

Vejledning

Krav til sikkerhedsledelsessystemer, hvad angår sikkerhedscertificering eller sikkerhedsgodkendelse

	<i>Udarbejdet af</i>	<i>Valideret af</i>	<i>Godkendt af</i>
<i>Navn</i>	S. D'ALBERTANSON	M. SCHITTEKATTE	C. CARR
<i>Position</i>	Projektmedarbejder	Projektleder	Kontorchef
<i>Dato</i>	04-09-2018	04-09-2018	04-09-2018
<i>Underskrift</i>			

Dokumenthistorik

<i>Version</i>	<i>Dato</i>	<i>Bemærkninger</i>
1.0	29.6.2018	Endelig version til offentliggørelse
1.1	10.7.2018	Figur 2 opdateret, tekst tilføjet til figur 3.
1.2	4.9.2018	Figur 2 opdateret

Dette dokument er en ikke juridisk bindende vejledning fra Den Europæiske Unions Jernbaneagentur. Det er med forbehold af de beslutningsprocesser, der er fastsat i den gældende EU-lovgivning. Endvidere henhører en bindende fortolkning af EU-retten under EU-Domstolens enekompetence.

0 Indledning

En ansøger om et EU-sikkerhedscertifikat eller en sikkerhedsgodkendelse skal påvise overholdelsen af de relevante krav til sikkerhedsledelsessystemer, som er fastlagt i Kommissionens delegerede forordning (EU) 2018/762. Til dette formål skal ansøgeren fremlægge dokumentation til den nationale sikkerhedsmyndighed eller, hvis relevant, Den Europæiske Unions Jernbaneagentur (herefter kaldet "agenturet") for, at ansøgeren har etableret sit sikkerhedsledelsessystem (SMS) i henhold til artikel 9 i direktiv (EU) 2016/798.

Dette vejledende dokument er et levende dokument, som er udarbejdet i samarbejde med de nationale sikkerhedsmyndigheder og sektorrepræsentanter, og som er beregnet på konstant at blive forbedret på baggrund af brugernes feedback og under hensyntagen til de erfaringer, der opnås under gennemførelsen af direktiv (EU) 2016/798, relaterede fælles sikkerhedsmetoder (CSM'er) og eventuelle andre relevante EU-forordninger.

0.1 Formålet med vejledningen

Dette vejledende dokument tager sigte på at medtage:

- *formålet med de enkelte vurderingskrav, der er indeholdt i bilag I og II til ovenstående fælles sikkerhedsmetoder, om nødvendigt suppleret med forklarende noter, som indeholder specifikke oplysninger om bestemte termer eller begreber, der anvendes i kravene*
- *en angivelse af, hvilken dokumentation en organisation kan fremlægge for at påvise den overensstemmelse, som ovenstående fælles sikkerhedsmetoder kræver*
- *en illustrativ liste over eksempler på dokumentation, der kan observeres i ansøgninger om et EU-sikkerhedscertifikat eller en sikkerhedsgodkendelse, når der foretages en vurdering, eller som ansøgeren kan anvende som referencemateriale til sin ansøgning*
- *illustrative referencer og standarder, der kan anvendes som hjælp ved vurderingen, udviklingen, gennemførelsen eller den løbende forbedring af et sikkerhedsledelsessystem, og*
- *en angivelse af, hvilke punkter en national sikkerhedsmyndighed evt. skal overveje i forbindelse med tilsynet med en jernbanevirksomhed eller infrastrukturforvalter.*

Bemærk, at med henblik på vurderingen af en ansøgning om et EU-sikkerhedscertifikat, der involverer jernbanetransport af farligt gods, kan en national sikkerhedsmyndighed have en direkte rolle som den kompetente myndighed i at vurdere de relevante dele af ansøgningen. Alternativt kan den have en koordinerende rolle og efter behov samarbejde og rådføre sig med andre myndigheder med kompetence inden for transport af farligt gods om de relevante dele af vurderingen.

0.2 Hvem henvender denne vejledning sig til?

Det foreliggende dokument er rettet mod:

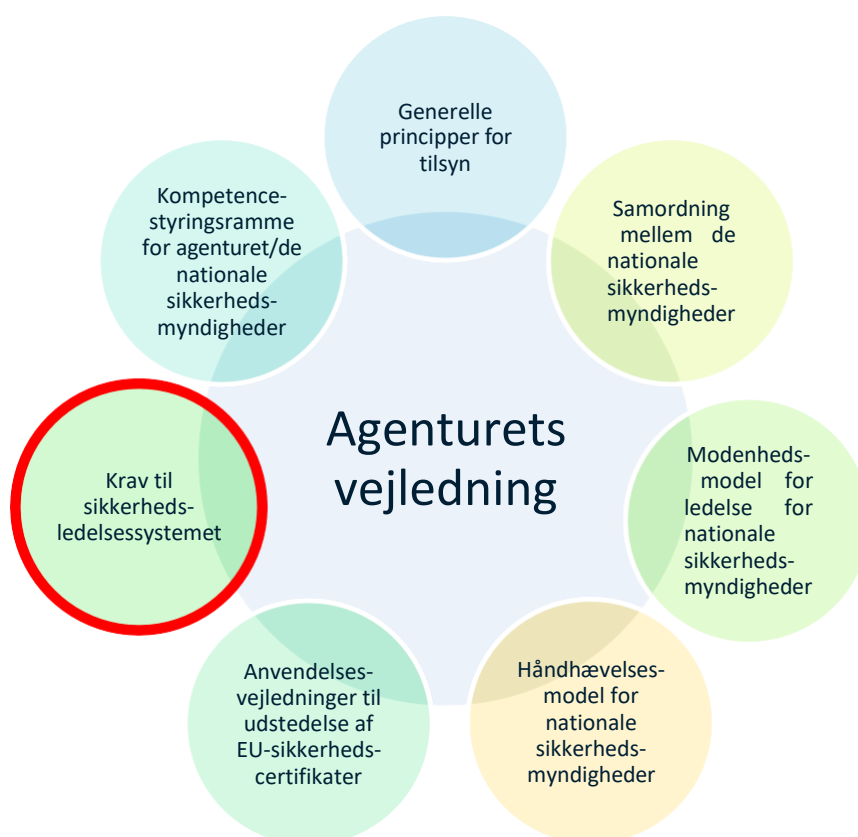
- *de nationale sikkerhedsmyndigheder og Den Europæiske Unions Jernbaneagentur, når de vurderer overensstemmelsen af jernbanevirksomhedernes sikkerhedsledelsessystem med de relevante krav til sikkerhedsledelsessystemer, og når de nationale sikkerhedsmyndigheder udfører tilsyn*
- *de nationale sikkerhedsmyndigheder, når de vurderer overensstemmelsen af infrastrukturforvalternes sikkerhedsledelsessystem med de relevante krav til sikkerhedsledelsessystemer, og når de udfører tilsyn efter tildelingen, og*
- *jernbanevirksomhederne og infrastrukturforvalterne (herefter også kaldet "ansøgerne") for at hjælpe dem med at udvikle, gennemføre, vedligeholde og løbende forbedre deres sikkerhedsledelsessystem i overensstemmelse med de relevante krav til sikkerhedsledelsessystemer (og andre gældende sikkerhedskrav) og for at informere dem om, hvad de kan forvente ved tilsynet.*

0.3 Anvendelsesområde

Noget, som denne vejledning ikke gør, er at foreskrive, hvilken dokumentation en ansøger bør fremlægge. Den grundlæggende årsag til dette er, at hver enkelt organisations sikkerhedsledelsessystem bør være skræddersyet til de specifikke risici, som organisationen skal styre. Hvert sikkerhedsledelsessystem er således et unikt system med dokumenterede oplysninger, der angiver de specifikke risikokontrolforanstaltninger og -systemer, som er indført i den enkelte organisation. Systemet udvikler sig over tid, i takt med at organisationen ændres. Derfor ville det være forkert at give en konkret liste over oplysninger, som en ansøger skal fremlægge. Hvis man gjorde dette, ville vurderingsprocessen være formålsløs, eftersom alle ansøgninger ville se ens ud, selv om de tilsvarende sikkerhedsledelsessystemer ikke gør det.

0.4 Vejledningens struktur

Dette dokument er en del af agenturets samling af vejledninger, som støtter jernbanevirksomheder, infrastrukturforvaltere, nationale sikkerhedsmyndigheder og agenturet i at opfylde deres roller og udføre deres opgaver i overensstemmelse med direktiv (EU) 2016/798.



Figur 1: Alle agenturets vejledninger

Oplysningerne i denne vejledning skal suppleres af specifikke vejledninger fra de nationale sikkerhedsmyndigheder, som beskriver og forklarer de meddelte nationale forskrifter, der er gældende for det relevante driftsområde, og de dokumenter, som skal indsendes ved ansøgningen om et EU-sikkerhedscertifikat i henhold til bestemmelserne i artikel 10, stk. 3, litra b), og artikel 10, stk. 8, i direktiv (EU) 2016/798 (jf. også agenturets ansøgningsvejledning om udstedelse af EU-sikkerhedscertifikater). For

infrastrukturforvaltere bør denne vejledning suppleres af vejledning fra nationale sikkerhedsmyndigheder om kravene til sikkerhedsgodkendelser som foreskrevet i artikel 12, stk. 1, i direktiv (EU) 2016/798.

Ved meddelte nationale forskrifter forstås der udelukkende de forskrifter, som en medlemsstat har meddelt til Kommissionen. I overensstemmelse med betragtning 12 i direktiv (EU) 2016/798 forventes det, at antallet af meddelte nationale forskrifter vil blive mindre med tiden. De vil enten blive erstattet af bestemmelser, som er fastlagt i tekniske specifikationer for interoperabilitet (TSI'er), andre EU-forordninger eller virksomhedsregler. Virksomhedsregler eller -standards vil blive vurderet som passende, hvis de er i overensstemmelse med TSI'en for delsystemet drift og trafikstyring i Den Europæiske Unions jernbanenet (herefter også kaldet TSI OPE), som afspejlet gennem de krav til sikkerhedsledelsessystemer, der er beskrevet i denne vejledning.

Denne vejledning er opbygget i henhold til kravene i bilag I og bilag II til Kommissionens delegerede forordning (EU) 2018/762. I de følgende afsnit er de enkelte krav medtaget i et gult tekstfelt for at gøre dem lettere at finde. Hvis der er forskel på de krav, der gælder for jernbanevirksomhederne, og de krav, der gælder for infrastrukturforvalterne, står den relevante tekst for sidstnævnte i parentes med **blåt**.

Direkte sammenligningstabeller for vurderingskriterierne i de tidligere forordninger (EU) 1158/2010 og (EU) 1169/2010 i forhold til kravene i Kommissionens delegerede forordning (EU) 2018/762 kan findes i Bilag 1 i denne vejledning. Tabellerne medtager også krydshenvisninger til bestemmelserne i ISO High Level Structure, hvor det er relevant. De har til formål at hjælpe ansøgerne med at påvise, at deres sikkerhedsledelsessystem overholder de nye krav, navnlig i de tilfælde, hvor ansøgeren allerede har fået et sikkerhedscertifikat eller en sikkerhedsgodkendelse, og/eller ansøgeren allerede har indført et andet ISO-ledelsessystem (f.eks. ISO 9001, 14001 eller 45001) (så de kan integreres sammen) eller har planer om at udvikle et sådant ved hjælp af denne model. Brug af denne tabel giver ikke en systematisk formodning om overholdelse af kravene i Kommissionens delegerede forordning (EU) 2018/762 CSM SMS for de organisationer, der har et ISO-certifikat.

0.5 ISO/IEC-retningslinjernes del 1 og det konsoliderede ISO-tillæg

ISO har udarbejdet officielle procedurer, der skal følges ved udviklingen og vedligeholdelsen af en international standard. I Annex SL, appendiks 2, i [ISO/IEC-retningslinjernes del 1 og det konsoliderede ISO-tillæg](#), indføres der en High Level Structure (HLS) for at bruge kernetekst i alle ledelsessystemstandards.

Bilag I og Bilag II til Kommissionens delegerede forordning (EU) 2018/762 sikrer en struktur, som er i overensstemmelse med ISO HLS, og som, hvor det er relevant, fremmer integrationen af forskellige ledelsessystemer, der har de samme kerneorganisationsprincipper og krav, men hvor den lovgivningsmæssige overholdelse og risikoområderne er specifikke for hver disciplin (f.eks. sikkerhed, miljø og kvalitet).

ISO-standarder og relevante vejledninger kan hjælpe jernbanevirksomhederne og infrastrukturforvalterne med at udvikle deres sikkerhedsledelsessystem (f.eks. er ISO 31000 et generisk dokument, som giver en bedre forståelse af risikostyring, ISO 31010 indeholder information om valg og anvendelse af risikovurderingsteknikker som FMECA, FTA, ETA og HAZOP, og ISO 55000 omhandler kravene til forvaltning af aktiver). Disse kan dog kun bidrage, hvis der er en omfattende viden om de jernbanerelaterede risici kontekst.

Selv om brugen af HLS sikrer konsekvens i forhold til ISO-ledelsessystemstandards, skal det understreges, at ovennævnte fælles sikkerhedsmetoder er forskrifter, der primært hjælper de nationale sikkerhedsmyndigheder eller agenturet med at vurdere ansøgningerne om bevilling af sikkerhedscertifikater eller sikkerhedsgodkendelser. Vurderinger i forbindelse med EU-sikkerhedscertifikater eller sikkerhedsgodkendelser vil som sådan være i modstrid med kravene til sikkerhedsledelsessystemer og ikke ISO HLS i sig selv. Det betyder med andre ord følgende: ISO-standarderne er baseret på frivillig certificering,

men i henhold til visse lovgivningsrammer giver de en formodning om overensstemmelse med de gældende regler for et specifikt område. Der er ingen bestemmelser, som giver ISO-standarderne en formodning om overensstemmelse med kravene i direktiv (EU) 2016/798 eller med Kommissionens delegerede forordning (EU) 2018/762.

Bestemmelse 4 til 10.2 i ISO/IEC-retningslinjernes del 1 og det konsoliderede tillæg 2016, Annex SL, appendiks 2, er gengivet eller tilpasset med tilladelse fra Den Internationale Standardiseringsorganisation, ISO. Den originale tekst kan ses i kildedokumentet. Dette dokument kan fås på [webstedet for ISO's centrale sekretariat](#). Ophavsretten tilhører ISO.

0.6 Sikkerhedsledelsessystemets formål

Sikkerhedsledelsessystemet har til formål at sikre, at organisationen styrer risici, der opstår i forbindelse med virksomhedsmål på en sikker måde og overholder alle de sikkerhedskrav, der gælder for den.

Ved at indføre en struktureret tilgang bliver det muligt at identificere farer og foretage en konstant risikostyring i forbindelse med en organisations egne aktiviteter med det formål at hindre ulykker. I denne tilgang tages der højde for de risici, der deles med andre aktører i jernbanesystemet (hovedsagelig jernbanevirksomheder, infrastrukturforvaltere og enheder med ansvar for vedligeholdelse, men også alle andre aktører, der har en potentiel indflydelse på jernbanesystemets sikre drift såsom fabrikanter, vedligeholdelsesvirksomheder, ihæندهavere, tjenesteydere, ordregivere, transportvirksomheder, afsendere, modtagere, lastevirksomheder, lossevirksomheder, uddannelsescentre samt passagerer og andre personer, der interagerer med jernbanesystemet, osv.). Gennemførelse af alle relevante elementer af et sikkerhedsledelsessystem på en passende måde kan give en organisation den nødvendige tillid til, at den styrer og vil fortsætte med at styre alle risici i forbindelse med sine aktiviteter under alle omstændigheder.

Modne organisationer anerkender, at effektiv risikostyring kun kan opnås gennem en proces, der samler tre kritiske dimensioner, nemlig en teknisk komponent med de anvendte redskaber og udstyr, en menneskelig komponent, hvor personer er i frontlinjen med deres færdigheder, uddannelse og motivation, og en organisatorisk komponent, der består af procedurer og metoder, som definerer opgaveforholdet.

Som følge heraf vil et passende sikkerhedsledelsessystem være i stand til at overvåge og forbedre alle tre dimensioner af sine risikokontrolforanstaltninger. Mange af funktionerne i sikkerhedsledelsessystemet for jernbanerne minder meget om den ledelsespraksis, man er fortalende for i forbindelse med kvalitet, sundhed og sikkerhed på arbejdspladsen, miljøbeskyttelse og business intelligence. Derfor kan principperne for god ledelse lettere integreres, sådan som det er angivet ovenfor, ved at bruge en fælles sikkerhedsmetode, som er baseret på ISO HLS, og som således muligvis ikke kræver en fuldstændig omlægning af organisationer, der allerede har indført sådanne systemer.

Man har anerkendt, at strukturerede ledelsessystemer tilfører værdi til forretningen gennem den effektive styring af grænseflader. Dette hjælper med at forbedre den overordnede indsats, indføre driftsmæssig effektivitet og styrke relationerne til kontrahenter og underkontrahenter, kunder og reguleringsmyndigheder, og det bidrager til at skabe en positiv sikkerhedskultur.

En ansøger skal tilrettelægge sit ledelsessystem i overensstemmelse med kravene i artikel 9 i direktiv (EU) 2016/798 for at opnå en sikker ledelse af sine operationer. Til dette formål skal ansøgeren påvise overholdelsen af kravene i bilag I og II i CSM SMS. Disse krav tager sigte på at give et fuldstændigt billede af organisationens sikkerhedsledelsessystem ifølge en såkaldt PDCA-cyklus (som omfatter planlægning, udførelse, kontrol og handling). Ansøgeren skal både tage højde for de enkelte krav og for, hvordan de passer sammen og udgør et sammenhængende sikkerhedsledelsessystem til styring af de relevante risici.

0.7 Sikkerhedsledelsessystem og procesorienteret tilgang

Et sikkerhedsledelsessystem er en måde at samle de forskellige tråde på for at kunne drive en sikker og velfungerende organisation. Disse elementer omfatter de mekanismer, der er indført for at leve op til internationale og nationale bestemmelser og standarder, krav på sektor- og forretningsniveau, resultaterne af risikovurdering og god praksis på tværs af virksomhedens forskellige aktiviteter. Sikkerhedsledelsessystemet bør derfor integreres i organisationens forretningsgange og bør endvidere ikke være et papirbaseret system, som er specifikt udviklet til at påvise lovgivningens overholdelse. Sikkerhedsledelsessystemet bør være en levende samling af bestemmelser, som hele tiden bliver mere modne, og som udvikler sig i takt med den organisation, de gælder for. At udforme et sikkerhedsledelsessystem kræver at organisationen forstår de risici, systemet skal styre, og de juridiske rammer, systemet opererer inden for, og for at have en klar idé om, hvordan en "god" indsats ser ud. Denne vejledning angiver de elementer i sikkerhedsledelsessystemet, som skal opfyldes, for at vurderingsmyndigheden kan udstede et EU-sikkerhedscertifikat. Bemærk dog, at kvaliteten af sikkerhedsledelsessystemet rækker ud over summen af dets elementer. Sikkerhedsledelsessystemet skal også fungere som et sammenhængende hele, hvor opfyldelse af det enkelte element skal sikre, at hele systemet fungerer korrekt.

De krav, som vurderingen af et sikkerhedsledelsessystem bliver bedømt ud fra, kan opfyldes ved hjælp af en dokumenteret proces (eller procedure osv.), men de bør også integreres inden for og på tværs af organisationens forskellige forretningsområder. F.eks. kan den nationale sikkerhedsmyndighed tjekke, at der eksisterer en politikerkklæring, men den skal også tjekke organisationens forpligtelse til at anvende den. En praktisk måde at gøre dette på er, at den nationale sikkerhedsmyndighed tjekker, hvordan sikkerhedsledelsessystemet overvåges og gennemgås af den øverste ledelse, hvordan personalet er involveret i dette, og hvordan resultaterne kommunikeres til personalet. På samme måde har organisationen måske ikke en specifik procedure eller specifikke procedurer til forvaltningen af sikkerhedsrelevant information, men den skal beskrive, hvordan de relevante afdelinger i virksomheden forvalter den på en passende måde (f.eks. meddelelse af sikkerhedsrelevant information til lokomotivføreren).

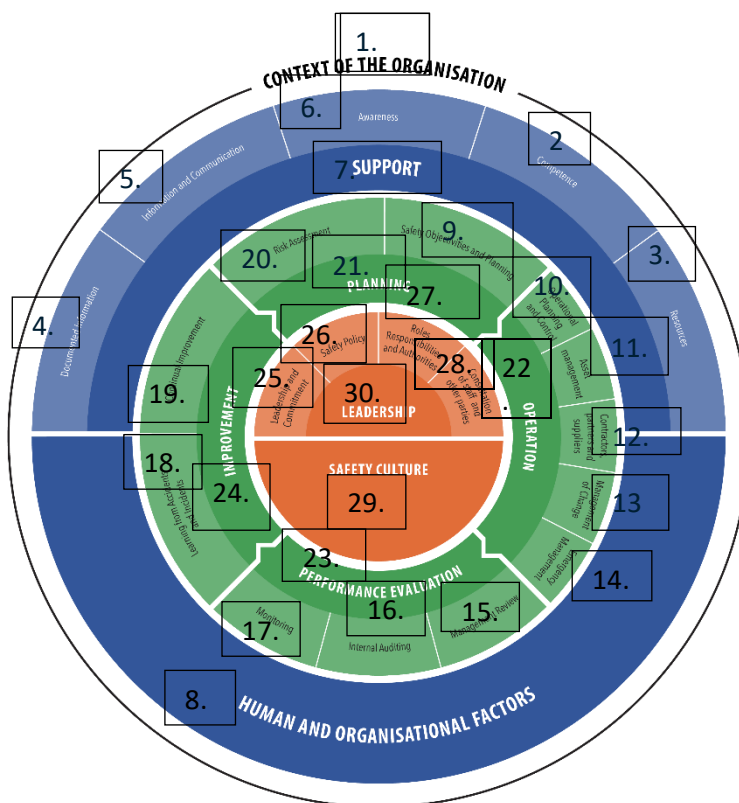
En vigtig udvikling i bilag I og bilag II til Kommissionens delegerede forordning (EU) 2018/762 CSM SMS er indførelsen af en procesorienteret tilgang. En sådan tilgang støttes også i ISO-ledelsessystemstandarderne, hvor de forskellige processer i ledelsessystemet er tæt forbundet med hinanden, og deres konsekvente anvendelse bidrager til opfyldelsen af organisationens mål. I bilag I og bilag II til Kommissionens delegerede forordning (EU) 2018/762 identificeres nogle vigtige forbindelser mellem processerne for at lette forståelsen af den procesorienterede tilgang, men det betyder ikke, at det kun er disse forbindelser, der eksisterer, eller at de bør påvises i overholdelsesøjemed. En organisations evne til at vise, hvordan processerne i dens ledelsessystem hænger sammen, er en god indikator for organisationens forståelse af, hvordan dens ledelsessystem fungerer effektivt.

Det kan observeres, at elementerne i et sikkerhedsledelsessystem følger en PDCA-cyklus (som omfatter planlægning, udførelse, kontrol og handling) (jf. [Figur 2](#)). PDCA-begrebet afspejler de funktionsmæssige forbindelser mellem de vigtigste elementer i et sikkerhedsledelsessystem:

- **Planlægning:** identificere risici og muligheder, opstille sikkerhedsmål og identificere de processer og foranstaltninger, der er nødvendige for at levere resultater i overensstemmelse med organisationens sikkerhedspolitik.
- **Drift:** udvikle, gennemføre og anvende processerne og foranstaltningerne som planlagt.
- **Præstationsevaluering:** overvåge og evaluere de opnåede resultater i forbindelse med de gennemførte processer og foranstaltninger, for så vidt angår målene og planlægningen, og rapportere resultaterne.
- **Forbedring:** iværksætte tiltag for løbende at forbedre sikkerhedsledelsessystemet og indsatsen på sikkerhedsområdet med henblik på at opnå de tilsigtede resultater.

Denne grundlæggende PDCA-proces suppleres med andre elementer i et sikkerhedsledelsessystem:

- **"Organisationens kontekst"**, som giver input til planlægningsfasen.
- **"Lederskab"**, som er drivkraften bag PDCA-cyklussen.
- Forskellige **"støtte"**-funktioner, som støtter alle elementerne i et sikkerhedsledelsessystem.



1	Context of the Organisation	Organisationens kontekst
2	Competence	Kompetence
3	Resources	Ressourcer
4	Documented Information	Dokumenteret information
5	Information and Communication	Information og kommunikation
6	Awareness	Bevidsthed
7	Support	Støtte
8	Human and organisational factors	Menneskelige og organisatoriske faktorer
9	Safety objectives and Planning	Sikkerhedsmål og -planlægning
10	Operational planning and control	Planlægning og styring af driften
11	Asset management	Forvaltning af aktiver
12	Contractors, partners and suppliers	Kontrahenter, partnere og leverandører
13	Management of change	Håndtering af ændringer
14	Emergency Management	Håndtering af nødsituationer
15	Management Review	Ledelsens evaluering

16	Internal auditing	Intern audit
17	Monitoring	Overvågning
18	Learning from accidents and incidents	Erfaringer fra ulykker og hændelser
19	Continual improvement	Løbende forbedring
20	Risk assessment	Risikovurdering
21	Planning	Planlægning
22	Operation	Drift
23	Performance evaluation	Præstationsevaluering
24	Improvement	Forbedring
25	Leadership and commitment	Lederskab og engagement [forpligtelse]
26	Safety policy	Sikkerhedspolitik
27	Roles, responsibilities and authorities	Organisatoriske roller, ansvarsområder og Bemyndigelser
28	Consultation of staff and other parties	Høring af personale og andre parter
29	Safety culture	Sikkerhedskultur
30	Leadership	Lederskab

Figur 2: Sikkerhedsledelsessystem for jernbanerne

0.8 Sikkerhedsledelsessystem og sikkerhedskultur

Sikkerhedskultur er en række adfærds- og tankemønstre, som i vid udstrækning deles inden for en organisation, når det gælder styringen af større risici i forbindelse med organisationens aktiviteter. Det indebærer selvfølgelig, at der kan være flere forskellige kulturer i spil inden for en organisation på grundlag af forhold som organisatorisk rolle, geografi eller andre fælles værdier. Dermed skabes sikkerhedskulturen på daglig basis gennem samspillet mellem aktørerne inden for en organisation, som både skal tilpasse sig til sit miljø og sikre integrationen af alle sine medlemmer.

Når det er sagt, er en direkte måde at beskrive sikkerhedskulturen på at kigge på de faktorer, der bidrager til adfærden. Sikkerhedsledelsessystemet udgør grundlaget: Ved at definere de ønskede arbejdsbetingelser og det forventede resultat definerer organisationen den foretrukne måde at arbejde på og de tekniske midler, der skal understøtte aktiviteten. For at udføre en sikker indsats vil organisationen foregribe uønskede situationer bedst muligt og indføre regler og metoder til at håndtere dem. Hertil kommer organisationens "adfærdsaspekt", dvs. kvaliteter, følelser, holdninger og forbindelser, som har en sådan indflydelse på samspilmønstrene mellem personer i organisationen, at det påvirker den måde, den tænker og handler på. Dette kulturelle aspekt drejer sig navnlig om de "uskrevne regler for en gruppe menneskers adfærd og beslutninger". Sammen fremmer (eller hæmmer) den strukturelle og kulturelle del af en organisation organisationens indsats.

Der er dog en stor risiko for, at en alt for bureaukratisk tilgang til sikkerhedsledelse er i modstrid med de driftsmæssige realiteter og resulterer i et sikkerhedsledelsessystem, som lever sit eget liv, dvs. hvor alle bestræbelser tager sigte på at udforme, vedligeholde og endda bevise eksistensen af et dokumenteret system, mens man ignorerer det driftsmæssige input, der er nødvendigt for rent faktisk at få det til at fungere efter hensigten. Dermed opstår der en kløft mellem "det arbejde, man forestiller sig" og "det arbejde, der udføres".

På den anden side er det muligt at bruge sikkerhedsledelsessystemet som et redskab til at udøve en positiv indflydelse på en organisations sikkerhedskultur og påvirke både det fysiske miljø og medarbejdernes adfærd

på en måde, som fremmer og letter sikkerheden. I sidste ende er det overensstemmelsen mellem organisationens strukturelle og kulturelle del, som skaber sikkerhed. For at hjælpe folk med at udføre deres opgaver er organisationen nødt til at forstå, hvordan mennesker (med deres evner og begrænsninger) anvender specifikationer til at løse problemer, og tage højde for denne viden, når deres arbejdsmiljø tilrettelægges. Det samme gælder for regler og forskrifter: Så længe der ikke tages hensyn til de arbejdstagere, der gennemfører dem, når arbejdsprocedurerne tilrettelægges, bliver de tvunget til at bryde reglerne for at få arbejdet gjort, når der opstår uoverensstemmelser eller konflikter.

I hele dette dokument vil de grundlæggende karakteristika, som er kendt for at bidrage til en positiv sikkerhedskultur, blive fremhævet. Endvidere giver Bilag 4 læseren grundlæggende viden om sikkerhedskultur og andre nyttige oplysninger, når organisationen skal udvikle sin egen strategi.

0.9 Understøttende dokumentation og dokumentere information

Dette dokument indeholder nogle angivelser af den dokumentation, som ansøgeren (dvs. jernbanevirksomheden eller infrastrukturforvalteren) skal fremlægge, når der ansøges om et sikkerhedscertifikat eller en sikkerhedsgodkendelse. Af de grunde, der er nævnt ovenfor, er der dog ingen nøjagtig angivelse af, hvad der skal fremlægges. For hvert krav er der en angivelse af den dokumentation, ansøgeren bør fremlægge, samt den relevante henvisning til det pågældende krav. Derudover gives der nogle eksempler på, hvordan denne dokumentation kan se ud i praksis. Det bør bemærkes, at eksemplerne gives for at fremme forståelsen og ikke er den eneste måde at påvise overholdelsen på, ligesom de heller ikke udgør en fuldstændig liste over mulige alternativer. Det skal desuden understreges, at når ansøgeren udarbejder en ansøgning, beskriver vedkommende, hvordan de enkelte krav er opfyldt. Vurderingspersonen eller ansøgeren kan bede om eller fremlægge den foreslåede information for at præcisere eller underbygge, hvordan kravet opfyldes. For ansøgeren og vurderingspersonen er det vigtigste ved hvert krav at sikre, at angivelserne om overholdelse indeholder henvisninger, som forklarer, hvor der kan findes yderligere dokumentation til støtte for disse punkter. Afsnittet med eksempler for hvert krav har til formål at vise, hvordan dette referencemateriale kan se ud.

Efter dette afsnit er der medtaget referencer, som kan hjælpe ansøgerne med udarbejdelsen af deres ansøgninger. Endelig har det sidste afsnit under hvert element til formål at etablere den nødvendige forbindelse til tilsynet. Her nævnes de spørgsmål, som en vurderingsperson måske vil fremhæve over for den nationale sikkerhedsmyndigheds team som interesseområder, der kan anvendes til at teste, at sikkerhedsledelsessystemet er komplet.

Bortset fra specifikke tilfælde foreskriver den tilgang, der anvendes i ISO-ledelsessystemstandarderne og i bilag I og bilag II til forordning (EU) 2018/762, heller ikke en bestemt slags dokumentation (f.eks. procedure), der forventes af ansøgeren. Den fleksibilitet, som ansøgeren får, har til formål at give organisationen mulighed for at præsentere sit sikkerhedsledelsessystem på en måde, der afspejler virksomhedens karakter og står i forhold til dens størrelse. Det vil også bidrage til, at man går væk fra en papirbaseret overholdelsestest og over til en vurdering af et levende system under udvikling, som på en korrekt måde afspejler en virksomheds sikkerhedsledelsessystem, sådan som det ser ud i praksis.

Termen "dokumenteret information" blev introduceret som en del af ISO HLS og fælles termer for ledelsessystemstandarder. Definitionen af "dokumenteret information" findes i *ISO 9000, bestemmelse 3.8.6*. Dokumenteret information kan anvendes til at kommunikere et budskab, fremlægge dokumentation for, hvad der var planlagt, og hvad der rent faktisk er blevet gjort, eller til vidensdeling. Det omfatter, men er ikke begrænset til, dokumenter og registreringer såsom procedurer, mødereferater, rapporter, formel kommunikation af mål, resultater, aftaler, kontrakter osv. En mere detaljeret forklaring findes i *Guidance on the requirements for Documented Information of ISO 9001:2015* på ISO's websted:

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

Termen "procedure" indebærer ikke, at der eksisterer et dokument, som står alene, og som udelukkende og i omfattende grad dækker håndteringen af hvert enkelt element i sikkerhedsledelsessystemet, eller at der anmodes om udarbejdelsen af et specifikt sæt nye dokumenter. Når der i dette dokument henvises til en procedure, menes der dokumenteret information (f.eks. papirdokumenter), som skildrer den proces, der skal anvendes. Når der henvises til en proces, menes der midlerne til at udføre en opgave eller nå et mål, som evt. kan være fastlagt i en procedure.

0.10 Krydshenvisninger til andre EU-forordninger og gældende lovkrav

Henvisninger til andre EU-forordninger styrker sammenhængen mellem de forskellige juridiske tekster og fastslår forbindelsen mellem dem. Sikkerhedsledelsessystemer bør altid være i overensstemmelse med den gældende juridiske tekst, medmindre andet er angivet (f.eks. overgangsbestemmelser eller forsinket gennemførelse). Når en EU-forordning ophæves, er alle henvisninger som regel henvisninger til den nye forordning (hvis de er medtaget heri).

Alle jernbanevirksomheder og infrastrukturforvaltere skal overholde en række lovkrav, som ikke blot omfatter de krav, der udelukkende vedrører sikkerhedsspørgsmål. Nogle af disse øvrige krav vil have en direkte eller indirekte indvirkning på, hvordan organisationen håndterer sit sikkerhedsansvar gennem sit sikkerhedsledelsessystem, f.eks. overholdelsen af den lovgivning, der hidrører fra direktiv (EU) 2016/797 om interoperabilitet, eller sikkerhedsrelevansen af de tjenester, som infrastrukturforvalterne leverer til jernbanevirksomhederne inden for rammerne af direktiv (EU) 2012/34. Derfor skal det sikkerhedsledelsessystem, som jernbanevirksomhederne og infrastrukturforvalterne anvender til at adressere sikkerhedsrisiciene, tilrettelægges på en sådan måde, at man sikrer overholdelsen af eventuelle andre lovkrav, hvis relevant.

Making the railway system
work better for society.

Indhold

0	Indledning	2
0.1	Formålet med vejledningen	2
0.2	Hvem henvender denne vejledning sig til?	2
0.3	Anvendelsesområde	3
0.4	Vejledningens struktur	3
0.5	ISO/IEC-retningslinjernes del 1 og det konsoliderede ISO-tillæg	4
0.6	Sikkerhedsledelsessystemets formål	5
0.7	Sikkerhedsledelsessystem og procesorienteret tilgang	6
0.8	Sikkerhedsledelsessystem og sikkerhedskultur	8
0.9	Understøttende dokumentation og dokumenteret information	9
0.10	Krydshenvisninger til andre EU-forordninger og gældende lovkrav	10
1	Organisationens kontekst	16
1.1	Lovkrav	16
1.2	Formål	16
1.3	Forklarende noter	17
1.4	Dokumentation	18
1.5	Eksempler på dokumentation	18
1.6	Referencer og standarder	19
1.7	Tilsynsspørgsmål	19
2	Lederskab	20
2.1	Lederskab og forpligtelse	20
2.1.1	Lovkrav	20
2.1.2	Formål	20
2.1.3	Forklarende noter	21
2.1.4	Dokumentation	21
2.1.5	Eksempler på dokumentation	22
2.1.6	Referencer og standarder	22
2.1.7	Tilsynsspørgsmål	22
2.2	Sikkerhedspolitik	24
2.2.1	Lovkrav	24
2.2.2	Formål	24
2.2.3	Forklarende noter	24
2.2.4	Dokumentation	24
2.2.5	Eksempler på dokumentation	25
2.2.6	Tilsynsspørgsmål	25
2.3	Organisatoriske roller, ansvarsområder, ansvarlighed og bemyndigelser	26

2.3.1	Lovkrav	26
2.3.2	Formål	26
2.3.3	Forklarende noter	26
2.3.4	Dokumentation	27
2.3.5	Eksempler på dokumentation	27
2.3.6	Referencer og standarder	28
2.3.7	Tilsynsspørgsmål	28
2.4	Høring af personale og andre parter	29
2.4.1	Lovkrav	29
2.4.2	Formål	29
2.4.3	Forklarende noter	29
2.4.4	Dokumentation	30
2.4.5	Eksempler på dokumentation	30
2.4.6	Tilsynsspørgsmål	30
3	Planlægning	31
3.1	Tiltag til imødegåelse af risici	31
3.1.1	Lovkrav	31
3.1.2	Formål	31
3.1.3	Forklarende noter	32
3.1.4	Dokumentation	34
3.1.5	Eksempler på dokumentation	34
3.1.6	Referencer og standarder	35
3.1.7	Tilsynsspørgsmål	35
3.2	Sikkerhedsmål og -planlægning	37
3.2.1	Lovkrav	37
3.2.2	Formål	37
3.2.3	Forklarende noter	37
3.2.4	Dokumentation	38
3.2.5	Eksempler på dokumentation	38
3.2.6	Tilsynsspørgsmål	38
4	Støtte	39
4.1	Ressourcer	39
4.1.1	Lovkrav	39
4.1.2	Formål	39
4.1.3	Forklarende noter	39
4.1.4	Dokumentation	39
4.1.5	Eksempler på dokumentation	39
4.1.6	Tilsynsspørgsmål	40
4.2	Kompetence	41
4.2.1	Lovkrav	41
4.2.2	Formål	41
4.2.3	Forklarende noter	42
4.2.4	Dokumentation	42
4.2.5	Eksempler på dokumentation	43

4.2.6	Referencer og standarder	44
4.2.7	Tilsynsspørgsmål	44
4.3	Bevidsthed	45
4.3.1	Lovkrav	45
4.3.2	Formål	45
4.3.3	Dokumentation	45
4.3.4	Eksempler på dokumentation	45
4.3.5	Tilsynsspørgsmål	46
4.4	Oplysning og kommunikation	47
4.4.1	Lovkrav	47
4.4.2	Formål	47
4.4.3	Forklarende noter	47
4.4.4	Dokumentation	48
4.4.5	Eksempler på dokumentation	48
4.4.6	Tilsynsspørgsmål	49
4.5	Dokumenteret information	50
4.5.1	Lovkrav	50
4.5.2	Formål	51
4.5.3	Forklarende noter	51
4.5.4	Dokumentation	52
4.5.5	Eksempler på dokumentation	53
4.5.6	Referencer og standarder	53
4.5.7	Tilsynsspørgsmål	53
4.6	Integration af menneskelige og organisatoriske faktorer	55
4.6.1	Lovkrav	55
4.6.2	Formål	55
4.6.3	Forklarende noter	55
4.6.4	Dokumentation	55
4.6.5	Eksempler på dokumentation	56
4.6.6	Referencer og standarder	57
4.6.7	Tilsynsspørgsmål	57
5	Drift	58
5.1	Planlægning og styring af driften	58
5.1.1	Lovkrav	58
5.1.2	Formål	59
5.1.3	Forklarende noter	60
5.1.4	Dokumentation	61
5.1.5	Eksempler på dokumentation	62
5.1.6	Referencer og standarder	63
5.1.7	Tilsynsspørgsmål	64
5.2	Forvaltning af aktiver	65
5.2.1	Lovkrav	65
5.2.2	Formål	65
5.2.3	Forklarende noter	66

5.2.4	Dokumentation	67
5.2.5	Eksempler på dokumentation	69
5.2.6	Referencer og standarder	73
5.2.7	Tilsynsspørgsmål	73
5.3	Kontrahenter, partnere og leverandører	74
5.3.1	Lovkrav	74
5.3.2	Formål	74
5.3.3	Forklarende noter	75
5.3.4	Dokumentation	75
5.3.5	Eksempler på dokumentation	75
5.3.6	Tilsynsspørgsmål	76
5.4	Håndtering af ændringer	77
5.4.1	Lovkrav	77
5.4.2	Formål	77
5.4.3	Forklarende noter	77
5.4.4	Dokumentation	78
5.4.5	Eksempler på dokumentation	78
5.4.6	Tilsynsspørgsmål	78
5.5	Håndtering af nødsituationer	79
5.5.1	Lovkrav	79
5.5.2	Formål	79
5.5.3	Forklarende noter	80
5.5.4	Dokumentation	80
5.5.5	Eksempler på dokumentation	80
5.5.6	Tilsynsspørgsmål	81
6	Præstationsevaluering	82
6.1	Overvågning	82
6.1.1	Lovkrav	82
6.1.2	Formål	82
6.1.3	Forklarende noter	82
6.1.4	Dokumentation	83
6.1.5	Eksempler på dokumentation	83
6.1.6	Tilsynsspørgsmål	83
6.2	Intern audit	85
6.2.1	Lovkrav	85
6.2.2	Formål	85
6.2.3	Forklarende noter	85
6.2.4	Dokumentation	85
6.2.5	Eksempler på dokumentation	86
6.2.6	Referencer og standarder	86
6.2.7	Tilsynsspørgsmål	86
6.3	Ledelsens evaluering	
6.3.1	Lovkrav	87
6.3.2	Formål	87

6.3.3	Dokumentation	87
6.3.4	Eksempler på dokumentation	88
6.3.5	Tilsynsspørgsmål	88
7	Forbedring	89
7.1	Erfaringer fra ulykker og hændelser	89
7.1.1	Lovkrav	89
7.1.2	Formål	89
7.1.3	Forklarende noter	90
7.1.4	Dokumentation	90
7.1.5	Eksempler på dokumentation	90
7.1.6	Referencer og standarder	91
7.1.7	Tilsynsspørgsmål	91
7.2	Løbende forbedringer	93
7.2.1	Lovkrav	93
7.2.2	Formål	93
7.2.3	Forklarende noter	93
7.2.4	Dokumentation	95
7.2.5	Eksempler på dokumentation	96
7.2.6	Tilsynsspørgsmål	96
	Bilag 1 — Sammenligningstabeller	97
	Bilag 2 — Gensidig accept af godkendelser, anerkendelser eller certifikater for produkter eller tjenester udstedt i henhold til EU-lovgivningen	105
	Bilag 3 — Sidesporsaktiviteter, kontraktlige aftaler og partnerskaber	110
	Bilag 4 — Sikkerhedskultur	114
	Bilag 5 — Menneskelige og organisatoriske faktorer	120
	Bilag 6 — Definitioner	124

1 Organisationens kontekst

1.1 Lovkrav

1.1 Organisationen skal:

- (a) beskrive driftens type, **karakter**, omfang og område
 - (b) udpege alvorlige sikkerhedsrisici, som dennes jernbanedrift medfører, uanset om driften udføres af organisationen selv eller af kontrahenter, partnere og leverandører under dens kontrol
 - (c) udpege interessenter (f.eks. tilsynsorganer, myndigheder, **jernbanevirksomheder**, infrastrukturforvaltere, kontrahenter, leverandører, partnere), herunder parter uden for jernbanesystemet af relevans for sikkerhedsledelsessystemet
 - (d) udpege og vedligeholde lovgivning og andre sikkerhedsrelaterede krav fra de interessenter nævnt i litra (c)
 - (e) sikre, at de krav, der er nævnt i litra d) tages i betragtning i forbindelse med udviklingen, gennemførelsen og opretholdelsen af sikkerhedsledelsessystemet
- beskrive sikkerhedsledelsessystemets anvendelsesområde med angivelse af hvilken del af forretningen, der er indgået i eller ikke indgår heri, og under hensyn til kravene nævnt i punkt (d).

1.2 I dette bilag forstås ved:

- (a) "karakter" i forbindelse med jernbanedrift, der udføres af infrastrukturforvaltere: driftens karakteristika i form af anvendelsesområde, herunder infrastrukturens udformning og konstruktion, vedligeholdelse af infrastrukturen, trafikplanlægning, trafikstyring og -kontrol, og i form af anvendelse af jernbaneinfrastrukturen, herunder konventionelle og/eller højhastighedstog, passagerbefordring og/eller godstransport
- (b) "omfang" i forbindelse med jernbanedrift, der udføres af infrastrukturforvaltere: det omfang, som er karakteriseret ved jernbanesporets længde og infrastrukturforvalterens anslåede størrelse målt på antal medarbejdere, der arbejder i jernbanesektoren.

