EUROPEAN UNION AGENCY FOR RAILWAYS

For et jernbanesystem som fungerer bedre for samfunnet.

Veileder

Krav til sikkerhetsstyringssystem for sikkerhetssertifisering eller sikkerhetsgodkjenning

	Utarbeidet av	*Bekreftet av*	*Godkjent av*
Navn	S. D'ALBERTANSON C. LAGAIZE DAVOINE A. PATACCHINI	M. SCHITTEKATTE	B. ACCOU
Stilling	Prosjektledere	Teamleder	Enhetsleder
Dato	26/04/2021		
Underskrift			

Dokumenthistorikk

Versjon	*Dato*	*Kommentarer*
1.0	29/6/2018	Endelig versjon for publisering
1.1	10/7/2018	Figur 2 oppdatert, bildetekst lagt til for figur 3.
1.2	04/9/2018	Figur 2 oppdatert
1.3	26/04/2021	Oppdateringer for å gjenspeile endringer i regelverket til ECM-forordningen, for å lage passende koblinger til Agency European Railway Safety Culture Model og ut fra erfaring, samt noen generelle rettelser i teksten.

Det nåværende dokumentet er en veiledning fra Den europeiske unions jernbanebyrå som ikke er juridisk bindende. Den påvirker ikke beslutningsprosessene som forutses av den gjeldende EU-lovgivningen. Videre er en bindende tolkning av EU-loven den eneste kompetansen til EU-domstolen.

0 Innledning

En som søker på et felles sikkerhetssertifikat eller en sikkerhetsgodkjenning skal utvise samsvar med de relevante kravene til sikkerhetsstyringssystemer som er fastsatt i forordning (EU) 2018/762. Til dette formål skal det fremlegges bevis i form av dokumentasjon til den nasjonale sikkerhetsmyndigheten eller, når det er relevant, Den europeiske unions jernbanebyrå (heretter kalt "Byrået"), om at et sikkerhetsstyringssystem (SMS) er opprettet i samsvar med artikkel 9 i Direktiv (EU) 2016/798.

Denne veilederen er et dokument som oppdateres fortløpende, og som er utarbeidet i samarbeid med nasjonale sikkerhetsmyndigheter og sektorrepresentanter, og er ment å bli forbedret på kontinuerlig basis basert på tilbakemeldinger fra brukere og erfaringer som er gjort under gjennomføringen av Direktiv (EU) 2016/798, relaterte felles sikkerhetsmetoder (CSM) og andre relevante EU-forordninger.

0.1 Formålet med veilederen

Denne veilederen tar sikte på å forklare:

- *Formålet med hvert av vurderingskravene som skissert i vedlegg I og II i ovennevnte CSM, supplert der det er nødvendig med forklarende notater som gir spesifikk informasjon om spesielle begreper eller ideer som anvendes i kravene;*
- *En indikasjon på hvilke bevis en organisasjon kan måtte tilveiebringe for å vise at de samsvarer med kravene ovennevnte CSM;*
- *En illustrerende liste over eksempler på bevis som kan ses i søknader for et felles sikkerhetssertifikat eller sikkerhetsgodkjenning ved gjennomføring av vurdering, eller som kan brukes av søkeren som referansemateriale for søknaden;*
- *Illustrerende referanser og standarder som kan brukes til å vurdere, utvikle, implementere eller forbedre et sikkerhetsstyringssystem på kontinuerlig basis; og*
- *Noen indikasjoner på hvilke problemer som kan måtte bli vurdert av en nasjonal sikkerhetsmyndighet under tilsyn av jernbanevirksomhet eller infrastrukturforvalter.*

Med henblikk på vurderingen av en søknad om et enkelt sikkerhetssertifikat som involverer transport av farlig gods med jernbane, kan en NSA spille en direkte rolle som kompetent myndighet i vurderingen av de relevante delene av søknaden. Alternativt kan den ha en koordinerende rolle som om nødvendig kontakt med enhver annen kompetent myndighet for transport av farlig gods som søker deres råd for de relevante delene av vurderingen etter behov.

0.2 Hvem gjelder denne veilederen for?

Det nåværende dokumentet er rettet mot:

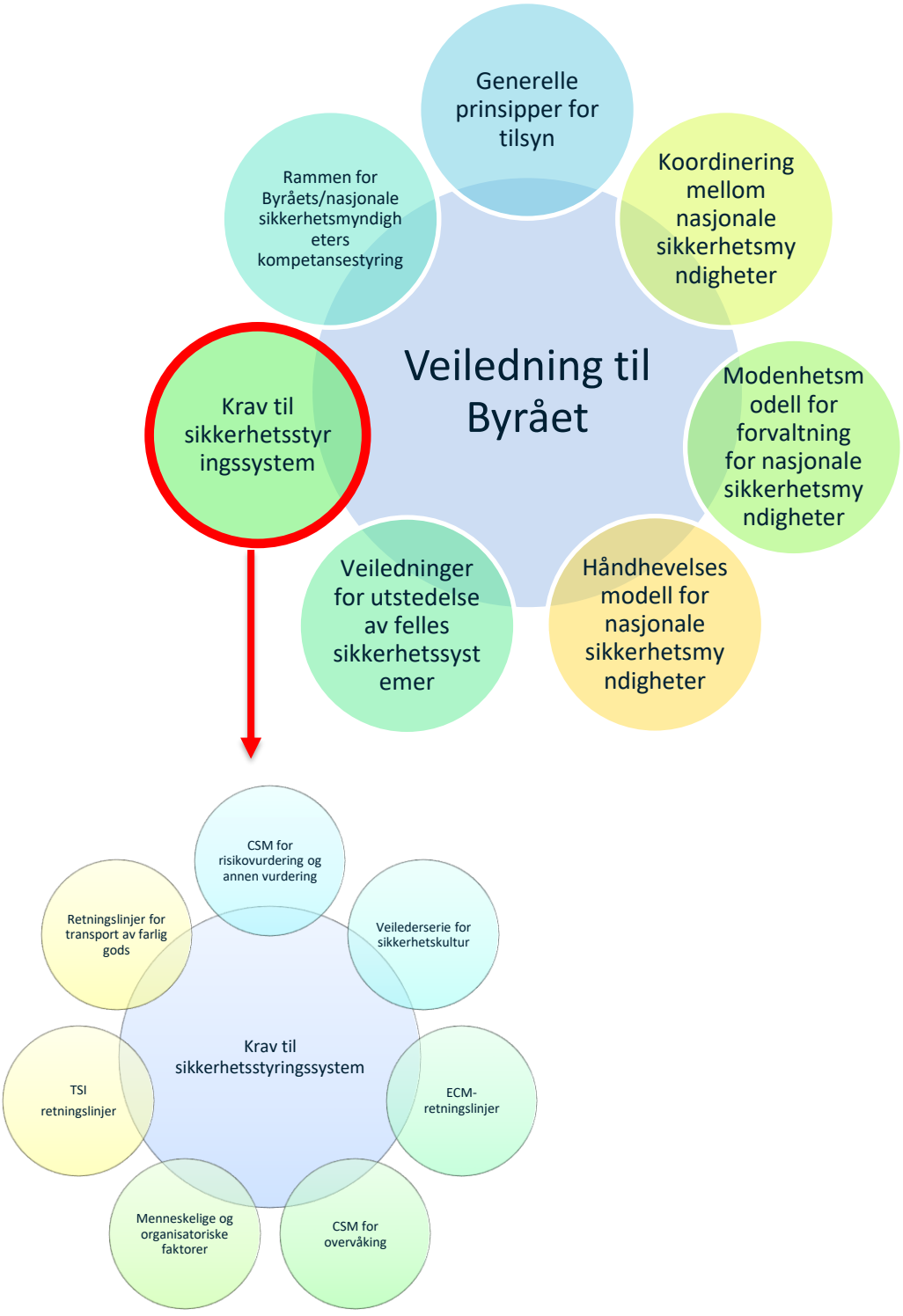
- *Nasjonal sikkerhetsmyndighet og Den europeiske unions jernbanebyrå når de vurderer om jernbanevirksomheters sikkerhetsstyringssystem overholder de relevante SMS-kravene og når de gjennomfører tilsyn;*
- *Nasjonal sikkerhetsmyndighet ved vurderingen av infrastrukturforvalternes sikkerhetsstyringssystem med de relevante SMS-kravene og når de gjennomfører tilsyn etter utstedelse; og*
- *Jernbanevirksomhetene og infrastrukturforvalterne (også kalt "Søker") for å bistå dem med å utvikle, implementere, vedlikeholde og kontinuerlig forbedre sikkerhetsstyringssystemet sitt i samsvar med de relevante SMS-kravene (og andre gjeldende sikkerhetskrav), og for å kjenne til hva som kan forventes under tilsynet.*

0.3 Omfang

Denne veilederen omhandler ikke hvilke bevis som skal fremlegges av søker. Årsaken til dette er at hver enkelt organisasjons SMS skal skreddersys for de spesifikke risikoene som organisasjonen må kontrollere. Således er hver enkelt SMS et unikt system av dokumentert informasjon, som gir en indikasjon på de spesifikke risikostyringstiltakene og -systemene som foreligger i en enkelt organisasjon og som utvikler seg over tid etter hvert som organisasjonen vokser. Det ville derfor bli feil å gi en forhåndsdefinert liste over informasjon som søkeren må oppgi. Dette ville gjøre vurderingsprosessen meningsløs, da alle søknader ville se lik ut, når de korresponderende SMS-punktene ikke er like.

0.4 Struktur i veilederen

Dette dokumentet er en del av byråets kompendium av veiledning som støtter jernbanebyråene, infrastrukturlederne, de nasjonale sikkerhetsmyndighetene og byrået i oppfylling av rollene deres og utførelse av oppgavene deres i henhold til direktiv (EU) 2016/798.



Figur 1: Kompendium av Byråets veiledninger

Informasjonen som i denne veilederen skal suppleres med spesifikk veiledning for nasjonale sikkerhetsmyndigheter, beskrive og forklare meddelte nasjonale regler som gjelder for det tiltenkte driftsområdet, samt dokumentene som skal medsendes søknaden om et felles sikkerhetssertifikat for å overholde bestemmelsene i artikkel 10(3)(b) og artikkel 10(8) i Direktiv (EU) 2016/798 (se også *Byråets søknadsveiledning for utstedelse av felles sikkerhetssertifikater*). For infrastrukturforvaltere bør denne

veilederen suppleres med veiledning laget av nasjonale sikkerhetsmyndigheter om kravene til sikkerhetstillatelser som foreskrevet i artikkel 12(1) i direktiv (EU) 2016/798.

Meddelte nasjonale regler betyr kun de reglene som har blitt meddelt av en medlemsstat til Kommisjonen. I samsvar med redegjørelse nr. 12 i Direktiv (EU) 2016/798, forventes det at antall meddelte nasjonale regler vil komme til å reduseres over tid. Disse vil enten bli erstattet av tiltak som er skissert i Tekniske spesifikasjoner for interoperabilitet (TSI), andre EU-forordninger eller selskapenes regler. Selskapenes regler eller standarder vil bli vurdert som hensiktsmessig gjennom etterlevelse av TSI knyttet til undersystemet for drifts- og trafikkstyring i jernbanenettet i EU (heretter også kalt TSI-OPE), som reflekteres gjennom kravene til sikkerhetsstyringssystemet som er forklart i denne veilederen.

Den foreliggende veiledningen er strukturert i samsvar med kravene i vedlegg I og vedlegg II i forordning (EU) 2018/762. I de følgende kapitlene er hvert av kravene vist i en gul ramme som en enkel referanse. Der det er forskjeller mellom kravene som gjelder for jernbanevirksomheter og kravene som gjelder for infrastrukturforvaltere, vises den relevante teksten for sistnevnte i gule bokser som viser kravene i blått.

Sammenlignings- eller korrelasjonstabeller mellom vurderingskriteriene i tidligere Forordning (EU) 1158/2010 og (EU) 1169/2010, og kravene i Forordning (EU) 2018/762, gis i Vedlegg 1 i denne veilederen. Tabellene inneholder også kryssreferanser til klausulene i ISO High Level Structure hvor det er aktuelt. Disse er tatt med for å hjelpe søkerne til å vise at sikkerhetsstyringssystemene deres samsvarer med de nye kravene, særlig i tilfeller der søkeren allerede har fått et sikkerhetssertifikat eller sikkerhetsgodkjenning og/eller der søkeren allerede anvender et annet ISO-styringssystem (f.eks. ISO 9001, 14001 eller 45001) (slik at de kan integreres sammen), eller har planer om å utvikle et system ved hjelp av denne modellen. Bruk av denne tabellen gir ingen systematisk forutsetning om samsvar med kravene fastsatt i Forordning (EU) 2018/762 for de organisasjonene som har et ISO-sertifikat.

0.5 ISO/IEC-direktiver del 1 og konsolidert ISO-tillegg

ISO har utviklet offisielle prosedyrer som skal følges når man utvikler og opprettholder en internasjonal standard. I vedlegg SL, tillegg 2 i ISO/IEC-direktivene del 1 og konsolidert ISO-tillegg er det innlemmet en høynivåstruktur (HLS) for bruk av kjernetekst i hver enkelt styringssystemstandard.

Vedlegg I og Vedlegg II i Forordning (EU) 2018/762 legger til rette for en struktur som er i samsvar med ISO HLS, forenkling av integrering av ulike styringssystemer der det måtte være aktuelt, som deler de samme organisatoriske kjerneprinsippene og kravene, men der lovformelig samsvar og risikoområder er spesifikke for hver kategori (f.eks. sikkerhet på arbeidsplassen, miljø, kvalitet).

ISO-standardene og relevant veiledning kan hjelpe jernbanevirksomheter og infrastrukturforvaltere til å utvikle sine egne sikkerhetsstyringssystemer (ISO 31000 er f.eks. et generelt dokument for bedre forståelse av risikostyring, ISO 31010 inneholder informasjon om valg og anvendelse av risikovurderingsteknikker som FMECA, FTA, ETA, HAZOP, og ISO 55000 inneholder krav til aktivaforvaltning). Disse er imidlertid bare til hjelp hvis man innehar gode kunnskaper om konteksten i jernbanerelaterte risikoer.

Hvis anvendelsen av høynivåstruktur sikrer et konsistent samsvar med standardene for ISO-styringssystemer, må det understrekes at ovennevnte felles sikkerhetsmetoder er forskrifter som primært tjener formålet med nasjonale sikkerhetsmyndigheter eller Byrået, ved vurdering av søknader om tildeling av sikkerhetssertifikater eller sikkerhetsgodkjenninger. Som sådan vil vurderinger for felles sikkerhetssertifikater eller sikkerhetsgodkjenninger gå imot SMS-kravene og ikke ISO HLS i seg selv. ISO-standardene er med andre ord basert på frivillig sertifisering, men enkelte juridiske rammeverk åpner for muligheten til å anta at de er i overensstemmelse med gjeldende regler som gjelder for et bestemt fagområde. Det foreligger ingen bestemmelser som automatisk gir ISO-standardene samsvar med kravene i Direktiv (EU) 2016/798 eller med Forordning (EU) 2018/762.

Klausul 4 til 10.2 som er hentet fra ISO/IEC-direktiver del 1 og konsolidert tillegg 2016, Vedlegg SL, Tillegg 2, er gjengitt eller tilpasset med tillatelse fra Den internasjonale standardiseringskomiteen (ISO). Vennligst se kildedokumentet for den originale teksten. Dette dokumentet kan lastes ned fra nettstedet til ISO Central Secretariat. Opphavsretten forblir hos ISO.

0.6 Formålet med sikkerhetsstyringssystemet

Formålet med sikkerhetsstyringssystemet er å sikre at organisasjonen styrer risikoene som oppstår som en konsekvens av forretningsmål på en trygg måte, samtidig som den overholder alle sikkerhetsforpliktelsene som gjelder for den.

Vedtaket om en strukturert tilnærming muliggjør at farer kan identifiseres, samt kontinuerlig risikostyring knyttet til organisasjonens egne aktiviteter, med sikte på å forebygge ulykker. Denne tilnærmingen tar i betraktning den felles risikoen ved samhandling med andre aktører i jernbanesystemet (hovedsakelig jernbanevirksomheter, infrastrukturforvaltere og foretak med ansvar for vedlikehold, men også andre aktører som har potensiell innvirkning på sikker drift av jernbanesystemet, som f.eks. produsenter, vedlikeholdsleverandører, brukere, tjenesteleverandører, entreprenører, transportører, avsendere, mottakere, laste-/losseoperatører, opplæringssentre i tillegg til passasjerer og andre som samhandler med jernbanesystemet osv.). Grundig implementering av alle relevante elementer i et sikkerhetsstyringssystem kan gi en organisasjon den nødvendige tilliten til at den kontrollerer, og vil fortsette å kontrollere, alle risikoene som er forbundet med virksomheten den driver, og under alle forhold.

Organisasjoner med erfaring innser at en effektiv risikostyring kun kan oppnås gjennom en prosess som bringer sammen tre kritiske komponenter: En teknisk komponent med bruk av verktøy og utstyr, en menneskelig komponent bestående av førstelinjepersonell og deres ferdigheter, opplæring og motivasjon, samt en organisatorisk komponent bestående av prosedyrer og metoder som definerer oppgaveforholdet.

Følgelig vil et godt sikkerhetsstyringssystem lykkes i å overvåke og forbedre alle de tre komponentene med sine risikostyringstiltak. Mange funksjoner i sikkerhetsstyringssystemene for jernbanedriften er svært like styringspraksisen som fremmes av pådrivere for kvalitet, helse og sikkerhet på arbeidsplassen, samt miljøvern og god næringslivspraksis. Således kan prinsippene for god styring enklere integreres som beskrevet ovenfor ved bruk av felles sikkerhetsmetoder som er basert på ISO HLS, og som derfor kanskje ikke krever en fullstendig restrukturering av organisasjoner som allerede har disse systemene på plass.

Det har blitt bragt på det rene at strukturerte styringssystemer gir verdiskaping til virksomheten gjennom effektiv styring av samhandling. Dette bidrar til å forbedre den generelle ytelsen, innføre effektivitet i driften, forbedre relasjoner med leverandører og underleverandører, kunder og myndigheter, samt bidra til å bygge en positiv sikkerhetskultur.

En søker må utforme sikkerhetsstyringssystemet slik at det møter kravene i artikkel 9 i Direktiv (EU) 2016/798, for å sikre en sikker ledelse av virksomheten sin. Til dette formål må den vise samsvar med kravene i vedlegg I og II i Forordning (EU) 2018/762. Disse kravene er utarbeidet for å danne et komplett bilde av organisasjonens sikkerhetsstyringssystem der man følger PDCA-hjulet: Plan (planlegg), do (utfør), check (kontroller/sjekk), act (korriger). Søkeren må vurdere hvert enkelt av kravene, samt hvordan de passer sammen for å danne et sammenhengende sikkerhetsstyringssystem som kontrollerer de relevante risikoene.

0.7 Sikkerhetsstyringssystem og prosesstilnærming

Et sikkerhetsstyringssystem er et middel til å trekke sammen de ulike trådene som må samles for å kunne drive en trygg og vellykket organisasjon. Disse elementene vil omfatte mekanismene som er på plass for å overholde internasjonale og nasjonale forskrifter og standarder, krav på sektor- og forretningsnivå, resultatene av risikovurderinger og god praksis på tvers av selskapets aktiviteter. Derfor bør

sikkerhetsstyringssystemet integreres i organisasjonens forretningsprosesser, og skal ikke bare være et papirbasert system som er spesielt utviklet for å bevise samsvar med lovgivende rammeverk. Sikkerhetsstyringssystemet bør være et dynamisk sett av ordninger som er i stadig utvikling på lik linje som organisasjonen utvikler seg. Å konstruere et sikkerhetsstyringssystem krever at en organisasjon forstår risikoene den må styre, det juridiske rammeverket den opererer i og har en klar idé om hvordan «god» ytelse ser ut. Denne veilederen angir elementene i et sikkerhetsstyringssystem som må oppfylles for at vurderingsmyndigheten skal kunne utstede ett enkelt sikkerhetssertifikat. Det bør imidlertid tas med i betraktning at kvaliteten på sikkerhetsstyringssystemet går utover summen av delene. Sikkerhetsstyringssystemet skal også fungere som en sammenhengende helhet hvor overholdelse av hver del bidrar til å sikre at hele systemet fungerer korrekt.

Kravene som ligger til grunn for vurderingen av et sikkerhetsstyringssystem kan oppfylles gjennom en dokumentert prosess (eller prosedyre, etc.), men det skal også integreres i og på tvers av organisasjonens ulike forretningsområder. Nasjonale sikkerhetsmyndigheter kan for eksempel sjekke at det foreligger en policyerklæring, men de må også kontrollere organisasjonens forpliktelse til å søke om det. En praktisk måte å gjøre dette på, er at nasjonale sikkerhetsmyndigheter kan kontrollere hvordan sikkerhetsstyringssystemet blir overvåket og vurdert på toppledelsesnivå, hvordan personalet er involvert i dette og hvordan resultatene formidles til dem. På samme måte har organisasjonen kanskje ikke bestemte prosedyrer for å håndtere sikkerhetsrelevant informasjon, men den må beskrive hvordan de relevante delene i virksomheten håndterer den på en egnet måte (f.eks. kommunikasjon av sikkerhetsrelevant informasjon til lokomotivfører).

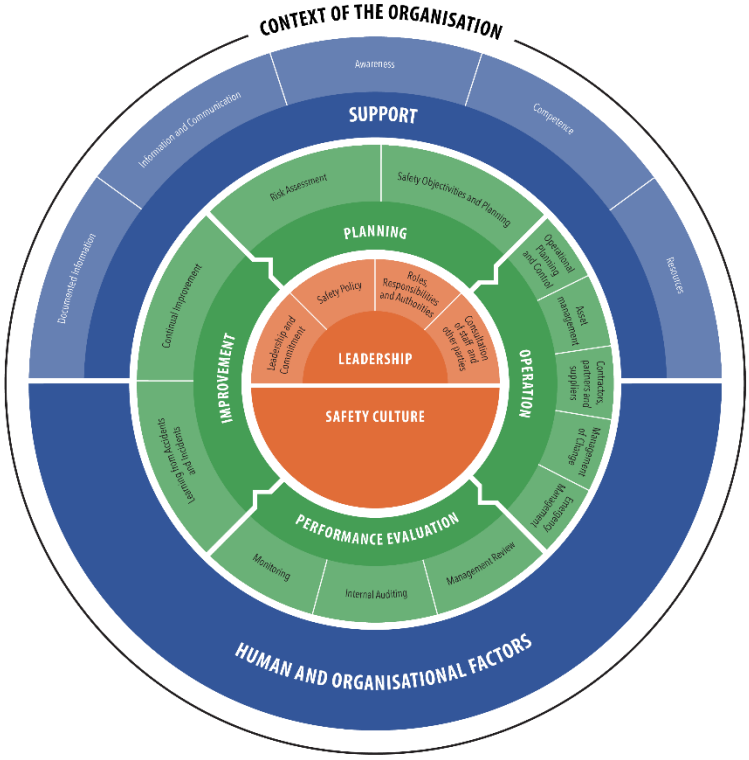
En viktig utvikling vedlegg I og vedlegg II i forordning (EU) 2018/762 er innføringen av en prosesstilnærming. Dette fremmes også i ISO-standarder for styringssystemer, der de ulike prosessene i styringssystemet er nært sammenknyttet, og konsekvent anvendelse bidrar til å oppnå organisasjonens mål. Vedlegg I og Vedlegg II i Forordning (EU) 2018/762 tar for seg noen viktige koblinger mellom prosesser for å legge til rette for forståelsen av prosesstilnærmingen, men dette betyr ikke at bare disse koblingene eksisterer eller at de skal anvendes for samsvarsformål. En organisasjons evner har til å vise hvordan prosessene i styringssystemet er knyttet sammen, er en god indikator på forståelsen av hvordan styringssystemet fungerer på en effektiv måte.

Sjekk elementene i sikkerhetsstyringssystemet for å anvende PDCA-hjulet: Plan (planlegg), do (utfør), check (kontroller/sjekk), act (korriger) (se Figur 2). PDCA-konseptet gjenspeiler de funksjonelle relasjonene mellom de viktigste elementene i sikkerhetsstyringssystemet:

- ***Planlegging**: Identifisere risikoer og muligheter, fastsette sikkerhetsmessige målsettinger og identifisere prosesser og tiltak som er nødvendige for å levere resultater i samsvar med organisasjonens sikkerhetspolicy;*
- ***Drift**: Utvikle, implementere og anvende prosesser og tiltak som planlagt;*
- ***Ytelsesevaluering**: Overvåke og evaluere den reelle ytelsen i implementerte prosessene og tiltakene med hensyn til mål og planlegging, og rapportere resultatene;*
- ***Forbedring**: Treffe tiltak for kontinuerlig forbedring av sikkerhetsstyringssystemet og sikkerhetsytelsen, for å oppnå de tilsiktede resultatene.*

Denne kjerneprosessen utfylles med andre elementer i sikkerhetsstyringssystemet:

- *"**Organisasjonens driftskontekst**" som inneholder innspill til planleggingsfasen;*
- *"**Ledelse**" som drivkraft for PDCA-hjulet;*
- *Ulike "**Støtte**"-funksjoner som understøtter alle elementene i sikkerhetsstyringssystemet.*



Figur 2: Sikkerhetsstyringssystem for jernbanedrift

0.8 Sikkerhetsstyringssystem, menneskelige og organisatoriske faktorer og sikkerhetskultur

Menneskelige og organisatoriske faktorer (HOF) integrerer kunnskap innen samfunnsvitenskap som ledelsesvitenskap, psykologi, sosiologi, designvitenskap og statsvitenskap, for å utvide omfanget av studier og undersøkelser mens man vurderer organisatoriske, institusjonelle, kulturelle eller politiske bidragsytere til sikkerhet. Faktisk er ergonomi (eller menneskelige faktorer), ifølge International Ergonomics Association, den vitenskapelige disiplinen som er opptatt av forståelsen av samhandlingen mellom mennesker og andre elementer i et system, og profesjonen som anvender teori, prinsipper, data og andre metoder for å designe for å optimere menneskelig velvære og generell systemytelse (se også definisjonen i Vedlegg 6).

Begrepet «organisatorisk» er blitt introdusert for å fremheve det overordnede organisatoriske analysenivået og ikke bare individnivået, selv om organisasjoner åpenbart er sammensatt av individer.

Undersøkelsen av menneskelige og organisatoriske faktorer er en del av sikkerhetsstyringsprosessen, hvor en (positiv) sikkerhetskultur er en del av resultatet (eller utfallet) av denne prosessen.

Sikkerhetskulturen er et sett av atferdsmønstre og tenkemåter, som i stor grad deles innenfor en organisasjon når det kommer til kontroll av alvorlig risiko knyttet til deres aktiviteter. Dette innebærer selvfølgelig at det kan være flere kulturer i spill i en organisasjon basert på spørsmål som jobbrolle, geografi eller andre felles verdier. Som sådan utvikles sikkerhetskulturen på daglig basis gjennom samhandling mellom aktørene, i sammenheng med en organisasjon som både trenger å tilpasse seg miljøet (se også definisjonen i Vedlegg 6).

Når det er sagt, er en direkte måte å beskrive sikkerhetskulturen på å se på faktorene som bidrar til atferden. Sikkerhetsstyringssystemet danner grunnlaget: Ved å definere antatte arbeidsforhold og forventede resultater, vil en organisasjon kunne definere foretrukne arbeidsmetoder og de tekniske midlene som anvendes i virksomheten. For å kunne arbeide trygt vil organisasjonen forutse uønskede situasjoner, og implementere regler og virkemidler for å håndtere dem. I tillegg kommer organisasjonens «menneskelige verden»: Egenskaper, følelser, betydninger og forhold som påvirker samhandlingsmønstre mellom personer i organisasjonen på en måte som påvirker måten de tenker og handler på. Denne kulturelle siden refererer hovedsakelig til de "uskrevne reglene som styrer atferd og avgjørelser i en gruppe mennesker". Sammen bidrar den strukturelle og kulturelle delen av organisasjonen (eller hemmer) organisatorisk yteevne.

Det foreligger imidlertid en høy risiko for at tilnærming til sikkerhetsstyring på et overdrevent byråkratisk nivå ikke samsvarer med realiteten, og resulterer i at et sikkerhetsstyringssystem lever sitt eget liv, dvs. alle krefter brukes på å utarbeide, vedlikeholde og til og med bevise at man har et dokumentert system, og man således ignorerer operative innspill som trengs for å få det til å fungere som ønsket, og skaper videre store misforhold mellom «forestilt arbeid» og «reelt arbeid».

På den annen side er det mulighet for å distribuere sikkerhetsstyringssystemet som et instrument for å utøve en positiv innflytelse på sikkerhetskulturen i organisasjonen, og påvirke det fysiske miljøet samt de ansattes atferd på en måte som fremmer og underbygger sikkerheten. Det er i siste instans samsvaret mellom den strukturelle og kulturelle delen av organisasjonen som danner grunnlaget for sikkerheten. Det er her menneskelige og organisatoriske faktorer bør spille en vesentlig rolle. For å bidra til at alle kan utføre oppgavene sine, må organisasjonen forstå hvordan mennesker (med sine evner og begrensninger) anvender aktiva (f.eks. utstyret i en togførers førerhytte eller annen samhandling mellom menneske og maskin) og spesifikasjoner for å løse problemer, og ta hensyn til denne kunnskapen når arbeidsmiljøet utformes. Det samme gjelder regler og forskrifter: Så lenge de ansatte som gjennomfører dem ikke blir hensyntatt når arbeidsprosedyrene utformes, vil de bli tvunget til å gå på akkord med reglene for å få arbeidet gjort når det oppstår inkonsekvens eller konflikter.

Byrået har sammen med representanter for sektoren utviklet den europeiske jernbanesikkerhetskulturmodellen (ERSCM) som er illustrert i Vedlegg 4 (oversettelser av veilederen for ERSCM finnes på alle EU-språk på nettstedet til European Railway Agency, du finner koblinger til dem i vedlegg 4). I dette dokumentet forklares de menneskelige og organisatoriske faktorene og de grunnleggende egenskapene som er kjent for å bidra til en positiv sikkerhetskultur. Videre gir Vedlegg 4 og Vedlegg 5 leseren annen nyttig informasjon for organisasjonen til å utvikle sine egne strategier. Leserne påminnes om at de står fritt til å bruke sine egne sikkerhetskulturmodeller for å støtte sine juridiske forpliktelser.

0.9 Bevis og dokumentert informasjon

Dette dokumentet gir noen indikasjoner på bevisene som søkeren (dvs. jernbanevirksomheten eller infrastrukturforvalteren) må fremlegge sammen med søknaden om sikkerhetssertifikat eller sikkerhetsgodkjenning, men oppgir ikke nøyaktig hva som trenger å fremlegges, av ovennevnte årsaker. For hvert av kravene er det oppgitt en indikasjon på bevis som søkeren må fremlegge, sammen med en henvisning til dette kravet. Det er gitt noen eksempler på hvordan dette beviset kan se ut i praksis. Det skal nevnes at eksemplene er ment som et hjelpemiddel til forståelse og at de ikke er det eneste som kan brukes som et bevis på etterlevelse, og de representerer heller ikke en fullstendig liste over mulige alternativer. Videre skal det nevnes at når søkeren utarbeider en søknad, må det beskrives hvordan hvert av kravene blir oppfylt. Sakkyndig eller søker kan be om eller fremlegge bevis for hvilken type informasjon som foreslås, for å avklare eller fremheve hvordan kravene blir oppfylt. For søker og sakkyndig er det viktigste punktet for hvert krav å sørge for at redegjørelse om etterlevelse er knyttet til referanser, der man forklarer hvor det kan finnes ytterligere bevis for å understøtte informasjonen. Kapittelet med eksemplene for hvert av kravene tar sikte på i indikere hvordan dette referansematerialet kan se ut.

Referanser, som kan være nyttige for en søker i å forberede en søknad, er oppført etter dette kapittelet. Til slutt tar den siste delen under hvert element sikte på å etablere den nødvendige tilknytningen til Tilsyn. Her er det gitt en indikasjon på problemstillinger som en sakkyndig kan ønske å fremheve overfor NSA-tilsynet, som interessepunkter som kan brukes til å teste helheten av sikkerhetsstyringssystemet.

På samme måte er tilnærmingen som anvendes i ISO-styringssystemstandarder, Vedlegg I og Vedlegg II til Forordning (EU) 2018/762 kun veiledende, med unntak av spesifikke tilfeller om bevisets art (f.eks. prosedyre) som kan forventes av søkeren. Fleksibiliteten som er overlatt til søkeren tar sikte på til å gi organisasjonen muligheten til å presentere sine sikkerhetsstyringssystemer på en måte som gjenspeiler virksomheten og står i forhold til omfanget. I tillegg vil dette bidra til å bevege seg bort fra en papirbasert test av etterlevelse, og heller til en vurdering av et dynamisk system i utvikling som på en egnet måte gjenspeiler virksomhetens sikkerhetsstyringssystemer, slik de virker i praksis.

Begrepet "dokumentert informasjon" ble introdusert som en del av ISO HLS og vanlige begreper for styringssystemstandarder. Definisjonen av "dokumentert informasjon" finnes i *ISO 9000 paragraf 3.8*. Dokumentert informasjon kan brukes til å formidle et budskap, gi bevis på hva som var planlagt, hva som faktisk er gjort, eller utveksling av kunnskap. Den inkluderer, men er ikke begrenset til, dokumenter og arkiver som prosedyrer, møtereferater, rapporter, formell kommunikasjon om mål, resultater, avtaler, kontrakter, osv. Ytterligere forklaringer finnes i *Veiledning for krav til dokumentert informasjon i ISO 9001:2015* tilgjengelig på ISO-nettsiden.

Begrepet "prosedyre" skal ikke være ment å innebære at det foreligger et frittstående dokument som utelukkende og omfattende dekker anvendelsen av hvert enkelt element i sikkerhetsstyringssystemet, eller å kreve at et spesifikk nytt sett med dokumenter utarbeides. Når dette dokumentet refererer til en prosedyre, viser det til dokumentert informasjon (f.eks. papirdokumenter) som beskriver trinnene som skal anvendes. Når det refereres til en prosess, viser dette til midler for å fullføre en oppgave eller nå et mål som kanskje ikke er beskrevet i en prosedyre.

0.10 Kryssreferanser til andre EU-forordninger og gjeldende lovfestede krav

Referanser til andre EU-forordninger styrker konsistensen mellom de ulike juridiske tekstene, samtidig som man anerkjenner forbindelsene mellom dem. Sikkerhetsstyringssystemet må alltid overholde gjeldende lovtekst, med mindre annet er angitt (f.eks. spesifikke overgangsbestemmelser, forsinket søknad). Når en EU-forordning oppheves, blir alle referanser vanligvis fortolket som referanser til den nye forordningen (hvis de angitt deri).

Alle jernbanevirksomheter og infrastrukturforvaltere må overholde en rekke lovfestede forpliktelser som strekker seg utover dem som bare omfatter sikkerhetsaspekter. Noen av disse andre forpliktelsene vil enten direkte eller indirekte påvirke hvordan organisasjonen håndterer sitt sikkerhetsansvar på ved hjelp av sikkerhetsstyringssystemet, for eksempel etterlevelse av lovgivningen som følger av direktiv (EU) 2016/797 (interoperabilitetsdirektivet) eller sikkerhetsrelevans for tjenesten som leveres av infrastrukturforvalterne til jernbanevirksomhetene innenfor rammeverket til Direktiv (EU) 2012/34. Derfor må sikkerhetsstyringssystemet som jernbanevirksomhetene og infrastrukturforvalterne bruker til å håndtere risikofaktorer, organiseres der det er nødvendig for å sikre at andre lovfestede forpliktelser overholdes.

EUROPEAN UNION AGENCY FOR RAILWAYS

For et jernbanesystem som
fungerer bedre for samfunnet.

Innhold

EUROPEAN UNION AGENCY FOR RAILWAYS

For et jernbanesystem som
fungerer bedre for samfunnet.

1 Organisasjonens driftskontekst

1.1 Lovbestemt krav

1.1 Organisasjonen skal:

(a) beskrive typen, karakteren, omfanget og området for virksomheten;

(b) identifisere de alvorlige sikkerhetsrisikoene som dens jernbanevirksomhet utgjør, enten de blir utført av organisasjonen selv eller av entreprenører, partnere og leverandører under dens kontroll;

(c) identifisere interesserte parter (f.eks. reguleringsorganer, myndigheter, jernbaneforetak, infrastrukturforvaltere, entreprenører, leverandører, partnere), inkludert partene utenfor jernbanesystemet som er relevante for sikkerhetsstyringssystemet;

(d) identifisere og opprettholde juridiske og andre krav knyttet til sikkerhet fra interesserte parter nevnt i punkt (c);

(e) sikre at kravene som er nevnt i bokstav d), tas med i betraktning ved utvikling, implementering og vedlikehold av sikkerhetsstyringssystemet;

(f) beskrive omfanget av sikkerhetsstyringssystemet, angi hvilken del av virksomheten som er inkludert eller ikke i dets omfang og ta hensyn til kravene som er nevnt i bokstav d).

1.2 For dette vedlegget gjelder følgende definisjoner:

(a) «karakter» i forbindelse med jernbanedrift som utføres av infrastrukturforvaltere vil si en karakterisering av driftens art etter dens omfang, herunder utforming og oppbygging av infrastrukturen, vedlikehold av infrastrukturer, trafikkplanlegging, trafikkstyring og kontroll, og bruk av jernbaneinfrastrukturen, inkludert konvensjonelle linjer og/eller høyhastighetslinjer, passasjertransport og/eller godstransport

(b) «omfang» i forbindelse med jernbanedriften som uføres av infrastrukturforvaltere, omfanget som karakteriseres av lengden på jernbanesporet og infrastrukturforvalterens estimerte størrelse med hensyn til antall ansatte i jernbanesektoren.

1.2 Formål

Søkeren skal så presist som mulig bevise overfor myndighetene at sikkerhetssystemet fullstendig dekker driften. Vurderingsmyndighetene må kunne se klart hva driftens art er, og hvordan den styres av sikkerhetsstyringssystemet. Søkeren skal bevise at man har en klar forståelse av forholdet til involverte parter og alvorlige risikoer man står overfor, hvem som er berørt og hvordan dette håndteres i sikkerhetsstyringssystemet.

1.3 Forklarende merknader

I pkt. 1.1 i lovteksten ovenfor, hvor kravet gjelder infrastrukturforvaltere, erstattes «type» med «karakter» og «område» slettes.

«Kravsorganisasjonen», dens driftskontekst og omfanget av sikkerhetsstyringssystemet **(1.1)** tar sikte på gi en bedre forståelse fra sakkyndiges perspektiv av organisasjonens virksomhet, interessentenes forventninger og miljøet organisasjonen opererer i. Organisasjonens art er utgangspunktet for vurderingen - når denne informasjonen er oppgitt i begynnelsen av søknaden kan søkeren beskrive hva de gjør og hvordan organisasjonen er strukturert, og dette vil igjen gjøre det mulig for sakkyndige å ta beslutninger om hvordan man skal planlegge vurderingen. Hvis organisasjonen for eksempel er sentralisert eller driver ulike virksomheter med omfattende lokal frihet til å planlegge og organisere aktivitetene sine, eller hvis organisasjonen leier inn flere eller færre leverandører, vil det være en tilsvarende forventning til at søkerens organisasjon og dens sikkerhetsstyringssystem er strukturert for å håndtere problemer som har oppstått. Organisasjonen bør tydelig forklare hvem dens entreprenører er, hvilken oppfølging/overvåking av dem som utføres (se også avsnitt 6.1) og hvordan ansvaret for ulike aspekter av operasjonen administreres av søkeren. Det bør også være klart hvor ansvaret ligger mellom sikkerhetsstyringssystemet til søkeren og de til enhver andre organisasjonene som det er samhandling med. Forklaringen av organisasjonens driftskontekst kan også indikere hvordan menneskelige og organisatoriske faktorer håndteres. Strukturen som er beskrevet i punkt 4 i ISO High Level Structure, kan bidra til å forstå det forberedende arbeidet som trengs før sikkerhetsstyringssystemet utarbeides. Det er ytterst viktig at den sakkyndige forstår omfanget av driften hvis vedkommende skal kunne foreta en skikkelig vurdering.

Typer operasjoner **(1.1 (a))** omfatter per definisjon passasjertransport (med eller uten høyhastighetstjenester) og gods (med eller uten farlig gods) og skiftetjenester. Det kan også omfatte andre spesielle typer operasjoner som testing av jernbanevogner, bruk av jernbanevogner for vedlikehold av jernbaneinfrastrukturen eller operasjoner på privateide sidespor. Mer informasjon om typen, omfanget og operasjonsområdet finnes i *Byråets søknadsveiledning for utstedelse av EU-sikkerhetssertifikater*. Ytterligere informasjon om sidesporoperasjoner finnes i Vedlegg 3.

For en infrastrukturforvalter karakteren og omfanget **(1.2)** av virksomhetens art og dens geografiske størrelse og kompleksitet. Karakteren gjenspeiler hva slags infrastruktur som er i bruk, hvor moderne den er, om den er høyhastighets eller konvensjonell eller begge deler, mens omfanget omhandler hva slags virksomhet som drives.

Det å identifisere alvorlige risikoer i dette tilfellet betyr at søkeren skal vise at de på bakgrunn av analysen er klar over hvilke av risikoene de står overfor, som er de viktigste. Identifikasjon av alvorlige risikoer innbefatter også at søkeren har utarbeidet et risikostyringssystem (eller er i ferd med å utarbeide det), og ut fra dette kan man:

- *analysere farlige hendelser og vurdere risiko,*
- *bli gjort oppmerksom på det mest viktige (når det gjelder konsekvenser og hyppighet) og*
- *prioritere tiltak som har som hensikt å forebygge ulykker**. (1.1 (b))***

Dette hjelper med å angi omgivelsene for organisasjonen, og viser vurderingsmyndigheten at de forstår miljøet de arbeider i. Andre aktørers eller eksterne parters aktiviteter (1.1 (c)) kan påvirke sikkerheten ved driften, og må i den forbindelse også vurderes som en del av risikovurderingen. Ytterligere informasjon om avtaleordninger og samarbeid finnes i Vedlegg 3.

Søkeren bør også gi nok informasjon til at sikkerhetssertifiseringsorganet kan forstå hva slags operasjon bedriften utfører og hvor; for eksempel frakten selskapet skal sørge for transport av, f.eks. tømmer, containere, kombitransport, semitrailere i lommevogner, gods inne i vogner eller på åpne vogner osv., og rutene som dekkes. For ulike typer varer kan bedriften trenge å ha ulike typer administrasjonsordninger referert til i sikkerhetsstyringssystemet (lasting, opplæring osv.)

Organisasjonens driftskontekst skal også beskrive hvordan jernbaneforetaket eller infrastrukturforvalteren planlegger å håndtere vedlikeholdet av alle kjøretøyene de skal bruke. For eksempel vil organisasjonen bruke en sertifisert Entity in Charge of Maintenance (ECM), eller ønsker organisasjonen å bli en ECM og vedlikeholde kjøretøy utelukkende for egen drift og selv oppfylle de relevante ECM-kravene (se vedlegg II i

forordning (EU) 2019/779 og tilhørende veileder), inne i sikkerhetsstyringssystemet. Søkeren må spesifisere forholdet mellom ulike avtaleparter for vedlikehold; dersom jernbaneforetaket f.eks. leier kjøretøy som vedlikeholdes av en tredjeparts ECM, bør dette spesifiseres. Ytterligere informasjon om styring av vedlikeholdsaktiviteter finnes i ERA Guide on Entities in Charge of Maintenance.

Identifikasjon av gjeldende sikkerhetskrav **(1.1 (d))** omfatter alt fra bestemmelsene i gjeldende EU-forordninger (f.eks. relevante felles sikkerhetsmetoder for sikkerhetsstyringssystemer, særlig Vedlegg I og Vedlegg II, felles sikkerhetsmetoder for risikovurdering og evaluering, felles sikkerhetsmetoder for overvåkning, relevante tekniske spesifikasjoner for interoperabilitet, gjennomføringsloven om praktiske ordninger for sikkerhetssertifisering og, hvor det måtte være aktuelt, gjennomføringsloven om praktisk ordning for vogngodkjenning og ECM-forordningen) og nasjonal lovgivning (f.eks. meldt nasjonal regelverk, nasjonal lovgivning), til alle andre krav som organisasjonen underlegger seg (f.eks. regler på sektor- eller bransjenivå for togdrift eller styringssystem og tekniske standarder som ISO, CEN/CENELEC, UIC).

I denne delen identifiserer organisasjonen de lovbestemmelsene den må overholde sammen med de sektorkravene og andre krav som den må overholde for å kunne kjøre tog sikkert. Det kan være ulike krav i ulike MS og sikkerhetsstyringssystemet må være i stand til å håndtere eventuelle konflikter mellom disse og det juridiske rammeverket. Ytterligere informasjon som er relevant for disse kravene, finnes i dokumenter som netterklæringer.

Dersom jernbaneforetaket planlegger å transportere farlig gods eller infrastrukturforvalteren planlegger å tillate transport av farlig gods på sin infrastruktur, må de begge oppfylle de spesifikke kravene fastsatt i forskrift om internasjonal transport av farlig gods, (RID) samt ev. nasjonale regler som gjelder. RID har spesifikke krav til opplæring av personell involvert i transport av farlig gods som sikkerhetsrådgiveren samt for eksempel krav til beredskapsplaner og disse bør dekkes i SMS (se også UIC – IRS 40471-3).

Med hensyn til dette dokumentet har begrepene "personal", "bemanning", "ansatte" og "arbeidere" samme betydning, det vil si personer som arbeider under direkte ledelse av søkerens organisasjon.

1.4 Bevis

- *For jernbanevirksomheter: Informasjon om operasjonens art, f.eks. passasjer og/eller gods, transport av farlig gods, geografisk dekning, (ved å inkludere kart eller ruteplan) og omfanget av operasjonen, bruk av underleverandører, partnerskap med andre operatører (navn), de ulike involverte aktørene (navn og type aktør), valg av sertifisert ECM med kopi av gyldig sertifikat. Den bør også identifisere typer rullende materiell, antall ansatte som er direkte ansatt og en indikasjon på hvor ekstra personell er innleid fra og, hvor søknaden er en fornyelse av et sertifikat, eventuelle endringer som er gjort siden siste vurdering;* ***(1.1 (a))***
- *For infrastrukturforvaltere: Informasjon om hvilke tjenester de utfører, for eksempel frakt og passasjertransport, sporveksling eller andre anleggstjenester (som nevnt i Vedlegg II til Direktiv 2012/34/EU) som har innvirkning på jernbanesikkerhet, geografisk dekning (ved å vedlegge et kart eller ruteplan) og omfanget av jernbanevirksomheten som foregår på jernbanenettet. Infrastrukturforvalteren bør også inkludere informasjon om sin bruk av underleverandører (navn), partnerskap med andre operatører (navn), ulike involverte aktører (navn og type), valg av sertifisert ECM med kopi av gyldig sertifikat. De bør også angi eventuelt rullende materiell (inkludert anlegg for vedlikehold eller måling av infrastruktur) de kan drive, og angi antall ansatte de sysselsetter og, i tilfelle fornyelser, eventuelle endringer i bemanningsordningene siden forrige vurdering;****(1.1(a))***
- *Søkeren må oppgi hva som er de mest alvorlige sikkerhetsrisikoene, som har innvirkning på virksomheten;* ***(1.1(b))***
- *Søkeren til et sikkerhetssertifikat eller en sikkerhetsgodkjenning må fremvise hvordan relevante forskriftskrav er identifisert, for eksempel CSM-vurderingskravene, de tekniske spesifikasjonene for interoperabilitet, da særlig dem som omfatter drifts- og trafikkstyringsundersystem (TSI OPE), gjeldende nasjonale bestemmelser og andre krav (sektorregler, andre regler) som må følges for å*

kunne kjøre tog trygt, samt hvordan det sikres at disse overholdes (prosessene i sikkerhetsstyringssystemet som bidrar til overholdelse); ***(1.1 1(c)-(d))***

- *Søkeren må identifisere interesserte parter som er relevante for vellykket implementering av deres sikkerhetsstyringssystem (dvs. at deres handlinger har en innvirkning eller potensiell innvirkning på sikkerhetsstyringssystemet, for eksempel kontraktører eller partnere) med en indikasjon på hvorfor de er nødvendige for vellykket drift av sikkerhetsstyringssystemet;****(1.1 (c) (d))***
- *For begge parter: Søkeren må angi hvor i dokumentasjonen for sikkerhetsstyringssystemet hvert av SMS-kravene, inkludert de relevante kravene i de gjeldende tekniske spesifikasjonene for interoperabilitet, særlig (TSI-OPE), og relevante meldte nasjonale bestemmelser og andre krav, er oppfylt* ***(1.1(e))***
- *Søkeren må komme med opplysninger om omfanget av sikkerhetsstyringssystemet (inkludert hvilke grenser det er mot andre deler av virksomheten, som for eksempel vedlikehold av kjøretøy).****(1.1(f))***

1.5 Eksempler på bevis

Et kart som viser det geografiske driftsområdet. Informasjon om rullende materiell som er godkjent for drift (inkludert eventuelt foreslått rullende materiell som det er foreslått å ha i drift i løpet av sertifikatets eller godkjenningens virketid, samt eventuelle begrensninger i bruksområdet). Informasjon om hvilke typer tjenester som skal utføres (passasjertransport og/eller frakt) er inkludert.

