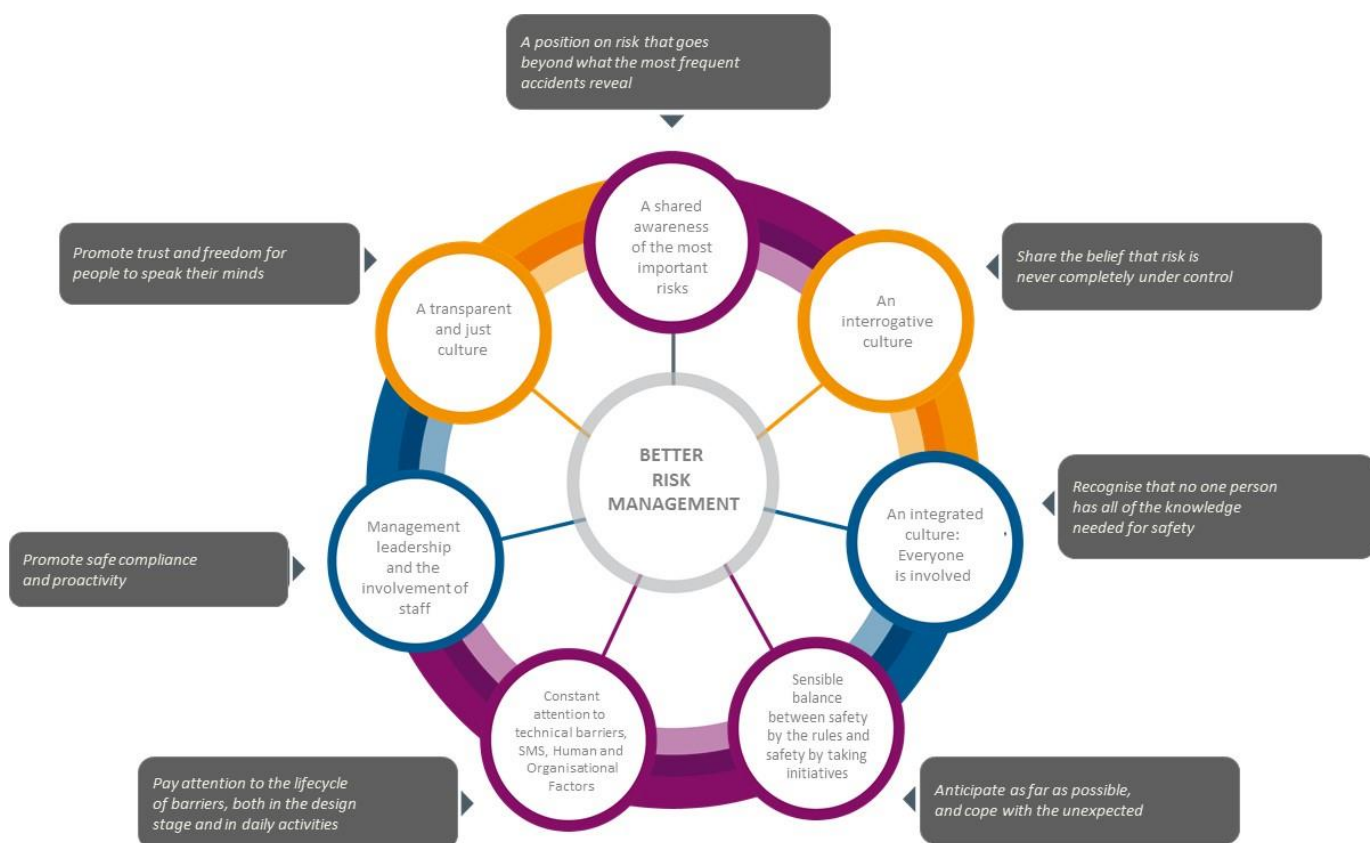
“Drošības kultūra” ir iesakņojies jēdziens, tomēr trūkst vienotas tā definīcijas. Definīcijas neesamības rezultātā teorētiskās diskusijas un praktiskie lietojumi ir nedaudz attālinājušies, un tas, kas būtībā ir sociāls koncepts, ir kļuvis par labas drošības kultūras iezīmi.