1.2 Formål

Ansøgeren bør så præcist som muligt dokumentere over for myndigheden, at vedkommendes sikkerhedsledelsessystem dækker alle aspekter af driften. Vurderingsmyndigheden bør tydeligt kunne se, hvilken karakter driften har, og hvordan driften styres via sikkerhedsledelsessystemet. Ansøgeren bør vise, at vedkommende har en klar forståelse af forholdet til sine interessenter og de alvorlige risici, som ansøgeren står over for, hvem der er berørt, og hvordan disse spørgsmål håndteres i sikkerhedsledelsessystemet.

1.3 Forklarende noter

I punkt 1.1 i ovennævnte juridiske tekst erstattes "type" af "karakter", og "område" slettes de steder, hvor kravet vedrører infrastrukturforvaltere.

Kravene til organisationen, dens kontekst og sikkerhedsledelsessystemets anvendelsesområde **(1.1)** tager sigte på at give en bedre forståelse — ud fra vurderingspersonernes perspektiv — af organisationens virksomhed, interessenternes forventninger og det miljø, som organisationen opererer i. Organisationens karakter er udgangspunktet for vurderingen. At medtage denne oplysning i starten af ansøgningen gør det muligt for ansøgerne at beskrive, hvad de gør, og hvordan deres organisation er opbygget. Dette giver så vurderingspersonen mulighed for at beslutte, hvordan vurderingen skal planlægges. Hvis organisationen f.eks. er centraliseret eller udfører forskellige aktiviteter med en omfattende lokal frihed til at planlægge og tilrettelægge aktiviteterne, eller hvis organisationen beskæftiger flere eller færre kontrahenter, vil der være en tilsvarende forventning om, at ansøgerens organisation og dennes sikkerhedsledelsessystem er opbygget til at tackle de spørgsmål, der opstår. I forklaringen af organisationens overordnede kontekst kan det også angives, hvordan de menneskelige og organisatoriske faktorer håndteres. Den struktur, der er fastsat i bestemmelse 4 i ISO HLS, kan hjælpe med at forstå det forberedende arbejde, der er nødvendigt inden sikkerhedsledelsessystemets etablering. Det er af afgørende vigtighed, at vurderingspersonen forstår driftens omfang, hvis vedkommende skal være i stand til at foretage en korrekt vurdering.

Driftens type **(1.1 (a))** dækker pr. definition passagertransport (med eller uden højhastighedstjenester), godstransport (med eller uden transport af farligt gods) og rangerydelser. Den kan også omfatte andre særlige typer aktiviteter såsom test af køretøjer, drift af køretøjer til vedligeholdelse af jernbaneinfrastruktur og aktiviteter på privatejede sidespor. Der findes flere oplysninger om driftens type, omfang og område i agenturets ansøgningsvejledning om udstedelse af EU-sikkerhedscertifikater. Der findes yderligere oplysninger om sidesporsaktiviteter i Bilag 3.

For en infrastrukturforvalter forstås ved karakteren og omfanget (1.2) af vedkommendes drift karakteren af forretningen og vedkommendes geografiske størrelse og kompleksitet. Karakteren afspejler den form for infrastruktur, der anvendes, hvor moderne den er, og om der køres med højhastighedstog eller konventionelle tog eller begge dele, mens omfanget adresserer den type forretning, der drives.

Hvis der identificeres alvorlige risici i dette tilfælde, bør ansøgeren vise, at denne gennem sin risikoanalyse er opmærksom på, hvilke risici der er de vigtigste. Angivelse af alvorlige risici betyder også, at ansøgerne har oprettet et sikkerhedsledelsessystem (eller forbereder oprettelsen af det), og at de ud fra dette kan:

- *analysere farlige tildragelser og vurdere risici*
- *blive klar over de vigtigste (med hensyn til konsekvenser og hyppighed) og*
- *prioritere foranstaltninger, der tager sigte på at forebygge ulykker **(1.1 (b))***

Det bidrager til at fastsætte organisationens kontekst og viser vurderingsmyndigheden, at de forstår det miljø, de arbejder i. De aktiviteter, der udføres af andre parter uden for jernbanesystemet **(1.1 (c))**, kan påvirke driftens sikkerhed, og derfor skal de også tages i betragtning ved risikovurderingen. Der findes flere oplysninger om kontraktlige aftaler og partnerskab i Bilag 3.

Angivelsen af de gældende sikkerhedsrelaterede krav **(1.1 (d))** omfatter bestemmelserne i de gældende EU-forordninger (f.eks. CSM SMS, navnlig bilag I og bilag II, CSM for risikovurdering og -evaluering, CSM for overvågning, relevante TSI'er, gennemførelsesretsakten om de praktiske bestemmelser med henblik på sikkerhedscertificering og, hvis relevant, gennemførelsesretsakten om de praktiske bestemmelser for typegodkendelse og ECM-forordningen), national lovgivning (f.eks. meddelte nationale forskrifter og national lovgivning) og alle andre krav, som organisationen overholder (f.eks. regler for jernbanedrift eller ledelsessystemer på sektor- eller brancheniveau samt tekniske standarder som ISO, CEN/CENELEC og UIC). I dette afsnit identificerer organisationen de lovgivningsbestemmelser, som den — ud over de sektorkrav og andre krav den skal overholde for at opretholde en sikker jernbanedrift — skal overholde.

I dette dokument har termene "personale", "medarbejdere" og "arbejdstagere" samme betydning, dvs. personer, som arbejder under ansøgerens organisations direkte kontrol.

1.4 Dokumentation

- *For jernbanevirksomheder: Oplysninger om driftens karakter, f.eks. passager- og/eller godstransport, transport af farligt gods, den geografiske dækning (ved at medtage et kort eller en ruteplan) og driftens omfang (herunder typer af rullende materiel og antal medarbejdere), og i tilfælde af fornyelser og ændringer af disse siden den seneste vurdering (1.1 (a)).*
- *For infrastrukturforvaltere: Oplysninger om karakteren af de aktiviteter, de udfører, f.eks. godstransport og/eller passagertransport, rangerydelser eller andre facilitetstjenester (som omhandlet i bilag II til direktiv 2012/34/EU), der har indvirkning på jernbanesikkerheden, den geografiske dækning (ved at medtage et kort eller en ruteplan) og omfanget af de jernbanevirksomhedsaktiviteter, der finder sted på nettet. Infrastrukturforvalterne bør også medtage oplysninger om eventuelt rullende materiel (herunder anlæg til infrastrukturvedligeholdelse eller -måling), de opererer med, og angive det antal medarbejdere, de beskæftiger, og i tilfælde af fornyelser og ændringer af disse siden den seneste vurdering (1(a)).*
- *Ansøgere om et sikkerhedscertifikat eller en sikkerhedsgodkendelse skal vise, hvordan de har identificeret de relevante lovkrav, f.eks. CSM kravene, de tekniske specifikationer for interoperabilitet, navnlig den specifikation, der vedrører delsystemet drift og trafikstyring (TSI OPE), samt de gældende nationale forskrifter, og hvordan ansøgerne overholder disse (de processer i sikkerhedsledelsessystemer, som understøtter overholdelse) (1.1 (c)-(d)).*
- *Ansøgeren skal identificere interessenter, der er relevante for vellykket gennemførelse af deres sikkerhedsledelsessystemer (dvs. deres handlinger har indvirkning eller potentiel indvirkning på sikkerhedsledelsessystemet for eksempel kontrahenter eller partnere) med angivelse af, hvorfor de er nødvendige til sikker drift af sikkerhedsledelsessystemet (1.1 (c) (d)).*
- *For begge: Ansøgerne bør angive, hvor i deres sikkerhedsledelsessystems dokumentation hvert af kravene til sikkerhedsledelsessystemer, herunder de relevante krav i de gældende tekniske specifikationer for interoperabilitet, navnlig TSI OPE, og relevante meddelte nationale forskrifter, er overholdt (1.1 (e)).*
- *Ansøgerne skal angive de alvorligste sikkerhedsrisici, som berører deres forretning (1.1(b)).*
- *Ansøgerne skal fremlægge oplysninger om sikkerhedsledelsessystemets anvendelsesområde (bl.a. hvor grænserne går til andre dele af forretningen) (1.1(f)).*

1.5 Eksempler på dokumentation

Et kort, der viser det geografiske driftsområde. Oplysninger om det rullende materiel, der er godkendt til driften (herunder, hvis relevant, enhver form for rullende materiel, som det foreslås at have i drift i certifikatets eller godkendelsens gyldighedsperiode, og eventuelle begrænsninger for anvendelsesområdet). Oplysninger om de typer af tjenester, som ansøgeren har til hensigt at levere (passager- og/eller godstransport) er medtaget.

Når ansøgeren er en infrastrukturforvalter, kan disse oplysninger f.eks. gives med henvisning til:

- *oplysningerne i jernbaneinfrastrukturregistret, som er oprettet i henhold til direktivet om interoperabilitet (artikel 49)*
- *indholdet i netvejledningen (navnlig afsnit I), der er etableret i henhold til direktiv 2012/34/EU, og*
- *strækningsoversigten (TSI OPE).*

Der er korrekte henvisninger til de oplysninger, der er angivet med henblik på opnåelse af en sikkerhedsgodkendelse eller et sikkerhedscertifikat, og der er passende dokumentation for, at oplysningerne overholder relevant EU-lovgivning.

En angivelse af nuværende og foreslået personale inden for EU-sikkerhedscertifikatets gyldighedsperiode, såfremt dette er kendt.

En jernbanevirksomhed fremlægger oplysninger om sine driftsmæssige grænseflader, bl.a. med infrastrukturforvalter(e), andre jernbanevirksomheder, kontrahenter og beredskabstjenester. Oplysningerne omfatter også infrastrukturforvalterens eventuelle specifikke krav, der påvirker jernbanevirksomhedens sikkerhedsledelsessystem.

For jernbanevirksomheders vedkommende kan en oversigtstabel, der indgives gennem one-stop-shoppen som en del af ansøgningen om et sikkerhedscertifikat, anvendes til at forklare, hvordan forordningerne og andre relevante krav bliver overholdt.

En infrastrukturforvalter bør også fremlægge en lignende liste over dem, den har driftsmæssige grænseflader med, f.eks. jernbanevirksomheder, der opererer på den styrede infrastruktur, kontrahenter, naboinfrastrukturforvaltere, byggepladser, lokale myndigheder (ved vejgrænseflader) og beredskabstjenester.

Oplysninger om de lovgivningsbestemmelser (både nationale og europæiske), der skal overholdes.

En beskrivelse af (herunder et organisationsdiagram for), hvordan sikkerhedsledelsessystemet er opbygget og forvaltes i organisationen, inklusive links til de forskellige afsnit i sikkerhedsledelsessystemet, hvor der findes nærmere oplysninger såsom driftsregler.

Et nyt eksemplar af den årlige rapport, som indeholder en oversigt over de mest alvorlige risici, organisationen står over for, og målene for styringen af disse, samt den metode, der anvendes til at vurdere dem, og hvordan de prioriteres.

1.6 Referencer og standarder

- *TSI OPE-ansøgningsvejledninger*

1.7 Tilsynsspørgsmål

Kontrol af de fremlagte oplysningers nøjagtighed i forhold til kendte oplysninger om eksisterende aktiviteter, hvis der ansøges om fornyelse af certifikatet, eller i forhold til andre tilgængelige oplysninger, hvis der er tale om en ny aktør.

Kontrol af, at sikkerhedsledelsessystemet som beskrevet omfatter de processer, regler og andre beskrivelser, der er nødvendige for at håndtere sikkerheden i praksis.

Kontrol af, at alle de grænseflader, organisationen har med andre, er afspejlet i sikkerhedsledelsessystemets tiltag til risikostyring.

2 Lederskab

2.1 Lederskab og engagement

2.1.1 Lovkrav

- 2.1.1. Den øverste ledelse skal udvise lederskab og engagement i forbindelse med udviklingen, gennemførelsen, vedligeholdelsen og løbende forbedring af sikkerhedsledelsessystemet ved at:
- (a) udvise ansvarlighed og påtage sig det overordnede ansvar for sikkerheden
 - (b) sikre opbakning til sikkerhed på forskellige ledelsesniveauer i organisationen i kraft af ledelsens aktiviteter og i dens forhold til personalet og kontrahenterne
 - (c) sikre, at sikkerhedspolitikken og sikkerhedsmålene fastsættes, forstås og kan forenes med organisationens strategiske kurs
 - (d) sikre, at kravene vedrørende sikkerhedsledelsessystemet integreres i organisationens forretningsgange
 - (e) sikre, at de fornødne ressourcer til sikkerhedsledelsessystemet er til rådighed
 - (f) sikre, at sikkerhedsledelsessystemet effektivt styrer de sikkerhedsrisici, som må tilskrives organisationen
 - (g) tilskynde personalet til at medvirke til at overholde kravene i sikkerhedsledelsessystemet
 - (h) fremme løbende forbedringer af sikkerhedsledelsessystemet
 - (i) sikre, at sikkerhedsaspektet tages i betragtning, organisationens forretningsmæssige risici udpeges og forvaltes, og redegøre for, hvordan konflikten mellem sikkerhedsaspektet og andre mål erkendes og håndteres
 - (j) fremme en positiv sikkerhedskultur

2.1.2 Formål

At sætte en klar og positiv retning for sikkerhedsledelsen vil have stor indflydelse på, hvordan risiciene styres. Vurderingsmyndigheden skal kunne stole på, at ansøgeren ønsker at tildele ressourcer, som gør det muligt for organisationen at skabe en sikker drift og gør det muligt for den at styre risiciene på en effektiv måde, og at den ansøgende organisations ledelse vil sikre, at dette sker. Ledelsens forpligtelse i forhold til menneskelige og organisatoriske faktorer er dokumenteret i politikker og mål samt i ledelsens adfærd. Endvidere vil en tilgang fra ledelsens side baseret på menneskelige og organisatoriske faktorer sikre, at uddannelses- og procedureudvikling baseres på den opgave, der skal udføres, inden for dens naturlige rammer, hvilket vil bidrage til at optimere både risikostyringen og indsatsen.

Sikkerhedspolitikken fastslår vigtigheden og prioriteringen af sikkerhed, herunder integrationen af menneskelige og organisatoriske faktorer samt fremme af sikkerhedskulturen.

Organisationen arbejder for en konstant og kollektivagt pågivenhed, bekæmper magelighed ("alt er under kontrol") og overforenkling ("overholdelse af procedurerne er tilstrækkeligt til at skabe sikkerhed") og fremmer en spørgende holdning. Endvidere er alle organisationens aktører klar over, at der uanset kvaliteten af planlægning, tilrettelæggelse, tekniske barrierer og procedurer altid kan være en forskel mellem det, der blev forventet, og det, der reelt sker. Alle mulige kilder anvendes til at opdage og i fællesskab analysere de situationer, som ikke er foregrebet på en passende måde.

Desuden er organisationens kommunikation om sikkerhed i tråd med de reelle ledelsesbeslutninger.

Hvis et sikkerhedsledelsessystem skal fungere effektivt og udvikles og forbedres i fremtiden, er det af afgørende vigtighed, at personer med ledelsesfunktion viser deres personale og de interesserede parter, at de sætter en positiv dagsorden for sikkerhedens håndtering. Det er personerne i lederstillinger, der har den største indflydelse på organisationskulturen, og det er derfor afgørende, at de kan kommunikere det rigtige budskab til dem, der arbejder under deres ansvar. Adfærden hos ledere på alle niveauer i organisationen samt den vægt, de tillægger sikkerhed i deres daglige beslutninger, har stor indflydelse på adfærden hos andre aktører, når de skal udføre deres sikkerhedsopgaver. Lederne bør også skabe et fysisk og socialt arbejdsmiljø, der gør det muligt at udføre frontlinjearbejdet sikkert.

2.1.3 Forklarende noter

"Den øverste ledelse" (**2.1.1**) er i denne sammenhæng dem, der træffer beslutninger som organisationens ledelse. Det vil typisk være den administrerende direktør, medlemmerne af den øverste ledelsesgruppe, bestyrelsesformanden og bestyrelsesmedlemmerne. Som gruppe og som enkeltpersoner skal "den øverste ledelse" udvise lederskab og engagement i og gennem sikkerhedsledelsessystemet.

Der skal lægges tilstrækkelig vægt på sikkerhedsrisiciene (**2.1.1 (ii)**) for at skabe en modvægt til andre forretningsrisici, så man undgår en situation, hvor ledelsen prioriterer forretningsbehovene på en sådan måde, at sikkerhedsindsatsen svækkes. Den øverste ledelse skal sikre, at målene håndteres på en sådan måde, at sikkerhedsindsatsen opretholdes, og risiciene styres i så vid udstrækning, som det med rimelighed kan lade sig gøre. Modsatrettede mål må ikke resultere i modsatrettede opgaver for medarbejderne, da dette kan føre til sikkerhedsproblemer.

En integreret tilgang baseret på menneskelige og organisatoriske faktorer inden for lederskab og ledelse er ensbetydende med at fastsætte mål, forventninger og ansvarlighed med hensyn til sikkerhedsadfærden på alle niveauer i organisationen og at sikre rettidig feedback og kommunikation.

2.1.4 Dokumentation

- Der er en sikkerhedspolitik og mål, og der er dokumentation for, at disse er tilgængelige for og forstås af hele personalet, og det forklares, hvordan de passer sammen med andre forretningsgange (**2.1.1 (a)(b)(g)(e)**).
- I sikkerhedspolitikken angives vigtigheden af at anvende en tilgang baseret på menneskelige og organisatoriske faktorer i alle sikkerhedsrelaterede processer for at opnå et højt sikkerhedsniveau i organisationen. Organisationen viser, hvordan problemer vedrørende menneskelige og organisatoriske faktorer i organisationsprocesser håndteres (**2.1.1 (c)**).
- Forbindelsen mellem sikkerhedsledelsessystemet og andre forretningsaktiviteter er tydeligt angivet i en procedure eller et organisationsdiagram (**2.1.1 (e),(i)**).
- Der er oplysninger tilgængelige i sikkerhedspolitikken eller i andre processer, som angiver, at ledelsen er forpligtet til at sørge for og opretholde tilstrækkelige ressourcer til, at sikkerhedsledelsessystemet kan fungere effektivt (**2.1.1 (e)**).
- Der er dokumentation for, at ledelsen fremmer en positiv sikkerhedskultur (**2.1.1 (j)**).
- Der er dokumentation, som viser, hvordan det sikres, at personalet forstår deres sikkerhedsroller og -ansvar, og hvordan det, de gør, har indvirkning på organisationens evne til at styre risici ved hjælp af sikkerhedsledelsessystemet (**2.1.1 (d)(f)(i)**).
- Der er dokumentation i sikkerhedspolitikken eller anden dokumentation for, at organisationen bestræber sig på at informere personalet om den vigtige rolle, de spiller, når det gælder om at sikre, at sikkerhedsledelsessystemet fungerer i praksis og giver en fornuftig risikostyring (**2.1.1 (e)**).
- Der er processer, som angiver, hvordan de menneskelige og organisatoriske faktorer bør håndteres og kommunikerer inden for organisationen, hvad angår organisationens forretningsmål og

organisatoriske processer, f.eks. projekter, undersøgelser af ulykker og hændelser, risikoanalyser og andre sikkerhedsrelaterede aktiviteter for organisationens eget personale, kontrahenter, partnere og leverandører (2.2.1 (c)(d)(e)).

- *Der er dokumentation for, at ledelsen har indført processer, der skal sikre, at organisationens underleverandører håndterer menneskelige og organisatoriske faktorer korrekt (2.2.1 (c)(d)(e)).*

2.1.5 Eksempler på dokumentation

Der fremlægges en sikkerhedspolitik, som er dateret og underskrevet af den administrerende direktør, og som klart angiver ledelsens forpligtelse i forhold til sikkerhed og forbedring af sikkerheden, og hvordan personalet er involveret i at styre sikkerhedsrisiciene. Sikkerhedspolitikken indeholder også en angivelse af, hvordan den skal gennemgås.

Der er opstillet en klar række sikkerhedsmål for organisationen, som er signifikante, målbare, opnåelige, relevante og tidsbestemte (SMART), og der er fastsat en klar metode i en procedure for oprettelsen af disse og for analysen af, om de opfyldes eller ej.

En entydig erklæring fra ledelsens side om, hvordan den fremmer en positiv sikkerhedskultur, og hvordan personalet involveres og engageres i processen.

En oversigt over de møder i den øverste ledelse, hvor sikkerhed er et fast rapporteringspunkt, samt hyppigheden af disse møder.

En entydig erklæring vedrørende organisationens forpligtelse til at sørge for tilstrækkelige ressourcer til, at sikkerhedsledelsessystemet kan fungere effektivt og styre risiciene.

Et organisationsdiagram, der tydeligt beskriver, hvordan sikkerhedsledelsessystemet fungerer, og hvem der er ansvarlig for hvad.

Der anvendes en tilgang baseret på menneskelige og organisatoriske faktorer ved udformning af nyt udstyr, f.eks. nye tog. Dette omfatter anvendelse af de tidligere brugeres erfaringer ved opstilling af designkravene, en analyse af opgaverne for at identificere kognitive og fysiologiske udfordringer, en reduktion af muligheden for designfejl ved at anvende retningslinjer for menneskelige faktorer såsom forskellige ISO- eller UIC-standarder, udførelse af en arbejdsbyrde- og træthedshåndteringsanalyse for at sikre, at personalet er i stand til at udføre opgaven, udføre risikoanalyser for at identificere potentielle problemer og identificere afhjælpende foranstaltninger. Der tages højde for både miljøfaktorer som sne, varme, regn osv. og for socioøkonomiske faktorer som organisatoriske prioriteringer, indkøb og national kultur.

Ledelsen viser gennem dokumenterede sikkerhedsrunderinger eller besøg på arbejdsstedet sin forpligtelse til at fremme en positiv sikkerhedskultur og dens ønske om at gå foran med sit eksempel.

2.1.6 Referencer og standarder

- [Sikkerhedskultur](#) (SKYbrary)

2.1.7 Tilsynsspørgsmål

Omfanget af enhver uoverensstemmelse mellem politikker og procedurer, der hører med til ovennævnte dokumentation, og den observerede virkelighed i forbindelse med tilsynet, samt i hvilket omfang organisationen er klar over denne uoverensstemmelse, er vigtige spørgsmålet ved tilsynet.

Omfanget af lederskabets faktiske forpligtelse i forhold til sikkerhedsledelsessystemet og fremme af sikkerhedskulturen samt medarbejdernes forpligtelse i forhold til organisationen bør testes i forbindelse med tilsynet ved at undersøge organisationens egne mekanismer til at forstå og udvikle denne kultur og sikkerhedsledelsessystemet.

Kontrol af, at organisationen kan påvise, at der sættes tilstrækkelige ressourcer af til udvikling, implementering, vedligeholdelse og løbende forbedring af sikkerhedsledelsessystemet.

Kontrol af, ved at interviewe den øverste ledelse og andet personale, hvordan ledelsen udtrykker sin forpligtelse i forhold til at forbedre sikkerheden. Finde ud af, hvor ofte og på hvilke måder de er i kontakt med personalet om sikkerhedsmæssige spørgsmål og/eller i forbindelse med fremme af en sikkerhedskultur (workshops, fora, særlige sikkerhedsdage osv.).

Kontrol af, om der er kommunikation fra den øverste ledelse med hensyn til mål, enten ved at de opfordrer alle medarbejdere til at bidrage til, at målene nås, eller ved at de takker alle for en forbedret indsats.

2.2 Sikkerhedspolitik

2.2.1 Lovkrav

- 2.2.1. Et dokument, der beskriver organisationens sikkerhedspolitik, er fastlagt af den øverste ledelse, og det er:
- (a) tilpasset typen, **karakteren** og omfanget af organisationens jernbanedrift
 - (b) godkendt af organisationens administrerende direktør (eller en eller flere repræsentanter for den øverste ledelse)
 - (c) aktivt implementeret, formidlet til og gjort tilgængeligt for hele personalet.
- 2.2.2. Sikkerhedspolitikken skal:
- (a) omfatte en forpligtelse til at overholde al lovgivning og andre sikkerhedsrelaterede krav
 - (b) sætte en ramme for at fastlægge sikkerhedsmål og evaluere organisationens sikkerhedsniveau i forhold til disse målsætninger
 - (c) omfatte en forpligtelse til at styre sikkerhedsrisici, hidrører fra egne aktiviteter som dem, der forårsages af andre
 - (d) omfatte en forpligtelse til løbende forbedringer af sikkerhedsledelsessystemet
 - (e) vedligeholdes i overensstemmelse med forretningsstrategien og evalueringen af organisationens sikkerhedsniveau.

2.2.2 Formål

Sikkerhedspolitikken er et vigtigt dokument til at vise, hvordan organisationen varetager sit sikkerhedsansvar og sit lederskab og forpligtelse i forhold til korrekt sikkerhedsledelse. Ansøgerne skal være i stand til at vise, at de har en sikkerhedspolitik, som opfylder ovenstående krav, og som giver en sammenfattende beskrivelse af den grundlæggende risikostyringsstruktur.

2.2.3 Forklarende noter

Sikkerhedspolitikken er et udtryk for ledelsens filosofi, og derfor er dette afsnit tæt forbundet med afsnit 3.1. F.eks. nævner lovkravet ovenfor ikke de menneskelige og organisatoriske faktorer direkte.

I punkt 2.2.1 (a), i ovennævnte juridiske tekst erstattes "type" af "karakter" de steder, hvor kravet vedrører infrastrukturforvaltere.

2.2.4 Dokumentation

- *For en jernbanevirksomhed: En skriftlig sikkerhedspolitik, som er underskrevet af den administrerende direktør, og som afspejler driftens type og omfang, underbygger overholdelsen af lovkravene og andre krav, sikrer en løbende forbedring af sikkerheden og udgør en ramme for fastlæggelsen af sikkerhedsmål (2.2.1 (a), (b)), (2.2.2 (a-c)).*
- *For en infrastrukturforvalter: En skriftlig sikkerhedspolitik, som er underskrevet af den administrerende direktør og afspejler jernbanedriftens karakter og omfang samt infrastrukturudviklingen, underbygger overholdelsen af lovkravene og andre krav, sikrer en løbende forbedring af sikkerheden og anvendes til at fastlægge sikkerhedsmål (2.2.2 (a-c)).*

- *For begge: Oplysninger, som angiver, at sikkerhedspolitikken er kommunikeret til hele personalet (2.2.1 (c)).*
- *Oplysninger om, at sikkerhedspolitikken vedligeholdes, så den altid er i overensstemmelse med organisationens forretningsstrategi (2.2.2 (d)).*
- *Dokumentation for, at sikkerhedspolitikken indeholder en forpligtelse til at overvåge sikkerhedsindsatsen og gennemgås regelmæssigt efter en analyse af sikkerhedsindsatsen samt ændres efter en gennemgang af organisationens sikkerhedsindsats i forhold til de opstillede mål. (2.2.2(b), (d))*

2.2.5 Eksempler på dokumentation

En sikkerhedspolitik, som er underskrevet og dateret af den administrerende direktør og nøjagtigt afspejler driftens type, omfang og karakter. I dokumentet gives der udtryk for forpligtelsen til løbende forbedring af sikkerhedsledelsessystemet.

Sikkerhedspolitikken gennemgås løbende efter en fastlagt cyklus, som er tilpasset forretningsstrategien.

Sikkerhedsmålene er i tråd med missions- og visionserklæringerne i sikkerhedspolitikken. De er kendt af medarbejderne, som er forpligtet til at arbejde for at nå målene.

Sikkerhedspolitikken indeholder oplysninger om eller henvisninger til processen for, hvordan den revideres for at undersøge, om der er behov for ændringer efter en gennemgang af organisationens sikkerhedsindsats i forhold til de opstillede mål.

Der eksisterer en proces for kommunikationen af sikkerhedspolitikken via organisationens intranet og visning af sikkerhedspolitikken på strategiske/operationelle steder.

2.2.6 Tilsynsspørgsmål

Under tilsynet er det vigtigt at teste, hvor godt sikkerhedspolitikken er kommunikeret til og forstået af hele personalet, og hvilken rolle den reelt spiller for tilvejebringelse af de sikkerhedsrammer, som organisationen arbejder inden for. Et vigtigt spørgsmål er, om dokumentet hjælper med at sætte dagsordenen eller blot eksisterer, fordi det er et lovkrav.

Kontrol af, at ændringer i organisationens sikkerhedsindsats har udløst en gennemgang af sikkerhedspolitikken.

Kontrol af, at sikkerhedspolitikken afspejler organisationens virkelighed.

2.3 Organisatoriske roller, ansvarsområder, ansvarlighed og bemyndigelser

2.3.1 Lovkrav

- 2.3.1. Ansvarsområder, ansvarlighed og bemyndigelser for personale, der varetager en rolle af sikkerhedsmæssig betydning (herunder ledelsen og andet personale, der medvirker i sikkerhedsrelaterede opgaver) skal fastlægges for alle niveauer i organisationen, dokumenteres over for, tildeles og formidles til personalet.
- 2.3.2. Organisationen skal sikre, at personale med delegeret ansvar for sikkerhedsrelaterede opgaver har bemyndigelse, kompetence og tilstrækkelige ressourcer til at varetage sine opgaver uden, at det berøres negativt af andre forretningsfunktioners aktiviteter.
- 2.3.3. Delegering af ansvar for sikkerhedsrelaterede opgaver skal dokumenteres og formidles til det relevante personale, som skal acceptere og forstå opgaverne.
- 2.3.4. Organisationen skal beskrive fordelingen af roller, der er omhandlet i afsnit 2.3.1, på forretningsfunktioner i og - hvor det er relevant - uden for organisationen (jf. 5.3. Kontrahenter, partnere og leverandører).

2.3.2 Formål

Formålet med dette krav er at få ansøgeren til at give et klart billede af organisationens opbygning og af, hvordan roller og ansvar tildeles og opretholdes over tid, lige fra frontlinjepositionerne til den øverste ledelse. Dette er afgørende for at forstå, hvor godt organisationens sikkerhedsledelsessystem styrer risiciene. Ansøgerne bør påvise, hvordan personale får tildelt aktiviteter, hvordan det sikres, at de pågældende har en klar forståelse af deres roller og ansvarsområder, og hvordan de bliver holdt ansvarlige for deres indsats.

2.3.3 Forklarende noter

Der kan være en kløft i forståelsen mellem sikkerhedsledelsesbestemmelserne på et driftsmæssigt plan og de ledelsesprocesser, der skal styre sikkerhedsledelsessystemet (f.eks. risikovurdering og overvågning). Identifikationen af relevante roller inden for sikkerhedsledelsessystemet (**2.3.1**) er ikke begrænset til dem, der er ansvarlige for ledelsen af sikkerhedsprocesserne såsom sikkerhedschefen eller sikkerhedsteamet, men omfatter alle roller, der er involveret i sikkerhedsrelaterede opgaver, f.eks. driftspersonalet, uanset om de har en ledende stilling i organisationen eller ej (dvs. de øverste ledere, funktionsledere og andre medarbejdere).

Udveksling af sikkerhedsrelaterede oplysninger bør sikres inden for roller, ansvarsområder, ansvarlighed og bemyndigelser (**2.3.1**). For eksempel hvem der er ansvarlig for at udsende meddelelser om sene ændringer til lokomotivførere. (jf. også **4.4.1** og **4.4.2**).

Sikkerhedsledelsessystemet bør være i overensstemmelse med CSM SMS (**1.1.1 (d)**), og den øverste ledelse er ansvarlig for at sikre, at sikkerhedsledelsessystemet overholder kravene. Den øverste ledelse kan delegerer nogle af sine ansvarsområder til relevant personale. Rapportering af indsatsen foretages i henhold til kravene til ledelsens evaluering (6.3), hvor relevant personale er ansvarligt for at rapportere sikkerhedsledelsessystemets resultater til den øverste ledelse.

"Sikkerhedsrelaterede opgaver" (**2.3.1**) er ikke begrænset til de opgaver, hvor sikkerheden håndteres direkte (dvs. sikkerhedskritiske opgaver, som udføres af medarbejderne, når de styrer eller påvirker et togs bevægelser, og som kan påvirke personers sundhed og sikkerhed som angivet i TSI OPE). Det omfatter også ikke-driftsmæssige opgaver, der påvirker sikkerheden.

Ved "delegering" (**2.3.3**) forstås overførsel af ansvar fra et højere til et lavere beføjelsesniveau, sædvanligvis med det formål at fremskynde organisationens reaktion på spørgsmål, der opstår. Sikkerhedsansvar kan delegeres, dvs. gives videre nedad i hierarkiet, inden for rammerne af de fastlagte ansvarsområder for jobbet,

forudsat at sådan delegering dokumenteres. Ansvarlighed på sikkerhedsområdet kan ikke delegeres. Hvis noget ikke bliver gjort, ikke virker eller ikke når sit mål, definerer sikkerhedsansvaret den ansvarlige persons forpligtelse til at påvise tilfredsstillende efterlevelse af sit sikkerhedsansvar. Kommunikation og accept af opgaver **(2.3.3)**, herunder sikkerhedsrelaterede opgaver, hører med til den normale forretningsgang for, hvordan personalet tildeles funktioner, og dette bør være genstand for audit.

Tildelingen af roller **(2.3.4)** kan påvises ved at fremlægge et passende organisationsdiagram.

Ledelsen bør have relevant viden om og forståelse af menneskelige og organisatoriske faktorer til at sikre, at specialister inddrages efter behov. Roller, ansvarsområder og ansvarlighed hos specialister inden for menneskelige og organisatoriske faktorer bør fastlægges i forhold til de opgaver, der skal udføres. **(2.3.3)**.

Der bør være en proces, som sikrer, at personer kan indberette nærvæd-fejl, hændelser og ulykker uden at skulle frygte konsekvenser. Politikken støtter den enkeltes ret og pligt til at gøre opmærksom på sikkerhedsproblemer og tolererer ikke chikane, intimidering, gengældelse eller diskrimination som følge heraf. Nøglen til succes for en åben rapporteringskultur er tillid og åbenhed i organisationen. Dette opbygges løbende og afhænger af ledelsens vilje til at foretage omfattende analyser, når hændelser og ulykker har fundet sted, og til at lytte og lære, inden der reageres. Konsekvens i håndteringen af sikkerhedsspørgsmål er vigtigt for opnåelsen af en åben rapporteringskultur.

2.3.4 Dokumentation

- *Et organisationsdiagram og relevant forklarende tekst, som viser organisationens opbygning og den måde, sikkerhedsledelsessystemet er tilrettelagt på, samt hvordan det hænger sammen med organisationens kontekst **(2.3.1)**, **(2.3.4)**.*
- *En liste over andre oplysninger, der giver en detaljeret oversigt over sikkerhedsansvaret inden for organisationens struktur **(2.3.1)**, **(2.3.3)**.*
- *Dokumentation for, at et kompetencestyringssystem til vurdering af, hvorvidt opgaverne er passende i forhold til de tildelte ansvarsområder, kompetencer og ressourcer, er indført og opretholdes for alle medarbejdere **(2.3.2)**.*
- *Dokumentation fra kompetencestyringssystemet eller andre procedurer for, at organisationen sikrer, at roller og ansvar kommunikerer til, accepteres af og klart forstås af personalet, og at de vil blive holdt ansvarlige for at udføre dem **(2.3.3)**.*
- *En beskrivelse af ansvaret for drift og vedligeholdelse, herunder en definition af de krav, som personale og kontrahenter (alt efter relevans) bør overholde **(2.3.4)**.*
- *Strategien for menneskelige og organisatoriske faktorer bør påvise kravene til, hvornår og hvordan eksperter inden for menneskelige og organisatoriske faktorer involveres, og hvad deres roller og ansvarsområder er **(2.3.1)**, (jf. også 4.6).*

2.3.5 Eksempler på dokumentation

Et organisationsdiagram ledsaget af yderligere tekst, som gør det muligt for vurderingspersonen at se, hvordan sikkerhedsledelsessystemet er opbygget, og hvordan dets forskellige dele hænger sammen med hinanden.

Processen for, hvordan sikkerhedsansvarsområder tildeles, og hvor delegering er tilladt, med eksempler på hvordan processen har fungeret.

Eksempler på jobbeskrivelser for sikkerhedsrelaterede opgaver, også dem, der ikke er direkte involveret i driften, og som har indirekte indflydelse på driftens udførelse (dvs. tildeling af opgaver, planlægning af driften, kommunikation af driftsmæssige oplysninger til personalet og tilsyn med driften).

En henvisning til kompetencestyringssystemet med oplysninger om, hvordan det er opbygget, og links til, hvor der kan findes nærmere oplysninger.

Den feedbackproces, der anvendes til at sikre, at oplysninger, som er videregivet i organisationen, er klart

forstået.

Proceduren eller procedurerne for fastlæggelsen af, hvilke kompetencer og ressourcer der er nødvendige for at understøtte sikkerhedsopgaver og -ansvarsområder på alle niveauer i hierarkiet.

Strategien for menneskelige og organisatoriske faktorer viser, hvordan disse er en integreret del af processer og projekter. Ekspertise og aktiviteter i forbindelse med menneskelige og organisatoriske faktorer er passende i forhold til organisationens eller projektets størrelse. Roller, ansvarsområder og ansvarlighed samt stadierne for involvering af en specialist inden for menneskelige faktorer er defineret i proces- eller projektplanen.

2.3.6 Referencer og standarder

- [Ansvarlighed og ansvarsområder på sikkerhedsområdet](#) (SKYbrary)

2.3.7 Tilsynsspørgsmål

Hvad tilsyn angår, er de vigtigste spørgsmål her et gradsspørgsmål. Det spørgsmål, der skal besvares, er: "I hvilken grad afspejler de fremlagte oplysninger den reelle situation i praksis?"

En undersøgelse af, hvor godt kompetencestyringssystemet fungerer, vil give svarene på de fleste spørgsmål i dette afsnit.

2.4 Høring af personale og andre parter

2.4.1 Lovkrav

- | |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>2.4.1. Personalet, dets repræsentanter og eksterne interessenter skal, når det er relevant, høres angående udvikling, vedligeholdelse og forbedring af sikkerhedsledelsessystemets relevante dele, som de har ansvaret for, og herunder driftsprocedurernes sikkerhedsaspekter.</p> <p>2.4.2. Organisationen skal lette høringen af personalet ved at indføre metoder og midler at inddrage personalet, registrere personalets udtalelser og give feedback på personalets udtalelser.</p> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

2.4.2 Formål

Ansøgerne bør fremlægge dokumentation for, at de aktivt inddrager deres eget personale (eller deres repræsentanter) samt eksterne interessenter i sikkerhedsledelsessystemets anvendelse og udvikling for at styre risiciene løbende. Dette viser også vurderingsmyndigheden, hvordan sikkerhedskulturen i organisationen ser ud, og hvor aktivt de inddrager relevante tredjeparter i håndteringen af sikkerheden på områder, hvor risikoen deles.

Organisationen anerkender, at ingen enkeltpersoner selv er i besiddelse af alle de oplysninger, der er nødvendige for at håndtere sikkerheden på en holdbar måde. Procesekspertes, sikkerhedsekspertes, støttetjenester, frontlinjepersonale, ledelse, tilsynsførende, fagforeninger og eksterne kontrahenter har og bruger alle viden og oplysninger, der er vigtige for sikkerheden. De bør have mulighed for at mødes, diskutere og give udtryk for deres synspunkter for at få den bedst mulige forståelse af situationen på arbejdspladsen. De organisatoriske grænseflader mellem tjenesteydelser, afdelinger og organisationer kræver særlig opmærksomhed. Udveksling af idéer og oplysninger om analyse og behandling af risici, ulykker og hændelser bør fremmes.

Inddragelse i rapportering af sikkerhedskritiske oplysninger og deltagelse i analyse af farlige situationer og hændelser understøttes af et tillidsbaseret klima. Endvidere anmodes der aktivt om tidligt input fra driftspersonalet i forbindelse med udførelse af risikovurdering, udformning eller transformering af tekniske installationer og udarbejdelse af nye procedurer.

2.4.3 Forklarende noter

Disse eksterne parter (**2.4.1**) kan høres om spørgsmål, der vedrører sikkerhedsledelsessystemet. F.eks. kan kontrahenter være ansvarlige for visse sikkerhedsrelaterede opgaver såsom klargøring af tog eller vedligeholdelse af infrastruktur. I forbindelse med risikovurdering af togklargøringsproceduren og vedligeholdelse af infrastruktur er det god praksis at inddrage disse kontrahenter i processen.

Ved eksterne parter forstås organisationer, der har en grænseflade til ansøgeren såsom kontrahenter, partnere, leverandører, relevante myndigheder, herunder lokale myndigheder, og beredskabstjenester.

Udviklingen af en positiv sikkerhedskultur fremmes af god og rettidig kommunikation af relevante oplysninger til de personer, der har brug for dem.

2.4.4 Dokumentation

- *Ansøgeren bør fremlægge detaljerede oplysninger om processen for høring af personale (eller deres repræsentanter) og relevante eksterne parter, herunder hvordan disse høringer medfører ændringer af sikkerhedsledelsessystemet eller specifikke driftsprocedurer (**2.4.1**), (**2.4.2**).*
- *Ansøgeren bør fremlægge oplysninger om det system, der er indført til at give personalet feedback om høringens resultater (**2.4.2**).*

2.4.5 Eksempler på dokumentation

Processen eller proceduren for høring af personalet (og, hvis relevant, deres repræsentanter) samt eksterne parter ved udvikling af sikkerhedsledelsessystemet.

Eksempler på referater af høringsmøder afholdt med personalet (og/eller deres repræsentanter) med en fortegnelse over resultater.

Eksempler på, hvordan udtalelser og forslag fra personalet indhentes i forbindelse med håndtering af ændringer (dvs. vedrørende et udkast til, en ændret eller en ny driftsprocedure), og hvordan de håndteres.

Et dokument eller en procedure, der viser, hvordan driftspersonalet, som skal håndtere et nyt eller udviklet teknisk system, bliver involveret på et tidligt tidspunkt (planlægning og udvikling) af arbejdet med henblik på at samle input, f.eks. om grænsefladen mellem menneske og maskine.

Der er procedurer, som angiver, hvordan de menneskelige og organisatoriske faktorer bør håndteres, og resultaterne kommunikeres inden for organisationen, hvad angår organisationens forretningsmål og organisatoriske processer, f.eks. projekter, undersøgelser af ulykker og hændelser, risikoanalyser og andre sikkerhedsrelaterede aktiviteter for organisationens eget personale, kontrahenter, partnere og leverandører.

Organisationen bør tydeligt definere sikkerhedsforventninger og nødvendig adfærd tydeligt. Organisationens prioriteringer tilpasses hinanden for at undgå modsatrettede mål. Der beskrives en proces for planlægning, risikovurdering og styring af aktiviteterne for at sikre, at sikkerheden ikke kompromitteres af andre forretningsinteresser, f.eks. ved hjælp af konservativ beslutningstagning. Sikkerhedsmålene er forbundet med sikkerhedskulturen. Ledelsen spiller en aktiv rolle i planlægningen og gennemførelsen af nødvendige ændringer af sikkerhedskulturen.

2.4.6 Tilsynsspørgsmål

Høring og inddragelse af relevant personale både internt og eksternt er en vigtig del af at sikre, at personer med relevant erfaring er i stand til at sætte et positivt aftryk på organisationens sikkerhedsledelsessystem.

Tilsynet på dette område bør være målrettet mod dokumentationen for, hvordan personale og eksterne parter høres, og deres bemærkninger tages i betragtning, og bør også dække dokumentationen for de

ændringer af sikkerhedsledelsessystemet, som dette medfører.

Der bør lægges særlig vægt på, hvordan der gives feedback, og hvordan læring opnås heraf.

3 Planlægning

3.1 Tiltag med henblik på at imødegå risici

3.1.1 Lovkrav

3.1.1. Risikovurdering

3.1.1.1. Organisationen skal:

- (a) udpege og analysere alle driftsmæssige, organisatoriske og tekniske risici af relevans for typen (*karakteren*), omfanget og området af den drift, som organisationen udfører. Sådanne risici skal omfatte menneskelige og organisatoriske faktorer som f.eks. arbejdspress, jobtilrettelæggelse, træthed eller procedurers egnethed og andre interessenters aktiviteter (jf. 1. Organisationens kontekst)
- (b) evaluere de i litra a) nævnte risici ved at anvende tilstrækkelige risikovurderingsmetoder
- (c) udvikle og iværksætte sikkerhedsforanstaltninger med udpegning af tilhørende ansvarsområder (jf. 2.3. Organisatoriske roller, ansvarsområder, ansvarlighed og bemyndigelser)
- (d) udvikle et system med henblik på at overvåge sikkerhedsforanstaltningerne effektivitet (jf. 6.1. Overvågning)
- (e) anerkende behovet for samarbejde med andre interessenter (f.eks. jernbanevirksomheder, infrastrukturforvaltere, fabrikker, vedligeholdelsesvirksomheder, enheder med ansvar for vedligeholdelse, ihændehavere af jernbanekøretøjer, leverandører af tjenesteydelser og ordregivere), når dette er relevant, om delte risici og iværksættelse af tilstrækkelige sikkerhedsforanstaltninger
- (f) kommunikere om risici til personalet og involverede eksterne parter (jf. 4.4. Information og kommunikation).