Dersom søkeren er en infrastrukturforvalter, kan denne f.eks. informasjonen tilveiebringes ved:

- *Informasjonen i Infrastrukturregisteret (RINF) satt opp i samsvar med direktiv (EU) 2016/797 (art. 49);*
- *Innholdet i netterklæringen (særlig i del I) som er opprettet i samsvar med Direktiv 2012/34/EU; og*
- *Ruteboken satt opp i samsvar med forordning (EU) 2019/773 (TSI OPE).*

Informasjonen som er gitt for å få en sikkerhetsautorisasjon eller sikkerhetssertifikat, er riktig gjengitt og er tilstrekkelig dokumentert til å bevise samsvar med relevant EU-lovgivning.

En indikasjon på nåværende og foreslått bemanning innenfor virketiden til det felles sikkerhetssertifikatet så sant dette er kjent.

En jernbanevirksomhet oppgir informasjon om operativ samhandling, herunder med infrastrukturforvalteren, andre jernbanevirksomheter, leverandører og beredskapstjenester. Denne informasjonen inkluderer eventuelle spesifikke krav fra infrastrukturforvalteren som påvirker jernbaneforetakets sikkerhetsstyringssystem.

For jernbanevirksomheter kan en kartleggingstabell som vedlegges som en del av søknadsfilen for et sikkerhetssertifikat, brukes til å forklare hvordan forskriftene og andre relevante krav overholdes.

Likeledes bør en infrastrukturforvalter tilveiebringe en tilsvarende liste over hvem de samhandler med, for eksempel jernbanevirksomheter som opererer i den kontrollerte infrastrukturen, dens leverandører, grensende infrastrukturforvaltere, anleggsplasser, lokale myndigheter (for knutepunkter) og beredskapstjenestene.

Informasjon om lovbestemmelser (både nasjonale og europeiske) som skal overholdes.

En beskrivelse (inkludert et organisasjonskart) som beskriver oppbyggingen av sikkerhetsstyringssystemet og hvordan det administreres i organisasjonen, og som inneholder koblinger til de ulike seksjonene i sikkerhetsstyringssystemet der mer detaljert informasjon, som driftsregler, kan finnes.

En nylig kopi av årsrapporten som beskriver i detalj de mest alvorlige risikoene organisasjonen står overfor og målene for å styre disse, hvordan man vurderer dem og hvordan de prioriteres.

En erklæring om du bruker en sertifisert ECM eller vedlikeholder kjøretøy utelukkende for din egen drift.

En oversikt over vedlikeholdsprosessen og type og nivå som er utført.

Det å ta hensyn til menneskelige og organisatoriske faktorer og forbedre sikkerhetskulturen vil ha en positiv innvirkning på samsvar med det relevante kravet til sikkerhetsstyringssystemet, og bevis på dette finnes i:

Et risikoregister eller en oversikt hvor scenarioer for operasjonssikkerhetsrisiko er dokumentert, inkludert hensyn til menneskelige og organisatoriske faktorer:

- *Enkeltpersoner (f.eks. menneskelige feil);*
- *Arbeidsplass (f.eks. fysisk miljø, som støy, mørke, vær); og*
- *Organisering (f.eks. arbeidsbelastning, kompetansestyring, oppgavedesign, ressurser, turnus).*

For å definere de mest alvorlige risikoene evalueres risikoscenarioer for å gi mulighet for en risikoprioritering (dette finnes i risikovurderingsprosessen, se 3.1.1). Risikoregisteret omfatter risiko knyttet til organisasjonens aktiviteter samt aktiviteter utført av entreprenører, samarbeidspartnere eller leverandører under dens kontroll. For hver alvorlige risiko er risikoeieren klart definert i sikkerhetsstyringssystemet.

Sikkerhetsstyringssystemet inneholder en beskrivelse av interessentene som er relevante for sikkerhetsstyringen, og beskriver hvordan forholdet til disse interessentene skal håndteres. Midlene for å dele de mest alvorlige risikoene med de berørte tredjepartene er angitt og noen eksempler er gitt (f.eks. kontrakter, møtereferat).

1.6 Referanser og standarder

- *TSI OPE-søknadsveiledning*
- *ECM-retningslinjer*
- *UIC – IRS 40471-3 Inspeksjoner av forsendelser av farlig gods*

1.7 Sjekkpunkter

Sjekk nøyaktigheten av informasjonen som er gitt mot kjent informasjon om eksisterende drift der det foreligger søknad om fornyet sertifikat, eller mot annen tilgjengelig informasjon dersom en ny aktør kommer på banen.

Sjekk at sikkerhetsstyringssystemet som beskrevet inneholder ordninger for å styre sikkerheten i praksis.

Sjekk at all samhandling organisasjonen har med andre parter, gjenspeiles i ordningen i sikkerhetsstyringssystemet for risikostyring.

2 Ledelse

2.1 Ledelse og forpliktelse

2.1.1 Lovbestemt krav

2.1.1. Toppledelsen skal vise til ledelse og forpliktelse til utvikling, implementering, vedlikehold og kontinuerlig forbedring av sikkerhetsstyringssystemet ved å:

(a) ta overordnet ansvar og ansvaret for sikkerheten;

(b) sikre forpliktelse til sikkerhet fra ledelsen på ulike nivåer i organisasjonen gjennom deres aktiviteter og i deres forhold til ansatte og kontraktører;

(c) sikre at sikkerhetsregler og sikkerhetsmål er etablert, forstått og er kompatible med organisasjonens strategiske retning;

(d) sikre integreringen av kravene til sikkerhetsstyringssystemet i organisasjonens forretningsprosesser;

(e) sikre at ressursene som trengs for sikkerhetsstyringssystemet er tilgjengelige;

(f) sikre at sikkerhetsstyringssystemet er effektivt med tanke på å kontrollere sikkerhetsrisikoen organisasjonen utgjør;

(g) oppmuntre ansatte til å støtte overholdelse av kravene til sikkerhetsstyringssystemet;

(h) fremme kontinuerlig forbedring av sikkerhetsstyringssystemet;

(i) sikre at sikkerhet vurderes når man identifiserer og administrerer organisasjonens forretningsrisiko og forklarer hvordan konflikt mellom sikkerhet og andre mål vil bli gjenkjent og løst;

(j) fremme en positiv sikkerhetskultur.

2.1.2 Formål

Et klart og positivt fokus på sikkerhetsstyring, vil ha en viktig effekt på hvordan risikoen styres. Vurderingsmyndighetene må være sikker på at søkeren bestreber seg på å tilordne ressurser slik at organisasjonen kan drives på en trygg måte og slik at den har en effektiv risikostyring, og at ledelsen i søkerens organisasjon er der for å sikre at dette virkelig skjer. Ledelsens engasjement i menneskelige og organisatoriske faktorer tilkjennegis av retningslinjer, målsettinger og i lederskap og ledelsens opptreden. Videre vil en ledelsens tilnærming til menneskelige og organisatoriske faktorer også føre til at opplæring og prosedyreutvikling er basert på oppgaven som skal utføres i sin naturlige setting, noe som vil bidra til å optimalisere både risikostyring og yteevne, siden den vil være basert på en nøyaktig beskrivelse av oppgaven («arbeid gjort»).

Sikkerhetspolicyen angir viktigheten og prioriteringen av sikkerhet, inkludert integrering av menneskelige og organisatoriske faktorer og fremming av sikkerhetskulturen.

Organisasjonen fremmer en konstant og kollektiv årvåkenhet, bekjemper selvtilfredshet ("alt er under kontroll") og overforenkling ("overholdelse av prosedyrer er nok for en god sikkerhet"), og utvikler et kritisk syn. Videre er alle aktører i organisasjonen klar over at uansett kvaliteten på planlegging og organisering, tekniske barrierer og prosedyrer, kan det alltid være et gap mellom hva som er forventet og hva som er realiteten. Alle mulige kilder brukes til å registrere og kollektivt analysere situasjoner man ikke har kommet i forkjøpet.

I tillegg er organisasjonens kommunikasjon om sikkerhet i tråd med faktiske beslutninger fra ledelsen.

For at et sikkerhetsstyringssystem skal kunne fungere effektivt og videre forbedres, er det avgjørende at dem som har lederroller viser overfor sine ansatte og interessenter at de setter en positiv dagsorden der sikkerheten kan styres. Det er de i ledelsesstillinger som har størst påvirkning på organisatorisk kultur, og det er derfor viktig at de kan kommunisere meldingene sine til de som arbeider for dem. Atferden til ledere på alle nivåer i organisasjonen og det fokus de har på sikkerheten i deres daglige beslutninger, vil i stor grad påvirke andre aktørers atferd når det gjelder å løse sine oppgaver på en sikker måte. I tillegg skal lederne skape de fysiske og sosiale arbeidsmiljøene der det utføres frontlinjearbeid på en sikker måte.

2.1.3 Forklarende merknader

"Toppledelse" **(2.1.1)** viser i denne sammenhengen til ledere som tar endelige beslutninger i organisasjonen. Vanligvis vil dette være administrerende direktør, medlemmer i toppledelsen, styreformann og styremedlemmer. Som en gruppe og som enkeltpersoner er "toppledelsen" pålagt å utvise godt lederskap og engasjement ved hjelp av sikkerhetsstyringssystemet.

Hvordan blir menneskelige og organisatoriske faktorer og sikkerhetskultur integrert?

Sikkerhetsrisikoen skal vektlegges tilstrekkelig **(2.1.1 (j))** for å balansere andre risikoer på arbeidsplassen, for å unngå situasjoner der ledelsen prioriterer forretningsbehov på en slik måte at det går utover sikkerheten. Toppledelsen må sørge for at målsettingene håndteres på en slik måte at sikkerheten opprettholdes, og at risikoen kan styres så langt det i rimelig grad er mulig. Motstridende mål må ikke resultere i motstridende oppgaver for enkeltpersoner, som kan føre til at det går utover sikkerheten.

En integrert tilnærming til menneskelige og organisatoriske faktorer til ledelse og styring vil si å sette mål, forventninger og ansvar i forhold til sikkerhetsatferden på alle nivåer i organisasjonen, og sikre betimelige tilbakemeldinger og kommunikasjon.

2.1.4 Bevis

- *Det foreligger sikkerhetspolicy og målsettinger og det foreligger bevis på at disse er tilgjengelige for og forstått av alle ansatte, og det er klargjort hvordan disse passer inn i andre forretningsprosesser og er koblet til kontinuerlig forbedring;**(2.1.1 (a)(b)(g)(e)(h))***
- *Sikkerhetspolicyen fastslår viktigheten av å anvende en tilnærming til menneskelige og organisatoriske faktorer i alle sikkerhetsrelaterte prosesser, for å oppnå et høyt sikkerhetsnivå i organisasjonen. Organisasjonen viser hvordan menneskelige og organisatoriske faktorer i organisatoriske prosesser håndteres;**(2.1.1 (c))***
- *Forholdet mellom sikkerhetsstyringssystemet og andre forretningsaktiviteter er tydelig fastsatt i en prosedyre eller et organisasjonskart;**(2.1.1 (e),(i))***
- *Det foreligger informasjon i sikkerhetspolicyen eller i andre prosesser for å indikere at ledelsen bestreber seg på å tilveiebringe og opprettholde tilstrekkelige ressurser for at sikkerhetsstyringssystemet skal fungere effektivt og forbedres over tid;**(2.1.1 (e), (h))***
- *Det foreligger bevis på at ledelsen fremmer en positiv sikkerhetskultur;**(2.1.1 (j), (h))***
- *Det foreligger bevis på hvordan det sikres at ansatte forstår deres sikkerhetsroller og ansvar, og hvordan de påvirker organisasjonens evne til risikostyring gjennom sikkerhetsstyringssystemet;**(2.1.1 (d)(f)(i))***
- *Det fremkommer i sikkerhetspolicyen eller annen dokumentasjon at organisasjonen søker å informere sine ansatte om den viktige rollen de spiller for å sikre at sikkerhetsstyringssystemet fungerer i praksis, for å oppnå en meningsfull risikostyring;**(2.1.1 (e))***

- *Det foreligger prosesser som beskriver hvordan menneskelige og organisatoriske faktorer skal håndteres og formidles i organisasjonen relatert til organisasjonens forretningsmål og organisasjonsprosesser, for eksempel prosjekter, granskning av hendelser og ulykker, risikoanalyser og andre sikkerhetsrelaterte aktiviteter for organisasjonens eget personale, leverandører, samarbeidspartnere og leverandører;**(2.2.1 (c)(d)(e))***
- *Det fremkommer at ledelsen har satt i gang prosesser for å sikre at menneskelige og organisatoriske faktorer blir riktig fulgt opp av organisasjonens underleverandører;**(2.2.1 (c)(d)(e))***

2.1.5 Eksempler på bevis

En sikkerhetspolicy som er undertegnet og datert av administrerende direktør, som klart beskriver ledelsens bestrebelser på å oppnå god sikkerhet og forbedring av sikkerheten, og hvordan de ansatte er involvert i risikostyring. Sikkerhetspolicyen beskriver også hvordan den skal gjennomgås.

Det å ta hensyn til menneskelige og organisatoriske faktorer og forbedre sikkerhetskulturen vil ha en positiv innvirkning på samsvar med det relevante kravet til sikkerhetsstyringssystemet, og bevis på dette finnes i:

Et klart sett med sikkerhetsmålsettinger fastsatt for organisasjonen, som er Spesifikke, Målbare, Attraktive, Realistiske og Tidsbestemte (SMART-modellen), og det finnes en klar metodikk i en prosedyre for å skape disse og for å analysere om man har nådd dem eller ikke. Sikkerhetsstyringssystemet inneholder bevis på at ledelsen har mål knyttet til operasjonell sikkerhet (ved siden av mål knyttet til helse og sikkerhet på arbeidsplassen).

En tydelig uttalelse fra ledelsen om hvordan de fremmer en positiv sikkerhetskultur og hvordan ansatte er involvert og engasjert i prosessen.

En oversikt over møtene som toppledelsen har og deres hyppighet, der sikkerhet er standard rapporteringspost.

En klar redegjørelse om organisasjonens bestrebelser på å tilveiebringe tilstrekkelige ressurser slik at sikkerhetsstyringssystemet fungerer effektivt for risikostyring.

Et organisasjonskart som tydelig beskriver hvordan sikkerhetsstyringssystemet fungerer, og hvem som er ansvarlig for hva.

Det gjøres en tilnærming til menneskelige og organisatoriske faktorer i designet av nytt utstyr, for eksempel nye tog. Dette inkluderer bruk av gjeldende brukererfaringer i å utarbeide designkrav, analysere oppgaver for å identifisere kognitive og fysiologiske utfordringer, redusere potensialet for manglende yteevne gjennom designet ved å anvende retningslinjer for menneskelige faktorer, som internasjonalt anerkjente standarder, foreta en styringsanalyse av arbeidsbelastning og utmattende arbeid for å sikre at bemanningen er i stand til å utføre sine oppgaver, utarbeide risikoanalyser for å identifisere potensielle problemer og identifisere utbedrende tiltak for disse. Miljøfaktorer som snø, varme, regn, etc. tas hensyn til på lik linje med sosioøkonomiske faktorer som organisatoriske prioriteringer, anskaffelser og nasjonal kultur.

Sikkerhetslederopplæring organiseres for ledere i sikkerhetsstillinger. Det foreligger periodisk ledertrening. Det foreligger lederopplæring som tar hensyn til sikkerhetsvisjonen, hvordan den blir integrert i sikkerhetspolicyen, samt hvordan man kommuniserer og anvender den.

Ledelsen demonstrerer gjennom registreringer av sikkerhetsturer eller besøk på anlegg sin forpliktelse til å fremme en positiv sikkerhetskultur og sitt ønske om å gå foran med et godt eksempel.

2.1.6 Referanser og standarder

- *Sikkerhetskultur (ERA-nettsiden)*

2.1.7 Sjekkpunkter

Omfanget av skillet mellom eventuelle retningslinjer og prosedyrer som er gitt som en del av bevisene ovenfor, og realiteten som observeres under tilsyn og i hvilken grad organisasjonen er klar over gapet mellom disse, er av sentral viktighet i tilsynet.

Omfanget av lederskapets og de ansattes engasjement i sikkerhetsstyringssystemet og fremming av sikkerhetskulturen, bør testes under tilsyn gjennom å undersøke organisasjonenes egne mekanismer for forståelse og utvikling av denne kulturen og sikkerhetsstyringssystemet.

Sjekk at organisasjonen kan vise til tilstrekkelige ressurser som er tilordnet utvikling, implementering, vedlikehold og kontinuerlig forbedring av sikkerhetsstyringssystemet.

Sjekk ved å intervjue toppledelsen og andre ansatte hvordan ledelsen uttrykker sin forpliktelse til forbedring av sikkerheten. Finn ut hvor ofte og på hvilke måter de er i kontakt med personalet om sikkerhetsspørsmål og/eller for å fremme sikkerhetskultur (workshops, fora, dedikerte sikkerhetsdager osv...).

Sjekk om det er kommunikasjon fra toppledelsen vedrørende målsettinger, enten i den hensikt å oppmuntre alle ansatte til å bidra til å nå målene, eller for å takke alle for en forbedret yteevne.

2.2 Sikkerhetspolicy

2.2.1 Lovbestemt krav

Et dokument som beskriver organisasjonens sikkerhetspolicy er etablert av toppledelsen og er:2.2.1.

(a) passende for organisasjonens type, karakter og omfanget av jernbanedriften;

(b) godkjent av organisasjonens administrerende direktør (eller en representant(er) for toppledelsen);

(c) aktivt implementert, kommunisert og gjort tilgjengelig for alle ansatte.

2.2.2. Sikkerhetspolicyen skal:

(a) omfatte en forpliktelse til å overholde alle juridiske og andre krav knyttet til sikkerhet

(b) gi et rammeverk for å sette sikkerhetsmål og evaluere organisasjonens sikkerhetsytelse opp mot disse målene

(c) omfatte en forpliktelse til å styre sikkerhetsrisikoer som oppstår både fra egne aktiviteter og som er forårsaket av andre

(d) omfatte en forpliktelse til kontinuerlig forbedring av sikkerhetsstyringssystemet

(e) vedlikeholdes i samsvar med forretningsstrategien og evalueringen av organisasjonens sikkerhetsprestasjoner

2.2.2 Formål

Sikkerhetspolicyen er et viktig dokument for å vise hvordan organisasjonen håndterer sitt sikkerhetsansvar, og sin ledelse og forpliktelse til korrekt sikkerhetsstyring. Søkeren skal kunne bevise at det foreligger en sikkerhetspolicy som oppfyller kravene ovenfor, og som i et sammendrag beskriver grunnstrukturen for risikostyring.

2.2.3 Forklarende merknader

Sikkerhetspolicyen er et uttrykk for lederskapets filosofi, og dette punktet er derfor nært knyttet til punkt 3.1.

I pkt. 2.2.1 i lovteksten ovenfor, hvor kravet gjelder infrastrukturforvaltere, erstattes «type» med «karakter».

Hvordan blir menneskelige og organisatoriske faktorer og sikkerhetskultur integrert?

Sikkerhetpolicyen uttrykker sikkerhetsvisjonen; selv om forskriftskravet ovenfor ikke direkte nevner menneskelige og organisatoriske faktorer, er det et tydelig fokus på menneskelige faktorer i organisasjonen og en erkjennelse av den viktige rollen som mennesker spiller i å levere en sikker og effektiv organisering og levering av forretningsmål. Menneskets rolle vurderes ved hver gjennomgang av drifts- og forretningsutviklingen.

2.2.4 Bevis

- *For en jernbanevirksomhet: En skriftlig sikkerhetspolicy undertegnet av administrerende direktør som gjenspeiler type og omfang av virksomheten, som underbygger samsvar med lovfestede krav og*

*andre krav, med fokus på kontinuerlig forbedring av sikkerheten, og som gir et rammeverk for å sette sikkerhetsmålsettinger.**(2.2.1 (a),(b)), (2.2.2 (a-c))***

- *For en infrastrukturforvalter: En skriftlig sikkerhetspolicy undertegnet av administrerende direktør som gjenspeiler karakteren og omfanget av jernbaneoperasjoner og infrastrukturutvikling, som underbygger samsvar med lovfestede krav og andre krav, med fokus på kontinuerlig forbedring av sikkerheten, og som brukes til å sette sikkerhetsmålsettinger;**(2.2.2 (a-c))***
- *For begge parter: Informasjon som viser at sikkerhetspolicyen har blitt formidlet til alle ansatte;**(2.2.1 (c))***
- *Informasjon om at sikkerhetspolicyen opprettholdes slik at den alltid er tilpasset organisasjonens forretningsstrategi og vurderingen organisasjonens sikkerhetsytelse;**(2.2.2 (d), (e))***
- *Bevis på at sikkerhetspolicyen anvendes til å overvåke sikkerhetsytelsen og gjennomgås periodevis etter analyse av sikkerhetsytelse og at den oppdateres etter gjennomgang av organisasjonens sikkerhetsytelse i forhold til de fastsatte målene.**(2.2.2(b), (d), (e))***

2.2.5 Eksempler på bevis

En sikkerhetspolicy undertegnet og datert av administrerende direktør som nøyaktig gjenspeiler virksomhetens type omfang og karakter. Dokumentet forplikter til kontinuerlig forbedring av sikkerhetsstyringssystemet

Sikkerhetspolicyen er oppdatert og blir gjennomgått regelmessig i tråd med forretningsstrategien.

Sikkerhetspolicyen inneholder informasjon eller referanser der prosessen er beskrevet for å gjennomgå den. Dette er for å identifisere om det er behov for endringer etter overvåking av organisasjonens sikkerhetsytelse i henhold til de fastsatte målene.

Sikkerhetspolicyen og andre tilknyttede retningslinjer brukes som et fokus for ledere, noe som resulterer i at de blir tolket på samme måte av alle ansatte.

Ansatte er aktivt er involvert i å gå gjennom og revidere sikkerhetspolicyen hvordan de brukes.

Sikkerhetspolicyen viser til en prosess/metodikk for risikobasert evaluering av forslag til beslutninger (i tråd med sikkerhetsvisjonen). Denne prosessen forklarer hvordan sikkerhet tas i betraktning som et hovedmål.

Sikkerhetspolicyen eller andre bestemmelser i sikkerhetsstyringssystemet som pålegger alle ansatte å stoppe når arbeidsforholdene blir utrygge.

Det er gjennomført en grunnleggende evaluering av organisasjonen med tanke på sikkerhetskultur. Svake punkter er identifisert av organisasjonen, kommunisert til personalet og tiltak for forbedring er angitt i sikkerhetspolicyen.

Det foreligger en prosess for å formidle sikkerhetpolicyen via organisasjonens intranett og for å vise den frem på strategiske/operasjonelle punkter.

Organisasjonen ser utover og ser etter eksterne læringsmuligheter til å utvikle dens effektivitet, og vurderer menneskelige faktorer når den gjør det.

2.2.6 Sjekkpunkter

Under tilsyn vil det være viktig å teste hvor godt sikkerhetspolicyen har blitt formidlet til alle ansatte og at de er innforstått med den, samt hvilken rolle den i realiteten spiller når man setter sikkerhetsrammene organisasjonen opererer i. Et sentralt spørsmål er om dokumentet bidrar til å sette dagsordenen, eller om det bare foreligger fordi det er et lovfestet krav.

Sjekk om endringer i organisatorisk sikkerhetsytelse har ført til en gjennomgang av sikkerhetspolicyen.

Sjekk at sikkerhetspolicyen gjenspeiler organisasjonens virkelighet.

2.3 Organisatoriske roller, ansvar, ansvarlighet og myndigheter

2.3.1 Lovbestemt krav

2.3.1.	Ansvarsområder, ansvarlighet og myndighet til ansatte som har en rolle som påvirker sikkerheten (inkludert ledelse og annet personell som er involvert i sikkerhetsrelaterte oppgaver) skal defineres på alle nivåer i organisasjonen, dokumenteres, tildeles og kommuniseres til dem.
2.3.2.	Organisasjonen skal sørge for at personell med delegert ansvar for sikkerhetsrelaterte oppgaver skal ha myndighet, kompetanse og passende ressurser til å utføre sine oppgaver uten å bli negativt påvirket av virksomheten til andre forretningsfunksjoner.
2.3.3.	Delegering av ansvar for sikkerhetsrelaterte oppgaver skal dokumenteres og kommuniseres til det aktuelle personalet, aksepteres og forstås.
2.3.4.	Organisasjonen skal beskrive tildelingen av roller som er nevnt i punkt 2.3.1. til forretningsfunksjoner innenfor og, der det er relevant, utenfor organisasjonen (se 5.3. Leverandører og samarbeidspartnere).

2.3.2 Formål

Målet med dette kravet er å få søkeren til å gi et klart bilde av organisasjonens struktur, samt hvordan roller og ansvar blir tildelt og opprettholdt over tid, hos alt fra ansatte i frontlinjestillinger til toppledelsen. Dette er nøkkelen til å forstå hvor godt organisasjonens sikkerhetsstyringssystem styrer risikoene. Søkeren skal demonstrere hvordan de tilordner kompetente ansatte til aktiviteter, hvordan de sikrer at de ansatte har en tydelig forståelse av rollene og ansvaret sitt, og hvordan personer holdes ansvarlig for ytelsen sin.

2.3.3 Forklarende merknader

Det kan forekomme et gap i forståelsen mellom reglene i sikkerhetsstyringssystemet på operativt nivå og styringsprosessene som skal drives av sikkerhetsstyringssystemet (f.eks. risikovurdering, overvåking). Identifikasjonen av roller som er relevante i sikkerhetsstyringssystemet **(2.3.1)** er ikke begrenset til dem som er ansvarlige for håndtering av sikkerhetsprosesser, som sikkerhetsledere eller sikkerhetsgrupper, men gjelder enhver rolle som er involvert i sikkerhetsrelaterte oppgaver, som driftspersonellet, og dette er uavhengig av om stillingene er lederstillinger eller ikke i organisasjonen (dvs. ledere, linjeledere, annet personell/ansatte/arbeidere).

"Delegering" **(2.3.3)** betyr overføring av ansvar fra en person i en høy stilling til en person i en lavere stilling, vanligvis med det formål å få fortgang i forhold som oppstår i organisasjonen. Sikkerhetsansvar kan delegeres, dvs. sendes nedover i organisasjonen, innenfor rammene av det definerte jobbansvaret, forutsatt at slik delegering dokumenteres. Sikkerhetsansvar kan ikke delegeres, det forblir juridisk hos toppledelsen. Dette definerer pliktfølelsen til den personen som holdes til ansvar dersom noe ikke er gjort, ikke fungerer, eller dersom mål ikke er nådd, for å vise til en tilfredsstillende utførelse av hans/hennes sikkerhetsansvar.

Tildeling av roller **(2.3.4)** kan vises ved å fremlegge et egnet organisasjonskart.

Hvordan blir menneskelige og organisatoriske faktorer og sikkerhetskultur integrert?

Innenfor roller, ansvar, ansvarsområder og myndigheter **(2.3.1)** bør utveksling av sikkerhetsrelatert informasjon dekkes. For eksempel hvem som har ansvaret for å gi sene endringsmeldinger for lokførere. **(se også 4.4.1 og 4.4.2)**.

Sikkerhetsstyringssystemet skal være i samsvar med CSM-vurderingskravene for sikkerhetsstyringssystemet **(1.1 (d))** og toppledelsen står ansvarlig for å sikre at sikkerhetsstyringssystem oppfyller dem. Toppledelsen

kan delegere noe av ansvaret til relevant personale. Ytelsesrapportering utføres i samsvar med kravene til gjennomgang av styringssystemet **(6.3)**, der relevant personale har ansvar for å rapportere om sikkerhetsstyringssystemets yteevne til toppledelsen.

Sikkerhetsrelaterte oppgaver **(2.3.1)** er ikke begrenset til oppgaver som direkte har med sikkerhet å gjøre (dvs. sikkerhetskritiske oppgaver som utføres av personalet når de styrer eller påvirker bevegelsen av et tog som kan påvirke helsen og personers sikkerhet, som angitt i TSI-OPE). Det inkluderer også ikke-operative oppgaver som påvirker sikkerheten, knyttet til risikovurderingen (f.eks. planlegging av drift, vaktliste, tildeling av kjøretøy). Der nye eller endrede roller og ansvar blir vurdert, er det en analyse av saker med menneskelige faktorer i forhold til endringen og måten pliktene faktisk utføres på innenfor organisasjonen.

Det finnes kriterier for å delegere og tilordne ansvar og oppgaver der nødvendig kompetanse og ferdigheter er identifisert. Disse kriteriene brukes og derfor er sikkerhetsoppgaver tydelig tilordnet, og de ansatte som utfører dem, har passende kompetanse, autoritet og ressurser til å levere dem, og de er klar over risikoene som er forbundet med sine oppgaver.

Kommunikasjon og aksept av oppgaver **(2.3.3)**, inkludert sikkerhetsrelaterte oppgaver, er en del av den normale forretningsprosessen for hvordan personalet tildeles funksjoner, og dette bør kunne revideres. Der delegering av ansvar utføres, er det en systematisk tilnærming til hvordan det gjøres.

Ledelsen skal ha tilstrekkelig kunnskap og forståelse av spørsmål om menneskelige og organisatoriske faktorer, for å sikre at det hentes inn ekspertise når det er nødvendig. Rollene, ansvaret og ansvarligheten for eksperter på menneskelige og organisatoriske faktorer, skal defineres i henhold til oppgavene som skal utføres. **(2.3.3)**.

Det bør være på plass en prosess for å sikre at enkeltpersoner kan rapportere nestenulykker, uønskede hendelser og ulykker uten frykt for reprimande. Policyen støtter opp om den enkeltes rettigheter og ansvar for å for å stille spørsmål ved sikkerheten, og har nulltoleranse for trakassering, trusler, reprimande eller diskriminering. Nøkkelen til suksess i en rettferdig kultur er tillit og åpenhet i organisasjonen. Dette er noe som bygges opp over tid, og avhenger av ledelsens vilje til å foreta omfattende analyser når det har forekommet uønskede hendelser og ulykker, samt å lytte og ta til seg informasjon før de reagerer. Konsistensen i å håndtere sikkerhetsspørsmål er viktig for å etablere en rettferdig kultur.

2.3.4 Bevis

- *Et organisasjonskart og relevant forklarende tekst som viser organisasjonens relevante sikkerhetsansvar og hvordan sikkerhetsstyringssystemet fungerer, og hvordan det er tilknyttet organisasjonens driftskontekst;**(2.3.1), (2.3.4)***
- *En liste over annen informasjon som beskriver sikkerhetsansvar i organisasjonens struktur;**(2.3.1), (2.3.3)***
- *Bevis på at det foreligger et kompetansestyringssystem og at det opprettholdes for alle ansatte, som vurderer tilstrekkeligheten til oppgavene med tildelt ansvar, kompetanse og ressurser.**(2.3.2)***
- *Bevis fra kompetansestyringssystemet eller andre HR-prosedyrer, f.eks. prestasjonsstyring, på at organisasjonen sikrer at roller og ansvar blir formidlet, akseptert og klart forstått av de ansatte, og at de vil bli holdt ansvarlig for å utføre dem;**(2.3.3)***
- *En beskrivelse av ansvaret for drift og vedlikehold, inkludert en definisjon av kravene som ansatte og leverandører skal etterleve;**(2.3.4)***
- *Strategien for menneskelige og organisatoriske faktorer skal vise til krav for når og hvordan ekspertise på menneskelige og organisatoriske faktorer blir hentet inn, og hva deres roller og ansvar er.**(2.3.1), (se også 4.6)***

2.3.5 Eksempler på bevis

Et organisasjonskart med tilleggstekst som gjør det mulig for sakkyndig å se hvordan sikkerhetsstyringssystemet er strukturert, og hvordan de ulike delene er relatert til hverandre.

Referanse til kompetansestyringssystemet (CMS) med informasjon om hvordan dette er strukturert, samt koblinger til der detaljene kan bli funnet, inkludert beskrivelser av HR-prosessen som støtter den, f.eks. prestasjonsstyring.

En tilbakemeldingsprosess brukes til å sikre at informasjon som har gått nedover i organisasjonen er tydelig forstått.

Det å ta hensyn til menneskelige og organisatoriske faktorer og forbedre sikkerhetskulturen vil ha en positiv innvirkning på samsvar med det relevante kravet til sikkerhetsstyringssystemet, og bevis på dette finnes i:

Organisasjonsstrukturen er i samsvar med ansvar som er tydelig fordelt på tvers av organisasjonen.

De overordnede retningslinjene og prosedyrene som dekker roller og ansvar, er konsistente i hele organisasjonen.

Prosessen dekker hvordan sikkerhetsansvar delegeres og hvor delegering er tillatt, med noen eksempler for å vise hvordan prosessen har fungert, med en klar forbindelse til opplegget for risikovurdering.

Eksempler på rollebeskrivelser av sikkerhetsrelaterte oppgaver, også de som ikke er direkte involvert i operasjoner og som indirekte påvirker leveransen av operasjonen (dvs. å tildele roller, planlegge drift og gi driftsinformasjon til personalet, overvåke driften), er tilgjengelige og gjennomgås når det er nødvendig (for eksempel ved endrede rutetider).

Sikkerhetsstyringssystemet inneholder bevis på at ansvar og risiko knyttet til oppgavene, er inkludert i kompetansestyringssystemet og i opplæringsprogrammer. Det er bevis (for eksempel har personen som ansvaret er delegert til, bekreftet dette skriftlig) at ansvaret formelt er akseptert.

Prosedyren(e) for å utarbeide hvilken kompetanse og ressurser som er nødvendig for å understøtte sikkerhetsoppgaver og ansvar på alle nivåer i hierarkiet.

Strategien for menneskelige og organisatoriske faktorer viser hvordan menneskelige organisatoriske faktorer er en integrert del av prosesser og prosjekter. Ekspertisen og aktiviteter knyttet til menneskelige og organisatoriske faktorer er passende for størrelsen på prosessen eller prosjektet. Rollene og ansvaret, samt ansvarligheten og stadiene for engasjement der det er nødvendig å bruke en ekspert på menneskelige faktorer er definert i prosessen eller prosjektplanen.

2.3.6 Referanser og standarder

- *Ansvarlighet og ansvar for sikkerhet (SKYbrary)*

2.3.7 Sjekkpunkter

For tilsyn vil hovedpunktene her være et spørsmål om grad. Spørsmålet som må besvares, er "i hvilken grad gjenspeiler oppgitt informasjon i praksis realiteten i situasjonen"?

En gjennomgang av kompetansestyringssystemets funksjon vil være veien å gå for å få svar på de fleste spørsmålene i denne delen.

2.4 Konsultasjon med ansatte og andre parter

2.4.1 Lovbestemt krav

2.4.1.	Personalet, deres representanter og eksterne interesserte parter skal, etter behov og der det er relevant, konsulteres for å utvikle, vedlikeholde og forbedre sikkerhetsstyringssystemet i de relevante delene de er ansvarlige for, inkludert sikkerhetsaspektene ved operasjonelle prosedyrer.
2.4.2.	Organisasjonen skal legge til rette for konsultasjon av personalet ved å tilby metoder og midler for å involvere personalet, registrere personalets mening og gi tilbakemelding på personalets mening.

2.4.2 Formål

Søker skal dokumentere at de aktivt involverer sitt eget personale (eller deres representanter), samt eksterne interessenter ved anvendelse og utvikling av sikkerhetsstyringssystemet for risikostyring over tid. Dette vil også gi vurderingsmyndighetene en indikasjon på hvordan sikkerhetskulturen er i organisasjonen, og hvor aktiv de involverer relevante tredjeparter i håndtering av sikkerheten i områder med delt risiko.

Organisasjonen innser at ingen enkeltpersoner alene besitter all den informasjonen som er nødvendig for å håndtere sikkerheten på en bærekraftig måte. Prosesseksperter, sikkerhetseksperter, støttetjenester, frontlinjepersonell, ledelse og arbeidsledere, fagforeninger, eksterne leverandører, besitter og anvender kunnskap og informasjon som er viktig for sikkerheten. De må gis anledning til å komme sammen for å drøfte og uttrykke sine synspunkter for å få en best mulig forståelse av hva som er realiteten på arbeidsplassen. Særlig oppmerksomhet er nødvendig ved de organisatoriske grensesnittene mellom tjenester, avdelinger og organisasjoner. Utvekslingen av ideer og informasjon om analyse og behandling av risiko, ulykker og hendelser bør fremmes.

Et miljø med tillit understøtter engasjement i rapportering av sikkerhetskritisk informasjon og deltakelse i analysering av farlige situasjoner og uønskede hendelser. I tillegg er det viktig med tidlig innspill fra driftspersonell når de utfører risikovurdering, designer eller bygger om tekniske installasjoner og nedtegner nye prosedyrer.

2.4.3 Forklarende merknader

Eksterne parter **(2.4.1)** betyr organisasjoner som har et grensesnitt med søkeren som entreprenører, partnere, leverandører, relevante offentlige etater, lokale myndigheter eller nødetatene.

Hvordan blir menneskelige og organisatoriske faktorer og sikkerhetskultur integrert?

Disse eksterne partene **(2.4.1)** kan konsulteres i saker som er relevante for styringssystemet. For eksempel kan leverandører være ansvarlig for noen sikkerhetsrelaterte oppgaver, som klargjøring av tog eller vedlikehold av infrastrukturen. Når prosedyrene for klargjøring av tog eller vedlikehold av infrastrukturen vurderes sammen med foreliggende risikoer, er det god en praksis at disse leverandørene er involvert i prosessen.

Sluttbrukernes ekspertise er viktig for å sikre en god forståelse av arbeidsforhold og prosedyrer, prosesser, verktøy og dokumentasjon i samsvar med deres formål. Konsultasjon av frontlinjearbeidere fra risikovurdering til valg og testing av dokumentasjon eller utstyr vil bidra til å utvikle bærekraftig og sikker ytelse (med bedre etterlevelse av personalet).

Utvikling av en positiv sikkerhetskultur fremmes av god kvalitet og betimelig kommunikasjon av relevant informasjon til dem det måtte gjelde.

2.4.4 Bevis

- *Søker skal fremlegge opplysninger om prosessen for konsultasjonspersonell (eller deres representanter) og relevante eksterne interessenter, herunder hvordan disse konsultasjonene settes ut i praksis med hensyn til endringer i sikkerhetsstyringssystemet eller spesifikke driftsprosedyrer;**(2.4.1), (2.4.2)***
- *Søker skal fremlegge informasjon om foreliggende system for tilbakemelding til personalet om utfallet av konsultasjonene.**(2.4.2)***

2.4.5 Eksempler på bevis

Prosessen eller prosedyren for konsultasjonspersonell (og hvis det er aktuelt, deres representanter) og interessenter i utviklingen av sikkerhetsstyringssystemet.

Det å ta hensyn til menneskelige og organisatoriske faktorer og forbedre sikkerhetskulturen vil ha en positiv innvirkning på samsvar med det relevante kravet til sikkerhetsstyringssystemet, og bevis på dette finnes i:

Eksempler på møtereferater etter konsultasjonsmøter med ansatte (og/eller deres representanter) og utfallet av dem.

Eksempler på hvordan meninger og forslag fra ansatte blir samlet når det skal gjøres endringer (f.eks. et utkast til/endret/ny driftsprosedyre) og hvordan de behandles.

Det fremlegges dokumentasjon/prosedyre som viser hvordan driftspersonalet, som skal håndtere et nytt eller utviklet teknisk system, blir involvert på et tidlig stadium (planlegging og utvikling) av arbeidet for å samle inn opplysninger, for eksempel om maskinens grensesnitt.

Prosedyrer som beskriver hvordan menneskelige og organisatoriske faktorer skal håndteres og utfallet formidles i organisasjonen relatert til organisasjonens forretningsmål og organisasjonsprosesser, for eksempel prosjekter, granskning av hendelser og ulykker, risikoanalyser og andre sikkerhetsrelaterte aktiviteter for eget personale, leverandører, samarbeidspartnere og leverandører.

Organisasjonen definerer klart sikkerhetsforventninger og påkrevd atferd. Organisatoriske prioriteringer blir tilpasset for å unngå motstridende målsettinger. En prosess for planlegging, risikovurdering og kontroll av aktiviteter for å sikre at sikkerheten ikke kompromitteres av andre forretningsinteresser er beskrevet, for eksempel ved bruk av konservativ beslutningstaking. Sikkerhetsmålsettinger er knyttet til sikkerhetskulturen. Ledelsen har en aktiv rolle i planleggingen og gjennomføringen av nødvendige endringer i sikkerhetskulturen.

2.4.6 Sjekkpunkter

Konsultasjon og involvering av relevant personell, både internt og eksternt, er en viktig del av å sikre at dem med relevant erfaring har en positiv innvirkning på organisasjonens sikkerhetsstyringssystem.

Tilsyn på dette området bør rettes mot historikk over hvordan personalet og eksterne parter blir konsultert og deres kommentarer tatt i betraktning, samt gi en oversikt over endringer i sikkerhetsstyringssystemet som stammer fra dette feltet

Det bør rettes spesiell oppmerksomhet mot hvordan tilbakemelding gis og hvordan man lærer fra dette.

3 Planlegging

3.1 Tiltak for å sette fokus på risiko

3.1.1 Lovbestemt krav

3.1.1. Risikovurdering

3.1.1.1. Organisasjonen skal:

(a) identifisere og analysere alle operasjonelle (inkludert menneskelige prestasjoner), organisatoriske og tekniske risikoer som er relevante for typen (karakteren), omfanget og området av operasjoner utført av organisasjonen. Slike risikoer skal omfatte slike som oppstår fra menneskelige og organisatoriske faktorer som arbeidsmengde, jobbdesign, tretthet eller egnethet av prosedyrer, og aktivitetene til andre interesserte parter (se 1. Organisasjonens driftskontekst);

(b) vurdere risikoene nevnt i bokstav a) ved å bruke hensiktsmessige risikovurderingsmetoder;

(c) utvikle og få på plass sikkerhetstiltak, med identifisering av tilhørende ansvar (se 2.3. Organisatoriske roller, ansvar, ansvarlighet og myndigheter);

(d) utvikle et system for å overvåke effektiviteten av sikkerhetstiltak (se 6.1. Overvåking);

(e) anerkjenne behovet for å samarbeide med andre interesserte parter (som jernbaneforetak, infrastrukturforvaltere, produsent, vedlikeholdsleverandør, enhet med ansvar for vedlikehold, jernbanekjøretøyets rettighetshaver, tjenesteleverandør og anskaffelsesenhet), der det er hensiktsmessig, om delte risikoer og innføring av tilstrekkelige sikkerhetstiltak;

(f) (kommunisere risikoer til ansatte og involverte eksterne parter (se 4.4. Informasjon og kommunikasjon).

3.1.1.2 Ved vurdering av risiko skal en organisasjon ta hensyn til behovet for å bestemme, sørge for og opprettholde et trygt arbeidsmiljø som er i samsvar med gjeldende lovgivning, særlig rådsdirektiv 89/391/EØF.

3.1.2. Planlegging for endring

3.1.2.1. Organisasjonen skal identifisere potensielle sikkerhetsrisikoer og passende sikkerhetstiltak (se 3.1.1. Risikovurdering) før implementering av en endring (se 5.4. Håndtering av endring) i samsvar med risikostyringsprosessen som er fastsatt i forordning (EU) nr. 402/2013, herunder vurdering av sikkerhetsrisikoer fra selve endringsprosessen.

3.1.2 Formål

Dette kravet går hjertet i sikkerhetsstyringssystemet, da det er rettet mot å få søkeren til å vise hvordan deres systemer identifiserer og håndterer risikoene de står overfor. Det krever også at søkeren viser hvordan de anvender utfallet fra risikovurderingen i praksis, for å forbedre risikostyringen og hvordan dette sjekkes over tid. Det er viktig å huske på at dette kravet ikke direkte handler om å håndtere risikoer fra endringer (som er et annet krav), men det er relatert til det. Det bør også merkes at det er et spesifikt krav om at risikovurdering

skal ta fatt i problemer relatert til menneskelig ytelse, for eksempel håndtering av jobbdesign og tretthetsrisiko.

Måten denne informasjonen er organisert og formidlet på som en del av sikkerhetsstyringssystemet, må beskrives av søker i søknaden, og innholdet bør gjenspeile de risikoene organisasjonen står overfor med hensyn til type, omfang og driftsområde (se driftskonteksten for organisasjonen). Det vil være hensiktsmessig å beskrive både risikoer der ansvaret hviler på søkeren, og risikoer som oppstår i forbindelse med tredjeparters aktiviteter.

En felles forståelse på tvers av organisasjonen av hvordan man kan forebygge store risikoer, anses som en prioritet for å oppnå god sikkerhetsstyring. Det at et scenario ikke forekommer ofte, bør ikke føre til at det blir ignorert. For å danne et mest mulig realistisk bilde av et bestemt scenario for risikostyring sammenlignet med realiteten, kan både sikkerhetsstyringseksperter og operatører i den mest utsatte delen av virksomheten bidra med sikkerhetsanalyse og risikovurdering. Resultatene fra disse vurderingene formidles i et tilgjengelig og forståelig format til alle aktører som bidrar til sikkerhet. Ledelsen åpner for drøftelser om store risikoer som må håndteres, for å sikre en felles forståelse av og bevissthet på disse. Videre er eksistensen av store risikoer fremhevet gjennom hele systemets virketid.

3.1.3 Forklarende merknader

Ved vurdering av søknaden skal søkeren vise hvordan de overholder Rådsdirektiv 89/391/EØF og korresponderende forordninger. Vurderingen vil fokusere på hvordan disse problemene løses, og ikke på selve problemene. Temaer som tretthet eller stresshåndtering, samt testing av fysisk og mental helse, kan håndteres rent juridisk innenfor rammene for arbeidsmiljø og sikkerhet, men de samhandler imidlertid med kompetansestyringssystemet (f.eks. for opptrening etter langtidsfravær) og med delegering av oppgaver (ansatte skal kun tildeles bestemte oppgaver hvis man mener de passer for dem), som angitt i TSI-OPE.

I pkt. 3.1.1.1 (a) i lovteksten ovenfor, hvor kravet gjelder infrastrukturforvaltere, erstattes «type» med «karakter» i forbindelse med vurderingen.

"Aktiviteter" **(3.1.1.1 (a))** viser her til både handlinger som interessenter (tjenesteleverandører, leverandører og andre) utfører på vegne av eller i forbindelse med en søker, samt aktiva som brukes for å utføre disse handlingene. Hovedpoenget er at søkeren må bevise at de har en robust prosess for risikovurdering, og at alle relevante risikoer håndteres. Enkelte risikoer (f.eks. hydrogeologiske risikoer, risiko ved planoverganger, stein som kastes på tog, inntrengere) må også tas i betraktning av organisasjonen når dette er hensiktsmessig og rimelig nødvendig. Disse problemene er imidlertid relatert til driftsmessige risikoer (siden de alle påvirker togdriften) og er kanskje ikke relatert til menneskelig yteevne.

"Andre interessenter" viser til både organisasjoner og enkeltpersoner. Dette kan være eksterne parter i forhold til jernbanesystemet **(1.1 (c))**.

En endring kan eller kan ikke være sikkerhetsrelatert **(3.1.2.1)**. Virkningen av eventuelle sikkerhetsrelaterte endringer må vurderes, og hensiktsmessige sikkerhetsforanstaltninger må identifiseres for å redusere de aktuelle risikoene til et akseptabelt nivå. Implementeringen av endringsstyringsprosessen kan også føre til sikkerhetsrisikoer, særlig når det besluttes å utsette implementeringen av en endring når det er nødvendig for å unngå at en annen sikkerhetsrisiko oppstår. Risikostyring **(3.1.1.1)** gjelder imidlertid ikke bare for endringsstyring. Generelt bør organisasjonen sørge for at sikkerhetsrisikoene som er knyttet til virksomheten behandles korrekt. Behovet for å identifisere, administrere og kontrollere disse sikkerhetsrisikoene som en del av søkerens sikkerhetsstyringssystem, går derfor videre enn endringsstyring og anvendelse av CSM vedrørende risikovurdering og annen vurdering.