Vienkāršs veids, kā raksturot drošības kultūru, ir aplūkot faktorus, kas veicina uzvedību. SMS nodrošina pamatu, ar politikas un procedūru starpniecību definējot un nosakot, kas ir vajadzīgs. Utopiskā pasaulē SMS būtu nevainojama un to ievērotu visi vadības pārstāvji un darbinieki. Diemžēl utopija ir utopija, un realitātē vadība un darbinieki cenšas piešķirt SMS saturam jēgu, pamatojoties uz savām vērtībām, attieksmi un pārliecību, kuru pamatā ir viņu personiskā pieredze, apvienojumā ar darbavietas un sabiedrības uzvedības normām. Ja SMS piemīt jēga un ja pastāv tās ievērošanas kultūra, tam seko pareizā uzvedība. Ja ne, rodas individuālas interpretācijas un tiek piemēroti alternatīvi risinājumi. To pamatā ir individuāla riska novērtēšana, kurā izsver faktorus, kas ietekmē pieņemtos lēmumus. Riska novērtēšana ir ne vien vērsta uz faktisko risku, bet arī ietver faktorus saistībā ar izdevīgumu, pieķeršanas risku, vadības solījumiem un praktisko rīcību u. tml. Tādējādi drošības kultūru nosaka SMS, jēgas piešķiršanas un uzvedības savstarpējā atkarība.

Lai novērtētu drošības kultūru, ir jābūt priekšstatam par minētajiem trīs faktoriem un to savstarpējo atkarību. Kā minēts iepriekš, nav vienota zinātniska un objektīva drošības kultūras kritērija. Tomēr ir iespējams, ņemot vērā minētos trīs faktorus, analizēt iezīmes, kas ietekmē drošības kultūru.

Piemēram, pēc politikas paziņojuma, teiksim, “Drošība pirmajā vietā”, var sekot izpēte par to, ko tas nozīmē darbiniekiem — vai viņi tam faktiski tic, vai vadības darbi atbilst tās vārdiem, kā tiek pieņemti lēmumi un ar kādu pamatojumu, kā organizācija reaģē, kad uz to tiek izdarīts spiediens, u. tml. Līdzīgu izpēti var veikt par citiem faktoriem, piemēram, pastāvīgu mācīšanos un izzinošu attieksmi. Apvienojot analīzes rezultātus, tiks radīts priekšstats par pašreizējo kultūras stāvokli. Laika gaitā šāds priekšstats var kļūt vispusīgāks, ļaujot izdarīt pārliecinošākus secinājumus.

Lai saprastu drošības kultūru organizācijā, speciālisti un pētnieki ir izstrādājuši modeļus, kas parasti ietver pozitīvas drošības kultūras raksturīgo iezīmju kopumu. Turpmāk 4. attēls attēlā ir atspoguļots viena šāda modeļa paraugs, kura pamatā ir nesen veikts Rūpnieciskās drošības kultūras institūta (ICSI) darbs.



4. attēls. Drošības kultūras iezīmes

A position on risk that goes beyond what the most frequent accidents reveal	Nostāja attiecībā uz risku, kas pārsniedz to, ko atklāj visbiežākie negadījumi
Share the belief that risk is never completely under control	Vienots uzskats, ka risks nekad nav pilnīgi kontrolējams
Recognise that no one person has all of the knowledge needed for safety	Atzīst, ka nevienai personai nav visu vajadzīgo zināšanu par drošību
Anticipate as far as possible, and cope with unexpected	Ciktāl iespējams, paredz un pārvar negaidīto
Pay attention to the lifecycle of barriers, both in the design stage and in daily activities	Pievērš uzmanību šķēršļu dzīves ciklam — gan plānošanas posmā, gan ikdienas darbībās
Promote safe compliance and proactivity	Veicina drošu atbilstību un proaktivitāti
Promote trust and freedom for people to speak their minds	Veicina uzticēšanos un cilvēku brīvību izteikties
A shared awareness of the most important risks	Vienota izpratne par visbūtiskākajiem riskiem
An interrogative culture	Izzinoša kultūra
An integrated culture: Everyone is involved	Integrēta kultūra: ikviens ir iesaistīts
Constant attention to technical barriers: SMS, Human and Organisational Factors	Pastāvīga uzmanības pievēršana tehniskiem šķēršļiem, SMS, cilvēkfaktoriem un organizatoriskajiem faktoriem
Management leadership and the involvement of staff	Vadības līderība un darbinieku iesaistīšana
A transparent and just culture	Pārredzama un taisnīga kultūra

Pamatojoties uz ICSI modeli, var konstatēt korelāciju starp lielāko daļu SMS elementu un dominējošajiem drošības kultūras elementiem, kā norādīts 6. tabula. tabulā.