3.1.1.2 Når en risiko vurderes, skal en organisation tage hensyn til behovet for at fastslå, tilvejebringe og opretholde et sikkert arbejdsmiljø, der overholder gældende lovgivning, navnlig direktiv 89/391/EØF.

3.1.2. Planlægning af ændringer

3.1.2.1. Organisationen skal udpege potentielle sikkerhedsrisici og tilstrækkelige sikkerhedsforanstaltninger (jf. 3.1.1. Risikovurdering) inden en ændring gennemføres (jf. 5.4. Styring af ændringer) i henhold til den risikostyringsproces, der er fastlagt i forordning (EU) nr. 402/2013, herunder overvejes sikkerhedsrisici hidrørende fra selve ændringsprocessen.

3.1.2 Formål

Dette krav vedrører selve essensen af sikkerhedsledelsessystemet. Det har til formål at få ansøgerne til at vise, hvordan deres systemer identificerer og styrer de risici, de står over for. Det kræves også, at ansøgerne viser, hvordan de i praksis bruger resultaterne af risikovurderingen til at forbedre risikostyringen, og hvordan de tjekker dette løbende. Det er vigtigt at huske, at dette krav ikke drejer sig direkte om håndtering af risici som følge af ændringer (hvilket er et andet krav), men er relateret til det. Det bør også bemærkes, at der er et særligt krav at tage højde for via risikovurderingen vedrørende den menneskelige ydeevne såsom risikostyring i forbindelse med arbejdets tilrettelæggelse og træthed.

Ansøgeren bør i ansøgningen beskrive, hvordan denne information tilrettelægges og kommunikeres som en

del af sikkerhedsledelsessystemet, og indholdet bør afspejle de risici, som organisationen er udsat for i betragtning af driftens type, omfang og område (jf. organisationens kontekst). Det er hensigtsmæssigt at medtage både de risici, som hører under ansøgerens ansvar, og de risici, som tredjeparters aktiviteter medfører.

En fælles forståelse i hele organisationen af, hvordan større risici forebygges, betragtes som en prioritet for god sikkerhedsledelse. Et scenarios lave hyppighed bør ikke føre til, at det ignoreres. For at sikre, at et valgt risikovurderingsscenarie er realistisk i forhold til de reelle aktiviteter, bør både sikkerhedsledelseksperter og operatører i den mest kritiske del af virksomheden bidrage til sikkerhedsanalysen og risikovurderingen. Resultaterne af disse vurderinger kommunikeres i et tilgængeligt og forståeligt format til alle de aktører, der bidrager til sikkerheden. Bestyrelsen og ledelsen fremmer diskussioner om store risici, der skal håndteres, for at sikre fælles forståelse og kendskab. Desuden understreges eksistensen af store risici i hele systemets livscyklus.

3.1.3 Forklarende noter

Med henblik på vurdering af ansøgningen bør ansøgerne vise, hvordan de overholder Rådets direktiv 89/391/EØF og de hertil knyttede forordninger. Vurderingen vil fokusere på at det påvises, at disse forhold håndteres, og ikke på forholdene i sig selv. Forhold som trætheds- eller stresshåndtering såvel som test af fysisk og psykisk egnethed kan håndteres som et juridisk spørgsmål inden for rammerne af sundhed og sikkerhed på arbejdspladsen. De berører dog også kompetencestyringssystemet (f.eks. uddannelse efter langvarigt fravær) og opgavetildelingen (medarbejdere bør kun tildeles bestemte opgaver, hvis det fastslås, at de er egnede til dem), som anført i TSI OPE.

I punkt 3.1.1.1 (a), i ovennævnte juridiske tekst erstattes "type" af "karakter" de steder, hvor kravet vedrører infrastrukturforvaltere, for så vidt angår vurdering.

"Aktiviteter" (**3.1.1.1 (a)**) betyder i den forbindelse både de handlinger, som interessenter (kontrahenter, leverandører og andre) udfører på vegne af eller sammen med en ansøger, og de aktiver, der anvendes til støtte for disse handlinger. Det væsentlige er, at ansøgerne skal påvise, at de har en solid proces for risikovurdering, og at alle relevante risici bliver adresseret. Nogle risici (f.eks. hydrogeologiske risici, risici ved jernbaneoverkørsler, sten kastet på togene, og uvedkommende på jernbanearealerne) skal også tages i betragtning af organisationen, når det er hensigtsmæssigt og rimeligt. Disse forhold er dog relateret til driftsmæssige risici (eftersom de alle vedrører togdriften) og kan ikke kun være relateret til den menneskelige ydeevne.

"Andre interessenter" betegner både organisationer og enkeltpersoner. Der kan være tale om parter uden for jernbanesystemet (**1.1.1 (c)**).

En ændring kan være sikkerhedsrelateret eller ej (**3.1.2.1**). Indvirkningen af alle sikkerhedsrelaterede ændringer bør vurderes, og relevante sikkerhedsforanstaltninger til reduktion af de relaterede risici til et acceptabelt niveau bør identificeres. Gennemførelsen af ændringshåndteringsprocessen kan også føre til sikkerhedsrisici, navnlig når det beslutes at udsætte gennemførelsen af en ændring, hvis dette er nødvendigt for helt eller delvist at undgå, at der opstår en anden sikkerhedsrisiko. Risikostyring (**3.1.1.1**) vedrører dog ikke kun ændringsstyring. Organisationens bør generelt sikre, at sikkerhedsrisiciene i forbindelse med driften styres i passende omfang. Nødvendigheden af at identificere, håndtere og styre disse sikkerhedsrisici, som et led i ansøgerens sikkerhedsledelsessystem, rækker således ud over blot at håndtere ændringer og anvende CSM for risikoevaluering og -vurdering.

CSM for risikoevaluering og -vurdering gælder for alle tekniske, driftsmæssige og organisatoriske ændringer (hvad sidstnævnte angår, ændringer med drifts- eller vedligeholdelsesmæssige konsekvenser). For hver sikkerhedsrelateret ændring skal ansøgeren/forslagsstilleren først beslutte, om ændringen er signifikant (eller ej). Hvis den vurderes som signifikant, skal det påvises, at risiciene i forbindelse med ændringen er acceptable, hvilket sker ved hjælp af principperne i denne CSM, og at kravene som følge af denne påvisning er blevet gennemført på en effektiv måde i det system, der skal ændres. Herefter vurderes den udførte risikovurdering af et uafhængigt vurderingsorgan eller anerkendt organ, som skriver en rapport om, hvorvidt analysen er

acceptabel eller ej. De nationale sikkerhedsmyndigheder vil tage hensyn til sådanne rapporter i deres tilsynsaktiviteter, men de kan ikke drage rapportens resultater i tvivl, medmindre de har grund til at tro, at processen med at vurdere risikovurderingen ikke er blevet fulgt korrekt. Hvis ændringen er sikkerhedsrelateret, men ikke signifikant, skal ansøgeren/forslagsstilleren dokumentere sin beslutning og skal stadig risikovurdere ændringen i henhold til risikostyringsprocessen i sikkerhedsledelsessystemet. I så fald er det ansøgerens ansvar at vælge de korrekte risikovurderingsmetoder til at begrunde, at de indførte risikokontrolforanstaltninger er tilstrækkelige til at styre de relaterede risici og give dem et acceptabelt niveau. Det skal bemærkes, at selv om det, der udløser anvendelsen af CSM for risikoevaluering og -vurdering, er, om en ændring er signifikant eller ej, kan en organisation vælge at anvende CSM for risikoevaluering og -vurdering under alle omstændigheder, f.eks. hvis den mener, at ændringen af kommercielle eller samfundsmæssige grunde fortjener en uafhængig vurdering af det arbejde, som organisationen har udført.

CSM for risikoevaluering og -vurdering omfatter seks kriterier, som bør undersøges for at fastslå "signifikansen". De er:

- **konsekvens af svigt:** *et plausibelt, værst tænkeligt scenarie i tilfælde af svigt i det system, der er under vurdering, under hensyntagen til sikkerhedsbarrierer uden for systemet*
- **nyskabelser, der anvendes til at gennemføre ændringen:** *dette gælder både for det, der er innovativt for jernbanesektoren, og det, som alene er nyt for den organisation, der gennemfører ændringen*
- **ændringens kompleksitet**
- **overvågning:** *manglende evne til at overvåge den gennemførte ændring i systemets samlede livscyklus og foretage hensigtsmæssige indgreb*
- **reversibilitet:** *manglende evne til at vende tilbage til systemet, som det var før ændringen, og*
- **akkumulation:** *vurdering af ændringens signifikans under hensyntagen til alle nylige sikkerhedsrelaterede ændringer, som ikke blev anset for signifikante, af det system, der er under vurdering.*

Disse elementer bruges til at vurdere, hvordan organisationernes beslutninger om "signifikans" i henhold til CSM for risikoevaluering og -vurdering er blevet truffet.

Selv om risikostyringsprocessen i CSM for risikoevaluering og -vurdering er gældende i tilfælde af sikkerhedsrelaterede og signifikante ændringer, er principperne bag den risikostyringsproces, som er vedtaget i forordningen, almindelig praksis ved risikostyring og kan derfor finde anvendelse i alle andre situationer, hvor der er behov for risikostyring.

Tilgangen til identifikation af sikkerhedskritiske arbejdsopgaver og -processer er systematisk, og der benyttes metoder, som vedrører menneskelige og organisatoriske faktorer, til at analysere sikkerhedskritiske arbejdsopgaver, f.eks. opgaveanalyse, HTA (hierarkisk opgaveanalyse) og TTA (tabellarisk opgaveanalyse). Der bør anvendes professionel ekspertise inden for menneskelige og organisatoriske faktorer ved udvælgelsen og anvendelsen af egnede metoder.

Risikovurderingsprocessen bør beskrive involveringen af specialister inden for menneskelige og organisatoriske faktorer og relevante kompetencer for brugerne og andre interessenter. Dette kunne f.eks. omfatte en beskrivelse af, i hvilken udstrækning specialister inden for menneskelige og organisatoriske faktorer bør involveres i risikoanalysen, og hvilket kompetenceniveau for de menneskelige og organisatoriske faktorer der er brug for.

Egnede metoder til at integrere menneskelige og organisatoriske faktorer i risikovurderingen beskrives, f.eks. opgaveanalyse, brugbarhedsanalyse, simulering, menneskelig HAZOP-analyse og "bow-tie"-analyse.

3.1.4 Dokumentation

- Ansøgerne bør fremlægge dokumentation for, at de har indført en risikovurderingsproces (herunder en beskrivelse af de anvendte metoder, det involverede personale og enhver validering eller verifikation, der er foretaget), som både omfatter de risici, der er identificeret som signifikante ændringer i henhold til CSM for risikoevaluering og -vurdering (Kommissionens gennemførelsesforordning (EU) 402/2015), og de risici, der betragtes som ikke-signifikante, men som bør styres alligevel, og processen omfatter alle driftsrisici, organisatoriske og tekniske risici **(3.1.1.1.(a),(b))**.
- Dokumentation for, at der er taget højde for risici, som vedrører menneskelige og organisatoriske faktorer, i risikovurderingerne. Strategien for menneskelige og organisatoriske faktorer bør vise, hvordan og hvornår menneskelige og organisatoriske faktorer er en integreret del af risikovurderingsvurderingen og vise brugen af passende metoder og ekspertise **(3.1.1.1(a))**.
- Dokumentation for den måde, relevante tredjeparter er involveret i risikoprocessen på, hvor det er relevant, herunder hvordan risici fra tredjeparter, der berører jernbanevirksomheders eller infrastrukturforvalteres aktiviteter, bliver styret **(3.1.1.1(a)), (3.1.1.1(c)), (3.1.1.1(f))**.
- Dokumentation for, at ansøgerne har indført en proces til at udvikle og iværksætte risikokontrolforanstaltninger, herunder en angivelse af, hvem der er ansvarlig for deres gennemførelse **(3.1.1.1 (c))**.
- Ansøgerne bør angive, hvordan de involverer relevant personale og kommunikerer resultaterne af risikovurderingen og de hermed forbundne kontrolforanstaltninger til det relevante personale **(3.1.1.1(f))**.
- Ansøgerne bør påvise, hvordan de overvåger risikokontrolforanstaltningernes effektivitet, herunder hvordan processer eller procedurer opdateres som påkrævet **(3.1.1.1 (d))**.
- I den fremlagte dokumentation bør ansøgerne angive, hvordan de tager højde for kravet om at overholde anden gældende lovgivning såsom Rådets direktiv 89/391/EØF **(3.1.1.2)**.
- Ansøgerne fremlægger dokumentation for, at indvirkningen af enhver ændring systematisk evalueres, som et led i ansøgerens ændringshåndteringsproces. Dette indebærer brug af risikovurdering, herunder brug af CSM for risikoevaluering og -vurdering med henblik på at identificere risiciene og de nødvendige kontrolforanstaltninger. Ansøgerne fremlægger også dokumentation for, at de kontrolforanstaltninger, der er identificeret under ændringshåndteringsprocessen, er blevet gennemført **(3.1.2.1)**.

3.1.5 Eksempler på dokumentation

En risikovurderingsproces eller -procedure, som efter behov beskriver, hvordan og hvornår der anvendes en fejlmulighed- og effektanalyse (FMEA), en fare- og funktionsevneanalyse (HAZOP) eller andre teknikker til at støtte gennemførelsen af kontrolforanstaltninger for at adressere risici.

Dokumentation som for eksempel et fareregister, som viser, at organisationen har indført en proces til systematisk vurdering af farer som første trin i styringen af risici, og som tilføjes resultaterne af overvågningen, straks opdateres, når nye risici opdages, og suppleres med relevant information om indførte sikkerhedsforanstaltninger til styring af risici (f.eks. teknisk udstyr, driftsprocedurer, uddannelse af personale).

En oversigt over proceselementerne for, hvordan der tages højde for menneskelige faktorer i risikovurderingsprocessen, og hvordan og hvor nødvendige tredjeparter involveres.

Procedure for, hvordan resultaterne af risikovurderingerne kommunikerer til personalet, evt. med illustrative eksempler.

Procedure for overholdelse af anden relevant EU-lovgivning såsom Rådets direktiv 89/391/EØF, for så vidt som personalerelaterede risici (dødsfald, forbigående eller permanente skader, nærved-hændelser) kan være omfattet af lovgivningen om sundhed og sikkerhed på arbejdspladsen. Kontrolforanstaltningerne bør dog være medtaget i eller supplere driftsreglerne.

Angivelse af en proces, der sikrer, at sikkerhedsrelaterede opgaver, som delegeres til hver enkelt

personalekategori, er udformet på en sådan måde, at:

- *mængden af opgaver, der skal udføres, ikke er for stor på de tidspunkter, hvor en sikkerhedsrelateret opgave udføres*
- *organisationen, hvis sikkerhedsrelaterede opgaver kombineres, er i stand til at påvise, at sikkerhedsniveauet opretholdes*
- *der ikke er et modsætningsforhold mellem udførelsen af sikkerhedsrelaterede opgaver og andre mål, som er fastsat for personalet (jf. 2.1.1 (j)).*

En strategi omhandlende menneskelige og organisatoriske faktorer er forbundet med risikovurderingsprocessen. Det viser, at resultaterne fra risikoanalyserne anvendes, og at sikkerhedsforøgende foranstaltninger gennemføres og vurderes.

3.1.6 Referencer og standarder

- [Agenturets vejledning i anvendelse af CSM for risikovurdering](#)
- [Risk acceptance criteria for technical systems and operational procedures used in various industries](#)
- [Guideline supporting the implementation of \(EU\) Regulation 2015/1136 on harmonised design targets \(CSM DT\) in the scope of the CSM on risk assessment](#)
- *ISO 31000:2018 Risikostyring*
- *ISO 31010:2019 Risikostyring — Teknikker til risikovurdering*

3.1.7 Tilsynsspørgsmål

Risikovurderingsprocessen bør have en central plads i sikkerhedsledelsessystemet, når der foretages tilsyn, og derfor bør det ud fra interviews og kontroller af dokumentation og processer være muligt at tjekke, om dette reelt er tilfældet. Af afgørende vigtighed i den forbindelse er eventuelle tilsynsresultater, som vil være relevante for den kommende fornyelse af et EU-sikkerhedscertifikat eller en sikkerhedsgodkendelse. Desuden bør eventuelle resultater fra tilsynet med risikovurderingsprocesserne efter behov udgøre et input til den nationale sikkerhedsmyndigheds tilsynsstrategi.

Følgende oplysninger kan fungere som input i forbindelse med senere tilsyn:

- *fareliste*
- *resultaterne af risikoanalysen, herunder rapporter fra risikovurderingsorganet eller -organerne, hvis relevant*
- *en begrundelse for brugen af risikovurderingsmetoder (f.eks. FMECA, FTA, ETA eller HAZOP), herunder en begrundelse for, hvordan risikovurderingskriterierne fastlægges, og hvordan risikoens alvor og sandsynligheden for, at risikoen opstår, bestemmes*
- *hvis relevant en klassificering af farlige hændelser efter emne, konsekvenser eller årsager (f.eks. en foreløbig fareliste).*

Personale med ansvarsområder, som er forbundet med risikovurdering, bør være bevidst om deres rolle og processens vigtighed og bør være i stand til at udføre den på en effektiv måde.

Det er navnlig vigtigt, at en række eksempler på risikovurdering bliver undersøgt, da de vil vise, om der tages tilstrækkeligt højde for risiciene ved hjælp af en passende metode. Herefter bør observationer i marken påvise, at de identificerede kontrolforanstaltninger er på plads.

3.2 Sikkerhedsmål og -planlægning

3.2.1 Lovkrav

- 3.2.1. Organisationen skal fastlægge sikkerhedsmål for relevante funktioner på relevante niveauer for at vedligeholde og, hvor det praktisk gennemførligt, at forbedre sit sikkerhedsniveau.
- 3.2.2. Sikkerhedsmålene skal:
 - (a) være i overensstemmelse med sikkerhedspolitikken og organisationens strategiske målsætninger (når dette er relevant)
 - (b) have sammenhæng med de prioriterede risici, der påvirker organisationens sikkerhedsniveau
 - (c) være målbare
 - (d) tage hensyn til gældende lovgivning og andre krav
 - (e) evalueres i forhold til de opnåede resultater og revideres, hvis det relevant
 - (f) formidles.
- 3.2.3. Organisationen skal have en plan eller flere planer, hvori det beskrives, hvordan den vil opfylde sine sikkerhedsmål.
- 3.2.4. Organisationen skal beskrive strategien og den plan eller de planer, der benyttes til at overvåge opfyldelsen af sikkerhedsmålene (jf. 6.1 Overvågning).

3.2.2 Formål

At sikre, at organisationen opfylder lovkravene, og at konceptet med løbende forbedring af sikkerheden kommunikerer til personalet og tages alvorligt af ledelsen.

Ansøgerne skal påvise, at de har meningsfyldte mål og en proces til at gennemføre og overvåge dem i hele deres livscyklus.

3.2.3 Forklarende noter

"Sikkerhedsniveau" betyder i denne sammenhæng organisationens indsats i forhold til sikkerhedsmålene samt resultaterne af sikkerhedsledelsessystemet og alle de processer og procedurer, der understøtter dette.

Den engelske term "safety objectives" anvendes synonymt med termen "safety targets", men sidstnævnte har som regel numerisk betydning. Sikkerhedsmål adskiller sig fra de fælles sikkerhedsmål (CST'er), der er fastlagt på medlemsstatsniveau. Nogle virksomheder kan dog bruge sidstnævnte som mål, der skal nås, for at opretholde eller forbedre deres sikkerhedsniveau.

Sikkerhedsmålene er knyttet til risici, da risiciene vil have indflydelse på organisationens sikkerhedsniveau (dvs. de tilsigtede resultater af sikkerhedsledelsessystemet og dermed succesen med at opfylde målene). Sikkerhedsmålene kan være kvantitative og være udtrykt som en reduktion af antallet af hændelser som en absolut værdi eller i procent. Sikkerhedsmålene kan også være kvalitative og være udtrykt som en generisk værdi, f.eks. at "sikkerheden i jernbaneoverkørsler skal forbedres", eller at "det nuværende sikkerhedsniveau skal opretholdes".

Målene bør gennemgås regelmæssigt ved hjælp af en tilgang, som omfatter planlægning, udførelse, kontrol og handling (PDCA), og der bør tages højde for resultaterne af risikovurderingen, tidligere overvågning samt undersøgelse af ulykker og hændelser, når der opstilles prioriteter med henblik på at opretholde og, når det er praktisk muligt, forbedre sikkerhedsniveauet.

Fastlæggelse og overvågning af sikkerhedsindikatorer, som underbygger organisationens beslutningstagning med hensyn til risikostyring, og hvorvidt disse indikatorer er effektive, giver input til opstillingen og gennemgangen af sikkerhedsmålene.

3.2.4 Dokumentation

- Der er SMARTe sikkerhedsmål, som passer ind i organisationens bredere forretningsbehov **(3.2.1), (3.2.2 (a), (b)), (c))**.
- Der er en angivelse af lovkravene, og hvordan de overholdes **(3.2.2 (d))**.
- Der er en beskrivelse af, hvordan disse mål kan opfyldes, og hvordan de kommunikeres til relevant personale **(3.2.2 (f)), (3.2.3)**.
- Der eksisterer en overvågningsproces, som er i overensstemmelse med kravene i CSM for overvågning (forordning EU) 1078/2012), for målene for at sikre, at de konsekvent er formålstjenlige, og at organisationen opfylder sine mål. **(3.2.2 e), (3.2.4)**.

3.2.5 Eksempler på dokumentation

Processen for, hvordan sikkerhedsmålene opstilles, prioriteres og overvåges, hvordan konflikter med andre mål undgås, og hvordan de løses, hvis de ikke kan undgås. Dette bør inkludere det niveau, hvorpå målene opstilles, og hvordan de bidrager til andre mål på andre niveauer, alt efter hvor dette er relevant. Det bør også inkludere grænsefladerne, timingen og andre nødvendige understøttende kvalitative eller kvantitative data.

Sikkerhedsmålene og planen for opfyldelsen af disse samt den proces, der skal følges, hvis det ser ud til, at sikkerhedsmålene ikke kan opfyldes.

Processen eller proceduren for at gøre resultaterne af overvågningsaktiviteter til sikkerhedsmål, handlingsplanen for at nå dem og de hermed forbundne indikatorer for opnåelsen.

3.2.6 Tilsynsspørgsmål

Et nøglespørgsmål i forbindelse med tilsynet er, i hvilken grad de opstillede mål kan opfyldes i praksis, og hvad der reelt sker, hvis det begynder at stå klart, at de sandsynligvis ikke opfyldes.

Hvordan sikkerhedsmålene opstilles og gennemgås — at der i målene fokuseres på sårbare eller kritiske aktiviteter/styring, og at der anvendes resultat- og aktivitetsindikatorer.

Hvordan organisationen påviser løbende forbedring i risikostyringen ved hjælp af sine sikkerhedsmål.

En evaluering af, om organisationen er i stand til at foretage effektiv overvågning af sit sikkerhedsniveau og dermed bruge CSM for overvågning til at vurdere indsatsen i forhold til sikkerhedsmålene og de hermed forbundne sikkerhedsindikatorer.

Man tager et eksempel på et mål (som f.eks. er fastlagt nogle år tidligere) og ser, om og hvordan det spores lige fra oprettelsen til den endelige opfyldelse (eller manglende opfyldelse).

4 Støtte

4.1 Ressourcer

4.1.1 Lovkrav

4.1.1. Organisationen skal tilvejebringe de nødvendige ressourcer, herunder kompetent personale og effektivt og anvendeligt udstyr, til at etablere, implementere, vedligeholde og løbende forbedre sikkerhedsledelsessystemet.

4.1.2 Formål

Formålet med dette krav er at sikre, at organisationen har indført processer til at tilvejebringe egnede ressourcer såsom teknisk udstyr eller systemer eller kompetent personale, således at organisationens sikkerhedsledelsessystem kan styre risikoen i overensstemmelse med målene.

4.1.3 Forklarende noter

Tildeling af egnede ressourcer er en forudsætning for at opnå et tilfredsstillende sikkerhedsniveau.

4.1.4 Dokumentation

- *Oplysninger om kompetencestyringssystemet (CMS) eller, såfremt der ikke er et kompetencestyringssystem, dokumentation for, hvordan organisationen sikrer, at den råder over egnet personale (4.1.1).*
- *Oplysninger om, hvordan organisationen sikrer, at den råder over tilstrækkeligt effektivt og egnet udstyr til at opfylde sine serviceforpligtelser og opretholde et effektivt sikkerhedsledelsessystem, som styrer risiciene (4.1.1).*
- *Oplysninger om tilrettelæggelsen af vedligeholdelsesfunktioner, og hvordan dette hænger sammen med tilvejebringelsen af egnede ressourcer til, at organisationen kan opfylde sine serviceforpligtelser (4.1.1).*

4.1.5 Eksempler på dokumentation

Angivelse af, hvordan kravene til personale fastlægges, således at sikkerhedsledelsessystemet fungerer effektivt, samt oplysning om relevante referenceprocedurer eller -processer, hvor der findes mere information.

Kompetencestyringsproceduren eller oplysninger om den proces, der skal sikre, at organisationen råder over kompetent personale i de relevante roller, med udførlige oplysninger om uddannelsesprogrammer alt efter behov (jf. også 4.2).

Angivelse af processen for ressourceallokering med henblik på at opfylde de driftsmæssige behov samt relevante henvisninger til støttedokumenter.

Et dokument, der fastlægger de tildelte ressourcer til planlagte store ændringer i organisationen (herunder vedrørende bemanning og levering af nødvendigt udstyr).

4.1.6 Tilsynsspørgsmål

Kontrol af, at kompetencerammen og udstyrskravene er klart forbundet med resultaterne af risikovurderingen.

Ved kontrollen af kompetencestyringssystemet bør den nationale sikkerhedsmyndighed tjekke, at organisationen råder over midler til at identificere og fastholde personale med de rigtige færdigheder, således at de kan udføre deres opgaver på en sikker måde. Det er af afgørende vigtighed, hvordan kompetencestyringssystemet opdateres.

Når de tilsynsførende ser på vedligeholdelsesaktiviteterne i forbindelse med dette krav, bør de tilstræbe at sikre, at jernbanevirksomheden eller infrastrukturforvalteren — når disse aktiviteter udliciteres — udfører sin tilsynsfunktion for at sikre, at kontrahenterne leverer et korrekt produkt, der er sikkert at bruge.

En undersøgelse af ledige stillinger inden for udvalgte områder af sikkerhedsledelsessystemet kan bruges som en indikator for, hvorvidt de menneskelige ressourcer er egnede eller ej.

På samme måde kan udstyrets anvendelse, f.eks. hvor mange reservedele der indkøbes, være en indikation

af det tilvejebragte udstyrs kvalitet og dermed ressourcernes egnethed.

4.2 Kompetence

4.2.1 Lovkrav

- 4.2.1. Organisationens kompetencestyringssystem skal sikre, at personale, der varetager en rolle, som påvirker sikkerheden, har kompetence inden for de sikkerhedsrelaterede opgaver, som det har ansvaret for (jf. 2.3. Organisatoriske roller, ansvarsområder, ansvarlighed og bemyndigelser), herunder som minimum:
- (a) fastlæggelse af de kompetencer (herunder viden, færdigheder, ikke-teknisk adfærd og holdninger), som er påkrævet for at løse sikkerhedsrelaterede opgaver
 - (b) udvælgelsesprincipper (grundlæggende uddannelsesniveau, krav til psykisk og fysisk egnethed)
 - (c) indledende oplæring, erfaring og kvalifikationer
 - (d) løbende efteruddannelse og regelmæssig ajourføring af eksisterende kompetencer
 - (e) periodisk kompetencevurdering og tjek af psykisk og fysisk egnethed for at sikre, at kvalifikationer og færdigheder vedligeholdes løbende
 - (f) specifik uddannelse i relevante dele af sikkerhedsledelsessystemet med henblik på at varetage deres sikkerhedsrelaterede opgaver.
- 4.2.2. Organisationen skal fastlægge et uddannelsesprogram som nævnt i afsnit 4.2.1, litra c), d) og f) for personale, som udfører sikkerhedsrelaterede opgaver, og med programmet skal det sikres, at:
- (a) uddannelsesprogrammet gennemføres i henhold til de fastlagte kompetencekrav og personalets individuelle behov
 - (b) uddannelsen i relevante tilfælde sikrer, at personalet kan fungere under alle driftsvilkår (normal drift, uregelmæssig drift og nøddrift)
 - (c) uddannelsens varighed og hyppigheden af suppleringsuddannelsen er tilpasset uddannelsesmålsætningerne
 - (d) der føres et register for hele personalet (jf. 4.5.3. Styring af dokumenteret information)
 - (e) uddannelsesprogrammet gennemgås og auditeres løbende (jf. 6.2. Intern audit), og ændringer foretages efter behov (jf. 5.4. Håndtering af ændringer).
- 4.2.3. Ordninger skal være etableret for personale, som vender tilbage til arbejdet efter ulykker/hændelser eller langvarigt tjenestefravær, og herunder ekstra uddannelse, når et behov for dette påvises.

4.2.2 Formål

Formålet med dette krav er at sikre, at organisationen har passende strukturer og ressourcer til at styre de risici, den står over for, og til at beskæftige personale, som er kompetent til at udføre sikkerhedsfunktionerne og navnlig de funktioner, der er kritiske for sikkerheden. Kompetencestyringssystemet gør det også muligt for organisationen løbende at opretholde færdigheder, viden og erfaring hos personalet.

Kompetence spiller en afgørende rolle, når det gælder om at sikre, at aktiviteterne udføres tilfredsstillende. Behovet for at have kompetent personale omfatter både frontlinjestøtte (herunder kontrahenter, konsulenter og leverandører af sikkerhedsrelaterede tjenester) og ledelsespersonale. Krav til ledelsens kompetence bliver ofte overset, men ledere træffer vigtige beslutninger, som kan have fundamentale og vidtrækkende konsekvenser for sundheden og sikkerheden. Disse krav bør omfatte bestemmelser om alle medarbejderes uddannelse i de nødvendige sikkerhedsstandarder, om kompetencens vedligeholdelse

uanset omstændighederne, herunder spørgsmål om personaletilgængelighed, og om overvågning af kompetenceniveauet i forhold til de nødvendige standarder.

I denne sammenhæng betragtes sikkerhed som en integreret komponent bestående af professionel adfærd og professionalisme — og ikke som et "yderligere lag", der skal tilføjes til de professionelle færdigheder. Endvidere er en organisations evne til med det samme at tackle uforudsete begivenheder i høj grad afhængig af kompetencen hos frontlinjepersonalet og deres supervisor. Disse kompetencer kan udvikles ved hjælp af eksempelvis øvelser og regelmæssig uddannelse i komplekse scenarier.

4.2.3 Forklarende noter

Der kan tilvejebringes et uddannelsesprogram **(4.2.2)** via et eksternt uddannelsescenter. I så fald bør organisationen sikre, at uddannelsescentret er kompetent til at tilbyde de relevante tjenester, enten fordi det er certificeret eller anerkendt i henhold til en national eller europæisk ordning eller gennem direkte overvågning af centrets uddannelsesaktiviteter og resultater. Uddannelsescentre kan opfylde alle en organisations uddannelsesbehov eller kun nogle få af dem, alt efter deres kompetencer på de relevante områder. Hvis et eksternt uddannelsescenter leverer uddannelse til en organisation, skal organisationen tjekke, at uddannelsen omfatter alle nødvendige elementer, og, såfremt det ikke er tilfældet, supplere den eksterne uddannelse med intern uddannelse efter behov.

"Holdninger" **(4.2.1 (a))** anvendes til at beskrive, hvordan personer reagerer på visse situationer, og hvordan deres adfærd er generelt (f.eks. om de er proaktive og kan komme overens med andre). Dette er meget vigtigt, når det gælder om at få de indbyrdes relationer inden for sikkerhedsledelsessystemet til at fungere.

Der bør være en systematisk tilgang til at sikre, at kompetencen inden for menneskelige og organisatoriske faktorer er tilgængelig, enten i de relevante roller baseret på en behovsanalyse eller på tilkaldebasis.

Kompetencen inden for menneskelige og organisatoriske faktorer bør f.eks. anvendes i projekter, som vedrører ny eller ændret udformning, i analyser af ulykker for at give et ikke-teknisk perspektiv eller i spørgsmål, der drejer sig om den menneskelige ydeevne.

4.2.4 Dokumentation

- Ansøgerne bør fremlægge oplysninger om deres kompetencestyringssystem, og hvordan det fungerer, for at opfylde kravene **(4.2.1), (4.2.2(a)-(e))**.
- Dokumentationen skal omfatte oplysninger om de uddannelsesprogrammer, der er indført for personalet (herunder efter behov oplysninger om organisationens krav til underviseres kompetencer), og hvordan uddannelsesprogrammer opdateres og gennemgås (herunder efter behov for sikkerhedsrådgiverens rolle under RID) **(4.2.2 (a)-(e))**.
- Dokumentationen skal omfatte ordninger for personale, som vender tilbage til arbejdet efter ulykker og hændelser eller langvarigt tjenestefravær, herunder hvordan der tilvejebringes ekstra uddannelse, når et behov for dette påvises **(4.2.3)**.
- Hvis ansøgerne bruger et anerkendt uddannelsescenter, der er certificeret i henhold til EU-forordninger, vil en kopi af det relevante certifikat give en formodning om overensstemmelse med ovenstående elementer, i den udstrækning de er dækket af denne certificeringsproces **(4.2.1 (a), (c)-(f), (4.2.2))**.
- Ansøgerne bør angive, hvordan de sikrer, at der ikke er forskel på kompetencerne hos deres eget personale og personalet hos eventuelle kontrahenter, leverandører og konsulenter, som de beskæftiger **(4.2.1 (a)-(f))**.
- Ansøgerne bør angive, hvordan behovet for kompetence inden for menneskelige og organisatoriske faktorer vurderes. Dette omfatter en definition af, i hvilke roller og processer der er behov for kompetence inden for menneskelige og organisatoriske faktorer, og hvilket kompetenceniveau der er påkrævet. De tilgængelige færdigheder inden for menneskelige faktorer (f.eks. formelle kvalifikationer inden for menneskelige faktorer, dvs. akademiske grader, internt/eksternt

anerkendte kompetencer og erfaring) skræddersyes og står i forhold til virksomhedens modenhed og kompleksitet. (4.2.1 (a-f)).

- *Ansøgerne bør oplyse om processen for bemyndigelse af personale til udførelse af centrale roller, herunder løbende styring af personalets kompetencer (4.2.1 (a)-(f), 4.2.2(d)).*

4.2.5 Eksempler på dokumentation

Kompetencestyringssystemet med en forklaring af dets løbende funktion, hvis relevant også for ikke-frontlinjepersonale, såvel som links til den underbyggende dokumentation, herunder de forskellige uddannelsesprogrammer, og hvordan udliciterede uddannelsescentre styres.

De kontraktlige aftaler (herunder specifikationer) med eventuelle certificerede uddannelsescentre samt dokumentation for deres certificering fremlægges.

Eksempler på uddannelsesprogrammer for personalegrupper.

De nødvendige kvalifikationer for specifikke sikkerhedsrelaterede roller, herunder psykiske eller fysiske krav.

Proceduren for undersøgelse af ulykker og hændelser, i det omfang den omfatter handlinger med henblik på at ændre uddannelsesprogrammerne i lyset af ulykker og hændelser, tidligere tilsyn osv.

Proceduren eller processen til at sikre, at personalet får specifik uddannelse og genopfriskning i følgende:

- *forventede ændringer, der vedrører interne regler, infrastruktur, organisationsstruktur osv.*
- *opdateringer i forhold til de tildelte opgaver (for lokomotivførere kan det f.eks. være nye ruter, nye lokomotivtyper eller nye tjenestetyper).*

Processen til at sikre, at:

- *kompetencen vedligeholdes ved hjælp af relevant praksis på området (for lokomotivførere kan det f.eks. være kendskab til driftsvilkårene, togkategorier, trækraftenheder, linjer og stationer) og/eller ved at planlægge specifik uddannelse, navnlig hvis der har været et langvarigt tjenestefravær (f.eks. sygdom) eller en ulykke/hændelse*
- *der træffes de nødvendige foranstaltninger, hvis der identificeres afvigelser eller upassende adfærd såsom en person eller udstyr, der tages ud af tjeneste i en periode, restriktioner med hensyn til anerkendte færdigheder, hvor der er identificeret en afvigelse, specifik uddannelse osv.*
- *der iværksættes passende tiltag for personalet efter ulykker og hændelser (f.eks. for lokomotivførere, der kører forbi et signal, personulykker osv. F.eks. sikrer organisationen, at lokomotivføreren er i stand til at genoptage tjenesten eller erstattes med en anden, som er kompetent til den tjeneste, der skal ydes)*
- *erfaringer efter alvorlige ulykker eller andre signifikante hændelser deles, navnlig hvis der opdages nye risici, som skal styres på driftsmæssigt plan*
- *der er en overvågningsproces for kompetencestyringssystemet, bl.a. med hensyn til hvordan dets effektivitet måles.*

Processen til at sikre, at der er passende kompetencer inden for menneskelige og organisatoriske faktorer, og at der er en systematisk tilgang til at sikre, at der sættes tilstrækkelig tid og ressourcer af til menneskelige og organisatoriske faktorer.

Kompetence inden for sikkerhedskultur er baseret på en behovsanalyse. Kompetencebehovet inden for sikkerhedskultur vurderes, og strategierne til at sikre de rette kompetencer og ressourcer påvises. Dokumentation for, at ledelsen fremmer grundlæggende viden om sikkerhedskulturen og dens betydning.

4.2.6 Referencer og standarder

- ISO 10015:1999 Kvalitetsstyring — Vejledning for uddannelse/træning
- ISO 10018: "Kvalitetsledelse — Personers involvering og kompetencer — Vejledning".

4.2.7 Tilsynsspørgsmål

Hvordan resultaterne af risikovurderingen er forbundet med en gennemgang af kompetencestyringssystemet.

Når man kigger på kompetencestyringssystemet, er det vigtigt at huske, at der vil være kompetencekrav, som ikke blot omfatter organisationens personale, men også har indflydelse på kontrahenter og andre.

Kompetencestyringssystemet bør tjekkes for at undersøge, hvor opdateret det er, og om uddannelsesaktiviteterne i det afspejler organisationens nuværende behov.

Organisationen bør have en metode til at sikre, at kontraktansatte, som udfører aktiviteter, er kompetente til at gøre dette. Dette er navnlig et problem i forbindelse med kontrahenter, hvor der udelukkende er tale om arbejdskraft, da kontrollen af kompetencerne måske ikke er så grundig i den forbindelse.

Det påkrævede kompetenceniveau for tilsvarende aktiviteter udført af fastansat personale og kontrahenter bør være det samme.

Der er indført et system, som sikrer, at opgaver og stillinger med et sikkerhedselement, herunder sikkerhedskritiske opgaver, bliver identificeret.

Der er et solidt og effektivt kompetencestyringssystem, som omfatter identifikation af nødvendig viden og færdigheder, uddannelse, vedligeholdelse og ressourcer med henblik på kompetence samt processer til rekruttering, uddannelse, vurdering, kompetenceovervågning og registrering, og det angives, hvordan alt dette bidrager til at opnå og vedligeholde kompetencen.

Fokus på de menneskelige faktorer — hvordan foregår vurderingen af den fysiske og psykiske egnethed (f.eks. for lokomotivførere og for andet personale, der udfører sikkerhedskritiske opgaver).

4.3 Bevidsthed

4.3.1 Lovkrav

4.3.1. Den øverste ledelse skal sikre, at den og dets personale, der spiller en rolle, som påvirker sikkerheden, er bevidst om relevansen, betydningen og konsekvenserne af deres aktiviteter og om, hvordan de bidrager til den korrekte anvendelse og effektiviteten af sikkerhedsledelsessystemet, herunder opfyldelse af sikkerhedsmålene (jf. 3.2 Sikkerhedsmål og -planlægning).

4.3.2 Formål

Bevidsthed betyder, at personalet gøres opmærksomt på organisationens sikkerhedspolitik, og hvordan de bidrager til sikkerheden i organisationen, hvilke farer og risici de skal være opmærksomme på, og resultaterne af undersøgelser af ulykker og hændelser. Begrebet dækker også, at personalet gøres bevidst om konsekvenserne af ikke at bidrage til sikkerhedsledelsessystemets gennemførelse, både fra deres og fra organisationens synspunkt. Formålet med dette krav er at adressere forhold omkring sikkerhedskultur inden for organisationen. Den øverste ledelse skal sætte dagsordenen og retningen for organisationen og fastlægge, hvordan forretningen skal køres. Personale, der arbejder inden for organisationen, følger ledelsens eksempel. Ansøgerne skal påvise, hvordan de adresserer sådanne spørgsmål i deres processer og procedurer.

4.3.3 Dokumentation

- Ansøgerne bør angive, hvor personalets nøglerolle i at opfylde organisationens mål afspejles i HR- eller andre processer, hvordan de stræber efter at måle dette, og hvilke skridt de tager for at opretholde og forbedre dette **(4.3.1)(jf. også 2.3)**.
- Oplysninger om kompetencestyringssystemets måde at fungere på **(4.3.1)**.

4.3.4 Eksempler på dokumentation

Sikkerhedspolitikken eller andet indeholder ledelsens forpligtelse til at fremme organisationens sikkerhedskultur med henblik på at sikre risikostyringen ved hjælp af en ledelsessystemtilgang. Politikken eller andet nævner også alle medarbejdernes indsats for at fremme sikkerhedskulturen via deres handlinger og ved at nå de opstillede sikkerhedsmål. Der er links til de specifikke procedurer, som har til formål at fremme disse idéer i hele organisationen.

Ovennævnte omfatter information om, hvordan organisationen udbreder sin tilgang til sikkerhedskulturen til sine kontrahenter, partnere og leverandører.

For selve politikkens vedkommende, indeholder kommunikationen fra den øverste ledelse omtale af målene, enten ved at de opfordrer alle medarbejdere til at bidrage til, at målene opfyldes, eller f.eks. i lykønskingsmeddelelser, hvor de takker for en forbedret indsats.

Oplysninger, som viser, at mellemledelsen og driftspersonalet er involveret i frontlinjesikkerhedsinitiativer (workshops, fora, særlige sikkerhedsdage, uddannelsesprogrammer for at gøre dem bevidste om deres rolle i sikkerhedsledelsessystemet osv.).

En beskrivelse af de kommunikationskanaler, der anvendes.

4.3.5 Tilsynsspørgsmål

Når personalet interviewes om dette spørgsmål, er det vigtigt at fastslå, hvilken forståelse folk har af de roller og ansvarsområder, der gælder for dem. Dette vil vise, om organisationen forstår vigtigheden af en effektiv organisationskultur eller bevidstgørelse, når sikkerhed opnås ved hjælp af sikkerhedsledelsessystemet.

Nøglespørgsmål i forbindelse med tilsynet er, hvad der er grundlaget for organisationens nuværende kultur, og hvilke skridt der træffes for at forbedre og udvikle den.

Kontrol af, hvordan efterlevelsen af sundheds- og sikkerhedsansvaret/-målene, risikobevidsthed og rapporteringskultur overvåges, idet der kigges efter forglemmelser, fejl, overtrædelser og andre uoverensstemmelser.

4.4 Information og kommunikation

4.4.1 Lovkrav

- 4.4.1. Organisationen skal fastlægge passende kommunikationskanaler til at sikre, at sikkerhedsrelateret information udveksles mellem de forskellige organisationsniveauer og med eksterne interessenter, bl.a. kontrahenter, partnere og leverandører.
- 4.4.2. For at sikre, at sikkerhedsrelateret information når frem til dem, der skal foretage vurderinger og træffe beslutninger, skal organisationen styre udpegningen, modtagelsen, behandlingen, udarbejdelsen og formidlingen af sikkerhedsrelateret information.
- 4.4.3. Organisationen skal sikre, at sikkerhedsrelateret information er:
- (a) relevant, fyldestgørende og forståelig for de tiltænkte brugere
 - (b) gyldig
 - (c) nøjagtig
 - (d) sammenhængende
 - (e) styret (jf. Styring af dokumenteretinformation)
 - (f) formidlet, inden den træder i kraft
 - (g) modtaget og forstået.