CSM for risikoevaluering og -vurdering gjelder for alle tekniske, operasjonelle eller organisatoriske endringer (for sistnevnte de som har en drifts- eller vedlikeholdskonsekvens). For hver sikkerhetsrelatert endring, må søker/forslagsstiller først avgjøre om endringen er betydelig (eller ikke). Hvis den anses å være det, må det

bevises at risikoene knyttet til endringen er akseptabel ved bruk av prinsippene som beskrevet i CSM, og at kravene som utledes fra dette har blitt effektivt implementert i systemet i løpet av endringen. Risikovurderingen som gjennomføres må deretter vurderes et uavhengig vurderingsorgan eller anerkjent organ, som utarbeider en rapport om analysen er godkjent eller ikke. Nasjonale sikkerhetsmyndigheter vil vurdere slike rapporter i deres tilsynsaktiviteter, men kan ikke komme med innsigelser på resultatene i rapporten, med mindre de har grunn til å tro at prosessen med å vurdere risikovurderingen ikke har blitt fulgt som den skulle. Når endringen er sikkerhetsrelatert men ikke betydelig, må søker/forslagsstiller dokumentere sin beslutning, og det vil fortsatt være nødvendig å risikovurdere endringen ved anvendelse av sikkerhetsstyringssystemet. I så fall er det søkers ansvar å velge egnede risikovurderingsmetoder, for å fastslå at risikokontrolltiltakene som er etablert er hensiktsmessige for å kontrollere de aktuelle risikoene på et akseptabelt nivå. Det skal bemerkes at mens utløsende faktor for anvendelsen av CSM for risikovurdering og annen vurdering er om en endring er betydelig eller ikke, kan en organisasjon likevel velge å anvende CSM under noen omstendigheter, for eksempel hvis man føler at endringen av kommersielle eller samfunnsmessige årsaker fortjener en uavhengig vurdering av arbeidet organisasjonen har utført. Ytterligere informasjon om hvordan man håndterer betydelige endringer finner du i ERA Guide on the Common Safety Method for Risk Evaluation and Assessment.

CSM vedrørende risikovurdering og annen vurdering inneholder seks kriterier som bør undersøkes for å fastslå om endringen er betydelig. Disse er:

- ***feilkonsekvens**: troverdig skrekkscenario ved feil i systemet vurderes, der man tar i betraktning eksistensen av sikkerhetsbarrikader utenfor systemet;*
- ***ny teknologi tas i bruk ved gjennomføring av endringen**: dette gjelder både nyskapninger i jernbanesektoren, og det som er nytt bare for organisasjonen som gjennomfører endringen;*
- *kompleksiteten av endringen;*
- ***overvåking**: manglende evne til å overvåke den gjennomførte endringen gjennom hele virketiden og iverksette egnede tiltak;*
- ***reversibilitet**: manglende evne til å tilbakeføre systemet som det var før endringen; og*
- ***tilleggsvurdering**: vurdering av endringens betydning ved å ta i betraktning til alle de siste sikkerhetsrelaterte endringene i systemet, og som ikke ble vurdert som betydelige.*

Disse elementene kan brukes til å vurdere hvordan beslutninger om «betydning» under CSM for risikovurdering og annen vurdering som er gjort av organisasjoner er tatt.

Selv om risikostyringsprosessen som er fastsatt i CSM vedrørende risikovurdering og annen vurdering gjelder for sikkerhetsrelaterte og betydelige endringer, er prinsippene som ligger til grunn for risikostyringsprosessen som er fastsatt i forordningen vanlig praksis for risikostyring, og gjelder således kanskje ikke i alle andre situasjoner hvor det kreves risikovurdering.

Hvordan blir menneskelige og organisatoriske faktorer og sikkerhetskultur integrert?

Menneskelige og organisatoriske faktorer brukes konsekvent, fra starten av, når man designer (nye) systemer. Alle nivåer i organisasjonen, inkludert frontlinjeoperatører, involveres på en proaktiv måte i risikovurderingen, som forutsetter forekomst av feil gjennom en brukersentrert tilnærming hvor virksomhetens organisasjonsstruktur, tilgjengelighet/bruk av utstyr, utforming av sikkerhetsoppgaver, kompetansestyringssystem og prosedyrer vurderes med tanke på vurdering av sikkerhetsrisiko og identifisering av sikkerhetstiltak.

Risikovurderingsprosedyren vil inneholde tilnærminger eller metoder for systematisk å ta hensyn til menneskelige og organisatoriske faktorer og ta sikte på å fjerne risiko ved kilden i alle prosesser og prosedyrer i risikostyringssystemet, når det er mulig. Hvis det ikke er mulig, bør strategien for menneskelige og organisatoriske faktorer ta sikte på å minimalisere konsekvensene av risikoene.

Det er en systematisk tilnærming for å identifisere sikkerhetsrelaterte arbeidsoppgaver og prosesser, og metoder fra området innen menneskelige og organisatoriske faktorer brukes til å analysere sikkerhetskritiske oppgaver, f.eks. oppgaveanalyse, HTA, (hierarkisk oppgaveanalyse), TTA (oppgaveanalyse i tabellform). Det bør brukes profesjonell ekspertise på menneskelige og organisatoriske faktorer for å velge og anvende egnede metoder.

Risikovurderingsprosessen bør beskrive involveringen av menneskelige og organisatoriske faktorer og relevant kompetanse, for brukere og andre interessenter. Den kan for eksempel inneholde en beskrivelse av i hvilken grad ekspertise på menneskelige og organisatoriske faktorer skal være involvert i risikoanalyse, og i hvilken grad kompetanse på menneskelige og organisatoriske faktorer er nødvendig.

Det er beskrevet egnede metoder for å integrere menneskelige og organisatoriske faktorer i risikovurderinger, f.eks. oppgaveanalyse, brukbarhetsanalyse, simulering, Human-HAZOP, Bow Tie.

3.1.4 Bevis

- *Søkeren skal fremlegge bevis for at det foreligger en risikovurderingsprosess (inkludert beskrivelse av metodene som brukes, involvert personell og eventuell validering eller verifisering) som omfatter både risiko identifisert som betydelige endringer under CSM vedrørende risikovurdering og annen vurdering (Kommisjonens implementeringsforordning (EU) 402/2013) og risikoer som ikke anses som betydelige, men som likevel skal kontrolleres, og prosessen dekker alle driftsmessige, organisatoriske og tekniske risikoer.**(3.1.1.1.(a),(b))***
- *Bevis på at risikoer forbundet med menneskelige og organisatoriske faktorer er hensyntatt i risikovurderingene. Strategien for menneskelige og organisatoriske faktorer skal vise hvordan og når menneskelige og organisatoriske faktorer er en integrert del av risikovurderingsprosessen, samt vise anvendelsen av hensiktsmessige metoder og ekspertise;**(3.1.1.1(a))***
- *Bevis på måter å involvere relevante tredjeparter i risikovurderingsprosessen, herunder hvordan risikoer fra tredjeparter som påvirker jernbanevirksomhetens eller infrastrukturforvalterens aktiviteter, håndteres;**(3.1.1.1(a)), (3.1.1.1(e)), (3.1.1.1(f))***
- *Bevis på at søkeren har etablert en prosess for å utvikle og iverksette risikostyringstiltak, herunder hvem som er ansvarlig for å sikre at de gjennomføres;**(3.1.1.1 (c)).***
- *Søkeren må beskrive hvordan de involverer og formidler resultatene av risikovurdering og korresponderende kontrolltiltak til relevant personell;**(3.1.1.1(f))***
- *Søkeren skal vise hvordan effektiviteten av risikostyringstiltakene overvåkes, herunder hvordan prosesser eller prosedyrer oppdateres etter behov;**(3.1.1.1 (d))***
- *Sammen med beviset skal søkeren beskrive hvordan behovet for å overholde annen gjeldende lovgivning overholdes, som bestemmelsene i Rådsdirektiv 89/391/EØF;**(3.1.1.2)***
- *Søker fremlegger bevis for å vise som en del av endringsstyringsprosessen, at virkningen av enhver endring systematisk evalueres. Dette vil innebære bruk av risikovurdering, herunder bruk av CSM vedrørende risikovurdering og annen vurdering, for å identifisere risikoer og kontrolltiltak som kreves. Søker fremlegger også bevis på at kontrolltiltakene som ble identifisert under endringsstyringsprosessen har blitt gjennomført;**(3.1.2.1)***

3.1.5 Eksempler på bevis

En risikovurderingsprosess eller -prosedyre, inkludert hvordan og når Feilmodi og effektanalyse (FMEA), Identifikasjon og analyse av farlige og operasjonelle forhold (HAZOP) eller andre teknikker brukes til å understøtte gjennomføringen av kontrolltiltak for å håndtere risikofaktorer.

Bevis som et fareregister, som viser at organisasjonen har en prosess for systematisk å evaluere farer som det første trinnet i å håndtere risiko, som oppdateres av resultatene etter overvåking, umiddelbart oppdateres når nye risikoer oppdages, supplert med passende informasjon om sikkerhetstiltakene som er

vedtatt for å holde risikoen under kontroll (f.eks. teknisk utstyr, lister over sikkerhetskritiske komponenter, operasjonelle prosedyrer, opplæring av personalet).

Prosedyre for å overholde annen relevant EU-lovgivning, som for eksempel Rådsdirektiv 89/391/EØF, med hensyn til risiko knyttet til ansatte (død, midlertidig eller permanent personskade, nestenulykker) omfattes av lovverket om helse og sikkerhet i arbeidslivet, men det bør inngå eller tillegges kontrolltiltak i driftsreglene.

Det å ta hensyn til menneskelige og organisatoriske faktorer og forbedre sikkerhetskulturen vil ha en positiv innvirkning på samsvar med det relevante kravet til sikkerhetsstyringssystemet, og bevis på dette finnes i:

En oversikt over prosesselementene for hvordan menneskelige og organisatoriske faktorer tas i betraktning i risikovurderingsprosessen, og hvordan og hvor nødvendige tredjeparter er involvert. Møtereferater som viser at sluttbrukere og eksperter på menneskelige og organisatoriske faktorer deltok, og at deres meninger ble tatt i betraktning.

Eksempler på utførte analyser som tar for seg antall og art av oppgaver som skal utføres, deres kompleksitet, repetisjon, delegering av oppgaver, arbeidsmengden (inkludert tidsplan, skift, bruk av maskiner og relevante instruksjoner osv.), klarheten og grundigheten i regler og arbeidsinstrukser, tilbakemeldinger fra personalet og måten korrigerende tiltak iverksettes på.

Prosedyren for å formidle resultatene av risikovurderinger til ansatte, med illustrerende eksempler etter behov.

En beskrivelse av prosessen som sikrer at sikkerhetsrelaterte oppgaver som delegeres til hver bemanningskategori er utformet på en slik måte at:

- *Størrelsen på oppgavene som skal utføres ikke er for stor når en sikkerhetsrelatert oppgave utføres;*
- *Når sikkerhetsrelaterte oppgaver er kombinert, kan organisasjonen vise at sikkerhetsnivået opprettholdes;*
- *Det er ingen motsetninger mellom utførelsen av sikkerhetsrelaterte oppgaver og andre mål som er delegert til ansatte (i samsvar med 2.1.1 (j)).*

En strategi for menneskelige og organisatoriske faktorer knyttet til risikovurderingsprosessene. Dette viser at resultatene fra risikoanalyser blir brukt og sikkerhetsforbedrende tiltak implementeres og evalueres.

Noen menneskelige og organisatoriske faktorer som behandles innenfor det juridiske rammeverket for helse og sikkerhet, og viktige temaer som tretthet, arbeidsrelatert stress og fysisk arbeidsmiljø (f.eks. renslighet, temperatur, lys), i dette tilfellet arbeidshelse og sikkerhetsdokumentasjon bør administreres gjennom sikkerhetsstyringssystemet.

3.1.6 Referanser og standarder

- *Veileder for Byrået for anvendelse av CSM vedrørende risikovurdering*
- *Risikoakseptkriterier for tekniske systemer og driftsprosedyrer som anvendes i ulike bransjer*
- *Retningslinjer for gjennomføring av Forordning (EU) 2015/1136 om harmoniserte standarder (CSM DT) i virkeområdet til CSM vedrørende risikovurdering*
- *ISO 31000:2018 Risikostyring*
- *ISO 31010:2019 Risikostyring - Risikovurderingsteknikk*
- *ISO45001:2018 Sikkerhetsstyringssystemer for arbeidsmiljø og sikkerhet – en praktisk veileder for små organisasjoner*
- *CENELEC - EN50126 Jernbaneapplikasjoner — Spesifikasjon og demonstrasjon av pålitelighet, tilgjengelighet, vedlikeholdstilpasning og sikkerhet (RAMS) Del 1: Elementært, krav og generelt, prosess*
- *Organ for nasjonal jernbanesikkerhet — Veileder til aktivaforvaltning (2019)*

3.1.7 Sjekkpunkter

Risikovurderingsprosessen bør være sentral i sikkerhetsstyringssystemet når man gjennomfører tilsyn, og derfor bør det være mulig ut fra samtaler og kontroll av dokumentasjon og prosesser å finne ut om dette egentlig er realiteten. Eventuelle funn fra tilsyn som ville være relevant for fremtidig fornyelse av et felles sikkerhetssertifikat eller sikkerhetsgodkjenning, er av stor betydning. I tillegg kan eventuelle funn fra tilsyn med risikovurderingsprosesser, være innspill i tilsynsstrategien til nasjonale sikkerhetsmyndigheter.

Følgende informasjon kan fungere som innspill for senere tilsyn:

- *Fareliste;*
- *Resultater fra risikoanalyse, inkludert rapporter fra risikovurderingsorganet eller -organene der det er aktuelt;*
- *Begrunnelse for bruken av risikovurderingsmetoder (f.eks. FMECA, FTA, ETA, HAZOP), inkludert hvordan risikovurderingskriterier er fastsatt og hvordan alvorlighetsgrad og sannsynlighet er fastslått;*
- *Etter behov en klassifisering av farlige hendelser etter emne, effekter eller årsaker (f.eks. foreløpig fareliste).*

Ansatte med ansvar knyttet til risikovurdering bør være oppmerksomme på deres rolle og betydningen av prosessen, samt inneha kompetanse til å utføre oppgaven på en effektiv måte.

Det er spesielt viktig at flere eksempler på risikovurderinger undersøkes, da det av disse vil fremkomme om risikoene vurderes på riktig måte ved hjelp av egnede metoder. Feltobservasjon bør da påvise at de identifiserte kontrolltiltakene er på plass.

3.2 Sikkerhetsmålsettinger og planlegging

3.2.1 Lovbestemt krav

3.2.1. Organisasjonen skal etablere sikkerhetsmål for relevante funksjoner på relevante nivåer for å opprettholde og, der det er praktisk rimelig, forbedre sin sikkerhetsytelse.

3.2.2. Sikkerhetsmålene skal:

(a) Være konsistente med sikkerhetspolicyen og organisasjonens strategiske mål (der det er aktuelt);

(b) Være knyttet til de prioriterte risikoene som påvirker organisasjonens sikkerhetsytelse;

(c) Være målbar;

(d) Tar hensyn til gjeldende juridiske og andre krav;

(e) Bli gjennomgått med hensyn til deres prestasjoner og revidert etter behov;

(f) Være kommunisert.

3.2.3. Organisasjonen skal ha plan(er) for å beskrive hvordan den vil nå sine sikkerhetsmål.

3.2.4. Organisasjonen skal beskrive strategien og planen(e) som brukes til å overvåke oppnåelsen av sikkerhetsmålene (se Overvåking).

3.2.2 Formål

Sikre at organisasjonen oppfyller lovfestede krav og sikrer at konseptet om kontinuerlig forbedring i sikkerheten formidles til ansatte og at ledelsen står for dette.

Søkeren må vise at det foreligger meningsfylte målsettinger og en prosess for å gjennomføre og overvåke dem i løpet av deres virketid.

3.2.3 Forklarende merknader

Sikkerhetsytelse betyr her organisasjonens yteevne mot sikkerhetsmålene og sikkerhetsstyringssystemets ytelse, samt alle prosesser og prosedyrer som underbygger dette.

Begrepet "sikkerhetsmålsettinger" kan byttes ut med begrepet "sikkerhetsmål", men sistnevnte har vanligvis en numerisk betydning. Sikkerhetsmålsettinger eller sikkerhetsmål er forskjellige fra Felles sikkerhetsmål (CST) som er fastsatt på medlemsstatsnivå, men enkelte selskaper kan bruke sistnevnte som mål som skal nås for å opprettholde eller forbedre sikkerhetsytelsen.

Med PDCA-hjulet kan målene vurderes regelmessig, og resultatene av risikovurdering og tidligere overvåking bør tas i betraktning, samt granskning av ulykker og uønskede hendelser ved å angi prioriteringer for å opprettholde og forbedre sikkerhetsytelsen der det måtte være nødvendig.

Oppsettet og overvåkingen av sikkerhetsytelsesindikatorer som underbygger organisasjonens beslutninger om risikostyring, og om disse er effektive, er innspill for å sette opp og vurdere sikkerhetsmålsettingene.

Hvordan blir menneskelige og organisatoriske faktorer og sikkerhetskultur integrert?

Sikkerhetsmålsettinger er knyttet til risiko, da sistnevnte vil påvirke organisasjonens sikkerhetsytelse (dvs. tiltenkt resultat fra sikkerhetsstyringssystemet og dermed at målene nås på en vellykket måte). Sikkerhetsmålsettingene kan være kvantitative, representert ved en reduksjon av antall hendelser som en

absolutt verdi eller i prosent. Sikkerhetsmålsettingene kan også være kvalitative, uttrykt som en generell verdi som «sikkerheten på planoverganger vil bli forbedret» eller «det nåværende sikkerhetsnivået vil bli opprettholdt». I dette tilfellet vil imidlertid forbedringsnivået eller nivået som sikkerheten skal opprettholdes på, måtte defineres og overvåkes i henhold til noen definerte kriterier for å avgjøre om sikkerhetsmålene blir oppfylt.

Organisasjonen definerer SMART-mål og formidler disse til de ansatte for å utvikle deres bevissthet rundt relevansen og viktigheten av aktivitetene sine, og hvordan de bidrar til oppnåelsen av sikkerhetsmålsettinger og planlegging for å håndtere sikkerhetsrisikoer. Personalet er også klar over at måloppnåelsen overvåkes og gjennomgås når det er nødvendig.

Målene er prioritert i henhold til risikovurderingen, i tråd med hverandre og med sikkerhetspolicyen.

3.2.4 Bevis

- Det foreligger et sett av SMART-sikkerhetsmålsettinger som passer inn i organisasjonens bredere forretningsbehov;**(3.2.1), (3.2.2 (a),(b)),(c))**
- En redegjørelse som oppgir de lovfestede kravene og hvordan de overholdes;**(3.2.2 (d))**
- Beskrivelse av hvordan disse målene kan oppnås og formidles til relevant personale;**(3.2.2 (f)), (3.2.3)**
- Det foreligger en overvåkingsprosess som er i samsvar med kravene i CSM vedrørende overvåking (Forordning (EU) 1078/2012), for å sikre at de er forenelig med formålet, og for at organisasjonen kan oppnå sine mål.**(3.2.2 (e)), (3.2.4)**

3.2.5 Eksempler på bevis

Prosessen hvor sikkerhetsmålsettinger er prioritert og overvåket, og hvordan konflikter med andre målsettinger unngås, og hvis ikke, hvordan dette løses. Dette bør omfatte nivået målene er satt ved og hvordan de bidrar til andre mål på andre nivåer der dette er hensiktsmessig. Den bør også inkludere grensesnittene, timingen og eventuelle nødvendige støttende kvalitative eller kvantitative data.

Sikkerhetsmålsettingene og planen som leveres sammen med prosessen som skal følges når det ser ut til at sikkerhetsmålsettingene ikke kan nås.

Sikkerhetsmålene er i samsvar med misjon og visjon som er nedtegnet i sikkerhetspolicyen, og ut fra dette kan man se at de er verdsatt av personalet, og deres engasjement i å oppnå dem er styrket.

Prosessen eller prosedyren for å utarbeide resultatene fra overvåkingsaktiviteter til sikkerhetsmålsettinger, planlegging av tiltak for å nå dem og relaterte indikatorer for oppnåelse.

Det å ta hensyn til menneskelige og organisatoriske faktorer og forbedre sikkerhetskulturen vil ha en positiv innvirkning på samsvar med det relevante kravet til sikkerhetsstyringssystemet, og bevis på dette finnes i:

Organisasjonens strategiske plan setter sikkerhet som hovedmål.

Bestemmelser som er tilstede i sikkerhetsstyringssystemet (risikostyringsprosessen) som forklarer hvordan konflikter mellom mål skal håndteres.

En prosess for å konsultere ansatte om sikkerhetsmål og prosessen for å definere og kommunisere individuelle sikkerhetsmål, og hvordan de formelt aksepteres av personalet. Prosessen som forklarer hvor personalet kan finne målene, hvordan de får vite sitt forventede bidragsnivå til å nå disse målene og hvordan de vurderes/måles med hensyn til suksess, konstrueres og planlegges oppnådd, er nødvendig.

En prosedyre for kommunikasjon av mål til personalet viser hvordan bevissthet utvikles og forståelse kontrolleres.

I en rapporteringsprosedyre der personalet indikerer oppnåelse av sikkerhetsmål.

3.2.6 Sjekkpunkter

Et nøkkelspørsmål for tilsyn vil være hvor oppnåelige de fastsatte målene er i praksis, og hva som i realiteten skjer dersom det begynner å bli klart at de sannsynligvis ikke kan nås.

Hvordan sikkerhetsmålsettingene er fastsatt og vurdert - at målene fokuserer på sårbare eller kritiske aktiviteter/kontroller og anvender resultat- og aktivitetsindikatorer

Hvordan organisasjonen utviser kontinuerlig forbedring i risikostyring gjennom sine sikkerhetsmålsettinger.

Hvordan overvåker organisasjonen effektivt sikkerhetsytelsen, og således bruker CSM vedrørende overvåking for å vurdere ytelsen mot sikkerhetsmålsettinger og relaterte sikkerhetsresultatindikatorer.

Hvordan utvikler mål (f.eks. et mål definert flere år tidligere) seg fra opprettelse til endelig oppnåelse (eller mislykkes).

EUROPEAN UNION AGENCY FOR RAILWAYS

For et jernbanesystem som
fungerer bedre for samfunnet.

4 Støtte

4.1 Ressurser

4.1.1 Lovbestemt krav

4.1.1.	Organisasjonen skal sørge for ressursene, inkludert kompetent personell og effektivt og brukbart utstyr, som er nødvendig for etablering, implementering, vedlikehold og kontinuerlig forbedring av sikkerhetsstyringssystemet.

4.1.2 Formål

Formålet med dette kravet er å sørge for at organisasjonen har prosesser på plass for å tilveiebringe tilstrekkelige ressurser, som teknisk utstyr eller systemer eller kompetent personell, for å åpne for at sikkerhetsstyringssystemet kontrollerer risikoen i samsvar med målene.

4.1.3 Forklarende merknader

Tildeling av tilstrekkelige ressurser er en forutsetning for å oppnå et passende sikkerhetsnivå.

Hvordan blir menneskelige og organisatoriske faktorer og sikkerhetskultur integrert?

Selskapet sørger for at de nødvendige ressursene tilføres personalet for å utføre sine oppgaver på en sikker måte. Dette inkluderer bemanning, utstyr og dokumentasjon. Dette kravet er også knyttet til risikovurderingen og de identifiserte sikkerhetstiltakene.

4.1.4 Bevis

- *Informasjon om kompetansestyringssystemet (CMS) eller i tilfeller der et CMS ikke foreligger, man viser hvordan organisasjonen sikrer at den innehar tilstrekkelig kompetent personell;**(4.1.1)***
- *Informasjon om hvordan organisasjonen skal sørge for at den innehar nok effektivt og brukbart utstyr, slik at organisasjonen kan oppfylle sine tjenesteforpliktelser og for å opprettholde et effektivt sikkerhetsstyringssystem som kontrollerer risiko;**(4.1.1)***
- *Informasjon om organisering av vedlikeholdsfunksjoner (se også vedlegg II i ECM-forordning 2019/779) og hvordan dette er relatert til tilstrekkelig ressursforvaltning, slik at organisasjonen kan oppfylle sine tjenesteforpliktelser.**(4.1.1)***

4.1.5 Eksempler på bevis

Kompetansebehandlingsprosedyren eller detaljer om prosessen som skal sikre at organisasjonen har kompetent bemanning i relevante roller, med detaljert vurdering og opplæringsprogrammer etter behov **(se også 4.2)**.

En redegjørelse som beskriver prosessen for ressurstildeling for å oppfylle driftsmessige behov sammen med relevante referanser til støttedokumenter.

Det å ta hensyn til menneskelige og organisatoriske faktorer og forbedre sikkerhetskulturen vil ha en positiv innvirkning på samsvar med det relevante kravet til sikkerhetsstyringssystemet, og bevis på dette finnes i:

En redegjørelse for hvordan bemanningskravene fastsettes, slik at sikkerhetsstyringssystemet fungerer effektivt sammen med detaljer om relevante referanseprosedyrer eller prosesser der ytterligere informasjon kan bli funnet.

En prosess som forklarer hvordan ressurser allokeres som et resultat av risikovurderingen og sikkerhetstiltakene som er besluttet for å utføre en oppgave: inkludert tid, bemanning, kompetanse (inkludert ikke-tekniske ferdigheter), prosedyrer, verktøy og utstyr.

Resultatene av oppgaveanalyser som viser at riktig tid og bemanning er definert med tanke på arbeidsbelastning. Prosessen utføres på samme måte for alle sikkerhetsoppgaver i alle forretningsenheter ('langdistanse'/'kortdistanse' transporttjenester, lokførere, sporveksling, vedlikeholdsaktiviteter...).

Et dokument som beskriver de allokerte ressursene for planlagte endringer i organisasjonen (inkludert bemanning og tilveiebringelse av nødvendig utstyr).

4.1.6 Sjekkpunkter

Sjekk at kravene til kompetanse og utstyr er tydelig knyttet til resultatene fra risikovurderingen

Ved å sjekke CMS kan nasjonale sikkerhetsmyndigheter sjekke at organisasjonen har på plass midler for å identifisere og opprettholde personell med egnede ferdigheter slik at de kan utføre sine oppgaver på en trygg måte. Hvordan CMS-systemet holdes oppdatert er av sentral betydning.

Når man ser på vedlikeholdsaktiviteter som relaterer seg til dette kravet, bør tilsynsførende part søke å sikre at når disse aktivitetene utføres, at jernbanevirksomheten eller infrastrukturforvalteren utfører sin tilsynsfunksjon for å sikre at leverandørene leverer et produkt som er trygt å bruke.

Sjekk av gap i utvalgte områder i sikkerhetsstyringssystemet kan brukes som en indikator på om det er tilstrekkelig for menneskelige ressurser.

Måten utstyret brukes på, f.eks. hvor mange reservedeler som er medbragt til stedet, kan være en indikasjon på kvaliteten på det leverte utstyret og således indikere tilstrekkelige ressurser.

4.2 Kompetanse

4.2.1 Lovbestemt krav

4.2.1. Organisasjonens kompetansestyringssystem skal sikre at personell som har en rolle som påvirker sikkerheten, er kompetent i de sikkerhetsrelaterte oppgavene de har ansvar for (se 2.3. Organisatoriske roller, ansvar, ansvarlighet og myndigheter), herunder minst:

(a) identifikasjon av kompetansen (inkludert kunnskap, ferdigheter, ikke-teknisk atferd og holdninger) som kreves for sikkerhetsrelaterte oppgaver;

(b) utvelgelsesprinsipper (grunnleggende utdanningsnivå, psykologisk og fysisk form som kreves);

(c) innledende opplæring, erfaring og kvalifikasjoner;

(d) løpende opplæring og periodisk oppdatering av eksisterende kompetanse;

(e) periodisk vurdering av kompetanse og kontroller av psykologisk og fysisk form for å sikre at kvalifikasjoner og ferdigheter opprettholdes over tid.

(f) spesifikk opplæring i relevante deler av sikkerhetsstyringssystemet for å kunne klare sine sikkerhetsrelaterte oppgaver.

4.2.2. Organisasjonen skal tilby et opplæringsprogram, som nevnt i punkt (c), (d) og (f) i avsnitt 4.2.1, for ansatte som utfører sikkerhetsrelaterte oppgaver som sikrer at:

(a) opplæringsprogrammet leveres i henhold til identifiserte kompetansekrav og individuelle behov hos personalet;

(b) der det er aktuelt, sikrer opplæringen at personalet kan operere under alle driftsforhold (normale, reduserte og i nødstilfeller);

(c) varigheten av opplæringen og frekvensen av oppfriskningsopplæringen er egnet for opplæringsmålene;

(d) det føres journal for alle ansatte (se 4.5.3. Kontroll på dokumentert informasjon);

(e) opplæringsprogrammet blir jevnlig gjennomgått og revidert (se 6.2. Internrevisjon) og endringer foretatt ved behov (se 5.4. Endringsstyring).

4.2.3. Ordninger for å komme tilbake i arbeid etter ulykker og uønskede hendelser eller langtidsfravær for ansatte, herunder hvordan andre opplæringsbehov der det er behov, identifiseres.

4.2.2 Formål

Formålet med dette kravet er å sikre at organisasjonen har på plass hensiktsmessige strukturer og ressurser for å kontrollere risikoen de står overfor, slik at man kan sette ut bemanning med kompetanse til å oppfylle sikkerhetsfunksjonene, og da særlig sikkerhetskritiske funksjoner. Kompetansestyringssystemet vil også gi organisasjonen muligheten til å opprettholde kompetansen, kunnskapen og erfaringen til de ansatte over tid.

Kompetanse spiller en sentral rolle for å sikre at aktivitetene utføres på en tilfredsstillende måte. Behovet for å ha kompetent bemanning omfatter både frontlinjestøtte (inkludert leverandører, konsulenter og leverandører av sikkerhetsrelaterte tjenester) og ansatte i lederstillinger. Krav til ledelseskompetanse blir ofte oversett, men ledere treffer imidlertid viktige beslutninger som kan ha fundamental og omfattende innvirkning på helse og sikkerhet. Dette kan omfatte å sørge for opplæring av alle ansatte i henhold til relevante sikkerhetsstandarder, opprettholde kompetansen uavhengig av omstendighetene, herunder

problemer som tilgjengelighet på bemanning og overvåking av kompetansen i forhold til standarder som skal følges.

I denne sammenheng er sikkerheten sett på som en integrert del av profesjonell atferd og fagkompetanse - og ikke som et "ekstra lag" som skal legges på toppen av faglige ferdigheter. I tillegg vil kapasiteten til en organisasjon med hensyn til å håndtere i reelle omstendigheter med uventede hendelser, være avhengig av kompetansen til frontlinjepersonell og deres overordnede. Slik kompetanse kan for eksempel utvikles med simulering og regelmessig opplæring i komplekse scenarioer.

4.2.3 Forklarende merknader

Et opplæringsprogram **(4.2.2)** kan tilveiebringes via et tredjeparts kurssenter. I så tilfelle skal organisasjonen sørge for at kurssenteret innehar kompetansen til å levere de relevante tjenestene, enten fordi det er sertifisert eller anerkjent som et senter under en nasjonal eller europeisk ordning, eller ved direkte overvåking av opplæringen og resultatene den gir. Et kurssenter kan enten levere all eller bare deler av nødvendig opplæring til en organisasjon, basert på deres kompetanse på de ulike feltene. Der et tredjeparts opplæringssenter gir en organisasjon opplæring, må denne organisasjonen kontrollere at opplæringen dekker de nødvendige elementene, og der de ikke gjør det, bør de supplere slik ekstern opplæring med intern opplæring etter behov.

Hvordan blir menneskelige og organisatoriske faktorer og sikkerhetskultur integrert?

Kompetanse er en integrert del av kompetansestyringssystemet, inkludert ikke-tekniske ferdigheter, holdninger og atferd. Nødvendige nivåer av nødvendig kompetanse for å utføre en oppgave er definert med henvisning til risikovurdering og oppgaveanalyser.

"Holdning" **(4.2.1 (a))** brukes til å beskrive hvordan mennesker reagerer på bestemte situasjoner og hvordan de oppfører seg generelt (for eksempel å være på offensiven, ha evnen til å komme overens med andre mennesker). Dette er svært viktig for å kunne samkjøre ulike deler av arbeidet i sikkerhetsstyringssystemet.

Det er en systematisk tilnærming som sikrer at kompetanse på menneskelige og organisatoriske faktorer er tilgjengelig i relevante roller basert på risikovurdering og oppgaveanalyser.

Kompetansen ved menneskelige og organisatoriske faktorer kan for eksempel brukes i risikovurdering, i prosjekter i forbindelse med nye eller modifiserte design, ved prestasjonsvurderinger og forbedring for å gi et ikke-teknisk perspektiv, eller vedrørende problemer med menneskelig yteevne. Spesifikk opplæring i menneskelige og organisatoriske faktorer for å øke bevisstheten gis til ledelse og ansatte som utfører sikkerhetsoppgaver.

4.2.4 Bevis

- *Søker skal fremlegge opplysninger om deres kompetansestyringssystem og hvordan det fungerer for å oppfylle forholdene som er oppgitt i kravene;**(4.2.1),(4.2.2(a)-(e))***
- *Beviset skal omfatte detaljer om opplæringsprogrammene som er på plass for personalet (inkludert, der det er nødvendig, informasjon om organisasjonens krav til kompetanse til kursholdere) og hvordan dette holdes oppdatert og gjennomgås (inkludert når det er nødvendig for rollen som sikkerhetsrådgiver under RID eller når det er aktuelt for kompetansen til vedlikeholdspersonell i henhold til kravene i vedlegg I og vedlegg II til forordning (EU) 2019/779 om ECM, **(4.2.2 (a)-(e))**;*
- *Beviset skal inneholde gjeldende ordninger for å komme tilbake i arbeid etter ulykker og uønskede hendelser eller langtidsfravær, herunder hvordan andre opplæringsbehov identifiseres;**(4.2.3)***

- *Dersom søker bruker et anerkjent kurssenter som er sertifisert i henhold til EU-forordninger, vil en kopi av det aktuelle sertifikatet gi en indikasjon på samsvar med punktene ovenfor, i den grad de er dekket av sertifiseringsprosessen;**(4.2.1 (a), (c)-(f), (4.2.2)***
- *Søker må oppgi hvordan det sikres at det for de samme oppgavene ikke er noen forskjeller mellom kompetansen til eget personale og annet personell fra leverandører, tjenesteleverandører og konsulenter som brukes;**(4.2.1 (a) - (f))***
- *Egnet opplæring i menneskelige og organisatoriske faktorer og bevisstgjøring gis til ledelse og ansatte som utfører sikkerhetsoppgaver; **(4.2.1), (4.2.2)***
- *Søker må oppgi hvordan kompetansebehov for menneskelige og organisatoriske faktorer vurderes, herunder å definere i hvilke roller og i hvilke prosesser kompetanse for menneskelige og organisatoriske faktorer er nødvendig, og hvilket kompetansenivå som er nødvendig. Tilgjengelig kapasitet for menneskelige faktorer (for eksempel formelle kvalifikasjoner for menneskelige faktorer, dvs. faglig grad, intern/ekstern anerkjent kompetanse og erfaring) er skreddersydd og står i forhold til selskapets erfaring og kompleksitet.**(4.2.1 (a)-(f))***
- *Søkeren bør gi informasjon om prosessen for å autorisere ansatte til å påta seg nøkkelroller, inkludert den løpende ledelsen av personalets kompetanse **(4.2.1 (a)-(f), 4.2.2(d)**.*

4.2.5 Eksempler på bevis

Kompetansestyringssystemet med en forklaring på hvordan det fungerer over tid, inkludert for personell som ikke jobber i frontlinjen der det er hensiktsmessig, samt linker til dokumentasjonen som understøtter dette, inkludert de ulike opplæringsprogrammene og hvordan tredjeparts kurssentre administreres.

Kontraktsfestede avtaler (inkludert kompetanseområde) med sertifiserte kurssentre, sammen med bevis på sertifiseringen deres, tilbys.

Eksempler på opplæringsprogrammer for grupper av ansatte.

Det å ta hensyn til menneskelige og organisatoriske faktorer og forbedre sikkerhetskulturen vil ha en positiv innvirkning på samsvar med det relevante kravet til sikkerhetsstyringssystemet, og bevis på dette finnes i:

Prosessen som viser hvordan kravene og kvalifikasjonene, inkludert psykologisk eller fysisk form, som anses nødvendig for spesielle sikkerhetsrelaterte roller, håndteres og etterleves, inkludert en forbindelse til risikovurdering og oppgaveanalyser.

En prosess som viser hvordan personalkrav og kvalifikasjoner håndteres, både når det gjelder:

- *Overholdelse av gjeldende krav angående fysisk og psykologisk form;*
- *Definere faglig kompetanse som anses nødvendig for hver sikkerhetsrelaterte rolle.*

Prosesser for periodisk re-evaluering av krav og opplæringsprogrammer viser en oppdatert situasjon og er hele tiden i tråd med tekniske, operasjonelle og organisatoriske endringer.

I en prosedyren eller prosess for å sikre at ansatte har spesifikk og oppfølgende opplæring i følgende:

- *Forventede endringer som påvirker interne regler, infrastruktur, organisasjonsstruktur, osv.;*
- *Oppdateringer av delegerte oppgaver (f.eks. for lokomotivførere, nye ruter, nye lokomotiver, ny type tjeneste).*

Sikkerhetsstyringssystemet en som beskriver hvordan opplæringsbehov for sikkerhetsoppgaver er identifisert og implementert i henhold til de spesifikke rollene. Den prosessrelaterte informasjonen brukes til å lage opplæringsmateriell og bestemmelsene garanterer at involvert personale blir kjent med risikoene som er knyttet til deres aktiviteter.

En prosedyre for granskning av uønskede hendelser og ulykker, i den utstrekning de fokuserer på tiltak for å gjøre endringer i opplæringsprogrammer i lys av ulykker og uønskede hendelser, tidligere tilsyn, osv.

En prosess for å la personalet stille spørsmål ved prosedyrer og beslutninger og rapportere rutinemessige og unormale avvik.

Sikkerhetsstyringssystemet som beskriver hvilke mekanismer for kunnskapsdeling som finnes i organisasjonen.

Prosessen som sikrer at:

- *Kompetansen opprettholdes av tilstrekkelig praksis innen feltet (f.eks. for lokomotivførere, kjennskap til driftsforhold, togkategorier, trekkvogner, linjer og stasjoner) og/eller ved planlegging av spesifikk opplæring, særlig hvor det har vært langtidsfravær (f.eks. pga. sykdom) eller ulykke/uønsket hendelse.;*
- *Kompetanse evalueres med jevne mellomrom for å sikre at den oppnådde kompetansen opprettholdes;*
- *Nødvendige tiltak er truffet der det er oppdaget avvik eller uakseptabel atferd, som for eksempel der en person eller deler av utstyr er tatt ut av tjeneste for en periode, og mht. restriksjoner med hensyn til anerkjente ferdigheter hvor det ble identifisert manglende etterlevelse, spesifikk opplæring, osv.*
- *Det blir truffet egnede for ansatte etter ulykker og uønskede hendelser (f.eks. for lokomotivførere som kjører på stoppsignal, ulykke som involverer personer, osv. For eksempel at organisasjonen forsikrer seg om at en lokomotivfører er egnet til å bli satt inn i tjeneste igjen eller blir erstattet med lokomotivfører som er kompetent til å drive tjenesten som skal gis);*
- *Man har tatt til seg lærdom etter alvorlige ulykker eller andre uønskede hendelser, og dette blir meddelt, særlig når det oppdages nye risikoer som må håndteres på operativt nivå;*
- *At det er en overvåkingsprosess for kompetansestyringssystemet, inkludert for hvordan effektiviteten måles.*

Sikkerhetsstyringssystemet som forklarer hvordan ledelsen er opplært til å kunne gjennomføre risikovurderinger før beslutninger tas, inkluderer menneskelige og organisatoriske faktorer i deres daglige aktiviteter (risikovurdering, ytelsesevaluering, forbedring...)

En prosess for å sikre kontinuitet i virksomheten og prosessen for tilbake-til-arbeid-ordninger med kobling til kompetansestyringssystemet.

Opplæringsprogrammet som viser at bestemte opplæringsmetoder er identifisert i henhold til treningsmålene og treningskriteriene:

- *veiledning*
- *opplæring på jobb*
- *simulatorer*
- *kriseopplæring*
- *opplæring i teamressursledelse*

Prosessen for å sikre at personalet har passende kompetanse, inkludert identifisering av nødvendig kompetanse, er knyttet til risikovurdering. Denne etablerte prosessen viser at det er en systematisk tilnærming som bruker kompetanse innen menneskelige og organisatoriske faktorer for personalet som utfører risikovurdering og fastsetter påfølgende sikkerhetsroller og -kompetanser for å sikre at nødvendige ressurser og kompetanse blir tildelt.

Sikkerhetskulturkompetanse blir basert på en behovsanalyse. Behov for sikkerhetskulturkompetanse vurderes, og strategier for å sikre riktig kompetanse og ressurser, er tilkjennegitt. Ledelsen viser at de innehar grunnleggende kunnskaper om sikkerhetskulturen, og fremmer viktigheten av den.

En prosess for å sikre at entreprenører, samarbeidspartnere og leverandører oppfyller samme kompetansekrav. De kontraktsmessige ordningene (eller partnerskapsavtalene) som tar for seg disse kravene og overvåkingen av kontraktens (eller partnerskapets) ytelse.

4.2.6 Referanser og standarder

- *ISO10015:2019 «Quality Management Guidelines for Competence Management and People Development»*
- *ISO10018:2020 «Kvalitetsledelse — Veiledning for personellets medvirkning»*

4.2.7 Sjekkpunkter

Hvordan utfallet fra en risikovurdering er knyttet til en gjennomgang av CMS.

Når man ser på kompetansestyringssystemet, er det viktig å huske at det vil være kompetansekrav som strekker seg utover organisasjonens ansatte, og som gjelder for leverandører og annet personell.

CMS-systemet bør sjekkes for å se hvor oppdatert det er, og om opplæringen som er gjort i henhold til det gjenspeiler organisasjonens foreliggende behov.

Organisasjonen bør ha på plass midler for å sikre at innleid personell har kompetanse til å utføre arbeidet. Dette er gjelder spesielt der bemanningsbyråenes kontroll av kompetanse gjerne ikke er så grundig som man skulle ønske.

Kompetansen som kreves for direkte ansatte og innleid personell som utfører de samme oppgavene, bør være på samme nivå.

Det foreligger et system som sikrer at oppgaver og poster med et sikkerhetselement, inkludert sikkerhetskritiske oppgaver, blir identifisert.

Det er et robust og effektivt kompetansestyringssystem, herunder identifisering av kunnskap og ferdigheter som trengs, opplæring, vedlikehold og ressurser for kompetanse; prosesser for rekruttering, opplæring, vurdering, kompetanseovervåking og registerføring, som viser hvordan alt dette bidrar til å nå og opprettholde kompetansenivået.

Fokus på menneskelige faktorer - hva gjøres i organisasjonen for å vurdere fysisk og mental helse (f.eks. lokomotivførere og for andre ansatte som utfører sikkerhetskritiske oppgaver).

4.3 Bevissthet

4.3.1 Lovbestemt krav

4.3.1.	Toppledelsen skal sørge for at de og deres ansatte som har en rolle som påvirker sikkerheten er klar over relevansen, viktigheten og konsekvensene av deres aktiviteter og hvordan de bidrar til riktig anvendelse av og effektiviteten til sikkerhetsstyringssystemet, inkludert oppnåelse av sikkerhetsmål. (se Sikkerhetsmål og planlegging).

4.3.2 Formål

Bevissthet betyr å gjøre de ansatte klar over sikkerhetspolicyen til organisasjonen og hvordan de bidrar til sikkerhet innenfor organisasjonen, farene og risikoene som de må være klar over, og resultatene av undersøkelser av ulykker og hendelser. Begrepet omfatter også å gjøre personalet oppmerksom på konsekvensene av ikke å bidra til gjennomføringen at sikkerhetsstyringssystemet, både fra deres og organisasjonens ståsted. Hensikten med dette kravet er å løse problemstillinger i sikkerhetskulturen i organisasjonen. Det er opp til toppledelsen å sette dagsordenen og hav organisasjonen arbeider mot, og fastsette hvordan man skal arbeide. Personell som jobber i organisasjonen er underlagt ledelsen. Søker må vise hvordan slike temaer håndteres i sine prosesser og prosedyrer.

4.3.3 Forklarende merknader

Dette kravet er knyttet til menneskelige og organisatoriske faktorer. Ytterligere informasjon om menneskelige og organisatoriske faktorer finnes i Vedlegg 5.

4.3.4 Bevis

- *Søker må oppgi hvor i deres personalressurser eller andre prosesser nøkkelrollen personalet har i å nå målene til organisasjonen gjenspeiles, hvordan de søker å bekrefte dette og hvilke skritt de tar for å opprettholde og forbedre dette;**(4.3.1)(se også 2.3)***
- *Informasjon om funksjonen av kompetansestyringssystemet.**(4.3.1)***

4.3.5 Eksempler på bevis

Det å ta hensyn til menneskelige og organisatoriske faktorer og forbedre sikkerhetskulturen vil ha en positiv innvirkning på samsvar med det relevante kravet til sikkerhetsstyringssystemet, og bevis på dette finnes i:

En redegjørelse i sikkerhetspolicyen eller i annen dokumentasjon om bestrebelsene på god organisasjonsstyring, for å fremme sikkerhetskulturen i organisasjonen for å sikre risikostyring gjennom et styringssystem. Dokumentet må også oppgi rollen til alt personale når det gjelder å fremme sikkerhetspolicyen gjennom sine handlinger og gjennom å nå de fastsatte sikkerhetsmålene. Det er vedlagt linker til de spesifikke prosedyrene som har som formål å fremme disse ideene på tvers av organisasjonen.

Overvåkingsprosessen inkluderer et punkt om forståelse på tvers av organisasjonen av sikkerhetsstyringssystemet og viktigheten og risikobevisstheten til hver enkelt oppgave.

At det er jevnlige medarbeiderundersøkelser med fokus på sikkerhet som viser at ansatte forstår hvordan sin rolle passer inn i organisasjonens overordnede sikkerhetsmål.

Opplæringsprogrammene inkluderer forklaringer av risiko, sikkerhetstiltak og sikkerhetsmål for gjennomføring av oppgavene og deloppgavene.

I en prosedyre som ansatte, entreprenører eller andre interessenter kan følge for å rapportere risikoen de er utsatt for.

En redegjørelse som inneholder en indikasjon på hvordan organisasjonen fremmer sin tilnærming til sikkerhet, menneskelige og organisatoriske faktorer og sikkerhetskulturen overfor sine leverandører, samarbeidspartnere og tjenesteleverandører.

I kommunikasjon fra toppledelsen vedrørende målsettinger, enten i den hensikt å oppmuntre alle til å bidra til å nå målene, eller for å takke alle for en forbedret yteevne.

I informasjon som viser at mellomledelsen og operasjonell bemanning er involvert i sikkerhetsinitiativer for frontlinjen (arbeidsgrupper, fora, dedikerte dager med fokus på sikkerhet, opplæringsprogrammer for å utvikle bevisstheten om deres rolle i sikkerhetsstyringssystemet, etc.).

En beskrivelse av kommunikasjonskanalene og kanalene som brukes, og hvordan de integrerer menneskelige og organisatoriske faktorer.

I en prosess for utforming av prosedyrer som forklarer hvordan berørte ansatte er involvert og hvordan risikoer og sikkerhetstiltak tas i betraktning, samt den potensielle innvirkningen av manglende overholdelse på operasjonelle aktiviteter.

4.3.6 Sjekkpunkter

I samtaler med personalet vedrørende i dette, er det viktig å fastslå hvilken forståelse de har av de roller og ansvarsområder som gjelder for dem. Dette vil indikere om organisasjonen er i stand til å forstå betydningen av en effektiv organisasjonskultur eller bevissthet når det kommer til å opptre sikkert i henhold til sikkerhetsstyringssystemet.

Hvordan organisasjonen har grunnlagt sin nåværende kultur og hvilke skritt som skal tas for å forbedre og utvikle den, er viktige spørsmål ved tilsyn.

Sjekk overvåking av hvordan ansvar og mål for sikkerhet og helse, risikobevissthet, rapporteringskultur - man ser etter forsømmelser, feil, brudd og andre avvik, blir etterlevd.

4.4 Informasjon og kommunikasjon

4.4.1 Lovbestemt krav

4.4.1. Organisasjonen skal definere tilstrekkelige kommunikasjonskanaler for å sikre at sikkerhetsrelatert informasjon utveksles mellom de ulike nivåene i organisasjonen og med eksterne interesserte parter inkludert entreprenører, partnere og leverandører.

4.4.2. For å sikre at sikkerhetsrelatert informasjon når frem til de som tar vurderinger og avgjørelser, skal organisasjonen administrere identifisering, mottak, behandling, generering og spredning av sikkerhetsrelatert informasjon.

4.4.3. Organisasjonen skal sikre at sikkerhetsrelatert informasjon er:

(a) relevant, fullstendig og forståelig for de tiltenkte brukerne

(b) gyldig

(c) korrekt

(d) konsekvent

(e) kontrollert (se Kontroll på dokumentert informasjon)

(f) kommunisert før den trer i kraft

(g) mottatt og forstått

4.4.2 Formål

Etterlevelse av disse kravene er utformet for å vise at søkeren har vist i søknaden egnede midler foreligger for å identifisere sikkerhetsrelatert informasjon på ulike nivåer, og for å formidle dette til rett tid og til de riktige personene. At de foretar regelmessige undersøkelser for å sikre at gjeldende risikostyring forblir relevant og oppdatert, og kan identifisere nye trusler og muligheter fra ekstern påvirkning (politisk, sosialt, miljømessig, teknologisk, økonomisk og lovmessig). At de er i stand til å sikre at informasjonen når de korrekte ansatte (spesielt sikkerhetskritiske ansatte) innenfor organisasjonen som må reagere på den. Dette vil inkludere hvordan de leverer relevant sikkerhetsrelatert informasjon til andre interesserte parter som de har kontakt med.