6. tabula: Saistība starp SMS prasībām un drošības kultūras iezīmēm

<i>SMS elementi</i>	<i>CSM SMS prasība</i>	<i>Drošības kultūras iezīmes</i>
Līderība un apņemšanās	2.1.	<ul style="list-style-type: none"> Izzinoša kultūra Pārredzama un taisnīga kultūra Vadības līderība un darbinieku iesaistīšana
Drošības politika	2.2.	Vadības līderība un darbinieku iesaistīšana
Struktūra un pienākumi	2.3.	Integrēta kultūra (ikviens ir iesaistīts)
Darbinieku un citu dalībnieku iesaistīšana	2.4.	<ul style="list-style-type: none"> Pārredzama un taisnīga kultūra Integrēta kultūra (ikviens ir iesaistīts) Vadības līderība un darbinieku iesaistīšana
Riska novērtējums	3.1.	<ul style="list-style-type: none"> Vienota izpratne par visbūtiskākajiem riskiem Pastāvīga uzmanība tehniskiem šķēršļiem, SMS, cilvēkfaktoriem un organizatoriskajiem faktoriem Saprātīgs līdzsvars starp drošību, ievērojot noteikumus, un drošību, uzņemoties iniciatīvas
Drošības mērķi un plānošana	3.2.	-
Resursi	4.1.	Integrēta kultūra (ikviens ir iesaistīts)
Kompetence	4.2.	<ul style="list-style-type: none"> Pārredzama un taisnīga kultūra Integrēta kultūra (ikviens ir iesaistīts)
Apzināšanās	4.3.	Vienota izpratne par visbūtiskākajiem riskiem
Informācija un saziņa	4.4.	Pārredzama un taisnīga kultūra
Dokumentēta informācija / SMS dokumentācija	4.5.	Pastāvīga uzmanība tehniskiem šķēršļiem, SMS, cilvēkfaktoriem un organizatoriskajiem faktoriem
Cilvēkfaktoru un organizatorisko faktoru integrēšana	4.6.	-
Ekspluatācijas pasākumi	5.1.	<ul style="list-style-type: none"> Vienota izpratne par visbūtiskākajiem riskiem Izzinoša kultūra Saprātīgs līdzsvars starp drošību, ievērojot noteikumus, un drošību, uzņemoties iniciatīvas
Aktīvu pārvaldība	5.2.	Vienota izpratne par visbūtiskākajiem riskiem
Darbuzņēmēji, partneri un piegādātāji	5.3.	<ul style="list-style-type: none"> Pārredzama un taisnīga kultūra Integrēta kultūra (ikviens ir iesaistīts)
Izmaiņu pārvaldība	5.4.	-
Ārkārtas situāciju pārvaldība	5.5.	Saprātīgs līdzsvars starp drošību, ievērojot noteikumus, un drošību, uzņemoties iniciatīvas
Uzraudzība	6.1.	Izzinoša kultūra
Iekšējā revīzija	6.2.	-
Vadības veikta pārskatīšana	6.3.	-

SMS elementi	CSM SMS prasība	Drošības kultūras iezīmes
Uzlabojumi/mācības no negadījumiem un starpgadījumiem	7.1.	<ul style="list-style-type: none"> Izzinoša kultūra Pārredzama un taisnīga kultūra
Pastāvīgi uzlabojumi	7.2.	<ul style="list-style-type: none"> Izzinoša kultūra Pārredzama un taisnīga kultūra

Sīkāka informācija par ICSI modeli ir atrodama ICSI tīmekļa vietnē (<http://www.icsi.eu.org>).

Piemērs, kā tiek īstenota stratēģija dzelzceļa drošības kultūras uzlabošanai lielā uzņēmumā — programma “PRISME”, ko īsteno uzņēmumā SNCF (Francija)

Pēc vairākiem nopietniem dzelzceļa satiksmes negadījumiem un vairākkārtējiem negadījumiem darba vietā SNCF 2014. gadā veica izpilddirektora sponsorētu plašu aptauju, lai noskaidrotu darbinieku priekšstatu par drošību.

“Aptaujas anketa tika izstrādāta pēc apspriešanās ar 20 mērķa grupām laikposmā no 2014. gada aprīļa līdz maijam. Tika aptvertas visas darbības un visi hierarhijas līmeņi. Lai garantētu aptaujas konfidencialitāti, aptaujas darbu veica neatkarīgs institūts. Aptauja tika īstenota atbilstoši standartam ISO 20252 un bija balstīta uz CAWI (“datorizēta aptauja tīmeklī”), un tā bija pieejama personālajos datoros, viedtālruņos un planšētdatoros.”

“Mērķa grupas sniedza ļoti vērtīgu informāciju. Konkrētāk, pateicoties mērķa grupām, tika konstatēta vajadzība vienkāršot dokumentāciju.”

Šī iniciatīva izrādījās veiksmīga, jo uz anketas jautājumiem atbildēja vairāk nekā 53 000 darbinieku no aptuveni 150 000 darbinieku.

Atbildes liecināja par diezgan lielu vienprātību, jo īpaši uzsverot vajadzību sekmēt dialogu un veicināt visu darbinieku ziņošanu. Tika konstatēts, ka nepieciešams priekšnosacījums drošības pastāvīgai uzlabošanai ir fundamentālas kultūras izmaiņas, kas atbalsta proaktīvu attieksmi visos uzņēmuma līmeņos, nevis reaktīva pieeja individuāliem notikumiem.