4.4.2 Formål

Overholdelsen af disse krav skal vise, at ansøgerne i deres ansøgning har påvist, at de råder over passende midler til at identificere sikkerhedsrelaterede oplysninger på forskellige niveauer og til at kommunikere dem i rette tid og til de rette personer. De har påvist, at de scanner markeds- og anden information (horizon scanning) for at sikre, at den aktuelle risikostyring stadig er relevant og opdateret, og at de kan identificere nye trusler og muligheder, der skyldes eksterne påvirkninger (af politisk, social, miljømæssig, teknologisk, økonomisk og juridisk karakter). At de er i stand til at sikre, at informationen når frem til det personale inden for deres organisation (specielt personale, der udfører sikkerhedskritiske opgaver), der skal reagere på dem. Dette omfatter, hvordan relevante sikkerhedsrelaterede oplysninger videregives til andre interessenter, som de har grænseflader til.

4.4.3 Forklarende noter

Organisationen angiver, hvilken type sikkerhedsrelaterede oplysninger der skal kommunikeres, hvordan de kommunikeres (**jf. også 4.5**), til hvem de kommunikeres, og på hvilke betingelser dette bliver iværksat og gennemført (**4.4.1**). De sikkerhedsrelaterede oplysninger udveksles mellem personale, der udfører opgaver inden for organisationen, med (under-)kontrahenter, partnere eller leverandører, mellem jernbanevirksomheder og infrastrukturforvaltere og, hvis relevant, mellem infrastrukturforvaltere.

Der skelnes mellem forskellige typer oplysninger:

- *sikkerhedsledelsessystemets dokumenter (jf. også 4.5)*
- *statiske oplysninger fra infrastrukturforvalteren med henblik på at tilrettelægge jernbanedriften såsom driftsregler og kendetegn for jernbaneinfrastrukturen (f.eks. sporvidde, tog længde, hældninger og akseltryk)*
- *oplysninger, som er nødvendige for jernbanedriftens planlægning såsom togkøreplaner, rutelister, midlertidige hastighedsbegrænsninger, ændringer af jernbaneinfrastrukturen, igangværende sporarbejde, begrænsninger af sporvidden, tog, som omdirigeres fra den planlagte rute, dele af linjen,*

hvor kun ét spor er i brug, prognoser for togdriften (herunder eventuelle ændringer af togruterne og/eller pendlertjenester)

- *oplysninger om styring af togtrafikken (mellem jernbanevirksomheder og infrastrukturforvaltere og, hvis relevant, mellem infrastrukturforvaltere), herunder identifikation af kompetent personale inden for hver organisation, som kan kontaktes i tilfælde af uregelmæssig drift eller nødsituationer (jf. også 5.5) i og uden for normal arbejdstid.*

De grundlæggende krav til udveksling af oplysninger **(4.4.2)** er identificeret i TSI OPE mellem jernbanevirksomheden og infrastrukturforvalteren, i ECM-forordningen mellem jernbanevirksomheden og enheden med ansvar for vedligeholdelse, og i CSM SMS mellem jernbanevirksomheden/ infrastrukturforvalteren og myndighederne (agenturet og den nationale sikkerhedsmyndighed).

Udveksling af oplysninger er arrangeret med relevante parter om sikkerhedsrisici vedrørende mangler og konstruktionsafvigelser eller funktionsfejl i tekniske systemer, herunder i strukturelle delsystemer, herunder oplysninger om eventuelle afhjælpende foranstaltninger taget for eksempel via SAIT (Safety Alert Tool)-aftalen, som agenturet har fremmet sammen med jernbanesektoren. Brugen af SAIT opfylder forpligtelsen til at udveksle sådanne oplysninger, jf. jernbanesikkerhedsdirektivet (artikel 4, stk. 5) og kravet i CSM for overvågning (artikel 4) og forordningen om enheder med ansvar for vedligeholdelse (artikel 5, stk. 5).

”Gyldig” betyder i ovenstående sammenhæng **(4.4.3 (b))** opdateret.

”Sammenhængende” betyder i ovenstående sammenhæng **(4.4.3 (d))** ikke modsatrettede, hvis de kommer fra forskellige kilder.

”Forstået” betyder i ovenstående sammenhæng **(4.4.3 (g))**, at ansøgerne påviser, at de har truffet foranstaltninger til at sikre, at sikkerhedskritiske oplysninger er blevet forstået af dem, de er rettet imod. Dette kan ske ved hjælp af ad hoc-uddannelse, ved hjælp af spørgsmål, hvor man tjekker forståelsen ved briefinger, eller i sikkerhedskritiske meddelelser, hvor der anvendes protokoller, som kræver en gentagelse af vigtige budskaber, f.eks. mellem trafiklederen og lokomotivføreren, for at bekræfte, at de er blevet forstået korrekt, eller på enhver anden måde, som opfylder kravet.

4.4.4 Dokumentation

- *Ansøgerne identificerer de forskellige kommunikationskanaler, der eksisterer i organisationen, og deres formål **(4.4.1)**.*
- *Ansøgerne skal f.eks. fremlægge dokumentation for eventuelle interne sikkerhedsvarslingssystemer, systemer, som giver personalet relevante rutinemæssige oplysninger, og systemer, som giver personalet relevante ad hoc-oplysninger **(4.4.2)**.*
- *Ansøgerne angiver, hvordan de sikrer sig, at de oplysninger, der er givet, er nået frem til de tiltænkte modtagere (navnlig dem, der har sikkerhedskritiske roller) og er blevet forstået af dem **(4.4.3)**.*

4.4.5 Eksempler på dokumentation

En klar erklæring på, hvordan der kommunikeres både opad og nedad med hensyn til forskellige typer og niveauer af oplysninger, herunder links til de specifikke procedurer for sikkerhedsvarsling og rutinekommunikation.

Erklæringen omfatter oplysninger om, hvilke foranstaltninger de træffer i forbindelse med de forskellige typer kommunikation for at sikre, at de når frem til det personale, de er tiltænkt, og at dette personale forstår, hvad der kommunikeres, f.eks. sikkerhedskritiske oplysninger.

Processen eller proceduren, der sikrer, at alle medarbejdere, som er involveret i en sikkerhedsrelateret opgave, får udleveret den korrekte version af dokumenterne på det rigtige tidspunkt.

Processen eller proceduren for bekræftelse af, at de sikkerhedsrelaterede dokumenter er udleveret.

Processen/proceduren for at sikre, at eksterne parter såsom infrastrukturforvalter(e), (andre) jernbanevirksomheder, myndigheder osv. får en kontaktperson, som kan kommunikere med dem (f.eks. sprogfærdigheder) og har adgang til det rette oplysningsniveau.

Kendskab til blanketsamlingen (jf. TSI OPE), som indeholder samlingen af kommunikationsprotokoller eller -medier til klar og hurtig udveksling af formaliserede oplysninger (papirbaserede eller papirløse medier såsom registreringsenheder), der vedrører driften, navnlig for togenes bevægelser ved uregelmæssig drift.

De sikkerhedsvarsler, der skal udveksles inden for organisationen eller med andre interesserede parter. Nogle typiske eksempler:

- *Jernbanevirksomhederne underretter infrastrukturforvalteren om eventuelle forstyrrelser, der kan have indvirkning på togenes bevægelser (fejl i rullende materiel, f.eks. varme akselkasser, således at infrastrukturforvalteren kan træffe risikokontrolforanstaltninger såsom standsning af trafikken på det tilstødende spor).*
- *Infrastrukturforvalteren underretter alle jernbanevirksomheder, der opererer i det relevante område, om infrastrukturfejl og eventuelle midlertidige sikkerhedsforanstaltninger såsom hastighedsreduktion.*

Hvad angår de roller, der har til opgave at håndtere grænsefladerne: Dokumentation for, hvem sikkerhedsvarslerne sendes til, alt afhængigt af driftsområdet (de er f.eks. medtaget i strækningsoversigten).

Processen eller proceduren for rundsending af oplysninger om ændringer af organisationens organisationsstruktur, både på mikro- og makroplan.

Kopier af instruktionerne til personale, som udfører sikkerhedsrelaterede opgaver, og som håndterer de driftsregler, der er relevante for nettet eller nettene. De skal være:

- *fyldestående: Alle regler og krav, der vedrører sikkerhedsopgaver, som er relevante for jernbanevirksomhedens drift, er identificeret og gengivet i de relevante dokumenter*
- *nøjagtige: Alle regler og krav er gengivet korrekt og uden fejl (f.eks. hvordan man skal handle ved et signal og sikkerhedsrelateret kommunikation)*
- *sammenhængende: Kravene til en enkelt person eller et enkelt team fra forskellige kilder er forenelige og sammenhængende og er ikke modsatrettede.*

4.4.6 Tilsynsspørgsmål

Kontrol af, at der anvendes teknikker og processer til opdatering af risikostyringen og informationssøgning (horizon scanning) for muligheder og trusler.

Kontrol af, at der er en proces for overvågning af brugen af formaliserede oplysninger.

Ved tilsynet er nøglespørgsmålene, hvor opdaterede oplysningerne er, og om de når rettidigt frem til **alle** relevante medarbejdere, f.eks. dem på natholdet eller dem, der har fjernarbejde fra organisationens hovedbaser.

4.5 Dokumenteret information

4.5.1 Lovkrav

4.5.1. Dokumentation for sikkerhedsledelsessystemet

4.5.1.1. Der findes en beskrivelse af sikkerhedsledelsessystemet og herunder:

- (a) fastlæggelse og beskrivelse af processer og aktiviteter i relation til jernbanens sikre drift, herunder sikkerhedsrelaterede opgaver og tilhørende ansvarsområder (jf. 2.3. Organisatoriske roller, ansvarsområder, ansvarlighed og bemyndigelser)
- (b) samspillet mellem disse processer
- (c) procedurer eller dokumenter, der beskriver, hvordan disse processer gennemføres
- (d) udpegning af kontrahenter, partnere og leverandører sammen med en beskrivelse af typen og omfanget af de leverede ydelser
- (e) udpegning af kontrakter og andre forretningsaftaler, som er indgået mellem organisationen og de øvrige parter, der er angivet i litra d), og som er påkrævet for at styre organisationens sikkerhedsrisici samt sikkerhedsrisici som følge af, at der benyttes kontrahenter
- (f) henvisning til dokumenteret information i henhold til denne forordning

4.5.1.2. Organisationens skal sikre, at en årlig sikkerhedsrapport forelægges den relevante nationale sikkerhedsmyndighed (eller myndigheder) i overensstemmelse med artikel 9, stk. 6, i direktiv (EU) 2016/798, herunder:

- (a) et resumé over vurderinger af sikkerhedsrelaterede ændrings signifikans og herunder en oversigt over signifikante ændringer i henhold til artikel 18, stk. 1, i forordning (EU) nr. 402/2013
- (b) organisationens sikkerhedsmål for det eller de kommende år, og hvordan alvorlige sikkerhedsrisici påvirker fastlæggelsen af disse sikkerhedsmål
- (c) resultaterne af intern undersøgelse af ulykker/hændelser (jf. 7.1 Erfaringer fra ulykker og hændelser) og andre overvågningsaktiviteter (jf. 6.1 Overvågning, 6.2 Intern audit, og 6.3 Ledelsens evaluering) i overensstemmelse med artikel 5, stk. 1, i forordning (EU) nr. 1078/2012
- (d) beskrivelse af fremdrift i behandlingen af anbefalinger fra de nationale undersøgelsesorganer (jf. 7.1 Erfaringer fra ulykker og hændelser)
- (e) organisationens sikkerhedsindikatorer, der er fastsat med henblik på at evaluere organisationens sikkerhedsniveau (jf. 6.1 Overvågning)
- (f) i relevante tilfælde konklusionerne af sikkerhedsrådgiverens årlige rapport som omhandlet i RID angående organisationens aktiviteter i relation til transport af farligt gods.

4.5.2. Udarbejdelse og opdatering

4.5.2.1. Organisationens skal sikre, at hensigtsmæssige formater og medier anvendes i forbindelse med udarbejdelse og opdatering af dokumenteret information vedrørende sikkerhedsledelsessystemet.

4.5.3. Styring af dokumenteret information

4.5.3.1. Organisationens skal styre dokumenteret information i relation til sikkerhedsledelsessystemet, navnlig hvad angår arkivering, distribution og styring samt ændringer heraf, for at sikre, at systemet er tilgængeligt, hensigtsmæssigt og sikret, når det er relevant.

4.5.2 Formål

Ansøgerne skal påvise, at det overordnede sikkerhedsledelsessystem er velegnet til typen og omfanget af de leverede tjenester og er i stand til at styre de risici, der opstår. Dette kræver:

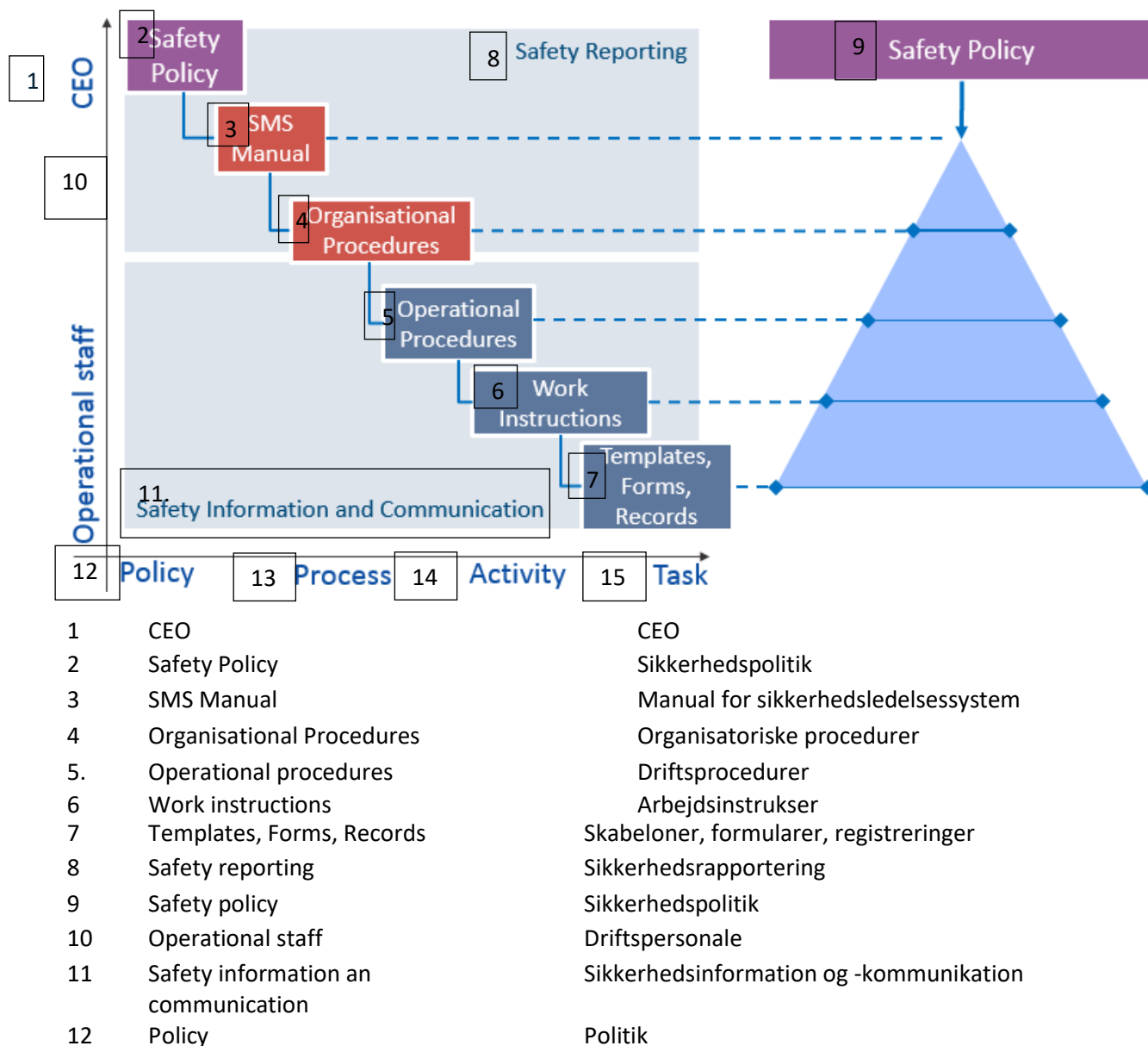
- en forklaring af ansøgernes sikkerhedspolitik, organisation og overordnede sikkerhedsledelsessystem samt
- detaljer om, hvordan kravene ovenfor i punkt 4.5.1.1 (a) til (f) og 4.5.1.2 (a) til (g) håndteres.

Ansøgerne skal ligeledes vise, hvordan deres dokumentation for sikkerhedsledelsessystemet håndteres, dvs. identifikation, oprettelse, vedligeholdelse, administration, lagring og opbevaring af dokumenterede oplysninger (dvs. dokumenter og registre/data) for at sikre, at den er opdateret, og at de korrekte versioner er tilgængelige for det relevante personale, når det er nødvendigt.

4.5.3 Forklarende noter

Alle dokumenter, hvor ansøgerne påviser, at deres sikkerhedsledelsessystem opfylder de gældende krav (4.5.1.1 (f)), hører med til sikkerhedsledelsessystemets dokumenteret information.

Følgende Figur 3 viser en typisk dokumentationsstruktur:



13	Process	Proces
14	Activity	Aktivitet
15	Task	Opgave

Figur 3: Typisk dokumentationsstruktur

Alt afhængigt af driftsområdet kan jernbanevirksomhederne fremsende forskellige rapporter **(4.5.1.2)** til de nationale sikkerhedsmyndigheder i de medlemsstater, hvor de opererer. Generelt omfatter rapporten kun den del af driften, der finder sted i den pågældende medlemsstat. Agenturet anbefaler dog, at den samme rapport dækker hele driftsområdet, da dette letter delingen af oplysninger mellem de nationale sikkerhedsmyndigheder, der fører tilsyn med den samme jernbanevirksomhed.

Sikkerhedsrådgiverens årlige rapport **(4.5.1.2 (f))**, såfremt der er tale om transport af farligt gods i henhold til direktiv 2008/68/EF med ændringer og RID, samt sikkerhedsrådgiverens årlige rapport om farligt gods udgør også et input til den årlige sikkerhedsrapport. Sikkerhedsrådgiveren skal opfylde specifikke funktioner, herunder rådgivning af den virksomhed, der har udpeget denne, med hensyn til sundheds-, sikkerheds- og miljøspørgsmål i forbindelse med transport af farligt gods og udarbejdelsen af de nødvendige rapporter.

Identifikationen, formatet (f.eks. sprog, softwareversion og grafik) og mediet (f.eks. papir eller elektronisk), der anvendes til dokumenteret information **(4.5.2.1)**, er overladt til organisationens skøn. Det behøver ikke at være en skriftlig papirmanual.

Dokumentstyringen **(4.5.3.1)** betegner den proces (eller procedure), der specificerer den interne styring — navnlig gennemgangen og godkendelsen af egnetheden inden udstedelse og brug — der skal tages i betragtning og gennemføres for de oplysninger, som skal dokumenteres. Den tager sigte på at identificere dokumenternes aktuelle revisionsstatus for at udelukke brugen af ugyldige eller forældede dokumenter. Den sikrer navnlig følgende:

- *De relevante udgaver af de dokumenter, der skal bruges, er tilgængelige alle de steder, hvor der udføres aktiviteter, som er vigtige for sikkerhedsledelsessystemets effektive funktion.*
- *Ugyldige eller forældede dokumenter fjernes straks fra alle udstedelses- og brugssteder eller beskyttes på anden måde mod utilsigtet brug.*
- *Alle forældede dokumenter, der opbevares af juridiske årsager eller med det formål at gemme viden, identificeres på passende vis.*

4.5.4 Dokumentation

- *Ansøgerne bør fremlægge en beskrivelse af sikkerhedsledelsessystemet, og hvordan det fungerer, med passende henvisninger til de relevante procedurer, hvor dette er nødvendigt **(4.5.1.1 (a)-(c))**.*
- *Ansøgerne bør angive, hvilke roller og ansvarsområder der eksisterer med hensyn til sikkerhedsrelaterede opgaver, og hvordan de risici, som ansøgernes og andres aktiviteter medfører, bliver styret **(4.5.1.1 (a))**.*
- *Ansøgerne skal fremlægge dokumentation for, at de har (eller har iværksat udarbejdelsen af) en årlig sikkerhedsrapport, der dækker punkterne i 4.5.1.2 ovenfor **(4.5.1.2(a)-(f))**.*
- *Ansøgerne bør angive, hvordan dokumenthåndteringssystemet fungerer, herunder hvordan oplysninger gøres tilgængelige og kan anvendes, hvor og hvornår det er nødvendigt, hvordan de ændres på en kontrolleret måde inden for systemet, og hvordan de opbevares og vedligeholdes på en sådan måde, at de hurtigt kan hentes. Desuden bør dokumenthåndteringssystemet gøre det muligt at opbevare oplysninger i faciliteter, som udgør et passende miljø, for at minimere ødelæggelse eller skader, og for at forhindre, at de går tabt. **(4.5.2.1), (4.5.3.1)**.*

4.5.5 Eksempler på dokumentation

En beskrivelse af sikkerhedsledelsessystemet og dets overordnede opbygning samt links til de dokumenter, der støtter processerne heri (f.eks. manual, organisatoriske procedurer og driftsprocedurer samt arbejdsinstrukser). Uanset det nye begreb "dokumenteret information", som er indført af ISO, kan organisationen bevare den traditionelle dokumentationsopbygning, hvis den er egnet til formålet.

En skitsering af, hvordan de forskellige dokumenter opbygges, offentliggøres, gøres tilgængelige, arkiveres, vedligeholdes/revideres og ophæves, med en henvisning til de relevante dokumentstyringsprocedurer.

Proceduren for udarbejdelse af den årlige rapport, hvis der ansøges om det første EU-sikkerhedscertifikat. Proceduren viser rapportens foreslåede layout.

Dokumenthåndteringsprocessen eller -proceduren, som skal vise, hvordan dokumenterne opdateres efter regelmæssig gennemgang og efter ulykker eller hændelser. Processen eller proceduren tager højde for en eskaleringsproces i de tilfælde, hvor de aftalte opdateringer ikke har fundet sted inden for den aftalte tidsfrist, eller hvor der ikke er nogen aftale om, hvordan dokumentet skal opdateres.

Der anvendes et kontrolleret sprog (dvs. korte, klare sætninger uden brug af jargon) for at fremme fælles forståelse og god datakvalitet.

Det personale, der har beføjelse til at godkende dokumenter til udstedelse, sikrer, at indholdet er nøjagtigt og forståeligt for alle slutbrugere (eller modtagere), som de er rettet til.

Når det er praktisk muligt, identificeres ændringernes karakter i dokumentet eller i relevante bilag for at lette gennemgangen og godkendelsen af disse.

Der fastsættes opbevaringsfrister for dokumenter og registreringer, som dokumenteres og overholdes.

4.5.6 Referencer og standarder

- *Guidance on the requirements for Documented Information of ISO 9001:2015, ISO/TC 176/SC2/N1286, som findes på: www.iso.org/tc176/sc02/public*

4.5.7 Tilsynsspørgsmål

Kontrol af, at de kontraktlige aftaler sikrer et effektivt tilsyn og effektiv risikostyring fra organisationens side (dvs. når tjenester udliciteres).

Når der foretages tilsyn, er det af afgørende vigtighed at fastslå, hvordan forholdet mellem dem, der styrer dokumenthåndteringssystemet, og dem, der er ansvarlige for at opdatere oplysninger og samarbejde med førstnævnte, ser ud i praksis. Det er på dette niveau, at der ofte kan opstå et svigt i styringen af dokumentationen, da det er sandsynligt, at de to dele af processen befinder sig i to forskellige ledelseskæder. Det kan for eksempel betyde, at vigtigheden af arbejdet med at opdatere dokumentation opfattes forskelligt, hvilket forsinker udviklingen og opdateringen af dokumentation med de pågældende risici.

Personalets mulighed for at få adgang til opdateret information/dokumentation.

Sikkerhedsledelsessystemets opbygning og måde at fungere på bør afspejle den måde, som arbejdet reelt udføres på, og ikke være en kunstig tilføjelse til sædvane og praksis.

4.6 Integration af menneskelige og organisatoriske faktorer

4.6.1 Lovkrav

- 4.6.1. Organisationen skal godtgøre, at menneskelige og organisatoriske faktorer integreres i sikkerhedsledelsessystemet efter en systematisk tilgang. Denne tilgang skal:
- a) omfatte udviklingen af en strategi og brug af fagkundskab og anerkendte metoder inden for menneskelige og organisatoriske faktorer
 - b) håndtere risici, der er forbundet med udformning og brug af udstyr, opgaver, arbejdsvilkår og organisatoriske tiltag, idet der tages hensyn til menneskelige evner og begrænsninger samt forhold, som påvirker den menneskelige ydeevne.

4.6.2 Formål

Ansøgeren viser, at anvendelsen af en systematisk tilgang til menneskelige og organisatoriske faktorer i risikostyringen er en integreret del af sikkerhedsledelsessystemet. At tage højde for disse elementer er vigtigt for at påvise, at ansøgeren er kompetent til at drive jernbanevirksomhed og har indbygget risikostyringssystemer i sit sikkerhedsledelsessystem for at håndtere de risici, som denne står over for.

4.6.3 Forklarende noter

Menneskelige og organisatoriske faktorer medfører et systemisk perspektiv, hvor der tages højde for samspillet mellem menneskelige, teknologiske og organisatoriske faktorer. Organisationen bør tage menneskelige og organisatoriske faktorer i betragtning gennem en livscyklustilgang. Det betyder, at den identificerer og behandler de menneskelige og organisatoriske faktorer i sikkerhedsledelsesaktiviteter, som er forbundet med forretningsmål, ledelse, drift, menneskelig ydeevne samt opgavernes og arbejdspladsens udformning i alle stadier af systemets livscyklus, f.eks. fra idriftsættelse til afvikling. En strategi for menneskelige og organisatoriske faktorer angiver en systematisk tilgang til integration af menneskelige og organisatoriske faktorer i sikkerhedsledelsesaktiviteter.

Organisationen bør inddrage relevant professionel ekspertise inden for menneskelige faktorer og organisatoriske faktorer, som er nødvendig at understøtte dens forretningsaktiviteter. Professionel ekspertise inden for menneskelige og organisatoriske faktorer indebærer, at det involverede personale bør have relevante kvalifikationer i henhold til definerede nationale og/eller internationale standarder for det pågældende emne. For eksempel ved at opfylde kravene til medlemskab af Centre for Registration of European Ergonomists eller tilsvarende organer. Store organisationer kan have en afdeling for menneskelige faktorer, hvor professionelle eksperter inden for menneskelige faktorer understøtter organisationen. En lille organisation kan give ledere på alle niveauer ansvaret for at identificere behovet for professionel ekspertise i menneskelige faktorer, hvis relevant.

Yderligere oplysninger om en strategi for menneskelige og organisatoriske faktorer findes i bilag 5.

4.6.4 Dokumentation

- *Ansøgerne gør i en strategi rede for, hvordan menneskelige og organisatoriske faktorer integreres, således at der tages relevant højde for risiciene i forbindelse med samspillet mellem menneskelig adfærd, organisatoriske forhold og teknologi i de relevante processer i sikkerhedsledelsessystemet. Det kan for eksempel indebære at have en plan for, hvordan de menneskelige og organisatoriske faktorer håndteres i forbindelse med et nyt signalsystem i alle*

livscyklussens stadier. Når ansøgerne gør dette, bør de gøre det klart, hvor der kan findes yderligere oplysninger om de relevante procedurer (4.6.1).

En brugercentreret designproces baseret på menneskelige og organisatoriske principper og metoder samt involvering af brugere anvendes i forbindelse med for eksempel ny eller ændret udformning, procedurer, træning, arbejdsbyrde og arbejdsmiljø for at sikre livslang sikkerhed og effektivitet af et system.

Der anvendes tilgængelige designstandards for menneskelige og organisatoriske faktorer og bedste praksis. Relevante standarder er for eksempel ISO 11064-serien Ergonomisk design af kontrolcentre og ISO 9241-serien Ergonomi — Interaktion mellem menneske og system.

Slutbrugere involveres i designprocessen, for eksempel i kravdefinitionen, den efterfølgende udvikling og testprocessen.

En brugercentreret designproces er en iterativ proces, der involverer flere faser. Analyser foretages for at forstå og specificere brugskonteksten (for eksempel bemanding og kompetenceanalyse, opgaveanalyse og risikoanalyse). Brugerkrav defineres ud fra disse analyser. Designløsninger, herunder design af grænseflader, arbejdspladser, træning, procedurer og organisation, udarbejdes med henblik på at opfylde brugernes krav. Evalueringer af designene foretages ved hjælp af formelle metoder såsom opgaveanalyse, simulering, risikovurdering, ekspertvurderinger, brugerevalueringer, verifikation og validering.

4.6.5 Eksempler på dokumentation

En kopi af strategien for menneskelige og organisatoriske faktorer, hvoraf det fremgår, hvordan brugen af ekspertise og teknikker inden for menneskelige og organisatoriske faktorer tages i betragtning.

Organisationen foretager ved hjælp af evidensbaserede metoder en analyse af drifts- og støtteprocesserne i alle livscyklussens stadier, lige fra udformning til bortskaffelse. Analysen bør identificere alle menneskelige og organisatoriske faktorer og de præstationspåvirkende faktorer, der har indvirkning på jernbanesikkerheden og de sikkerhedsledelsesaktiviteter, der er nødvendige for at styre risikoen.

Strategien for menneskelige og organisatoriske faktorer bør påvise de sikkerhedsledelsesaktiviteter, der er indført, samt en tilgang til at overvåge og forbedre dens effektivitet. Strategien bør baseres på en proaktiv tilgang, men omfatte reaktive aktiviteter efter behov.

De sikkerhedsledelsesaktiviteter, som er relateret til støttefunktioner og -systemer, opgavetilrettelæggelse, personaleniveauer, uddannelse, udformning og anvendelse af udstyr, procedurer og kommunikationsprotokoller, bør identificeres.

En sådan strategi kan for eksempel omfatte, hvordan menneskelige og organisatoriske faktorer integreres i ændringshåndteringsprocessen. Integration af de menneskelige faktorer er den proces, hvor menneskelige faktorer og ergonomi integreres i systemudviklingsprocessen. Integrationsplanen for de menneskelige faktorer giver en systematisk tilgang til definitionen af forbindelsen mellem alle projektaktiviteter og de menneskelige faktorer. Ved teknologi til menneskelige faktorer (human factor engineering) forstås integration af de menneskelige egenskaber i systemdefinition, design, udvikling og evaluering med henblik på at optimere menneske- maskine-ydeevnen under driftsforhold.

Hvis driftsprocesserne involverer komplekse arbejdsmønstre, bør strategien for menneskelige og organisatoriske faktorer omfatte et program for håndtering af træthedsrisiko.

4.6.6 Referencer og standarder

- Wickens, C.D., Lee, J.D., Liu, Y & Gordon Becker, S.E (2004). *An Introduction to Human Factors Engineering*. New Jersey: Pearson Education. ISBN-13: 978-0131837362
- ISO-standardserier, f.eks.
- ISO 6385:2004-serien *Ergonomiske principper for tilrettelæggelse af arbejdsystemer*
- ISO 11064-serien *Ergonomisk design af kontrolcentre*
- ISO 9241-serien *Ergonomi — Interaktion mellem menneske og system*
- ISO 10075-serien *Ergonomiske principper relateret til psykisk arbejdsbelastning*
- EEMUA 191. *Alarm systems, a guide to design, management and procurement*
- UIC 651 *Layout of driver's cabs in locomotives, railcars, multiple unit trains and driving trailers*
- Rail Safety & Standards Board (2008). *Understanding Human Factors, a guide for the railway industry*

4.6.7 Tilsynsspørgsmål

Kontrol af, at der tages højde for spørgsmål vedrørende menneskelige faktorer i beslutningstagningsprocesserne for risikohåndtering ved hjælp af risikovurdering, håndtering af ændringer og forvaltning af aktiver.

Kontrol af, at driftsdokumenterne afspejler forpligtelsen til at forvalte menneskelige faktorer gennem ergonomisk design (f.eks. brugervenligt design, almindeligt sprog, grafik til støtte for instruktionerne og nem håndtering af opdateringer) med henblik på at støtte risikohåndteringen.

Kontrol af — når det gælder overvågningen af indsatsen — at jernbanevirksomhederne/infrastrukturforvalterne i deres analyse har fokus på menneskelige faktorer som en primær eller underliggende årsag til ulykker, hændelser eller farlige tildragelser.

Kontrol af, om der er dokumenterede eksempler på trufne korrigerende foranstaltninger, som er udformet til at fjerne de faktorer, der påvirker den menneskelige ydeevne og forringer sikkerheden.

5 Drift

5.1 Planlægning og styring af driften

5.1.1 Lovkrav

- 5.1.1. I forbindelse med planlægningen, udviklingen, gennemførelsen og gennemgangen af sine driftsprocesser skal organisationen sikre, at der under driften:
- (a) anvendes risikoacceptkriterier og risikokontrolforanstaltninger (jf. 3.1.1 Risikovurdering)
 - (b) stilles en eller flere planer for, hvordan sikkerhedsmålene opfyldes, til rådighed (jf. 3.2 Sikkerhedsmål og -planlægning)
 - (c) indsamles information for at måle den korrekte anvendelse og effektiviteten af driftsrelaterede ordninger (jf. 6.1 Overvågning).
- 5.1.2. Organisationen skal sikre, at dens driftsrelaterede ordninger overholder de sikkerhedsrelaterede krav i de gældende tekniske specifikationer for interoperabilitet og relevante nationale forskrifter samt andre relevante krav (jf. 1. Organisationens kontekst).
- 5.1.3. Med henblik på at styre risici, når dette er relevant for sikkerheden i forbindelse med driften (jf. 3.1.1 Risikovurdering), skal følgende som minimum tages i betragtning:
- (a) planlægning af eksisterende eller nye togruter og -tjenester, herunder indførelsen af nye køretøjstyper, behovet for at lease køretøjer og/eller ansætte personale fra eksterne parter og udveksle information om driftsrelateret vedligeholdelse med vedligeholdelsesansvarlige enheder
 - (b) udvikling og gennemførelse af togkøreplaner
 - (c) klargøring af tog eller køretøjer inden kørsel, herunder tjek før afgang og oprangering af tog
 - (d) togtrafik eller køretøjsbevægelser på forskellige driftsvilkår (normal drift, uregelmæssig drift og nøddrift).
 - (e) tilpasning af driften i forhold til anmodninger fra enheder med ansvar for vedligeholdelse om at tage køretøjer ud af drift og meddelelse om genindsættelse i drift
 - (f) godkendelser af køretøjsbevægelser
 - (g) anvendelighed af grænseflader i trækraftenheder og togkontrolcentre samt det udstyr, der benyttes af vedligeholdelsespersonale
- 5.1.3 Med henblik på at styre risici, når dette er relevant for sikkerheden i forbindelse med driften (jf. 3.1.1. Risikovurdering), skal følgende som minimum tages i betragtning:
- a. fastlæggelse af sikre grænser for transport med henblik på trafikplanlægning og -styring ud fra infrastrukturens konstruktionsmæssige karakteristika
 - b. trafikplanlægning, herunder køreplan og kanaltildeling
 - c. trafikstyring i realtid i normal tilstand og forringet funktionstilstand, hvor der er indført anvendelsesmæssige begrænsninger i trafikken, og håndtering af afbrydelse af trafikken

d. **fastsættelse af vilkår for usædvanlige transporter.**

- 5.1.4. Med henblik på at styre allokeringen af ansvarsområder, når dette er relevant for sikkerheden i forbindelse med driften, skal organisationen fastlægge ansvarsfordelingen for den sikre koordinering og styring af togtrafikken og køretøjsbevægelser og fastlægge, hvordan relevante opgaver, der berører den sikre levering af alle ydelser, allokeres til kompetent personale i organisationen (jf. 2.3 Organisatoriske roller, ansvarsområder, ansvarlighed og bemyndigelser) og til andre eksterne, kvalificerede parter, når dette er relevant (jf. 5.3 Kontrahenter, partnere og leverandører).
- 5.1.4 Med henblik på at styre allokeringen af ansvarsområder, når dette er relevant for sikkerheden i forbindelse med driften, skal organisationen fastlægge ansvarsfordelingen for den sikre drift af jernbanenettet og fastlægge, hvordan relevante opgaver, der berører den sikre levering af alle ydelser, allokeres til kompetent personale i organisationen (jf. 2.3. Organisatoriske roller, ansvarsområder, ansvarlighed og bemyndigelser) og til andre eksterne, kvalificerede parter, når dette er relevant (jf. 5.3. Kontrahenter, partnere og leverandører).
- 5.1.5. Med henblik på at styre information og kommunikation, når dette er relevant for sikkerheden i forbindelse med driften (jf. 4.4 Oplysning og kommunikation), skal det relevante personale (f.eks. togpersonalet) underrettes om de nærmere omstændigheder ved eventuelle særlige kørselsbetingelser og herunder relevante ændringer, som kan udmønte sig i en fare, midlertidige eller varige driftsmæssige begrænsninger (eksempelvis i forhold til særlige køretøjstyper eller særlige ruter) og vilkår for usædvanlige transporter, når det er relevant.
- 5.1.5 Med henblik på at styre information og kommunikation, når dette er relevant for sikkerheden i forbindelse med driften (jf. 4.4 Oplysning og kommunikation), skal det relevante personale (f.eks. trafikledere) oplyses om særlige krav til ruteføring for tog og køretøjsbevægelser og herunder relevante ændringer, som kan udmønte sig i en fare, midlertidige eller varige driftsmæssige begrænsninger (eksempelvis som følge af sporvedligeholdelse) og vilkår for usædvanlige transporter, når dette er relevant.
- 5.1.6. Med henblik på at styre kompetencer, når dette er relevant for sikkerheden i forbindelse med driften (jf. 4.2 Kompetencer), skal organisationen i overensstemmelse med gældende lovgivning sikre (jf. 1. Organisationens kontekst), at:
- (a) personalets uddannelse og arbejdsinstrukser overholder forskrifterne, og at der træffes korrigerende foranstaltninger, når det er påkrævet
 - (b) tilbyde personalet særlig uddannelse, hvis der ventes ændringer, som påvirker gennemførelsen af driften eller personalets opgavebeskrivelse
 - (c) vedtage egnede foranstaltninger for personalet efter ulykker og hændelser.

5.1.2 Formål

Ansøgerne bør påvise, at de har indført relevante processer til at håndtere driftsmæssige risici via sikkerhedsledelsessystemet. De bør bl.a. sikre, at medarbejderne forstår deres roller, de driftsmæssige risici, de står overfor, og hvilke kontrolforanstaltninger der er, og at medarbejderne har den nødvendige kompetence og uddannelse til at håndtere disse i henhold til sikkerhedsledelsessystemets dokumentation.

Ansøgerne bør sikre, at køretøjerne eller infrastrukturen drives sikkert i henhold til de gældende krav under forskellige driftsvilkår (dvs. normal drift, uregelmæssig drift og nøddrift). Dette omfatter også brugen af aktiver til testformål (f.eks. test af køretøjers køreegenskaber, inden der gives tilladelse) og under særlige omstændigheder (f.eks. usædvanlige transporter såsom transport af store, udelelige stykker, der ikke kan transporteres med andre transportmidler, for eksempel betonbjælker/overliggere til broer osv.).

5.1.3 Forklarende noter

I punkt 5.1.3, 5.1.4 og 5.1.5 i ovennævnte juridiske tekst erstattes bestemmelserne i sort med bestemmelserne med blå, i de tilfælde hvor kravet vedrører infrastrukturforvaltere.

I henhold til direktiv (EU) 2016/798 skal jernbanevirksomheder og infrastrukturforvaltere indføre et sikkerhedsledelsessystem for at styre de sikkerhedsrisici, der er forbundet med deres jernbanedrift. Inden for sikkerhedsledelse er der almindelig enighed om, at sikkerheden i videst muligt omfang bør integreres i de normale forretningsgange. Årsagen til dette er, at virksomhedens fokus i så fald er lige så meget på sikkerhed som på alle andre forretningsgange, hvilket vil reducere konflikterne mellem de forskellige processer.

Det fremgår af ISO's vejledende dokument (N360), som ledsager Annex SL, at sigtet med artikel 8 (Drift) er at specificere de elementer, der skal gennemføres under organisationens drift for at sikre, at ledelsessystemkravene opfyldes, og at de vigtige risici og muligheder tackles. Det nævnes desuden, at yderligere (disciplinspecifikke) krav i forbindelse med planlægning og styring af driften kan fastlægges. Der står navnlig, at de ikke går ud over virksomhedens forretning, men giver tilstrækkelige rammer til at kontrollere, hvordan vigtige sikkerhedsspørgsmål bliver håndteret i organisationens forretningsgange.

Der er tilføjet udtrykkelige forbindelser mellem de driftsmæssige krav og andre ledelsessystemkrav (tilsvarende den tilgang, der anvendes i bilag III til ECM-forordningen) for at understrege, at der skal tages højde for specifikke driftsmæssige krav, når det gælder de relevante ledelsessystemkrav (f.eks. er jernbanevirksomhedernes ruteplanlægning en aktivitet, der bør være genstand for risikovurdering). Denne tilgang er ikke beregnet på at være udtømmende, men tager sigte på at identificere særlige forhold, som myndighederne (på baggrund af deres erfaring) betragter som signifikante, og som derfor bør undersøges i forbindelse med deres vurdering eller tilsynsaktiviteter. Jernbanevirksomhederne og infrastrukturforvalterne bør ikke blot fokusere på disse specifikke krav, når de udvikler og gennemfører deres sikkerhedsledelsessystem (og f.eks. se bort fra andre sikkerhedsrisici).

Jernbanevirksomhederne og infrastrukturforvalterne skal under alle omstændigheder anvende kravene til sikkerhedsledelsessystemer (f.eks. risikovurdering, overvågning, kompetence, oplysning og kommunikation) på alle deres relevante forretningsgange for at påvise, at sikkerhedsrisiciene styres i passende omfang.

Sikkerhedsledelsessystemets integration i forretnings-/driftsprocesserne er af afgørende betydning, og for at nå dette mål skal organisationen overholde de gældende tekniske specifikationer for interoperabilitet (5.1.2) såsom TSI OPE samt meddelte nationale forskrifter, når grænsefladekravene ikke er fuldstændigt dækket af de tekniske specifikationer for interoperabilitet. Acceptable måder for overholdelse af krav kan også offentliggøres af medlemsstaten eller dens myndighed for at lette overholdelsen af de nationale regler. Som minimum bør følgende driftsprocesser tages i betragtning, hvor det er relevant:

- *infrastrukturdrift (styring af infrastrukturruter og udstyr, autorisation af køretøjsbevægelser under alle betingelser og sikring af infrastrukturvedligeholdelse: spor-, togkontrol- og signalsystem(er))*
- *togdrift (udvikling af ruter og relevante køreplaner, administration af togklargøring, sikring af togkørsel, ledsagelse, test, vedligeholdelse og reparation af køretøjer)*
- *rangering (flytning af køretøjer med henblik på at samle et tog eller skille det ad).*

TSI OPE er vigtige her, da de indeholder de grundlæggende driftsprincipper ("Fundamental Operating Principles", FOP), som bør afspejles i de relevante dele af sikkerhedsledelsessystemet, og derfor kan overensstemmelsen med TSI OPE anvendes til at påvise overholdelse af de relevante krav til sikkerhedsledelsessystemer, der er nævnt ovenfor.

Udveksling af oplysninger til driftsmæssige formål om vedligeholdelse (**5.1.3 (a)**) med ECM'er og ihæندهavere er omhandlet i artikel 5, stk. 3, i ECM-forordningen. Dette omfatter vedligeholdelsesplanen og de restriktioner, som ECM'en har fastlagt under vedligeholdelsen (planlægning på kort sigt).

Hvis der henvises til udvikling og gennemførelse af togkøreplaner (**5.1.3 (b)**), betyder dette, at ansøgerne

bør påvise, hvordan de ved hjælp af risikovurdering har håndteret den risiko, som aktiviteten udgør inden for deres organisation og ved grænsefladen til andre aktører, f.eks. påvise, at de har taget højde for

- *den yderligere arbejdsbyrde for trafiklederne, når antallet af tog på visse tidspunkter forøges*
- *passende driftsaftaler med den eller de relevante infrastrukturforvalter(e) om standsning af trafikken, udbedring, udveksling af oplysninger og alle andre tjenester, der anses for at være nødvendige*
- *håndtering af risiciene i forbindelse med sporvedligeholdelse, når togene kører 24 timer i døgnet.*

Nye togtjenester **(5.1.3 (a))** kan omfatte nye typer gods, der skal transporteres.