4.4.3 Forklarende merknader

Organisasjonen spesifiserer hvilken type sikkerhetsrelatert informasjon som skal formidles, hvordan den skal formidles **(se også 4.5)**, overfor hvem og under hvilke forhold dette vil bli iverksatt og behandlet **(4.4.1)**. Sikkerhetsrelatert informasjon utveksles mellom ansatte som utfører oppgaver i organisasjonen, med underleverandører, samarbeidspartnere eller tjenesteleverandører, mellom jernbanevirksomheter og infrastrukturforvaltere og, der det er relevant, mellom infrastrukturforvaltere.

Det skilles mellom ulike typer informasjon:

- *Dokumentasjon for sikkerhetsstyringssystemet **(se også 4.5)**;*
- *Statisk informasjon som kreves fra infrastrukturforvalteren for å utforme jernbanedrift som driftsregler og egenskaper ved jernbaneinfrastrukturen (f.eks. sporvidde, toglengde, stigningsvinkler og akselbelastning);*
- *Informasjon som kreves for planlegging av jernbanedriften, for eksempel rutetabeller, rutelister, midlertidige hastighetsbegrensninger, endringer i jernbaneinfrastrukturen, pågående jernbanearbeid, begrensninger i sporvidde, tog som skal omdirigeres fra den planlagte ruten, deler*

av linjen som skal brukes som enkeltspor, rutemeldinger (inkludert eventuelle endringer i togruter og/eller pendlingstjenester);

- *Informasjon om togtrafikkstyring (mellom jernbanevirksomheter og infrastrukturforvaltere og, der det er relevant, mellom infrastrukturforvaltere), herunder identifisering av kompetent bemanning i hver organisasjon som kan kontaktes i tilfelle nedsatt drift eller nødsituasjoner **(se også 5.5)**, i og utenfor hovedarbeidstiden.*

Grunnleggende krav til utveksling av opplysninger **(4.4.2)** er identifisert i TSI-OPE mellom jernbanevirksomheten og infrastrukturforvalteren i ECM-forordningen mellom jernbanevirksomheten og ECM, i CSM vedrørende sikkerhetsstyringssystemkrav mellom jernbanevirksomheten/infrastrukturforvalteren og myndighetene (Byrået, NSA).

Det er på plass ordninger for utveksling av informasjon med relevante parter angående sikkerhetsrisikoer knyttet til defekter og konstruksjonsavvik eller funksjonsfeil i tekniske systemer, inkludert de i strukturelle delsystemer, inkludert informasjon om eventuelle korrigerende tiltak for eksempel gjennom SAIT (Safety Alert Tool) system som Byrået har fremmet med jernbanesektoren. Bruk av SAIT oppfyller forpliktelsen fastsatt i jernbanesikkerhetsdirektivet (artikkel 4(5)) og kravet i CSM om overvåking (artikkel 4) og forordningen om vedlikeholdsansvarlige (artikkel 5(5) om å utveksle slik informasjon).

«Gyldig» i ovennevnte sammenheng **(4.4.3 (b))** betyr oppdatert.

"Konsekvent" i ovennevnte sammenheng **(4.4.3 (d))** betyr at noe ikke er motstridende hvis det kommer fra forskjellige kilder.

"Forstått" i ovennevnte sammenheng **(4.4.3 (g))** betyr at søkeren viser at de har gått til nødvendige skritt for å sikre at sikkerhetskritisk informasjon er innforstått av dem den er rettet mot. Dette kan gjøres direkte ved å stille kontrollspørsmål ved orienteringsmøter eller i sikkerhetskritisk kommunikasjon ved bruk av protokoller, om situasjoner som krever at viktige meldinger blir bekreftet flere ganger, f.eks. mellom signalgiver og lokomotivfører, for å bekrefte at de har blitt riktig forstått, eller ved hjelp av andre midler som oppfyller kravet.

Dette kravet er knyttet til menneskelige og organisatoriske faktorer. Mer informasjon om menneskelige og organisatoriske faktorer finnes i Vedlegg 5.

4.4.4 Bevis

- *Søker beskriver ulike kommunikasjonskanaler som brukes i organisasjonen og formålet med disse;**(4.4.1)***
- *Søker må fremlegge bevis på f.eks. internt sikkerhetsvarslingssystem, eventuelle systemer som gir bemanningen relevant og rutinemessig informasjon, og eventuelle systemer som gir bemanningen relevant informasjon og ad hoc-informasjon;**(4.4.2)***
- *Søker må beskrive hvordan de kan få bekreftet at informasjonen som har blitt formidlet har nådd ut til dem den er ment for (spesielt de som har sikkerhetskritiske roller), og at den har blitt forstått av dem den er ment for.**(4.4.3)***

4.4.5 Eksempler på bevis

Prosessen/prosedyren for å sikre at eksterne parter, som infrastrukturforvalter(e), (andre) jernbanevirksomheter, myndigheter etc., får oppgitt en kontaktperson som kan kommunisere med dem (f.eks. språkferdigheter) og som har tilgang til omfattende informasjon.

Prosessen eller prosedyren for at sikkerhetsrelaterte dokumenter bekreftes mottatt.

For roller som er betrodd administrasjon av samhandling: Bevis på hvem sikkerhetsvarselet sendes til, avhengig av driftsområdet (f.eks. sikkerhetsalarmene i ruteboken eller informasjon om forsinkelser);

Det å ta hensyn til menneskelige og organisatoriske faktorer og forbedre sikkerhetskulturen vil ha en positiv innvirkning på samsvar med det relevante kravet til sikkerhetsstyringssystemet, og bevis på dette finnes i:

I en klar redegjørelse om hvordan kommunikasjon både oppover og nedover for ulike informasjonstyper og -nivåer fungerer, herunder koblinger til spesifikke prosedyrer for sikkerhetsvarsler og rutinekommunikasjon.

I en prosess eller prosedyre som beskriver hvilke skritt som er tatt for ulike kommunikasjonstyper for å sikre at den når ut til dem den er ment for, og at dem den er ment for forstår hva som blir kommunisert, da for eksempel sikkerhetskritisk informasjon.

Prosessen eller prosedyren som sikrer at hver medarbeider som er involvert i en sikkerhetsrelatert oppgave, har riktig versjon av dokumentene til rett tid, for å sikre involvering og evne til raskt å handle eller reagere i normale, mindre gode og i nødssituasjoner.

TSI OPE inneholder krav til ulike dokumenter, inkludert noen som refererer til kommunikasjon mellom jernbaneforetakenes og infrastrukturforvalternes ansatte. Det er en bevissthet om alle disse dokumentene (regelbok, rutebok, rutetider, skjemabøker ...), og de inneholder settet med kommunikasjonsprotokoller eller medier for tydelig og raskt å utveksle formalisert informasjon som påvirker driften, spesielt for togbevegelser i mindre optimal modus.

Sikkerhetsvarsler som skal utveksles i organisasjonen eller med andre interessenter. Typiske eksempler:

- *Jernbanevirksomheten gir informasjon til infrastrukturforvalter om forhold som kan ha negativ innflytelse på togdriften (feil på rullende materiell, f.eks. akselbokser, slik at infrastrukturforvalteren kan måtte treffe risikobegrensende tiltak som stopp av trafikk på tilstøtende spor).*
- *Infrastrukturforvalter gir informasjon om infrastrukturfeil og eventuelle midlertidige sikkerhetsforanstaltninger som hastighetsreduksjon, til alle jernbanevirksomheter som opererer i det aktuelle området.*

Prosessen eller prosedyren for å formidle informasjon om større eller mindre endringer i organisasjonsstrukturen i organisasjonen.

Kopier av instruksjonene som er gitt til dem som utfører sikkerhetsrelaterte oppgaver og følger driftsregler som er relevante for nettet/nettene, som er:

- *Fullstendige: Alle regler og krav som er relevante for sikkerhetsoppgaver som er relevante for driften av jernbanevirksomheten, identifiseres og innarbeides i aktuell dokumentasjon;*
- *Nøyaktige: Hver av reglene og kravene er korrekt innarbeidet og uten feil (f.eks. hva man skal gjøre før et signal, sikkerhetsrelatert kommunikasjon);*
- *Konsekvent: Kravene som gjelder for en enkeltperson eller et enkelt arbeidslag fra forskjellige kilder, må være forenelige og konsekvente, og ikke motstridende.*

Prosessen for å registrere informasjon er etablert i de relevante interne reglene, ved bruk av passende kommunikasjonskanal.

Opplæringsprogrammene identifiserer hvordan kommunikasjon styres og hvordan kommunikasjonsferdigheter er integrert i kompetansestyringssystemet.

Rapporteringsprosessen som gjør det mulig for ansatte å rapportere om sikkerhetsspørsmål innenfor rettferdig kulturpoliicy, forklarer hvordan denne tilbakemeldingen blir analysert og verdsatt slik at latente systemfeil kan sees og vurderes i risikostyringsprosessen. Prosessen inkluderer også måten tilbakemeldingen på rapportering gis til ansatte.

Prosedyren som forklarer de ulike møtetypene og relevante resultater (f.eks. møtereferater, notater, …), viser hvordan sikkerhetskommunikasjon styres både opp og ned i hele selskapet.

4.4.6 Sjekkpunkter

Sjekk at det foreligger teknikker og prosesser som brukes til å holde seg oppdatert i risikostyring, foreta regelmessige undersøkelser for muligheter eller trusler.

Sjekk at det foreligger en prosess for å overvåke bruken av formell informasjon.

Ved tilsyn er det viktig å vite hvor oppdatert informasjonen er og om den når **alle** relevante medarbeidere til rett tid, for eksempel dem som er på nattskift eller dem som jobber langt borte fra organisasjonens hovedkvarter.

4.5 Dokumentert informasjon

4.5.1 Lovbestemt krav

4.5.1. Dokumentasjon til sikkerhetsstyringssystem

4.5.1.1. Det er en beskrivelse av sikkerhetsstyringssystemet, inkludert:

(a) identifisering og beskrivelse av prosessene og aktivitetene knyttet til sikkerhet ved jernbanedrift, inkludert sikkerhetsrelaterte oppgaver og tilhørende ansvar (se 2.3. Organisatoriske roller, ansvar, ansvarlighet og myndigheter);

(b) samspillet mellom disse prosessene;

(c) prosedyrene eller andre dokumenter som beskriver hvordan disse prosessene implementeres;

(d) identifisering av entreprenører, partnere og leverandører med en beskrivelse av type og omfang av leverte tjenester;

(e) identifisering av kontraktsmessige ordninger og andre forretningsavtaler, inngått mellom organisasjonen og andre parter identifisert under (d), som er nødvendige for å kontrollere sikkerhetsrisikoen til organisasjonen og de som er knyttet til bruken av entreprenører;

(f) henvisning til dokumentert informasjon som kreves i denne forordningen.

4.5.1.2. Organisasjonen skal sørge for at en årlig sikkerhetsrapport sendes til den eller de relevante nasjonale sikkerhetsmyndighetene i samsvar med artikkel 9 nr. 6 i direktiv (EU) 2016/798, inkludert:

(a) en syntese av beslutningene om betydningsnivået til de sikkerhetsrelaterte endringene, inkludert en oversikt over vesentlige endringer, i samsvar med artikkel 18 nr. 1 i gjeldende artikkel 18 nr. 1 i forordning (EU) nr. 402/2013;

(b) organisasjonens sikkerhetsmål for påfølgende år og hvordan alvorlige sikkerhetsrisikoer påvirker innstillingen av disse sikkerhetsmålene;

(c) resultatene av intern etterforskning av ulykker/hendelser (se 7.1 Lære av ulykker og hendelser) og andre overvåkingsaktiviteter (se 6.1 Overvåking, 6.2 Internrevisjon og 6.3 Ledelsens gjennomgang), i samsvar med artikkel 5(1) i forordning (EU) nr. 1078 /2012;

(d) detaljer om fremskritt med å adressere utestående anbefalinger fra de nasjonale etterforskningsorganene (se 7.1 Lære av ulykker og hendelser);

(e) organisasjonens sikkerhetsindikatorer angitt for å evaluere organisasjonens sikkerhetsytelse (se 6.1 Overvåking);

(f) der det er aktuelt, konklusjonene i årsrapporten til sikkerhetsrådgiveren som referert til i RID om organisasjonens aktiviteter knyttet til transport av farlig gods.

4.5.2. Opprette og oppdatere

4.5.2.1. Organisasjonen skal sørge for at det ved opprettelse og oppdatering av dokumentert informasjon knyttet til sikkerhetsstyringssystemet, brukes tilstrekkelige formater og medier.

4.5.3. Kontroll på dokumentert informasjon

4.5.3.1. Organisasjonen skal kontrollere dokumentert informasjon knyttet til sikkerhetsstyringssystemet, særlig dets lagring, distribusjon og kontroll av endringer, for å sikre tilgjengelighet, egnethet og beskyttelse der det er hensiktsmessig.

4.5.2 Formål

Søker må bevise at sikkerhetsstyringssystemet generelt sett er tilstrekkelig for typen og omfanget av tjenestene som drives, og at det er i stand til å håndtere risikoer som kan oppstå. Dette krever:

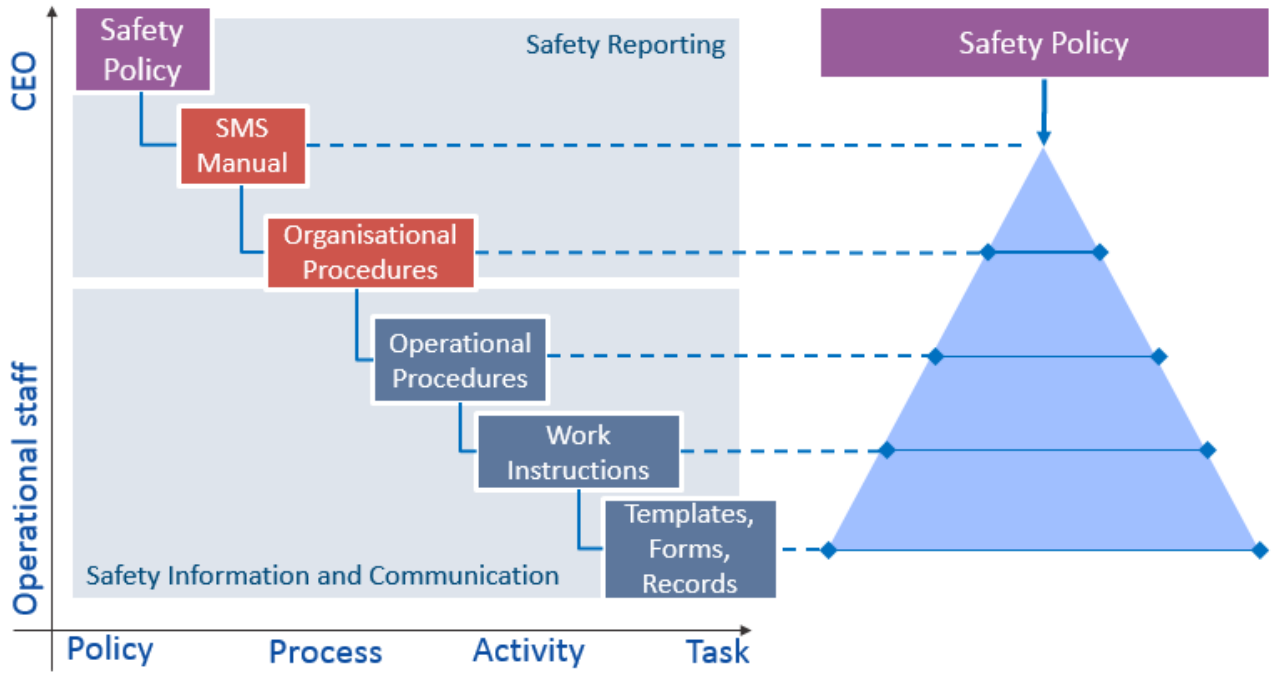
- *En forklaring av søkerens sikkerhetspolicy, organisering og gode ordninger i sikkerhetsstyringssystemet; og*
- *Mer detaljerte ordninger som fastsatt i ovennevnte krav i paragrafene 4.5.1.1 (a) til (f) og 4.5.1.2 (a) til (f).*

Søker skal også vise hvordan dokumentasjonen for sikkerhetsstyringssystemet administreres, dvs. identifisering, opprettelse, vedlikehold, håndtering, lagring og oppbevaring av dokumentert informasjon (dvs. dokumenter og poster/data), for å sikre at den er oppdatert og at riktige versjoner er tilgjengelig for relevant personell når det er nødvendig.

4.5.3 Forklarende merknader

Eventuelle dokumenter der søker viser at sikkerhetsstyringssystemets samsvar med gjeldende krav **(4.5.1.1 (f))** er en del av den dokumenterte informasjonen til sikkerhetsstyringssystemet.

Følgende Figur 3 viser en typisk dokumentasjonsstruktur:



Figur 3: Typisk dokumentasjonsstruktur:

Avhengig av driftsområdet kan jernbanevirksomhetene sende inn ulike rapporter **(4.5.1.2)** til de nasjonale sikkerhetsmyndighetene i medlemsstatene der de driver virksomhet. Generelt vedrører omfanget av rapporten bare den delen av driften som foregår i den respektive medlemsstaten. Byrået anbefaler imidlertid at denne rapporten dekker hele driftsområdet, da dette kan lette utvekslingen av informasjon mellom nasjonale sikkerhetsmyndigheter som fører tilsyn med jernbanevirksomheten.

Årsrapport fra sikkerhetsrådgiver **(4.5.1.2 (f))** med hensyn til transport av farlig gods, i henhold til Direktiv 2008/68/EF med endringer og RID, årsrapport fra sikkerhetsrådgiver for farlig gods er også et innspill for den

årlige sikkerhetsrapporten. Sikkerhetsrådgiveren er pålagt å oppfylle bestemte funksjoner, herunder å rådgi virksomheten som utnevnte vedkommende, med hensyn til helse, miljø og sikkerhet i forbindelse med transport av farlig gods og utarbeidelse av nødvendige rapporter.

Identifikasjon, format (f.eks. språk, programvareversjon og grafikk) og medium (f.eks. papirbasert, elektronisk) som brukes til dokumentert informasjon **(4.5.2.1)** bestemmes etter organisasjonens skjønn. Dette trenger ikke å være i form av en papirbasert håndbok.

Hvordan blir menneskelige og organisatoriske faktorer og sikkerhetskultur integrert?

Dokumentkontrollen **(4.5.3.1)** betegner prosessen (eller prosedyren) som spesifiserer internkontroller, særlig gjennomgang og godkjenning for tilstrekkelighet før utstedelse og bruk, som må vurderes og implementeres for informasjon som skal dokumenteres. Den tar sikte på å identifisere gjeldende revideringsstatus på dokumentasjonen, for å hindre at det anvendes ugyldige eller foreldede dokumenter. Dette vil spesifikt sikre at:

- *Relevante utgaver av aktuelle dokumenter er tilgjengelige på alle steder der det utføres aktiviteter der det er avgjørende at sikkerhetsstyringssystemet fungerer effektivt;*
- *Ugyldige eller foreldede dokumenter blir straks tatt ut av bruk, eller på annen måte sikret mot utilsiktet bruk;*
- *Alle foreldede dokumenter som oppbevares for juridiske formål eller for kunnskapens del identifiseres deretter.*

4.5.4 Bevis

- *Søker skal komme med en beskrivelse av sikkerhetsstyringssystemet og hvordan det fungerer med egnet skilting ved relevante prosedyrer når det er nødvendig;**(4.5.1.1 (a) - (c))***
- *Søkeren bør angi hvem dens entreprenører, leverandører og partnere er og hvordan relasjonene kontrolleres og overvåkes for å sikre at sikkerhetsrisikoer både for søkeren og de som den har kontraktsforhold med, blir håndtert for å ivareta sikkerheten **(4.5.1.1 (d), (e))**.*
- *Søkeren bør oppgi relevante prosedyre(r) som viser at den kan kontrollere dokumentert informasjon **(4.5.1.1 (f))***
- *Søker skal beskrive foreliggende roller og ansvar i forhold til sikkerhetsrelaterte oppgaver, og hvordan risikoen fra søkers og andre aktiviteter håndteres;**(4.5.1.1 (a))***
- *Søker skal fremlegge bevis på at de har (eller har ordninger på plass for å utarbeide) en årlig sikkerhetsrapport som dekker punktene som er oppført i 4.5.1.2 ovenfor;**(4.5.1.2 (a)-(f))***
- *Søker skal beskrive hvordan dokumentstyringssystemet fungerer, blant annet hvordan informasjonen blir tilgjengeliggjort og er egnet for bruk hvor og når det er nødvendig, hvordan informasjonen endres på en kontrollert måte i systemet og hvordan den lagres og vedlikeholdes på en slik måte at den er lett å hente frem. Informasjonen i dokumentstyringssystemet bør i tillegg oppbevares på en tilstrekkelig beskyttet installasjon for å minimere risikoen for forringelse eller skade, og for å hindre tap.**(4.5.2.1), (4.5.3.1)***

4.5.5 Eksempler på bevis

En beskrivelse av sikkerhetsstyringssystemet, strukturen av det og linking til dokumentene som omhandler prosessene deri (f.eks. håndbøker, organisatoriske og operative prosedyrer, arbeidsinstrukser). Selv om ISO har lansert et nytt konseptet med dokumentert informasjon, kan organisasjonen fortsette med den foreliggende dokumentasjonsstrukturen, dersom den er egnet for formålet.

En oversikt over hvordan de ulike dokumentene er strukturert, publisert, tilgjengeliggjort, arkivert, vedlikeholdt/revidert og opphevet med henvisning til relevante dokumentkontrollprosedyrer.

Prosedyren for å utarbeide årsrapporten sammen med en kopi av en tidligere versjon, hvis søkeren er ny, angir prosedyren foreslått oppsett av rapporten.

Oppbevaringstider for dokumenter og registre er fastsatt, dokumentert og overholdt.

Det å ta hensyn til menneskelige og organisatoriske faktorer og forbedre sikkerhetskulturen vil ha en positiv innvirkning på samsvar med det relevante kravet til sikkerhetsstyringssystemet, og bevis på dette finnes i:

Dokumenthåndteringsprosessen eller -prosedyren som beskriver hvordan dokumenter oppdateres etter regelmessig gjennomgang, samt etter ulykker eller uønskede hendelser. Prosessen eller prosedyren som beskriver opptrappingsprosessen i tilfeller der avtalte oppdateringer ikke har funnet sted innenfor den fastsatte tidsrammen, eller hvor det ikke er enighet om hvordan dokumentet skal oppdateres.

At det er et konsist språk (dvs. bruk av korte, klare setninger og unngå sjargong) anvendes for en bedre felles forståelse og god datakvalitet.

Der det måtte være av praktisk betydning, kan endringene fremheves i dokumentet eller eventuelle vedlegg for å lette gjennomgangen og godkjenningen i tillegg til at ansatte forstår dem.

Prosessen for utforming av prosedyrer forklarer hvordan den tar hensyn til menneskelige og organisatoriske faktorer, for eksempel:

- *Innhold og relevans: relevans for oppgaven utført av personen/personene, inkludert hvordan frontlinjeoperatørene er aktivt involvert i utformingen av disse prosedyrene;*
- *Flyt: hvordan beskrivelsen av prosesser og relevante ansvarsområder (hvem gjør hva) er definert, støttet av flytskjemaer;*
- *Omfang: integrering av bredere driftsscenario for å sikre forståelse av inngående og utgående informasjon for oppgaven som skal utføres;*
- *Grensesnitt: inneholder uttømmende identifikasjon og beskrivelse av grensesnitt. Det er klart når prosedyren skal brukes og når den ikke lenger er aktuell på grunn av endringer i oppgaven eller arbeidssituasjonen. Klare formål og omfangsregler for anvendelse av prosedyren;*
- *Gyldighet: oppdatert og gitt i tide for håndhevelse;*
- *Tilstrekkelighet og helhet: tilstrekkelig for hvordan arbeidet skal utføres og omfatter alle detaljer som er nødvendige*
- *Bevissthet: personalet har god forståelse for eksisterende prosedyrer/regler/krav, personalet har forståelse for sikkerhetsårsakene til prosedyrene og den potensielle innvirkningen av manglende etterlevelse på operasjonelle aktiviteter.*
- *Handling/respons: prosedyrer viser tydelig hvilken handling som følger av hver kommunikasjon og forventet respons*
- *Prestasjon under stress/nødsituasjon: prosedyrer er enkle å utføre under stress i en nødsituasjon*
- *Fleksibilitet: prosessene gir fleksibilitet for de ansatte til å reagere i nødstilfeller for å minimere de negative konsekvensene.*
- *Personalkonsultasjon: Personalet blir konsultert under utviklingen av prosedyrene – de vet best hvordan de skal få jobben gjort – og kan gi kommentarer eller alternative løsninger.*
- *Testperiode: prosedyren gjennomgår en testperiode, med gjennomgang av utfallet før ikrafttredelse.*
- *Revisjon: effektiviteten av prosedyren er gjenstand for periodisk gjennomgang, og gjennomgangen tar hensyn til resultatene av overvåking, revisjoner og erfaringer fra tidligere hendelser. Den er orientert mot kontinuerlig forbedringsånd og organisatorisk læring.*
- *Endringsledelse: Prosedyrer gjennomgås i tilfelle nytt utstyr eller nye prosesser kommer inn. Håndtering av endring i prosedyrer er viktig fordi det gjør det mulig å tilpasse dem til selskapenes mål og ordninger og sikre at de relevante risikoene håndteres.*

Personalet som har myndighet til å godkjenne dokumenter for utstedelse, sørger for at innholdet er nøyaktig og at det kan forstås av alle sluttbrukere (eller mottakere) det måtte gjelde.

4.5.6 Referanser og standarder

- *Veiledning til kravene til dokumentert informasjon i ISO 9001:2015, ISO/TC 176/SC2/N1286*

4.5.7 Sjekkpunkter

Sjekk at kontraktsforholdene åpner for en effektiv overvåking og risikostyring i organisasjonen (dvs. ved outsourcing av tjenester).

Noe som er av vesentlig betydning når det skal gjennomføres tilsyn, er å fastslå hvordan forholdet mellom dem som administrerer dokumentstyringssystemet og dem som har ansvaret for å oppdatere informasjonen, og at disse opprettholder kommunikasjonen med hverandre, fungerer i praksis. Det er på dette nivået at et sammenbrudd i kontrollen av dokumentasjon ofte kan oppstå, siden det er sannsynlig at de to delene av prosessen er i to forskjellige styringskjeder. Dette kan for eksempel føre til at viktigheten av arbeidet med å oppdatere dokumentasjon oppfattes ulikt, noe som fører til at det oppstår tidsforsinkelser i oppdatering av dokumentasjon med tilhørende risiko.

De ansattes tilgang til oppdatert informasjon/dokumentasjon.

Strukturen og driftsforholdene i sikkerhetsstyringssystemet bør gjenspeile virkeligheten av måten arbeidet utføres på, og ikke noe tilgjort som kommer på toppen av vanlig praksis.

4.6 Integrering av menneskelige og organisatoriske faktorer

4.6.1 Lovbestemt krav

4.6.1. Organisasjonen skal demonstrere en systematisk tilnærming til å integrere menneskelige og organisatoriske faktorer i sikkerhetsstyringssystemet. Denne tilnærmingen skal:

(a) omfatte utvikling av en strategi og bruk av ekspertise og anerkjente metoder fra feltet menneskelige og organisatoriske faktorer

(b) tar for seg risiko knyttet til utforming og bruk av utstyr, oppgaver, arbeidsforhold og organisatoriske ordninger med hensyn til menneskelige evner så vel som begrensninger, og påvirkning på menneskelige prestasjoner

4.6.2 Formål

Søker viser at praksisen med en systematisk tilnærming til menneskelige og organisatoriske faktorer i målrisiko, er en integrert del av sikkerhetsstyringssystemet. Det er viktig å imøtekomme disse elementene for å vise at søkeren er kompetent til å drive en jernbanevirksomhet, og har risikostyringssystemer integrert i sikkerhetsstyringssystemet for å håndtere risikoene de står overfor.

4.6.3 Forklarende merknader

Menneskelige og organisatoriske faktorer innebærer i tillegg å få et systematisk perspektiv, der samspillet mellom menneskelige, teknologiske og organisatoriske faktorer tas i betraktning. Organisasjonen bør vurdere menneskelige og organisatoriske faktorer gjennom en livssyklustilnærming. Dette betyr å identifisere og håndtere menneskelige og organisatoriske faktorer i sikkerhetsstyringsaktiviteter som er relatert til forretningsmessige målsettinger, ledelse, drift, menneskelig yteevne, utforming av arbeidsoppgaver og arbeidsplass på alle stadier av systemets virketid, for eksempel fra oppstart til avvikling. En strategi for menneskelige og organisatoriske faktorer spesifiserer en systematisk tilnærming til integrering av menneskelige og organisatoriske faktorer i sikkerhetsstyringsaktiviteter.

Organisasjonen bør utvikle nødvendig kompetanse når det gjelder menneskelige og organisatoriske faktorer den trenger for å støtte sin forretningsvirksomhet, spesielt for sikkerhetsroller. Dette dekker også ansatte med ansvar for å integrere menneskelige og organisatoriske faktorer i risikovurdering. Kompetanse innen menneskelige og organisatoriske faktorer betyr at de involverte medarbeiderne har fått dedikert opplæring som er definert i kompetansestyringssystemet. Profesjonell ekspertise på menneskelige og organisatoriske faktorer betyr enten å ha personale som er opplært på et passende nivå for å oppfylle kravet eller ha tilgang til noen som er kvalifisert til en definert nasjonal og/eller internasjonal standard i faget. Store organisasjoner kan ha en avdeling med ekspertise på menneskelige faktorer, som en hjelp i organisasjonen. En mindre organisasjon kan gi ledere alle nivåer ansvaret for å identifisere behovet for ekstern ekspertise på yrkesmessige menneskelige faktorer når det er aktuelt.

Dette kravet er knyttet til menneskelige og organisatoriske faktorer. Mer informasjon om en strategi for menneskelige og organisatoriske faktorer finnes i Vedlegg 5.

4.6.4 Bevis

- *Søker må beskrive hvordan menneskelige og organisatoriske faktorer systematisk blir integrert, slik at risikoer forbundet med samspillet mellom menneskelig atferd, organisatoriske faktorer og teknologi, tas i betraktning i de prosessene i sikkerhetsstyringssystemet. I denne henseende bør*

*søkeren vise til hvor ytterligere informasjon om de relevante prosedyrene kan bli funnet eller til handlingsplaner for progressiv integrering/utvikling, og angi aktivitetene, hvem som vil ha ansvaret for dem og tidsrammen;**(4.6.1)***

- *Tilgjengelige designstandarder for menneskelige og organisatoriske faktorer og beste praksiser brukes. Relevante standarder er for eksempel ISO Series 11064 Ergonomic design of control centres og ISO Series 9241 Ergonomics of human-system interaction.*
- *En brukersentrert designprosess som er basert på menneskelige og organisatoriske prinsipper og metoder samt involvering av brukere, anvendes i forbindelse med for eksempel ny eller modifisert design, prosedyrer, opplæring, arbeidsbelastning og arbeidsmiljø for å sikre livslang sikkerhet og effektivitet av et system. Sluttbrukere er involvert i designprosessen, for eksempel i kravdefinisjonen, påfølgende utviklings- og testprosess. En brukersentrert designprosess er en iterativ prosess som involverer flere faser. Det gjøres analyser for å forstå og spesifisere brukskonteksten (for eksempel bemannings- og kompetanseanalyse, oppgaveanalyse og risikoanalyse). Brukerkrav defineres basert på disse analysene. Designløsninger, inkludert design av grensesnitt, arbeidsplasser, opplæring, prosedyrer og organisering, produseres for å møte brukerkravene. Evalueringer av designene gjøres ved hjelp av formelle metoder, som for eksempel oppgaveanalyse, simulering, risikovurdering, ekspertevalueringer, brukerevalueringer, verifikasjon og validering. Mer spesifikt dekker dette menneskelige og organisatoriske faktorer integrasjon i risikovurdering, informasjon og kommunikasjon og dokumentert informasjon;**(3.1, 4.4 og 4.5)***
- *Produsenter og leverandører er involvert og klar over menneskelige faktorer i utformingen av kjøretøy, utstyr (menneske-maskin-grensesnitt) og IT-systemer, og de nødvendige kravene utledet fra prosessen som er beskrevet i punktpunktet ovenfor er inkludert i spesifikasjonene og kontraktene;**(5.2)***
- *Partnere, leverandører og entreprenører er involvert i promotering og integrering av menneskelige og organisatoriske faktorer;**(5.3)***
- *Ytelsesevalueringsprosessene inkluderer menneskelige og organisatoriske faktorers prinsipper og metoder, kombinert fra risikovurderingen;**(6)***
- *Forbedringsprosessene, inkludert ulykkesundersøkelser inkluderer analyser av menneskelige og organisatoriske faktorer.**(7)***

4.6.5 Eksempler på bevis

En kopi av strategien for menneskelige og organisatoriske faktorer, som beskriver hvordan bruk av ekspertise og teknikker innen menneskelige og organisatoriske faktorer er beskrevet. Sikkerhetspolicyen viser til strategien for menneskelige og organisatoriske faktorer.

Organisasjonen utfører en risikoanalyse ved hjelp av bevisbaserte metoder for drifts- og støtteprosesser på alle stadier i virketiden, fra design til utrangering. Analysen identifiserer alle menneskelige og organisatoriske faktorer og ytelsespåvirkende faktorer, som vil ha innvirkning på jernbanesikkerheten og sikkerhetsstyringsaktiviteter som er nødvendig for å kontrollere de identifiserte risikoene.

Strategien for menneskelige og organisatoriske faktorer viser at det foreligger sikkerhetsstyringsaktiviteter, samt en tilnærming til overvåking og forbedring av effektiviteten. Strategien er være basert på en proaktiv tilnærming, men inkluderer også reaktive aktiviteter etter behov.

Menneskelige faktorers metoder, f.eks. oppgaveanalyser og brukervennlighetsanalyse, brukes som input til utforming, struktur og innhold i prosedyrer, og fullskala simuleringer involverer nåværende operative ansatte for å optimalisere prosedyrer. Sikkerhetsstyringsaktiviteter knyttet til støttefunksjoner, oppgaveutforming,

bemanningsnivå, opplæring, design og bruk av utstyr, prosedyrer og kommunikasjonsprotokoller, identifiseres og knyttes til resultatene av risikovurderingen.

Strategien omfatter hvordan menneskelige og organisatoriske faktorer integreres i endringsledelsesprosessen. Integrering av menneskelige faktorer er prosessen for å integrere menneskelige faktorer og ergonomi i systemteknikkprosessen. Integreringsplanen for menneskelige faktorer gir en systematisk tilnærming i å definere forholdet mellom alle prosjektaktiviteter og feltet for menneskelige faktorer. Menneskelige og tekniske faktorer er integrering av menneskelige egenskaper i systemdefinisjon, design, utvikling og evaluering, for å optimalisere samhandlingen mellom menneske og maskin.

Siden operasjonelle prosesser involverer komplekse arbeidsmønstre, omfatter strategien for menneskelige og organisatoriske faktorer risikostyringsprogram for tretthet.

Det er en klar sammenheng mellom resultatene av risikovurderingen, strategien for menneskelige og organisatoriske faktorer og sikkerhetsmålene. Sistnevnte inkluderer progressiv integrering av menneskelige og organisatoriske faktorer, f.eks.: kartlegge den virkelige situasjonen til selskapet, identifisere hull, utvikle planer for integrering eller forbedring av menneskelige og organisatoriske faktorer i deres sikkerhetsstyringssystem, slik at prosessen og relevant dokumentasjon kontrolleres over tid.

Det er en forklaring på hvordan strategien eller deler av den formidles til personalet, gjennom ulike prosesser som kommunikasjon av sikkerhetspolicy, bevisstgjøring eller sikkerhetsmål.

4.6.6 Referanser 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-standardserien, f.eks.*
- *ISO Series 6385:2004 Ergonomic principles in the design of work systems*
- *ISO Series 11064 Ergonomic design of control centres*
- *ISO Series 9241 Ergonomics of human-system interaction*
- *ISO Series 10075 Ergonomic principles related to mental work-load*
- *CENELEC - EN5016-1 Jernbaneapplikasjoner — Spesifikasjon og demonstrasjon av pålitelighet, tilgjengelighet, vedlikeholdstilpasning og sikkerhet (RAMS) Del 1: Elementært, krav og generelt, kapittel 5.6 (spesielt § 5.6.4)*
- *EEMUA 191. Alarm systems, a guide to design, management and procurement*
- *UIC 651 Layout of drivers' 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 Sjekkpunkter

Sjekk at menneskelige faktorer vurderes i beslutningsprosesser for risikostyring gjennom risikovurdering, endringsstyring og aktivaforvaltning.

Sjekk at driftsdokumentasjonen gjenspeiler bestrebelsene på å håndtere menneskelige faktorer gjennom ergonomisk design (for eksempel: brukervennlig design, lettforståelig språk, grafikk for å forstå instruksjonene, enkel administrasjon av oppdateringer) for å bidra til god risikostyring.

Sjekk at jernbanevirksomheten/infrastrukturforvalteren i overvåking av ytelsen, retter fokuset av analysen på menneskelige faktorer som primær eller underliggende årsak til ulykker, uønskede hendelser eller farlige situasjoner.

Sjekk om det finnes dokumenterte eksempler på korrigerende tiltak som er utarbeidet for å eliminere faktorer som påvirker den menneskelige yteevnen og svekker sikkerheten.

5 Drift

5.1 Driftsplanlegging og kontroll

5.1.1 Lovbestemt krav

5.1.1. Ved planlegging, utvikling, implementering og gjennomgang av sine operasjonelle prosesser, skal organisasjonen sikre at under drift:

(a) brukes det risikoakseptkriterier og risikokontrolltiltak (se 3.1.1 Risikovurdering)

(b) leveres det plan(er) for å oppnå sikkerhetsmålene (se 3.2 Sikkerhetsmål og planlegging)

(c) det innhentes informasjon for å måle riktig anvendelse og effektivitet av de operative ordningene (se 6.1 Overvåking)

5.1.2. Organisasjonen skal sikre at dens driftsordninger er i samsvar med de sikkerhetsrelaterte kravene i gjeldende tekniske spesifikasjoner for interoperabilitet og relevante nasjonale regler og eventuelle andre relevante krav (se 1. Organisasjonens omgivelser).

5.1.3. For å kontrollere risikoer der det er relevant for sikkerheten til operasjonelle aktiviteter (se 3.1.1 Risikovurdering) skal minst følgende tas i betraktning:

(a) planlegging av eksisterende eller nye togruter og nye togtjenester, inkludert innføring av nye kjøretøytyper, behov for å lease kjøretøy og/eller leie inn personale fra eksterne parter og utveksling av informasjon om vedlikeholdet for driftsformål med ansvarlige enheter vedlikehold

(b) utvikling og implementering av togtider

(c) klargjøring av tog eller kjøretøy før bevegelse, inkludert kontroller før avgang og togsammensetning

(d) kjøring av tog eller forflytning av kjøretøy under de forskjellige driftsforholdene (normal, degradert og nødstilfelle)

(e) tilpasning av driften til forespørsler om fjerning fra drift og melding om tilbakeføring til drift utstedt av enheter med ansvar for vedlikehold

(f) autorisasjoner for forflytning av kjøretøy

(g) brukervennligheten av grensesnitt i togførerhus og togkontrollsentraler og med utstyr som brukes av vedlikeholdspersonell.

5.1.3 For å kontrollere risikoer der det er relevant for sikkerheten til operasjonelle aktiviteter (se 3.1.1. Risikovurdering) skal minst følgende tas i betraktning:

(a) identifikasjon av sikre grenser for transport for trafikkplanlegging og kontroll basert på infrastrukturens designkarakteristikk

(b) trafikkplanlegging, inkludert rutetabell og tildeling av togtraseer;

(c) sanntids trafikkstyring i normal modus og i degraderte moduser med bruk av trafikkbegrensninger for bruk og styring av trafikkforstyrrelser;

(d) fastsettelse av vilkår for å kjøre eksepsjonelle forsendelser.

5.1.4. For å kontrollere ansvarsfordelingen der det er relevant for sikkerheten til driftsmessige aktiviteter, skal organisasjonen identifisere ansvar for å koordinere og administrere sikker kjøring av tog og forflytning av kjøretøy og definere hvordan relevante oppgaver som påvirker sikker levering av alle tjenester tildeles kompetent personell innen organisasjonen (se 2.3 Organisatoriske roller, ansvar og myndigheter) og til andre eksterne kvalifiserte parter når det er hensiktsmessig (se 5.3 Entreprenører, partnere og leverandører).

5.1.4 For å kontrollere ansvarsfordelingen der det er relevant for sikkerheten til driftsmessige aktiviteter, skal organisasjonen identifisere ansvar for å planlegge og drive jernbanenettet og definere hvordan relevante oppgaver som påvirker sikker levering av alle tjenester tildeles kompetent personell innen organisasjonen (se 2.3. Organisatoriske roller, ansvar og myndigheter) og til andre eksterne kvalifiserte parter når det er hensiktsmessig (se 5.3. Entreprenører, partnere og leverandører.

5.1.5. For å kontrollere informasjon og kommunikasjon der det er relevant for sikkerheten til driftsmessige aktiviteter (se 4.4 Informasjon og kommunikasjon) skal relevant personell (f.eks. togmannskap) informeres om detaljene for spesifiserte reiseforhold, inkludert relevante endringer som kan resultere i en fare, midlertidige eller permanente driftsrestriksjoner (f.eks. på grunn av spesifikke kjøretøytyper eller spesifikke ruter) og vilkår for eksepsjonelle forsendelser, der disse er påkrevd.

5.1.5 For å kontrollere informasjon og kommunikasjon der det er relevant for sikkerheten til operasjonelle aktiviteter, (se 4.4 Informasjon og kommunikasjon), skal relevant personale (f.eks. signalgivere) informeres om spesifikke rutekrav for tog og bevegelser av kjøretøy, inkludert relevante endringer som kan resultere i en fare , midlertidige eller permanente driftsrestriksjoner (f.eks. på grunn av sporvedlikehold) og betingelser for eksepsjonelle forsendelser.

5.1.6. For å kontrollere kompetanse der det er relevant for sikkerheten ved driftsmessige aktiviteter (se 4.2 Kompetanse), skal organisasjonen sikre, i samsvar med gjeldende lovgivning (Se 1. Organisasjonens kontekst), for de ansatte:

(a) overholdelse av opplærings- og arbeidsinstruksene deres, og korrigerende tiltak iverksettes der det er nødvendig;

(b) spesifikk opplæring i tilfelle forventede endringer som påvirker driften av operasjoner eller deres oppgavetildeling;

(c) vedtak av tilstrekkelige tiltak etter ulykker og hendelser.

5.1.2 Formål

Søker skal vise at det foreligger relevante prosesser for å håndtere operasjonelle risikoer gjennom sikkerhetsstyringssystemet, herunder å sørge for at de ansatte er innforstått med deres roller, operasjonelle risikoer de står overfor, og hvilke kontrolltiltak som foreligger, og at de har riktig kompetanse og opplæring i å håndtere disse i samsvar med sikkerhetsstyringssystemets dokumentasjon.

Søker skal sørge for at vognene eller infrastrukturen drives trygt i samsvar med gjeldende krav under ulike driftsforhold (dvs. normal drift, redusert drift og nødsituasjoner), inkludert bruk av aktiva for testformål (f.eks. testing av hvordan vognene oppfører seg når de er i bevegelse, før det gis godkjenning) og ved spesialforsendelser (f.eks. transport av uvanlig materiale eller store deler som ikke kan deles opp og som ikke kan transporteres ved hjelp av andre transportmidler, som betongbjelker/bærebjelker for broer, etc.).

5.1.3 Forklarende merknader

I pkt. 5.1.3, 5.1.4 og 5.1.5 i lovteksten ovenfor, hvor kravet gjelder infrastrukturforvaltere, er klausulene i svart erstattet med de i blått.

Direktiv (EU) 2016/798 fastsetter at jernbanevirksomheter og infrastrukturforvaltere skal etablere et sikkerhetsstyringssystem for å håndtere sikkerhetsrisikoer i forbindelse med jernbanevirksomheten. Den generelle oppfatningen innen sikkerhetsstyring, er at sikkerheten skal integreres i normale forretningsprosesser så langt det lar seg gjøre. Årsaken til dette er at forretningsfokuset således er like mye rettet på sikkerheten som andre forretningsprosesser, noe som vil føre til mindre konflikter mellom de ulike prosessene.

ISO fastsetter i veiledningsdokumentet (N360), som støttevedlegg til Vedlegg SL, at hensikten med paragraf 8 (Drift) er å spesifisere de elementene som må implementeres i organisasjonens virksomhet, for å sikre at styringssystemkravene oppfylles, samt for å sikre at prioriterte risikoer og muligheter blir tatt i betraktning. I tillegg er det oppgitt at tilleggskrav (spesifikke for kategori) knyttet til driftsplanlegging og kontroll kan komme til å gjelde. De skal ikke være ødeleggende for selskapets virksomhet, men tilveiebringe et tilstrekkelig rammeverk for å kontrollere hvordan viktige sikkerhetsaspekter skal håndteres i organisasjonens forretningsprosesser.

Det har blitt lagt til eksplisitte koblinger mellom driftskrav og andre styringssystemkrav (tilsvarende tilnærmingen som er vedtatt i Vedlegg II i Forordning (EU) 2019/779) for å gjøre det klart at spesifikke driftskrav skal vurderes i forhold til relevante styringssystemkrav (f.eks. er planlegging av ruter for jernbanevirksomheter en aktivitet som bør være gjenstand for risikovurdering). Denne tilnærmingen er ikke ment å være inngående, men har som formål å identifisere bestemte spørsmål som myndighetene mener er viktige (basert på deres erfaring), og som derfor bør undersøkes når de foretar vurdering eller tilsyn. Jernbanevirksomheter og infrastrukturforvaltere bør ikke bare fokusere på disse spesifikke kravene når de utvikler og implementerer sine sikkerhetsstyringssystemer (f.eks. uten hensyn til andre sikkerhetsrisikoer). Jernbanevirksomheter og infrastrukturforvaltere må alltid anvende sikkerhetsstyringssystemkrav (f.eks. risikovurdering, overvåking, kompetanse, informasjon og kommunikasjon) for alle relevante forretningsprosesser for å vise at sikkerhetsrisikoene er tilstrekkelig kontrollert.

Integreringen av sikkerhetsstyringssystemet i forretnings-/driftsprosessene er av ytterst viktig betydning, og for å oppnå dette målet må organisasjonen overholde gjeldende TSI **(5.1.2)**, som TSI-OPE, og regler fra nasjonale bestemmelser når samhandlingskravene ikke er fullt ut spesifisert i tekniske spesifikasjoner for interoperabilitet (TSI). Godkjente metoder for etterlevelse kan også bli kunngjort av medlemsstaten eller dets myndigheter, for å lette etterlevelsen av deres nasjonale bestemmelser. Som et minimum bør følgende driftsprosesser vurderes der det er relevant:

- *Driftsinfrastrukturen (kontroll av infrastrukturruter og utstyr, godkjenning av vognbevegelser under alle forhold og sikring av vedlikehold av infrastruktur: Spor og styringskommando og signalsystem(er),*
- *Drift av tog (utvikling av ruter og relevante rutetabeller, administrasjon av klargjøring av tog, sikre togdrift, og ledsage, teste, vedlikeholde og reparere vogner)*
- *Sporveksling (flytting av vogner for å montere eller demontere et tog).*

TSI-OPE er her viktig, fordi det beskriver Grunnleggende driftsprinsipper (FOP), som bør gjenspeiles i de relevante delene av sikkerhetsstyringssystemet, og således kan samsvar med TSI-OPE brukes til å vise samsvar med de relevante sikkerhetsstyringssystemkravene som nevnt ovenfor.

Infrastrukturforvalteren skal identifisere og utstede vilkår og tiltak for å bruke en vogn for testing på jernbanenettet innen den fastsatte tidsrammen som er angitt i artikkel 21(3) og 21(5) i Direktiv (EU) 2016/797 **(5.1.2)**.

Registreringer av rutekompatibilitetskontroller inkluderer egenskapene til kjøretøyet/toget som vurderes i forhold til de tiltenkte operasjonsrutene, inkludert mulige avviksruter identifisert av infrastrukturforvalterne (se avsnitt 4.2.2.5 i TSI OPE)

Kjennetegn på driftsruter er basert på register over infrastruktur (RINF) og/eller informasjon gitt av infrastrukturforvalter.

Hvis problemer identifiseres av en av partene, bør en felles løsning av jernbaneforetaket og infrastrukturforvalteren iverksettes.

Ny togtjeneste **(5.1.3 (a))** kan omfatte nye typer gods som skal transporteres.

«Sikre grenser» **(5.1.3(a))** for infrastrukturforvaltere betyr både sikre fysiske infrastrukturgrenser der dette er nødvendig og sikkerhetsgrenser for infrastruktur og kommando og kontroll der disse er påkrevd av designgrensene for den infrastrukturen.