Augstākā līmeņa vadība attiecīgi apņēmas īstenot **uzņēmuma vispārēju drošības politiku**, kuras mērķis ir sasniegt izcilu drošības līmeni un kurā ir noteikts, ka drošība ir galvenā prioritāte uzņēmuma vērtību sarakstā un ir nepieciešama, lai sasniegtu izcilus darbības rādītājus.

Pamatojoties uz aptauju un papildu salīdzinošo novērtēšanu, valdes līmenī izveidota darba grupa izstrādāja vērīenīgu rīcības plānu ar nosaukumu “PRISME”, ko veido seši elementi. Aptauja, kas tika veikta 2015. gada novembrī, parādīja, ka 93 % darbinieku minētos elementus uzskata par “svarīgiem” un “ļoti svarīgiem”.

Tie ir šādi:

- attīstīt proaktīvu (**“Proactive”**) rīcību — mācīties no kļūdām un problēmām;
- izveidot uz riska (**“Risk”**) analīzi balstītu sistēmu — paredzēt un apzināt darbības un noteikt to prioritātes;
- kontrolēt saskarnes (**“Interfaces”**) — vērsties pret sadrumstalotību un labāk sadarboties;
- vienkāršot (**“Simplify”**) procesus, dokumentāciju un darbības veidus — pielāgot tos darba realitātei, lai palielinātu efektivitāti;
- radīt labvēlīgu organizatorisko (**“Managerial”**) vidi, lai ikviens ir personīgi iesaistīts — samazināt negadījumu risku līdz iespējami zēmam līmenim;
- apgūt rīkus un ieviest inovācijas (**“Equipment”**) — nodrošināt ikvienam mūsdienīgas darba metodes, drošu vidi un drošu tīklu.

Plānā **“PRISME”** ir paredzētas šādas konkrētas darbības:

- vienu dienu ilga apmācība 8000 vadītāju par cilvēkfaktoriem un organizatoriskajiem faktoriem;
- taisnīgas un godīgas kultūras attīstīšana un veicināšana;
- saziņas un informācijas izplatīšanas rīku uzlabošana (**“2 mois Sécurité”** (**“divu mēnešu drošība”**), rādītāji, drošības akcijas);
- drošības pārvaldības sistēmas un drošības noteikumu pārskatīšana;
- riska analīzes uzlabošana, lai labāk ņemtu vērā sistēmiskus aspektus.

Lai gan šīs programmas efektivitāte vēl tiek novērtēta, jau ir apzināti vairāki tās sniegtie ieguvumi:

- ir uzlabojusies starpgadījumu izmeklēšanas kvalitāte, ņemot vērā organizatoriskos faktorus;
- ir uzlabojusies darbinieku tūlītēja ziņošana par gandrīz notikušiem negadījumiem un problēmām;
- ir uzlabojusies saziņa.

Pēc darbinieku ieskatiem, vadības rīcība ir kļuvusi atbalstošāka un proaktīvāka.

5. pielikums. Cilvēkfaktori un organizatoriskie faktori

Cilvēkfaktori un organizatoriskie faktori — ievads

Cilvēkfaktori un organizatoriskie faktori (COF) ir daudzdisciplīnu joma, kas vērsta uz to, kā palielināt drošību, uzlabot veiktspēju un palielināt lietotāju apmierinātību. COF ir uz lietotāju orientēta pieeja, proti, tās izstrādes pamatā ir skaidra izpratne par lietotājiem, uzdevumiem un vidi. Sākumpunkts vienmēr ir lietotāja spējas, ierobežojumi un tas, kā tie tiek ietekmēti un kā tie mijiedarbojas ar sistēmām, ko izmanto uzdevuma veikšanā. Mērķis ir noteikt, kā vislabāk veikt uzdevumu drošā un efektīvā veidā. Uzsvars tiek likts uz izmantojamību. COF izmanto gan, lai proaktīvi nodrošinātu labus izstrādes procesus, gan lai ātri identificētu galvenās problēmas, kad kaut kas nav izdevies.

Piemēram, projektējot jaunus riteņus, nepietiek tikai ar projektēšanas standartu piemērošanu. Procesā ir jāiesaista vilcienu vadītāji, pavadoni un tehniskās apkopes personāls, lai izmantotu viņu pieredzi un izpratni par to, kā uzdevumus veikt droši un efektīvi. Piemēram, process var būt saistīts ar konkrētas stacijas vai līnijas jautājumiem, tehniskās apkopes darbinieku pieejamību un piekļuves iespējām, uzdevumu prioritātēm kabīnē, saziņas prasībām vai pasažieru uzvedību stacijās.