Køretøjsbevægelser **(5.1.3 (d))** har en bredere betydning end togbevægelser (dvs. planlagte køretøjsbevægelser) og tilladelser, der gives inden togafgang. Det kan også omfatte udbedring af et tog, der er gået i stykker, flytning af maskiner til sporvedligeholdelse eller ikke-planlagt udskiftning af en beskadiget togvogn før et togs afgang.

I overensstemmelse med UIC leaflet 502-1, artikel 1, stk. 1, foreslås følgende definition af termen "usædvanlige transporter" **(5.1.5)**: *"En transport betragtes som usædvanlig, hvis dens eksterne dimensioner, vægt eller karakteristika med hensyn til fast udstyr eller en vogn hos en jernbanevirksomhed, der er involveret i transporten, skaber særlige vanskeligheder, og den derfor kun kan accepteres under særlige tekniske vilkår eller driftsvilkår".*

Infrastrukturforvalteren bør identificere og angive betingelser og foranstaltninger til at anvende et køretøj til test på nettet inden for den givne tidsfrist, som angivet i artikel 21, stk. 3, og artikel 21, stk. 5, i direktiv (EU) 2016/797 **(5.1.2)**.

Registreringer af rutekompatibilitetskontroller omfatter karakteristika for køretøj/tog set i forhold til de planlagte driftsruter, herunder eventuelle afvigelsesruter, der er identificeret af infrastrukturforvalterne (TSI OPE (EU) 2015/995 4.2.2.5).

Karakteristika for driftsruter er på grundlag af infrastrukturregister (RINF) og/eller oplysninger fra infrastrukturforvalteren.

Hvis der identificeres problemer af en af parterne, bør jernbanevirksomheden og infrastrukturforvalteren træffe beslutning i fællesskab.

Menneskelige og organisatoriske faktorer bør tages i betragtning ved planlægning af driften i forbindelse med f.eks. vagtplaner, træthedshåndtering, stress, arbejdsmiljø (fysisk og psykosocialt), arbejdspladser, arbejdsprocesser osv.

Planlægningen og styringen af driften udvikles med henblik på løbende forbedring af sikkerhedskulturen. Sikkerhedskulturen bør tages i betragtning i forbindelse med f.eks. arbejdsbyrde, arbejdsmiljø (fysisk og psykosocialt), arbejdsprocesser osv. Formålet er at sikre, at konsekvenserne af tiltag eller ændringer ikke har negativ indvirkning på den menneskelige ydeevne eller organisationens sikkerhed.

5.1.4 Dokumentation

- *Oplysninger om, at organisationen, når den planlægger, udvikler, gennemfører og gennemgår sine driftsprocesser, stræber efter at opfylde sikkerhedsmålene, træffer risikovurderingsforanstaltninger og overvåger resultaterne, herunder passende henvisninger til, hvor der kan findes yderligere oplysninger om procedurerne **(5.1.1 (a)-(c))**.*
- *Dokumentation for, at organisationen er bevidst om og reelt gennemfører alle kategorier af obligatoriske sikkerhedskrav, der gælder for driften, og skitserer, hvordan sikkerhedsledelsessystemet sikrer overholdelsen af dem.*
- *Oplysninger om, at ansøgerne sikrer, at deres driftsrelaterede tiltag overholder de gældende krav (lovgivning, standarder osv.) **(5.1.2)**.*
- *I forbindelse med typegodkendelser og/eller ibrugtagningstilladelser for er infrastrukturforvalteren i stand til at identificere og sørgе for **(5.1.2)**:*

- driftsbetingelser for anvendelsen af køretøjet til test på nettet, baseret på de oplysninger, som ansøgerne fremlagde til godkendelsen
 - alle nødvendige foranstaltninger, der skal træffes på infrastrukturplan for at sørge for sikker og pålidelig drift under testene på nettet, og/eller
 - alle nødvendige foranstaltninger i infrastrukturanlæggene for at udføre testene på nettet.
- Hvad angår kontrollen inden brug af godkendte køretøjer (omarbejdning af artikel 23, stk. 1, i interoperabilitetsdirektivet (IOD)) og især rutekompatibilitetskontrollen (omarbejdning af artikel 23, stk. 1, litra a), b), i IOD), kan jernbanevirksomheden inden for sit sikkerhedsledelsessystem identificere og tilvejebringe ((5.1.3 (a)) CSM SMS)) bevisprocedurer og registreringer, der viser, at køretøjet er foreneligt med den rute, på hvilken det skal idriftsættes, og er korrekt integreret i togets oprangering (jf. også TSI OPE 2015/995 4.2.2.5).
 - Dokumentation for de driftsrelaterede dokumenters overensstemmelse med kravene til forvaltning af drift (og vedligeholdelse) ved de organisatoriske og fysiske grænser, f.eks. de organisatoriske, tekniske og driftsmæssige grænseflader til naboinfrastruktur, grænsestationer, samarbejde med andre jernbanevirksomheder eller infrastrukturforvaltere osv. **(5.1.2)**.
 - Oplysninger om, hvordan risiciene ved driftsaktiviteter håndteres ved hjælp af risikovurderingsprocessen og dækker de elementer, der er medtaget i ovennævnte krav **(5.1.3 (a),(c)-(f))**.
 - Dokumentation for, at artikel 14, stk. 2, i direktiv (EU) 2016/798 overholdes af enheden med ansvar for vedligeholdelse **(5.1.3 (f))**.
 - Oplysninger om, hvordan ansvaret, herunder ansvaret for håndtering af træthedsrisikoen, styres med henblik på driftsaktiviteternes sikkerhed **(5.1.4)**.
 - Oplysninger om, hvordan organisationen styrer information og kommunikation med henblik på driftsaktiviteternes sikkerhed **(5.1.5)**.
 - Oplysninger om kompetencestyringssystemet og de hermed forbundne procedurer, samt hvordan disse hænger sammen med specifikke arbejdsinstrukser med det formål at opretholde driftsaktiviteternes sikkerhed **(5.1.6)**.
 - Dokumentation for, at de driftsrelaterede dokumenter (procedurer, arbejdsinstrukser osv.) opdateres, når og hvor det er nødvendigt **(jf. også 4.5.3)**.

5.1.5 Eksempler på dokumentation

En liste over de obligatoriske krav (herunder de tekniske specifikationer for interoperabilitet), og hvordan organisationen overholder dem **(jf. også 2)**.

En forklaring af, hvordan de driftsmæssige risici håndteres ved hjælp af risikovurderingsprocessen, og hvordan det sikres, at sikkerhedsmålene for driften opfyldes. Der medtages links til, hvor de relevante procedurer kan findes.

En angivelse af, hvordan kompetencestyringssystemet bidrager til styring af de driftsmæssige risici, og hvordan oplysnings- og kommunikationsflowet håndteres for at sikre, at risici styres korrekt.

Nærmere oplysninger om vedligeholdelsessystemet for rullende materiel, herunder links til detaljeret dokumentation til støtte for dette (såfremt der ikke er nogen ECM eller certificeringsordning).

Nærmere oplysninger om de tjek før afgang (TSI OPE), der er indført for at sikre overensstemmelseskontrollen af:

- bremseevne (udarbejdelse af bremseseddel)
- togenes oprangering
- signaler foran og bagpå
- belastning og betingelser for trukne køretøjer.

En kopi af processen for identifikation af afvigelser, og hvordan det sikres, at alle nødvendige foranstaltninger træffes, f.eks. foranstaltninger, der medfører, at køretøjet tages ud af drift, at ødelagte/defekte komponenter/udstyr/køretøjer udskiftes, eller at der indføres driftsmæssige begrænsninger.

Et dokument, der angiver de køretøjstyper, som skal anvendes på de enkelte særlige ruter, og den type aktiviteter, der skal udføres, navnlig eventuelle:

- *driftsmæssige begrænsninger som følge af særlige køretøjstyper*
- *begrænsninger som følge af anvendelsen af særlige køretøjstyper på særlige ruter*
- *yderligere vedligeholdelseskrav for særlige ruter (jf. også 5.2).*

Et dokument, der beskriver eventuelle yderligere krav til håndteringen af uregelmæssige situationer (f.eks. hændelser med et køretøj) for det eller de pågældende net, der ligger inden for driftsområdet.

Der er en proces for træthedshåndtering, som er gældende for de medarbejdere, der har uregelmæssige arbejdstider. Processen bygger på evidensbaserede metoder og professionel ekspertise. I processen tages der højde for, at en række faktorer skal tages i betragtning ved en samlet tilgang til håndtering af træthedsrisiko. Træthedshåndtering bør omfatte planlægning og styring af arbejdsmiljøet og arbejdsopgaverne for så vidt muligt at minimere trætheds indvirkning på medarbejdernes årvågenhed og ydeevne, hvilket skal ske på en måde, der passer til risikoeksponeringsniveauet og driftens karakter.

Hvad angår overholdelsen af de grundlæggende driftsprincipper (FOP) i TSI OPE, fremlægges der dokumentation for, at jernbanevirksomheden kan sikre følgende (kun til illustrative formål):

- *Et tog må kun køre på en del af en linje, hvis togets oprangering er forenelig med infrastrukturen (FOP 3)*

Dette drejer sig om en bekræftelse af togets forenelighed med infrastrukturen på den rute, det planlægges at køre på, før der gives tilladelse til kørsel. Foreneligheden mellem et tog og infrastrukturen påvirkes primært af køretøjets dimensioner og enhver last, der placeres på det, frirummet mellem toget og infrastrukturen eller togene på de tilstødende spor (sporvidden), togets minimumsbremseevne, et togs vægt og længde samt infrastrukturens kapacitet og funktion.

Der er dokumentation for, at:

- *der foretages tjek før afgang for at sikre — før et tog begynder eller fortsætter sin rejse — at dets passagerer, personale og gods transporteres sikkert (FOP 4)*

Dette vedrører toget, og hvorvidt det er klar til at køre. Det omfatter f.eks. følgende: togets bremseevne, den hastighed, som toget må køre med, togets sammensætning og sammenkobling, identifikation, lastning og sikring af gods, tilstrækkelige oplysninger til togklargøring og driftspersonalet. Formålet er at forhindre togsammenstød og afsporinger som følge af en række risici.

5.1.6 Referencer og standarder

- *ISO N360 JTCG konceptdokument til støtte for AnnexSL*
- *UIC leaflet 502-1*
- [*RID*](#)
- *Vejledning om TSI OPE*

5.1.7 Tilsynsspørgsmål

Tilsynet med driftsaktiviteter bør finde sted med fokus på særskilte områder, som undersøges nøje for at se, hvordan de afspejles i sikkerhedsledelsessystemet hos den organisation, der føres tilsyn med, og hvorvidt den har det rigtige personale, som gør det rigtige på det rigtige sted. Dette vil gøre det muligt for den nationale sikkerhedsmyndighed at se, om aktiviteterne er dækket ind under sikkerhedsledelsessystemet som en sammenhængende helhed eller administreres separat med svage forbindelser til sikkerhedsmålene og den overordnede strategi.

Tilsynet bør navnlig tjekke:

- *Hvordan dokumenter vedrørende sikkerhedsledelsessystemet omsættes til ensartede lokale instrukser, der anvendes til at styre risiko på driftsniveauet.*
- *Håndtering af nødsituationer eller ikke-rutinemæssige situationer.*
- *Hvordan driftsgrænser/driftsbegrænsninger håndteres, herunder grænsefladerne til andre parter.*
- *Tiltag til håndtering af træthed.*
- *Håndtering af farlige stoffer.*
- *Regler for transport af farligt gods, herunder uddannelse, roller og ansvarsområder for organisationens personale, som i kapitel 1.3, 1.4 og 1.8 i RID samarbejder efter behov med andre kompetente myndigheder på området for transport af farligt gods.*
- *Overensstemmelse med de grundlæggende driftsprincipper i TSI OPE.*

5.2 Forvaltning af aktiver

5.2.1 Lovkrav

- 5.2.1. Organisationen skal styre sikkerhedsrisici i tilknytning til fysiske aktiver i hele deres livscyklus (jf. 3.1.1. Risikovurdering) fra udformning til bortskaffelse og opfyldte kravene vedrørende menneskelige faktorer i alle livscyklusfaser.
- 5.2.2. Organisationen skal:
- (a) sikre, at aktiverne benyttes til det tiltænkte formål, samtidig med at deres sikre driftstilstand, artikel 14, stk. 2, i direktiv (EU) 2016/798, når dette er relevant, og deres forventede funktion opretholdes
 - (a) sikre, at aktiverne benyttes til det tiltænkte formål, samtidig med at deres sikre driftstilstand og forventede præstationsniveau vedligeholdes
 - (b) forvalte aktiverne under normal og uregelmæssig drift
 - (c) påvise tilfælde af manglende overensstemmelse med kravene til driften før eller under driften af aktivet, så hurtigt som praktisk muligt, herunder indføre driftsmæssige begrænsninger om nødvendigt for at sikre, at aktivets sikre driftstilstand opretholdes (jf. 6.1. Overvågning).
- 5.2.3. Organisationen skal sikre, at dens ordninger for forvaltning af aktiver i relevante tilfælde overholder alle væsentlige krav i de gældende tekniske specifikationer for interoperabilitet (jf. 1. Organisationens kontekst).
- 5.2.4. Med henblik på at styre risici, når dette er relevant for levering af vedligeholdelse (jf. 3.1.1. Risikovurdering), skal følgende som minimum tages i betragtning:
- (a) fastlæggelse af behovet for vedligeholdelse med henblik på at bevare aktivet i en sikker driftstilstand ud fra den planlagte og den faktiske brug af aktivet og dets konstruktionsmæssige karakteristika
 - (a) fastlæggelse af behovet for vedligeholdelse med henblik på at bevare infrastrukturen i en sikker driftstilstand ud fra den planlagte og faktiske brug af infrastrukturen samt dennes konstruktionsmæssige karakteristika
 - (a) styring af, at aktivet tages ud af drift med henblik på vedligeholdelse, hvis defekter er påvist, eller når aktivets tilstand forringes uden for kriterierne for sikker driftstilstand som omhandlet i litra a)
 - (b) styring af aktivets genindsættelse i drift, eventuelt med anvendelsesmæssige begrænsninger efter vedligeholdelse med det formål at sikre, at det er i en sikker driftstilstand
 - (c) styring af overvågnings- og måleudstyr for at sikre, at det er egnet til det tilsigtede formål.
- 5.2.4. Med henblik på at styre information og kommunikation, når dette er relevant for en sikker forvaltning af aktiver (jf. 4.4. Information og kommunikation) skal organisationen tage følgende i betragtning:
- (a) udveksling af relevant information internt i organisationen eller med eksterne vedligeholdelsesansvarlige enheder (jf. 5.3. Kontrahenter, partnere og leverandører), navnlig med hensyn til sikkerhedsrelaterede funktionsfejl, ulykker og hændelser samt eventuelle begrænsninger i anvendelsen af aktivet
 - (b) sporbarheden af al nødvendige information og herunder information i relation til litra a) (jf. 4.4. Information og kommunikation, og 4.5.3. Styring af dokumenteret information)
 - (c) etableringen og vedligeholdelsen af registre over alle aktiver og herunder styringen af ændringer, der påvirker aktivers sikkerhed (jf. 5.4. Styring af ændringer).

5.2.2 Formål

Ansøgerne bør påvise, hvordan de forvalter deres aktivers livscyklus lige fra design til bortskaffelse ved hjælp af de procedurer og regler, der er fastlagt i sikkerhedsledelsessystemet. Ansøgerne bør påvise, at de har anvendt en menneskecentreret tilgang i alle livscyklussens stadier. De bør angive, hvor forvaltningen af deres aktiver kommer i berøring med forskellige elementer af deres sikkerhedsledelsessystem såsom kompetencestyring, planlægning af driften og overvågning. Ansøgerne bør have den målsætning at påvise, at de har indført et solidt system til forvaltning af aktiver, som afspejler de risici, driftens type og omfang giver.

5.2.3 Forklarende noter

Ved "aktiv" (5.2) forstås ethvert stykke udstyr (fast eller mobilt), enhver struktur, software eller anden komponent, som kræver løbende vedligeholdelse, og som anvendes til jernbanedrift. Aktiver opdeles i dem, der forvaltes af jernbanevirksomheden (hovedsagelig køretøjer), og dem, der forvaltes af en infrastrukturforvalter (alle infrastrukturkomponenter såsom spor, togkontrol- og signaludstyr, udstyr til skift fra et spor til et andet, strømforsyning, jernbaneoverkørsler, anlægsarbejde som broer, viadukter, tunneller, perroner, elevatorer, rulletrapper osv. En komplet liste findes i bilag I til direktiv (EU) 2012/34.

Et aktivs livscyklus omfatter følgende faser:

- a) design
- b) implementering (konstruktion/fremstilling, installation, test og idriftsættelse)
- c) drift og vedligeholdelse
- d) reparation, ændring og modernisering, som involverer styring af ændringer
- e) fornyelse, udrangering og bortskaffelse.

Det er vigtigt for en organisation at vise, hvordan den fastholder og vedligeholder (system- og sikkerhedskravene vedrørende sine aktiver, og hvordan disse kontrolleres, valideres og spores.

Hvis vedligeholdelsen udliciteres til en tredjepart, er det organisationens ansvar at specificere og overvåge, at aktivets funktion er i overensstemmelse med organisationens fastlagte standarder.

Lige så snart der er indført processer til håndtering af de risici, der er forbundet med sikkerhedskritiske aktiver, overvåger organisationen aktivernes funktion i forhold til disse risici og dens egne forventninger.

Hvis det er sandsynligt, at aktiver skal fornys, udrangeres eller bortskaffes, fastlægger og dokumenterer organisationen processerne til håndtering af eventuelle risici i forbindelse med sådanne aktiviteter.

Disse processer er kun relevante for organisationer, der udfører eller vil kunne udføre sådanne aktiviteter.

I forbindelse med fornyelsen af et aktiv, der er ved at være udtjent, sikrer organisationen, at erstatningsaktivet opfylder sikkerhedskriterierne. Som en del af denne proces gennemgås alle sikkerhedsanalyserne.

Krav vedrørende vedligeholdelse (5.2.4) stammer fra ECM-forordningen, idet godsvogne er et aktiv, som en jernbanevirksomhed og evt. en infrastrukturforvalter bør forvalte. Kravene i ECM-forordningen er mere specifikke og konkrete, mens ovenstående krav hovedsagelig omhandler grænsefladen mellem jernbanevirksomhedens eller infrastrukturforvalterens sikkerhedsledelsessystem og ECM'ens vedligeholdelsessystem med det formål at sikre, at aktiverne er sikre at bruge og vedligeholde. Risikovurderingen bør ligeledes medtage den potentielle sikkerhedspåvirkning af enhver udskiftning i forbindelse med vedligeholdelsen (som hører med til aktivets livscyklus) i henhold til kravene i direktiv (EU) 2016/797 og de relevante tekniske specifikationer for interoperabilitet.

Det er ikke alle aktiver, der reguleres af tekniske specifikationer for interoperabilitet (5.2.3), og selv om en TSI er gældende (f.eks. TSI INF), er det kun det, der er nødvendigt for interoperabiliteten, som reguleres, hvilket betyder, at der stadig kan være brug for andre sikkerhedskrav. Overholdelse af de væsentlige krav i de relevante TSI'er (og ikke kun de væsentlige sikkerhedskrav) er stadig nødvendigt i tilfælde af udskiftning, fornyelse eller opgradering i henhold til bestemmelserne i direktiv (EU) 2016/797.

Termen "sikker driftstilstand" (5.2.4 (a)) betyder, at aktivet skal anvendes inden for dets sikre brugsgrænser.

De sikre brugsgrænser kan udvikle sig i hele systemets levetid, men de skal fastlægges under hensyntagen til interoperabilitetsparametrene. Der kan identificeres mangler **(5.2.4 (b))**, og på baggrund af en root cause-analyse kan de sikre brugsgrænser tilpasses tilsvarende. For køretøjer har sikker driftstilstand den betydning, der er angivet i artikel 14, stk. 2, i direktiv (EU) 2016/798.

Aktivernes konfiguration **(5.2.5 (c))** omfatter den unikke identifikation af aktiverne, deres placering, eventuel udført vedligeholdelse osv. (og ikke blot konfigurationsstyringen af ændringer). Konfigurationsstyringen af (tekniske) ændringer er gældende for udskiftning.

Der skal udpeges en enhed med ansvar for vedligeholdelse (ECM) i henhold til artikel 14, stk. 1, i direktiv (EU) 2016/798 for at sikre, at de køretøjer, hvis vedligeholdelse enheden har ansvaret for, er i en sikker driftstilstand. Det er ikke nødvendigt med en detaljeret beskrivelse af de aktiviteter, der udføres af en ECM, som er certificeret i henhold til forordning (EU) 445/2011. Til gengæld er det nødvendigt at angive, hvilke elementer og hvilke aspekter der er dækket af ECM-certifikatet, og hvordan grænsefladen til ECM'en forvaltes, navnlig hvilke oplysninger der udveksles mellem ansøgeren og ECM'en, og hvordan dettesker.

Hvad angår køretøjer vedligeholdt af ikke-certificerede ECM'er (dv'. ECM'er, som ikke er certificeret i henhold til forordning (EU) 445/2011), er det ansøgernes ansvar at sikre, at de køretøjer, de anvender, er i en sikker driftstilstand, ved at holde øje med, at de ikke-certificerede ECM'er har udviklet og gennemført deres vedligeholdelsessystem på en effektiv måde i henhold til artikel 14, stk. 2, artikel 14, stk. 3, og bilag III i direktiv 2016/798. Såfremt de ikke-certificerede ECM'er ikke tilhører ansøgerens organisation, bør overholdelsen af lovkravene sikres ved hjælp af kontraktlige aftaler.

I tilfælde af et partnerskab mellem jernbanevirksomheder forbliver hver jernbanevirksomhed fuldt ud ansvarlig for en sikker drift og dermed for styringen af risici i forbindelse med sine aktiviteter, herunder levering af vedligeholdelsesfunktioner for køretøjer. Det er ikke tilstrækkeligt, at en jernbanevirksomhed bruger sin partnerjernbanevirksomheds sikkerhedscertifikat som et middel til at styre risiciene i forbindelse med levering af vedligeholdelse, hvis det ikke underbygges af kontraktlige aftaler mellem partnerjernbanevirksomhederne. Disse kontraktlige aftaler skal udvikles i fællesskab og overvåges af den enkelte partner. De er også en del af de enkelte sikkerhedsledelsessystemer, og derfor er de genstand for de respektive nationale sikkerhedsmyndigheders tilsyn. De respektive nationale sikkerhedsmyndigheder bør koordinere deres indsats for at håndtere eventuelle grænseoverskridende grænsefladeproblemer, som de kontraherende enheder har skabt.

5.2.4 Dokumentation

- *Oplysninger om systemet til forvaltning af aktiver inden for organisationens sikkerhedsledelsessystem, herunder relevante forbindelser til andre områder såsom risikovurdering, planlægning af driften, håndtering af ændringer osv. (5.2.1), (5.2.2), (5.2.5 (a)-(b)):*

Designfasen

- *Dokumentation for processer og høring med henblik på at fastlægge kravene til aktiverne.*
- *Dokumentation for risikohåndteringsstrategier i forbindelse med indkøb og idriftsættelse af nye eller ændrede aktiver.*
- *Dokumentation for alle relevante processer for design og levering af aktiver.*
- *Processerne for håndtering af risici i designfasen.*
- *Dokumentation for de redskaber, der anvendes til at garantere sikkerheden.*
- *Nærmere oplysninger om de standarder eller andre sikkerhedsoplysninger, der følges ved design og vedligeholdelse af aktivet, samt eventuelle test, der anvendes til at bekræfte overensstemmelsen.*
- *Eksistensen af en manual eller lignende, som medtager processerne for drift og vedligeholdelse af aktiver og for håndtering af risici i drifts- og vedligeholdelsesfasen.*

Implementeringsfasen

- Dokumentation for de processer for sikkerhedsrisikohåndtering, test og validering, der dækker konstruktion/fremstilling og idriftsættelse af aktivet, og hvorvidt det er driftsklart.

Drifts- og vedligeholdelsesfasen

- Dokumentation for den aktuelle overensstemmelse med standarder og processer samt håndtering af de identificerede risici.
- Vedligeholdelsesplaner og -procedurer for aktiverne.
- Dokumentation for organisationens aktiviteter med hensyn til at identificere og fjerne risici.
- Dokumentation for de processer, der anvendes til at rapportere og administrere eventuelle funktionsproblemer og korrigerende foranstaltninger.
- Dokumentation for, at funktionen sammenlignes med et aktivs forventede strategiske levetid med henblik på at tjekke funktionen og planlægge fornyelser.
- Processerne for at identificere fejl og mangler og iværksætte korrigerende foranstaltninger.
- Håndtering af nødsituationer eller ikke-rutinemæssige situationer, som kan have indflydelse på aktivets sikkerhed.
- Dokumentation for, at forvaltning af aktiver tages i betragtning ved tilfælde, der skal anmeldes, og håndtering af delte risici ved grænsefladerne (jf. også 3.1).

Fornyelses-, udrangerings- og bortskaffelsesfasen

- Dokumentation for processerne håndtering af risici i forbindelse med fornyelse, udrangering eller bortskaffelse af aktiver, alt efter hvad der er relevant for organisationens omfang og karakter.
- Dokumentation for en systematisk tilgang til de menneskelige og organisatoriske faktorer i alle livscyklusstadier af forvaltningen af aktiver (5.2.1).
- Dokumentation for de driftsrelaterede dokumenters overensstemmelse med kravene til forvaltning (drift) og vedligeholdelse ved de organisatoriske og fysiske grænser, f.eks. de organisatoriske, tekniske og driftsmæssige grænseflader til naboinfrastruktur, grænsestationer og samarbejde med andre jernbanevirksomheder eller infrastrukturforvaltere (5.2.3).
- Oplysninger om, at ansøgerne påviser, at deres vedligeholdelsesordninger overholder de relevante krav (lovgivning, standarder osv.) (5.2.3).
- Såfremt der er tale om køretøjer, en kopi af ECM-certifikatet eller dokumentation for, at artikel 14, stk. 2, artikel 14, stk. 3, og bilag III i direktiv (EU) 2016/798 overholdes af enheden med ansvar for vedligeholdelse (5.2.4 (a)-(d)).

Såfremt der er tale om partnerskaber mellem jernbanevirksomheder, hvor køretøjet vedligeholdes af en partner:

Dokumentation for, at der er indgået kontraktlige aftaler mellem partnerne, herunder:

- udveksling af oplysninger som beskrevet i artikel 5 i forordning (EU) 445/2011
- teknisk support, når det er påkrævet, navnlig med hensyn til togkontrollsystemer
- kontrol af de kontraherende vedligeholdelsesværksteders evne til at udføre vedligeholdelse
- overvågning af køretøjer og udveksling af relevante oplysninger som følge af denne overvågning (jf. også 6.1).
- Såfremt der er tale om aktiver, hvor der kræves et overensstemmelsescertifikat i henhold til EU-lovgivningen eller nationale regler, en kopi af dette certifikat ledsaget af en forklaring af, i hvilket omfang det anvendes som et led i sikkerhedsledelsessystemet (5.2.4 (a)-(d)).
- Oplysninger om, hvordan dokumentstyringen, som hører med til sikkerhedsledelsessystemet, fungerer med hensyn til forvaltning af aktiver, herunder dokumentation for, at vedligeholdelsesdokumentationen (procedurer, arbejdsinstrukser osv.) opdateres, når og hvor det er nødvendigt (5.2.5 (a)-(c)).
- Dokumentation for konfigurationsstyringen af aktiver i hele deres livscyklus, herunder eventuelle ændringsstyringsprocesser, som er indført med henblik på at styre grundlæggende rekonfigurationer (5.2.5 (c)).

5.2.5 Eksempler på dokumentation

Designfasen

Organisationen dokumenterer alle relevante processer og oplysninger, som vedrører design og leveringen af aktiver, ved hjælp af konfigurationsstyringsprocesser (eller et konfigurationsstyringssystem). Disse skitserer de tekniske og organisatoriske aktiviteter, som fastlægger og opretholder kontrollen med aktivet i hele dets livscyklus.

Organisationen fastlægger og dokumenterer en proces til håndtering af de risici, der er forbundet med designet af aktivet, ved at:

- *fastsætte kravene til alle nye og/eller ændrede aktiver (jf. også 1) og høre de relevante interessenter om dem (jf. også 2.4)*
- *håndtere de risici, der er forbundet med sådanne ændrings gennemførelse (jf. også 3.1), og*
- *håndtere de risici, der er forbundet med indkøb af aktiver og kontraktstyring, hvor dette er relevant (jf. også 3.1 og 5.3).*

Dette omfatter fare- og sikkerhedsanalyser for at identificere de områder, der har den største risiko for fejl, i forhold til organisationens farelogbog. Dette kan opnås ved at identificere sikkerhedskritiske systemer og opstille centrale målsætninger for indsatsen ved hjælp af passende risikoidentificeringsteknikker såsom:

- *en RAMS-analyse (pålidelighed, tilgængelighed, vedligeholdelsesvenlighed og sikkerhed) af aktivernes udformning (hvor de centrale kriterier for indsatsen på sikkerhedsområdet meddeles til designerne for at sikre, at aktivet er egnet til formålet) og*
- *en analyse af fejltilstande, virkninger og kritikalitet ("Failure Modes, Effects and Criticality Analysis", FMECA) og/eller af pålidelighedscentreret vedligeholdelse ("Reliability Centred Maintenance", RCM) med henblik på at håndtere risiciene i designfasen og støtte udarbejdelsen af en vedligeholdelsesplan.*

Disse krav styres efter de specifikke standarder og processer, der anvendes til udformning, vedligeholdelse og drift af jernbaneinfrastruktur og rullende materiel, sådan som de identificeres af organisationen. Organisationens påviser, at:

- *sikkerhedskritiske systemer udformes efter funktionelle specifikationer*
- *der er en testplan for validering og idriftsættelse, som bekræfter, at aktivet er egnet til formålet og er sikkert at bruge og vedligeholde, og*
- *der er udfærdiget drifts- og vedligeholdelsesdokumentation, som skitserer processerne for opdatering, gennemgang og vedligeholdelse af aktiver (jf. også 4.5).*

Organisationen påviser, at den anvender passende systemudviklingsprocesser og sikkerhedsprocesser (f.eks. EN50126/8/9 for komplekse systemer) i tilgangen til design og indkøb. Dette kan opnås ved at udarbejde en systemudviklingsplan ("Systems Engineering Management Plan", SEMP), som specificerer proceduren for at identificere og registrere interessenter, systemkrav og sikkerhedsbehov.

Implementeringsfasen

For at sikre vellykket og sikker implementering af aktivet fastlægger organisationen processer til styring af risiciene i forbindelse med aktivets konstruktion, test og idriftsættelse i overensstemmelse med processerne i sikkerhedsledelsessystemet.

Organisationen gennemfører også en proces til styring af:

- *test, verifikation og validering af aktivets system- og sikkerhedskrav, som evt. kan opnås ved hjælp af en plan for test og idriftsættelse ("Testing and Commissioning Management Plan") eller tilsvarende, og*
- *aktivets driftsklarhed, som kan opnås med en tjekliste for driftsklarhed.*

Drifts- og vedligeholdelsesfasen

Organisationen har udfærdiget dokumentation for aktivets drift og vedligeholdelse, som skitserer de processer, den anvender til at opdatere, gennemgå og vedligeholde sine aktiver. Den beskriver driftens

omfang og, hvis relevant, de risikostyringsstrategier, der er indført for at dække alle relevante aktiviteter.

Denne dokumentation:

- sikrer, at aktivet anvendes og vedligeholdes i overensstemmelse med aktivets design
- identificerer og medtager alle sikkerhedsrelaterede betingelser, som specificerer, hvordan brugen af aktivet kan være begrænset, samt betingelserne for dets anvendelse, og
- specificerer de løbende kontroller, der skal foretages.

Processen for konfigurering af design og levering af det foreslåede aktiv (beskrevet i designfasen) udvides til at omfatte hele dets livscyklus ved hjælp af følgende:

- etablering og vedligeholdelse af registre over alle aktiver ved at oprette et aktivregister. Det indeholder oplysninger såsom den unikke identifikation af aktiverne, deres placering, eventuel udført vedligeholdelse osv.
- styring af dokumenter og oplysninger om aktiverne i overensstemmelse med organisationens sikkerhedsledelsessystem (jf. også 4.4 og 4.5)
- bestemmelse af aktivernes kritikalitet på baggrund af resultaterne af en sikkerhedsrisikovurdering. Sikkerhedskritiske aktiver identificeres i aktivregistret.

Organisationen viser, hvordan oplysninger om aktiver udfærdiges, vedligeholdes og integreres i farelogbogen.

Organisationen overvåger den aktuelle overensstemmelse med de udpegede standarder og processer for at sikre, at jernbanedriften fortsat er sikker og effektiv. I dette øjemed fastlægger organisationen processer for at sikre følgende:

- Aktiverne anvendes og vedligeholdes i henhold til de relevante manualer.
- Aktivernes tilstand overvåges.
- Udstyr, som er nødvendigt til at teste eller inspicere aktiver, bliver tilstrækkeligt kontrolleret, kalibreret og vedligeholdt.
- Alle risici i forbindelse med aktivernes drift og vedligeholdelse bliver håndteret i overensstemmelse med risikostyringsprocesserne og al lovgivning om sundhed og sikkerhed på arbejdspladsen.
- Reservedele er tilgængelige til vedligeholdelse, navnlig for sikkerhedskritiske aktiver. Dette kan opnås ved at bestemme behovet for reservedele til aktiverne ud fra aktivernes kritikalitet, som identificeret ved hjælp af pålidelighedscentreret vedligeholdelse ("Reliability Centred Maintenance", RCM).

Organisationen påviser, at den har planlagt aktivernes vedligeholdelse med henblik på at:

- adressere kompetence-, kapacitets- og ressourcekrav
- opfylde behovet for styring af informationer og registreringer
- fremlægge detaljerede planer, som er udarbejdet ved hjælp af en risikobaseret proces, og som definerer de forskellige vedligeholdelsesniveauer og fastlagte standardorganisationsstrukturer, procedurer og ansvarsområder for aktivernes vedligeholdelse, og
- sikre kalibrering af det værktøj og udstyr, der bliver anvendt til vedligeholdelsen.

Dette kan navnlig omfatte:

- en teknisk vedligeholdelsesplan ("Technical Maintenance Plan", TMP) og
- arbejdsinstrukser, som udvikles ud fra og auditeres imod TMP.

Planlægning dokumenteres og styres ved hjælp af et computerbaseret vedligeholdelsesstyringssystem (jf. også 4.5).

Organisationen har indført processer til at sikre følgende:

- Når et køretøj eller udstyr anvendes til en opgave:
 - Overensstemmelse med den opgave/mission, der skal udføres (f.eks. de enkelte typer rullende materiels tekniske kompatibilitet med ruterne), kontrolleres i forbindelse med og inden afgang.
 - Vedligeholdelse af sikkerhedskritiske komponenter foretages i henhold til planen (forebyggende

vedligeholdelse med vedligeholdelsestjeks hyppighed og type).

- *Der fastlægges vedligeholdelsestjek, når der identificeres fejl, eller når de overskrider deres sikre brugsgrænser (korrigerende vedligeholdelse), medmindre der er indført driftsmæssige begrænsninger.*
- *Når et ændringsbehov identificeres, skal de nødvendige foranstaltninger træffes hurtigst muligt såsom udtagelse af drift eller opstilling af driftsmæssige begrænsninger.*
- *Der er arbejdsinstrukser tilgængelige for alle sikkerhedskritiske aktiviteter.*
- *Alle udførte opgaver bekræftes skriftligt (signed-off).*
- *Dokumentation for udført vedligeholdelse styres (jf. også 4.5).*
- *Der er kompetencebaseret uddannelse tilgængelig for alle sikkerhedskritiske systemer (jf. også 4.1).*

Der er en proces/procedure til at sikre, at driftsmæssige begrænsninger, uanset om de er midlertidige eller permanente (f.eks. som følge af specifikke køretøjstyper eller specifikke ruter):

- *tages i betragtning, når et køretøj eller udstyr anvendes til en opgave/mission*
- *kommunikeres rettidigt til det personale, der betjener køretøjet eller udstyret (f.eks. lokomotivføreren eller togføreren).*

Organisationen påviser, at den:

- *forstår sine sikkerhedskritiske aktivers funktion ved at identificere, hvad der skal overvåges, måles og rapporteres*
- *fastlægger og registrerer metoden for og hyppigheden af overvågning, måling, analyse og evaluering af de sikkerhedskritiske aktivers funktion*
- *overvåger tendenserne sammenlignet med et aktivs forventede strategiske levetid (jf. også 6.1)*
- *rapporterer funktionsproblemer på baggrund af sikkerhedsrisikoniveauet og eskalerer problemer med sikkerhedsniveauet, således at de imødegås i tilstrækkelig grad*
- *anvender overvågningsresultaterne til at tilpasse vedligeholdelsesplanen, hvor dette er relevant*
- *opretter kanaler til kommunikation af alle resultater (jf. også 4.4)*
- *forbedrer de sikkerhedskritiske aktivers overensstemmelse med standarderne ved at:*
 - *gennemgå drifts- og vedligeholdelsesstyring og vurdere risikoen for, at aktiverne ikke overholder de forud fastlagte standarder*
 - *identificere den eller de grundlæggende årsag(er) (root causes) til problemer med sikkerhedsniveauet og*
 - *identificere de foranstaltninger, der kan være nødvendige for, at aktiverne kan vende tilbage til en sikker driftstilstand*
- *løbende forbedrer sikkerhedsledelsessystemet ved at identificere potentielle risici og træffe korrigerende foranstaltninger (jf. også 7.2) og*
- *dokumenterer, hvor muligheder er blevet udnyttet til at reducere eller fjerne risikoen, og hvordan dette blev opnået.*

Organisationen har indført processer til at identificere eventuelle fejl eller mangler, som aktiverne kan blive ramt af, og sikre, at der iværksættes passende korrigerende foranstaltninger. Disse er i tråd med bestemmelserne og vedligeholdelsesprogrammerne eller -planerne og:

- *sikrer passende registrering af fejl og mangler og de heraf følgende korrigerende foranstaltninger*
- *adresserer sikkerhedskritiske fejl og mangler*
- *sikrer passende rapportering af tilfælde, der skal anmeldes, og*
- *koordinerer uplanlagte reparationer af sikkerhedsrelaterede aktiver.*

Organisationen:

- *dokumenterer fejlhåndteringsprocessen*
- *bruger passende analyseteknikker til sikkerhedskritiske funktioner såsom "root cause-analysis" (RCA)*
- *foretager fejlregistrering, hvilket kan omfatte fejlkoder, fejltilstande, effekt, kritikalitet og korrigerende foranstaltninger*
- *udvikler procedurer til at håndtere almindelige reparationsaktiviteter og*

- *indfører en feedbackproces for ingeniørteamene eller de tekniske teams med henblik på at gennemgå og forbedre systemerne og minimere risikoen for fremtidige fejl.*

Dette opnås ved hjælp af fejlrapportering, analyse og korrigerende foranstaltninger (FRACAS), hvor man:

- *registrerer de fejl, der blev opdaget og registreret i forbindelse med test og idriftsættelse, og de fejl, der opstod under drift eller vedligeholdelse*
- *administrerer de efterfølgende korrigerende foranstaltninger, der træffes for at afhjælpe dem.*

Organisationen dokumenterer alle fejl og korrigerende foranstaltninger og kræver, at en teknisk kompetent person tjekker eventuelle uplanlagte reparationer.

Der er en proces/procedure for håndtering af uregelmæssig drift eller nødsituationer ved forvaltningen af aktiver.

Organisationen har fastlagt processer med henblik på at håndtere eventuelle grænsefladerisici, der kan opstå i forbindelse med drift og vedligeholdelse af aktiverne (**jf. også 3.1.1**). Disse dækker grænsefladerne mellem aktiverne og mellem de aktører, der bruger dem.

Fornyelses-, ud rangerings- og bortskaffelsesfasen

Organisationen forstår, hvilken tilstand dens aktiver er i, og når de forringes, reagerer den tilsvarende ved at udskifte eller vedligeholde dem.

Organisationen har udarbejdet en testplan for validering og idriftsættelse, som bekræfter, at det nye aktiv er egnet til formålet og er sikkert at bruge og vedligeholde. Hvis organisationen forlænger et eksisterende aktivs levetid, sørger den for at indhente passende sikkerhedsoplysninger, for eksempel historiske data, for at sikre, at det stadig er sikkert at bruge.

Der foretages overvågning af tendenserne sammenlignet med den forventede funktion (jf. drifts- og vedligeholdelsesfasen).

Når jernbaneinfrastruktur eller rullende materiel tages ud af drift, håndterer organisationen på en passende måde risiciene ved at tage aktivet ud af drift.

Håndtering af ændringer af sikkerhedskritiske aktiver

I situationer, hvor organisationen søger at ændre konfigurationsgrundlaget for sikkerhedskritiske aktiver, gennemfører den en ændringshåndteringsproces for at sikre effektiv håndtering af sikkerhedsrisici og fastlægger konfigurationsgrundlag for alle sikkerhedskritiske aktiver med den hertil knyttede software (uanset om de er indbygget i eksisterende systemer eller er enkeltstående programmer). Hvis en operatør ændrer konfigurationsgrundlaget for sikkerhedskritiske aktiver, skal vedkommende, hvis muligt:

- *håndtere de risici, der opstår som følge af disse aktivers ændring*
- *spore serie- og modelnumrene*
- *validere de funktionelle krav i forhold til specifikationerne og risikokontrolforanstaltningerne*
- *styre frigivelsen af konfigurationsemnerne og*
- *sikre, at status for alle aktiver, der er genstand for konfigurationsstyring, er opdateret.*

Organisationens ændringer af fastlagte grundlag og driftsvilkår eller vedligeholdelsesplanen for sikkerhedskritiske aktiver må ikke på nogen måde forringe jernbanedriftens sikkerhed.

Anvendelse af fælles sikkerhedsmetoder

Der er en proces/procedure til overvågning af, at enheder med ansvar for vedligeholdelse (ECM'er) anvender CSM for risikovurdering og CSM for overvågning, alt efter hvad der er relevant (dvs. som enten er lovbestemt og/eller fastlagt i kontraktlige aftaler).

Integration af menneskelige faktorer

Der er en systematisk proces for integration af menneskelige faktorer i hele et systems livscyklus, f.eks. hensyntagen til tilrettelæggelsen af opgaver, arbejdsprocedurer, arbejdsmiljø og passende ressourcer i relation til aktivet, som sikrer, at de menneskelige og organisatoriske faktorer tages i betragtning og tackles i tilstrækkelig grad.

Organisationens program angiver rammerne for, hvordan de angivne menneskelige og organisatoriske faktorer skal identificeres, gennemgås, vedtages og skride frem med henblik på at opnå løsninger gennem design- eller ændringshåndteringsprocessen. Programmet angiver forbindelserne med andre parter med hensyn til design- eller ændringsaktiviteten.

Der gives oplysninger om brugen af sikkerhedsvarslingsredskabet (SAIT) (jf. 5.4.3).

5.2.6 Referencer og standarder

- [Guide for the application of the Art 14 \(a\) of the Safety Directive and Commission Regulation \(EU\) No 445/2011 on a system of certification of entities in charge of maintenance for freight wagons](#)
- CENELEC — EN50126 Railway Applications — The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) Part 1: Basic, Requirements and Generic, Process
- Office of the National Rail Safety Regulator — Asset management guideline (2015)

5.2.7 Tilsynsspørgsmål

Set ud fra et tilsynsperspektiv er det vigtigt, at der er fokus på forvaltningen af aktivet i hele dets livscyklus lige fra design til bortskaffelse og ikke på enkelte fejl og mangler i forvaltningen af aktivet, medmindre disse har direkte konsekvenser for sikkerheden.

I tilsynet bør der tages højde for, hvordan eksisterende aktiver med tidligere gældende standarder bliver forvaltet og vedligeholdt.

I tilsynet bør der tages højde for, om og hvordan organisationen anvender SAIT.