Vognbevegelse **(5.1.3 (d))** har en bredere betydning enn tog i bevegelse (dvs. planlagt bevegelse av kjøretøyer) og godkjenning utstedt før togavgang. Det kan også omfatte slep av et havarert tog, kjøring av sporvedlikeholdsmaskiner eller uplanlagt utskifting av en skadet vogn før togavgang.

I henhold til Artikkel 1.1 i UIC-hefte 502-1 foreslås følgende definisjon av begrepet «spesialforsendelser» **(5.1.5)**: «*En forsendelse anses å være en spesialforsendelse dersom dens ytre dimensjoner, vekten eller dens egenskaper i forhold til det faste utstyret eller vognen til en jernbanevirksomhet som er involvert i transporten fører til særegne vanskeligheter, og således kun kan aksepteres under spesielle tekniske eller driftsmessige forhold*». TSI OPE definerer spesialforsendelser som: *«Et kjøretøy og/eller last som på grunn av konstruksjon/design, dimensjoner eller vekt ikke oppfyller rutens parametere og krever spesiell myndighet for bevegelsen og kan kreve spesielle forhold over en del eller hele reisen.»*

Hvordan blir menneskelige og organisatoriske faktorer og sikkerhetskultur integrert?

Utveksling av informasjon for driftsformål ved vedlikehold av vogner **(5.1.3 (a))** under ECM-forordningen og dem som anvender den, er beskrevet i artikkel 5(3) i Forordning (EU) 2019/779. Dette omfatter vedlikeholdsplan og eventuelle begrensninger fastsatt i ECM-forordningen under vedlikehold (kortsiktig planlegging).

Når det henvises til utvikling og gjennomføring av rutetabeller **5.1.3 (b))**, betyr dette at søker skal vise hvordan man ved risikovurdering har håndtert risikoer for aktivitetene i organisasjonen og ved samhandling med andre aktører. For eksempel at de har tatt hensyn til

- *Den ekstra arbeidsbelastningen for signalpersonalet når det kommer flere tog til bestemte tider;*
- *Egnede driftsavtaler med relevant infrastrukturforvalter for å stoppe trafikken, gjenoppta trafikken, utveksle informasjon og eventuelle andre tjenester som anses nødvendig*
- *Administrere risikoer knyttet til sporvedlikehold når togene er i drift 24 timer i døgnet.*

Organisasjonen anvender en proaktiv risikovurderingsprosess som gjør det mulig å identifisere risikoer som gjelder dens jernbanedrift, inkludert risikoer for delt grensesnitt og de som oppstår fra menneskelige og organisatoriske faktorer (se også 3.1). Den reduserer også risikoen for overdreven tillit til nedarvede prosedyrer eller regler.

Organisasjonen anvender risikoakseptkriterier for å avgjøre om eksisterende handlinger er tilstrekkelige til å holde eller redusere risikoene til et akseptabelt nivå eller om nye handlinger skal identifiseres på annen måte. Organisasjonen integrerer deretter sine operasjonelle aktiviteter og samsvar med TSI-ene så langt disse er relatert til operasjoner i sin overvåkingsprosess (se avsnitt ***6 Ytelsesevaluering*** nedenfor).

Menneskelige og organisatoriske faktorer bør vurderes i operasjonell planlegging for kontinuerlig forbedring av sikkerhetskultur i forbindelse med for eksempel arbeidsplaner, utmattelseshåndtering, stress,

arbeidsmiljø (fysisk og psykososialt), arbeidsplasser og arbeidsprosesser osv. Dette for å sikre at konsekvensene av endringene eller ordningene har ikke en negativ innvirkning på menneskelig ytelse eller organisasjonssikkerhet.

5.1.4 Bevis

- *Informasjon som viser at ved planlegging, utvikling, gjennomføring og gjennomgang av driftsprosesser man planlegger å nå sikkerhetsmålsettinger, og anvender risikovurderingstiltak og overvåker resultatene, herunder egnet skilting der ytterligere informasjon om prosedyrer kan bli funnet;**(5.1.1 (a)-(c))***
- *Bevis på at organisasjonen er klar over og faktisk gjennomfører alle obligatoriske sikkerhetskrav i alle kategorier som gjelder for driften, og en skissering av hvordan sikkerhetsstyringssystemet sikrer at de overholdes.*
- *Informasjon der søkeren forsikrer om at driftsordningene samsvarer med gjeldende krav (lovgivning, standarder, osv.);**(5.1.2)***
- *I rammeverket for godkjenning av vogntyper og/eller godkjenning for idriftsetting av vogner, er infrastrukturforvalteren i stand til å identifisere og tilveiebringe **(5.1.2)**:*
    - *Driftsforhold som skal anvendes for bruk av vognen for tester på jernbanenettet, basert på informasjon som er oppgitt av søkeren for godkjenningen;*
    - *Eventuelle nødvendige tiltak som skal tas på infrastruktursiden for å sikre en trygg og pålitelig drift under testing på jernbanenettet, og/eller*
    - *Eventuelle nødvendige tiltak i infrastrukturinstallasjonene for å utføre testing på jernbanenettet.*

- For kontrollen før bruk av autoriserte kjøretøy (artikkel 23.1 i direktiv (EU) 2016/797) og spesielt rutekompatibilitetssjekk (artikkel 23.1(a) i direktiv (EU) 2016/797) er jernbaneforetaket, innenfor sitt sikkerhetsstyringssystem, i stand til å identifisere og fremskaffe **(5.1.3 (a))** bevisprosedyrer og registreringer som viser at kjøretøyet er kompatibelt med ruten der det er ment å operere på og er riktig integrert i sammensetningen av toget (se også avsnitt 4.2.2.5 i TSI OPE).
- Bevis på at driftsdokumentasjonen står i samsvar til kravene til styring av driften (og vedlikeholdet) ved organisatoriske og fysiske grenser, f.eks. organisatorisk, teknisk og driftsmessig samhandling med nærliggende infrastruktur, grensende stasjoner, samhandling med andre jernbanevirksomheter eller infrastrukturforvaltere, etc.;**(5.1.2)**
- Informasjon om hvordan risikoen for driftsaktiviteter håndteres gjennom risikovurderingsprosessen og dekker punktene som er angitt i kravene ovenfor, inkludert for menneskelige og organisatoriske faktorer;**(5.1.3 (a) - (g))**
- Bevis på at artikkel 14(2) i Direktiv (EU) 2016/798 overholdes av det ansvarlige organet for vedlikehold;**(5.1.3(f))**
- Informasjon om hvordan ansvaret for sikkerheten, inkludert ansvaret for tretthetsrisikostyring, håndteres for driftsaktiviteter;**(5.1.4)**
- Informasjon om hvordan organisasjonen håndterer informasjon og kommunikasjon for sikkerheten ved driftsaktiviteter;**(5.1.5)**
- Informasjon om kompetansestyringssystemet og tilhørende prosedyrer, samt hvordan disse kobles til bestemte arbeids- eller oppgaveinstruksjoner for å opprettholde sikkerheten ved driftsaktivitetene;**(5.1.6)**
- Bevis på at driftsdokumentasjonen (prosedyrer, arbeidsinstrukser, etc.) oppdateres når og der det er nødvendig **(se også 4.5.3).**

5.1.5 Eksempler på bevis

En liste over de obligatoriske kravene (inkludert TSI) og hvordan disse overholdes **(se også 2)**.

En forklaring på hvordan driftsrisikoer håndteres gjennom risikovurderingsprosessen og hvordan det sikres at sikkerhetsmålsettingene ved driften nås. Linker til der man kan finne relevante prosedyrer.

En redegjørelse for hvordan felles sikkerhetsmetoder bidrar til kontroll av driftsrisikoer, og hvordan informasjons- og kommunikasjonsflyten håndteres for å sikre korrekt risikostyring.

Detaljer om vedlikeholdssystemet for rullende materiell.

Detaljert om prosedyren for kontroll før togavgang (TSI-OPE) som foreligger for å sikre ensartet kontroll av:

- *Bremseegenskaper (klargjøring av bremseplaten);*
- *Togsammensetning;*
- *Fremre og bakre signaler;*
- *Tilstand på last og vogner.*

En kopi av prosessen for å identifisere uoverensstemmelser og hvordan det sikres at det treffes nødvendige tiltak, som for eksempel å ta vogn ut av drift, utskifting av ødelagt/defekt komponent/utstyr/kjøretøy eller iverksetting av driftsbegrensninger.

Et dokument som beskriver vogntypene som skal brukes på hver enkelt rute og hvilken drift som skal utføres, og som spesifikt beskriver:

- *Driftsbegrensninger som gjelder for bestemte vogntyper;*
- *Begrensninger som gjelder for bruk av bestemte vogntyper på bestemte ruter;*
- *Ekstra vedlikeholdskrav for bestemte ruter **(se også 5.2)**.*

I forhold til etterlevelse av Fundamental Operational Principles (FOP) i TSI-OPE, fremlegges det bevis på at jernbanevirksomheten kan forsikre om at (kun for illustrative formål):

- *Et tog kan kun gå på en del av linjen dersom togsammensetningen er kompatibel med infrastrukturen (FOP 3)*

  Dette gjelder bekreftelse av togkompatibilitet i forhold til infrastrukturen på ruten der det er planlagt å gå, før togdriften er godkjent. Kompatibilitet mellom tog og infrastruktur påvirkes <u>først og fremst</u> av dimensjonene på en vogn og hvilken last den transporterer; klaringene mellom toget og infrastrukturen eller togene på tilstøtende spor (måling); minimum påkrevd bremsekapasitet på toget; vekten og lengden på et tog og kapasiteten på infrastrukturen.

  Det foreligger bevis på at:

- *Kontroll før togavgang skal finne sted for å sikre at passasjerer, bemanning og gods føres trygt frem, før et tog starter på eller fortsetter med reisen (FOP 4).*

  Dette gjelder toget og om det er klart for å settes i gang. Noen eksempler: Togets bremsekapasitet, hastigheten som toget har lov til å kjøre i, formasjonen og koplingen av toget, identifikasjon, lasting og sikring av gods, tilveiebringelse av tilstrekkelig informasjon til å lære opp klargjøringspersonell og driftspersonell. Formålet er å forhindre kollisjoner og avsporinger som følge av eksisterende risikoer.

Det å ta hensyn til menneskelige og organisatoriske faktorer og forbedre sikkerhetskulturen vil ha en positiv innvirkning på samsvar med det relevante kravet til sikkerhetsstyringssystemet, og bevis på dette finnes i:

I et dokument som beskriver eventuelle tilleggskrav for å håndtere situasjoner med nedsatt drift (f.eks. hendelser med vogn) for jernbanenettet som er berørt av driften.

Personene som har ansvaret for å planlegge og levere de operative aktivitetene, er opplært til å ta hensyn til menneskelige og organisatoriske faktorer, for både å integrere menneskelige ytelsesevner og begrensninger, inkludert identifiserte risikoer og sikkerhetstiltak.

Sikkerhetsinformasjon blir identifisert og følger menneskelige og organisatoriske faktorers prinsipper (se avsnitt ***4.4 Informasjon og kommunikasjon*** nedenfor).

I en prosess for tretthetsstyring som gjelder for ansatte med uregelmessige arbeidstider. Prosessen er basert på bevisbaserte metoder og faglig kompetanse. Prosessen tar hensyn til at en rekke faktorer må vurderes, ved å ha en helhetlig tilnærming til tretthetsrisikostyring. Programmet for tretthetsstyring omfatter planlegging og tilsyn av arbeidsmiljøet og arbeidsoppgavene, for å minimere effekten tretthet har på årvåkenhet og yteevne som langt som praktisk og mulig og innen rimelighetens grenser, på en måte som samsvarer med risikoeksponeringsnivået og driftens art.

5.1.6 Referanser og standarder

- *ISO N360 JTCG konseptdokument som bilag til Vedlegg SL*
- *UIC-hefte 502-1*
- *Vedlegg II til direktiv 2008/68/EF (RID)*
- *Veiledning for TSI-OPE*

5.1.7 Sjekkpunkter

Tilsynet med driftsaktiviteter skal gjennomføres ved å fokusere på særskilte områder og undersøke disse i detalj, for å se hvordan de er gjenspeilet i sikkerhetsstyringssystemet for organisasjonen som føres tilsyn med, og om de har egnet bemanning på rett sted som utfører arbeidet korrekt. Dette vil gjøre det mulig for NSA å se om aktivitetene er omfattet av sikkerhetsstyringssystemet som en sammenhengende helhet, eller håndteres separat med svake koblinger til sikkerhetsmålsettingene og den grunnleggende strategien.

Tilsyn bør særlig kontrollere:

- *Hvordan dokumenter om sikkerhetsstyringssystemet på høyere nivå oversettes til konsistente lokale instruksjoner som brukes til å håndtere risiko på operasjonelt nivå;*
- *Håndtering av nødsituasjoner eller andre situasjoner som ikke er en del av rutinen;*
- *Hvordan driftsgrenser/-begrensninger styres, herunder samhandlingsordninger med andre parter;*
- *Ordninger for tretthetsstyring;*
- *Håndtering av farlige stoffer;*
- *Ordninger for transport av farlig gods, herunder opplæring, roller og ansvar for organisasjonens ansatte, som beskrevet i kapittel 1.3, 1.4 og 1.8 i RID, og om nødvendig ha kontakt med en annen myndighet som har kompetanse om transport av farlig gods;*
- *Etterlevelse av de grunnleggende driftsprinsippene som er beskrevet i TSI-OPE.*

5.2 Aktivaforvaltning

5.2.1 Lovbestemt krav

5.2.1. Organisasjonen skal håndtere sikkerhetsrisikoen knyttet til fysiske aktiva gjennom hele livssyklusen (se 3.1.1. Risikovurdering), fra design til utrangering, og oppfylle kravene til menneskelige faktorer for bruk.

5.2.2. Organisasjonen skal:

(a) sikre at aktiva brukes til det formålet som er tiltenkt samtidig som de opprettholder deres sikre driftstilstand, i samsvar med artikkel 14(2) i direktiv (EU) 2016/798 der det er relevant, og deres forventede ytelsesnivå;

(b) administrere aktiva i normal og degradert drift;

(c) oppdage så snart som praktisk mulig tilfeller av manglende overholdelse av driftskrav før eller under driften av aktivaet, inkludert bruk av bruksbegrensninger som er hensiktsmessig for å sikre en sikker driftstilstand for aktivaet (se 6.1. Overvåking).

5.2.3. Organisasjonen skal sikre at dens aktivaforvaltningsordninger, der det er aktuelt, er i samsvar med alle grunnleggende krav som er angitt i de relevante tekniske spesifikasjonene for interoperabilitet (se 1. Kontekst for organisasjonen).

5.2.4. For å kontrollere risikoer der det er relevant for levering av vedlikehold (se 3.1.1. Risikovurdering) skal minst følgende tas i betraktning:

(a) identifisering av behovet for vedlikehold for å holde aktivaet i en sikker driftstilstand, basert på den planlagte og reelle bruken av aktivaet og dens designegenskaper;

(b) styring av fjerning av en ressurs fra drift med tanke på vedlikehold, når mangler er identifisert eller når aktivaets tilstand forringes utenfor grensene for en sikker driftstilstand som nevnt i punkt (a);

(c) styring av tilbakeføring til drift av aktivaet med eventuelle restriksjoner for bruk etter at vedlikehold er levert for å sikre at den er i en sikker driftstilstand;

(d) styring av overvåkings- og måleutstyr for å sikre at det er egnet til det tiltenkte formålet.

5.2.5. For å kontrollere informasjon og kommunikasjon der det er relevant for sikker forvaltning av aktiva (se 4.4. Informasjon og kommunikasjon), skal organisasjonen ta hensyn til:

(a) utveksling av relevant informasjon innen organisasjonen eller med eksterne enheter som er ansvarlige for vedlikehold (se 5.3. Entreprenører, partnere og leverandører), spesielt om sikkerhetsrelaterte funksjonsfeil, ulykker, hendelser samt eventuelle restriksjoner for bruk av aktivaet;

(b) sporbarheten av all nødvendig informasjon, inkludert informasjonen knyttet til punkt (a) (se 4.4. Informasjon og kommunikasjon og 4.5.3. Kontroll på dokumentert informasjon);

(c) etablering og vedlikehold av registre over alle aktiva, inkludert styring av endringer som påvirker sikkerheten til aktiva (se 5.4. Endringsstyring).

5.2.2 Formål

Søker må vise hvordan deres aktiva forvaltes gjennom levetiden fra design til utrangering, gjennom prosedyrer og ordninger som er angitt i sikkerhetsstyringssystemet. Søker må vise at det har blitt anvendt en menneskelig sentrert tilnærming for hver fase i løpet av levetiden. Det må beskrives hvor forvaltningen av aktiva grenser til ulike elementer i sikkerhetsstyringssystemet, som kompetansestyring, driftsplanlegging og

overvåking. Søker bør vise at det foreligger et robust system for aktivaforvaltning som gjenspeiler risikoer som oppstår fra virksomhetens type og omfang.

5.2.3 Forklarende merknader

"Aktiva" **(5.2)** viser til alt utstyr (fast eller mobilt), strukturer, programvare eller andre komponenter som krever vedlikehold over tid, og som er anskaffet for å drive jernbanevirksomheten. Aktiva vil bli delt inn i hva som forvaltes av jernbanevirksomheten (hovedsakelig vogner, men også annet utstyr, som hjulsatsdreiebenker, verneutstyr og dataprogrammer som tilbys for sikkert vedlikehold av aktiva) og hva som forvaltes av infrastrukturforvalteren (alle infrastrukturkomponenter, for eksempel skinner, utstyr for styringskommando/signalering, sporveksling, kraftforsyning, planoverganger, byggeteknikk, for eksempel broer, viadukter, tunneler, plattformer, heiser, rulletrapper, etc. En fullstendig liste kan finnes i Vedlegg I til Direktiv (EU) 2012/34).

Livssyklusen omfatter følgende faser:

a) Design;
b) Gjennomføring (bygging/produksjon, installasjon, testing og idriftsetting);
c) Drift og vedlikehold;
d) Reparasjoner, endringer og ettermontering, som innebærer endringsstyring;
e) Utskifting, avvikling og kassering.

Det er viktig for en organisasjon å vise hvordan den fanger opp og opprettholder (system- og) sikkerhetskrav for sine aktiva, og hvordan disse blir verifisert, validert og sporet.

Hvis vedlikeholdet er satt bort til en tredjepart, er det organisasjonens ansvar å spesifisere og overvåke at aktivaets ytelse overholder organisasjonens fastsatte standarder.

Når det foreligger prosesser for å håndtere risikoer forbundet med sikkerhetskritiske aktiva, bør overvåke organisasjonen aktivaytelsen mot sådan risikoer og egne forventninger.

Der det er sannsynlig at aktiva skal utskiftes, avvikles eller kasseres, må organisasjonen etablere og dokumentere prosesser for å håndtere eventuelle risikoer forbundet med slike aktiviteter.

Disse prosessene er bare relevante for organisasjoner som enten utfører slike aktiviteter eller som sannsynligvis vil gjøre det.

For utskifting av et aktiva som nærmer seg slutten av levetiden, må organisasjonen sikre at erstatningsaktivaet oppfyller fastsatte kriterier for sikkerhetsytelse. Som en del av denne prosessen må alle sikkerhetsanalyser gjennomgås.

Krav knyttet til vedlikehold **(5.2.4)** er utledet av ECM-forordningen, hvor rullende materiell er et aktiva som en jernbanevirksomhet og muligens en infrastrukturforvalter skal forvalte. Disse kravene i Vedlegg II til Forordning (EU) 2019/779 er mer spesifikke og veiledende, mens de ovennevnte kravene hovedsakelig omfatter samhandling mellom jernbanevirksomheten eller infrastrukturforvalterens sikkerhetsstyringssystem og ECMs vedlikeholdssystem, med sikte på å forsikre om at aktiva er trygge for drift og vedlikehold. Ytterligere detaljer finnes i ECM-forordningen og den medfølgende veilederen. Risikovurderingen bør også fokusere den potensielle sikkerhetsfaktorer ved eventuelt erstatningsutstyr i løpet av vedlikeholdet (som er en del av livssyklusen til aktiva) i samsvar med kravene i Direktiv (EU) 2016/797 og relevante TSI-er.

Ikke alle aktiva er regulert av TSI **(5.2.3),** og selv om en TSI skulle gjelde (f.eks. TSI INF), reguleres bare hva som er nødvendig for interoperabilitet, noe som betyr at andre sikkerhetskrav fortsatt kan være nødvendig. Etterlevelse av de essensielle kravene i relevante TSI-er (ikke bare grunnleggende krav til sikkerhet) skal opprettholdes ved bruk av erstatningsutstyr, utskifting eller oppgradering.

Begrepet "sikker driftstilstand" **(5.2.4 (a))** betyr at aktivaet skal drives innenfor dets sikre bruksgrenser. Sikkerhetsgrensene for bruk kan være i utvikling gjennom hele systemets levetid, men skal defineres med tanke på interoperabilitetsparametrene. Defekter kan identifiseres **(5.2.4 (b))** og på grunnlag av en årsaksanalyse kan de sikre bruksgrensene tilpasses i henhold til den. For vogner betyr en sikker driftstilstand en sikker tilstand under drift i samsvar med artikkel 14(2) i Direktiv (EU) 2016/798.

Aktivakonfigurasjon **(5.2.5 (c))** inkluderer den unike identifikasjonen på aktivaene, deres lokasjon, eventuelt vedlikehold som er gjort, etc. (og ikke bare konfigurasjonsstyring av endringer). Konfigurasjonsstyringen for (tekniske) endringer gjelder for erstatningsutstyr.

Det skal utnevnes en ECM (enhet med ansvar for vedlikehold) i samsvar med artikkel 14(1) i Direktiv (EU) 2016/798, for å sikre at vogner enheten driver vedlikehold på, er i forsvarlig driftstilstand. Det er ikke nødvendig å komme med detaljerte beskrivelser av aktiviteter som er utført av en ECM som er sertifisert i samsvar med Forordning (EU) nr. 2019/779. På den annen side er det nødvendig å angi hvilke elementer og hvilke aspekter som er omfattet av ECM-sertifikatet, og hvordan samhandling med ECM håndteres, spesielt hvilken informasjon som utveksles mellom søkeren og ECM, og hvordan dette gjøres. Hvis ECM ikke er direkte kontrahert av jernbaneforetaket, men er en tredjepart i en kontrakt mellom en kjøretøyeier (eller rettighetshaveren) og jernbaneforetaket, kan informasjonsutvekslingen gjennomføres via en mellommann, men må fortsatt være effektiv og rettidig i begge retninger.

Når det gjelder samarbeid mellom jernbanevirksomheter, forblir hver enkelt jernbanevirksomhet fullt ut ansvarlig for at driften utføres på en sikker måte, og kontrollerer således risikoer knyttet til virksomheten. Dersom en jernbanevirksomhet bruker et samarbeidspartners sikkerhetssertifikat for å kontrollere risikoer som er knyttet til vedlikehold, er dette ikke tilstrekkelig dersom det ikke er avtalefestet mellom de samarbeidende virksomhetene. Disse avtaleordningene må utvikles og overvåkes av hver av partene og være en del av begge parters sikkerhetsstyringssystemer, og er således underlagt tilsyn av respektive NSA. Respektive NSA skal koordinere for å løse eventuelle samhandlingsproblemer på tvers av grensene som kan ha blitt skapt av partene i avtalen.

Hvordan blir menneskelige og organisatoriske faktorer og sikkerhetskultur integrert?

Menneskelige faktorer integreres gjennom livssyklusen til alle systemer og delsystemer, basert på resultatene av risikovurdering som allerede inkluderte menneskelige og organisatoriske faktorer og de definerte sikkerhetstiltakene.

Dette inkluderer en brukersentrert tilnærming i designfasen av systemet som kan være sammensatt av funksjonstildeling (menneske/maskin), intervjuer og oppgaveanalyser (for hver deloppgave). Spesifikasjoner for aktivaene er basert på brukernes behov, inkludert brukerytelse og begrensninger.

Sikkerhetstiltak er definert under hensyntagen til arbeidsmiljøet, organisasjonen og bemanningen, team og kommunikasjon, utformingen av prosedyrer (inkludert drift og vedlikehold av aktivaet), og tilstrekkelige ressurser i forbindelse med aktivaet som sikrer at menneskelige og organisatoriske faktorer vurderes og tas tak i på en hensiktsmessig måte. Dette kan omfatte spesifikasjoner om f.eks. arbeidsplassinnredning, ergonomisk utforming av utstyr (verktøy, maskineri, materialer), brukbarheten til utstyret, tilbakemeldingene som forventes fra det, kvaliteten på utstyret, inspeksjons-/vedlikeholdsplanen og toleransen for feil.

5.2.4 Bevis

- *Informasjon om aktivaforvaltningssystemet i organisasjonens sikkerhetsstyringssystem, inkludert relevante linker til andre områder som risikovurdering, driftsplanlegging, endringsstyring, osv.* ***(5.2.1), (5.2.2), (5.2.5 (a)-(b))****;*

Designfasen

- *Bevis på prosesser og konsultasjoner for å fastslå behov for aktiva;*
- *Bevis på risikostyringsstrategier i forhold til anskaffelse og bruk av nye eller modifiserte aktiva;*
- *Dokumentasjon på alle relevante prosesser for design og levering av aktiva;*
- *Prosesser for risikostyring i designfasen;*
- *Bevis på verktøyene som brukes til å trygge sikkerheten;*
- *Informasjon om standarder eller annen sikkerhetsinformasjon som design og vedlikehold av aktiva er gjenstand for, og eventuelle tester som anvendes til å bekrefte samsvar;*
- *Om det foreligger en håndbok eller lignende som beskriver prosessene for drift og vedlikehold av aktiva, og for risikostyring i drifts- og vedlikeholdsfasen;*

Implementeringsfasen

- *Bevis på sikkerhetsrisikostyring, testing og validering av prosesser som dekker bygging/produksjon og idriftsetting av aktiva og at det er klart til å settes i drift;*

Drifts- og vedlikeholdsfasen

- *Bevis på kontinuerlig etterlevelse av standarder og prosesser, samt styring av identifiserte risikoer;*
- *Vedlikeholdsplaner og prosedyrer for vedlikehold av aktiva;*
- *Bevis på organisasjonens aktiviteter med å identifisere og eliminere risikoer;*
- *Bevis på prosessene som anvendes til å rapportere om og håndtere eventuelle sikkerhetsytelsesproblemer, samt iverksette korrigerende tiltak;*
- *Bevis på anvendelse av ytelsesvalidering mot den antatte strategiske levetiden til et aktiva, for sporing av ytelse og planlegging av utskifting;*
- *Prosesser for å identifisere feil og svikt, og iverksetting av korrigerende tiltak*
- *Håndtering av nødsituasjoner eller andre situasjoner som ikke er en del av rutinen, som kan påvirke sikkerheten ved aktivaet;*
- *Bevis på at aktivaforvaltning er hensyntatt for meldepliktige hendelser og styring av felles risikoer ved samhandling;* ***(se også 3.1)***

Utskifting, avvikling og kassering

- *Bevis på prosesser for håndtering av risiko knyttet til utskifting, avvikling eller kassering av aktiva, som er i samsvar med organisasjonens omfang og art;*

- *Bevis på en systematisk tilnærming for håndtering av menneskelige og organisatoriske faktorer i alle faser i løpet av aktivaets livssyklus;* ***(5.2.1)***
- *Bevis på at driftsdokumentasjonen står i samsvar til kravene til styring av (driften og) vedlikeholdet ved organisatoriske og fysiske grenser, f.eks. organisatorisk, teknisk og driftsmessig samhandling med nærliggende infrastruktur, grensende stasjoner, samhandling med andre jernbanevirksomheter eller infrastrukturforvaltere, etc.;****(5.2.3)***
- *Informasjon der søkeren viser at vedlikeholdsordningene samsvarer med foreliggende krav (lovgivning, standarder, osv.);****(5.2.3)***
- *Når det gjelder kjøretøy, blir en kopi av ECM-sertifikatet (dette kan innehas av jernbaneforetaket eller av en enhet som jernbaneforetaket er avhengig av for å yte kjøretøyvedlikehold, eller til og med outsourcet med hensyn til vedlikeholdsfunksjoner) eller (til 16. juni 2022) bevis for at artikkel 14(2), 14(3) og vedlegg III i direktiv (EU) 2016/798 overholdt av enheten som er ansvarlig for vedlikehold;* ***(5.2.4 (a)-(d))***

Ved partnerskap mellom jernbanevirksomheter der vognene vedlikeholdes av samarbeidspartner:
Bevis på at det foreligger avtaler mellom partene, herunder:

- Utveksling av informasjon som beskrevet i artikkel 5 i Forordning (EU) 2019/779;

- Teknisk støtte når det er hensiktsmessig, spesielt for gamle CCS-systemer;
- Kontroll av evnen verkstedene vedlikeholdsleverandøren har til å utføre vedlikeholdet;
- Overvåking av vogner og utveksling av relevant informasjon som følge av denne overvåkingen;**(se også 6.1)**

- Med hensyn til aktiva som krever et samsvarssertifikat i henhold til EU-lovgivningen eller nasjonale bestemmelser, en kopi av sådan sertifikat sammen med en forklaring på i hvilken grad det er vesentlig som en del av sikkerhetsstyringssystemet. **(5.2.4 (a)-(d))**
- Informasjon om hvordan dokumentstyringsdelen i sikkerhetsstyringssystemet fungerer i forhold til aktivaforvaltning, herunder bevis på at vedlikeholdsdokumentasjonen (prosedyrer, arbeidsinstrukser, etc.) oppdateres når og der det er nødvendig; **(5.2.5 (a)-(c))**
- Bevis på konfigurasjonsstyring av aktiva gjennom hele livssyklusen, inkludert eventuelle foreliggende prosesser for endringsstyring for å håndtere grunnkonfigurasjoner; **(5.2.5 (c))**

5.2.5 Eksempler på bevis

Designfasen

Organisasjonen dokumenterer alle relevante sikkerhetsrelaterte prosesser og informasjon knyttet til design og levering av aktiva ved anvendelse av konfigurasjonsstyringsprosess (eller et konfigurasjonsstyringssystem). Disse skisserer de tekniske og organisatoriske aktivitetene som etablerer og opprettholder kontroll over aktiva gjennom hele livssyklusen.

Organisasjonen etablerer og dokumenterer en prosess for å håndtere risikoer knyttet til designet på aktivaløsningen, ved å:

- *Fastsette krav til eventuelle nye og/eller modifiserte aktiva **(se også 1)** og drøfter dem med relevante interessenter **(se også 2.4)**;*
- *Håndtere risikoer forbundet med å gjennomføre slike endringer **(se også 3.1)**; og*
- *Håndtere risikoer knyttet til anskaffelse av aktiva og kontraktstyring når det er relevant **(se også 3.1 og 5.3)**.*

Disse omfatter fare-/sikkerhetsanalyser for å identifisere områder som er mest utsatt for feil, og som gjennomgås i forhold til organisasjonens farelogg. Dette gjøres ved å identifisere sikkerhetskritiske systemer og etablere grunnleggende ytelsesmålsettinger gjennom anvendelse av hensiktsmessige risikoidentifisering, for eksempel:

- *RAMS-analyse (pålitelighet, tilgjengelighet, vedlikeholdstilpasning og sikkerhet) av design av aktiva (hvor grunnleggende kriterier til sikkerheten formidles til utviklere for å sikre at aktivaet er egnet for formålet); og*
- *FMECA-analyse (feilmodus, effekter og kritikalitet) og/eller RCM (pålitelighetsstyrt vedlikehold) for å håndtere risikoer i designfasen og sørge for at vedlikeholdsplanene opprettholdes.*

Disse kravene anvendes mot de spesifikke standardene og prosessene som anvendes for design, vedlikehold og drift av jernbaneinfrastrukturen og rullende materiell, som identifisert av organisasjonen. Organisasjonen skal vise at:

- *Sikkerhetskritiske systemer er utformet for funksjonelle spesifikasjoner;*
- *Det foreligger en plan for validering og idriftsetting for å bekrefte at aktiva er egnet for formålet og trygt å betjene og vedlikeholde; og*
- *Det er utarbeidet drifts- og vedlikeholdsdokumentasjon, som beskriver prosesser for oppdatering, gjennomgang og vedlikehold av aktiva **(se også 4.5)**.*

Organisasjonen viser at den anvender hensiktsmessige systemtekniske prosesser og prosesser for å sørge for god sikkerhet (f.eks. EN50126/8/9 for komplekse systemer) i dens tilnærming til design og anskaffelser. Dette

kan gjøres ved å utarbeide en SEMP-plan (systemteknisk styringsplan), som spesifiserer prosedyren for å identifisere og protokollføre interessenter, systemkrav og sikkerhetsbehov.

Implementeringsfasen

For å sikre en vellykket og sikker implementering av aktivaet, skal organisasjonen etablere prosesser for å håndtere risikoer knyttet til konstruksjon, testing og idriftsetting, i tråd med prosessene i sikkerhetsstyringssystemet.

Det må også implementeres en prosess som omfatter:

- *Testing, verifisering og validering av system- og sikkerhetskravene til aktiva, som kan gjøres ved å anvende en "Styringsplan for testing og idriftsetting" eller tilsvarende; og*
- *Sjekk av at aktivaet er klart for drift, som kan gjøres med en sjekkliste for driftsklarhet.*

Drifts- og vedlikeholdsfasen

Organisasjonen har utviklet en drifts- og vedlikeholdsdokumentasjon for aktiva, som skisserer prosessene for sikkerhetsstyring som anvendes til å oppdatere, gjennomgå og vedlikeholde sine aktiva. Denne skal beskrive omfanget av driften og, der det er aktuelt, risikostyringsstrategiene som foreligger for å dekke alle relevante aktiviteter.

Denne dokumentasjonen:

- *Skal sikre at aktiva driftes og vedlikeholdes i samsvar med oppbyggingen av aktivaet;*
- *Skal identifisere og innlemme alle sikkerhetsrelaterte forhold, som beskriver hvordan bruken av aktiva kan være begrenset, og foreliggende bruksvilkår; og*
- *Beskriver de pågående kontrollene som skal utføres.*

Prosessen for å konfigurere design og levering av foreslåtte aktiva (beskrevet i designfasen), er utvidet til å dekke hele livssyklusen ved å:

- *Etablere og vedlikeholde oppføringer over alle aktiva gjennom å opprette et aktivaregister. Dette inneholder informasjon som f.eks. unik identifikasjon på aktiva, lokasjon, eventuelt utført vedlikehold, osv.;*
- *Administrasjon av dokumenter og informasjon om aktiva i samsvar med organisasjonens sikkerhetsstyringssystem **(se også 4.4 og 4.5)**; og*
- *Fastslå kritikaliteten av aktiva, basert på resultatene av en sikkerhetsrisikovurdering. Sikkerhetskritiske aktiva skal føres opp i aktivaregisteret.*

Organisasjonen skal vise hvordan informasjon om aktiva er utviklet, vedlikeholdt og innarbeidet i fareloggen.

Organisasjonen skal på kontinuerlig basis overvåke etterlevelse av fastsatte standarder og prosesser, for å sikre at jernbanedriften fortsetter å være sikker og effektiv. For dette formål skal organisasjonen etablere prosesser for å sikre at:

- *Aktiva driftes og vedlikeholdes i samsvar med relevante håndbøker;*
- *Tilstanden på aktiva overvåkes;*
- *Utstyr som trengs for å teste eller inspisere aktiva kontrolleres, kalibreres og vedlikeholdes korrekt.*
- *Eventuelle risikoer knyttet til drift og vedlikehold av aktiva håndteres i samsvar med risikostyringsprosessene og alle HMS-regler på arbeidsplassen; og*
- *Reservedeler er tilgjengelig for vedlikehold, spesielt for sikkerhetskritiske aktiva. Dette kan gjøres ved å fastslå behovet for reservedeler for aktiva basert på kritikalitet, som identifisert ved anvendelse av "pålitelighetsstyrt vedlikehold" (RCM).*

Organisasjonen demonstrerer at den har på plass vedlikeholdsplaner for aktiva for å:

- *Ta hensyn til krav til kompetanse, kapasitet og ressurser;*

- *Tilrettelegge for informasjonsstyring og loggføring;*
- *Tilveiebringe detaljerte planer som er etablert gjennom en risikobasert prosess, og som definerer de ulike vedlikeholdsnivåene og etablerte standarder for organisasjonsstrukturer, prosedyrer og ansvar for vedlikehold av aktiva; og*
- *Sørge for kalibrering av verktøy og utstyr som skal brukes ved vedlikehold.*

Dette kan spesifikt omfatte:

- *En teknisk vedlikeholdsplan (TMP); og*
- *Arbeidsinstrukser som er utledet fra og revidert mot TMP.*

Planlegging dokumenteres og kontrolleres ved hjelp av et styringssystem for vedlikehold av datamaskiner **(se også 4.5)**.

Organisasjonen skal ha på plass prosesser på plass for å sikre at:

- *Når en vogn eller noe utstyr er dedikert en oppgave som:*
  - *Samsvaret i oppgaven/oppdraget som skal utføres (f.eks. at hver type rullende materiell er kompatibel med rutene) kontrolleres ved inspeksjon og før togavgang;*
  - *Vedlikehold av minst sikkerhetskritiske komponenter gjøres i henhold til foreliggende plan (forebyggende vedlikehold med hyppighet og arbeid som skal utføres);*
  - *Vedlikeholdsarbeid er definert når det registreres feil, eller når sikre bruksgrenser overskrides (korrigerende vedlikehold), med mindre det er implementert driftsbegrensninger;*
  - *Det treffes nødvendige tiltak så snart som mulig etter at det er registrert behov for endringer, for eksempel når utstyr tas ut av drift eller ved justering av driftsbegrensninger.*
- *Arbeidsinstrukser er tilgjengelige for alle sikkerhetskritiske aktiviteter;*
- *Alle oppgaver er klarert for samsvar;*
- *Dokumentasjon om utført vedlikehold er kontrollert **(se også 4.5)**; og*
- *Kompetansebasert opplæring er tilgjengelig i alle sikkerhetskritiske systemer **(se også 4.1)**.*

Det er en prosess/prosedyre for å sikre at driftsbegrensninger, enten midlertidige eller permanente (f.eks. på grunn av bestemte vogntyper eller bestemte ruter) er:

- *Hensyntatt når en vogn eller noe utstyr er dedikert en oppgave/et oppdrag;*
- *Formidlet til rett tid til ansatte som fører vognen eller utstyret (f.eks. lokomotivfører, togleder).*

Organisasjonen skal vise at den:

- *Forstår ytelsen til sine sikkerhetskritiske aktiva ved å identifisere hva som må overvåkes, måles og rapporteres;*
- *Har etablert og protokollfører metoden og hyppigheten for overvåkning, måling, analyse og evaluering av ytelsen til sikkerhetskritiske aktiva;*
- *Overvåker ytelsen mot den forventede strategiske levetiden på et aktiva **(se også 6.1)**;*
- *Rapporterer om ytelsesproblemer basert på sikkerhetsrisikonivået og rapporterer videre sikkerhetsproblemer slik at de blir tatt hånd om på en egnet måte;*
- *Resultatene fra overvåkingen brukes til å tilpasse vedlikeholdsplanen der det er relevant;*
- *Etablerer kommunikasjonskanaler for å formidle resultatene **(se også 4.4)**;*
- *Forbedrer samsvaret ved sikkerhetskritiske aktiva med standarder ved å:*
  - *Gjennomgå drifts- og vedlikeholdskontroller og vurdere risikoen for at aktiva ikke oppfyller fastsatte standarder;*
  - *Identifisere årsaken(e) til sikkerhetsproblemene; og*
  - *Identifisere tiltak som kan være nødvendig å iverksette for å få aktiva tilbake til sikker driftstilstand;*
- *Kontinuerlig forbedre sikkerhetsstyringssystemet ved å identifisere potensielle farer og iverksette korrigerende tiltak **(se også 7.2)**; og*

- *Dokumentere når det er iverksatt tiltak for å redusere eller eliminere risiko, og hvordan dette ble oppnådd.*

Organisasjonen må ha på plass prosesser for å identifisere eventuelle feil eller svikt som kan oppstå på deres aktiva, og sørge for at korrigerende tiltak iverksettes. Disse skal være i tråd med bestemmelsene og vedlikeholdsprogrammene eller -planene, og:

- *Sikre at feil registreres og resulterende korrigerende tiltak iverksettes;*
- *Håndtere sikkerhetskritiske feil;*
- *Sikre rapportering av meldepliktige hendelser; og*
- *koordinere reparasjoner på sikkerhetsrelatert aktiva som ikke er planlagt.*

Organisasjonen:

- *Dokumenter feilhåndteringsprosessen;*
- *Anvender egnede analyseteknikker for sikkerhetskritiske funksjoner, for eksempel "årsaksanalyse" (RCA);*
- *Implementerer registrering av feil, som kan inkludere feilkoder, feilmodus, effekt, kritikalitet og korrigerende tiltak;*
- *Utvikler prosedyrer for håndtering av vanlige reparasjonsaktiviteter; og*
- *Innfører en tilbakemeldingsprosess for teknisk personell for å gjennomgå og forbedre systemene og minimere risikoen for fremtidige feil.*

Dette oppnås ved anvendelse av feilrapportering, analyse og korrigerende tiltak (FRACAS), som:

- *Registrering av feil som ble oppdaget og registrert under testing og idriftsetting, samt eventuelle feil som oppstod under drift eller vedlikehold; og*
- *Administrasjon av etterfølgende korrigerende tiltakene som er truffet for å håndtere dem.*

Organisasjonen må dokumentere alle feil og korrigerende tiltak, og få en teknisk kompetent person til å kontrollere eventuelle reparasjoner som ikke er planlagt.

Det er en prosess/prosedyre for håndtering av nedsatt drift eller nødsituasjoner i aktivaforvaltning.

Organisasjonen har etablert prosesser for å håndtere risikoer ved samhandling som oppstår under driften og vedlikeholdet av aktiva **(se også 3.1.1)**. Dette omfatter samhandling mellom aktiva og mellom aktører som bruker dem.

Utskiftings-, avviklings- og kasseringsfasen

Organisasjonen må kjenne til tilstanden på sine aktiva, og når tilstanden forringes må aktiva skiftes ut eller utbedres deretter.

Organisasjonen har etablert en plan for validering og idriftsetting for å bekrefte at et nytt aktiva er egnet for formålet og trygt å betjene og vedlikeholde. Hvis organisasjonen utvider levetiden til et eksisterende aktiva må det hentes frem relevant sikkerhetsinformasjon, for eksempel historikk, for å sikre at det forblir sikkert i bruk.

Realitet mot forventet ytelse må overvåkes (se drifts- og vedlikeholdsfasen).

Ved kassering av jernbaneinfrastruktur eller rullende materiell må organisasjonen håndtere risikoene ved å ta aktiva ut av drift.

Håndtering av endringer i sikkerhetskritiske aktiva

I situasjoner der organisasjonen ønsker å endre konfigurasjonsgrunnlaget for sikkerhetskritiske aktiva, må det implementeres prosess for endringsstyring for å sikre effektiv risikostyring, og etableres et konfigurasjonsgrunnlag for alle sikkerhetskritiske aktiva med tilknyttet programvare (enten integrert i

eksisterende systemer eller frittstående programvare). Hvis en operatør endrer konfigurasjonsgrunnlaget for sikkerhetskritiske aktiva, må man der det er det mulig:

- *Håndtere risikoer som følge av endringer i sådan aktiva;*
- *Registrere serienummer og modellnummer;*
- *Validere funksjonelle krav mot spesifikasjoner og risikostyringstiltak;*
- *Kontrollere frigjøring av konfigurasjonselementer; og*
- *Sikre at status på alle aktiva under konfigurasjonsstyringen er oppdatert.*

Organisasjonens endringer i etablerte grunnlag, driftsforhold eller vedlikeholdsplaner for sikkerhetskritiske aktiva, må ikke redusere sikkerheten ved jernbanedriften på noen måte.

Anvendelse av felles sikkerhetsmetoder

Det er en prosess/prosedyre for å påse at enheter som er ansvarlig for vedlikehold (f.eks. ECM), bruker kontrollen av anvendelse av CSM vedrørende risikovurdering og CSM vedrørende overvåking der det er aktuelt (dvs. enten som kreves av lov og/eller er avtalefestet).

Det å ta hensyn til menneskelige og organisatoriske faktorer og forbedre sikkerhetskulturen vil ha en positiv innvirkning på samsvar med det relevante kravet til sikkerhetsstyringssystemet, og bevis på dette finnes i:

Organisasjonens risikoregister inneholder sikkerhetsrisikoer knyttet til alle faser som inngår i aktivaforvaltningens livssyklus og identifiserer underliggende menneskelige og organisatoriske faktorer relaterte grunnårsaker for hvert risikoscenario knyttet til aktivaets livssyklusstyring.

Organisasjonens program må spesifisere et rammeverk for hvordan identifiserte menneskelige og organisatoriske risikoer vil bli gjennomgått, akseptert og utviklet for å komme frem til løsninger gjennom hele prosessen for design og endringsstyring. Programmet må spesifisere forholdet til andre parter knyttet til design eller endringer.

For eksempel:

- *Sluttbrukere er en del av behovsanalysen; dette kan inkludere oppgaveanalyser og intervjuer, noen representanter for personalet er involvert fra design til testfaser;*
- *Det er prosedyrer og dedikerte midler for å sikre en klar kommunikasjon mellom drifts- og vedlikeholdsteam, så vel som med ECM(er);*
- *Sluttbrukere er også involvert i endringshåndteringsprosessene, inkludert automatisering. Tilbakemelding kan gis av ansatte til prosjektteamet, og denne tilbakemeldingen analyseres og forbedringstiltak iverksettes. Møtereferatene og rapportene om endringsledelse viser tydelig deres engasjement og hensynet til deres bekymringer;*
- *Alle berørte brukere identifiseres som en del av risikovurderingen og opplæring gis til dem som en del av kompetansestyringssystemet, for å sikre at personalet forblir kompetent;*
- *Produsenter og leverandører er involvert i prosessen med design og endringsledelse for å sikre passende hensyn til menneskelige faktorer.*

Informasjon om bruken av verktøy for sikkerhetsvarsling (SAIT) tilbys. **(se 5.4.3)**.

5.2.6 Referanser og standarder

- *ECM-retningslinjer*
- *ERA avklaringsnotat om sikker integrasjon*
- *CENELEC - EN50126 Jernbaneapplikasjoner — Spesifikasjon og demonstrasjon av pålitelighet, tilgjengelighet, vedlikeholdstilpasning og sikkerhet (RAMS) Del 1: Elementært, krav og generelt, prosess*
- *Organ for nasjonal jernbanesikkerhet — Veileder til aktivaforvaltning (2019)*

- *ISO 55000:2014 Forvaltning av anlegg og verdier - Oversikt, prinsipper og terminologi*
- *ISO 55001:2014 Forvaltning av anlegg og verdier - Styringssystemer - Krav*

5.2.7 Sjekkpunkter

Fra et tilsynsperspektiv er det viktig at det fokuseres på forvaltningen av aktivaet gjennom hele levetiden, fra design til kassering, og ikke på individuelle feil i aktivaforvaltningen, med mindre disse går direkte utover sikkerheten.

Tilsynet bør ta i betraktning hvordan eksisterende aktiva som er utdatert i henhold til gjeldende standarder, håndteres og vedlikeholdes.

Tilsyn bør vurdere om og hvordan organisasjonen bruker SAIT.

5.3 Leverandører og samarbeidspartnere

5.3.1 Lovbestemt krav

5.3.1. Organisasjonen skal identifisere og kontrollere sikkerhetsrisikoer som oppstår fra utkontrakterte aktiviteter, herunder drift eller samarbeid med entreprenører, partnere og leverandører.

5.3.2. For å kontrollere sikkerhetsrisikoene som er nevnt i punkt 5.3.1, skal organisasjonen definere kriteriene for valg av entreprenører, partnere og leverandører og kontraktskravene de må oppfylle, inkludert:

(a) de juridiske og andre kravene som er knyttet til sikkerhet (se 1. Organisasjonens driftskontekst);

(b) det kompetansenivået som kreves for å levere oppgavene fastsatt i kontrakten (se 4.2. Kompetanse);

(c) ansvaret for oppgavene som skal utføres;

(d) forventet sikkerhetsytelse som skal opprettholdes under kontrakten;

(e) forpliktelsene knyttet til utveksling av sikkerhetsrelatert informasjon (se 4.4. Informasjon og kommunikasjon).

(f) sporbarheten til sikkerhetsrelaterte dokumenter (se 4.5. Dokumentert informasjon).

5.3.3. I samsvar med prosessen fastsatt i artikkel 3 i forordning (EU) nr. 1078/2012, skal organisasjonen overvåke:

(a) sikkerhetsytelsen til alle aktiviteter og operasjoner til entreprenører, partnere og leverandører for å sikre at de overholder kravene fastsatt i kontrakten;

(b) entreprenørers, partneres og leverandørers bevissthet om sikkerhetsrisikoer de medfører for organisasjonens virksomhet.