Dažādu operatoru zināšanas un pieredzi var vislabāk iekļaut iteratīvā procesā, kurā lietotājs, projektēšanai un izstrādei attīstoties, pastāvīgi izvērtē vilciena projektu un izstrādi. Tas palīdz novērst izplatītu kļūdu izstrādes procesā, proti, koncentrēšanos uz cilvēka mijiedarbību ar individuālām sistēmām, nevis uz uzdevumu izpildi kopumā. Piemēram, dažādiem piegādātājiem ir atšķirīgs priekšstats par to, kādām ir jābūt trauksmju prioritātēm, un, ja nav visaptveroša redzējuma, galu galā lietotājs bieži vien tiek pārslogots ar informāciju, kas ir tikai daļēji būtiska uzdevuma veikšanai, un tas tiek darīts tikai tāpēc vien, ka tehniskais projekts sniedz iespēju parādīt informāciju, bet lietotājam tā, iespējams, nebūs vajadzīga. COF analīze palīdz atšķirt vajadzību zināt no tā, ko var būt noderīgi zināt.

COF ietver sistēmiskas perspektīvas izmantošanu, proti, ne tikai aplūko cilvēkfaktorus, tehnoloģiskos un organizatoriskos faktorus kā tādus, bet arī uzsver dažādo faktoru mijiedarbību. Piemēram, ja vilciena vadītājs ir bijis iesaistīts starpgadījumā sakarā ar garāmbraukšanu aizliedzošajam signālam, faktori, ko ir ieteicams izpētīt (uzskaitījums nav izsmelošs), ir saistīti ar nogurumu, kognitīvo pārslodzi, kompetenci u. tml. (cilvēkfaktori), tehnoloģijas ietekmi uz veiktspēju, piemēram, cilvēka–sistēmas saskarnes, iekārtojumu, signālu izvietojumu (tehnoloģiskie faktori), organizācijas ietekmi uz veiktspēju, piemēram, apmācību, SMS, organizatoriskajām prioritātēm (organizatoriskie faktori), kā arī mijiedarbību starp šīm trīs jomām, piemēram, iepirkuma ietekmi uz projektu vai izmaiņu pārvaldību, ieviešot jaunu projektu.

Metodes tiek pārņemtas no daudzām un dažādām jomām, piemēram, eksperimentālās psiholoģijas, rūpnieciskās tehnoloģijas, organizatoriskās psiholoģijas, socioloģijas, vadības zinātnes, kognitīvās inženierzinātnes, ergonomikas, datorzinātnes un drošības inženierzinātnes. Tā kā COF uzsvars tiek likts uz lietotāju, bieži izmantota metode ir uzdevumu analīze. Uzdevumu analīze sniedz projektētājam izpratni par veicamajiem uzdevumiem un par to, kā tie ir saistīti ar sistēmām, ar kurām mijiedarbojas lietotājs, un par organizatoriskajiem apstākļiem, kas ietekmē veiktspēju. Pamatojoties uz uzdevumu analīzi, var veikt turpmāku analīzi, piemēram, cilvēka–sistēmas mijiedarbības, darba slodzes, cilvēku uzticamības/riska, antropometrijas un biometrijas analīzi. Galvenais ir nodrošināt, ka lietotājam ir vislabākie sasniedzamie darba apstākļi, lai tas varētu droši un efektīvi darboties.

Plašāka informācija par cilvēkfaktoriem un organizatoriskajiem faktoriem ir atrodama turpmāk norādītajos avotos.

- Salvendy, G. (2012). *Handbook of Human Factors and Ergonomics*. New Jersey: Wiley & Sons. ISBN-13: 978-0470528389
- Wickens, C.D., Lee, J.D., Liu, Y & Gordon Becker, S.E (2004. gads). *An Introduction to Human Factors Engineering*. New Jersey: Pearson Education. ISBN-13: 978-0131837362

Stratēģija, lai atbalstītu cilvēkfaktoru un organizatorisko faktoru integrēšanu drošības pārvaldības sistēmā

Organizācijai ir jāizstrādā stratēģija, lai nodrošinātu, ka organizācijā visos attiecīgajos procesos tiek sistemātiski un konsekventi piemērotas zināšanas par cilvēkfaktoriem, metodes un uz cilvēku vērsta pieeja. Šāda pieeja nozīmē, ka vispirms tiek ņemtas vērā cilvēku vajadzības, spējas un uzvedība un tad notiek projektēšana, ko pielāgo minētajām vajadzībām, spējām un uzvedībai.

Cilvēkfaktoru un organizatorisko faktoru (COF) stratēģija var ietvert elementus, kas saistīti ar turpmāk norādīto.