5.3 Kontrahenter, partnere og leverandører

5.3.1 Lovkrav

- 5.3.1. Organisationen skal udpege og styre sikkerhedsrisici, der hidrører fra udliciterede aktiviteter og herunder drift eller andet samarbejde med kontrahenter, partnere og leverandører.
- 5.3.2. Med henblik på at styre de sikkerhedsrisici, der er omhandlet i afsnit 5.3.1., skal organisationen fastlægge kriterier for udvælgelse af kontrahenter, partnere og leverandører samt de kontraktlige forpligtelser, som disse skal opfylde, herunder:
 - (a) lovkrav og andre sikkerhedsrelaterede krav (jf. 1. Organisationens kontekst)
 - (b) det kompetenceniveau, der er nødvendigt for at udføre de opgaver, der er omfattet af kontrakten (jf. 4.2. Kompetence)
 - (c) ansvaret for de opgaver, som skal udføres
 - (d) det forventede sikkerhedsniveau der skal opretholdes i kontraktens løbetid
 - (e) forpligtelserne vedrørende udveksling af sikkerhedsrelateret information (jf. 4.4. Information og kommunikation)
 - (f) sporbarheden af sikkerhedsrelaterede dokumenter (jf. 4.5. Dokumenteret information)
- 5.3.3. I overensstemmelse med den proces, der er fastsat i artikel 3 i forordning (EU) nr. 1078/2012, skal organisationen overvåge:
 - (a) sikkerhedsniveauet for samtlige aktiviteter og operationer, som er udført af udført af kontrahenter, partnere og leverandører for at sikre, at de opfylder kravene i kontrakten
 - (b) kontrahenters, partners og leverandørers bevidsthed om de sikkerhedsrisici, som deres aktiviteter medfører for organisationens drift.

5.3.2 Formål

Ansøgerne skal påvise, at de er i stand til at identificere, vurdere og styre risici, der opstår som følge af aktiviteter udført af kontrahenter og andre leverandører, som ansøgerne har en arbejdsmæssig forbindelse til. Dette er ikke blot et spørgsmål om risikovurdering, og det kræver heller ikke en liste over alle risici eller relevante risikokategorier, men det pålægges ansøgerne at vise, hvordan systemer og procedurer som helhed er udformet og tilrettelagt for at fremme identifikation, vurdering og styring af disse risici. Dette indebærer også, at kontrakten skal indeholde oplysning om, hvordan sikkerhedsrelaterede oplysninger udveksles. Brugen af veludarbejdede kontrakter er generelt en accepteret måde at håndtere risici på. Organisationen har dog stadig hovedansvaret for håndtering af kontrahenter og kontrol af deres leveringer i forhold til de fastsatte specifikationer. Brugen af kontrahenter eller underkontrahenter betyder ikke, at jernbanevirksomhederne/infrastrukturforvalterne delegerer noget af deres ansvar for at sikre, at de udliciterede tjenester udføres i henhold til de standarder, der blev fastlagt inden driften.

Ansøgerne bør dokumentere, at de har indført processer til bedømmelse af kontrahenters og andre leverandørers kompetence og til vurdering af disses sikkerhedsniveau som en del af indkøbsprocessen.

De enkelte organisationer er ansvarlige for at udføre den overvågningsproces, der er taget højde for i CSM for overvågning, og for ved hjælp af kontraktlige aftaler at sikre, at risikokontrolforanstaltninger truffet af deres kontrahenter også overvåges i henhold til den fællessikkerhedsmetode. Hvis organisationerne identificerer relevante sikkerhedsrisici med hensyn til fejl eller funktionsfejl ved teknisk udstyr, skal de i henhold til CSM for overvågning rapportere disse risici til andre involverede parter, så de kan træffe alle nødvendige korrigerende foranstaltninger for at sikre systemets sikkerhed.

5.3.3 Forklarende noter

Der findes flere oplysninger om kontraktlige aftaler og partnerskaber i Bilag 3.

5.3.4 Dokumentation

- Dokumentation for, hvordan organisationens sikkerhedsledelsessystem kommer i berøring med kontrahenters og leverandørers ledelsessystemer til risikostyring **(5.3.1)**.
- Dokumentation for, at der udarbejdes kontraktlige aftaler på grundlag af resultaterne af risikovurderingen **(5.3.1) (jf. også 3.1)**.
- Der er processer, som angiver, hvordan de menneskelige og organisatoriske faktorer bør adresseres og kommunikeres til underleverandører samt ledelsen af disse **(5.3.1)**.
- Dokumentation for, hvordan organisationen styrer dokumenter, der vedrører kontrahenter og leverandører **(5.3.2(a)-(d))**.
- Dokumentation for, hvordan organisationen udvælger kontrahenter og leverandører med henblik på at sikre, at de er kompetente, og at sikkerhedsrisiciene håndteres korrekt **(5.3.2(a)-(e))**.
- Processen til at sikre, at vigtige sikkerhedsoplysninger deles med kontrahenter og leverandører eller rapporteres af disse **(5.3.2 (d))**.
- Organisationens proces eller procedure til overvågning af, at kontrahenter, partnere og leverandører, som den har en arbejdsmæssig forbindelse til, er i stand til at håndtere de risici, de står over for **(5.3.3 (a)-(b))**.
- Dokumentation for, at kontrahenter, partnere eller leverandører overvåges regelmæssigt i henhold til CSM for overvågning (forordning (EU) 1078/2012) for at sikre, at produktet eller tjenesten er i overensstemmelse med de fastlagte krav og sikkerhedsmålsætninger **(5.3.3 (a)) (jf. også 6.1)**.

5.3.5 Eksempler på dokumentation

Procedure for udvælgelse og overvågning af kontrahenter, partnere og leverandører. Det fremgår klart af proceduren, at de standarder, der gælder for kontrahenter, er de samme som dem, der gælder for fastansat personale, og hvad rollerne og ansvarsområderne er. Proceduren dokumenterer den nødvendige udveksling af oplysninger mellem sikkerhedsledelsessystemerne til ansøgerne og kontrahenter, partnere og leverandører.

Der fremlægges dokumentation for de sikkerhedsmål, som kontrahenter, partnere og leverandører forventes at nå, og de indikatorer, der vil blive anvendt til at måle dem.

Strategien for menneskelige og organisatoriske faktorer specificerer, hvordan disse punkter dækkes hos kontrahenter og underkontrahenter.

Dokumenthåndteringsproceduren, som omhandler organisationens standarder, der gælder for kontrahenter, partnere og leverandører (jf. også 4.5.1.1 (e) Dokumenthåndtering).

En liste/oversigt over organisationens kontrahenter, partnere og leverandører til intern eller ekstern brug, med angivelse af de produkter og/eller tjenester, de leverer **(jf. også 4.5.1.1 (d) og (e))**, og angivelse af, hvilken indvirkning de har på sikkerheden samt foranstaltningerne til at styre de identificerede risici (f.eks. udveksling af oplysninger, præcisering af ansvarsområder, uddannelse) **(jf. også 3.1.1.1 (a))**.

Proceduren for kompetencestyringssystemet, som hænger sammen med kontrahenternes, partnernes og leverandørernes procedure.

Processen/proceduren for håndtering af kontrahenter, partnere og leverandører omfatter, hvordan grænsefladerisici som følge af kontrahenters, partners og leverandørers aktiviteter håndteres og deles med dem og, hvis relevant, hvordan de medtages i kontraktlige arrangementer, og hvordan udvekslingen af oplysninger integreres i sikkerhedsledelsessystemet.

Den relevante audit-/inspektionsplanlægningsproces for organisationens kontrahenter, partnere og leverandører med nogle eksempler på registreringen af disse aktiviteter såsom audit-/inspektionsrapporter eller -resultater.

Processen eller proceduren for, hvordan relevante krav, der er gældende for kontrahenter, partnere eller leverandører, identificeres og deles med dem, og, hvis relevant, hvordan de medtages i kontraktlige aftaler, hvilket dokumenteres korrekt i dokumenthåndteringssystemet, så oplysningernes sporbarhed sikres.

Proceduren i dokumenthåndteringssystemet til at håndtere certifikater, tilladelser, anerkendelser eller andre typer dokumentation, der viser overholdelsen af de krav, som er gældende for kontrahenter, partnere eller leverandører, og som løbende kontrollerer deres gyldighed (f.eks. ved hjælp af overvågningsaktiviteter).

5.3.6 Tilsynsspørgsmål

Ved tilsyn med en organisation kan det, for at få et fuldstændigt billede af styringens og overvågningens omfang, være nødvendigt at udføre tilsynsaktiviteter rettet mod en kontrahent eller leverandør, som arbejder for den pågældende organisation. Det kan ligeledes være nødvendigt at få adgang til den dokumentation, som kontrahenten eller leverandøren arbejder på, og undersøge, hvordan den hænger sammen med procedurerne i organisationens sikkerhedsledelsessystem.

Tiltag til at sikre, at kontrahenters og leverandørers kompetence og indsats på sikkerhedsområdet er en integreret del af indkøbsprocessen.

5.4 Styring af ændringer

5.4.1 Lovkrav

5.4.1. Organisationen skal gennemføre og styre ændringer i sikkerhedsledelsessystemet for at opretholde eller forbedre sikkerhedsniveauet. Dette skal omfatte beslutninger i de forskellige faser af ændringsprocessen og den efterfølgende gennemgang af sikkerhedsrisiciene (jf. 3.1.1. Risikovurdering).

5.4.2 Formål

Det er vigtigt, at ansøgerne kan identificere og reagere på nye risici, der kan opstå i deres aktiviteter, ved efter behov at anvende kravene om styring af ændringer i direktiv (EU) 2016/798 og CSM for risikovurdering (Kommissionens gennemførelsesforordning (EU) 402/2015). Det bør påvises, at sikkerhedsledelsessystemet indeholder procedurer til at evaluere disse risici og gennemføre nye risikokontrolforanstaltninger, hvor det er relevant. Dette bør omfatte alle typer og niveauer af ændringer — signifikante og mindre, permanente og midlertidige, øjeblikkelige og langsigtede. Det bør gælde for ændringer af:

- aktivitetstyper
- udstyr
- procedurer
- organisation
- personale eller
- grænseflader.

Processen bør gøre det muligt at vurdere risiciene på en forholdsmæssig og pålidelig måde, herunder spørgsmål vedrørende menneskelige faktorer, hvis relevant, og rimelige kontrolforanstaltninger, der skal vedtages.

Ændringer i roller, ansvarsområder, redskaber og udstyr, arbejdsmiljø, processer og procedurer understøttes af en analyse af menneskelige og organisatoriske faktorer for at identificere eventuelle sikkerhedsrisici i forbindelse med ændringen. Anvendte metoder kan for eksempel være opgaveanalyse, analyse af brugbarhed, simulering, risikovurdering, HAZOP og sikkerhedsundersøgelse. Eksempler på ændringer, der

forudsætter en risikovurdering med en tilgang, der omfatter menneskelige og organisatoriske faktorer. Det kan for eksempel gælde for ændringer af arbejdsprocedurer som følge af ændret udstyr, ændrede arbejdsplaner eller omfordeling af ansvarsområder.

5.4.3 Forklarende noter

Ikke alle ændringer er genstand for risikovurdering **(5.4.1)**. Hvis ændringerne håndteres aktivt via andre processer i sikkerhedsledelsessystemet såsom de daglige aktiviteter, bør de ikke betragtes som en ændring, der kræver håndtering via den formelle ændringsproces.

Roller, ansvarsområder, ansvarlighed og bemyndigelser, der skal defineres **(jf. også 2.3)**, omfatter håndtering af ændringer **(5.4.1)**, f.eks. tildeling af roller til en ændringsstyringsenhed.

Personalet bør høres under ændringshåndteringsprocessen **(jf. også 2.4)**.

Ændringer af roller, ansvarsområder, metoder og processer foretages ved hjælp af en analyse af sikkerhedskulturelementer, der påvirkes af ændringen, for at identificere mulige sikkerhedsrisici. Sikkerhedsrisici som følge af nedskæringer, ledelsesændringer eller udlicitering af aktiviteter, herunder aktiviteter eller samarbejde med kontrahenter, partnere og leverandører, bør håndteres og prioriteres på samme måde som interne risici.

5.4.4 Dokumentation

- En beskrivelse af processen for styring af ændringer **(5.4.1)**.
- En beskrivelse af de procedurer og metoder, der anvendes til at evaluere nye eller ændrede risici og gennemføre nye **(5.4.1)**.
- kontrolforanstaltninger, herunder henvisninger til, hvor de detaljerede processer kan findes **(5.4.1)**.
- Oplysninger om, hvordan organisationen identificerer signifikante ændringer, og beslutninger om, hvornår den skal anvende processerne i CSM for risikovurdering, eller hvornår den skal foretage en risikovurdering i henhold til sikkerhedsledelsessystemets procedurer **(5.4.1)**.
- Oplysninger om de tiltag med hensyn til styring af ændringer, som organisationen har indført for håndteringen af køretøjstilladelser og ændringer af EU-sikkerhedscertifikatet eller sikkerhedsgodkendelsen **(5.4.1)**.
- Oplysninger om processen for underretning af den relevante nationale sikkerhedsmyndighed om ændringerne, inden en ny jernbanetransportaktivitet starter **(5.4.1)**.

5.4.5 Eksempler på dokumentation

En kopi af ændringshåndteringsproceduren som en del af ansøgningen. Dette dokument dækker behovet for risikovurdering af alle ændringer i henhold til forskellige lovkrav. Et eksempel på en logbog over problemer og antagelser, der gennemgås regelmæssigt, efterhånden som ændringen skrider frem. Endelig dækker proceduren også processen for, hvordan den eller de relevante nationale sikkerhedsmyndighed(er) underrettes om ændringerne.

Ændringshåndteringsprocessen henviser til brug af risikovurderingsprocessen, og resultaterne tages med i betragtning ved udviklingen, gennemførelsen og gennemgangen af driftsprocesserne.

5.4.6 Tilsynsspørgsmål

For at fastslå, om tiltag til styring af ændringer i sikkerhedsledelsessystemet er tilstrækkeligt pålidelige, er det nødvendigt at følge et antal ændringer af forskellig art gennem den fastlagte proces for at se, om de (a) er blevet styret korrekt, og om der er taget ordentlig højde for de risici, der følger af ændringerne, og (b) om nogen af de opsamlede erfaringer er blevet indarbejdet i revideringen af sikkerhedsledelsessystemets procedurer.

Vurdering af, om tiltag til styring af ændringer er i overensstemmelse med CSM for risikovurdering.

Organisationen har indført processer til gennemførelse og løbende overvågning af relevante TSI'er, nationale forskrifter og andre standarder, der, hvis relevant, viser, hvordan disse anvendes i hele livscyklussen for udstyr eller aktiviteter.

5.5 Håndtering af nødsituationer

5.5.1 Lovkrav

- 5.5.1. Organisationen skal udpege nødsituationer og tilhørende rettidige foranstaltninger, der skal træffes for at håndtere disse (jf. 3.1.1. Risikovurdering) og genoprette normal driftstilstand i overensstemmelse med forordning (EU) nr. 2015/995.
- 5.5.2. Organisationen skal for hver udpeget type nødsituation sikre, at
- (a) redningstjenesterne kan kontaktes med det samme
 - (b) redningstjenesterne får al relevant information både på forhånd, så de kan forberede deres indsats, og når nødsituationen opstår
 - (c) førstehjælp leveres internt.
- 5.5.3. Organisationen skal fastlægge og dokumentere alle parter roller og ansvar i overensstemmelse med forordning (EU) nr. 2015/995.
- 5.5.4. Organisationen skal have handlingsplaner, alarmeringsplaner og informationsplaner for nødsituationer; disse skal omfatte ordninger med henblik på at:
- (a) alarmere alt personale med ansvar for håndtering af nødsituationer
 - (b) kommunikere information til alle parter (f.eks. infrastrukturforvalter, [jernbanevirksomheder](#), kontrahenter, myndigheder, redningstjenester), herunder instrukser for nødsituationer til passagerer
 - (c) træffe de nødvendige beslutninger i forhold til typen af nødsituation
- 5.5.5. Organisationen skal beskrive, hvordan ressourcer og midler til håndtering af nødsituationer er blevet tildelt (jf. 4.1. Ressourcer), og hvordan uddannelsesbehov er blevet påvist (jf. 4.2. Competence).
- 5.5.6. Beredskabsplanerne skal afprøves regelmæssigt i samarbejde med andre interessenter og om nødvendigt opdateres.
- 5.5.7. Organisationen skal sikre, at kompetent, ledende personale med tilstrækkelige sprogkundskaber let kan kontaktes af infrastrukturforvalteren, så sidstnævnte kan gives den rette information.
- 5.5.7. [Organisationen skal koordinere nød- og beredskabsprocedurer med alle jernbanevirksomheder, som har jernbanedrift på den pågældende organisations infrastruktur, med beredskabstjenesterne for at lette deres hurtige indgriben og med enhver anden part, der kan være involveret i en nødsituation.](#)
- 5.5.8. Organisationen skal have en procedure for at kontakte den enhed, der er ansvarlig for vedligeholdelsen, eller ihændeleveren af jernbanekøretøjet, hvis en nødsituation opstår.
- 5.5.8 [Organisationen skal have ordninger for at stoppe driften og jernbanetrafikken øjeblikkeligt, hvis det er nødvendigt, og informere alle interessenter herom.](#)
- 5.5.9 [I forbindelse med grænseoverskridende infrastruktur skal samarbejdet mellem de relevante infrastrukturforvaltere lette den nødvendige koordinering og det nødvendige beredskab hos de kompetente beredskabstjenester på begge sider af grænsen.](#)

5.5.2 Formål

Pålidelige systemer til håndtering af nødsituationer er af afgørende vigtighed for alle ansvarlige parter og bør omfatte de oplysninger, som beredskabstjenesterne skal have for at kunne udarbejde deres beredskabsplaner for større hændelser. De aspekter af sikkerhedsledelsessystemet, som er direkte relevante for beredskabsordningerne, er også vigtige, f.eks. uddannelse i nødsituationer og test af beredskabsplaner.

5.5.3 Forklarende noter

Nødsituationer **(5.5.1)** hænger sammen med resultaterne af organisationens risikovurdering, selv om TSI OPE (jf. bestemmelse 4.2.3.7) indeholder en ikke-udtømmende liste over nødsituationer.

Bestemmelserne 5.5.7 og 5.5.8 i ovennævnte juridiske tekst erstattes af bestemmelserne med blåt, i de tilfælde hvor vurderingen vedrører infrastrukturforvalteren. Bestemmelse 5.5.9 med blåt ovenfor vedrører kun infrastrukturforvalteren.

5.5.4 Dokumentation

Ansøgeren forventes at give en oversigt over følgende:

- *De typer nødsituationer, der er dækket, herunder uregelmæssig drift, og de procedurer, der er indført for at håndtere dem **(5.5.1)**.*
- *Oplysninger fra ansøgeren, som gør det muligt for beredskabstjenesterne at planlægge deres beredskab ved en større ulykke på jernbanerne. Hvis relevant, henvises der til pligterne i henhold til gældende EU-lovgivning og eventuelle relevante grænseoverskridende ordninger **(5.5.2 (a) og (b))**.*
- *Planer, roller og ansvarsområder (også for dem med særlige færdigheder, der er udpeget til at assistere infrastrukturforvalteren eller omvendt), uddannelse og ordninger med henblik på at vedligeholde kompetencer, ordninger til effektiv kommunikation med beredskabstjenester og relevant personale, kommunikation med personer berørt af hændelser såsom passagerer, eller berørte tredjeparter (dette bør omfatte et dokument, der beskriver alle parter roller og ansvarsområder, hvordan ressourcer og midler er tildelt, og hvordan uddannelseskrav er identificeret), og procedurerne for genindsættelse i normal drift efter en nødsituation **(5.5.1), (5.5.3), (5.5.4 (a)-(c)), (5.5.5), (5.5.7) (5.5.8 og 5.5.9 i de krav, der kun gælder for infrastrukturforvaltere)**.*
- *De specifikke aspekter af sikkerhedsledelsessystemet, som er direkte relevante for beredskabet, f.eks. uddannelse i nødsituationer og test af beredskabsplaner for at identificere eventuelle svagheder **(5.5.6)**.*
- *Proceduren til at kontakte den relevante enhed med ansvar for vedligeholdelse eller ihændeleveren i tilfælde af en nødsituation, der berører en eller flere af deres køretøjer **(5.5.8 i de krav, der kun gælder for jernbanevirksomheder)**.*

5.5.5 Eksempler på dokumentation

En kopi af proceduren eller procedurerne for håndtering af nødsituationer og planerne (f.eks. afhjælpningsprocedurerne) i forbindelse hermed. Proceduren dækker hele det net, der opereres på, efter behov med specifikke regler for tunneller og andre højrisikosteder samt for grænseoverskridende samarbejde, personale, roller og ansvarsområder. Den omfatter links til infrastrukturforvalterens beredskabsprocedurer, og hvordan man kontakter andre relevante parter såsom enheden med ansvar for vedligeholdelse, hvis relevant. Når en jernbanevirksomheds driftsområde omfatter flere infrastrukturforvaltere, bør jernbanevirksomheden tage højde for forskellene mellem beredskabsprocedurerne (og brugeraftalerne) med disse infrastrukturforvaltere.

I proceduren henvises der til kravene i kompetencestyringssystemet for personale, som skal reagere på nødsituationer, ligesom det sikres, at kontraktansatte er i stand til at opfylde samme standarder.

Beredskabsproceduren omfatter processen for, hvordan ofre for ulykker og deres familier får vejledning om klageprocedurerne.

Proceduren omfatter (hvis relevant) information om, hvad der sker i en nødsituation, hvor farligt gods er involveret. Organisationen (jernbanevirksomheden) har indført en proces til at sikre, at:

- *lastevirksomheden, tankvognsejeren (hvis privatejet), ejeren eller ihændehaven og operatøren (hvis der er tale om en tankcontainer), modtageren osv. Kan kontaktes med det samme*
- *infrastrukturforvalteren får relevant information så hurtigt som muligt (f.eks. om vognenes registreringsnummer, vognenes placering i toget, UN-nummer, RID-klassifikationskode og fareidentifikationsnummer på det farlige gods i henhold til RID-bestemmelserne)*
- *organisationen (infrastrukturforvalteren) har en proces til at sørge for, at myndighederne (f.eks. redningstjenester og politiet samt andre beredskabstjenester og myndigheder) får relevant information om farligt gods (jf. eksemplerne ovenfor).*

5.5.6 Tilsynsspørgsmål

For at kunne foretage en korrekt vurdering af procedurerne i sikkerhedsledelsessystemet for håndtering af nødsituationer kan det være nødvendigt at krydstjekke procedurerne i sikkerhedsledelsessystemet mod procedurerne hos relevante grænsefladeaktører (navnlig forholdet mellem vigtige aktører som jernbanevirksomheder, infrastrukturforvaltere og beredskabstjenester) for at sikre, at de processer, der er indført til håndtering af sådanne hændelser, udgør en sammenhængende helhed.

Kontrol af, at der forefindes planer for alle forventelige nødsituationer.

Regler for test af beredskabsplaner og koordinerede øvelser med beredskabstjenester er ikke begrænset til skrivebordsøvelser.

Der eksisterer beskrivelse af grænsefladerne til andre interessenter, og de omfatter test, kontrol, kommunikation, koordination og kompetence.

6 Præstationsevaluering

6.1 Overvågning

6.1.1 Lovkrav

- 6.1.1. Organisationen skal gennemføre overvågning i overensstemmelse med forordning (EU) nr. 1078/2012:
- (a) For at kontrollere den rette anvendelse og effektiviteten af alle sikkerhedsledelsessystemets processer og procedurer, herunder driftsmæssige, organisatoriske og tekniske sikkerhedsforanstaltninger
 - (b) for at kontrollere den rette anvendelse af sikkerhedsledelsessystemet som helhed og konstatere, om de forventede slutresultater opnås
 - (c) for at undersøge, om sikkerhedsledelsessystemet overholder kravene i denne forordning
 - (d) for at fastlægge, gennemføre og evaluere effektiviteten af de korrigerende foranstaltninger (jf. 7.2. Løbende forbedring), når dette er relevant, hvis der påvises tilfælde af manglende overensstemmelse med litra a), b) og c).
- 6.1.2. Organisationen skal regelmæssigt overvåge udførelsen af sikkerhedsrelaterede opgaver på alle organisationsniveauer og gribe ind, hvis disse opgaver ikke løses på korrekt vis.

6.1.2 Formål

Organisationen bør fremlægge dokumentation for, at den har indført en proces til overvågning af anvendelsen og effektiviteten af sikkerhedsledelsessystemet, og at denne proces er passende i forhold til driftens størrelse, omfang og type. Organisationen bør påvise, at processen kan identificere, evaluere og korrigere eventuelle fejl i sikkerhedsledelsessystemets funktion.

6.1.3 Forklarende noter

Kontrolforanstaltningernes effektivitet betyder, at organisationen har indført en proces til at tjekke, at når en risikovurdering er udført, og de relevante kontrolforanstaltninger er truffet, disse gennemgås efter et stykke tid for at sikre, at den forventede reduktion af sikkerhedsrisikoen er blevet opnået som følge af deres anvendelse (6.1.1 (d)).

Den udførte overvågning bør omfatte en analyse af, hvorvidt strategien for menneskelige og organisatoriske faktorer har været vellykket.

Sikkerhedsniveauet vurderes systematisk i lyset af strategien for forbedring af sikkerhedskulturen. Det betyder, at organisationen bør se på, hvordan forbedringer i sikkerhedskulturer passer ind i og er en del af målet for sikkerhedsforbedringen.

Der foretages rutinemæssigt selvkritiske og objektive vurderinger af organisationens programmer, praksis og indsats med hensyn til sikkerhedskulturen. Sikkerhedsoplysninger, som f.eks. stammer fra programmet for korrigerende foranstaltninger, menneskelig ydeevne, analyse af ulykker og hændelser, undersøgelser samt

relevante interne og eksterne driftserfaringer, bliver systematisk indsamlet og evalueret for at se tendenserne og undgå organisationens og enkeltpersoners laden stå til eller magelighed.

En vellykket vurdering kan give input til en forbedring af sikkerhedsniveauet ved at give et klart billede af, hvordan organisationens sikkerhedskultur påvirker sikkerheden. Vurderingen tager sigte på at identificere sikkerhedskulturens styrker og svagheder ved at sammenligne den faktiske kultur med den, man stræber efter. Det gør det muligt at prioritere de områder, der skal forbedres, og at gennemføre ændringer af f.eks.

processer, uddannelse og adfærd. Vurdering af sikkerhedskulturen er en metode til at arbejde proaktivt på at forbedre sikkerhedsniveauet og øge sikkerhedsmargenerne. Det anbefales, at der foretages uafhængige vurderinger af sikkerhedskulturen hvert tredje til femte år, og at organisationen foretager selvevalueringer hvert år eller hvert andet år.

6.1.4 Dokumentation

- *Oplysninger om, hvordan ansøgeren har gennemført CSM for overvågning **(6.1.1 (a))**.*
- *Oplysninger om, hvordan det ved hjælp af overvågningsprocessen identificeres, hvorvidt de forventede sikkerhedsresultater er nået eller ej **(6.1.1 (b))**.*
- *Dokumentation for, at sikkerhedsledelsessystemet er blevet ændret som følge af afhjælpningen af de fejl i processerne i sikkerhedsledelsessystemet, der blev identificeret under overvågningen **(6.1.1 (c))**.*
- *Organisationen bør have en proces til fastsættelse af standarder for indsatsen samt indikatorer for overvågningen i forbindelse med driftsprocesserne og for de gennemførte ændringer. Der bør være et program til løbende vurdering af indsatsen i de processer, som vedrører menneskelige og organisatoriske faktorer, samt resultatet af disse processer, f.eks. personalets overholdelse af de gennemførte procedurer og brugen af nyt udstyr **(6.1.2)**.*

6.1.5 Eksempler på dokumentation

En angivelse af, at CSM for overvågning anvendes, og at der er en procedure, som dækker denne aktivitet. Proceduren beskriver, hvordan indsatsen i forhold til sikkerhedsresultater måles og korrigeres ved hjælp af ændringshåndterings- og risikovurderingsprocessen, og hvordan fejl i sikkerhedsledelsessystemet bliver rettet.

Organisationen har indført processer og procedurer til systematisk evaluering af, at ordningerne for medtagelse af menneskelige og organisatoriske faktorer er hensigtsmæssige, og at de opnåede resultater er i overensstemmelse med standarderne for indsatsen.

Organisationen har indført processer og procedurer til systematisk evaluering af personalets indsats i sikkerhedskritiske arbejdsopgaver. Disse processer er baseret på en proaktiv tilgang og sætter standarder for indsatsen og en systematisk evaluering. Der anvendes evidensbaserede metoder, f.eks. forvaltning af personaleressourcer.

6.1.6 Tilsynsspørgsmål

Undersøgelse af overvågningsprocessen og de resultater og foranstaltninger, den har givet anledning til, er af afgørende vigtighed for fastlæggelsen af, hvorvidt sikkerhedsledelsessystemet er et "levende" dokument under udvikling, hvor erfaringerne medfører forbedringer, eller om det er et fast dokument, som ikke ændrer sig med tiden.

Undersøgelse af en række vigtige risikoområder og kontrolforanstaltninger samt test af deres korrekte anvendelse og effektivitet i hele sikkerhedsledelsessystemet er af afgørende vigtighed for, at den nationale sikkerhedsmyndighed kan fastslå overensstemmelsen med CSM for overvågning.

6.2 Intern audit

6.2.1 Lovkrav

- 6.2.1. Organisationen skal gennemføre interne audits på en uafhængig, upartisk og gennemsigtig måde for at indsamle og analysere information til brug for sine overvågningsaktiviteter (jf. 6.1.Overvågning) og herunder
- (a) udarbejde en tidsplan over planlagte interne audit, der kan opdateres afhængigt af resultaterne af tidligere audit og overvågning af resultaterne.
 - (b) udpege og udvælge kompetente auditorer (jf. 4.2. Competence).
 - (c) analysere og evaluere resultaterne af de gennemførte audit
 - (d) fastlægge behovet for korrigerende foranstaltninger eller forbedringer.
 - (e) verificere disse foranstaltningers fuldførelse og effektivitet.
 - (f) dokumentere gennemførelsen og resultaterne af audit
 - (g) formidle auditresultaterne til den øverste ledelse.

6.2.2 Formål

Ansøgerne skal påvise, at de har et internt auditsystem, som omfatter kompetent personale og giver relevant output, der tages i betragtning af ledelsen, og som sikrer, at sikkerhedsledelsessystemet overholder lovkravene.

6.2.3 Forklarende noter

Interne audits (**6.2.1**) er overvågningsredskaber i den betydning, der er medtaget i CSM for overvågning. Selv om det er et separat krav, skal det bidrage til opfyldelse af overvågningsmålsætningerne i henhold til CSM for overvågning.

Interne audits (**6.2.1**) har til formål at give oplysninger om, hvorvidt sikkerhedsledelsessystemet er i overensstemmelse med de gældende krav (**6.1.1 ©**) og gennemføres og vedligeholdes på en effektiv måde (**6.1.1 (a), (b) og (d)**). De gældende krav henviser til kravene i bilag I og bilag II til CSM for overensstemmelsesvurdering og dermed til alle andre gældende krav, som organisationen skal overholde (**jf. også 1.1**).

Auditorerne er ansvarlige for at verificere fuldførelsen og effektiviteten af de korrigerende foranstaltninger eller forbedringer (**6.2.1 (c)**), der skal foretages i henhold til auditresultaterne.

6.2.4 Dokumentation

- Dokumentation for, at der er en intern auditproces eller -ramme, som sikrer planlagte audits og yderligere målrettede audits som reaktion på sikkerhedsdata (**6.2.1 (a)**).
- Dokumentation for, at der er et kompetencestyringssystem, som medtager elementer, der vedrører de interne auditorers kompetence (**6.2.1 (b)**).
- Dokumentation for, at der er blevet fulgt op på resultaterne fra både interne og eksterne audits (**6.2.1 (c), (d), (e), (f)**).
- Dokumentation for, at auditresultaterne er blevet drøftet af den øverste ledelse, og at der er truffet relevante foranstaltninger som følge heraf (**6.2.1 (g)**).

6.2.5 Eksempler på dokumentation

Der er indført en intern auditprocedure for planlagte og yderligere audits, som omfatter den øverste ledelses

drøftelse af resultaterne.

Eksempler på auditrapporter og en logbog over resultaterne fra interne audits, hvor det angives, hvilke foranstaltninger der er truffet for at følge op på dem.

Resultaterne af de auditaktiviteter, der udføres i hele organisationen, bliver indsamlet og analyseret og udgør grundlaget for de anbefalinger, der anvendes i den regelmæssige ledelseevaluering.

Proceduren henviser til kompetencestyringssystemet. Kompetencestyringssystemet påviser, at auditorerne har fulgt en passende auditoruddannelse (f.eks. ISO).

6.2.6 Referencer og standarder

- ISO 19011:2018 — *Vejledning i auditering af sikkerhedsledelsessystemer*

6.2.7 Tilsynsspørgsmål

Når der foretages tilsyn, er det af afgørende vigtighed, at planlægningen af audits og resultaterne af de gennemførte audits undersøges. Dette vil vise, om de gennemførte audits er rettet mod de rigtige områder, om resultaterne er rimelige, og om det personale, der foretager audits, er kompetent.

Kontrol af, at de områder, der er valgt til audit, passer til organisationens risikoprofil.

Der er en mekanisme, som udløser uplanlagte audits, og dette gøres ved at gennemgå en række eksempler.

6.3 Ledelsens evaluering

6.3.1 Lovkrav

- 6.3.1. Den øverste ledelse skal evaluere, om sikkerhedsledelsessystemet fortsat er tilstrækkeligt og effektivt og herunder skal den som minimum overveje:
- (a) status for gennemførelsen af udestående handlinger fra tidligere evalueringer
 - (b) ændrede interne og eksterne forhold (jf. 1. Organisationens kontekst)
 - (c) organisationens sikkerhedsniveau i relation til:
 - (i.) opfyldelsen af dens sikkerhedsmålsætning
 - (ii.) resultaterne af dens overvågningsaktiviteter, herunder observationer fra interne audit samt interne undersøgelser af ulykker/hændelser og status over deres respektive tiltag
 - (iii.) de relevante resultater fra tilsynsaktiviteter, der foretages af den nationale sikkerhedsmyndighed
 - (d) henstillinger med henblik på forbedring.
- 6.3.2. Den øverste ledelse skal ud fra resultaterne af sin evaluering påtage sig det overordnede ansvar for planlægningen og gennemførelsen af nødvendige ændringer i sikkerhedsledelsessystemet.

6.3.2 Formål

En stærk sikkerhedsledelse fra ledelsens side er afgørende for en produktiv og effektiv funktion af en organisations sikkerhedsledelsessystem samt dets fortsatte udvikling over tid. Organisationen bør påvise, at ledelsen er aktivt involveret i evalueringen af sikkerhedsledelsessystemets resultater og dets fremtidige udvikling.

6.3.3 Dokumentation

- *Processer for, at ledelsesmøderne dækker evalueringen af sikkerhedsledelsessystemet og fremskridtene med hensyn til interne henstillinger fra audits og evalueringer (6.3.1 (a)-(d)).*
- *Registreringer af, hvordan organisationen har klaret sig i forhold til sine sikkerhedsmålsætninger (6.3.1 (c),(i)).*
- *Dokumentation for, at anbefalinger fra den nationale sikkerhedsmyndighed er taget i betragtning i sikkerhedsledelsessystemet (6.3.1 (c), (iii)).*
- *Organisationen kan påvise, at den har indført processer til fastlæggelse og opstilling af mål, der passer til driftens type, omfang og relevante risici. Den vurderer jævnligt indsatsen i forhold til målene og overensstemmelsen med procedurerne, og den anvender sikkerhedsdata til at overvåge, gennemgå og gennemføre ændringer af driftsrelaterede ordninger (6.3.1).*
- *Dokumentation for, at ledelsen spiller en aktiv rolle i planlægningen og gennemførelsen af de nødvendige ændringer af sikkerhedskulturen (6.3.2).*

Der er processer og værktøjer til systematisk at indberette alle typer identificerede risici, fejl, nærvædfejl, mangler og hændelser samt for kategorisering og analyse af det indberettede fra et perspektiv baseret på menneskelige og organisatoriske faktorer med henblik på at fastslå underliggende årsager og effektive foranstaltninger.

Ekspertise inden for menneskelige og organisatoriske faktorer anvendes i processen for undersøgelse af ulykker.

Der er systematiske processer for brug af læring om forhold vedrørende menneskelige og organisatoriske faktorer til uddannelse og design.

Læring fra undersøgelser af ulykker og hændelser kommunikeres til medarbejderne i organisationen og bruges til uddannelse, design og andre områder for at mindske sandsynligheden for gentagelse.

Resultaterne af undersøgelser af ulykker rapporteres på ledelsesmøder og betragtes som et vigtigt redskab til erfaringsopsamling og forbedring.

- *Der er indført en kvalitetssikringsproces til undersøgelse af ulykker.*

6.3.4 Eksempler på dokumentation

Proceduren, som dækker gennemgangen af og fremskridtene med hensyn til interne henstillinger fra audits og evalueringer foretaget af den øverste ledelse, ledsaget af referater fra udvalgte møder.

Logbogen over problemer, som viser de anbefalinger, der er givet, og fremskridtene med at rette de fejl, ledelsen har registreret.

Proceduren for ledelsens evaluering af resultaterne fra interne undersøgelser af ulykker og de relevante output fra den nationale sikkerhedsmyndigheds tilsyn.

Der gives oplysning om, hvilke indikatorer der følges op på fra den øverste ledelses side, samt hyppigheden heraf.

6.3.5 Tilsynsspørgsmål

I forbindelse med tilsynet er det vigtigt at holde øje med, at processen til sikring af, at ledelsen evaluerer sikkerhedsledelsessystemets effektivitet, og at det resulterer i reelle ændringer på driftsmæssigt plan.

Ledelsens bevidsthed om ændringer i interne og eksterne forhold. Kontrol af, om ledelsen foretager f.eks. afsøgning af markedsinformationer (horizon scanning) eller benytter andre teknikker såsom PESTLE-analyse (politisk, økonomisk, social, teknologisk, juridisk og miljømæssig analyse) som grundlag for udviklingen af deres sikkerhedsledelsessystem.

Forbindelsen mellem resultaterne af ledelsens evaluering, og hvordan de er et input til den årlige sikkerhedsrapport.

7 Forbedring

7.1 Erfaringer fra ulykker og hændelser

7.1.1 Lovkrav

7.1. Erfaringer fra ulykker og hændelser

7.1.1. Ulykker og hændelser i forbindelse med organisationens jernbanedrift skal:

- (a) indmeldes, registres, undersøges og analyseres for at fastslå deres årsager
- (b) indberettes til nationale organer, når det er relevant.

7.1.2. Organisationen skal sikre, at:

- (a) anbefalingerne fra den nationale sikkerhedsmyndighed, det nationale undersøgelsesorgan og industrien eller fra interne undersøgelser evalueres og gennemføres, hvis det er hensigtsmæssigt eller påbudt
- (b) relevante rapporter/information fra andre interessenter såsom jernbanevirksomheder, infrastrukturforvaltere, enheder med ansvar for vedligeholdelsen og ihændehavere af jernbanekøretøjer tages i betragtning.

7.1.3. Organisationen skal bruge informationer fra undersøgelsen til at gennemgå risikovurderingen (jf. 3.1.1. Risikovurdering) for at drage erfaringer med det sigte at forbedre sikkerheden og, når det er relevant, indføre korrigerende foranstaltninger og/eller forbedringer (jf. 5.4. Styling af ændringer).

7.1.2 Formål

Organisationen bør påvise, at den undersøger ulykker og hændelser for at opsamle erfaring og forbedre risikostyringen, at personalet, som gør dette, er kompetent til at foretage undersøgelser, også af spørgsmål vedrørende menneskelige og organisatoriske faktorer, at ulykker indberettes til de relevante myndigheder, og at der udarbejdes anbefalinger og rapporter, som ledelsen følger op på.

Analysen af uønskede hændelser har ikke til formål at placere skylden eller at fastslå, at en afdeling er "mere ansvarlig end en anden", men snarere at forstå og udbedre de organisatoriske svagheder, der gjorde hændelserne mulige. Den vigtigste udfordring, når hændelserne analyseres, er således at forebygge "nabohændelser". Hvis analysen nøjes med at identificere de umiddelbare årsager, vil det kun være muligt at forebygge den næste lignende hændelse. Hvis analysen derimod gør det muligt at identificere de tekniske og organisatoriske "root causes", vil forbedringsforanstaltningerne gøre det muligt at forebygge en anden type ulykke, der har de samme mekanismer. Hvis analysen f.eks. viser, at en procedure ikke var opdateret, og at den korrigerende foranstaltning kun tager sigte på at korrigere denne procedure, vil effekten være begrænset. Hvis analysen går længere og identificerer svagheder i processen for opdatering af procedurerne, kan den positive effekt af en forbedringsforanstaltning være langt mere omfattende.

Hertil kommer, at organisationen opnår en "dobbelt erfaringsopsamling". Der er nemlig ikke blot fokus på hændelsernes forløb, men også på organisationens evne til at skabe forbedringer ved at fokusere på de elementer, som enten fremmer eller hæmmer overførslen af viden og information i hele organisationen.

Der opfordres til rapportering af farlige situationer og "højpotentiale"-hændelser, og dette gøres nemt. Hvis det er nødvendigt, eksisterer der mekanismer, som gør rapporteringen anonym. Hvis rapporteringen sker med navn, hjælper de medarbejdere og team, der sendte rapporterne, med analysen og med at finde en beredskabsløsning på kort sigt. Der afholdes drøftelser i teamene, og de trufne foranstaltninger meddeles til de pågældende medarbejdere og til hele organisationen, hvis relevant.

Desuden foretages analysen af farlige hændelser på en tværgående måde, hvor man anvender et forskelligartet sæt kompetencer og tager alle de berørte parter synspunkter i betragtning (evt. også eksterne

parters).

Man fremmer en "åben rapporteringskultur", hvor man anerkender og styrker positive sikkerhedsinitiativer (rapportering af hændelser, involvering af personalet i analysen, løbende forbedring, støtte til kolleger osv.). Denne åbne rapporteringskultur bør fjerne enhver frygt for bebrejdelser ved at definere en bredt accepteret grænse mellem, hvad der accepteres, og hvad der ikke gør. Retten til at lave en fejl accepteres.

7.1.3 Forklarende noter

Termene "nærved-fejl" og "andre farlige tildragelser" er medtaget i definitionen af "hændelse" i henhold til direktiv (EU) 2016/798. Det er ligeledes vigtigt at undersøge nærved-fejl og andre farlige tildragelser for at håndtere sikkerheden på en proaktiv måde.

Erfaringsopsamling fra ulykker og hændelser bør fremme delingen af oplysninger med andre interessenter (infrastrukturforvaltere, andre jernbanevirksomheder eller ECM'er) med henblik på at udvikle samarbejdet og støtte den overordnede forbedring af sikkerhedsledelsessystemets resultater.

Hvad angår undersøgelser, som kræver et perspektiv baseret på menneskelige og organisatoriske faktorer, bør undersøgerne enten være uddannede eller have adgang til passende ekspertise, når de skal undersøge de pågældende spørgsmål.

7.1.4 Dokumentation

- *Oplysninger om indberetningsprocessen for ulykker/hændelser, herunder hvordan root causes identificeres og analyseres, herunder indberetning inden for organisationen og til kompetente myndigheder og andre parter (7.1.1).*
- *Oplysninger om den metode, organisationen bruger i forbindelse med undersøgelsen, herunder de menneskelige og organisatoriske faktorer, for at gennemgå risikoanalysen og evalueringsprocessen efter en hændelse (7.1.3).*
- *Dokumentation for, at der er fulgt op på anbefalinger fra de kompetente myndigheder på grundlag af indberetninger af ulykker og hændelser, og at eventuelle identificerede nødvendige ændringer er blevet foretaget (7.1.2 (a), (b)).*
- *Gennemgang af tidligere hændelser for at identificere faktorer, som er relevante for en aktuel hændelse. Der er dokumentation for en mere omfattende organisatorisk erfaring fra hændelser og erfaring på nationalt og internationalt plan (7.1.3).*
- *Der er en metode for gennemførelse af undersøgelser baseret på viden om og de nyeste metoder for menneskelige og organisatoriske faktorer.*
- *Der eksisterer et uddannelsesprogram for undersøgere af ulykker og hændelser, hvor perspektivet baseret på menneskelige og organisatoriske faktorer bliver anvendt.*

7.1.5 Eksempler på dokumentation

Proceduren for undersøgelse af ulykker, som beskriver undersøgelsesmetoderne og medtager en henvisning til kompetencestyringskravene for undersøgere af ulykker og hændelser.

Et uddrag af forskellige typer ulykkes- og hændelsesrapporter, som viser, at undersøgelserne er foretaget af en kompetent person, at resultaterne er evidensbaserede, og at henstillingerne er blevet fulgt op.