5.3.2 Formål

Søker må vise at man har evnen til å identifisere, vurdere og kontrollere risikoer som oppstår i forbindelse med leverandøraktiviteter eller andre samarbeidspartneres aktiviteter. Det er ikke bare et spørsmål om risikovurdering, og det krever heller ikke en liste over alle risikoer eller kategorier av relevante risikoer, men det krever at søkeren viser hvordan systemene og prosedyrene i sin helhet er designet og organisert for å tilrettelegge for identifikasjon, vurdering og kontroll av disse risikoene. Dette inkluderer behovet for at kontrakten skal angi hvordan sikkerhetsrelatert informasjon utveksles. Bruk av nøye formulerte avtaler er en allment akseptert måte å håndtere risiko på. Hovedansvaret for å administrasjon av leverandører og kontroll av leveransen mot de fastsatte spesifikasjonene, ligger imidlertid hos organisasjonen. Bruken av leverandører eller underleverandører betyr ikke at jernbanevirksomheten eller infrastrukturforvalteren delegerer noe av ansvaret sitt for å sikre at de avtalte tjenestene utføres til de standarder som er fastsatt før driften starter.

Søkeren skal demonstrere at denne har prosesser på plass for å fastsette kompetansen til entreprenører og andre leverandører, og til å vurdere sikkerhetsytelsen deres som en del av anskaffelsesprosessen.

Hver enkelt organisasjon er ansvarlig for å utføre overvåkingsprosessen som er fastsatt i CSM om overvåking, og sikre at det gjennom avtaleordninger føres tilsyn med risikokontrolltiltak som er implementert av leverandørene i samsvar med CSM. Hvis organisasjoner identifiserer eventuelle relevante sikkerhetsrisikoer som mangler eller funksjonsfeil på teknisk utstyr, kreves det i henhold til CSM om overvåkning å rapportere disse risikoene til andre involverte parter, slik at de kan ta nødvendige grep for å ivareta sikkerheten ved systemet.

5.3.3 Forklarende merknader

Ytterligere informasjon om avtaleordninger og samarbeid finnes i Vedlegg 3.

Hvordan blir menneskelige og organisatoriske faktorer og sikkerhetskultur integrert?

Prosessene som er satt opp av selskapet for å kontrollere sine risikoer inkluderer aktivitetene til entreprenører, partnere og leverandører. Risikoer og sikkerhetstiltak som er definert av selskapet, kommuniseres til entreprenører, leverandører og samarbeidspartnere og inkluderes i spesifikasjonene for hver type utkontraktert aktivitet. Dette kan også dekke overvåking av ytelsen til den utkontrakterte aktiviteten (se avsnitt ***6.1 Overvåking*** nedenfor).

Strategien for menneskelige og organisatoriske faktorer kan dekke relevante spørsmål knyttet til entreprenører, partnere og leverandører.

Roller, ansvar og kompetanse som er nødvendig for å utføre de utkontrakterte oppgavene, er klart definert i kontraktene. Disse kompetansene er de samme som er beskrevet i kompetansestyringssystemet for internt personale.

Kontraktene inneholder bestemmelser om hvordan sikkerhetsinformasjon og kommunikasjon forvaltes for å sikre samme sikkerhetsnivå som beskrevet for intern informasjon og kommunikasjon. Dette inkluderer også kunnskapsdeling.

5.3.4 Bevis

- *Bevis på hvordan organisasjonens sikkerhetsstyringssystem samhandler med styringssystemene til leverandører for å kontrollere foreliggende risikoer;* ***(5.3.1)***
- *Bevis på at det utarbeides avtaleordninger basert på resultater fra risikovurdering;* ***(5.3.1) (se også 3.1)***
- *Det foreligger prosesser som beskriver hvordan menneskelige og organisatoriske faktorer skal håndteres og formidles i forbindelse med bruk av underleverandører, samt administrasjon av dem;****(5.3.1)***
- *Bevis på hvordan organisasjonen styrer dokumentasjonen som omfatter leverandører;* ***(5.3.2(a)-(d))***
- *Bevis på hvordan organisasjonen velger ut leverandører for å sikre at de er kompetente og at sikkerhetsrisikoer håndteres korrekt;* ***(5.3.2(a)-(e))***
- *Det foreligger prosess for å sikre formidling av viktig sikkerhetsinformasjon til eller fra leverandører;* ***(5.3.2 (d))***
- *Bevis på hvordan dokumentkontrollprosedyren sikrer håndtering av sikkerhetsrelaterte dokumenter som er relevante for entreprenører og leverandører (5.****3.2(f)).***
- *Prosessen eller prosedyren for overvåking som organisasjonen har etablert for å sikre at leverandørenes samarbeidspartnere eller ansatte er i stand til å håndtere risikoene de står overfor;* ***(5.3.3 (a)-(b))***
- *Bevis på at samarbeidspartnere eller leverandører føres regelmessig tilsyn med i samsvar med CSM om overvåking (Forordning (EU) 1078/2012) for å sikre at deres produkter eller tjenester oppfyller spesifikke krav og sikkerhetsmålsettinger.* ***(5.3.3 (a)) (se også 6.1)***

5.3.5 Eksempler på bevis

Bevis for sikkerhetsmålene som entreprenører, partnere og leverandører forventes å oppnå, og indikatorene som vil bli brukt for å måle dem, er oppgitt.

Dokumentstyringsprosedyren som omfatter organisasjonsstandarder som skal anvendes av samarbeidspartnere og leverandører (se også 4.5.1.1 (e) Dokumentstyring).

En liste/oversikt over samarbeidspartnere og leverandører for intern eller ekstern bruk, med spesifikasjon av produkter og/eller tjenester de leverer **(se også 4.5.1.1 (d) og (e))** og en beskrivelse av hva som kan virke inn på sikkerheten, sammen med tiltakene for å kontrollere de identifiserte risikoene (f.eks. utveksling av informasjon, klargjøring av ansvar, opplæring) **(se også 3.1.1.1 (a))**.

Det å ta hensyn til menneskelige og organisatoriske faktorer og forbedre sikkerhetskulturen vil ha en positiv innvirkning på samsvar med det relevante kravet til sikkerhetsstyringssystemet, og bevis på dette finnes i:

Den aktuelle prosessen for revisjons-/inspeksjonsplanlegging for samarbeidspartnere og leverandører med noen eksempler på sådan aktiviteter, for eksempel revisjons-/inspeksjonsrapporter eller funn og tilknyttede handlingsplaner.

Strategien for menneskelige og organisatoriske faktorer forklarer hvordan disse problemene dekkes hos entreprenører, partnere og leverandører.

I en prosedyre som entreprenører, samarbeidspartnere og leverandører velges ut og føres tilsyn med. Prosedyren gjør det klart at standardene som skal anvendes av leverandørene, er de samme som for direkte ansatt personale og hva rollene og ansvaret omfatter. Prosedyren dokumenterer den nødvendige informasjonsutvekslingen mellom sikkerhetsstyringssystemene til søkeren og samarbeidspartnere/leverandører.

Prosedyren for kompetansestyringssystemet som knytter seg til systemene hos samarbeidspartnere og leverandører.

Prosessen/prosedyren for administrasjon av samarbeidspartnere og leverandører må inkludere hvordan samhandlingsrisikoer som oppstår som følge av samarbeidspartneres eller leverandørers virksomheter håndteres og meddeles hvordan utveksling av informasjon er integrert i SMS det er relevant for, og hvordan disse inngår i avtaleordninger og hvordan utvekslingen av informasjon integreres i sikkerhetsstyringssystemet.

Prosessen eller prosedyren for hvordan relevante krav som gjelder samarbeidspartnere eller leverandører identifiseres og meddeles, og der det er relevant, hvordan de inngår i avtaleordninger som er korrekt dokumentert i dokumentstyringssystemet, slik at informasjonen kan spores.

Prosedyren for dokumentstyringssystemet for administrasjon av sertifikater, godkjenninger, anerkjennelser eller annen form for dokumentasjon som viser at kravene mot samarbeidspartnere eller leverandører etterleves, og som kontrollerer gyldigheten over tid (f.eks. gjennom tilsyn).

5.3.6 Sjekkpunkter

Ved tilsyn i en organisasjon kan det for å få et komplett bilde av omfanget av kontroll og overvåkning, være nødvendig å gjennomføre tilsyn hos en samarbeidspartner eller leverandør sammen med en som arbeider i organisasjonen. Det kan også være nødvendig å få tilgang til dokumentasjonen som samarbeidspartneren eller leverandøren jobber med, og undersøke hvordan den er tilknyttet prosedyrene i organisasjonens sikkerhetsstyringssystem.

Ordninger for å sikre at samarbeidspartneres og leverandørers sikkerhetsytelse og kompetanse er en integrert del av anskaffelsesprosessen.

5.4 Endringsstyring

5.4.1 Lovbestemt krav

5.4.1. Organisasjonen skal implementere og kontrollere endringer i sikkerhetsstyringssystemet for å opprettholde eller forbedre sikkerhetsytelsen. Dette skal inkludere beslutninger på de ulike stadiene av endringshåndteringen og den påfølgende gjennomgangen av sikkerhetsrisikoer (se 3.1.1. Risikovurdering).

5.4.2 Formål

Det er viktig at søker kan identifisere og reagere på nye risikoer som kan oppstå ved driften, ved å CSM for risikovurdering og annen vurdering (Forordning (EU) 402/2013) etter hva som egner seg. Sikkerhetsstyringssystemet må vise at det foreligger prosedyrer for å vurdere disse risikoene og iverksette nye risikokontrolltiltak der det er aktuelt. Dette skal imøtekomme alle typer og nivåer i endringene: betydelige og mindre, permanente og midlertidige, umiddelbart og langsiktig. Den bør gjelde endringer av teknisk, operasjonell eller organisatorisk karakter.

5.4.3 Forklarende merknader

Ikke alle endringer er underlagt risikovurdering **(5.4.1)**. Når endringer håndteres aktivt gjennom andre prosesser i sikkerhetsstyringssystemet, som den daglige driften, trenger de ikke å anses som en endring som krever håndtering gjennom den formelle endringsprosessen.

Roller, ansvar og ansvarlighet som skal defineres **(se også 2.3)** inkluderer endringsstyring **(5.4.1)**, for eksempel tilordning av roller til et styre for endringsstyringen.

Hvordan blir menneskelige og organisatoriske faktorer og sikkerhetskultur integrert?

Prosessen for endringsledelse åpner for at risikoer kan vurderes på en proporsjonal og robust måte, inkludert menneskelige og organisatoriske faktorer (HOF) når det er hensiktsmessig, og for å kunne iverksette kontrolltiltak.

De ansatte konsulteres under endringsprosessen **(se også 2.4)**.

Sikkerhetsrisikoer som følge av nedskjæringer eller outsourcing av aktiviteter, herunder drift eller samarbeid med samarbeidspartnere og leverandører, håndteres og prioriteres på lik linje med interne risikoer.

5.4.4 Bevis

- *En beskrivelse av prosessen for endringsstyring;* ***(5.4.1)***
- *En beskrivelse av prosedyrene og metodene som anvendes til å evaluere nye eller endrede risikoer og implementere nye;* ***(5.4.1)***
- *Kontrolltiltak inkludert skilting som anviser hvor detaljerte prosesser kan finnes;* ***(5.4.1)***
- *Informasjon om hvordan organisasjonen identifiserer vesentlige endringer og beslutninger om når man skal anvende prosessene i CSM vedrørende risikovurdering og annen vurdering, eller når man skal utføre risikovurdering i henhold til prosedyrene for sikkerhetsstyringssystemet;* ***(5.4.1)***
- *Informasjon om ordninger i endringsstyringen som organisasjonen har etablert for administrasjon av vogngodkjenninger og endringer i felles sikkerhetssertifikat eller sikkerhetsgodkjenning;* ***(5.4.1)***
- *Informasjon om prosessen for varsling til relevante sikkerhetsmyndigheter om endringene, før ny jernbanetransport settes i drift.* ***(5.4.1)***

5.4.5 Eksempler på bevis

En kopi av prosedyren for endringsstyring som en del av søknaden. Dette dokumentet dekker behovet for risikovurdering av alle endringer i henhold til ulike lovfestede krav. Et eksempel på et problem- og planleggingslogg som regelmessig blir vurdert ved fremdriften i endringene. Til sist skal prosedyren også dekke prosessen for hvordan relevante nasjonale sikkerhetsmyndigheter blir varslet om endringene.

Prosessen for endringsstyring viser til bruken av risikovurderingsprosessen og utfall tas i betraktning når man utvikler, implementerer og vurderer driftsprosesser.

Det å ta hensyn til menneskelige og organisatoriske faktorer og forbedre sikkerhetskulturen vil ha en positiv innvirkning på samsvar med det relevante kravet til sikkerhetsstyringssystemet, og bevis på dette finnes i:

Endringer i roller, ansvar, verktøy og utstyr, arbeidsmiljøer, prosesser og prosedyrer støttes av en analyse av menneskelige og organisatoriske faktorer som identifiserer mulige sikkerhetsrisikoer knyttet til endringen. Metoder som brukes, omfatter for eksempel oppgaveanalyse, brukervennlighetsanalyse, simulering, risikovurdering, HAZOP og sikkerhetsundersøkelse. Det er eksempler på endringer som skal innledes med risikovurdering ved bruk av menneskelige og organisatoriske faktorer. Spesielt gjelder dette endring av arbeidsprosedyrer på grunn av modifisert utstyr, endringer i arbeidsplaner eller omfordeling av ansvar.

I eksempler på prosjekter som viser hvordan menneskelige og organisatoriske faktorer har blitt tatt i betraktning som en del av styringen av endringsprosessen fra starten, gjennom analyse av virksomhetens behov: tekniske endringer som nytt utstyr eller oppgraderinger, organisatoriske eller operasjonelle endringer, med forventet innvirkning på eksisterende situasjon osv., og derved unngå dårlig design som ville ha svekket bedriftens ytelse. Det er møtereferater som analyserer effekten endringen vil ha på organisasjonens kultur, og hvordan dette er formidlet til ledelsen.

Roller og ansvar for å håndtere endring og tilhørende sikkerhetsrisikoer er tilstrekkelig definert, og kompetansestyringssystemet viser at ansvarlige er opplært til å integrere menneskelige og organisatoriske faktorer.

Prosjektfarelogg opprettes i løpet av hvert prosjekt og identifiserer underliggende menneskelige og organisatoriske faktorer-relaterte grunnårsaker for hvert sikkerhetsrelatert risikoscenario. Det inkluderer også potensielle konsekvenser for entreprenører, partnere og leverandører, som er involvert når det er nødvendig.

Prosjektrisikovurderinger gjennomføres i de tidlige stadiene av prosjektet, og disse involverer sluttbrukere. Risikovurdering blir sett på som en pågående prosess som tar opp pågående problemstillinger under endringsprosessen (f.eks. utviklende forutsetninger og oppdatering av nye identifiserte risikoer).

I administrative prosesser/ordninger mellom ulike organisasjoner, gi planer og prosjektdetaljer osv. til ulike parter. Fagforeninger og andre interessenter involveres tidlig i prosessen for store beslutninger eller endringer.

Verktøyene som brukes, er de samme som er angitt i kapittelet om risikovurdering, dvs. oppgaveanalyse, brukbarhetsanalyse, simulering, risikovurdering, HAZOP, sikkerhetsundersøkelse.

5.4.6 Sjekkpunkter

For å fastslå om ordninger for endringsstyring i sikkerhetsstyringssystemet er robuste nok, vil det være nødvendig å følge en rekke endringer av ulike typer gjennom den definerte prosessen for å påvise om de har (a) blitt håndtert hensiktsmessig og risikoer som følge av endringene er hensiktsmessig vurdert, og (b) om det har blitt innlemmet eventuelle erfaringer i revisjoner av prosedyrene i sikkerhetsstyringssystemet.

Vurdering av etterlevelse av ordningene i endringsstyringen mot CSM vedrørende risikovurdering.

Organisasjonen må ha på plass prosesser for implementering og kontinuerlig overvåking av relevante TSI-er, nasjonale bestemmelser og andre standarder, hvor det er hensiktsmessig å vise hvordan disse anvendes gjennom hele livssyklusen til utstyret eller driften.

5.5 Beredskapsstyring

5.5.1 Lovbestemt krav

5.5.1. Organisasjonen skal identifisere nødsituasjoner og tilhørende rettidige tiltak som skal iverksettes for å håndtere dem (se 3.1.1. Risikovurdering) og for å gjenopprette normale driftsforhold i samsvar med forordning (EU) nr. 2015/995.

5.5.2. Organisasjonen skal sikre at, for hver identifisert type nødssituasjon:

(a) kan nødetatene kontaktes umiddelbart;

(b) nødetatene gis all relevant informasjon både på forhånd, for å forberede sin beredskap, og ved en nødsituasjon;

(c) førstehjelp ytes internt.

5.5.3. Organisasjonen skal identifisere og dokumentere rollene og ansvaret til alle parter i samsvar med forordning (EU) nr. 2015/995.

5.5.4. Organisasjonen skal ha handlingsplaner, varsler og informasjon i nødstilfeller, inkludert ordninger for å:

(a) varsle alle ansatte med ansvar for beredskapsledelse;

(b) kommunisere informasjon til alle parter (f.eks. infrastrukturforvalter, jernbaneforetak, entreprenører, myndigheter, nødetater), inkludert nødinstruksjoner for passasjerer;

(c) ta eventuelle avgjørelser som kreves i samsvar med typen nødssituasjon.

5.5.5. Organisasjonen skal beskrive hvordan ressurser og midler til beredskapsledelse er fordelt (se 4.1. Ressurser) og hvordan opplæringskrav er identifisert (se 4.2. Kompetanse).

5.5.6. Beredskapsordningene testes jevnlig i samarbeid med andre interessenter og oppdateres når det er hensiktsmessig.

5.5.7. Organisasjonen skal sørge for at kompetent personell med ansvar, med tilstrekkelige språkkunnskaper, enkelt og uten opphold kan kontaktes av infrastrukturforvalteren og gi denne det riktige informasjonsnivået.

5.5.7. Organisasjonen skal koordinere beredskapsplaner med alle jernbaneforetak som opererer på organisasjonens infrastruktur, med nødetatene, for å lette deres raske inngripen, og med enhver annen part som kan være involvert i en nødsituasjon.

5.5.8. Det er en prosedyre for å kontakte enheten som er ansvarlig for vedlikehold eller jernbanekjøretøyholder i nødstilfelle.

5.5.8. Organisasjonen skal ha ordninger for å stanse driften og jernbanetrafikken umiddelbart, om nødvendig, og informere alle interesserte parter.

5.5.9. For grenseoverskridende infrastruktur skal samarbeidet mellom de relevante infrastrukturforvalterne legge til rette for nødvendig koordinering og beredskap for de kompetente nødetatene på begge sider av grensen.

5.5.2 Formål

Robuste systemer for beredskapsplanlegging er avgjørende for enhver HMS-ansvarlig, og må dekke informasjonen som skal formidles til beredskapstjenestene, slik at de kan utarbeide hendelsesresponsplaner. Aspektene ved sikkerhetsstyringssystemet som er direkte relevante for beredskapsordningene, for eksempel opplæring i nødhjelp og utprøving av beredskapsplaner, er også viktig.

5.5.3 Forklarende merknader

Nødsituasjoner **(5.5.1)** er tilknyttet resultatene fra organisasjonens risikovurdering, selv om TSI-OPE (se punkt 4.2.3.7) har en omfattende liste over nødssituasjoner.

Førstehjelp gitt internt **(5.5.4 (c))** betyr at selskapet er i stand til å administrere førstehjelp for nødsituasjoner identifisert i punkt 5.5.1.

Punktene 5.5.7 og 5.5.8 i lovteksten ovenfor erstattes av punktene i blå tekst der vurderingen gjelder Infrastrukturforvalter. **Punkt 5.5.9** i blått ovenfor gjelder kun infrastrukturforvalteren.

Hvordan blir menneskelige og organisatoriske faktorer og sikkerhetskultur integrert?

Beredskapsledelse er knyttet til ressursstyring, roller og ansvar, og kompetansestyringssystemet, for å sikre personalets bevissthet og opplæring (inkludert vedlikehold av kompetanse). Dette inkluderer utvikling av kompetanse (inkludert ikke-tekniske ferdigheter som motstand mot stress, motstandskraft...) for aktørene som er opptatt av beredskapsplaner og prosedyrer.

5.5.4 Bevis

Søker forventes å gi oversikt over:

- *Typer nødstilfeller som dekkes, herunder nedsatt drift og foreliggende prosedyrer for å håndtere dem;* ***(5.5.1)***
- *Informasjon fra søker for å gjøre det mulig for beredskapstjenestene å planlegge hvordan de skal respondere ved en storulykke på jernbanen, der det er hensiktsmessig å henvise til forpliktelser i henhold til gjeldende EU-lovgivning og eventuelle relevante grenseoverskridende ordninger;* ***(5.5.2 (a) og (b))***
- *Det forventes at bedrifter i sin risikovurdering identifiserer hvilken førstehjelp de selv kan yte og hva nødetatene må yte* ***(5.5.2 (c)).***
- *Planer, roller og ansvar (herunder for dem med dedikert kompetanse som er satt til å bistå infrastrukturforvalteren eller omvendt), opplæring og ordninger for å opprettholde kompetansen, og ordninger for effektiv kommunikasjon med beredskapstjenestene, relevant personale og kommunikasjon med dem som berøres av uønskede hendelser som passasjerer eller berørte tredjeparter (dette skal inkludere et dokument som beskriver alle parters roller og ansvar, hvordan ressurser og midler er tilordnet og der krav til opplæring er identifisert); prosedyrene for å komme tilbake til normal drift etter en nødsituasjon;* ***(5.5.1), (5.5.3), (5.5.4 (a)-(c)), (5.5.5), (5.5.7) (5.5.8 og 5.5.9 fra infrastrukturforvaltere kun lovpålagte krav)***
- *Slike spesifikke aspekter ved sikkerhetsstyringssystemet som er direkte relevante for beredskapsordningene, for eksempel opplæring i nødhjelp og utprøving av beredskapsplaner, er også viktig for å identifisere eventuelle svakheter;* ***(5.5.6)***
- *Prosedyren for å kontakte ansvarlig enhet som har ansvaret for vedlikehold eller rettighetshaveren, ved nødsituasjoner som berører en av deres vogner;* ***(5.5.8 fra jernbanevirksomheten kun lovpålagte krav)***

5.5.5 Eksempler på bevis

En kopi av prosedyrer for beredskapsstyring og tilknyttede planer (f.eks. prosedyrer for berging). Prosedyren må dekke hele jernbanenettet som drives, med spesifikke ordninger som er nødvendige for tunneler og andre

steder med høy risiko og for grenseoverskridende samarbeid, bemanning og roller og ansvar, og som inkluderer linker til beredskapsordninger hos infrastrukturforvalteren og hvordan man kommer i kontakt med andre relevante parter, som ECM, der det er relevant. Når et jernbaneforetaks virkeområde inneholder flere infrastrukturforvaltere, bør jernbaneforetaket ta hensyn til forskjellene mellom beredskapsordningene (og brukeravtalene) med disse infrastrukturforvalterne.

Nødprosedyrene skal omfatte prosessen der ofre for uønskede hendelser og deres pårørende får veiledning om klageprosedyrer.

Prosedyren (dersom relevant) må inneholde informasjon om hva som skjer i en nødssituasjon der farlig gods er involvert, og organisasjonen (jernbanevirksomheten) skal ha etablert en prosess for å sikre at:

- *Lastefirmaet, tankvognens eier der den er privateid, eieren eller rettighetshaveren og operatøren i tilfelle en tank, mottakeren, etc., kan kontaktes umiddelbart.*
- *Infrastrukturforvalteren må gis relevant informasjon så snart som mulig (f.eks. vognens registreringsnummer, vognens posisjon i togrekken, UN-nummer, RID-klassifiseringskode og fareidentifikasjonsnummer for farlig gods i samsvar med RID-bestemmelsene);*
- *Organisasjonen (infrastrukturforvalteren) må ha etablert en prosess for å sikre at myndighetene (f.eks. redningstjenester, politi, andre beredskapstjenester og myndigheter) får relevant informasjon om farlig gods (se eksemplene ovenfor).*

Det å ta hensyn til menneskelige og organisatoriske faktorer og forbedre sikkerhetskulturen vil ha en positiv innvirkning på samsvar med det relevante kravet til sikkerhetsstyringssystemet, og bevis på dette finnes i:

Prosedyren som etablerer scenarioene for identifiserte potensielle nødsituasjoner, vurderer risikoene knyttet til de forskjellige situasjonene (med de identifiserte grensesnittene), inkludert de som oppstår fra menneskelige og organisatoriske faktorer. Sikkerhetstiltakene som er identifisert for å redusere disse risikoene, er integrert i de berørte planene, prosessene og prosedyrene (inkludert driftsprosedyrer).

Prosedyrene som beskriver sammenhengen mellom beredskapsplanlegging og risikostyring.

Referanse i prosedyren til kompetansestyringssystemets krav for ansatte som skal respondere på nødsituasjoner, samt sørge for at innleid bemanning kan imøtekomme de samme standardene.

Det er en prosedyre som beskriver ledelsen av beredskapsøvelser (teoretisk og praktisk) på jevnlig basis med alle berørte parter (både interne og eksterne), hvordan tilbakemeldinger fra beredskapsøvelser samles inn ved hjelp av overvåkingsaktiviteter (se avsnitt ***6.1 Overvåking*** nedenfor). for å iverksette handlinger/tiltak for å forbedre beredskapsplanene og -prosedyrene og kompetansen til alle berørte aktører (se ***7.2. Kontinuerlig forbedring*** nedenfor).

Det er en prosedyre som inneholder informasjon om hvordan beredskapsøvelser brukes til kompetansestyring og til å forbedre prosessen.

Det er en prosedyre som beskriver kontinuitetsstyringen som skal iverksettes for å unngå avvik i standarder/prosedyrer når de utsettes for en uventet innvirkning på driften.

Det er en prosedyre som beskriver hvordan beredskapsplanene kommer på plass for å sikre en effektiv og rask intervensjon for å redde liv etter en ulykke.

Bestemmelsene sikrer at organisasjonens ansatte og nødetater har enkel tilgang til dokumentasjon knyttet til beredskaps- og forretningskontinuitetsplaner for å unngå ytterligere forverring av situasjonen.

Det er en prosedyre som beskriver hvordan anbefalinger gitt av andre parter (myndigheter, nødetater) og beste praksis vurderes for gjennomgang av beredskapsplanene og prosedyrene.

5.5.6 Sjekkpunkter

For å kunne korrekt vurdere prosedyrene i sikkerhetsstyringssystemet for beredskapsstyring, kan det være nødvendig å kryssjekke prosedyrene i sikkerhetsstyringssystemet med prosedyrene hos relevante aktører det samhandles med (spesielt forholdet mellom sentrale aktører som jernbanevirksomhet, infrastrukturforvalter og beredskapstjenestene) for å sikre at prosessene som foreligger for håndtering av slike hendelser er helhetlige.

Sjekk at det foreligger planer for alle forutsigbare nødsituasjoner.

Ordninger for utprøving av beredskapsplaner og koordinerte ordninger med beredskapstjenester, og ikke begrenset til teoretiske øvelser.

Det må foreligge samhandlingsordninger med andre interessenter og inkludere testkontroll, kommunikasjon, koordinering og kompetanse.

EUROPEAN UNION AGENCY FOR RAILWAYS

For et jernbanesystem som fungerer bedre for samfunnet.

6 Ytelsesevaluering

6.1 Overvåking

6.1.1 Lovbestemt krav

6.1.1.	Organisasjonen skal utføre overvåking i samsvar med forordning (EU) nr. 1078/2012: (a) for å kontrollere riktig anvendelse og effektiviteten til alle prosesser og prosedyrer i sikkerhetsstyringssystemet, inkludert operasjonelle, organisatoriske og tekniske sikkerhetstiltak; (b) for å kontrollere riktig anvendelse av sikkerhetsstyringssystemet som helhet, og om det oppnår de forventede resultatene; (c) for å undersøke om sikkerhetsstyringssystemet er i samsvar med kravene i denne forskriften; (d) for å identifisere, implementere og evaluere effektiviteten til de korrigerende tiltakene (se 7.2. Kontinuerlig forbedring), etter behov, hvis det oppdages et relevant tilfelle av manglende overholdelse av punkt (a), (b) og (c).
6.1.2.	Organisasjonen skal jevnlig overvåke på alle nivåer i organisasjonen utførelsen av sikkerhetsrelaterte oppgaver og gripe inn dersom disse oppgavene ikke blir utført på riktig måte.

6.1.2 Formål

Organisasjonen skal fremlegge bevis på at det foreligger en prosess for å overvåke anvendelsen av og effektiviteten ved sikkerhetsstyringssystemet, og at denne prosessen er egnet i forhold til driftens størrelse, omfang og type. Organisasjonen skal demonstrere at prosessen kan identifisere, evaluere og korrigere eventuelle mangler i funksjonen til SMS.

6.1.3 Forklarende merknader

Effektiviteten av kontrolltiltakene betyr at organisasjonen har en prosess på plass for å kontrollere at når en risikovurdering er utført, og det er gjennomført hensiktsmessige kontrolltiltak, vil disse vurderes etter en viss tid for å forsikre seg om at forventet reduksjon i sikkerhetsrisiko som følge av anvendelsen av tiltakene er oppnådd **(6.1.1 (d))**.

Hvordan blir menneskelige og organisatoriske faktorer og sikkerhetskultur integrert?

Selvkritiske og objektive vurderinger av organisasjonens sikkerhetskulturprogrammer, praksis og ytelse, utføres rutinemessig. Sikkerhetsinformasjon fra for eksempel korrigerende handlingsprogrammer, menneskelig yteevne, hendelses- og ulykkesanalyse, undersøkelser og relevant intern og ekstern driftserfaring, samles systematisk inn og evalueres for å identifisere trender og unngå organisatoriske og individuelle avvik eller selvtilfredshet.

En vellykket vurdering kan bidra til å forbedre sikkerhetsytelsen ved å danne et klart bilde av hvordan organisasjonens sikkerhetskultur påvirker sikkerheten. Evalueringen søker å identifisere sterke og svake sider i sikkerhetskulturen ved å sammenligne hvordan kulturen er, med hva den skal ta sikte på. Dette gjør det

mulig å prioritere områder for forbedring og gjennomføring av endringer, for eksempel i behandling, opplæring og atferd. Evaluering av sikkerhetskulturen er et middel for å arbeide proaktivt for å forbedre sikkerhetsytelsen og øke sikkerhetsmarginene. Det anbefales å foreta uavhengige evalueringer av sikkerhetskulturen hvert tredje til femte år, og organisatoriske egenvurderinger hvert år eller annethvert år.

6.1.4 Bevis

- *Informasjon om hvordan søkeren har implementert CSM vedrørende overvåking(Forordning (EU) 1078/2012); **(6.1.1 (a))***
- *Informasjon om hvordan overvåkingsprosessen kan se om de forventede resultatene blir oppfylt; **(6.1.1 (b))***
- *Bevis på at sikkerhetsstyringssystemet har blitt tilpasset som følge av korrigering av feil i sikkerhetsstyringssystemprosessene som er identifisert under overvåkingen**; (6.1.1 (c))***
- *Bevis på at det er en gjennomgang av effektiviteten av korrigerende tiltak iverksatt etter bevis på manglende overholdelse av prosessene i sikkerhetsstyringssystemet;**(6.1.1 (d))***
- *Organisasjonen bør på plass ha en prosess for å fastsette ytelsesstandarder og indikatorer for overvåking relatert til driftsprosesser, samt for gjennomførte endringer. Det bør være et program for kontinuerlig vurdering av ytelsen til prosesser relatert til menneskelige og organisatoriske faktorer, samt resultatene fra disse prosessene, for eksempel at personalet overholder implementerte prosedyrer, og bruker nytt utstyr korrekt. **(6.1.2)***
- *Sikkerhetsytelsen vurderes systematisk i lys av sikkerhetsforbedringsstrategien. Dette betyr at organisasjonen bør se etter hvordan forbedring av sikkerhetskultur passer inn i og er en del av målet om sikkerhetsforbedring.**(6.1.2)***

6.1.5 Eksempler på bevis

En redegjørelse som viser at CSM vedrørende overvåking (Forordning (EU) 1078/2012) er anvendt, og at det foreligger en prosedyre som dekker denne aktiviteten. Prosedyren beskriver hvordan ytelsene i forhold til sikkerhetsmålene måles og korrigeres gjennom endringsstyring og risikovurderingsprosessen, og hvordan feil i sikkerhetsstyringssystemet blir korrigert.

Det å ta hensyn til menneskelige og organisatoriske faktorer og forbedre sikkerhetskulturen vil ha en positiv innvirkning på samsvar med det relevante kravet til sikkerhetsstyringssystemet, og bevis på dette finnes i:

Organisasjonen har prosesser og prosedyrer for systematisk å vurdere at ordningene for å inkludere menneskelige og organisatoriske faktorer er tilstrekkelige, og at de oppnådde resultatene er i samsvar med ytelsesstandardene.

Organisasjonen har prosesser og prosedyrer for systematisk å vurdere yteevnen til personalet i sikkerhetskritiske arbeidsoppgaver. Disse prosessene er basert på en proaktiv tilnærming, som fastsetter standarder for yteevne og systematisk evaluering. Det anvende bevisbaserte metoder, for eksempel bemanningsstyring.

Overvåkingsprosessen inkludert bestemmelser om tildelte ressurser, inkludert bemanning og kompetanse for personalet som er involvert i overvåkingsaktiviteter.

Overvåkingen som utføres ved å integrere kontrollen av implementeringen og effektiviteten av prosesser og prosedyrer som integrerer menneskelige og organisatoriske faktorer sikkerhetstiltak avledet fra risikovurderingsprosessen. Overvåkingen integrerer derfor spesifikke menneskelige og organisatoriske faktorer, inkludert i driftsaktiviteter. Dette dekker også vurdering og vedlikehold av kompetanse (tekniske og ikke-tekniske ferdigheter, holdninger, atferd...) for ansatte (internt eller eksternt) som utfører sikkerhetsoppgaver (se avsnitt ***4.2 Kompetanse*** ovenfor).

Overvåkingen som skal gjennomføres, herunder analysen av hvor vellykket strategien for menneskelige og organisatoriske faktorer har vært.

Overvåkingsprosessen inkludert analysen av rapporteringen gjort av personalet. Sikkerhetshåndteringssystemet inneholder en rettferdig kulturprosess, der grov uaktsomhet, forsettlige krenkelser og destruktive handlinger straffes. Målet er å utvikle en rapporteringskultur der ansatte føler seg komfortable med å rapportere fordi de ikke får skylden for utilsiktede feil eller mangler. Dette forklarer også hvordan sikkerhetsrelaterte problemer/hendelser kan rapporteres av ansatte, entreprenører eller andre relevante interessenter.

Overvåkingsprosessen er en del av å forbedre den organisatoriske opplæringen. Analysen av rapporteringen fra personalet analyseres som en del av overvåkingsprosessen med sikte på å forbedre sikkerhetstiltakene og prosessene og prosedyrene i sikkerhetsstyringssystemet.

Overvåkingsresultatene analyseres fra et sikkerhetskulturperspektiv og inkluderes i prosessen for sikkerhetskulturvurdering.

6.1.6 Referanser og standarder

- *CSM for overvåking-søknadsveiledning*

6.1.7 Sjekkpunkter

Sjekk om overvåkingsprosessen og funnene og tiltakene som er iverksatt som følge av dem, er avgjørende for å fastslå om sikkerhetsstyringssystemet er et "dynamisk" dokument i utvikling ettersom erfaring medfører forbedring, eller om det er et statisk dokument som ikke endres over tid.

Undersøkelser av en rekke viktige risikoområder og kontroller og utprøving for korrekt anvendelse og effektivitet gjennom sikkerhetsstyringssystemet er ytterst viktig, slik at NSA kan etablere samsvar med CSM vedrørende overvåking.

6.2 Internrevisjon

6.2.1 Lovbestemt krav

6.2.1. Organisasjonen skal gjennomføre internrevisjoner på en uavhengig, upartisk og transparent måte for å samle inn og analysere informasjon i forbindelse med sine overvåkingsaktiviteter (se 6.1. Overvåking), inkludert:

(a) En tidsplan for planlagte internrevisjoner som kan revideres avhengig av resultatene fra tidligere revisjoner og overvåking av ytelse;

(b) Identifisering og valg av kompetente revisorer (se 4.2. Kompetanse);

(c) Analysen og evalueringen av resultatene av revisjonene;

(d) Identifisering av behovet for korrigerende eller forbedrende tiltak;

(e) Verifiseringen av gjennomføringen og effektiviteten av disse tiltakene;

(f) Dokumentasjonen knyttet til gjennomføring og resultater av revisjoner;

(g) Formidling av resultatene av revisjoner til toppledelsen.

6.2.2 Formål

Søker skal vise at det foreligger et internt revisjonssystem som involverer kompetent personale og genererer meningsfulle resultater, og som behandles av ledelsen og sikrer at sikkerhetsstyringssystemet fungerer i samsvar med lovfestede krav.

6.2.3 Forklarende merknader

Internrevisjoner **(6.2.1)** er overvåkingsverktøy i henhold til CSM vedrørende overvåking (Forordning (EU) 1078/2012). Selv om det er et eget krav, er det ment å bidra til å nå målene med overvåking i samsvar med CSM vedrørende overvåking.

Internrevisjonene **(6.2.1)** tar sikte på å innhente opplysninger om hvorvidt sikkerhetsstyringssystemet er i samsvar med gjeldende krav **(6.1.1 (c))** og at det gjennomføres og vedlikeholdes på en effektiv måte **(6.1.1 (a), (b) og (d))**. Gjeldende krav refererer til kravene i Vedlegg I (eller Vedlegg II) i Forordning (EU) 2018/762, og dermed til eventuelle andre gjeldende krav som organisasjonen kan være underlagt **(se også 1.1)**.

Revisor har ansvaret for å verifisere fullstendigheten og effektiviteten av korrigerende eller utbedrende tiltak **(6.2.1 (c))** som skal tas som et resultat av funnene fra revisjonen.

6.2.4 Bevis

- *Bevis på at det foreligger en internrevisjonsprosess eller rammeverk som åpner for planlagte revisjoner og ytterligere målrettede revisjoner, som respons på ytelsessikkerhetsdata;* ***(6.2.1 (a))***
- *Bevis på at det foreligger et kompetansestyringssystem som omfatter elementer som tar i betraktning kompetansen til dem som utfører internrevisjonen;* ***(6.2.1 (b))***
- *Bevis på at det er iverksatt tiltak som følge av funn fra revisjoner både internt og eksternt;* ***(6.2.1 (c), (d), (e), (f))***
- *Bevis på at resultatene fra revisjonene har blitt drøftet på toppledelsesnivå, og relevante tiltak iverksatt som et resultat av dette****. (6.2.1 (g))***

6.2.5 Eksempler på bevis

Det må foreligge en internrevisjonsprosedyre for planlagte og supplerende revisjoner, inkludert drøfting av resultatene på toppledelsesnivå.

Eksempler på revisjonsrapporter og en oversikt over funnene fra internrevisjoner, som indikerer hvilke tiltak som er iverksatt for å håndtere dem.

Resultater fra revisjonsarbeid utført på tvers av organisasjonen er samlet inn, analysert og det har blitt gitt anbefalinger som skal brukes ved ledelsens periodiske gjennomgang.

Prosedyren har kompetansestyringssystemet som referanse. CMS viser at revisorene har fulgt egnede revisorstandarder (f.eks. ISO).

Det å ta hensyn til menneskelige og organisatoriske faktorer og forbedre sikkerhetskulturen vil ha en positiv innvirkning på samsvar med det relevante kravet til sikkerhetsstyringssystemet, og bevis på dette finnes i:

Internrevisjonsprosessen inkludert bestemmelser om tildelte ressurser, inkludert bemanning og kompetanse for personalet som er involvert. Kompetansekrav til personell som utfører internrevisjon, er integrert i kompetansestyringssystemet, inkludert for de spesifikke menneskelige og organisatoriske faktorkompetansene. Opplæringseksempler viser at menneskelige og organisatoriske faktorer var inkludert.

Internrevisjonen som integrerer kontrollen av implementeringen og effektiviteten av prosesser og prosedyrer som integrerer menneskelige og organisatoriske faktorer sikkerhetstiltak avledet fra risikovurderingsprosessen (se ovenfor ***6.1 Overvåking***).

Organisasjonen har prosesser og prosedyrer for systematisk å integrere menneskelige og organisatoriske faktorer i internrevisjoner. Målet er å kontrollere effektiviteten av sikkerhetstiltakene for menneskelige og organisatoriske faktorer og evaluere oppnåelsen av sikkerhetsmålene, inkludert menneskelige og organisatoriske faktorer.

Eksempler på internrevisjoner som viser at menneskelige og organisatoriske faktorer tas i betraktning mens man analyserer resultatene av revisjonene, identifiserer behov for korrigerende eller forbedringstiltak og formidler disse til toppledelsen.

Organisasjonen har prosesser og prosedyrer for systematisk integrering av evaluering av ansattes ytelse ved å utføre sikkerhetskritiske arbeidsoppgaver og operasjonelle aktiviteter.

Prosessen som beskriver styring av kommunikasjon angående resultater, anbefalinger/tiltak som peker mot en delt og transparent tilnærming.

6.2.6 Referanser og standarder

- *ISO 19011:2018 — Retningslinjer for revisjon av ledelsessystemer*
- *CSM for overvåking-søknadsveiledning*

6.2.7 Sjekkpunkter

Ved gjennomføring av tilsyn er det avgjørende at planleggingen av og resultatene fra revisjonene undersøkes. Dette vil avdekke om revisjonene retter seg mot de rette områdene, om resultatene virker fornuftige og om personalet som utfører revisjonene er kompetente og uavhengige.

Sjekk at områdene som er valgt ut for revisjon står i forhold til organisasjonens risikoprofil.

Det må foreligge en mekanisme som utløser ekstraordinære revisjoner, og dette brukes ved å gjennomgå noen eksempler.

6.3 Gjennomgang av ledelsen

6.3.1 Lovbestemt krav

6.3.1. Toppledelsen skal regelmessig gjennomgå den fortsatte tilstrekkeligheten og effektiviteten til sikkerhetsstyringssystemet, inkludert i det minste hensynet til:

(a) detaljer om fremgang med å håndtere utestående tiltak fra tidligere ledelsesgjennomganger;

(b) endrede interne og eksterne omstendigheter (se 1. Organisasjonens kontekst);

(c) organisasjonens sikkerhetsytelse knyttet til:

(i.) oppnåelse av dens sikkerhetsmål;

(ii.) resultatene fra dens overvåkingsaktiviteter, inkludert internrevisjonsfunnene, og interne undersøkelser av ulykker/hendelser og status for deres respektive handlinger;

(iii.) de relevante resultatene fra tilsynsaktiviteter utført av den nasjonale sikkerhetsmyndigheten;

(d) anbefalinger for forbedring.

6.3.2. Basert på resultatene fra sin ledelsesgjennomgang, skal toppledelsen ta det overordnede ansvaret for planlegging og implementering av nødvendige endringer i sikkerhetsstyringssystemet.

6.3.2 Formål

Sterk sikkerhetsledelse fra ledelsen er viktig for at et organisasjons sikkerhetsstyringssystem skal fungere effektivt, og for systemets kontinuerlige utvikling over tid. Organisasjonen skal demonstrere at ledelsen er aktivt involvert i gjennomgangen av ytelsen til sikkerhetsstyringssystemet og utviklingen av det for fremtiden.

Hvordan blir menneskelige og organisatoriske faktorer og sikkerhetskultur integrert?

Ledelsens gjennomgang er knyttet til alle prosesser og prosedyrer i sikkerhetsstyringssystemet, den kan deretter integrere menneskelige og organisatoriske faktorer med sikte på å forbedre dem.

6.3.3 Bevis

- *Prosesser for ledermøter som dekker gjennomgang av sikkerhetsstyringssystemet og fremdriften i interne anbefalinger som følge av revisjon og gjennomgang;* ***(6.3.1 (a)-(d))***
- *Historikk over hvordan organisasjonen har hatt fremdrift mot sine sikkerhetsmålsettinger;* ***(6.3.1(c),(i))***
- *Bevis på at anbefalinger fra relevante nasjonale sikkerhetsmyndigheter er hensyntatt i sikkerhetsstyringssystemet;* ***(6.3.1 (c),(iii))***
- *Organisasjonen må kunne vise at det foreligger prosesser for å fastslå og fastsette mål i samsvar med type, omfang og relevante risikoer, regelmessig vurdere fremdriften mot målsettingene, etterleve prosedyrer og anvende sikkerhetsdata for å overvåke, gjennomgå og gjennomføre endringer i driftsordninger.* ***(6.3.1)***
- *Bevis på at ledelsen påtar seg en aktiv rolle i planleggingen og gjennomføringen av nødvendige endringer i sikkerhetsstyringssystemet;* ***(6.3.2)***
    - *Det finnes prosesser og verktøy for systematisk å rapportere alle typer identifiserte risikoer, feil, nestenulykker, mangler og hendelser, samt for å kategorisere og analysere det som*

rapporteres fra et menneskelig og organisatorisk faktorperspektiv for å kunne finne bakenforliggende årsaker og effektive tiltak;
  - *Ekspertise innen menneskelige og organisatoriske faktorer brukes ved granskning av ulykker;*
  - *Det er systematiske prosesser for å tilbakeføre erfaringer fra menneskelige og organisatoriske faktorer til opplæring og design;*
  - *Erfaringer fra ulykkes- og hendelsesundersøkelser kommuniseres til ansatte i organisasjonen, og føres tilbake til opplæring, design og andre områder for å redusere sannsynligheten for gjentakelse;*
  - *Resultater fra ulykkesgranskning rapporteres på ledermøter og betraktes som et viktig verktøy for å ta lærdom og forbedre seg.*
- *Det er en forsikringsprosess på plass for ulykkesundersøkelser.*

6.3.4 Eksempler på bevis

Prosedyre som dekker gjennomgang og fremdrift for interne anbefalinger som følge av revisjoner og vurderinger gjennomført av toppledelsen, samt møtereferater fra utvalgte møter.

Problemloggen må inneholde anbefalinger som er gitt, samt fremdriften i å korrigere feil som er sporet av ledelsen.

Prosedyren for ledelsens vurdering av resultatene fra intern ulykkesgranskning og relevante resultater fra tilsyn fra nasjonale sikkerhetsmyndigheter.

Det gis informasjon om hvilke indikatorer som følges opp av toppledelsen og med hvilken frekvens.

Eksemplene på bevis som det vises til ovenfor, bør vise hvordan menneskelige og organisatoriske faktorer er integrert i ledelsens gjennomgang.

6.3.5 Sjekkpunkter

Under tilsynet er det viktig å observere at prosessen for å sikre at ledelsen gjennomgår effektiviteten av sikkerhetsstyringssystemet, resulterer i reelle endringer på driftsnivå.

Ledelsens bevissthet på endringer i interne og eksterne forhold. Sjekk om ledelsen gjennomfører f.eks. horisontskanning eller andre teknikker som PESTLE-analyse (politisk, økonomisk, sosialt og teknologisk, juridisk og miljømessig) for å få oversikten over utviklingen av sikkerhetsstyringssystemet.

Sammenhengen/koblingen mellom resultatene av ledelsesgjennomgangen og hvordan de inngår i den årlige sikkerhetsrapporten.

7 Forbedring

7.1 Ta lærdom av ulykker og uønskede hendelser

7.1.1 Lovbestemt krav

7.1.	Ta lærdom av ulykker og uønskede hendelser
7.1.1.	Ulykker og hendelser knyttet til organisasjonens jernbanedrift skal:
	(a) rapporteres, loggføres, undersøkes og analyseres for å fastslå årsakene deres;
	(b) rapporteres til nasjonale organer etter behov.
7.1.2.	Organisasjonen skal sikre at:
	(a) anbefalinger fra den nasjonale sikkerhetsmyndigheten, det nasjonale granskingsorganet og bransje-/internundersøkelser blir evaluert og implementert hvis det er hensiktsmessig eller pålagt i et mandat;
	(b) relevante rapporter/informasjon fra andre interesserte parter som jernbaneforetak, infrastrukturforvaltere, enheter med ansvar for vedlikehold og jernbanekjøretøyholdere vurderes og tas i betraktning.
7.1.3.	Organisasjonen skal bruke informasjon knyttet til undersøkelsen for å gjennomgå risikoanalysen og evalueringen (se 3.1.1. Risikovurdering), for å lære med sikte på å forbedre sikkerheten og, der det er aktuelt, å vedta korrigerende tiltak og/eller forbedringstiltak (se 5.4. Endringsstyring).

7.1.2 Formål

Organisasjonen må vise at ulykker og uønskede hendelser granskes, for å ta lærdom av dem og forbedre risikokontroll, at personalet som har denne oppgaven er kompetent til å foreta granskning, blant annet i forhold til mennesker og organisatoriske faktorer, at ulykker rapporteres til relevante myndigheter, og at ledelsen iverksetter tiltak på grunnlag av anbefalinger og rapporter.