Līderība

- *Līderība un apņemšanās:*
 - vadības apņemšanās ievērot COF ir skaidri noteikta politikā un mērķos;
 - pastāv process/pamatnostādnes, kas nosaka, kā COF ir jāpiemēro projektos;
 - COF ir projektēšanas procesā un projekta pārvaldībā integrēta daļa.
- *Drošības politika:*
 - drošības politikā ir skaidri noteikts, ka visos ar drošību saistītajos procesos ir jāpiemēro COF aspekts.
- *Organizatoriskās funkcijas, pienākumi, pārskatatbildība un pilnvaras:*
 - ir skaidri noteiktas COF speciālista funkcijas, pienākumi un pārskatatbildība;
 - pastāv process, kas nosaka, kā COF speciālisti regulāri piedalās projektos un procesos.

Plānošana

- *Rīcība riska novēršanai:*
 - apraksts, kā COF aspekts tiek ņemts vērā riska analīzēs;
 - COF speciālistu iesaistīšana riska analīzēs.

Atbalsts

- *Resursi un kompetence:*
 - sistemātiska pieeja, lai nodrošinātu COF kompetenci attiecīgu funkciju veikšanai, pamatojoties uz vajadzību analīzi;
 - ir atvēlēts laiks un resursi COF prasību izpildes nodrošināšanai.
- *Apzināšanās*
 - organizācijā ir vispārējas zināšanas par sistemātisko pieeju, lai nodrošinātu COF kompetenci attiecīgu funkciju veikšanai.

Ekspluatācija

- *Ekspluatācijas plānošana un kontrole:*
 - COF ņem vērā ekspluatācijas plānošanā.
- *Aktīvu pārvaldība*
 - organizācijai ir pamatnostādnes par to, kā piemērot uz cilvēku vērstu pieeju katrā dzīves cikla posmā.
- *Izmaiņu pārvaldība*
 - COF vienmēr novērtē kā izmaiņu pārvaldības procesa daļu.

Veiktspējas izvērtēšana

- *Uzraudzība*
 - sistemātiski novērtē drošības rādītājus, ņemot vērā COF stratēģiju.

Uzlabojumi

- *No negadījumiem un starpgadījumiem gūtā mācība:*

- *COF zināšanas un metodes tiek izmantotas negadījumu izmeklēšanas procesā;*
 - *ir ieviesta metodika izmeklēšanas veikšanai, pamatojoties uz COF zināšanām un metodēm;*
 - *ir mācību programma, kas paredzēta negadījumu un starpgadījumu izmeklētājiem, piemērojot COF aspektu.*
- *Pastāvīgi uzlabojumi*
 - *process organizācijas COF pārvaldības procesu pastāvīgai uzlabošanai.*

6. pielikums. Definīcijas

Tādu vārdu kā “vajadzētu”, “ir jābūt” u. tml. vēlējuma un vajadzības izteiksmes līdzekļu lietošana šajā dokumentā norāda uz pastāvošu juridisku prasību, kas ir jāizpilda.