En kopi af proceduren/processen, som sporer de korrigerende/afhjælpende foranstaltninger, der er identificeret efter en ulykke/hændelse.

Der fremlægges oplysninger om brugen af sikkerhedsvarslingsredskabet (SAIT) for at holde øje med og underrette andre organisationer om forhold, der vedrører specifikke aktiver.

Uddannede undersøgere er til rådighed.

Der eksisterer et uddannelsesprogram for undersøgere af ulykker og hændelser.

Referater fra bestyrelsesmøder, som viser, at resultaterne af undersøgelsen af en ulykke/hændelse og de hermed forbundne anbefalinger (dvs. korrigerende foranstaltninger og/eller forbedringsforanstaltninger) rapporteres tilbage til ledelsen, og hvordan de har indflydelse på evalueringen af sikkerhedsledelsessystemet (**jf. også 6.3**).

Ved undersøgelser af ulykker og hændelser anvendes der en tilgang baseret på menneskelige og organisatoriske faktorer. Undersøgelserne har et systemisk perspektiv, dvs. at man ikke bare kigger på de menneskelige, teknologiske og organisatoriske faktorer i sig selv, men også lægger vægt på samspillet mellem de forskellige faktorer. Hvis en lokomotivfører f.eks. har været involveret i en hændelse med forbikørsel af et stopsignal ved passering af et farepunkt, omfatter de foreslåede faktorer, der skal undersøges, f.eks. træthed, kognitiv overbelastning, kompetence osv. (menneskelige faktorer), teknologiens indflydelse på indsatsen, f.eks. grænseflader mellem menneske og system, design, signalplacering (teknologiske faktorer), organisationens indflydelse på indsatsen, f.eks. uddannelse, sikkerhedsledelsessystem, organisatoriske prioriteringer (organisatoriske faktorer) såvel som samspillet mellem de tre områder, f.eks. indkøbets indflydelse på design eller håndtering af ændringer med indførelsen af nyt design.

7.1.6 Referencer og standarder

- IAEA (2002) — *Safety culture in nuclear installations: Guidance for use in the enhancement of safety culture*. IAEA TECDOC-1529. Den Internationale Atomenergiorganisation, Wien (2002).
- Mathis, T.L. & Galloway, S.M. (2013) — *Steps to safety culture excellence*.
- Kecklund, L., Lavin, M. & Lindvall, J. (2016) — *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*, Wien, 22.-26. Februar 2016
- RSSB (2015) — *Safety Culture and behavioural development: Common factors for creating a culture of continuous development* (www.sparkrail.org)

7.1.7 Tilsynsspørgsmål

Kompetencen hos undersøgere af ulykker/hændelser er af afgørende vigtighed for at nå frem til fornuftige anbefalinger og sørge for passende forebyggende foranstaltninger. De, der foretager tilsynet, bør holde øje med ledelsens indgriben i resultaterne af rapporter om ulykker og hændelser, som kan påvirke kvaliteten af rapporten og rapportens resultater.

Resultaterne af en intern undersøgelse har medført organisatorisk erfaringsopsamling, som er registreret i dokumenter, rapporter eller andre informationskanaler (dvs. intranettet, virksomhedens medarbejderblad osv.).

Organisationskulturen i forbindelse med rapportering af hændelser og nærvæd-hændelser.

7.2 Løbende forbedring

7.2.1 Lovkrav

7.2.1.	Organisationen skal løbende forbedre sit sikkerhedsledelsessystems tilstrækkelighed og effektivitet, idet der tages hensyn til den ramme, der er fastsat i forordning (EU) nr. 1078/2012, og som minimum skal resultaterne af følgende aktiviteter indgår i overvejelserne: <ul style="list-style-type: none">(a) overvågning (jf. 6.1. Overvågning)(b) intern audit (jf. 6.2. Intern audit)(c) ledelsens evaluering (jf. 6.3. Ledelsens evaluering)(d) erfaringer fra ulykker og hændelser (jf. 7.1. Erfaringer fra ulykker og hændelser).
7.2.2.	Organisationen skal fastlægge midler til at motivere personale og andre interessenter til aktivt at forbedre sikkerheden som led i den organisatoriske læring.
7.2.3.	Organisationen skal udarbejde en strategi for løbende forbedringer af sin sikkerhedskultur baseret på fagkundskab og anerkendte metoder med henblik på at påvise adfærdsrelaterede problemstillinger, der påvirker sikkerhedsledelsessystemets forskellige dele, og iværksætte tiltag for at tage højde for disse.

7.2.2 Formål

Løbende forbedring er en vigtig del af et effektivt sikkerhedsledelsessystem. Formålet med dette krav er at få ansøgerne til at vise, at de gør deres bedste for at sikre forbedring, og at deres sikkerhedsledelsessystem understøtter dette.

Den øverste ledelse deltager i **fælles refleksion** for løbende at forbedre organisationens sikkerhedskultur.

Denne fælles refleksion er forankret i en strategi rettet mod **kulturelle normer**, der i væsentlig grad påvirker sikkerhedsniveauet, og som bør vurderes højere eller gøres til genstand for ændringer.

7.2.3 Forklarende noter

Løbende forbedring (**7.2.1**) fokuserer på de elementer i sikkerhedsledelsessystemet, som evaluerer og fører til forbedringsforanstaltninger, men ikke på de elementer, der allerede er genstand for forbedring, eftersom de allerede er omfattet af overvågningsaktiviteterne.

Ved organisatorisk læring (**7.2.2**) forstås processen med at forbedre indsatsen gennem bedre viden og forståelse.

Sikkerhedskultur (**7.2.3**) har her den definition, der henvises til i 2.1.1 j) og den tilknyttede note. En positiv sikkerhedskultur motiverer organisationer og personer og gør dem i stand til at stræbe efter at forbedre sikkerheden og indsatsen. Den øger jobtilfredsheden og jobfastholdelsen og giver omkostningsmæssige fordele. Den kan også bidrage til overholdelsen af de lovgivningsmæssige forventninger, eftersom sikkerhedsmyndighederne og lovgiverne i stadig større grad anerkender den rolle, sikkerhedskulturen spiller for effektiv sikkerhedsledelse. Mere specifikt kan en positiv sikkerhedskultur føre til:

- en reduktion af de driftsmæssige risici gennem en mere omfattende risikovurdering og en bedre forståelse af risiciene fra personalets side
- færre arbejdsulykker ved at fjerne risici identificeret gennem øget rapportering af nærvæd-fejl
- færre usikre handlinger og forhold gennem øget engagement fra personalets side og udvikling af lederskab
- færre udgifter i forbindelse med arbejdsulykker, usikre handlinger og forhold

- *en forbedret indsats ved hjælp af styrket personaleuddannelse, engagement og reduktion af ulykker, usikre handlinger og forhold.*
- *et forbedret og mere effektivt sikkerhedsledelsessystem med procedurer og regler, der svarer bedre til virkeligheden.*

På grund af kulturs grundlæggende karakteristika, som skabes via det daglige samspil og som er vanskelige at ændre, bør denne strategi anses for at være langsigtet og ejet og understøttet af den øverste ledelse.

Der er mange måder at forbedre sikkerhedskulturen på, f.eks.:

- *Udvikling af et system til deling af bekymringer. Dette kan være anonymt, alt afhængigt af organisationens modenhed, men med en voksende tillid kan det være åbent og tilgængeligt for alle. Det er vigtigt, at feedback bliver indbygget i systemet, så man sikrer, at medarbejderne føler sig involveret og mærker et tilhørsforhold.*
- *Ændring af indkøb og kontraktbetingelser for at fremme en god sikkerhedskultur for leverandører. Sikkerhedskulturen kunne være et kriterium for valg af leverandører.*
- *Synlig belønning af sikker adfærd. Belønningen kan antage mange former, lige fra større årlig betaling gennem bonusser til ugentlige sikkerhedsbelønninger for en enestående indsats.*
- *Opstilling af specifikke mål for ledere med hensyn til sikkerhedsledelse, f.eks. en opfordring til ledelsen om at indtage en mere synlig rolle på området ved at gå foran med et godt eksempel.*

Ved vurdering af sikkerhedskulturen bør der anvendes en tilgang med flere metoder. Dataindsamlingsmetoder bør være baseret på samfundsvidenskabelig forskning. Det indebærer, at data indsamles ved hjælp af feltarbejde i hele organisationen, og at der anvendes teknikker som observationer, dokumentanalyse og interviews.

Vurderingernes resultater bør kommunikeres på alle niveauer i organisationen. Der bør følges op på dem for at fremme og opretholde en positiv sikkerhedskultur, forbedre sikkerhedsledelsen og fremme en holdning, hvor man lærer af sine erfaringer.

Identifikation og valg af relevante kulturelle normer er ofte en kompleks opgave¹, der bør udføres omhyggeligt.

Denne opgave bør inddrage personale på alle niveauer i hele organisationen og ofte også ud over organisationen (f.eks. kontrahenter).

Viden om personalets holdninger og overbevisninger kan indsamles gennem en spørgeskemaundersøgelse, men en sådan metode anses normalt for at være utilstrækkelig til at etablere kulturelle normer, der påvirker sikkerheden. Ekspertes bør, eventuelt ud fra undersøgelsesresultaterne, gennemføre observationer, individuelle interviews og fokusgrupper for at fastslå en mere præcis diagnose.

Bemærk: En fokusgruppe samler en lille gruppe af personer (normalt 4-15), som under ledelse af en moderator fokuserer på et specifikt emne. Fokusgrupper har til formål at diskutere snarere end at give individuelle svar på formelle spørgsmål samt at producere kvalitative data.

¹ Diversitet i organisationens aktiviteter og størrelse er enkle eksempler på parametre, der følger med denne opgaves kompleksitet.

På basis af diagnosen kan der, med støtte fra den øverste ledelse, udarbejdes en handlingsplan, der skal sikre bedre kulturel forståelse og bidrage til en ændring af kulturelle normer. Den øverste ledelse overvåger gennemførelsen af de identificerede tiltag og opdaterer løbende planen.

For at sikre strategiens holdbarhed bør diagnosen revideres hvert 2.-5. år med samme tilgang. Hyppigheden afhænger af resultaterne af den indledende øvelse.

I mange højriskbrancher udarbejdes denne diagnose ofte inden for rammerne af en sikkerhedskulturvurdering, der fører til en handlingsplan (jf. Figur 2: Sikkerhedskulturvurderinger).

Vurderingen af sikkerhedskulturen kan foretages af en uafhængig enhed eller af organisationen selv. Fordelen ved en uafhængig vurdering er, at organisationen får et mere objektivt billede af sikkerhedskulturen. Der er dog risiko for, at organisationen bliver misforstået eller har svært ved at acceptere konklusionerne. Fordelen ved en vurdering foretaget af organisationen selv er, at den foretages internt med organisationens eget personale, som har indgående viden om organisationen. Ulempen er, at status og hierarkier kan forstyrre billedet. Eksempler på karakteristika i en sikkerhedskulturvurdering:

- Omfatter en 2/3-uges vurderingsproces og et forberedende trin.
- Involverer et tværfagligt review-team.
- Dataindsamling er baseret på samfundsvidenskabelige metoder (herunder interviews, fokusgrupper, observationer).
- Vurderingens rammer er hele organisationen og dens grænseflader.
- Baseret på en sikkerhedskulturmodel eller en sikkerhedskulturramme.
- Den øverste ledelse tillægger vurderingen stor betydning og anser den som en læringsmulighed.
- Resultaterne forplanter sig i hele organisationen.
- Der følges op på resultaterne ved at udarbejde/revidere en strategi med henblik på løbende at forbedre de valgte normer for sikkerhedskulturen.

Figur 2: Sikkerhedskulturvurderinger

Forbedringen af strategien og processerne vedrørende menneskelige og organisatoriske faktorer er en integreret del af den løbende forbedring af sikkerhedsledelsessystemet.

En systematisk tilgang defineres som en trinvis proces, der håndterer de spørgsmål, som er relateret til sikkerhedskulturen. F.eks. at have en proces for risikoobservation, rapportering af ulykker og hændelser, og hvordan oplysningerne bruges, samt den erfaring, der er opsamlet, med henblik på løbende forbedring.

Yderligere oplysninger om sikkerhedskultur findes i bilag 4.

7.2.4 Dokumentation

- *Oplysninger om processen for sammenligning af dokumentation med henblik på at påvise løbende forbedring af sikkerhedsledelsessystemet (7.2.1).*
- *Procedurer for, hvordan organisationen tager resultaterne fra overvågning, intern audit, ledelsens evaluering og erfaringer fra ulykker og hændelser i betragtning med henblik på at forbedre sikkerhedsledelsessystemet (7.2.1).*
- *Oplysninger om, hvordan organisationen søger at engagere personalet og andre i at forbedre sikkerhedsledelsessystemet (7.2.2).*

- Ansøgerne bør i en strategi redegøre for, hvordan sikkerhedskulturen udvikles, så der tages korrekt højde for risiciene i forbindelse med sikkerhedskulturen i de relevante processer i sikkerhedsledelsessystemet. Når ansøgerne gør dette, bør de gøre det klart, hvor der kan findes yderligere oplysninger om de relevante procedurer (7.2.3).
- Sikkerhedskulturen vurderes løbende med henblik på at identificere forbedringer (7.2.3).
- Forbedringer af sikkerhedskulturen foretages ved hjælp af PDCA-cyklussen for at sikre, at foranstaltningerne har en indvirkning. De opnåede erfaringer gennemføres, og deres indvirkning evalueres systematisk (7.2.3).

7.2.5 Eksempler på dokumentation

Proceduren, der dækker overvågning, intern audit, gennemgang på ledelsesplan og undersøgelse af ulykker og hændelser, navnlig de afsnit, der omhandler de opnåede erfaringer i forhold til sikkerhedsledelsessystemet.

"Close Call"-initiativet inden for Network Rail (www.safety.networkrail.co.uk/alerts-and-campaign/close-call), hvor medarbejderne opfordres til aktivt at underrette organisationen om svagheder/mangler eller situationer, hvor der er en sikkerheds- eller sundhedsrisiko.

Eksempler på referater fra de regelmæssige fagforenings-/ledelsesmøder om sundhed og sikkerhed, som viser, hvor situationer, der anses for at være uvisse/usikre eller kræver yderligere overvejelse, er blevet drøftet.

Resultaterne af undersøgelser af ulykker rapporteres på ledelsesmøder og betragtes som en vigtigt redskab til læring og forbedring.

En kopi af strategien til forbedring af sikkerhedskulturen, og hvordan den hænger sammen med de forskellige dele af sikkerhedsledelsessystemet.

Strategien giver tilstrækkelig dokumentation for, at der er faglig kompetence og den nødvendige uddannelse og erfaring på området for sikkerhedskultur for at gennemføre og udvikle strategien.

Den påkrævede type uddannelse og kompetence er relateret til forståelsen af begrebet "sikkerhedskultur" og de midler og metoder, der skal anvendes til at måle og arbejde for løbende forbedringer. Det afgørende aspekt er, at sikkerhedskulturen forstås som et holistisk begreb, der har indflydelse på alle dele af sikkerhedsledelsessystemet, og at sikkerhedskulturen ikke kan behandles som et separat element.

Der er en proces for løbende evaluering af sikkerhedsforbedrende foranstaltninger. Effekterne af de sikkerhedsforbedrende foranstaltninger identificeres og bringes til udførelse, så de kan evalueres.

7.2.6 Tilsynsspørgsmål

I forbindelse med tilsynet bør ledelsens forpligtelse i forhold til løbende forbedring af sikkerhedsledelsessystemet undersøges ved hjælp af interviews og ved at analysere dokumentationen. Er der en risikobaseret tilgang til forbedringen, dvs. er den forbundet med sårbare og kritiske kontrolforanstaltninger?

Organisationens brug af modenhedsmodeller til at undersøge sikkerhedsledelsessystemets resultater bør undersøges, såfremt sådanne eksisterer.

Bilag 1 — Sammenligningstabeller

Nedenstående tabeller indeholder en direkte sammenligning mellem vurderingskravene i bilag II til de tidligere forordninger (EU) 1158/2010 og (EU) 1169/2010 og kravene i bilag I og bilag II til Kommissionens delegerede forordning (EU) 2018/762. Den skal lette overgangen fra den tidligere sikkerhedscertificeringsordning i henhold til direktiv 2004/49/EF til den nye som indført i direktiv (EU) 2016/798.

At der er tilsvarende krav i Kommissionens delegerede forordning (EU) 2018/762 er ikke et bevis for, at jernbanevirksomhederne eller infrastrukturforvalterne er i stand til at overholde de relevante krav til sikkerhedsledelsessystemer i henhold til artikel 9 i direktiv (EU) 2016/798. Detaljeniveauet mellem de tidligere og de nye vurderingskrav kan stadig være forskelligt, selv om de i en vis udstrækning bygger på fælles principper. Desuden er det ikke alle vurderingskrav i bilag I og bilag II til Kommissionens delegerede forordning (EU) 2018/762, der har tilsvarende krav i de tidligere forordninger. Der kræves så yderligere dokumentation fra jernbanevirksomhederne og infrastrukturforvalterne for at overholde de nye vurderingskrav (eller dele af dem).

Kravene til sikkerhedsledelsessystemer i kommissionens delegerede forordning (EU) 2018/762, som ikke har noget tilsvarende krav i forordning (EU) 1158/2010 og/eller forordning (EU) 1169/2010, skal betragtes som nye krav, og i den henseende skal ansøgerne fremlægge yderligere dokumentation for at påvise overholdelse af disse. I de fleste tilfælde er det ikke muligt at få et perfekt match mellem kriterierne i de tidligere forordninger og kravene i den nye forordning om fastlæggelse af CSM. I disse tilfælde vil sammenligningen således være baseret på hensigten med kravene. Det kan også være tilfældet, at kravene er gjort mere udtrykkelige i Kommissionens delegerede forordning (EU) 2018/762, men at hensigten er den samme. I så fald skal kravene i denne forordning ikke betragtes som nye, men kan bruges af de forskellige parter som en hjælp til at forstå, hvilken dokumentation der forventes af ansøgerne.

Jernbanevirksomheder og infrastrukturforvaltere, som er villige til at udvikle et integreret ledelsessystem, henvises også til ISO High Level Structure (HLS)². På samme måde er den kendsgerning, at jernbanevirksomhederne eller infrastrukturforvalterne har et ledelsessystem, som er certificeret efter en eller flere ISO-ledelsessystemstandarder (f.eks. ISO 9001, ISO 14001 eller ISO 45001), ikke et bevis for, at de er i stand til at opfylde de relevante krav til sikkerhedsledelsessystemer i henhold til artikel 9 i direktiv (EU) 2016/798.

Tabel 1: Direkte sammenligning — Vurderingskriterier/krav, som er fælles for jernbanevirksomheder og infrastrukturforvaltere

<i>Forordning (EU) 1158/2010 og 1169/2010 Kriteriets ID</i>	<i>Forordning (EU) 2018/762 Kravets ID</i>	<i>ISO HLS Bestemmelse nr.</i>	<i>Kommentar</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)	Ikke relevant	
A.5	4.4 4.5.1.1	7.4	

² ISO/IEC Directives, Part 1, consolidated supplement 2016, Annex SL Appendix 2.

<i>Forordning (EU) 1158/2010 og 1169/2010 Kriteriets ID</i>	<i>Forordning (EU) 2018/762 Kravets ID</i>	<i>ISO HLS Bestemmelse nr.</i>	<i>Kommentar</i>
A.6	6.1.1 5.4.1	9.1 8.1	
B.1	5.2.4	Ikke relevant	Vedligeholdelse er en fase i aktivets livscyklus.
B.2	5.2.4	Ikke relevant	Vedligeholdelse er en fase i aktivets livscyklus.
B.3	2.3.1 4.2.1	5.3 7.2	En definition og tildeling af ansvaret for vedligeholdelse findes først og fremmest i 2.3.1. En identifikation af de kompetencer, der kræves til vedligeholdelse, findes først og fremmest i 4.2.1.
B.4	6.1.1 5.2.5	9.1 7.4	Dataindsamling (funktionsfejl, mangler) og analyse indgår i overvågningsprocessen. Udveksling af oplysninger mellem dem, der er ansvarlige for de daglige aktiviteter, og dem, der er ansvarlige for vedligeholdelsen, indgår i den oplysnings- og kommunikationsproces, der anvendes ved forvaltning af aktiver.
B.5	6.1.1	Ikke relevant	Som omhandlet i artikel 4, stk. 2, i CSM Mo.
B.6	6.1.1	9.1	Præstationsevalueringen og vedligeholdelsens resultater indgår i den overvågningsproces, der anvendes for vedligeholdelsen.
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)	Ikke relevant	
C.4	5.2.5 (b) 5.3.2 (c)	Ikke relevant	
C.5	5.3.2 (c) 5.3.3 (a)	Ikke relevant	
D.1	3.1.1.1 (a)	Ikke relevant	
D.2	3.1.1.1 (c)	Ikke relevant	
D.3	6.1.1	Ikke relevant	
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	
F.1	4.5.1.1 (a)	4.4	

<i>Forordning (EU) 1158/2010 og 1169/2010 Kriteriets ID</i>	<i>Forordning (EU) 2018/762 Kravets ID</i>	<i>ISO HLS Bestemmelse nr.</i>	<i>Kommentar</i>
F.2	2.3 4.5.1.1 (a)	5.3 4.4	
F.3	2.3.1 2.3.4	Ikke relevant	
F.4	4.5.1.1 (a) 4.2.1 2.3.1 2.3.2 2.3.3	4.4 5.3	En definition af sikkerhedsrelaterede opgaver indgår i beskrivelsen af sikkerhedsledelsessystemet, herunder tildelingen af ansvarsområder. Ansvarsområderne defineres for hver relevant rolle inden for sikkerhedsledelsessystemet.
G.1	4.5.1.1 (a) 2.3.1	4.4 5.3	En definition af sikkerhedsrelaterede opgaver indgår i beskrivelsen af sikkerhedsledelsessystemet, herunder tildelingen af ansvarsområder. Ansvarsområderne defineres for hver relevant rolle inden for sikkerhedsledelsessystemet.
G.2	6.1.1 6.2.1	9.1 9.2	Intern audit har til formål at kontrollere, at organisationen overholder de gældende krav.
G.3	2.1.1 (d)(i) 2.3.2	Ikke relevant	
G.4	2.3.1	5.3	
G.5	4.1.1	7.1	Bemærk, at der her er et link til kriteriet i 1158/2010 N2(d)
H.1	2.4.1	Ikke relevant	
H.2	(udgået)	Ikke relevant	Personale, som udfører sikkerhedsrelaterede opgaver, bør involveres i sikkerhedsledelsessystemets udvikling, vedligeholdelse og forbedring. Det overlades til organisationen at gennemføre krav. 2.4.1 på en sådan måde, at dets overholdelse kan spores.
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	Sikkerhedsmålene skal være i overensstemmelse med sikkerhedspolitikken, som skal passe til jernbanedriftens type og omfang.
K.3	3.2.4	6.2	Sikkerhedsmålene er ikke begrænset til de fælles sikkerhedsmål, der er opstillet på medlemsstatsniveau.
K.4	6.1.1 5.4	9.1 8.1	

<i>Forordning (EU) 1158/2010 og 1169/2010 Kriteriets ID</i>	<i>Forordning (EU) 2018/762 Kravets ID</i>	<i>ISO HLS Bestemmelse nr.</i>	<i>Kommentar</i>
K.5	3.2.4 (tilpasset)	9.1	Henvisning til overvågningsstrategien og -plan(erne) i henhold til CSM Mo.
L.1	6.1.1 5.4	9.1 8.1	
L.2	4.2 4.4 4.5 5.2.2 (a)	Ikke relevant	Brug af kompetent personale, procedurer, specifikke dokumenter og rullende materiel er medtaget i punkterne om henholdsvis kompetence, information og kommunikation, dokumentet information og forvaltning af aktiver.
L.3	1.1.1 © 6.1.1 6.1.2	4.3 9.2	Overensstemmelse med de gældende krav er først og fremmest medtaget i 3.1.2.2 (ikke specifikt for vedligeholdelse). Overvågning sikrer korrekt anvendelse af procedurerne. Intern audit sikrer, at procedurerne er i overensstemmelse med de gældende krav.
M.1	3.1.2.1 5.4.1	6.1 8.1	I henhold til ISO foretages der først en planlægning af ændringen, herunder risikoidentificering –g -vurdering, hvorefter ændringen gennemføres.
M.2	3.1.2.1	Ikke relevant	
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	Ikke relevant	
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	Ikke relevant	
P.1	4.4.3	Ikke relevant	
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	

<i>Forordning (EU) 1158/2010 og 1169/2010 Kriteriets ID</i>	<i>Forordning (EU) 2018/762 Kravets ID</i>	<i>ISO HLS Bestemmelse nr.</i>	<i>Kommentar</i>
Q.2	7.1.2	Ikke relevant	
Q.3	7.1.3	10.2	
R.1	5.5.1	Ikke relevant	
R.2	5.5.2	Ikke relevant	
R.3	5.5.3	Ikke relevant	
R.4	5.5.4	Ikke relevant	
R.5	5.5.5	Ikke relevant	
R.6	5.5.1	Ikke relevant	
R.7	5.5.6	Ikke relevant	
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) til (f)	9.2	
S.5	6.2.1 (g) 6.3.1	9.3	
S.6	6.2.1	9.2	

I tabellen nedenfor foretages en direkte sammenligning af de tidligere vurderingskriterier og de nye krav til sikkerhedsledelsessystemer, der kun gælder for jernbanevirksomheder.

Tabel 2: Direkte sammenligning — Vurderingskriterier/krav, som er specifikke for jernbanevirksomheder

<i>Forordning (EU) 1158/2010 Kriteriets ID</i>	<i>Forordning (EU) 2018/762 Bilag I Kravets ID</i>	<i>ISO HLS Bestemmelse nr.</i>	<i>Kommentar</i>
R.8	5.5.7	Ikke relevant	
R.9	5.5.8	Ikke relevant	

I tabellen nedenfor foretages en direkte sammenligning af de tidligere vurderingskriterier og de nye krav til sikkerhedsledelsessystemer, der kun gælder for infrastrukturforvaltere.

Tabel 3: Direkte sammenligning — Vurderingskriterier/krav, som er specifikke for infrastrukturforvaltere

Forordning (EU) 1169/2010 Kriteriets ID	Forordning (EU) 2018/762 Bilag II Kravets ID	ISO HLS Bestemmelse nr.	Kommentar
R.8	5.5.7	Ikke relevant	
R.9	5.5.8	Ikke relevant	
T.1	5.2.1	Ikke relevant	Sikker udformning og installation af infrastrukturen indgår i aktivets livscyklus.
T.2	3.1.2 5.4.1	Ikke relevant	En identifikation af den tekniske ændring af infrastrukturen findes først og fremmest i 3.1.2. Styring af den tekniske ændring af infrastrukturen findes først og fremmest i 5.4.1.
T.3	3.1.2	Ikke relevant	Overholdelse af de gældende regler for infrastrukturens udformning findes først og fremmest i 3.1.2.
U.1	5.1.1 5.1.3	Ikke relevant	Styring af infrastrukturens sikkerhed findes først og fremmest i 5.1.1.
U.2	5.1.1	Ikke relevant	Styring af sikkerheden ved infrastrukturens fysiske og/eller driftsmæssige grænser findes først og fremmest i 5.1.1.
U.3	5.1.3 (c) 5.5.7	Ikke relevant	Styring af normal og uregelmæssig drift findes først og fremmest i 5.1.3 (c).
U.4	5.1.2 5.2.3	Ikke relevant	
V.1	5.2.4 6.1.1	Ikke relevant	Styring af infrastrukturen findes først og fremmest i 5.2.4. Audits og inspektioner (hvis relevant) indgår i overvågningsaktiviteterne.
V.2	5.2.4	Ikke relevant	Styring af infrastrukturen findes først og fremmest i 5.2.4.
V.3	5.2.3	Ikke relevant	
W.1	5.1.3	Ikke relevant	
W.2	5.1.1	Ikke relevant	Styring af sikkerheden ved de fysiske og/eller driftsmæssige grænser for trafikkontrol- og signalsystemet findes først og fremmest i 5.1.1.
W.3	5.1.2 5.2.3	Ikke relevant	

I tabellen nedenfor foretages en direkte sammenligning af ISO HLS og de nye krav til
sikkerhedsledelsessystemer.

Tabel 4: Direkte sammenligning — ISO High Level Structure

ISO HLS Bestemmelse nr.	Forordning (EU) 2018/762 Kravets ID	Kommentar
4.1	1.1.1 (a) 1.1.1 (b)	
4.2	1.1.1 € 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	CSM RA anvendes for at bestemme, om en ændring er sikkerhedsrelateret (eller ej), og om den er signifikant (eller ej). Den "virtuelle" sontring, som ISO foretager mellem det strategiske niveau (bestemmelse 6 i ISO HLS) og det taktiske niveau (bestemmelse 8 i ISO HLS) af planlægningen tages op til revurdering på baggrund af EU-lovgivningen og navnlig anvendelsen af ovennævnte CSM (uanset ændringernes karakter).
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	
7.4	4.4	
7.5.1	4.5.1	
7.5.2	4.5.2	
7.5.3	4.5.3	

<i>ISO HLS Bestemmelse nr.</i>	<i>Forordning (EU) 2018/762 Kravets ID</i>	<i>Kommentar</i>
8.1	5.1 5.2 5.3 5.4 5.5	I henhold til ISO's vejledende dokument (N360) tager bestemmelse 8 i ISO HLS sigte på at specificere de krav, der skal gennemføres med hensyn til organisationens drift, for at sikre, at ledelsessystemkravene opfyldes, og at man ser på de vigtige risici og muligheder. Det nævnes desuden, at yderligere (disciplinspecifikke) krav i forbindelse med planlægning og styring af driften kan fastlægges. I den henseende er kravene i 5.X i tråd med ISO's tilgang. De griber navnlig ikke ind i virksomhedens forretning, men giver tilstrækkelige rammer til at kontrollere, hvordan vigtige sikkerhedsspørgsmål bliver håndteret i virksomhedens forretningsgange.
9.1	6.1	Begrebet "overvågning" henviser til den overvågningsramme, der er defineret i CSM for overvågning, og har derfor en bredere betydning end begrebet "overvågning, måling, analyse og evaluering", som defineres i bestemmelse 9.1 i ISO HLS.
9.2	6.2	Interne audits er overvågningsredskaber i den betydning, der er medtaget i CSM for overvågning. Selv om det er et separat krav, skal det opfylde overvågningsmålsætningerne i henhold til CSM for overvågning.
9.3	6.3	
10.1	7.1	
10.2	7.2	

Bilag 2 — Gensidig accept af godkendelser, anerkendelser eller certifikater for produkter eller tjenester udstedt i henhold til EU-lovgivningen

Den myndighed, som udsteder EU-sikkerhedscertifikatet eller sikkerhedsgodkendelsen, kan tage certifikater udstedt af andre organer i betragtning, f.eks. ISO-overensstemmelsesvurderingsorganer, for at undgå dobbeltarbejde i forbindelse med vurderingen og yderligere omkostninger for ansøgeren. Den endelige beslutning ligger altid hos den udstedende myndighed.

I henhold til artikel 3, stk. 12, i gennemførelsesforordning (EU) 2018/763 skal den udstedende myndighed i forbindelse med vurderingen af ansøgninger om EU-sikkerhedscertifikater dog acceptere godkendelser, anerkendelser eller certifikater for produkter eller tjenester fra jernbanevirksomheder eller deres kontrahenter, partnere eller leverandører, som er udstedt i henhold til relevant EU-lovgivning, som bevis på jernbanevirksomhedernes evne til at opfylde de tilsvarende krav til sikkerhedsledelsessystemer for den pågældende type produkt eller tjeneste. Selv om der ikke er en tilsvarende bestemmelse i EU-lovgivningen om vurderingen af ansøgninger om sikkerhedsgodkendelser, opfordres de nationale sikkerhedsmyndigheder også til at anvende samme princip.

Følgende tabel giver en oversigt over de forskellige tilfælde, der hidtil er taget højde for i EU-lovgivningen, og indeholder illustrative eksempler på typer af produkter eller tjenester, som kan være omfattet i hvert tilfælde.

Tabel 5: Godkendelser, anerkendelser eller certifikater for produkter eller tjenester udstedt i henhold til EU-lovgivningen

<i>Tilfælde</i>	<i>Type af produkter eller tjenester</i>	<i>Gældende EU-lovgivning</i>	<i>Forordning (EU) 2018/762 Kravets ID</i>	<i>Kommentar</i>
ECM-certifikat	Vedligeholdelse af køretøjer	Artikel 14, stk. 4, i direktiv (EU) 2016/798	5.2 5.3	I de tilfælde, der er taget højde for i artikel 14, stk. 4, i direktiv (EU) 2016/798, giver certificering af enheder med ansvar for vedligeholdelse og af vedligeholdelsesværksteder, hvor det er relevant, tilstrækkelig dokumentation for, at jernbanevirksomhederne og infrastrukturforvalterne ved hjælp af deres sikkerhedsledelsessystem er i stand til at styre risiciene i forbindelse med vedligeholdelse af godsvogne, herunder brugen af kontrahenter.

<i>Tilfælde</i>	<i>Type af produkter eller tjenester</i>	<i>Gældende EU-lovgivning</i>	<i>Forordning (EU) 2018/762 Kravets ID</i>	<i>Kommentar</i>
Anerkendelse	Uddannelse af lokomotivførere	Direktiv 2007/59/EF Afgørelse 2011/765/EU	4.2.2	Uddannelsescentre bør være anerkendt af den kompetente myndighed til at give kurser til lokomotivførere og lokomotivføreraspiranter i henhold til direktiv 2007/59/EF. Uddannelsescentre spiller en vigtig rolle, når det gælder om at sikre, at lokomotivførere er kompetente til de sikkerhedsrelaterede opgaver, de skal udføre. I den henseende bør uddannelsescentre være kompetente med hensyn til den uddannelse, de giver, og deres anerkendelse af en kompetent myndighed bør, hvor det er relevant, tages i betragtning af sikkerhedscertificeringsorganet og den nationale sikkerhedsmyndighed, når de foretager en vurdering af kompetencestyringssystemet.

<i>Tilfælde</i>	<i>Type af produkter eller tjenester</i>	<i>Gældende EU-lovgivning</i>	<i>Forordning (EU) 2018/762 Kravets ID</i>	<i>Kommentar</i>
Lokomotivførerlicens og -certifikat	Lokomotivføreres kompetence og egnethed	Direktiv 2007/59/EF	4.2.1	Licenser og certifikater udstedt i henhold til direktiv 2007/59/EF giver tilstrækkelig dokumentation for lokomotivføreres kompetence og egnethed. Dette forhindrer ikke organisationen i at påvise, at dens foranstaltninger med hensyn til kompetence og egnethed er tilstrækkelige.
EU-sikkerhedscertifikat	Vedligeholdelse og inspektion af infrastruktur Rangering Test af rullende materiel	Artikel 10 i direktiv (EU) 2016/798	5.3	Infrastrukturforvalterne kan udlicitere vedligeholdelsen eller inspektionen af deres infrastruktur til virksomheder, der kører med specialkøretøjer på sporet. Leverandører af rangerydelser eller test kan ligeledes blive anmodet om at have et sikkerhedscertifikat. I de ovenstående tilfælde giver EU-sikkerhedscertifikatet tilstrækkelig dokumentation for, at jernbanevirksomhederne og infrastrukturforvalterne ved hjælp af deres sikkerhedsledelsessystemer er i stand til at styre risiciene i forbindelse med brugen af kontrahenter og leverandører.

<i>Tilfælde</i>	<i>Type af produkter eller tjenester</i>	<i>Gældende EU-lovgivning</i>	<i>Forordning (EU) 2018/762 Kravets ID</i>	<i>Kommentar</i>
Køretøjsomsætningstilladelse/typegodkendelse	Typegodkendelse	Direktiv (EU) 2016/797	5.2	Typegodkendelsen sikrer gennem design, tilrettelæggelse, verifikation og validering, at der er overensstemmelse med de væsentlige krav i al gældende lovgivning (herunder sikkerhedskravene), således at køretøjet kan bruges sikkert på de jernbanenet, det er beregnet til, i henhold til de brugsbetingelser og -begrænsninger, der er angivet i det tekniske dossier for køretøjet/køretøjstypen.

I specifikke tilfælde er besiddelsen af et certifikat (eller tilsvarende), som er udstedt i henhold til EU-lovgivningen, muligvis ikke tilstrækkeligt til at styre alle sikkerhedsrisici i forbindelse med det produkt, der leveres til, eller de tjenester, der anvendes af jernbanevirksomhederne og infrastrukturforvalterne.

F.eks. er jernbanevirksomheder i et partnerskab stadig fuldt ud ansvarlige for en sikker drift og dermed for styringen af risici i forbindelse med deres aktiviteter, herunder levering af vedligeholdelse af køretøjer. Det er ikke tilstrækkeligt, at en jernbanevirksomhed bruger sin partners EU-sikkerhedscertifikat som et middel til at styre risiciene i forbindelse med levering af vedligeholdelse, hvis det ikke underbygges af stærke, effektive kontraktlige aftaler mellem partnerne. Disse kontraktlige aftaler skal udvikles i fællesskab og overvåges ved anvendelsen af hver enkelt partners procedurer for sikkerhedsledelsessystemer. De er også en del af de enkelte sikkerhedsledelsessystemer og derfor genstand for de respektive nationale sikkerhedsmyndigheders tilsyn.

EU-sikkerhedscertifikatet kan således bruges som et middel til at styre risiciene i forbindelse med levering af vedligeholdelse og som et middel til at overholde kravene til styring af risiciene i forbindelse med vedligeholdelse af køretøjer, når følgende tre betingelser er opfyldt:

1. Der skal være indgået kontraktlige aftaler mellem partnerjernbanevirksomhederne, der omfatter aspekter, som vedrører vedligeholdelse af køretøjer, f.eks.:
 - a) udveksling af oplysninger som beskrevet i artikel 5 i forordning (EU) 445/2011
 - b) teknisk support, når det er påkrævet, navnlig med hensyn til togkontrolsystemer
 - c) kontrol af de kontraherende vedligeholdelsesværksteders evne til at udføre vedligeholdelse
 - d) effektiv overvågning af køretøjer og udveksling af oplysninger som følge af denne overvågning.

2. *Disse kontraktlige aftaler udvikles som et resultat af risikovurderingen, og de enkelte jernbanevirksomheder skal overvåge dem regelmæssigt i henhold til CSM for overvågning (forordning (EU) 1078/2012). Resultatet af denne overvågning udveksles derefter formelt mellem de to partnerjernbanevirksomheder.*
3. *De to partners sikkerhedsledelsessystem indeholder tilstrækkelige processer og procedurer til at opfylde betingelse 1 og 2 ovenfor.*

I andre tilfælde kan den nationale lovgivning kræve, at man for en specifik type produkt eller tjeneste er i besiddelse af et nationalt certifikat (eller tilsvarende), der udstedes af et kompetent organ (f.eks. den nationale sikkerhedsmyndighed), hvilket også kan bruges som bevis for, at jernbanevirksomhederne eller infrastrukturforvalterne er i stand til at opfylde de relevante krav i Kommissionens delegerede forordning (EU) 2018/762. F.eks. kan nationale certifikater udstedt til ECM'er og/eller vedligeholdelsesværksteder for andre køretøjer end godsvogne også — på samme måde som ECM-certifikatet — give en rimelig garanti for, at de køretøjer, de står for vedligeholdelsen af, er i en sikker driftstilstand.

Bilag 3 — Sidesporsaktiviteter, kontraktlige aftaler og partnerskaber

Sidesporsaktiviteter

I dette dokument forstås der ved "sidespor" jernbaneinfrastruktur, som er forbundet med et jernbanenet, der hører under en infrastrukturforvalters ansvarsområde (dvs. infrastrukturen af et jernbanesystem, som falder ind under anvendelsesområdet for direktiv (EU) 2016/798). Sidespor kan evt. være en del af dette jernbanenet, alt afhængigt af ovenstående direktivs gennemførelse i national ret i de enkelte medlemsstater.

Aktiviteter udført i sidespor såsom lastning af godsvogne er industrielle aktiviteter, der berører specifikke jernbaneaktiviteter som oprangering, klargøring og flytning af køretøjsgrupper, der kan være tog eller bliver brugt i tog. Dette omfatter sammenkobling af forskellige køretøjer, så de udgør grupper af køretøjer eller tog, og flytning af dem.

Disse sidespor kan være (men er ikke begrænset til):

- *infrastruktur, der anvendes til at parkere jernbanekøretøjer, når de ikke er i brug*
- *intermodale terminaler*
- *infrastruktur, der anvendes til service på passagerkøretøjer såsom rengøring eller let vedligeholdelse*
- *infrastruktur, der tilhører og administreres af et vedligeholdelseskædet for jernbanekøretøjer*
- *industriområder eller anlæg, hvor industrielle aktiviteter med lastning/losning af godsvogne finder sted.*

Aktiviteter udført i et sidespor udføres af en "sidesporsoperatør". En sidesporsoperatør kan være en jernbanevirksomhed, en infrastrukturforvalter, en tjenesteudbyder (f.eks. rengøring af passagerkøretøjer), en industriel organisation (f.eks. en kemisk fabrik, som laster/losser tankvogne) eller en underleverandør til denne industrielle organisation. I førstnævnte tilfælde har organisationen truffet den forretningsbeslutning at blive en jernbanevirksomhed eller er en jernbanevirksomhed, der planlægger at håndtere sidespor ud over de nuværende jernbaneaktiviteter. I sidstnævnte tilfælde er infrastrukturforvalteren infrastrukturforvalter for sidesporene eller opererer som en jernbanevirksomhed under dennes sikkerhedsgodkendelse.

"Sidesporsoperatøren" styrer risiciene i forbindelse med sundhed og sikkerhed på arbejdspladsen via sit arbejdsmiljøledelsessystem, som er indført i henhold til international og national lovgivning. Når "sidesporsoperatøren" ikke er en jernbanevirksomhed, omfatter dette ledelsessystem sundheds- og sikkerhedsforpligtelserne i forbindelse med eksterne medarbejdere, navnlig hos jernbanevirksomheder, f.eks. når lokomotivførerne kommer ind på sidesporet. Sideløbende hermed styrer jernbanevirksomheden risiciene i forbindelse med sundhed og sikkerhed på arbejdspladsen via sit arbejdsmiljøledelsessystem i henhold til international og national lovgivning.

Tilfælde 1: Sidesporsoperatøren er jernbanevirksomhed "Y"

Denne jernbanevirksomhed styrer, ved hjælp af sit sikkerhedsledelsessystem, risiciene i forbindelse med jernbanedriften i sin sidesporsinfrastruktur og på jernbanenettet, som hører under en infrastrukturforvalters ansvarsområde. Denne risikostyring omfatter risiciene i forbindelse med skader på køretøjer som følge af alle aktiviteter, der udføres i sidesporet, herunder også oprangering, klargøring og drift af tog.

I praksis er det undertiden svært at bestemme den ansvarlige jernbanevirksomhed. F.eks. ankommer et tog fra jernbanevirksomhed "X" i et sidespor (lokomotivføreren og lokomotivet er hyret), og jernbanevirksomhed "Y", som står for sidesporets drift, overtager det som et nyt tog (lokomotivføreren og lokomotivet er hyret), og i mellemtiden er der sidesporsaktiviteter, som skal udføres. I dette tilfælde gælder de ovenstående sikkerhedsprincipper. Der er fælles grænsefladerisici, som skal tages i betragtning i sikkerhedsledelsessystemet i jernbanevirksomhed "Y" (f.eks. skader på køretøjer som følge af sidesporsaktiviteter som lastning). Desuden skal overførslen af information om køretøjerne fra jernbanevirksomhed "X" til jernbanevirksomhed "Y" også tages i betragtning. Dette omfatter en forsikring om, at køretøjet er i en sikker driftstilstand, når jernbanevirksomhed "X" overfører det til

sidesporsoperatøren, og ligeledes når det videreoverføres via jernbanevirksomhed "Y". Jernbanevirksomhed "Y", som er ansvarlig for sidesporsaktiviteterne, forbliver fuldt ud ansvarlig for risikostyringen i forbindelse med de vedligeholdelsesaktiviteter, der udføres herpå.

Tilfælde 2: Sidesporsoperatøren er ikke en jernbanevirksomhed

Fire undertilfælde kan tages i betragtning:

- **Undertilfælde 2.1**, når sidesporsoperatøren er infrastrukturforvalteren.
- **Undertilfælde 2.2 og 2.3**, når sidesporsoperatøren, som ikke er infrastrukturforvalter, kun udfører aktiviteter på sin egen infrastruktur, men ikke på jernbanenettet, der hører under infrastrukturforvalterens ansvarsområde.
- **Undertilfælde 2.4** omfatter jernbanedrift udført af en sidesporsoperatør, som ikke er infrastrukturforvalter, på jernbanenettet, der hører under infrastrukturforvalterens ansvarsområde.