I tillegg bør organisasjonen anvende "double-loop-læring": Fokuset for lærdommen er ikke bare på realiteten ved uønskede hendelser, men også organisasjonens evne til å forbedre seg, ved å fokusere på elementer som enten fremmer eller hemmer formidlingen av kunnskap og informasjon på tvers av organisasjonen.

7.1.3 Forklarende merknader

Begrepene «nestenulykker» og «andre farlige hendelser» inngår i definisjonen av «hendelse» i samsvar med Direktiv (EU) 2016/79. Det er like viktig å granske nestenulykker og andre farlige hendelser for å proaktivt ivareta sikkerheten.

Lærdom fra ulykker og uønskede hendelser bør utveksles med andre interessenter (infrastrukturforvalteren, andre jernbanevirksomheter, ECM-er, for å utvikle samarbeidet og fremme den generelle forbedringen av sikkerhetsstyringssystemet).

For granskninger som må ses fra et perspektiv med menneskelige og organisatoriske faktorer, må granskningspersonalet enten være opplært eller ha tilgang til egnet ekspertise for å undersøke problemene.

Hvordan blir menneskelige og organisatoriske faktorer og sikkerhetskultur integrert?

Analysen av ulykker/hendelser handler ikke om å skylde på en person eller en avdeling som er «mer ansvarlig enn en annen», men heller ha som mål å være en hjelp til forståelse og åpne for forbedringer av organisatoriske svakheter som førte til at hendelsen fant sted. Den viktigste utfordringen når man analyserer uønskede hendelser er å forhindre også "nærliggende" hendelser. Hvis analysen ender med å identifisere de umiddelbare årsakene, vil det bare være mulig å forhindre neste lignende hendelse. Hvis analysen på den annen side gjør det mulig å identifisere tekniske og organisatoriske hovedårsaker, vil tiltak for forbedring åpne for å kunne forebygge andre typer ulykker som deler de samme mekanismene. Hvis for eksempel analysen gjør det klart at en prosedyre ikke har blitt oppdatert, og at korrigerende tiltak bare har som mål å korrigere denne prosedyren, vil effekten være begrenset. Hvis analysen går dypere inn i materien og identifiserer svakheter i prosessen for oppdateringsprosedyrer, vil den positive effekten fra tiltak for forbedring være mye bredere.

Selskapet kan bruke rapporteringsstrukturen som er fastsatt i artikkel 4 i forordning (EU) 2020/572 «*om rapporteringsstrukturen som skal følges for etterforskningsrapporter for jernbaneulykker og hendelser*» for å identifisere elementene om menneskelige og organisatoriske faktorer som skal undersøkes og integrere dem i rapportene sine. Merk: dette er imidlertid bare én av referansemodellene som finnes, og kan brukes.

Oppfordre til rapportering av farlige situasjoner og hendelser med høy risiko, og la det være enkelt. Om nødvendig kan det tilrettelegges for mekanismer som gjør rapporteringen anonym. Hvis rapporteringen er nominativ, kan medarbeiderne og gruppene som sendte rapportene bistå med analyse og/eller finne kortsiktige løsninger. Det kan organiseres gruppediskusjoner og tiltakene kan formidles til de berørte medarbeiderne og i hele organisasjonen etter behov.

7.1.4 Bevis

- *Informasjon om rapportprosess for ulykker/uønskede hendelser, herunder hvordan hovedårsaken identifiseres og analyseres, inkludert rapportering innenfor organisasjonen og til andre kompetente myndigheter og andre parter;* ***(7.1.1)***
- *Informasjon om fremgangsmåten organisasjonen følger i forbindelse med granskning, inkludert menneskelige og organisatoriske faktorer, for å gjennomgå risikoanalysen og evalueringsprosessen etter en uønsket hendelse;* ***(7.1.3)***
- *Bevis på at anbefalinger fra kompetente myndigheter har blitt fulgt opp som følge av rapporter for ulykker og uønskede hendelser, og eventuelle nødvendige identifiserte endringer har blitt gjennomført;* ***(7.1.2 (a), (b))***
- *Gjennomgang av tidligere uønskede hendelser for å identifisere relevante faktorer i forhold til en hendelse. Bevis på bredere organisatorisk lærdom fra uønskede hendelser og erfaringer, nasjonalt og internasjonalt.* ***(7.1.3)***
- *Det er en metodikk for å gjennomføre undersøkelser basert på kunnskap om menneskelige og organisatoriske faktorer og moderne metoder.*
- *Det foreligger et opplæringsprogram for dem som gransker uønskede hendelser og ulykker, der man anvender et perspektiv på menneskelige og organisatoriske faktorer.*
- *En "rettferdig kultur" bør fremmes, som anerkjenner og forsterker positive sikkerhetsinitiativer (rapportering av hendelser, medarbeideres involvering i analyser og kontinuerlig forbedring, støtte opp om kolleger, etc.). Denne "rettferdige kulturen" bør eliminere enhver frykt for skyld, ved i stor utstrekning definere en grense mellom hva som kan og hva som ikke kan aksepteres. Man skal ha rett til å gjøre feil.*

7.1.5 Eksempler på bevis

Prosedyren for ulykkesgranskning som beskriver granskningsmetodene, med referanse til kompetansestyringskrav til dem som gransker ulykker og uønskede hendelser.

Et utdrag fra rapporter for ulykker og uønskede hendelser av ulike typer, som viser at granskning har blitt utført av kompetent personell, og funn basert på beviser og anbefalinger er fulgt opp.

En kopi av prosedyren/prosessen som sporer korrigerende/forebyggende tiltak som er fastsatt etter en ulykke/uønsket hendelse.

Informasjon om bruken av verktøy for sikkerhetsvarsling (SAIT) tilbys for å holde oversikt over og gi råd til andre organisasjoner om saker som berører bestemte aktiva.

Opplærte granskere er tilgjengelig.

Det å ta hensyn til menneskelige og organisatoriske faktorer og forbedre sikkerhetskulturen vil ha en positiv innvirkning på samsvar med det relevante kravet til sikkerhetsstyringssystemet, og bevis på dette finnes i:

Kompetansekrav til ansatte som utfører undersøkelser, inngår i selskapets kompetansestyringssystem. Det foreligger et opplæringsprogram for dem som gransker uønskede hendelser og ulykker, der man blant annet integrerer menneskelige og organisatoriske faktorer systematisk.

Rapportene viser en grundig analyse av hendelser som fører til konsekvente handlingsplaner på alle nivåer i sikkerhetsstyringssystemet, og fremmer en vilje til å lære av hendelser gjennom endringer i atferd på tvers av virksomheten. Referater fra møter og utveksling av kommunikasjon viser at når hendelser inkluderer eksterne parter, er det bevis på at resultatene av analyser og handlinger deles åpent.

Ledelsen erkjenner at hendelser og ulykker er forårsaket av flere faktorer, noen stammer fra ledelsesbeslutninger, og referater fra styremøter viser at resultatene av ulykkes-/hendelsesundersøkelser og tilhørende anbefalinger (dvs. korrigerende og/eller forbedringstiltak) rapporteres tilbake til ledelsen. og hvordan de informerer gjennomgangen av sikkerhetsstyringssystemet **(se også 6.3)**.

En tilnærming til menneskelige og organisatoriske faktorer blir tatt i undersøkelser av hendelser og ulykker, og referert til i strategier for menneskelige og organisatoriske faktorer og sikkerhetskultur og i alle relaterte prosesser (risikovurdering, ytelsesevaluering, kontinuerlig forbedring...)

De innledende og kontinuerlige opplæringsprogrammene til personalet viser at handlinger fra erfaringene er integrert, med et spesielt fokus på risikoer for menneskelige og organisatoriske faktorer og hvordan de kan reduseres.

Granskningen har et systematisk perspektiv, det vil si ikke bare å se på de menneskelige, teknologiske og organisatoriske faktorene i seg selv, men også fokus på samspillet mellom faktorene. Hvis for eksempel en lokomotivfører har vært involvert i en passhendelse (SPAD), omfatter de foreslåtte granskningspunktene relevante problemer, f.eks. tretthet, kognitiv overbelastning, kompetanse, etc. (menneskelig), teknologisk innvirkning på yteevnen, som for eksempel grensesnitt mellom menneske og system, layout, signalplassering (teknologi), organisasjonens innflytelse på yteevnen, som opplæring, sikkerhetsstyringssystem, organisasjonsprioriteringer (organisasjon) og samspillet mellom de tre områdene som innflytelse på anskaffelser mht. design eller endringsstyring med innføring av nytt design.

Analysen av farlige hendelser gjøres på tvers av et mangfoldig sett av ferdigheter, og ta i betraktning synspunkter fra alle berørte parter (inkludert eksterne parter der det er relevant).

En «rettferdig kultur»-policy og eksisterende rapporteringsverktøy som fremmer en rapporteringskultur og en spørrende holdning blant ansatte. Alle rutinemessige og unormale avvik som rapporteres av personalet, blir analysert og fører til implementering av forbedringstiltak der det er nødvendig. Kommunikasjon til berørte ansatte om hvilke tiltak som ble iverksatt gjennomføres systematisk.

7.1.6 Referanser og standarder

- *ERA-nettside om sikkerhetskultur*
- *ERAs nettside for menneskelige og organisatoriske faktorer*
- *Kommisjonens gjennomføringsforordning (EU) 2020/572 av 24. april 2020 om rapporteringsstrukturen som skal følges for etterforskningsrapporter for jernbaneulykker og hendelser*
- *IAEA (2002) — Sikkerhetskultur på kjernekraftanlegg: Veiledning for anvendelse i forbedring av sikkerhetskulturen. IAEA TECDOC-1529. Internasjonalt atomenergibyrå, Wien (2002).*
- *Mathis, T.L. & Galloway, S.M. (2013) — Skritt for en god sikkerhetskultur.*
- *Kecklund, L., Lavin, M. & Lindvall, J. (2016) — Sikkerhetskultur: Et krav til nye forretningsmodeller. Lærdommer fra andre høyrisikobransjer. I framgang presentert av Den internasjonale konferansen om menneskelige og organisatoriske aspekter ved sikring av atomenergisikkerhet — gjennomgang av 30 års sikkerhetskultur, Wien 22. til 26. februar 2016*
- *RSSB (2015) — Sikkerhetskultur og atferdsutvikling: Felles faktorer for å skape en kultur med kontinuerlig utvikling (www.sparkrail.org)*

7.1.7 Sjekkpunkter

Kompetansen til dem som gransker ulykker/uønskede hendelser er kritisk, for å kunne komme med meningsfulle anbefalinger og få på plass egnede forebyggende tiltak. De som utfører tilsyn, bør be om innblanding fra ledelsens side når det gjelder utfallet av rapporter for ulykker og uønskede hendelser, som kan påvirke kvaliteten på rapporten og utfall som kan utledes fra den.

Resultatene fra en intern granskning har ført til organisatorisk lærdom, som kan spores i dokumenter, rapporter eller andre informasjonskanaler (f.eks. intranett, interne bedriftsblader, etc.)

Organisasjonskulturen knyttet til rapportering om uønskede hendelser og nestenulykker.

7.2 Kontinuerlig forbedring

7.2.1 Lovbestemt krav

7.2.1. Organisasjonen skal kontinuerlig forbedre tilstrekkeligheten og effektiviteten til sitt sikkerhetsstyringssystem under hensyntagen til rammeverket fastsatt i forordning (EU) nr. 1078/2012, og minst resultatene av følgende aktiviteter:

(a) Overvåking (se 6.1. Overvåking);

(b) Internrevisjon (se 6.2. Internrevisjon);

(c) Gjennomgang av ledelsen (se 6.3. Gjennomgang av ledelsen);

(d) Ta lærdom av ulykker og uønskede hendelser (se 7.1. Ta lærdom av ulykker og uønskede hendelser).

7.2.2. Organisasjonen skal sørge for midler for å motivere ansatte og andre interesserte parter til å være aktive for å forbedre sikkerheten som en del av den organisatoriske læringen.

7.2.3. Organisasjonen skal legge frem en strategi for kontinuerlig å forbedre sikkerhetskulturen, stole på bruk av ekspertise og anerkjente metoder for å identifisere atferdsproblemer som påvirker de ulike delene av sikkerhetsstyringssystemet og for å iverksette tiltak for å håndtere disse.

7.2.2 Formål

Kontinuerlig forbedring spiller en viktig rolle i et effektivt sikkerhetsstyringssystem. Formålet med dette kravet er å få søker til å vise bestrebelsene på å gjøre forbedringer, og at sikkerhetsstyringssystemet støtter dette.

Toppledelsen engasjerer seg i en **kollektiv refleksjon** for å kontinuerlig forbedre sikkerhetskulturen i organisasjonen.

Denne kollektive refleksjonen er nedfelt i en strategi som retter seg mot **kulturelle egenskaper** som i betydelig grad påvirker sikkerhetsytelsen og som fortjener å bli bedre verdsatt eller gjenstand for endring.

7.2.3 Forklarende merknader

Kontinuerlig forbedring **(7.2.1)** fokuserer på elementene i sikkerhetsstyringssystemet som evaluerer og fører til forbedrende tiltak, men ikke på elementene som allerede er gjenstand for forbedring, siden de allerede er en del av overvåkingsaktivitetene.

Hvordan blir menneskelige og organisatoriske faktorer og sikkerhetskultur integrert?

Organisasjonslæring **(7.2.2)** viser til prosessen med forbedrende tiltak gjennom bedre kunnskap og forståelse.

Sikkerhetskultur **(7.2.3)** er definert som i 2.1.1 (j). En positiv sikkerhetskultur motiverer til og gjør det mulig for organisasjoner og enkeltpersoner å gjøre seg anstrengelser for å forbedre sikkerheten og ytelsen. Den øker jobbtilfredsheten, gjør at organisasjonen holder på medarbeiderne sine og åpner for kostnadsbesparelser. Den kan også bidra til å møte lovfestede forventninger, da sikkerhetsmyndigheter og tilsynsmyndigheter i økende grad anerkjenner rollen sikkerhetskulturen spiller i effektiv sikkerhetsstyring. Nærmere bestemt kan en positiv sikkerhetskultur føre til:

- *Reduserte risikoer i driften gjennom en mer omfattende risikovurdering og forbedret forståelse av risikoer i arbeidsstyrken;*
- *Reduksjon av personskader ved å eliminere farer som er identifisert gjennom økt rapportering om nestenulykker,*
- *Reduksjon av usikre handlinger og forhold gjennom forbedret engasjement i arbeidsstyrken og lederutvikling;*
- *Reduksjon i kostnader relatert til personskader, usikre handlinger og forhold;*
- *Forbedret yteevne gjennom økt personalopplæring, engasjement, samt reduksjon i personskader, usikre handlinger og forhold.*
- *Et forbedret og mer effektivt sikkerhetsstyringssystem, med prosedyrer og bestemmelser som bedre samsvarer med virkeligheten.*

På grunn av kulturens grunnleggende egenskaper, som skapes gjennom daglige interaksjoner og som vanskelig å endre, anses denne strategien som langsiktig, eid og oppmuntret av toppledelsen.

Det finnes en rekke måter å forbedre sikkerhetskulturen på:

- *Utvikle et system der man kan komme med bekymringsmeldinger. Dette avhenge av organisasjonens erfaring skje anonymt, men med være åpent og tilgjengelig for alle for å skape tillit. Det er viktig at tilbakemeldinger innarbeides i systemet for å gjøre at medarbeiderne får en følelse av involvering og tilhørighet.*
- *Endre innkjøps- og avtalevilkår for å oppfordre til en god sikkerhetskultur hos leverandørene. Sikkerhetskulturen kan være et kriterium for valg av leverandører.*
- *Synlig belønning av trygg atferd. Belønningen kan skje på en rekke måter, fra økt årslønn til bonuser til ukentlige belønninger for god sikkerhetsatferd;*
- *Sette konkrete mål for hvordan ledere har fokus på sikkerheten, for eksempel ved å oppfordre ledelsen til å ha en mer synlig rolle i å legge listen og foregå med et godt eksempel:*
- *Etc.*

Resultatene fra evalueringen bør formidles til alle nivåer i organisasjonen. Resultatene bør brukes til å fremme og opprettholde en positiv sikkerhetskultur, for å forbedre sikkerhetsstyringen og for å fremme en læringsholdning i organisasjonen.

Identifisering og utvelgelse av relevante kulturelle trekk er ofte en kompleks oppgave[1] som bør utføres nøye.

Denne oppgaven bør faktisk involvere ansatte på alle nivåer i hele organisasjonen og ofte utenfor (f.eks. entreprenører).

Selv om de ansattes oppfatninger og tro kan samles inn gjennom en spørreskjemaundersøkelse, anses en slik metode generelt som utilstrekkelig for å etablere kulturelle trekk som påvirker sikkerheten. Eventuelt styrt av undersøkelsesresultatene bør eksperter gjennomføre observasjoner, individuelle intervjuer og fokusgrupper for å etablere en mer nøyaktig diagnose.

Merk: En fokusgruppe samler et lite antall personer (vanligvis mellom 4 og 15) med en moderator for å fokusere på et spesifikt emne. Fokusgrupper tar sikte på en diskusjon i stedet for individuelle svar på formelle spørsmål, og produserer kvalitative data.

Basert på denne diagnosen kan en handlingsplan som tar sikte på å verdsette eller bidra til å endre kulturelle trekk, defineres og støttes av toppledelsen. Toppledelsen overvåker implementeringen av de identifiserte handlingene og reviderer den deretter.

[1] Mangfold av aktiviteter og størrelse på organisasjonen er enkle eksempler på parametere som går med kompleksiteten til denne oppgaven.

For å sikre bærekraft i strategien bør diagnosen revideres hvert 2.–5. år med samme tilnærming. Frekvensen avhenger av resultatene av den første øvelsen.

I flere høyrisikobransjer blir denne diagnosen ofte utført innenfor en *sikkerhetskulturvurdering*. Vurdering av sikkerhetskultur kan gjennomføres uavhengig eller ved egenvurdering. Fordelen ved en uavhengig vurdering er at organisasjonen får et mer objektivt bilde av sikkerhetskulturen, men har den risikoen at organisasjonen kan bli misforstått eller har problemer med å godta konklusjonene. Fordelen med en egenvurdering er at den gjennomføres internt med organisasjonens eget personale, som har inngående kunnskaper om organisasjonen. Ulempen er at status og hierarkier kan virke forstyrrende. Noen kjennetegn ved en sikkerhetskulturvurdering er listet opp nedenfor:

- *Inkluderer en 2/3-ukers vurderingsprosess og et forberedende stadium;*
- *Involverer et tverrfaglig vurderingsteam;*
- *Datainnsamling er avhengig av samfunnsvitenskapelige metoder (inkludert intervjuer, fokusgrupper, observasjoner);*
- *Vurderingsomfang er hele organisasjonen og dens grensesnitt;*
- *Basert på en sikkerhetskulturmodell eller rammeverk;*
- *Toppledelsen er engasjert og anser vurderingen som en læringsmulighet;*
- *Resultatene spres i hele organisasjonen;*
- *Resultatene blir utført for å designe/revidere en strategi for å kontinuerlig forbedre de valgte egenskapene til sikkerhetskulturen.*

Forbedring av strategier og prosesser for menneskelige og organisatoriske faktorer er en integrert del av den kontinuerlige forbedringen av sikkerhetsstyringssystemet.

En systematisk tilnærming er definert som en trinnvis prosess for å håndtere problemer som er knyttet til sikkerhetskulturen. Dette kan for eksempel være å ha på plass en prosess for risikoobservasjon, rapportering av uønskede hendelser og ulykker, samt hvordan informasjonen blir brukt, og det er tatt lærdom for kontinuerlig forbedring.

Mer informasjon om sikkerhetskultur og menneskelige og organisatoriske faktorer finnes i hhv. Vedlegg 4 og Vedlegg 5.

7.2.4 Bevis

- *Informasjon om prosessen for å samle inn bevis for å vise til kontinuerlig forbedring av sikkerhetsstyringssystemet;* ***(7.2.1)***
- *Prosedyrer som beskriver hvordan organisasjonen følger opp resultatene fra overvåking, internrevisjon, ledelsens gjennomgang og lærdom fra ulykker og uønskede hendelser, for å forbedre sikkerhetsstyringssystemet;* ***(7.2.1)***
- *Informasjon om hvordan organisasjonen søker å engasjere medarbeidere og andre i å forbedre sikkerhetsstyringssystemet;* ***(7.2.2)***
- *Søker må i beskrive strategien for hvordan sikkerhetskulturen utvikles, slik at risikoer som er forbundet med sikkerhetskulturen, tas i betraktning i de relevante prosessene i sikkerhetsstyringssystemet. I denne henseende bør søkeren vise til hvor ytterligere informasjon om de relevante prosedyrene kan bli funnet;* ***(7.2.3)***
- *Sikkerhetskulturen må vurderes kontinuerlig for å se etter rom for forbedringer;****(7.2.3)***
- *Forbedringer i sikkerhetskulturen kan anvendes ved hjelp av PDCA-hjulet for å sikre at tiltakene faktisk har en virkning. Lærdommen bør implementeres og systematisk evalueres for virkning.****(7.2.3)***

7.2.5 Eksempler på bevis

Prosedyren som dekker overvåking, internrevisjon, ledelsens gjennomgang og granskning av ulykker og uønskede hendelser, spesifikt det som omhandler lærdommen som bør være tatt for sikkerhetsstyringssystemet.

«Nestenulykker»-initiativet i Network Rail, hvor medarbeiderne oppfordres til å være aktive i å varsle organisasjonen om svakheter/hull i systemet eller situasjoner der det foreligger risikoer for helse og sikkerhet.

Det å ta hensyn til menneskelige og organisatoriske faktorer og forbedre sikkerhetskulturen vil ha en positiv innvirkning på samsvar med det relevante kravet til sikkerhetsstyringssystemet, og bevis på dette finnes i:

Eksempler på møtereferater fra periodiske fagforeningsmøter/HMS-møter, som viser hvor situasjoner som er ansett som usikre/utrygge eller krever videre vurdering, har blitt diskutert.

Resultatene fra ulykkesundersøkelser rapporteres på ledermøter og anses som et viktig verktøy for læring og forbedring, som tar hensyn til menneskelige og organisatoriske faktorer på en systemisk og systematisk måte.

En kopi av strategien for å forbedre sikkerhetskulturen, og hvordan dette knytter seg til de ulike delene i sikkerhetsstyringssystemet.

Strategien viser til tilstrekkelig bevis på at det foreligger faglig kompetanse og nødvendig opplæring og erfaring, på feltet der sikkerhetskultur blant ansatte skal ta sikte på å utføre og utvikle strategien.

Type opplæring og kompetanse som kreves knyttet til forståelse av begrepet sikkerhetskultur, og måter og metoder for å måle ytelsen og jobbe mot kontinuerlig forbedring. Et ytterst viktig aspekt er at det er forståelse for sikkerhetskulturen som et helhetlig konsept som påvirker alle deler av sikkerhetsstyringssystemet, og at sikkerhetskulturen ikke kan behandles som et separat element.

Det er en prosess for kontinuerlig å evaluere sikkerhetsforbedrende tiltak. Effektene av de sikkerhetsforbedrende tiltakene identifiseres og settes ut i livet slik at de kan evalueres.

Referat fra ledelsens gjennomgang viser at ledelsen anerkjenner at hendelser, ulykker og avvik er forårsaket av flere faktorer, og at noen stammer fra prosedyrer og ledelsesbeslutninger.

Referatene fra ledergjennomgangsmøter viser hvordan korrigerende tiltak fra overvåkingsaktiviteter, internrevisjoner og hendelses- og ulykkesundersøkelsesprosesser tar hensyn til menneskelige og organisatoriske faktorer og er definert på ethvert nivå av sikkerhetsstyringssystemet og organisasjonen. De viser også hvordan resultatene brukes til å forbedre risikovurderingen **(se 3.1)**.

Prosedyrene som dekker overvåking, internrevisjon, ledelsesgjennomgang og etterforskning av ulykker og hendelser er knyttet til bevisstgjøringsprosessen **(se 4.3)** og kompetansestyringssystemet **(se 4.2)**.

7.2.6 Sjekkpunkter

Ved tilsyn bør ledelsens engasjement i kontinuerlig forbedring av sikkerhetsstyringssystemet bli testet gjennom samtaler, samt gjennom en dokumentasjonsanalyse. Gjøres det en risikobasert tilnærming til å målretta forbedring, dvs. i tilknytning til sårbare og kritiske kontroller?

Organisasjonens bruk av modenhetsmodeller for å undersøke ytelsen av et sikkerhetsstyringssystem, bør undersøkes der dette foreligger.

Vedlegg 1 — Korrelasjonstabeller

Tabellene nedenfor viser en kolonnebasert sammenligning mellom vurderingskravene som er skissert i Vedlegg II til tidligere Forordning (EU) 1158/2010 og (EU) 1169/2010, og kravene i Vedlegg I og Vedlegg II til Forordning (EU) 2018/762. Formålet er å legge til rette for overgangen fra det gamle sikkerhetssertifiseringsregimet i henhold til Direktiv 2004/49/EF til det nye, som ble innført av Direktiv (EU) 2016/798.

Å ha korrespondanse med Forordning (EU) 2018/762 gir ikke bevis for jernbanevirksomheters eller infrastrukturforvalteres evne til å oppfylle de relevante kravene i sikkerhetsstyringssystemet i samsvar med Artikkel 9 i Direktiv (EU) 2016/798. Detaljene i de tidligere og nye vurderingskravene kan fortsatt variere, selv om de til en viss grad deler felles prinsipper. I tillegg er det ikke alle vurderingskravene i vedlegg I og vedlegg II til forordning (EU) 2018/762 som samsvarer med den tidligere forskriften. Det kreves videre at jernbanevirksomhetene og infrastrukturforvalterne viser at de etterlever de nye vurderingskravene (eller deler av dem).

Kravene til sikkerhetsstyringssystem i Forordning (EU) 2018/762 som ikke korresponderer med dem i Forordning (EU) 1158/2010 og/eller Forordning (EU) 1169/2010, skal betraktes som nye krav, og i den forbindelse skal søker fremlegge ytterligere bevis som viser samsvar med dem. I de fleste tilfeller er det ikke mulig å oppnå et fullstendig samsvar mellom kriteriene i den tidligere forordningen og kravene i den nye CSM-forordningen. I slike tilfeller er sammenligningen således basert på hensikten med kravene. Det kan også forekomme at kravene er gjort mer eksplisitt i forordning (EU) 2018/762 mens de deler samme hensikt. I slike tilfeller skal kravene i Forordningen ikke betraktes som nye, men kan anvendes av de ulike partene som en hjelp til å forstå hvilke bevis som kan forventes at søkeren legger frem.

Korrespondanse med ISO High Level Structure (HLS)[2] er også gitt til jernbanevirksomheter og infrastrukturforvaltere som ønsker å utvikle et integrert styringssystem. Likeledes inneholder ikke et styringssystem som er sertifisert mot én eller flere ISO-styringssystemstandarder (f.eks. ISO 9001, ISO 14001 eller ISO 45001) et bevis for jernbanevirksomheters eller infrastrukturforvalters evne til å oppfylle de relevante sikkerhetsstyringssystemkravene i samsvar med Artikkel 9 i Direktiv (EU) 2016/798.

Tabell 1: Kolonnebasert sammenligning — vurderingskriterier/krav som er felles for jernbanevirksomheter og infrastrukturforvaltere

Forordning (EU) 1158/2010 og 1169/2010 Kriterium-ID	*Forordning (EU) 2018/762 Krav-ID*	*ISO HLS klausul nr.*	*Forklaring*
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)	I/T	
A.5	4.4 4.5.1.1	7.4	
A.6	6.1.1 5.4.1	9.1 8.1	
B.1	5.2.4	I/T	Vedlikehold er en fase i løpet av livssyklusen til et aktiva.

[2] ISO/IEC-direktiver, Del 1, konsolidert tillegg 2016, Vedlegg SL Vedlegg 2.

Forordning (EU) 1158/2010 og 1169/2010 Kriterium-ID	*Forordning (EU) 2018/762 Krav-ID*	*ISO HLS klausul nr.*	*Forklaring*
B.2	5.2.4	I/T	Vedlikehold er en fase i løpet av livssyklusen til et aktiva.
B.3	2.3.1 4.2.1	5.3 7.2	Definisjon og tilordning av ansvar for vedlikehold finnes i stor grad i 2.3.1. Beskrivelse av kompetansen som kreves for vedlikehold finnes i stor grad i 4.2.1.
B.4	6.1.1 5.2.5	9.1 7.4	Datainnsamling (funksjonsfeil, svikt) og analyse er en del av overvåkingsprosessen. Utveksling av data mellom de som er ansvarlige for den daglige driften og de som er ansvarlige for vedlikeholdet, er en del av informasjons- og kommunikasjonsprosessen som anvendes i aktivaforvaltningen.
B.5	6.1.1	I/T	Referert til i Art. 4(2) i CSM vedrørende overvåking.
B.6	6.1.1	9.1	Evaluering av ytelse og resultater fra vedlikehold er en del av overvåkingsprosessen som anvendes for vedlikehold.
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)	I/T	
C.4	5.2.5 (b) 5.3.2 (c)	I/T	
C.5	5.3.2 (c) 5.3.3 (a)	I/T	
D.1	3.1.1.1 (a)	I/T	
D.2	3.1.1.1 (c)	I/T	
D.3	6.1.1	I/T	
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	
F.2	2.3 4.5.1.1 (a)	5.3 4.4	
F.3	2.3.1 2.3.4	I/T	

Forordning (EU) 1158/2010 og 1169/2010 Kriterium-ID	*Forordning (EU) 2018/762 Krav-ID*	*ISO HLS klausul nr.*	*Forklaring*
F.4	4.5.1.1 (a) 4.2.1 2.3.1 2.3.2 2.3.3	4.4 5.3	Definisjon av sikkerhetsrelaterte oppgaver er en del av beskrivelsen i sikkerhetsstyringssystemet, herunder ansvarsfordeling. Ansvar er definert for hver enkelt relevant rolle i sikkerhetsstyringssystemet.
G.1	4.5.1.1 (a) 2.3.1	4.4 5.3	Definisjon av sikkerhetsrelaterte oppgaver er en del av beskrivelsen i sikkerhetsstyringssystemet, herunder ansvarsfordeling. Ansvar er definert for hver enkelt relevant rolle i sikkerhetsstyringssystemet.
G.2	6.1.1 6.2.1	9.1 9.2	Internrevisjon tar sikte på å sjekke at organisasjonen overholder gjeldende krav.
G.3	2.1.1 (d)(i) 2.3.2	I/T	
G.4	2.3.1	5.3	
G.5	4.1.1	7.1	Merk at det er en kobling her til kriteriet i 1158/2010 N2(d)
H.1	2.4.1	I/T	
H.2	(fjernet)	I/T	Personell som utfører sikkerhetsrelaterte oppgaver, bør være involvert i å utvikle, vedlikeholde og forbedre sikkerhetsstyringssystemet. Det er opp til organisasjonen å implementere krav. 2.4.1 på en slik måte at etterlevelsen av det er sporbar.
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	Sikkerhetsmålsettingene må være i samsvar med sikkerhetspolicyen, som videre bør være egnet for typen og omfanget til jernbanevirksomheten.
K.3	3.2.4	6.2	Sikkerhetsmålsettinger er ikke begrenset til felles sikkerhetsmålsettinger som er fastsatt på medlemsstatsnivå.
K.4	6.1.1 5.4	9.1 8.1	
K.5	3.2.4 (tilpasset)	9.1	Referanse til overvåkingsstrategi og plan(er) samsvarer med CSM vedrørende overvåking.
L.1	6.1.1 5.4	9.1 8.1	
L.2	4.2 4.4 4.5 5.2.2 (a)	I/T	Bruk av kompetent personell, prosedyrer, spesifikke dokumenter og rullende materiell, er kontrollert under kompetanse, informasjon og kommunikasjon og dokumentert informasjon og aktivaforvaltning.

Forordning (EU) 1158/2010 og 1169/2010 Kriterium-ID	*Forordning (EU) 2018/762 Krav-ID*	*ISO HLS klausul nr.*	*Forklaring*
L.3	1.1.1 (e) 6.1.1 6.1.2	4.3 9.2	Etterlevelse av gjeldende krav er for det meste framsatt i 3.1.2.2 (ikke spesifikt for vedlikehold). Overvåking sikrer korrekt anvendelse av prosedyrene. Internrevisjon sikrer at prosedyrene samsvarer med de gjeldende kravene.
M.1	3.1.2.1 5.4.1	6.1 8.1	I samsvar med ISO skal endringer først planlegges, inkludert risikoidentifikasjon og vurdering, og deretter kan endringen gjennomføres.
M.2	3.1.2.1	I/T	
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	I/T	
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	I/T	
S.1	4.4.3	I/T	
S.2	4.5.2 4.5.3	7.5.2 7.5.3	
S.3	4.5.3	7.5.3	
Q.1	7.1.1	10.1	
Q.2	7.1.2	I/T	
Q.3	7.1.3	10.2	
R.1	5.5.1	I/T	
R.2	5.5.2	I/T	
R.3	5.5.3	I/T	
R.4	5.5.4	I/T	
R.5	5.5.5	I/T	
R.6	5.5.1	I/T	

Forordning (EU) 1158/2010 og 1169/2010 Kriterium-ID	*Forordning (EU) 2018/762 Krav-ID*	*ISO HLS klausul nr.*	*Forklaring*
R.7	5.5.6	I/T	
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	

Tabellen nedenfor inneholder en kolonnebasert sammenligning mellom tidligere vurderingskriterier og de nye sikkerhetsstyringssystemkravene som kun gjelder for jernbanevirksomheter.

Tabell 2: Kolonnebasert sammenligning — spesifikke vurderingskriterier/krav for jernbanevirksomheter

Forordning (EU) 1158/2010 Kriterium-ID	*Forordning (EU) 2018/762 Vedlegg I Krav-ID*	*ISO HLS klausul nr.*	*Forklaring*
R.8	5.5.7	I/T	
R.9	5.5.8	I/T	

Tabellen nedenfor inneholder en kolonnebasert sammenligning mellom tidligere vurderingskriterier og de nye sikkerhetsstyringssystemkravene som kun gjelder for infrastrukturforvaltere.

Tabell 3: Kolonnebasert sammenligning — spesifikke vurderingskriterier/krav for infrastrukturforvaltere

Forordning (EU) 1169/2010 Kriterium-ID	*Forordning (EU) 2018/762 Vedlegg II Krav-ID*	*ISO HLS klausul nr.*	*Forklaring*
R.8	5.5.7	I/T	
R.9	5.5.8	I/T	
T.1	5.2.1	I/T	Sikkert design og installasjon av infrastrukturen er en del av livssyklusen til et aktiva.
T.2	3.1.2 5.4.1	I/T	Beskrivelse av tekniske endringer i infrastrukturen finnes i stor grad i 3.1.2. Håndtering av tekniske endringer i infrastrukturen finnes i stor grad i 5.4.1.

Forordning (EU) 1169/2010 Kriterium-ID	*Forordning (EU) 2018/762 Vedlegg II Krav-ID*	*ISO HLS klausul nr.*	*Forklaring*
T.3	3.1.2	I/T	Etterlevelse av gjeldende regler som omhandler designet på infrastrukturen finnes i stor grad i 3.1.2.
U.1	5.1.1 5.1.3	I/T	Sikkerhetsstyring av infrastrukturen finnes i stor grad i 5.1.1.
U.2	5.1.1	I/T	Sikkerhetsstyring for fysiske grenser og/eller driftsgrenser i infrastrukturen finnes i stor grad i 5.1.1.
U.3	5.1.3 (c) 5.5.7	I/T	Håndtering av normal og nedsatt drift finnes i stor grad i 5.1.3 (c).
U.4	5.1.2 5.2.3	I/T	
V.1	5.2.4 6.1.1	I/T	Vedlikehold av infrastrukturen finnes i stor grad i 5.2.4. Revisjoner og inspeksjoner (der det er relevant) inngår i overvåkingsaktivitetene.
V.2	5.2.4	I/T	Vedlikehold av infrastrukturen finnes i stor grad i 5.2.4.
V.3	5.2.3	I/T	
W.1	5.1.3	I/T	
W.2	5.1.1	I/T	Sikkerhetsstyring for fysiske grenser og/eller driftsgrenser for trafikkontroll og signalsystemer finnes i stor grad i 5.1.1.
W.3	5.1.2 5.2.3	I/T	

Tabellen nedenfor inneholder en kolonnebasert sammenligning mellom tidligere ISO HLS og de nye sikkerhetsstyringssystemkravene.

Tabell 4: Kolonnebasert sammenligning — ISO High Level Structure

ISO HLS klausul nr.	*Forordning (EU) 2018/762 Krav-ID*	*Forklaring*
4.1	1.1.1 (a) 1.1.1 (b)	
4.2	1.1.1 (c) 1.1.1 (d)	
4.3	1.1.1 (e) 1.1.1 (f)	
4.4	4.5.1.1 (a)	
5.1	2.1	

ISO HLS klausul nr.	*Forordning (EU) 2018/762 Krav-ID*	*Forklaring*
5.2	2.2	
5.3	2.3	
6.1	3.1.1 3.1.2	CSM for risikovurdering og annen vurdering anvendes for å avgjøre om en endring er sikkerhetsrelatert (eller ikke), og deretter om den er vesentlig (eller ikke). Det "virtuelle" skillet som er dannet av ISO mellom det strategiske nivået (ISO HLS Paragraf 6) og det taktiske nivået (ISO HLS Paragraf 8) i planleggingen, er revurdert i lys av EUs regulerende rammeverk, og særlig anvendelsen av ovennevnte CSM (uavhengig av endringene).
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	
8.1	5.1 5.2 5.3 5.4 5.5	I henhold til ISO veiledningsdokumentet (N360), er hensikten med paragraf 8 i ISO-HLS å spesifisere kravene som må implementeres i organisasjonens virksomhet, for å sikre at styringssystemkravene oppfylles, samt for å sikre at prioriterte risikoer og muligheter blir tatt i betraktning. I tillegg er det oppgitt at tilleggskrav (spesifikke for kategori) knyttet til driftsplanlegging og kontroll kan komme til å gjelde. På denne måten er kravene i 5.X sammenhengende med ISO-tilnærmingen. De skal ikke være ødeleggende for selskapets virksomhet, men tilveiebringe et tilstrekkelig rammeverk for å kontrollere hvordan viktige sikkerhetsaspekter skal håndteres i selskapets forretningsprosesser.
9.1	6.1	Begrepet "overvåking" refererer til overvåkingsrammene som er definert i CSM vedrørende overvåkning, og har derfor en bredere betydning som viser til overvåking, måling, analyse og evaluering definert i paragraf 9.1 i ISO HLS.

ISO HLS klausul nr.	*Forordning (EU) 2018/762 Krav-ID*	*Forklaring*
9.2	6.2	Internrevisjoner er overvåkingsverktøy i henhold til CSM vedrørende overvåking. Selv om det er et eget krav, er det ment å nå målene med overvåking i samsvar med CSM vedrørende overvåking.
9.3	6.3	
10.1	7.1	
10.2	7.2	

Vedlegg 2 — Kryssaksept av godkjenninger, anerkjennelser eller sertifikater for produkter eller tjenester som leveres i samsvar med EU-regelverket

Den utstedende myndighet for felles sikkerhetssertifikat eller sikkerhetsgodkjenning, kan godta sertifikater som er utstedt av andre organer, for eksempel ISO-samsvarsvurderingsorganer, for å unngå dobbel vurdering og tilleggskostnader som søker må dekke. Den endelige avgjørelsen ligger alltid hos utstedende myndighet.

I henhold til Artikkel 3(12) i Forordning (EU) 2018/763 skal imidlertid utstedende myndighet ved vurdering av søknader om felles sikkerhetssertifikat, akseptere godkjenninger, anerkjennelser eller sertifikater for produkter eller tjenester som leveres av jernbanevirksomheter eller deres samarbeidspartnere eller leverandører, og som er utstedt i samsvar med relevant EU-regelverk, som bevis på at jernbanevirksomheten imøtekommer de korresponderende kravene i sikkerhetsstyringssystemet for den aktuelle typen produkt eller tjeneste. Selv om det ikke foreligger tilsvarende bestemmelser i EU-regelverket for vurdering av søknader om sikkerhetsgodkjenninger, oppfordres også de nasjonale sikkerhetsmyndighetene til å anvende samme prinsipp.

Følgende tabell viser de ulike tilfellene som eksisterer så langt i EU-regelverket, og inneholder illustrerende eksempler på typer produkter eller tjenester som kan dekkes av hvert tilfelle.

Tabell 5: Godkjenninger, anerkjennelser eller sertifikater for produkter eller tjenester som leveres i samsvar med EU-regelverket

Tilfelle	*Type produkter eller tjenester*	*Gjeldende EU-regelverk*	*Forordning (EU) 2018/762 Krav-ID*	*Forklaring*
ECM-sertifikat	Vedlikehold av vogner	Artikkel 14(4) i Direktiv (EU) 2016/798 Forordning (EU) 2019/779	5.2 5.3	I tilfeller fastsatt i Artikkel 14(4) i Direktiv (EU) 2016/798, inneholder sertifisering av enheter med ansvar for vedlikehold tilstrekkelig bevis på at jernbanevirksomheter og infrastrukturforvaltere gjennom deres sikkerhetsstyringssystem er i stand til å kontrollere risikoer knyttet til vedlikehold av kjøretøyer, herunder bruk av leverandører.

Tilfelle	*Type produkter eller tjenester*	*Gjeldende EU-regelverk*	*Forordning (EU) 2018/762 Krav-ID*	*Forklaring*
Anerkjennelse	Opplæring av lokomotivførere	Direktiv 2007/59/EF Beslutning 2011/765/EU	4.2.2	Opplæringssentre bør anerkjennes av kompetent myndighet for å arrangere opplæringskurs for lokomotivførere og lokomotivførerkandidater, i samsvar med Direktiv 2007/59/EF. Opplæringssentrene spiller en viktig rolle for å sikre at lokomotivførere er kompetente for de sikkerhetsrelaterte oppgavene som er tildelt dem. I denne sammenheng bør opplæringssentrene være kompetente med hensyn til opplæringen de gir, og det faktum at de er anerkjent av en kompetent myndighet bør, der det er relevant, tas i betraktning av sikkerhetssertifiseringsorganet og nasjonale sikkerhetsmyndigheter når det gjennomføres en vurdering av kompetansestyringssystemet.
Lokomotivførersertifikat	Lokomotivførere s kompetanse og dugelighet	Direktiv 2007/59/EF	4.2.1	Lisenser og sertifikater utstedt i samsvar med Direktiv 2007/59/EF, gir tilstrekkelig bevis på lokomotivførernes kompetanse og dugelighet. Dette fritar ikke organisasjonen fra å måtte vise at deres ordninger for kompetanse og dugelighet er tilstrekkelige.

Tilfelle	*Type produkter eller tjenester*	*Gjeldende EU-regelverk*	*Forordning (EU) 2018/762 Krav-ID*	*Forklaring*
Felles sikkerhetssertifikat	Vedlikehold og inspeksjon av infrastruktur Sporveksling Testing av rullende materiell	Artikkel 10 i Direktiv (EU) 2016/798	5.3	Infrastrukturforvaltere kan bruke underleverandører for vedlikehold eller inspeksjon av infrastrukturen for selskaper som bruker spesialvogner på jernbanen. Likeledes kan sporvekslings- eller testoperatører bli bedt om å måtte besitte et sikkerhetssertifikat. I de ovennevnte tilfellene er felles sikkerhetssertifikat tilstrekkelig bevis på at jernbanevirksomhetene og infrastrukturforvalterne gjennom sikkerhetsstyringssystemet kan kontrollere risikoen knyttet til bruken av leverandører.
Tillatelse til idriftsetting/godkjenning av vogntype	Godkjenning av vogn(type)	Direktiv (EU) 2016/797	5.2	Godkjenning av vogn(type) sikrer, gjennom design, produksjon, verifisering og validering, samsvar med de grunnleggende kravene i all gjeldende lovgivning (inkludert sikkerhet), og at den kan sikkert kan tas i bruk på jernbanenettene der den skal operere, i henhold til bruksgrensene og bruksvilkårene som er angitt i det tekniske registeret for vognen/vogntypen.

I noen tilfeller er det ikke sikkert at besittelse av et sertifikatet (eller tilsvarende) som er utstedt i samsvar med EU-reglementet, er tilstrekkelig til å kontrollere alle sikkerhetsrisikoer knyttet til produktene som leveres til, eller tjenestene som brukes av, jernbanevirksomheter og infrastrukturforvaltere.

For eksempel har jernbanevirksomheter i samarbeid det fulle ansvar for en trygg drift, og således å kontrollere risikoen knyttet til deres aktiviteter, herunder å sørge for vedlikehold på vognene. Dersom en jernbanevirksomhet bruker et samarbeidspartners felles sikkerhetssertifikat for å kontrollere risikoer som er knyttet til vedlikehold, er dette ikke tilstrekkelig dersom det ikke er grundig avtalefestet mellom de samarbeidende virksomhetene. Disse avtaleordningene må utvikles og overvåkes i fellesskap ved anvendelse prosedyrer i begge parters sikkerhetsstyringssystemer, og er således underlagt tilsyn av respektive NSA.

Således kan et felles sikkerhetssertifikatet brukes som et middel til å kontrollere risikoer knyttet til vedlikeholdsleverandører, og som et middel for å overholde kravene til kontroll av risiko forbundet med vedlikehold av vogner, når de tre følgende betingelsene er oppfylt:

1. Det må foreligge avtaleordninger mellom samarbeidende jernbanevirksomheter som omfatter aspekter knyttet til vedlikehold av vogner som:

   a) Utveksling av informasjon som beskrevet i Artikkel 5 i Forordning (EU) 2019/779;
   b) Teknisk støtte når det er hensiktsmessig, spesielt for gamle CCS-systemer;
   c) Kontroll av evnen verkstedene vedlikeholdsleverandøren har til å utføre vedlikeholdet;
   d) Effektiv overvåking av vogner og utveksling av informasjon som følge av denne overvåkingen.

2. Disse avtaleordningene må være utarbeidet på grunnlag av risikovurdering, og må overvåkes regelmessig av hver enkelt jernbanevirksomhet mot CSM vedrørende overvåking (Forordning (EU) 1078/2012). Resultatene av denne overvåkingen må deretter formelt utveksles mellom begge de samarbeidende jernbanevirksomhetene.
3. Sikkerhetsstyringssystemet hos begge partnerne må inneholde tilstrekkelige prosesser og prosedyrer for å oppnå betingelsene 1 og 2 ovenfor.

I andre tilfeller kan nasjonal lovgivning kreve at en bestemt type produkt eller tjeneste har et nasjonalt sertifikat (eller tilsvarende) som skal utstedes av et kompetent organ (f.eks. den nasjonale sikkerhetsmyndigheten), som også kan brukes som bevis på jernbanevirksomhetenes eller infrastrukturforvalternes evne til å oppfylle de relevante kravene i Forordning (EU) 2018/762. For eksempel kan nasjonale sertifikater utstedt til ECM og/eller vedlikeholdsverksteder som utfører vedlikehold på andre vogner enn godsvogner også gi en rimelig forsikring, i likhet med ECM-sertifikatet, om at vognene de utfører vedlikehold på er i sikker driftstilstand.

Vedlegg 3 — Sidesporoperasjoner, avtaleordninger og samarbeid

Sidesporoperasjoner

I dette dokumentet forstås «sidespor» en jernbaneinfrastruktur som er knyttet til et jernbanenett som er underlagt en infrastrukturforvalter (dvs. infrastrukturdelen av jernbanesystemet som omfattes av Direktiv (EU) 2016/798). Sidespor kan eller kan ikke være en del av dette jernbanenettet, avhengig av gjennomføringen av ovennevnte Direktiv i hver enkelt medlemsstat.

Aktiviteter som gjøres på sidesporene, som lasting av vogner, er industrielle aktiviteter som etterfølgende samhandler med spesifikke jernbaneaktiviteter som sammensetning, klargjøring og kjøring av vogner som kan være tog eller bli brukt i tog. Dette inkluderer sammenkobling av ulike vogner for å danne vogngrupper eller tog, og kjøre dem.

Sidespor kan være (men er ikke begrenset til):

- *Infrastruktur som brukes til å parkere jernbanevogner mellom operasjonene.*
- *Intermodale terminaler;*
- *Infrastruktur som brukes til tjenester på passasjervogner, som rengjøring eller lett vedlikehold;*
- *Infrastruktur som tilhører og administreres av et vedlikeholdsverksted for jernbanevogner;*
- *Industriområder eller anlegg der det utføres industrielle aktiviteter for lasting/lossing av godsvogner.*

Aktivitetene på sidesporene utføres av en "sidesporoperatør". En sideoperatør kan være en jernbanevirksomhet, en infrastrukturforvalter, en tjenesteleverandør (f.eks. for rengjøring av passasjervogner), et industriselskap (for eksempel et kjemikalieanlegg som laster og losser tankvogner) eller en underleverandør av sådan industriselskap. I så tilfelle har sådan selskap tatt påtatt seg rollen som en jernbanevirksomhet, eller er en jernbanevirksomhet som planlegger å utføre sidesporaktiviteter i tillegg til gjeldende jernbaneaktiviteter. I sistnevnte tilfelle er infrastrukturforvalter den som er infrastrukturforvalteren for sidesporene, eller den som opptrer som en jernbanevirksomhet under sikkerhetsgodkjenning.