Negadījums	Nevēlams vai neparedzēts pēkšņs notikums vai īpaša šādu notikumu virkne ar negatīvām sekām; negadījumus iedala šādi: sadursmes, nobraukšana no sliekšņa, negadījumi uz pārbrauktuvē, negadījumi ar cilvēkiem, kuros iesaistīts kustībā esošs ritošais sastāvs, ugunsgrēki un citi (Direktīva (ES) Nr. 2016/798).
Darbības telpa	Tīkls vai tīkli vienā vai vairākās dalībvalstīs, kur dzelzceļa pārvadājumu uzņēmums plāno veikt savu darbību (Direktīva (ES) Nr. 2016/798).
Aktīvu pārvaldība	Pieeja, ko izmanto organizācija, lai nodrošinātu fizisko aktīvu drošību, atbilstību paredzētajam mērķim un komerciālo dzīvotspēju no projektēšanas un būvniecības visā aktīva dzīves ciklā līdz ekspluatācijas pārtraukšanai.
Revīzija	Sistemātisks, neatkarīgs un dokumentēts process, ko izmanto revīzijas pierādījumu iegūšanai un to objektīvai izvērtēšanai, lai noteiktu, cik tāl ir izpildīti revīzijas kritēriji (ISO 9000).
Darbības iezīmes	Darbības raksturojums, ņemot vērā tās tvērumu, ietverot infrastruktūras projektēšanu un būvniecību, infrastruktūras tehnisko apkopi, satiksmes plānošanu, satiksmes pārvaldību un vadību un ņemot vērā dzelzceļa infrastruktūras izmantojumu, ietverot parastās un/vai ātrgaitas dzelzceļa līnijas, pasažieru un/vai kravu pārvadājumus.
Kompetence	Spēja piemērot zināšanas un prasmes, lai sasniegtu iecerētos rezultātus (ISO 9000).
Pastāvīgi uzlabojumi	Atkārtota darbība, ko veic, lai uzlabotu veiktspēju (t. i., izmērāms rezultāts) (ISO 9000).
Dokumentu pārvaldība	Dokumentētas informācijas identifikācijas, radīšanas, uzturēšanas, pārvaldības, uzglabāšanas un saglabāšanas process (vai procedūra).
Darbības apjoms	<p>Attiecībā uz dzelzceļa darbībām, ko veic dzelzceļa pārvadājumu uzņēmumi, — apjoms, ko raksturo pasažieru skaits un/vai kravu apjoms un dzelzceļa pārvadājumu uzņēmuma noteiktais lielums pēc to darbinieku skaita, kuri strādā dzelzceļa nozarē (t. i., mikrouzņēmums, mazs uzņēmums, vidējs uzņēmums vai liels uzņēmums) (Direktīva (ES) Nr. 2016/798).</p> <p>Attiecībā uz infrastruktūras pārvaldītāju veiktajām dzelzceļa darbībām tas ir apjoms, ko raksturo dzelzceļa sliežu ceļa garums un aplēstais infrastruktūras pārvaldītāja lielums, ko izsaka kā dzelzceļa nozarē strādājošo darba ņēmēju skaitu (Regula (ES) 2018/[...] [CSM attiecībā uz SMS]).</p>
Apdraudējums	Apstākļi, kas var izraisīt avāriju (Regula (ES) Nr. 402/2013).
Cilvēkfaktori un organizatoriskie faktori	Visas cilvēku veikspējas iezīmes un organizatoriskie aspekti, kas jāņem vērā, lai nodrošinātu sistēmas vai organizācijas drošību un efektivitāti visā tās darbības garumā.
Uz cilvēku vērsta pieeja	Pieeja, saskaņā ar kuru vispirms tiek ņemtas vērā cilvēku vajadzības, spējas un uzvedība un tad notiek projektēšana, ko pielāgo minētajām vajadzībām, spējām un uzvedībai.

Starpgadījums	Jebkāds notikums, kas nav negadījums vai smags negadījums un kam ir vai var būt ietekme uz dzelzceļa pārvadājumu drošību (Direktīva (ES) 2016/798). Starpgadījumi ietver gandrīz notikušus negadījumus.
Infrastrukturā pārvaldītājs	Jebkura iestāde vai uzņēmums, kas konkrēti atbild īpaši par dzelzceļa infrastruktūras izveidi, pārvaldību un uzturēšanu, tostarp par satiksmes pārvaldību un kustības vadības un signalizācijas sistēmu; infrastruktūras pārvaldītāja funkcijas visā tīklā vai tīkla daļā var uzticēt veikt dažādām iestādēm vai uzņēmumiem (Direktīva 2012/34/ES).
Ieinteresētā persona	Persona vai organizācija, kas var ietekmēt kādu lēmumu vai darbību, ko var ietekmēt kāds lēmums vai darbība vai kas var uzskatīt, ka to ietekmējis kāds lēmums vai darbība (ISO 9000) saistībā ar drošības pārvaldības sistēmu.
Izmeklēšana	Process, ko veic negadījumu un starpgadījumu novēršanai, un tajā ietilpst informācijas vākšana un analīze, secinājumu izdarīšana, ieskaitot cēloņu noteikšanu, un vajadzības gadījumos arī drošības ieteikumu izstrādāšana (Direktīva (ES) 2016/798).
Pārvaldības sistēma	Savstarpēji saistītu vai mijiedarbojošos organizācijas elementu kopums, ko izmanto, lai noteiktu politikas virzienus un mērķus, un šo mērķu sasniegšanas procesi (ISO 9000).
Uzraudzība	Dzelzceļa pārvadājumu uzņēmumu, infrastruktūras pārvaldītāju vai par tehnisko apkopi atbildīgo struktūrvienību pasākumi, ko veic, lai pārbaudītu, vai pārvaldības sistēmas tiek pareizi piemērotas un ir efektīvas (Regula (ES) Nr. 1078/2012).
Valsts noteikums	Visi saistošie noteikumi, kas pieņemti kādā dalībvalstī, neatkarīgi no struktūras, kura tos izdevusi, un kas ietver dzelzceļa drošības vai tehniskās prasības, kuras nav ar Savienības vai starptautiskajiem noteikumiem paredzētās dzelzceļa drošības vai tehniskās prasības, un kas minētajā dalībvalstī ir piemērojami dzelzceļa pārvadājumu uzņēmumiem, infrastruktūras pārvaldītājiem vai trešām personām (Direktīva (ES) 2016/798).
Process	Savstarpēji saistītu un mijiedarbīgu pasākumu kopa, kas sākotnējos datus pārvērš rezultātā (ISO 9000).
Dzelzceļa infrastruktūra	Nodrošinājums, kas vajadzīgs, lai ir iespējama dzelzceļa ekspluatācija, tostarp: <ul style="list-style-type: none"> • sliežu ceļi un saistītās sliežu ceļu konstrukcijas; • tehniskās apkopes ceļi, signalizācijas sistēmas, sakaru sistēmas, ritošais sastāvs; • vadības sistēmas, vilcienu vadības sistēmas un datu pārvaldības sistēmas; • paziņojumi un zīmes; • elektroenerģijas padeves un elektriskās vilces sistēmas; • saistītās ēkas, darbnīcas, depo un parki un • iekārtas, mašīnas un aprīkojums.