Undertilfælde 2.1: Når aktiviteter i sidesporene deles mellem en eller flere jernbanevirksomhed(er) og en infrastrukturforvalter (eller en hvilken som helst organisation, der handler på dennes vegne), skal de enkelte jernbanevirksomheder informeres om alle sikkerhedshændelser, der har fundet sted under infrastrukturforvalterens aktiviteter i forbindelse med kontraktlige aftaler. Det omfatter skader samt ulykker og hændelser, der involverer køretøjer.

Disse kontraktlige aftaler styres i de respektive sikkerhedsledelsessystemer for de enkelte jernbanevirksomheder og for infrastrukturforvalteren.

Via sit sikkerhedsledelsessystem styrer jernbanevirksomheden risiciene i forbindelse med sine egne aktiviteter i relation til den modtagne information.

Undertilfælde 2.2: Togenes oprangering og klargøring foretages af jernbanevirksomheden (sammenkobling og klargøring) i sidesporsinfrastrukturen. Jernbanevirksomheden skal informeres om alle (sikkerheds)hændelser, der har fundet sted under sidesporsoperatørens aktiviteter (f.eks. lastning eller rengøring) i forbindelse med kontraktlige aftaler. Det omfatter skader samt ulykker og hændelser, der involverer køretøjer.

Disse kontraktlige aftaler styres i jernbanevirksomhedens sikkerhedsledelsessystem.

Via sit sikkerhedsledelsessystem styrer jernbanevirksomheden risiciene i forbindelse med sine egne efterfølgende aktiviteter i relation til den modtagne information.

Undertilfælde 2.3: Togenes oprangering foretages helt/delvist af sidesporsoperatøren eller af en organisation, der arbejder på vegne af sidesporsoperatøren.

Når et tog er oprangeret, overføres det til en jernbanevirksomhed.

Ligesom i undertilfælde 2.2 skal jernbanevirksomheden informeres om alle hændelser, der har fundet sted under sidesporsoperatørens aktiviteter (f.eks. lastning eller rengøring) og under oprangering i forbindelse med kontraktlige aftaler. Hændelserne omfatter skader samt ulykker og hændelser, der involverer køretøjer.

Disse kontraktlige aftaler styres i jernbanevirksomhedens sikkerhedsledelsessystem.

Via sit sikkerhedsledelsessystem styrer jernbanevirksomheden risiciene i forbindelse med sine egne aktiviteter i relation til den modtagne information.

Undertilfælde 2.4: Dette undertilfælde supplerer undertilfælde 2.3. Derfor vil kun jernbanevirksomhedens yderligere pligter blive nævnt herefter.

Sidesporsoperatøren kører tog eller flytter køretøjsgrupper fra sin jernbaneinfrastruktur og ind på jernbanenettet, som hører under en infrastrukturforvalters ansvarsområde.

Eksempler:

- *Sidesporsoperatøren flytter toget eller køretøjsgrupperne fra en oplagsplads til en passagerstations perroner eller til en parkeringsplads i tilknytning til en passagerstation.*
- *Sidesporsoperatøren flytter toget eller køretøjsgrupperne fra et industrianlæg til et udfletningspunkt (skiftespor) i tilknytning til en godsstation.*

Sidesporsoperatøren er hverken en jernbanevirksomhed eller en infrastrukturforvalter, men de aktiviteter, der udføres på en infrastrukturforvalters net, skal være omfattet af et EU-sikkerhedscertifikat eller en sikkerhedsgodkendelse.

Sidesporsoperatørens jernbanedrift på jernbanenettet, som hører under en infrastrukturforvalters ansvarsområde, skal være omfattet af enten en jernbanevirksomheds EU-sikkerhedscertifikat eller en infrastrukturforvalters sikkerhedsgodkendelse. Det betyder, at jernbanevirksomheden eller infrastrukturforvalteren skal styre risiciene i forbindelse med de aktiviteter, som sidesporsoperatøren udfører i tilknytning til ordningerne for forvaltning af underleverandører, i deres sikkerhedsledelsessystem.

Jernbanevirksomhederne og infrastrukturforvalteren skal under alle omstændigheder nøjagtigt beskrive omfanget af alle deres jernbaneaktiviteter og af de aktiviteter, som berører andre jernbaneaktiviteter, for at gøre de nationale sikkerhedsmyndigheders tilsyn med sikkerhedsledelsessystemet effektivt. Jernbanevirksomhedernes og infrastrukturforvalternes evne til at give en klar og fuldstændig beskrivelse af deres aktiviteter og af andre aktiviteter, der berører jernbanedrift, er afgørende for at sikre, at sikkerhedsledelsessystemet er effektivt, og at de nationale sikkerhedsmyndigheders tilsyn er effektivt.

De kontraktlige aftaler i alle ovenstående undertilfælde skal indeholde en klar angivelse af (men er ikke begrænset til):

- *Det, den enkelte kontraherende part skal gøre.*
- *Den forventede kvalitet af output/tjenesteydelser.*
- *Tildeling af roller og ansvarsområder.*
- *Hvilke oplysninger der skal udveksles, samt hvornår og hvordan de skal udveksles mellem de kontraherende parter. Oplysningerne omfatter indberetning af hændelser som beskrevet i alle undertilfælde ovenfor og de særlige karakteristika ved sidesporsinfrastrukturen såsom hastighedsgrænser, vægtgrænser eller hældningsgrader.*
- *Kompetencekrav.*
- *Arbejdsmiljøskrav (som stammer fra risikovurdering, nationale krav osv.).*

Kontraktlige aftaler og partnerskaber

Jernbanevirksomheden er ansvarlig for at sørge for sikker togdrift ved at koordinere og administrere togdriften. Kontraktlige aftaler (der sædvanligvis består af rammeaftaler, særaftaler og tillæg) udgør grundlaget for et effektivt samarbejde mellem de forskellige jernbanevirksomheder, hvad enten de er nye eller etablerede, og skal overholde bestemmelserne i EU-lovgivningen og national lovgivning samt alle andre gældende krav.

Derfor skal jernbanevirksomheden styre risiciene ved sine aktiviteter, herunder samarbejdet med partnere og brugen af (under)leverandører. Den nationale sikkerhedsmyndighed fører så tilsyn med, at jernbanevirksomheden opfylder sine lovgivningsmæssige forpligtelser på en gennemsigtig og omhyggelig måde.

Jernbanevirksomhederne kan ikke udlicitere deres sikkerhedsansvar for at koordinere og administrere en sikker togdrift. Det betyder dog ikke, at der ikke eksisterer nogen samarbejdsrelation mellem jernbanevirksomhederne. Grundprincipperne ovenfor gælder også for samarbejdet mellem jernbanevirksomhederne. Den jernbanevirksomhed, der er ansvarlig for en sikker togdrift, skal være tydeligt identificeret i alle aftaler mellem de involverede parter og skal være i besiddelse af et EU-sikkerhedscertifikat. Denne jernbanevirksomhed kan enten forvalte ressourcerne (personale og køretøjer) direkte via sit

sikkerhedsledelsessystem, eller den kan vælge (helt eller delvist) at udlicitere brugen af ressourcer (f.eks. leasing af køretøjer eller ansættelse af lokomotivførere) til en anden part. I sidstnævnte tilfælde har jernbanevirksomheden stadig ansvaret for at styre risiciene i forbindelse med brugen af (under)leverandører, idet den via sikkerhedsledelsessystemet overvåger kontraktforholdet i henhold til [forordning \(EU\) 1078/2012](#). Jernbanevirksomheden skal således kontrollere, at disse ressourcer overholder lovkravene og andre gældende sikkerhedskrav (f.eks. køretøjer i sikker driftstilstand, rutekompatibilitet, personaleuddannelse, lokomotivførere med gyldig licens og certifikat til en specifik rute).

Et EU-sikkerhedscertifikat udstedt af et sikkerhedscertificeringsorgan (og genstand for et tilsvarende tilsyn fra en national sikkerhedsmyndigheds side) til den kontraherende part (dvs. partneren eller underleverandøren) kan give den jernbanevirksomhed, der er ansvarlig for sikker drift, en tilstrækkelig forsikring for, at sikkerhedsledelsessystemet opfylder de relevante krav. De kontraktlige aftaler omfatter overførsel af information, der er relevant for sikkerheden (f.eks. tidligere hviletid for lokomotivførerne), mellem de kontraherende parter.

De principper, der ligger til grund for jernbanevirksomhedernes samarbejde, er de samme uanset samarbejdets karakter, dvs. uanset om der er tale om partnerskab eller en (hel eller delvis) udlicitering af jernbaneaktiviteterne i forbindelse med indenlandsk eller grænseoverskridende drift. Karakteren og omfanget af de foranstaltninger, som jernbanevirksomhederne skal gennemføre, og omfanget af den nationale sikkerhedsmyndigheds tilsyn med disse samarbejdsaftaler, står dog i forhold til graden af samarbejde mellem jernbanevirksomhederne.

F.eks. er det sandsynligt, at et grænseoverskridende samarbejde mellem jernbanevirksomhederne (dvs. brugen af eksterne køretøjer og/eller personale) kræver flere kontrolforanstaltninger end andre samarbejdsrelationer, eftersom driften overlades til en anden jernbanevirksomhed med et andet sprog og med driftsregler for rullende materiel, der kan være forskellige fra den ene medlemsstat til den anden. Derimod ville anvendelse af eksterne lokomotivførere eller køretøjer naturligvis kræve mindre overvågning og dermed færre tilsynsaktiviteter fra den nationale sikkerhedsmyndigheds side.

Bilag 4 — Sikkerhedskultur

Introduktion til sikkerhedskultur og en strategi for forbedring af sikkerhedskulturen

Kultur opstår som følge af spillet mellem mennesker i deres dagligdag og bidrager til at definere adfærdsforventninger og samfundsnormer. Kultur er et komplekst begreb, der omfatter en lang række faktorer, som udvikler sig med tiden alt afhængigt af omstændighederne, miljøet og erfaringerne i en nation, en stat, et samfund og/eller en organisation.

Sikkerhedskulturen er de elementer i kulturen, der specifikt drejer sig om sikkerhed. Selv om det er muligt at give en beskrivelse af nogle af de elementer, der bidrager til en sikkerhedskultur, er det umuligt at samle alle de oplysninger, som udgør sikkerhedskulturen. Der eksisterer ikke nogen fælles videnskabelig, objektiv målemetode for sikkerhedskulturen. Dette skyldes, at de bidragende faktorer varierer, ikke blot mellem organisationerne, men også inden for den enkelte organisation. Forskellige afdelinger har forskellige sikkerhedskrav og -behov, f.eks. driftsmæssige og finansielle krav og behov, og den fremherskende sikkerhedskultur vil udvikle sig ud fra disse. Eksterne faktorer såsom lovkrav, uddannelsesniveau, samfundsstrukturer og den nationale kultur bidrager også til en organisations sikkerhedskultur.

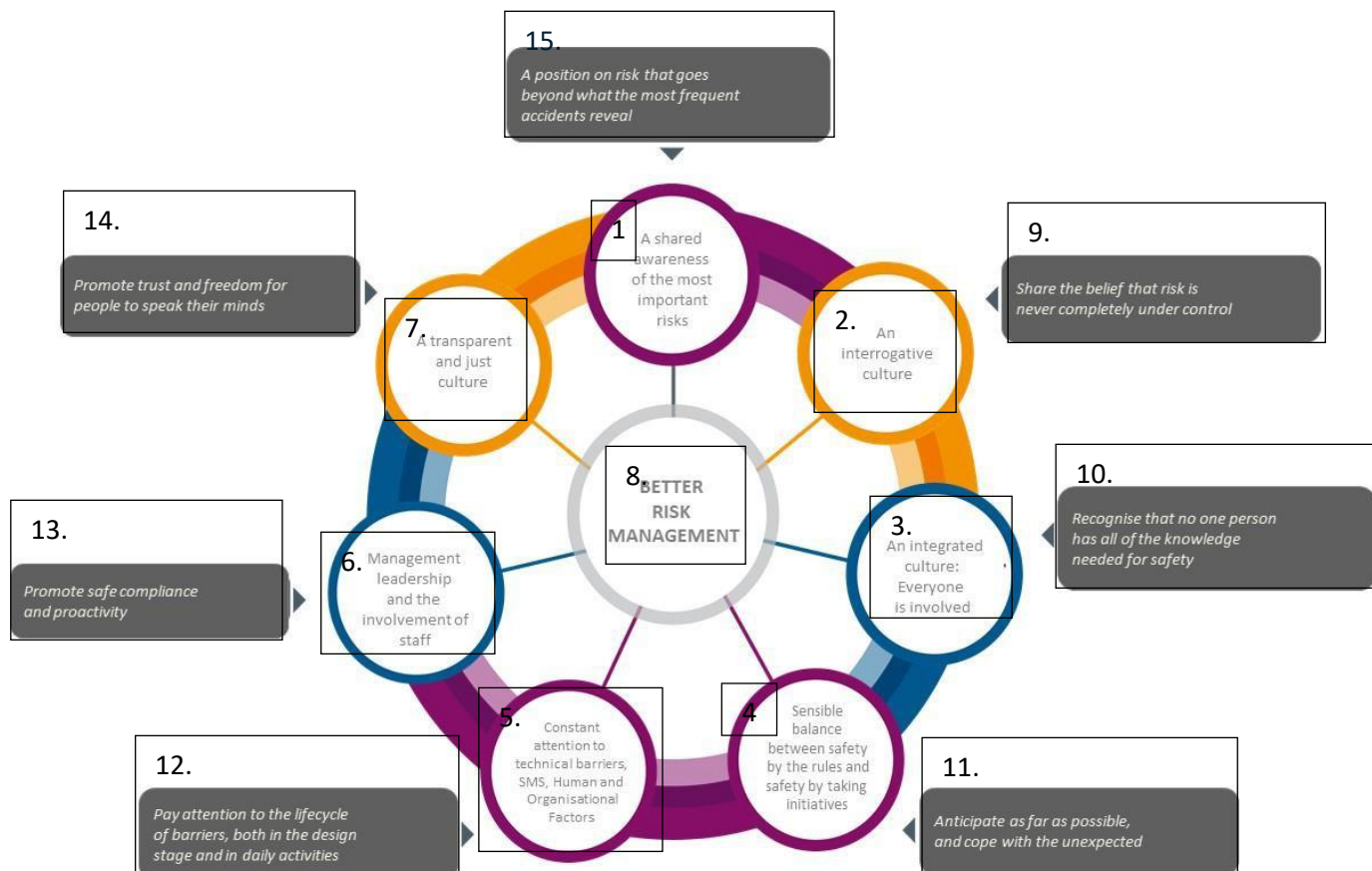
Sikkerhedskultur er et etableret begreb. Det mangler dog en fælles definition. Den manglende definition har betydet, at den teoretiske diskussion og den praktiske anvendelse i en vis grad har fjernet sig fra hinanden, og det, der i bund og grund er en social konstruktion, er blevet gjort til kendetegn på en god sikkerhedskultur.

Når det er sagt, er en simpel måde at beskrive sikkerhedskulturen på at se på de faktorer, der bidrager til adfærden. Sikkerhedsledelsessystemet udgør grundlaget, da det fastlægger og foreskriver kravene ved hjælp af politikker og procedurer. I den ideelle verden er sikkerhedsledelsessystemet perfekt, og hele ledelsen og personalet overholder det. Desværre ser virkeligheden anderledes ud. Der sker nemlig det, at ledelsen og personalet forsøger at finde en mening med sikkerhedsledelsessystemets indhold ud fra deres værdier, holdninger og overbevisninger, som stammer fra den personlige erfaring kombineret med arbejdspladsens og samfundets adfærdsnormer. Hvis sikkerhedsledelsessystemet giver mening, og der er en overholdelseskultur, vil den korrekte adfærd følge efter. Hvis ikke, vil der blive foretaget personlige fortolkninger og anvendt alternative løsninger. De vil være baseret på en individuel risikovurdering med en opvejning af faktorer, som har indflydelse på de beslutninger, der bliver truffet. Risikovurderingen vil ikke blot fokusere på den reelle risiko, men også medtage faktorer, der vedrører bekvemmelighed, risikoen for at blive opdaget, ledelsens ord og handlinger osv. Sammenhængen mellem sikkerhedsledelsessystemet, hvorvidt det giver mening og personernes adfærd definerer således sikkerhedskulturen.

Hvis man vil måle sikkerhedskulturen, kræver det indsigt i de tre faktorer og deres indbyrdes sammenhæng. Som nævnt tidligere eksisterer der ikke nogen fælles videnskabelig, objektiv målemetode for sikkerhedskulturen. I stedet kan de karakteristika, der har indflydelse på sikkerhedskulturen, analyseres i lyset af de tre faktorer.

F.eks. kan en politikerklæring som "Sikkerheden først" blive fulgt op af en undersøgelse af, hvad det betyder for medarbejderne — tror de rent faktisk på det, gør ledelsen det, den siger, hvordan bliver beslutningerne truffet og på hvilket grundlag, hvordan reagerer organisationen under pres osv. Der kan foretages lignende undersøgelser af andre faktorer såsom efteruddannelse og en spørgende holdning. At kombinere analyseresultaterne vil give et billede af kulturens aktuelle tilstand. Med tiden kan der sammensættes et mere omfattende billede, som muliggør nogle vægtigere konklusioner.

For at forstå sikkerhedskulturen i en organisation har specialister og forskere udviklet modeller, der sædvanligvis indebærer en række egenskaber ved en positiv sikkerhedskultur. [Figur 4](#) er et eksempel på en sådan model, der er baseret på nyere arbejde i ICSI (Institute for an Industrial Safety Culture)



Figur 4: Egenskaber ved en sikkerhedskultur

- | | | |
|----|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| 1 | A shared awareness of the most important risks | En fælles bevidsthed om de vigtigste risici |
| 2 | An interrogative culture | En interrogativ kultur |
| 3 | An integrated culture: everyone is involved | En integreret kultur (alle er inddraget) |
| 4 | Sensible balance between safety by the rules and safety by taking initiatives | Fornuftig balance mellem sikkerhed efter reglerne og sikkerhed ved at tage initiativer |
| 5 | Constant attention to technical barriers, SMS, human and organisational factors | Konstant opmærksomhed på tekniske barrierer, sikkerhedsledelsessystemet, menneskelige og organisatoriske faktorer |
| 6 | Management leadership and the involvement of staff | Ledelse, lederskab og inddragelse af personalet |
| 7 | A transparent and just culture | En gennemsigtig og åben rapporteringskultur |
| 8 | Better risk management | Bedre risikostyring |
| 9 | Share the belief that risk is never completely under control | Dele overbevisningen om, at risiko aldrig er fuldstændig under kontrol |
| 10 | Recognise that no one person has all of the knowledge needed for safety | Erkende, at ingen ved alt i forbindelse med sikkerhed |
| 11 | Anticipate as far as possible, and cope with the unexpected | Imødesee mest muligt, og håndtere det uventede |
| 12 | Pay attention to the lifecycle of barriers, both in the design stage and in daily activities | Være opmærksom på livscyklussen for hindringer, både under udformningen og i de daglige aktiviteter |

13	Promote safe compliance and proactivity	Sørge for at fremme sikker overensstemmelse og proaktivitet
14	Promote trust and freedom for people to speak their minds	Sørge for at fremme tilliden og andres frihed til at sige deres mening
15	A position on risk that goes beyond what the most frequent accidents reveal	En holdning til risiko, der ligger ud over, hvad de hyppigste ulykker afslører

På baggrund af ICSI-modellen kan der findes en sammenhæng mellem de fleste af elementerne i sikkerhedsledelsessystemer og de fremherskende egenskaber ved en sikkerhedskultur, sådan som det er vist i Tabel 6.

Tabel 6: Forbindelserne mellem krav til sikkerhedsledelsessystemer og egenskaberne ved en sikkerhedskultur

<i>Elementer i sikkerhedsledelsessystemer</i>	<i>CSM SMS</i>	<i>Egenskaber ved en sikkerhedskultur</i>
Lederskab og engagement	2.1	<ul style="list-style-type: none"> • Spørgende kultur • Gennemsigtig og åben rapporteringskultur • Ledelse, lederskab og inddragelse af personale
Sikkerhedspolitik	2.2	Ledelse, lederskab og inddragelse af personale
Struktur og ansvarsområder	2.3	Integreret kultur (alle er inddraget)
Inddragelse af personale og andre parter	2.4	<ul style="list-style-type: none"> • Gennemsigtig og åben rapporteringskultur • Integreret kultur (alle er inddraget) • Ledelse, lederskab og inddragelse af personale
Risikovurdering	3.1	<ul style="list-style-type: none"> • Fælles bevidsthed om de vigtigste risici • Konstant opmærksomhed på tekniske barrierer, sikkerhedsledelsessystemet, menneskelige og organisatoriske faktorer • Fornuftig balance mellem sikkerhed efter reglerne og sikkerhed ved at tage initiativer
Sikkerhedsmålsætninger og -planlægning	3.2	-
Ressourcer	4.1	Integreret kultur (alle er inddraget)

<i>Elementer i sikkerhedsledelsessystemer</i>	<i>CSM SMS</i>	<i>Egenskaber ved en sikkerhedskultur</i>
Kompetence	4.2	<ul style="list-style-type: none"> • Gennemsigtig og åben rapporteringskultur • Integreret kultur (alle er inddraget)
Bevidsthed	4.3	Fælles bevidsthed om de vigtigste risici
Oplysning og kommunikation	4.4	Gennemsigtig og åben rapporteringskultur
Dokumenterede oplysninger/dokumentation for sikkerhedsledelsessystem	4.5	Konstant opmærksomhed på tekniske barrierer, sikkerhedsledelsessystemet, menneskelige og organisatoriske faktorer
Integration af menneskelige og organisatoriske faktorer	4.6	-
Driftsaktiviteter	5.1	<ul style="list-style-type: none"> • Fælles bevidsthed om de vigtigste risici • Spørgende kultur • Fornuftig balance mellem sikkerhed efter reglerne og sikkerhed ved at tage initiativer
Forvaltning af aktiver	5.2	Fælles bevidsthed om de vigtigste risici
Kontrahenter, partnere og leverandører	5.3	<ul style="list-style-type: none"> • Gennemsigtig og åben rapporteringskultur • Integreret kultur (alle er inddraget)
Forvaltning af ændringer	5.4	-
Håndtering af nødsituationer	5.5	Fornuftig balance mellem sikkerhed efter reglerne og sikkerhed ved at tage initiativer
Overvågning	6.1	Spørgende kultur
Intern revision	6.2	-
Ledelsens evaluering	6.3	-
Forbedring/erfaringsopsamling fra ulykker og hændelser	7.1	<ul style="list-style-type: none"> • Spørgende kultur • Gennemsigtig og åben rapporteringskultur
Løbende forbedringer	7.2	<ul style="list-style-type: none"> • Spørgende kultur • Gennemsigtig og åben rapporteringskultur

Yderligere oplysninger om ICSI-modellen findes på webstedet (<http://www.icsi.eu.org>).

Et eksempel på en strategi for forbedring af jernbanesikkerhedskulturen i en stor virksomhed: PRISME-programmet implementeret i SNCF (Frankrig)

Efter en række alvorlige jernbaneulykker og på hinanden følgende arbejdsulykker gennemførte SNCF i 2014 en storskalaundersøgelse, sponsoreret af den administrerende direktør, med det formål at forstå, hvordan personalet opfattede sikkerhed.

"Spørgeskemaet blev udviklet efter samråd med 20 fokusgrupper mellem april og maj 2014. Alle aktiviteter og alle hierarkiske niveauer blev taget i betragtning. For at sikre fortroligheden blev undersøgelsesarbejdet udført af et uafhængigt institut. Undersøgelsen overholdt standarden ISO 20252 og blev foretaget ved hjælp af CAWI-metoden (computer assistance for web interview), som er tilgængelig på private computere, smartphones, tablets."

"Fokusgrupperne leverede særdeles brugbare oplysninger. Navnlig behovet for at forenkle dokumentationen blev identificeret via fokusgrupperne."

Initiativet var en succes, idet mere end 53.000 medarbejdere ud af ca. 150.000 besvarede spørgeskemaet. Undersøgelsen resulterede i en forholdsvis konsensuspræget diagnose, der understregede behovet for at fremme dialog og rapportering fra alle medarbejdere. En dyb kulturel forandring, der understøtter proaktive holdninger på alle niveauer i virksomheden, snarere end en reaktiv tilgang til individuelle begivenheder, blev identificeret som en nødvendig drivkraft for løbende at forbedre sikkerheden.

På den baggrund forpligtede den øverste ledelse sig til at implementere en **generel sikkerhedspolitik for virksomheden**, der sigter mod at nå det højeste sikkerhedsniveau og hvori det fastslås, at sikkerheden ligger øverst på listen over virksomhedens værdier og er et uundværligt middel til at opnå et meget højt indsatsniveau.

På grundlag af undersøgelsen og yderligere benchmarking udarbejdede en arbejdsgruppe på bestyrelsesniveau en ambitiøs handlingsplan, PRISME, der består af seks elementer. En undersøgelse fra november 2015 viste, at disse elementer anerkendes som "vigtige" og "meget vigtige" af 93 % af personalet.

Elementerne er følgende:

- *Udvikle en proaktiv ("Proactive") adfærd: for at lære af fejl og problemer*
- *Udvikle et system baseret på risikoanalyse ("Risk"): for at forudse, identificere og prioritere handlinger*
- *Kontrollere interfaces ("Interfaces"): for at bekæmpe silotænkning og blive bedre til at samarbejde*
- *Forenkle ("Simplify") processerne, dokumentationen og driftstilstande: for at tilpasse dem til virkeligheden på arbejdspladsen med henblik på større effektivitet*
- *Skabe et ledelsesmæssigt ("Managerial") godt arbejdsmiljø, så alle er personligt involveret: for at mindske risikoen for ulykker til det lavest mulige niveau*
- *Erhverve redskaber og innovativt udstyr ("Equipment"): for at sikre moderne arbejdsmetoder for alle, et sikkert miljø og et sikkert netværk for alle.*

Følgende konkrete tiltag er blevet implementeret i PRISME:

- *1-dags undervisning i menneskelige og organisatoriske faktorer for 8 000 ledere*
- *Udvikling og fremme af en retfærdig og åben rapporteringskultur*
- *Styrkelse af kommunikations- og formidlingsredskaber ("2 mois Sécurité" (2-måneders sikkerhed), indikatorer, sikkerheds-flash)*
- *Revision af sikkerhedsledelsessystem og sikkerhedsregler*
- *Forbedring af risikoanalyse for bedre at kunne tage systemiske aspekter i betragtning.*

Programmets effektivitet vurderes i øjeblikket, men en række fordele er allerede blevet identificeret:

- *Forbedret kvalitet af undersøgelser af hændelser under hensyntagen til organisatoriske faktorer*
- *Forbedret spontan indberetning af nærvæd-fejl og problemer fra personalets side*
- *Forbedret kommunikation.*

Ledelsesadfærd opfattes af personalet som værende mere understøttende og proaktiv.

Bilag 5 — Menneskelige og organisatoriske faktorer

Introduktion til menneskelige og organisatoriske faktorer

Menneskelige og organisatoriske faktorer er et tværfagligt område, hvor der fokuseres på, hvordan man øger sikkerheden, styrker indsatsen og øger brugertilfredsheden. Menneskelige og organisatoriske faktorer er en brugercentreret tilgang, dvs. designet bygger på en udtrykkelig forståelse af brugere, opgaver og miljøer. Udgangspunktet er altid brugerens færdigheder og begrænsninger, og hvordan disse påvirkes af og interagerer med de systemer, man møder under opgavens udførelse. Målet er at identificere, hvordan opgaven bedst kan udføres på en sikker og effektiv måde. Der er lagt vægt på brugbarhed. Menneskelige og organisatoriske faktorer anvendes både som en proaktiv måde at sikre gode designprocesser på og som en reaktiv måde at identificere de vigtigste problemer på, når noget er gået galt.

Når der f.eks. skal designes nye køretøjer, er det ikke nok bare at anvende designstandarderne. Lokomotivførerne, togførerne og vedligeholdelsespersonalet bør inddrages, så de kan byde ind med deres erfaring og forståelse af, hvordan opgaverne udføres sikkert og effektivt. Der kan f.eks. være tale om specifikke stations- eller linjespørgsmål, tilgængelighed og adgang for vedligeholdelsespersonalet, opgaveprioriteringer i førerhuset, kommunikationskrav eller passageradfærd på stationerne.

Den bedste måde at tage de forskellige aktørers viden og erfaring i betragtning på er gennem en iterativ proces, hvor brugeren løbende evaluerer togets design og udvikling, efterhånden som det skrider frem. Dette hjælper med at forebygge en almindelig fejl i designprocessen, nemlig at fokusere på menneskets samspil med de enkelte systemer i stedet for opgaveudførelsen generelt. F.eks. har forskellige leverandører forskellige opfattelser af, hvordan alarmer skal prioriteres, og uden et holistisk perspektiv ender brugeren ofte med at få alt for mange informationer, som er af begrænset relevans for opgavens udførelse. Selv om det tekniske design giver mulighed for at vise informationerne, er det ikke sikkert, at brugeren har brug for dem. En analyse af menneskelige og organisatoriske faktorer hjælper med at skelne mellem det, der er nødvendigt at vide ("need to know"), og det, der er rart at have ("nice to have").

Med de menneskelige og organisatoriske faktorer får man et systemisk perspektiv, dvs. at man ikke bare kigger på de menneskelige, teknologiske og organisatoriske faktorer i sig selv, men også lægger vægt på samspillet mellem de forskellige faktorer. Hvis en lokomotivfører f.eks. har været involveret i en hændelse såsom forbikørsel af et stopsignal ved passering af et farepunkt er de foreslåede faktorer, der skal undersøges (listen er ikke udtømmende), relateret til træthed, kognitiv overbelastning, kompetence osv. (menneskelige faktorer), teknologiens indflydelse på indsatsen, f.eks. grænseflader mellem menneske og system, udformning, signalplacering (teknologiske faktorer), organisationens indflydelse på indsatsen, f.eks. uddannelse, sikkerhedsledelsessystem, organisatoriske prioriteringer (organisatoriske faktorer) såvel som samspillet mellem de tre områder, f.eks. indkøbets indflydelse på design eller håndtering af ændringer med indførelsen af nyt design.

Metoderne stammer fra mange forskellige områder, f.eks. eksperimentel psykologi, industriel produktionsteknik, organisationspsykologi, sociologi, managementvidenskab, kognitive teknikker, ergonomi, computervidenskab og sikkerhedsteknik. Eftersom der i menneskelige og organisatoriske faktorer er fokus på brugeren, er opgaveanalyse en almindeligt anvendt metode. Opgaveanalyse giver designeren forståelse af de opgaver, der skal udføres, og hvordan disse opgaver hænger sammen med de systemer, som brugeren interagerer med, og de organisatoriske forhold, der har indflydelse på indsatsen. Ud fra opgaveanalysen kan der foretages yderligere analyse såsom interaktionen mellem menneske og system, arbejdsbyrde, menneskelig pålidelighed/risiko, antropometri og biometrisk analyse. Det vigtige er at sikre, at brugeren har den bedst mulige arbejdsituation med henblik på en sikker og effektiv indsats.

Følgende referencer giver yderligere information om menneskelige og organisatoriske faktorer:

- 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). *An Introduction to Human Factors Engineering*. New Jersey: Pearson Education. ISBN-13: 978-0131837362

Strategi for at støtte integrationen af menneskelige og organisatoriske faktorer i sikkerhedsledelsessystemet

Organisationen skal sørge for en strategi for at sikre, at menneskelige faktorer som viden, metoder og en menneskecentreret tilgang anvendes systematisk og konsekvent på alle relevante processer i organisationen. En sådan tilgang betyder, at man først tager højde for menneskers behov, færdigheder og adfærd, og at man derefter tilrettelægger udformningen således, at disse behov, færdigheder og adfærd imødekommes.

Strategien for de menneskelige og organisatoriske faktorer indeholder elementer, der er forbundet med:

Lederskab

- *Lederskab og forpligtelse*
 - *Ledelsens forpligtelse i forhold til menneskelige og organisatoriske faktorer er klart angivet i politikker og målsætninger*
 - *Der er en proces/retningslinje for, hvordan menneskelige og organisatoriske faktorer skal anvendes i projekter*
 - *Menneskelige og organisatoriske faktorer er en integreret del af designprocessen og projektledelsen.*
- *Sikkerhedspolitik*
 - *I sikkerhedspolitikken skal det klart være angivet, at menneskelige og organisatoriske faktorer skal inddrages i alle sikkerhedsrelaterede processer.*
- *Organisatoriske roller, ansvarsområder, ansvarlighed og bemyndigelser*
 - *Roller, ansvarsområder og ansvarlighed skal være klart defineret for specialisten inden for menneskelige og organisatoriske faktorer*
 - *Der er en proces for, hvordan eksperter inden for menneskelige og organisatoriske faktorer regelmæssigt deltager i projekter og processer.*

Planlægning

- *Tiltag med henblik på at imødegå risici*
 - *En beskrivelse af, hvordan perspektivet for menneskelige og organisatoriske faktorer tages i betragtning i risikoanalyser*
 - *Inddragelse af specialister inden for menneskelige og organisatoriske faktorer i risikoanalyser.*

Støtte

- *Ressourcer og kompetence*
 - *En systematisk tilgang for at sikre, at relevante roller har kompetence inden for menneskelige og organisatoriske faktorer på baggrund af en behovsanalyse*
 - *Der sættes tid og ressourcer af til at sikre, at kravene vedrørende menneskelige og organisatoriske faktorer er opfyldt.*
- *Bevidsthed*
 - *Universel viden i organisationen om den systematiske tilgang for at sikre kompetence inden for menneskelige og organisatoriske faktorer i relevante roller.*

Drift

- *Planlægning og styring af driften*
 - *Menneskelige og organisatoriske faktorer tages i betragtning ved planlægning af driften.*
- *Forvaltning af aktiver*
 - *Organisationen har retningslinjer for anvendelsen af en menneskecentreret tilgang i alle livscyklussens stadier.*
- *Håndtering af ændringer*
 - *Menneskelige og organisatoriske faktorer skal altid vurderes som et led i processen med håndtering af ændringer.*

Præstationsevaluering

- **Overvågning**
 - *Indsatsen på sikkerhedsområdet vurderes systematisk i lyset af strategien for menneskelige og organisatoriske faktorer.*

Forbedring

- **Erfaringsopsamling fra ulykker og hændelser**
 - *Ekspertise og metoder vedrørende menneskelige og organisatoriske faktorer anvendes i undersøgelsesprocessen for ulykker*
 - *Der eksisterer en metode til at foretage undersøgelser baseret på viden om og metoder for menneskelige og organisatoriske faktorer*
 - *Der eksisterer et uddannelsesprogram for undersøgere af ulykker og hændelser, hvor perspektivet for menneskelige og organisatoriske faktorer bliver anvendt.*
- **Løbende forbedring**
 - *En proces for løbende forbedring af organisationens processer til håndtering af menneskelige og organisatoriske faktorer.*

Bilag 6 — Definitioner

Brugen af ord eller termer i hele dokumentet som "skal" eller "bør" angiver, at der eksisterer et lovkrav, som det er nødvendigt at overholde.

Ulykke	En uønsket eller utilsigtet pludselig begivenhed eller en specifik kæde af sådanne begivenheder, der har skadelige følger; ulykker inddeles i følgende kategorier: togsammenstød, afsporinger, ulykker i jernbaneoverkørsler, personulykker forårsaget af rullende materiel i bevægelse, brand og andre ulykker (direktiv (EU) 2016/798).
Driftsområde	Et eller flere net i en eller flere medlemsstater, hvor en jernbanevirksomhed har til hensigt at drive virksomhed (direktiv (EU) 2016/798).
Forvaltning af aktiver	Den tilgang, som en organisation anvender for at sikre, at fysiske aktiver forbliver sikre, formålstjenlige og økonomisk rentable i hele deres livscyklus lige fra deres projektering og konstruktion, og til de tages ud af drift.
Auditering	Systematisk, uafhængig og dokumenteret proces til opnåelse af auditeringsdokumentation og en objektiv evaluering heraf for at bestemme, i hvilket omfang auditeringskriterierne er opfyldt (ISO 9000).
Driftens karakter	Driftens karakteristik i form af anvendelsesområde, herunder infrastrukturens udformning og konstruktion, vedligeholdelse af infrastrukturen, trafikplanlægning, trafikstyring og -kontrol, og anvendelse af jernbaneinfrastrukturen, herunder konventionelle og/eller højhastighedstog, passagerbefordring og/eller godstransport.
Kompetence	Evnen til at anvende viden og færdigheder til at nå de tilsigtede resultater (ISO 9000).
Løbende forbedring	Tilbagevendende aktivitet for at forbedre indsatsen (dvs. et målbart Resultat, præstation) (ISO 9000).
Dokumentstyring	Processen (eller proceduren) med at identificere, oprette, vedligeholde, administrere, lagre og opbevare dokumenteret information.
Driftens omfang	Er i forbindelse med jernbanedrift, der udføres af jernbanevirksomheder, det omfang, der defineres ved antallet af passagerer og/eller omfanget af gods og ved en jernbanevirksomheds anslåede størrelse målt i antal ansatte, der arbejder i jernbanesektoren (dvs. som en mikrovirksomhed eller en lille, mellemstor eller stor virksomhed) (direktiv (EU) 2016/798). Er i forbindelse med jernbanedrift, der udføres af infrastrukturforvaltere, det omfang, som er karakteriseret ved jernbanesporets længde og infrastrukturforvalterens anslåede størrelse målt på antal ansatte, der arbejder i jernbanesektoren (forordning (EU) 2018/762 CSM SMS).
Fare	En situation, der kunne føre til en ulykke (forordning (EU) 402/2013).
Menneskelige og organisatoriske faktorer	Alle de karakteristika vedrørende den menneskelige ydeevne og alle de organisatoriske aspekter, der skal tages i betragtning for at sikre livslang sikkerhed og effektivitet i et system eller en organisation.
Menneskecentreret tilgang	En tilgang, hvor der først tages højde for menneskers behov, færdigheder og adfærd, og hvor man derefter tilrettelægger udformningen således, at disse behov, færdigheder og adfærd imødekommes.

Hændelse	Enhver anden tildragelse end en ulykke eller en alvorlig ulykke, som berører eller kan berøre jernbanedriftens sikkerhed (direktiv (EU) 2016/798). Dette omfatter næved-fejl.
Infrastrukturforvalter	Ethvert organ eller enhver virksomhed, der navnlig er ansvarlig for anlæg, forvaltning og vedligeholdelse af jernbaneinfrastruktur, herunder trafikstyring, togkontrol og signaler; infrastrukturforvalterens funktioner på et net eller en del af et net kan tildeles forskellige organer eller virksomheder (direktiv 2012/34/EU).
Interessent	Person eller organisation, der kan påvirke, påvirkes af eller opfatte sig selv som påvirket af en beslutning eller aktivitet (ISO 9000) i forbindelse med sikkerhedsledelsessystemet.
Undersøgelse	En proces, der gennemføres for at forebygge ulykker og hændelser, og som omfatter indsamling og analyse af oplysninger, dragning af konklusioner, herunder fastlæggelse af årsager, og i givet fald fremsættelse af sikkerhedsrelaterede anbefalinger (direktiv (EU) 2016/798).
Ledelsessystem	En række elementer, som er indbyrdes forbundne eller påvirker hinanden gensidigt, og som en organisation anvender til at fastlægge politikker og målsætninger, samt processerne for at nå disse målsætninger [sæt af indbyrdes forbunden eller samspillende element i en organisation, der anvendes til at fastlægge politikker og mål og processer for at opfylde disse mål] (ISO 9000).
Overvågning	De tiltag, som jernbanevirksomheder, infrastrukturforvaltere eller enheder med ansvar for vedligeholdelsen indfører for at kontrollere, at deres ledelsessystem anvendes korrekt og effektivt (forordning (EU) 1078/2012).
National forskrift	Alle bindende forskrifter, der vedtages i en medlemsstat, uanset hvilket organ der udsteder dem, og som indeholder sikkerhedsmæssige eller tekniske krav, bortset fra krav, der er fastsat af Unionen, eller internationale forskrifter, og som finder anvendelse i den pågældende medlemsstat for jernbanevirksomheder, infrastrukturforvaltere eller tredjeparter (direktiv (EU) 2016/798).
Proces	En række aktiviteter, som er indbyrdes forbundne eller påvirker hinanden gensidigt, og som gør input til output [sæt af indbyrdes forbundne eller samspillende aktiviteter, der anvender input til at levere et tilsigtet resultat] (ISO 9000).
Jernbaneinfrastruktur	De faciliteter, som er nødvendige for, at en jernbane kan fungere, herunder: <ul style="list-style-type: none"> • jernbanespor og hermed forbundne sporstrukturer • tilkørselsveje, signalsystemer, kommunikationssystemer, rullende materiel • styringssystemer, togkontrolsystemer og datastyringssystemer • tavler og skilte • elforsyning og elektriske togdriftssystemer • tilknyttede bygninger, værksteder, depoter og oplagspladser • anlæg, maskiner og udstyr.

Jernbanevirksomhed	<p>En jernbanevirksomhed som defineret i artikel 3, nr. 1), i direktiv 2012/34/EU og enhver anden offentlig eller privat virksomhed, hvis aktivitet består i at levere gods- og/eller persontransportydelser med jernbane, idet den pågældende virksomhed skal stille trækraft til rådighed; dette omfatter også virksomheder, der kun stiller trækraft til rådighed (direktiv (EU) 2016/798).</p> <p>Enhver offentlig eller privat virksomhed, som er godkendt i henhold til dette direktiv, og hvis hovedaktivitet består i at levere gods- og/eller persontransportydelser med jernbane med et krav om, at den pågældende virksomhed stiller trækraft til rådighed; dette omfatter også virksomheder, der kun stiller trækraft til rådighed (direktiv 2012/34/EU).</p>
Risiko	Den hyppighed, hvormed ulykker og hændelser medfører skade (forårsaget af en fare) og denne skades alvorsgrad (forordning (EU) 402/2013).
Risikoanalyse	Systematisk anvendelse af alle tilgængelige oplysninger til at identificere farer og estimere risikoen (forordning (EU) 402/2013).
Risikovurdering	Den samlede proces, som omfatter en risikoanalyse og en risikoevaluering (forordning (EU) 402/2013).
Risikoevaluering	En procedure, der med afsæt i risikoanalysen fastslår, om der er opnået et acceptabelt risikoniveau (forordning (EU) 402/2013).
Risikostyring	Den systematiske anvendelse af politikker, procedurer og praksis med henblik på at analysere og evaluere risici og holde risici under kontrol (forordning (EU) 402/2013).
Sikkerhedskultur	Samspillet mellem kravene i sikkerhedsledelsessystemet, hvordan mennesker får dem til at give mening ud fra deres holdninger, værdier og overbevisning og det, de rent faktisk gør, hvilket kan ses i deres beslutninger og adfærd. En positiv sikkerhedskultur er karakteriseret ved en kollektiv forpligtelse blandt ledere og enkeltpersoner til altid at handle på en sikker måde, især når de konfronteres med konkurrerende mål (forordning (EU) 2018/762 CSM SMS).
Mål	<p>Resultat, der skal opnås.</p> <p>Et sikkerhedsmål skal være specifikt, målbart, opnåeligt, realistisk og tidsbaseret. Den skal også opstilles for relevante funktioner og niveauer i organisationen.</p>
Partner	En kommerciel enhed, som en anden kommerciel enhed har en form for alliance med. Denne forbindelse kan være en kontraktlig, eksklusiv aftale, hvor begge enheder forpligter sig til ikke at indgå alliancer med tredjeparter.
Partnerskab	En samarbejdsrelation, hvor parterne, kaldet partnere, aftaler at samarbejde for at fremme deres fælles interesser.
Sikkerhedsledelsessystem	Den organisation og de systemer og procedurer, en infrastrukturforvalter eller en jernbanevirksomhed etablerer for at opnå en sikker ledelse af sine operationer (direktiv (EU) 2016/798).
Øverste ledelse	Person eller gruppe af personer, som leder og styrer en organisation på højeste niveau (ISO 9000).

Driftstype	Den type, der defineres som persontrafik med eller uden højhastighedstrafik, godstrafik med eller uden transport af farligt gods og rangerydelser alene (direktiv (EU) 2016/798).
------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------