"Sidesporoperatøren" kontrollerer risikoer forbundet med arbeidsmiljø og sikkerhet gjennom sitt foreliggende HMS-styringssystem i henhold til internasjonal og nasjonal lovgivning. Når "sidesporoperatøren" ikke er en jernbanevirksomhet, må dette styringssystemet ta hensyn til HMS-forpliktelsene knyttet til eksterne arbeidere, da særlig dem hos jernbanevirksomhetene, for eksempel når lokomotivførere kjører inn på et sidespor. Parallelt må jernbanevirksomheten kontrollere risikoer forbundet med arbeidsmiljø og sikkerhet gjennom sitt HMS-styringssystem i henhold til internasjonal og nasjonal lovgivning.

Eksempel 1: Sidesporoperatøren er en jernbanevirksomhet "Y"

Denne jernbanevirksomheten kontrollerer, gjennom sitt sikkerhetsstyringssystem, risikoer knyttet til deres jernbaneoperasjoner på sidesporene og på jernbanenettet under en infrastrukturforvalters ansvar. Denne risikokontrollen inkluderer risikoer forbundet med skade på vogner forårsaket av alle aktiviteter som utføres på sidesporet, herunder også sammensetning, klargjøring og kjøring av tog.

I praksis er det noen ganger vanskelig å fastslå hvem som er den ansvarlige jernbanevirksomheten. For eksempel ankommer et tog fra jernbanevirksomheten "X" et sidespor (lokfører og lokomotiv er innleid) og jernbanevirksomheten "Y", som driver sidesporet, tar det over som et nytt tog (lokfører og lokomotiv er innleid) og i mellomtiden må sidesporoperasjoner utføres. I et slikt tilfelle gjelder ovennevnte sikkerhetsprinsipp. Det er felles samhandlingsrisikoer som må vurderes i jernbanevirksomheten "Y" sitt sikkerhetsstyringssystem (f. eks. skader på vogner fra sidesporoperasjoner, som lasting). I tillegg må utveksling av informasjon om vognene fra jernbanevirksomhet "X" til jernbanevirksomhet "Y" også vurderes. Dette omfatter forsikring om at vognen er i sikker tilstand når jernbanevirksomhet "X" overfører den til sidesporoperatøren, og likeledes når den overføres videre via jernbanevirksomhet "Y". Jernbanevirksomhet

"Y" som er ansvarlig for sidesporaktiviteter, står fortsatt helt og fullt ansvarlig for kontrollen av risikoer knyttet til vedlikeholdsaktiviteter som utføres derpå.

Eksempel 2: Sidesporoperatøren er ikke en jernbanevirksomhet

Dette kan deles opp i fire undereksempler:

- ***Undereksempel 2.1*** *når sidesporoperatøren er infrastrukturforvalteren.*
- ***Undereksempel 2.2 og 2.3*** *når sideoperatøren, som ikke er infrastrukturforvalter, kun driver aktiviteter på sin egen infrastruktur men ikke på jernbanenettet underlagt infrastrukturforvalters ansvar.*
- ***Undereksempel 2.4*** *omfatter jernbanedrift utført av en sidesporoperatør, som ikke er infrastrukturforvalter, på jernbanenettet underlagt infrastrukturforvalterens ansvar.*

Undereksempel 2.1: Når driften på sidesporene deles mellom jernbanevirksomhet(er) og en infrastrukturforvalter (eller eventuelt en organisasjon som handler på vegne av den), må hver jernbanevirksomhet informeres om alle sikkerhetsrelaterte hendelser som har oppstått under infrastrukturforvalterens drift gjennom avtaleordninger. Dette inkluderer skader, ulykker og uønskede hendelser som involverer vogner.

Disse avtaleordningene kan håndteres gjennom hvert av jernbanevirksomhetenes sikkerhetsstyringssystem, og infrastrukturforvalterens sikkerhetsstyringssystem.

Gjennom sikkerhetsstyringssystemet kontrollerer jernbanevirksomheten risikoer knyttet til egen drift i forhold til mottatt informasjon.

Undereksempel 2.2: Togsammensetning og klargjøring gjøres av jernbanevirksomheten (kobling, klargjøring) på sidesporinfrastrukturen. Jernbanevirksomheten må informeres om alle (sikkerhetsrelaterte) hendelser som har funnet sted i løpet av driften hos sidesporoperatøren (f.eks. lasting eller rengjøring) gjennom avtaleordninger. Dette inkluderer skader, ulykker og uønskede hendelser som involverer vogner.

Disse avtaleordningene kan styres gjennom jernbanevirksomhetens sikkerhetsstyringssystem.

Gjennom sikkerhetsstyringssystemet kontrollerer jernbanevirksomheten risikoer knyttet til egen drift i forhold til mottatt informasjon.

Undereksempel 2.3: Togsammensetningen utføres helt/delvis av sidesporoperatøren eller av en organisasjon som arbeider på vegne av sidesporoperatøren.

Etter at et tog er sammensatt, overføres det til en jernbanevirksomhet.

Akkurat som i undereksempel 2.2, må jernbanevirksomheten informeres om alle (sikkerhetsrelaterte) hendelser som har funnet sted i løpet av driften hos sidesporoperatøren (f.eks. lasting eller rengjøring) og ved togsammensetning gjennom avtaleordninger. Sådan hendelser inkluderer skader, ulykker og uønskede hendelser som involverer vogner.

Disse avtaleordningene kan styres gjennom jernbanevirksomhetens sikkerhetsstyringssystem.

Gjennom sikkerhetsstyringssystemet kontrollerer jernbanevirksomheten risikoer knyttet til egen drift i forhold til mottatt informasjon.

Undereksempel 2.4: Dette undereksempelet supplerer undereksempel 2.3. Således er kun jernbanevirksomhetens ytterligere forpliktelser beskrevet her.

Sidesporoperatøren kjører tog eller flytter vogngrupper fra jernbaneinfrastrukturen sin til jernbanenettet som er underlagt en infrastrukturforvalters ansvar.

For eksempel:

- *Tog eller vogngrupper flyttes fra et serviceverksted til plattformene ved en passasjerterminal eller til en parkeringsplass knyttet til en passasjerterminal;*
- *Tog eller vogngrupper flyttes fra et industrianlegg til et utvekslingssted (utvekslingsspor) knyttet til en fraktstasjon.*

Sidesporoperatøren er verken en jernbanevirksomhet eller en infrastrukturforvalter, men aktivitetene som utføres på jernbanenettet til en infrastrukturforvalter, må dekkes av et felles sikkerhetssertifikat eller en sikkerhetsgodkjenning.

Jernbanedriften som sidesporoperatøren har drevet på jernbanenettet som er underlagt en infrastrukturforvalters ansvar, er enten dekket av et sikkerhetssertifikatet til en jernbanevirksomhet eller av sikkerhetsgodkjenningen til en infrastrukturforvalter. Dette innebærer at jernbanevirksomheten eller infrastrukturforvalteren må kontrollere risikoer knyttet til aktiviteter utført av sidesporoperatøren, gjennom ordninger for administrasjon av underleverandører i deres sikkerhetsstyringssystem.

Jernbanevirksomhetene og infrastrukturforvalteren må i alle tilfeller nøye beskrive omfanget av all deres jernbanedrift og deres aktiviteter som samhandler med annen jernbanedrift, slik at nasjonale sikkerhetsmyndigheters tilsyn av sikkerhetsstyringssystemet blir effektivt. Jernbanevirksomheters og infrastrukturforvalters evne til å gi en klar og fullstendig beskrivelse av driften, samt andre aktiviteter som knytter seg til jernbanedriften, er avgjørende for å sikre effektiviteten av sikkerhetsstyringssystemet og effektiviteten av nasjonale sikkerhetsmyndigheters tilsyn.

Avtaleordningene i alle ovennevnte undereksempler må klart beskrive (men er ikke begrenset til):

- *Hva skal gjøres av hver av partene i avtalen;*
- *Den forventede kvaliteten på resultater/tjenester;*
- *Tildeling av roller og ansvar;*
- *Hva, når og hvordan informasjon vil bli utvekslet mellom partene. Informasjonen må inkludere rapportering om hendelser som beskrevet i alle undereksemplene ovenfor, samt de spesifikke egenskapene til infrastrukturen for sidesporet, som fartsgrenser, vektgrenser eller helningsforhold;*
- *Kompetansekrav;*
- *HMS-krav (utledet fra risikovurdering, nasjonale krav, osv.).*

Avtaleordninger og samarbeid

Jernbanevirksomheten er ansvarlig for å sørge for en sikker drift av toget, ved å koordinere og administrere togoperasjonene. Avtaleordninger (som regel bestående av rammeavtaler, særskilte avtaler og vedlegg) utgjør grunnlaget for et effektivt samarbeid mellom ulike jernbanevirksomheter, det være seg nye eller etablerte aktører, og må overholde bestemmelsene i europeisk og nasjonal lovgivning, samt eventuelle andre gjeldende krav.

Således må jernbanevirksomheten kontrollere risikoen ved driften, herunder samarbeid med samarbeidspartnere og bruken av (under)leverandører. NSA fører så tilsyn med at jernbanevirksomheten oppfyller sine lovfestede forpliktelser transparent og omhyggelig.

Jernbanevirksomheter kan ikke outsource deres sikkerhetsansvar for å koordinere og håndtere en sikker drift av togene deres. Dette virker imidlertid ikke ugunstig for foreliggende samarbeidsregimer mellom jernbanevirksomhetene. Grunnprinsippene ovenfor gjelder også for samarbeid mellom jernbanevirksomheter. Jernbanevirksomheten som er ansvarlig for å sørge for en sikker togdrift, må være tydelig identifisert i alle avtaler mellom de involverte partene, og må besitte et felles sikkerhetssertifikat. Denne jernbanevirksomheten kan enten forvalte ressursene direkte (bemanning, vogner) via sikkerhetsstyringssystemet, eller bestemme seg for å sette dem bort enten delvis eller helt (f.eks. leasing av vogner, ansettelse av lokførere) til en leverandør. I sistnevnte tilfelle sitter jernbanevirksomheten fortsatt med ansvaret for å kontrollere risikoer knyttet til bruken av (under)leverandører ved kontrollere at avtalen

gjennomføres i henhold til sikkerhetsstyringssystemet sitt og Forordning (EU) 1078/2012, og således må det kontrolleres at disse ressursene overholder lovfestede krav og andre gjeldende sikkerhetskrav (f.eks. at vogner er i sikker driftstilstand, rutekompatibilitet, personalutdanning, lokførere med gyldig lisens og sertifikat for en bestemt rute).

Et felles sikkerhetssertifikat som er utstedt av et sikkerhetssertifiseringsorgan (og overvåket av en NSA i henhold til dette) til avtaleparten (dvs. samarbeidspartneren eller underleverandøren), kan gi tilstrekkelig forsikring til jernbanevirksomheten som er ansvarlig for sikker drift, om at sikkerhetsstyringssystemet oppfyller de relevante kravene. Avtaleordningene omfatter utveksling av informasjon som er relevante for sikkerheten (f.eks. tidligere hviletid for lokomotivførere) mellom avtalepartene.

Prinsippene for samarbeid mellom jernbanevirksomhetene forblir de samme uavhengig av samarbeidsregimer, dvs. samarbeid eller bortsetting av (delvis eller helt) jernbanedrift i innenlandsk eller grenseoverskridende drift. Arten og omfanget av tiltakene som skal gjennomføres av jernbanevirksomhetene, og i hvilken utstrekning NSA skal føre tilsyn med samarbeidsordningene, står imidlertid i forhold til samarbeidsomfanget mellom jernbanevirksomhetene.

For eksempel vil grenseoverskridende samarbeid mellom jernbanevirksomheter (dvs. bruk av eksterne vogner og/eller bemanning) trolig kreve større kontroll enn noen andre samarbeidsordninger, fordi driften blir satt bort til en annet jernbanevirksomhet med andre språk og driftsregler for rullende materiell, som kan variere fra medlemsstat til medlemsstat. I motsetning til dette vil det bare være behov for mindre kontroll og dermed mindre tilsynsaktiviteter fra NSA.

Vedlegg 4 — Sikkerhetskultur

Introduksjon til sikkerhetskultur og en strategi for forbedring av sikkerhetskultur

Kultur oppstår fra samspillet mellom mennesker i hverdagen, og bidrar til å definere samfunnets atferdsmessige forventninger og normer. Kultur er et kompleks konsept som involverer en rekke faktorer som utvikler seg over tid, avhengig av omstendigheter, miljø og opplevelser i en nasjon, stat, samfunn og/eller organisasjon.

Sikkerhetskultur refererer til elementene i kulturen som spesifikt angår sikkerheten. Det er mulig å gi en beskrivelse av noen av faktorene som bidrar til en god sikkerhetskultur, men imidlertid umulig å samle sammen all informasjon som omfatter sikkerhetskulturen. Det finnes ingen enkel vitenskapelig måling av sikkerhetskulturen. Dette skyldes at de faktorene som bidrar til den varierer, ikke bare mellom organisasjoner, men også i dem. Ulike avdelinger har forskjellige sikkerhetskrav og behov, for eksempel driftsmessige og økonomiske, og den rådende sikkerhetskulturen vil utvikle seg ut fra disse. Eksterne faktorer som forskriftsmessige krav, utdanningsnivåer, samfunnsstrukturer og nasjonal kultur vil også bidra til å forme en organisasjons sikkerhetskultur.

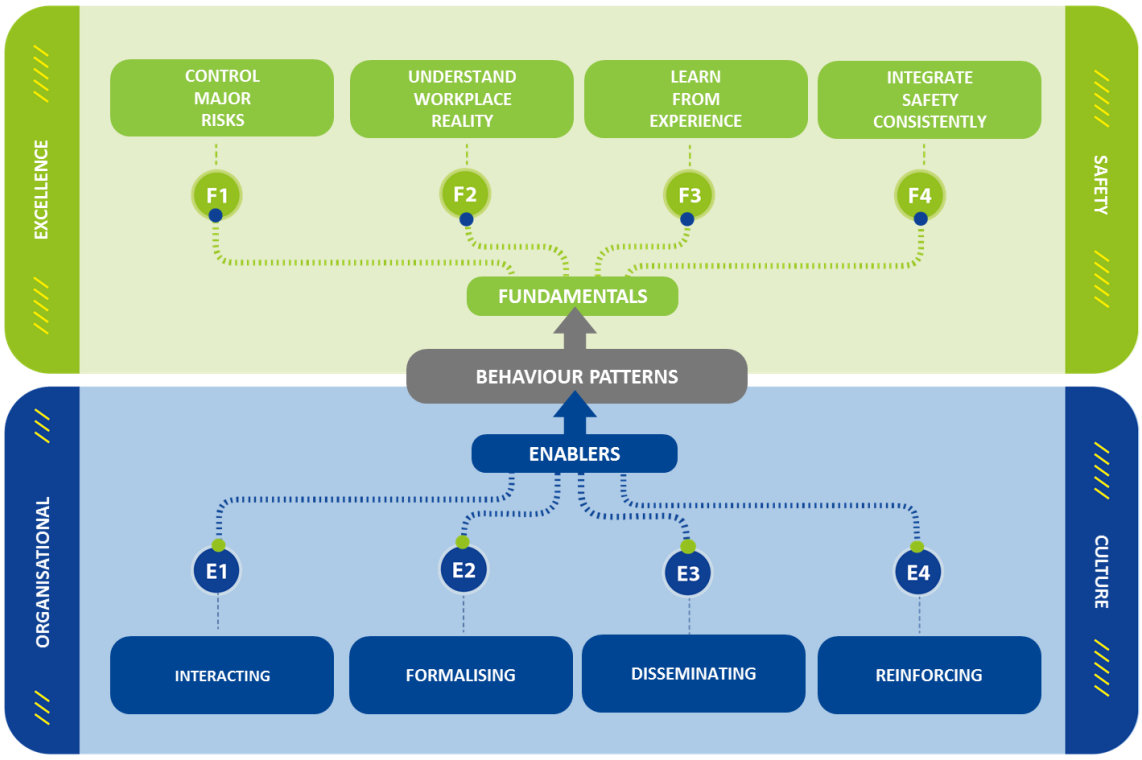
Sikkerhetskultur er et etablert konsept. Konseptet mangler imidlertid en definisjon man enes om. I denne sammenhengen har Byrået, sammen med representanter for sektoren, utviklet følgende forståelse som gjelder for enhver jernbaneorganisasjon: «*Sikkerhetskultur viser til samhandlingen mellom kravene i sikkerhetsstyringssystemet, hvordan de virker fornuftig basert på holdninger, verdier og overbevisninger, og hvordan de egentlig fungerer i beslutninger og atferd*.»

Når det er sagt, er en enkel måte å beskrive sikkerhetskulturen på å se på faktorene som bidrar til atferden. Sikkerhetsstyringssystemet danner grunnlaget ved å definere og pålegge hva som kreves, gjennom retningslinjer og prosedyrer. I utopien vil sikkerhetsstyringssystemet være perfekt, og all ledelse og personale vil etterleve det. Utopi er dessverre bare utopi, og det som skjer er at ledelse og personale prøver å gi innholdet i sikkerhetsstyringssystemet mening basert på verdier, holdninger og meninger på grunnlag av en kombinasjon av personlig erfaring og arbeidsstandarder og arbeidsforholdene på arbeidsplassen og i samfunnet. Hvis sikkerhetsstyringssystemet gir mening og det er en kultur for etterlevelse, vil korrekt atferd følge av dette. Hvis ikke dette er tilfellet blir det gjort individuelle tolkninger, og det vil bli anvendt alternative løsninger. Disse vil være basert på en individuell risikovurdering som veier opp faktorer som påvirker avgjørelser som er truffet. Risikovurderingen vil ikke bare fokusere på den faktiske risikoen, men omfatter også forhold knyttet til anvendelighet, risikoen for å bli tatt, ledelsens ord og handling, etc. Gjensidig avhengighet mellom sikkerhetsstyringssystemet, det at det gir mening, samt atferd, definerer derfor sikkerhetskulturen.

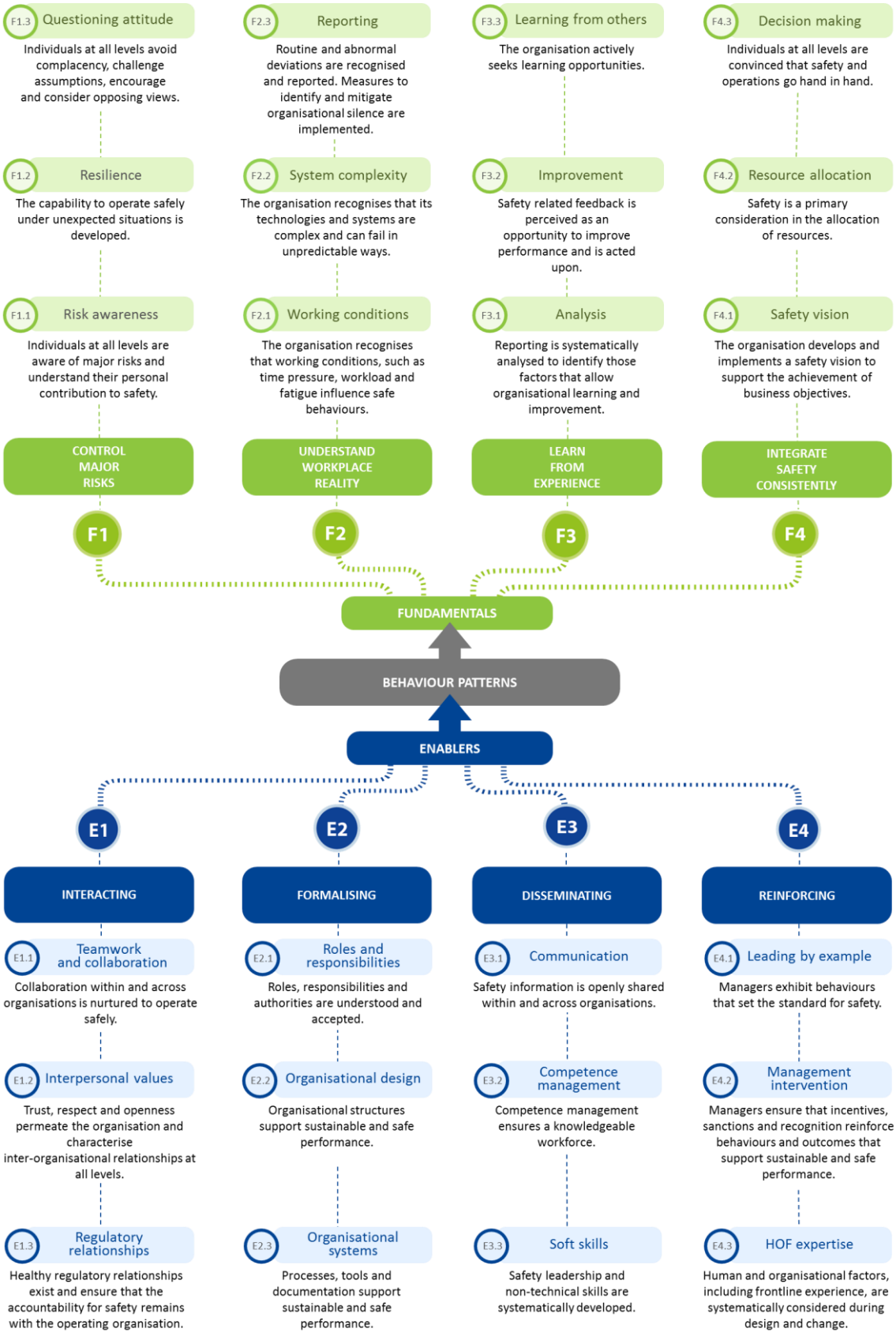
Vurdering av sikkerhetskulturen krever innsikt i de tre faktorene og deres gjensidige avhengighet. Som nevnt tidligere, finnes det ingen enkel vitenskapelig måling av sikkerhetskulturen. I stedet kan egenskaper som påvirker utvikling av sikkerhetskulturen analyseres i lys av de tre faktorene.

For eksempel kan retningslinjer som "Sikkerheten først" følges opp ved å undersøke hva de betyr for medarbeiderne — har de troen på dem, går ledelsen i bresjen, hvordan tas beslutninger og på hvilke grunnlag, hvordan reagerer organisasjonen når den er under press, osv. Lignende undersøkelser kan gjøres for andre faktorer, som kontinuerlig læring og en kritisk holdning. Når resultatene av analysen settes sammen, vil det dannes et bilde av tilstanden på kulturen. Over tid kan et mer omfattende bilde dannes, slik at det treffes mer fundamenterte konklusjoner.

Den europeiske jernbanesikkerhetskulturmodellen (se Figur 4) ble utviklet som et konseptuelt og evaluerende rammeverk som kan brukes til å bedre forstå konseptet sikkerhetskultur, og for å vurdere og forbedre sikkerhetskulturen til enhver jernbaneorganisasjon.



Figur 4: Modellen for europeisk jernbanesikkerhetskultur



Figur 5: Egenskaper ved modellen for europeisk jernbanesikkerhetskultur

Side om side sammenligninger mellom kravene i sikkerhetsstyringssystemet og modellen for europeisk jernbanesikkerhetskultur

Tabellene nedenfor inneholder en kolonnebasert sammenligning mellom European Safety Culture Model Fundamentals and Enablers og sikkerhetsstyringssystemkravene i Forordning (EU) 2018/762.

Nøye bruk av tabellene, sammen med veilederen om den europeiske sikkerhetskulturmodellen, bør gjøre det mulig for organisasjonen å se hvilke av kravene i sikkerhetsstyringssystemet som har sterke koblinger til egenskapene til den europeiske sikkerhetskulturmodellen og derfor tillate dem å utarbeide prosesser og prosedyrer som bedre ta hensyn til ønsket organisatorisk atferd.

Tabell 6: Side ved side sammenligning – SMS-krav/Modell for europeisk jernbanesikkerhetskultur

SMS-krav	*Kobling til modellen for europeisk jernbanesikkerhetskultur*
1. Organisasjonens driftskontekst	F1.1, F2.2, F3.3 F4.1 E1.1, E2.1, E2.2, E3.1, E4.3
2.1 Ledelse og forpliktelse	F1.1, F2.1, F2.2, F4.1 E1.1, E2.1, E3.1
2.2 Sikkerhetspolicy	F1.1, F2.1, F2.2, F4.1 E1.1, E3.1
2.3 Organisatoriske roller, ansvar, ansvarlighet og myndigheter	F1.1, F2.1, F2.2, F2.3, F3.1, F 3.2, F4.1, F4.2 E1.1, E2.1, E2.2, E3.1, E3.2, E4.3
2.4 Konsultasjon med ansatte og andre parter	F1.1, F2.1, F2.2, F2.3, F3.1, F3.2, F4.1, F4.2, E1.1, E2.2, E2.3, E3.1, E4.3
3.1 Tiltak for å sette fokus på risiko	F1.1, F2.1, F2.2, F2.3, F3.1, F3.2 F3.3, F4.1, F4.3 E1.1, E2.1, E2.2, E2.3, E3.1, E3.2, E4.3
3.2 Sikkerhetsmålsettinger og planlegging	F1.1, F2.1, F2.2, F2.3, F3.1, F 3.2, F4.1, F4.2 E1.1, E2.2, E2.3, E3.1, E4.3
4.1 Ressurser	F1.1, F2.1, F2.2, F4.1, F4.2, E1.1, E1.2, E2.1, E2.2, E2.3, E3.1, E3.2, E3.3, E4.3
4.2 Kompetanse	F1.1,F1.2, F1.3, F2.1, F2.2, F2.3, F3.1, F3.2, F4.1, F4.2, F4.3 E1.1, E2.1, E2.2, E2.3, E3.1, E3.2, E3.3, E4.1, E4.2, E4.3
4.3 Bevissthet	F1.1, F1.2, F2.2, F2.3, F3.1, F3.2, F4.1, F4.3 E1.1, E1.2, E2.1, E3.1, E3.2, E3.3, E4.1, E4.2
4.4 Informasjon og kommunikasjon	F1.1, F1.2, F2.2, F2.3, F3.1, F3.2, F4.1, F4.3 E2.1, E3.1, E3.2, E3.3, E4.2
4.5 Dokumentert informasjon	F1.1, F1.2, F2.2, F2.3, F3.1, F3.2, F4.1, F4.3 E2.1, E2.2, E2.3, E3.1, E3.2, E3.3, E4.2
4.6 Integrering av menneskelige og organisatoriske faktorer	F1.1, F1.2, F2.2, F2.3, F3.1, F3.2, F4.1, F4.3 E2.1, E2.2, E2.3, E3.1, E3.2, E3.3, E4.3
5.1 Driftsplanlegging og kontroll	F1.1, F2.1, F2.2, F3.1, F3.2, F4.1, F4.2 E2.1, E2.3, E3.1, E3.2, E3.3, E4.3
5.2 Aktivaforvaltning	F2.1, F2.2, F4.1, F4.2, F4.3, E1.1, E2.3, E3.1, E3.2, E4.3
5.3 Leverandører og samarbeidspartnere	F1.1, F2.1, F2.2, F4.1, F4.2, F4.3 E1.1, E2.3, E3.1, E3.2, E4.3
5.4 Endringsstyring	F1.1, F2.1, F2.2, F4.1, F4.2, F4.3 E1.1, E2.3, E3.1, E3.2, E4.3

SMS-krav	*Kobling til modellen for europeisk jernbanesikkerhetskultur*
5.5 Beredskapsstyring	F1.1, F1.2, F1.3, F2.1, F2.2, F3.1, F3.2, F3.3, F4.1, F4.2, F4.3 E1.1, E2.3, E3.1, E3.2, E3.3, E4.1, E4.2, E4.3
6.1. Overvåking	F1.1, F1.2, F1.3, F2.1, F2.2, F3.1, F3.2, F4.1, F4.2 F4.3 E1.1, E1.2, E2.1, E2.3, E3.1, E3.2, E3.3, E4.1, E4.2, E4.3
6.2 Internrevisjon	F1.1, F1.2, F1.3, F2.1, F2.2, F3.1, F3.2, F4.1, F4.2, F4.3 E1.1, E2.1, E2.3, E3.1, E3.2, E3.3, E4.1, E4.2, E4.3
6.3. Gjennomgang av ledelsen	F1.1, F1.2, F1.3, F2.1, F2.2, F3.1, F3.2, F4.1, F4.2, F4.3 E1.1, E2.1, E2.3, E3.1, E3.2, E3.3, E4.1, E4.2, E4.3
7.1. Ta lærdom av ulykker og uønskede hendelser	F1.1, F1.3, F2.1, F2.2, F2.3, F3.1 , F3.2, F4.1, F4.3 E1.3, E2.1, E2.3, E3.1, E3.2, E3.3, E4.2, E4.3
7.2. Kontinuerlig forbedring	F1.1, F1.3, F2.1, F2.2, F2.3, F3.1, F3.2, F4.1, F4.3 E2.1, E2.3, E3.1, E3.2, E3.3, E4.2, E4.3

Tabell 7: Side ved side sammenligning – Modell for europeisk jernbanesikkerhetskultur/SMS-krav

Attribtutt til modellen for europeisk jernbanesikkerhetskultur	*Kobling til SMS-krav*
F 1.1 Risikobevissthet	1, 2.1, 2.2, 2.3, 2.4, 3.1, 3.2, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2
F1.2 Utholdenhet	4.1, 4.2, 4.3, 4.5, 4.6, 5.5, 6.1, 6.2, 6.3
F1.3 Ha en kritisk holdning	5.5, 6.1, 6.2, 6.3, 7.1, 7.2
F2.1 Arbeidsforhold	2.1, 2.2, 2.3, 2.4, 3.1, 3.2, 4.1, 4.2, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2
F2.2 Systemekompleksitet	1, 2.1, 2.2, 2.3, 2.4, 3.1, 3.2, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2
F2.3 Rapportering	2.3, 2.4, 3.2, 4.2, 4.3, 4.4, 4.5, 4.6, 7.1, 7.2
F3.1 Analyse	2.3, 2.4, 3.2, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2
F3.2 Forbedring	2.3, 2.4, 3.2, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2
F3.3 Å lære av andre	3.1, 5.5
F4.1 Sikkerhetsvisjon	1, 2.1, 2.2,2.3, 2.4, 3.1, 3.2, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2
F4.2 Ressurstildeling	2.3, 2.4, 3.2, 4.1, 4.2, 5.1, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3
F4.3 Beslutningstaking	3.1, 3.2, 4.2, 4.3, 4.4, 4.5, 4.6, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2, 7.3
E1.1 Teamarbeid og samarbeid	1, 2.1, 2.2, 2.3, 2.4, 3.1, 3.2, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2
E1.2 Mellommenneskelig verdi	4.1, 4.3, 6.1
E1.3 Lovbestemt forhold	7.1
E2.1 Roller og ansvar	1, 2.1, 2.3, 3.1, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 6.1, 6.2, 6.3, 7.1, 7.2
E2.2 Organisasjonsdesign	1, 2.1, 2.3, 2.4, 2.4, 3.1, 3.2, 4.1, 4.2, 4.4, 4.5
E2.3 Organisasjonssystemer	2.4, 3.1, 3.2, 4.1, 4.2, 4.5, 4.6, 5.1, 5.2, 5.3, 5.4, 5.56.1, 6.2, 6.3, 7.1, 7.2
E3.1 Kommunikasjon	2.1, 2.2, 2.3, 2.4, 3.1, 3.2, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2
E3.2 Kompetansestyring	3.1, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2

Attribtutt til modellen for europeisk jernbanesikkerhetskultur	*Kobling til SMS-krav*
E3.3 Myke ferdigheter	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 6.1, 6.2, 6.3, 7.1, 7.2
E4.1 Gå foran med et godt eksempel	4.2, 4.3, 5.5, 6.1, 6.2, 6.3
E4.2 Intervensjon fra ledelsen	4.2, 4.3, 4.4, 4.5, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2
E4.3 HOF kompetanse	1, 2.3, 2.4, 3.1, 3.2, 4.1, 4.2, 4.6, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2

Ytterligere informasjon om sikkerhetskultur finnes på ERAs nettsider.

Vedlegg 5 — Menneskelige og organisatoriske faktorer

Introduksjon til menneskelige og organisatoriske faktorer

Menneskelige og organisatoriske faktorer (MOF) er et tverrfaglig felt som fokuserer på hvordan man kan øke sikkerheten, forbedre ytelsen og øke brukertilfredsheten. MOF er en brukersentrert tilnærming, det vil si at modellen er basert på en eksplisitt forståelse av brukere, oppgaver og miljøer. Utgangspunktet er alltid brukerens evner og begrensninger, og hvordan disse påvirkes og samhandler med systemene som brukes når arbeidsoppgaver utføres. Målet er å identifisere hvordan man best kan utføre arbeidsoppgavene på en trygg og effektiv måte. Det legges vekt på anvendelighet. MOF brukes både som et proaktivt middel for å sikre gode designprosesser, samt som et tilbakevirkende middel til å identifisere grunnleggende årsaker når noe har gått galt.

Når man for eksempel skal designe en ny bil, er det ikke nok å bare bruke designstandardene. Lokomotivførere, ledere og vedlikeholdspersonell bør være involvert for å få frem deres erfaringer og forståelsen av hvordan de skal utføre arbeidsoppgavene sine trygt og effektivt. Dette kan for eksempel være relatert til spesifikke stasjons- eller linjeproblemer, tilgjengelighet og tilgang til vedlikeholdspersonell, oppgaveprioriteringer i førerhuset, kommunikasjonskrav eller passasjeratferd på stasjoner.

Man kan innhente kunnskap og erfaring fra ulike operatører på best mulig måte gjennom en iterativ prosess, der brukeren evaluerer design og utvikling av toget på kontinuerlig basis i løpet av designets og utviklingens fremdrift. Dette bidrar til å forhindre en felles feil i designprosessen, altså å fokusere på menneskets samspill med individuelle systemer i stedet for utføring av oppgaver generelt. Ulike leverandører har for eksempel ulikt syn på hvordan alarmer skal prioriteres, og uten et helhetlig perspektiv ender ofte brukeren opp med å bli overlesset med informasjon som er av begrenset relevans for å utføre oppgaven. Dette fordi teknisk design gir muligheten til å vise informasjonen, men der brukeren har kanskje ikke behov for den. MOF-analyse kan hjelpe til å skille mellom behovet for å vite og "kjekt å ha".

MOF innebærer å ha et systematisk perspektiv, det vil si ikke bare å se på de menneskelige, teknologiske og organisatoriske faktorene i seg selv, men også ha fokus på samspillet mellom de ulike faktorene. Hvis for eksempel en lokomotivfører har vært involvert i en passhendelse, omfatter de foreslåtte granskningspunktene relevante problemer (ikke en uttømmende liste), f.eks. tretthet, kognitiv overbelastning, kompetanse, osv. (menneskelig), teknologisk innvirkning på yteevnen, som for eksempel grensesnitt mellom menneske og system, layout, signalplassering (teknologi), organisasjonens innflytelse på yteevnen, som opplæring, sikkerhetsstyringssystem, organisasjonsprioriteringer (organisasjon) og samspillet mellom de tre områdene som innflytelse på anskaffelser mht. design eller endringsstyring med innføring av nytt design.

Metodene er hentet fra en rekke forskjellige felt, for eksempel eksperimentalpsykologi, industriteknikk, organisasjonspsykologi, sosiologi, ledelsesvitenskap, kognitiv teknikk, ergonomi, datavitenskap og sikkerhetsteknikk.

Siden MOF fokuserer på brukeren, er en oppgaveanalyse en vanlig anvendt metode. En oppgaveanalyse gir designeren en forståelse av oppgavene som skal utføres, og hvordan de relaterer seg til systemer som brukeren samhandler med og organisatoriske faktorer som har innvirkning på yteevnen. Basert på oppgaveanalysen kan det gjennomføres videre analyser, som analyser av samhandling mellom menneske og system, arbeidsbelastning, menneskelig pålitelighet/risiko, samt antropometrisk og biometrisk analyse. Nøkkelen er å sikre at brukeren har best mulig arbeidssituasjon for en trygg og effektiv prestasjonsevne.

Ytterligere informasjon om menneskelige og organisatoriske faktorer finnes på ERA-nettstedet.

Strategi for å underbygge integrering av menneskelige og organisatoriske faktorer i sikkerhetsstyringssystemet

Organisasjonen bør sette opp en strategi for å sikre at menneskelige faktorer, kunnskaper, metoder og en menneskelig sentrert tilnærming systematisk og konsekvent anvendes i alle relevante prosesser i organisasjonen. En slik tilnærming innebærer først å vurdere behovene, evnene og atferden til mennesker, og deretter å utarbeide en strategi for å imøtekomme slike behov, evner og atferd.

Strategien menneskelige og organisatoriske faktorer (MOF) kan inneholde elementer som knytter seg til:

Ledelse

- *Ledelse og forpliktelse*
  - *Ledelsens engasjement til MOF er tydelig beskrevet i retningslinjer og målsettinger;*
  - *Det foreligger en prosess/veileder som viser hvordan MOF skal anvendes i prosjekter;*
  - *MOF er en integrert del av designprosessen og prosjektstyringen.*
- *Sikkerhetspolicy*
  - *Sikkerhetspolicyen definerer klart at det bør anvendes et MOF-perspektiv i alle sikkerhetsrelaterte prosesser.*
- *Organisatoriske roller, ansvar, ansvarlighet og myndigheter*
  - *Klart definerte roller, ansvar og ansvarlighet hos MOF-ekspertisen;*
  - *Det foreligger en prosess for hvordan MOF-ekspertisen jevnlig deltar i prosjekter og prosesser.*

Planlegging

- *Tiltak for å sette fokus på risiko*
  - *En beskrivelse av hvordan MOF-perspektivet tas i betraktning i risikoanalyser;*
  - *Involvering av HOF-spesialister og frontlinjearbeidere inkludert de som har grensesnitt i risikoanalyser.*

Støtte

- *Ressurser og kompetanse*
  - *Systematisk tilnærming med bruk av menneskelig og organisatorisk faktorkompetanse for å sikre at sikkerhetsrelevante roller har tilstrekkelige ressurser basert på risikovurderingen.*
  - *Kobling mellom risikovurderingen, de sikkerhetsrelaterte oppgavene og kompetansestyringssystemet for å sikre at personalet kontinuerlig demonstrerer den identifiserte kompetansen;*
  - *Det tilordnes tid og ressurser for å sikre at MOF-kravene er imøtekommet.*
- *Bevissthet*
  - *Systematisk bruk av kompetanse om menneskelige og organisatoriske faktorer i organisasjonen for å sikre at ansatte i relevante roller er klar over rollen de spiller i sikkerheten.*

Drift

- *Driftsplanlegging og kontroll*
  - *MOF er hensyntatt i driftsplanleggingen.*
- *Aktivaforvaltning*
  - *Organisasjonen har veiledning for å anvende en menneskelig sentrert tilnærming i hvert trinn av levetiden.*
- *Endringsstyring*
  - *MOF skal alltid vurderes som en del av håndteringen av endringsprosessen.*

Ytelsesevaluering

- *Overvåking*
  - *Sikkerhetsytelsen vurderes systematisk i lys av MOF-strategien.*

Forbedring

- *Ta lærdom av ulykker og uønskede hendelser*
  - *MOF-ekspertise og metoder brukes ved granskning av ulykker;*
  - *Det foreligger en metode for å gjennomføre granskning basert på MOF-kunnskap og metoder;*
  - *Det foreligger et opplæringsprogram for dem som gransker uønskede hendelser og ulykker, der man anvender et MOF-perspektiv.*
- *Kontinuerlig forbedring*
  - *Prosess for kontinuerlig forbedring av organisasjonsprosessene for styring av MOF.*

Vedlegg 6 – Definisjoner

Bruken av ordene eller begrepene i dokumentet, for eksempel "må", "bør" eller "skal", indikerer at det foreligger et lovfestet krav som må etterleves. Definisjoner som finnes i relatert jernbanesikkerhetslovgivning, som for eksempel jernbanesikkerhetsdirektivet (EU) 2016 798, CSM for Risk Evaluation and Assessment (EU) 402/2013 og i de relevante tekniske spesifikasjonene for interoperabilitet, gjelder for dette dokumentet, men er ikke gjengitt nedenfor.

Ulykke	En uønsket eller utilsiktet plutselig hendelse eller en kjede av slike hendelser som får skadelige konsekvenser; ulykker er delt inn i følgende kategorier: kollisjoner; avsporinger; ulykker på planoverganger; ulykker med personer som involverer rullende materiell i bevegelse; brann og andre hendelser (Direktiv (EU) 2016/798).
Driftsområde	Ett eller flere nett i én eller flere medlemsstater, hvor en jernbanevirksomhet har til hensikt å drive sin virksomhet (Direktiv (EU) 2016/798).
Aktivaforvaltning	Tilnærmingen som brukes av en organisasjon for å sikre at fysiske eiendeler forblir sikre, egnet til bruk og kommersielt levedyktige fra design og konstruksjon, og gjennom hele livssyklusen og frem til avvikling.
Revisjon	En systematisk, uavhengig og dokumentert prosess for å skaffe revisjonsbevis og evaluere dette objektivt, for å fastslå at omfanget av revisjonskriteriene er oppfylt (ISO 9000).
Forretningsenhet	En forretningsenhet er en avdeling eller et funksjonsområde i en organisasjon. Det kan dreie seg om ulike roller og formål, f.eks. menneskelige ressurser, produksjon, langdistansetransport, logistikk, sporveksling.
Driftens art	Driftens art etter dens omfang, herunder utforming og oppbygging av infrastrukturen, vedlikehold av infrastrukturer, trafikkplanlegging, trafikkstyring og kontroll, og bruk av jernbaneinfrastrukturen, inkludert konvensjonelle linjer og/eller høyhastighetslinjer, passasjertransport og/eller godstransport
Kompetanse	Evnen til å anvende kunnskaper og ferdigheter for å nå ønskede resultater (ISO 9000).
Kontinuerlig forbedring	Gjentakende aktivitet for å forbedre ytelsen (dvs. målbart resultat) (ISO 9000).
Dokumentstyring	Prosessen (eller prosedyren) for identifisering, utarbeiding, vedlikehold, styring, lagring og oppbevaring av dokumentert informasjon.
Driftsomfang	I forbindelse med jernbanedriften som utføres av jernbanevirksomhetene, karakteriseres omfanget av passasjerantall og/eller godsvolum og den estimerte størrelsen på en jernbanevirksomhet med hensyn til antall ansatte som arbeider i jernbanesektoren (dvs. som mikrobedrifter eller små, mellomstore eller store bedrifter) (Direktiv (EU) 2016/798). I forbindelse med jernbanedriften som uføres av infrastrukturforvaltere, omfanget som karakteriseres av lengden på jernbanesporet og infrastrukturforvalterens estimerte størrelse med hensyn til antall ansatte i jernbanesektoren (Forordning (EU) 2018/762).
Fare	Et forhold som kan føre til en ulykke (Forordning (EU) 402/2013).

Menneskelige og organisatoriske faktorer	Alle menneskelige ytelsesegenskaper og organisatoriske aspekter som må vurderes for å ivareta sikkerheten og effektiviteten i et system eller en organisasjon gjennom hele levetiden.
Menneskelig sentrert tilnærming	En tilnærming som innebærer først å vurdere behovene, evnene og atferden til mennesker, og deretter å utarbeide en strategi for å imøtekomme slike behov, evner og atferd.
Uønsket hendelse	Enhver hendelser, unntatt en ulykke eller alvorlig ulykke, som påvirker sikkerheten ved jernbanedriften (Direktiv (EU) 2016/798). Dette inkluderer nestenulykker.
Infrastrukturforvalter	Ethvert organ eller selskap som er spesifikt ansvarlig for å etablere, administrere og vedlikeholde jernbaneinfrastrukturen, inkludert trafikkstyring og kontrollkommando og signalering. Infrastrukturforvalterens funksjoner på et jernbanenett eller en del av et jernbanenett kan tildeles ulike organisasjoner (Direktiv 2012/34/EU).
Interessent	Person eller organisasjon som enten kan påvirke, bli påvirket av eller som oppfatter seg selv som påvirket av en beslutning eller aktivitet (ISO 9000) som er knyttet til sikkerhetsstyringssystemet.
Granskning	En prosess som gjennomføres med det formål å forebygge ulykker og uønskede hendelser, som omfatter innsamling og analyse av informasjon, komme frem til konklusjoner, herunder å fastslå årsak, og når det er hensiktsmessig, utarbeide sikkerhetsanbefalinger (Direktiv (EU) 2016/798).
Styringssystem	Et sett med elementer i en organisasjon for å fastsette retningslinjer og målsettinger, og prosessene for å nå disse målsettingene, og som er forbundet med eller samhandler med hverandre (ISO 9000).
Overvåking	Ordninger som er innført av jernbanevirksomheter, infrastrukturforvaltere eller virksomheter med ansvar for vedlikehold, for å kontrollere at styringssystemet anvendes korrekt og at det fungerer (Forordning (EU) 1078/2012).
Nasjonal bestemmelse	Alle bindende bestemmelser som er vedtatt i en medlemsstat, uavhengig av organet som fastsetter dem, som inneholder krav til jernbanesikkerhet eller tekniske krav, unntatt krav som er fastsatt i EU eller internasjonale bestemmelser, og som gjelder i jernbanevirksomheters, infrastrukturforvalteres eller tredjeparts jernbanevirksomhet (Direktiv (EU) 2016/798).
Prosess	Et sett av aktiviteter som er forbundet med eller samhandler med hverandre, og som gjør teori om til praksis (ISO 9000).
Jernbaneinfrastruktur	Fasiliteter som er nødvendige for at en jernbane skal kunne fungere, herunder: • Jernbanespor og tilknyttede sporstrukturer; • Sideveier, signalanlegg, kommunikasjonssystemer, rullende materiell; • Kontrollsystemer, togstyringssystemer og databehandlingssystemer; • Varsler og skilting; • Elektrisk kraftforsyning og elektriske trekksystemer; • Tilknyttede bygninger, verksteder, depoter og gårder; og • Anlegg, maskiner og utstyr.

Jernbanevirksomhet	En jernbanevirksomhet som definert i Artikkel 3(1) i Direktiv 2012/34/EU, og ethvert annet offentlig eller privat foretak som har som formål å yte transport av gods og/eller passasjerer på jernbane, på grunnlag av at foretaket skal sørge for trekkraft, inkludert foretak som kun leverer trekkraft (Direktiv (EU) 2016/798). Ethvert offentlig eller privat foretak som er lisensiert i henhold til dette direktivet, som har som hovedvirksomhet er å yte tjenester for godstransport og/eller passasjertransport på jernbane med krav om at foretaket sørger for trekkraft. Dette inkluderer også foretak som kun leverer trekkraft (Direktiv 2012/34/EU).
Risiko	Hyppigheten av forekomsten av ulykker og uønskede hendelser som medfører skade (som følge av fare) og alvorlighetsgraden av skadene (Forordning (EU) 402/2013).
Risikoanalyse	Systematisk anvendelse av all tilgjengelig informasjon for å identifisere farer og anslå risikoer (Forordning (EU) 402/2013).
Risikovurdering	Den samlede prosessen som omfatter en risikoanalyse og en risikovurdering (Forordning (EU) 402/2013).
Risikoevaluering	En prosedyre basert på risikoanalysen for å fastslå om det er oppnådd et akseptabelt risikonivå (Forordning (EU) 402/2013).
Risikostyring	Systematisk anvendelse av styringspolicyer, prosedyrer og praksis for arbeidsoppgaver, for å analysere, evaluere og kontrollere risikoene (Forordning (EU) 402/2013).
Sikkerhetskultur	Samhandlingen mellom kravene i sikkerhetsstyringssystemet, hvordan de virker fornuftig basert på holdninger, verdier og overbevisninger, og hvordan de egentlig fungerer i beslutninger og atferd. En positiv sikkerhetskultur er preget av et kollektivt engasjement fra ledere og enkeltpersoner til alltid å handle på en trygg måte, spesielt når de står overfor konkurrerende mål (Forordning (EU) 2018/762).
Mål	Resultatene som skal oppnås. En sikkerhetsmålsetting må være spesifikk, målbar, oppnåelig, realistisk og tidsbasert. Den må også angis for relevante funksjoner og nivåer i organisasjonen.
Samarbeidspartner	Et kommersielt foretak som et annet kommersielt foretak har inngått samarbeid med. Dette forholdet kan være en avtalebasert, eksklusiv beheftelse, der begge foretakene forplikter seg til å ikke samarbeide med noen tredjeparter.
Samarbeid	En ordning der partene, også kalt samarbeidspartnere, blir enig om å samarbeide for å fremme felles interesser.
Sikkerhetsstyringssystem	Organisering, ordninger og prosedyrer fastsatt av en infrastrukturforvalter eller en jernbanevirksomhet, for å sikre en sikker drift av virksomheten (Direktiv (EU) 2016/798).
Toppledelse	Person eller gruppe som styrer og kontrollerer en organisasjon på høyeste nivå (ISO 9000).
Driftstype	Typen kjennetegnes ved passasjertransport, inkludert eller ekskludert høyhastighetstjenester, godstransport, inkludert eller ekskludert farlig gods, og kun skiftetjenester (Direktiv (EU) 2016/798).