Dzelzceļa pārvadājumu uzņēmums	<p>Dzelzceļa pārvadājumu uzņēmums, kā definēts Direktīvas 2012/34/ES 3. panta 1. punktā, vai cits valsts vai privāts uzņēmums, kas nodarbojas ar kravu un/vai pasažieru dzelzceļa pārvadājumiem, ar nosacījumu, ka šim uzņēmumam ir jānodrošina vilce, tostarp uzņēmumi, kas nodrošina tikai vilci (Direktīva (ES) 2016/798).</p> <p>Jebkurš publisks vai privāts uzņēmums, kam ir piešķirta licence saskaņā ar šo direktīvu un kura galvenais saimnieciskās darbības veids ir pakalpojumu sniegšana attiecībā uz kravas un/vai pasažieru pārvadāšanu pa dzelzceļu ar noteikumu, ka uzņēmums nodrošina vilci; šī definīcija ietver arī uzņēmumus, kas nodrošina tikai vilci (Direktīva 2012/34/ES).</p>
Risks	Tādu (apdraudējuma izraisītu) avāriju un starpgadījumu iespējamības biežums, kas rada kaitējumu, un šāda kaitējuma izraisīto seku nopietnība (Regula (ES) Nr. 402/2013).
Riska analīze	Visas pieejamās informācijas sistemātiska izmantošana, lai noteiktu apdraudējumus un aplēstu risku (Regula (ES) Nr. 402/2013).
Riska novērtējums	Vispārējais process, kas ietver gan riska analīzi, gan riska noteikšanu (Regula (ES) Nr. 402/2013).
Riska noteikšana	Uz riska analīzi balstīta procedūra nolūkā noteikt, vai ir sasniegts pieļaujams riska līmenis (Regula (ES) Nr. 402/2013).
Riska pārvaldība	Sistemātiska pārvaldības politikas, procedūru un prakses piemērošana riska analīzē, noteikšanā un kontrolē (Regula (ES) Nr. 402/2013).
Drošības kultūra	Mijiedarbība starp drošības pārvaldības sistēmas prasībām, to, kā cilvēki, pamatojoties uz savu attieksmi, vērtībām un pārliecību, tās saprot, un viņu faktisko rīcību, par ko liecina lēmumi un uzvedība. Pozitīvu drošības kultūru raksturo vadītāju un indivīdu kopīga apņemšanās vienmēr rīkoties droši, it īpaši, ja ir jāsasniedz konkurējoši mērķi (Regula (ES) 2018/[..] [CSM attiecībā uz SMS]).
Mērķis	<p>Sasniedzamais rezultāts.</p> <p>Drošības mērķim jābūt konkrētam, izmērāmam, sasniedzamam, reālistiskam un ar noteiktu termiņu. Tam arī jābūt noteiktam attiecīgo funkciju līmeņos organizācijā.</p>
Partneris	Komerctruktūra, ar kuru kādai citai komercstruktūrai ir noslēgta jebkāda veida savienība. Šādas attiecības var būt līgumiska, ekskluzīva vienošanās, kurā abas struktūras apņemas nesadarboties ar trešām personām.
Partnerība	Pasākums, kurā puses, kas zināmas kā partneri, vienojas sadarboties savu abpusējo interešu veicināšanai.
Drošības pārvaldības sistēma	Struktūra, pasākumi un procedūras, ko infrastruktūras pārvaldītājs vai dzelzceļa pārvadājumu uzņēmums noteicis, lai garantētu savu darbību drošu pārvaldību (Direktīva (ES) 2016/798).
Augstākā līmeņa vadība	Persona vai personu grupa, kas vada un kontrolē organizāciju visaugstākajā līmenī (ISO 9000).
Darbības veids	Veids, ko raksturo pasažieru pārvadājumi, ietverot vai neietverot ātrgaitas dzelzceļa pārvadājumus, kravu pārvadājumi, ietverot vai neietverot bīstamo kravu pārvadājumus, un tikai manevru pakalpojumi (Direktīva (ES) 2016/798).

