Trafik-, Bygge- og Boligstyrelsen
Danish Transport, Construction and Housing Authority

Vejledning i Sikkerhedsledelse

efter bekendtgørelse nr. 712 af 20. maj 2020 om sikkerhedsgodkendelse, EU-sikkerhedscertifikat og sikkerhedscertifikat på jernbaneområdet

Version 1
19. juni 2020

Indhold

Indledning **4**

Vejledning **6**

1. Virksomhedens rammer og vilkår 6
   1.1. Forståelse af virksomheden og dens rammer og vilkår *6*
   1.2. Eksterne krav *6*
   1.3. Identifikation af farer *7*
   1.4. Sikkerhedsledelsessystem *8*
2. Lederskab 9
   2.1. Lederskab og forpligtelse *9*
   2.2. Sikkerhedspolitik *10*
   2.3. Roller, ansvar og beføjelser i organisationen *10*
3. Planlægning 11
   3.1. Håndtering af farer *11*
   3.2. Sikkerhedsmål og handlingsplaner *12*
4. Støtteaktiviteter og -funktioner 13
   4.1. Organisering *13*
   4.2. Sikring af kompetencer *15*
   4.3. Bevidsthed *17*
   4.4. Kommunikation *17*
   4.5. Sikkerhedsledelsessystemets dokumentation *18*
5. Godkendelse og drift 21
   5.1. Godkendelse af infrastruktur og køretøjer *21*
   5.2. Drift *22*
   5.3. Vedligehold af infrastruktur og køretøjer *23*
   5.4. Nødberedskab og afværgeforanstaltninger *24*
   5.5. Registrering og håndtering af ulykker og forløbere til ulykker *25*
   5.6. Opsamling af data om fejl og mangler opstået under driften *26*
   5.7. Afvigelser fra sikkerhedsledelsessystemet, som identificeres løbende *26*
   5.8. Styring af eksterne leverancer *27*
   5.9. Eksterne krav *28*
   5.10. Håndtering af ændringer *29*
   5.11. Dispensationer *30*
6. Overvågning 30
   6.1. Overvågning, måling, analyse og evaluering *30*
   6.2. Sikkerhedsmål *31*
   6.3. Sikkerhedsindikatorer *32*
   6.4. Operationelle inspektioner *32*
   6.5. Intern audit (systemaudit) *33*
7. Forbedring 35
   7.1. Generelt *35*
   7.2. Ledelsens evaluering *35*
   7.3. Afvigelser og korrigerende handlinger *38*

Bilag **40**

Krydsreferencetabel: Bek. 712, Bek. 147, Bek. 13/14 og ISO 9001:2015 40

Indledning

Infrastrukturforvaltere og jernbanevirksomheder på bybaner skal have et sikkerhedsledelsessystem, der opfylder kravene i bilag 1[1] til bekendtgørelse nr. 712 af 20. maj 2020 om sikkerhedsgodkendelse, EU-sikkerhedscertifikat og sikkerhedscertifikat på jernbaneområdet. Bekendtgørelsen er nyaffatet som følge af reglerne i 4. jernbanepakke, der er gældende fra 16. juni 2020.

Bybaner, herunder letbaner

I forhold til bybaner er der ikke ændringer i forhold til kravene til sikkerhedsledelsessystemer i bekendtgørelse nr. 147 af 30. januar 2017 om sikkerhedsgodkendelse og sikkerhedscertifikat på jernbaneområdet.

For en lettere gennemgang af hvad et sikkerhedsledelsessystem indebærer, henvises til *"Introduktion til sikkerhedsledelse"* [2].

Jernbanevirksomheder og infrastrukturforvaltere på den konventionelle jernbane

Jernbanevirksomheder, infrastrukturforvaltere og virksomheder, der kører på eget ansvar (herunder entreprenører), der er omfattet af reglerne i direktiv 2016/798/EU (jernbanesikkerhedsdirektivet), skal have et EU-certifikat, der opfylder kravene i Kommissionens delegerede forordning 762/2018/EU, uanset om de skal køre national eller grænseoverskridende kørsel. Denne forordning[3] vil ikke blive beskrevet yderligere i denne vejledning, da vejledningen er henvendt til bybaner.

Formålet med denne vejledning er med udgangspunkt i bekendtgørelsens bilag 1 at forklare, hvad kravene til et sikkerhedsledelsessystem indebærer, og hvordan disse kan opfyldes.

Vejledningen erstatter Trafikstyrelsens "Vejledning i sikkerhedsledelse" fra 7. oktober 2013. Således forventes det, at denne vejledning også benyttes af virksomheder, der er godkendt hhv. certificeret efter bekendtgørelse 13 hhv. 14 af 4. januar 2007.

Trafik-, Bygge- og Boligstyrelsen har endvidere udarbejdet en vejledning i sagshåndtering ved udstedelse af sikkerhedscertifikat og sikkerhedsgodkendelse.

Kravene til de forskellige typer af virksomheder

Som udgangspunkt er kravene til sikkerhedsledelsessystem ens for alle virksomheder uanset type og størrelse.

Men for at få et effektivt system, er det vigtigt, at den enkelte virksomhed udarbejder et sikkerhedsledelsessystem, der passer til virksomheden. Mindre virksomheder har ikke nødvendigvis behov for ligeså omfattende arbejdsgange og systemer som større virksomheder.

Til gengæld er der forskel på, hvilke aktiviteter der er omfattet af sikkerhedscertifikatet og sikkerhedsgodkendelsen. Generelt for "andre virksomheder, der kan opnå sikkerhedscertifikat", (dem der arbejder for jernbanevirksomheder og infrastrukturforvaltere) gælder, at sikkerhedscertifikatet udelukkende omfatter de aktiviteter, der foretages i forbindelse med virksomhedens kørsel. En entreprenørvirksomhed får altså ikke et sikkerhedscertifikat, der dækker entreprenørens faglige kompetencer i forbindelse med vedligeholdelse af infrastruktur. Ansvaret for infrastrukturvedligeholdelse er alene infrastrukturforvalterens.

[1] Bilag 1 gælder kun for bybaner, herunder letbaner (Infrastrukturforvaltere og entreprenører skal opfylde CSM SLS (762/2018/EU) på lige fod med jernbanevirksomhederne)

[2] https://www.trafikstyrelsen.dk/da/Jernbanesikkerhed/Ans%C3%B8g-om-godkendelse-og-tilladelse/Introduktion-til-sikkerhedsledelsessystem#

[3] https://eur-lex.europa.eu/legal-content/DA/TXT/?qid=1592306706807&uri=CELEX:32018R0762

Læsevejledning

Det anbefales at virksomhederne starter med at læse vejledningen til krav 1, Virksomhedens rammer og vilkår. Herefter bør vejledningen anvendes som et opslagsværk. Det kan dog anbefales virksomheder, der ansøger om sikkerhedsgodkendelse eller -certifikat første gang at læse vejledningen i sin helhed.

Bekendtgørelsens krav er i vejledningen anført ordret i grønne bokse.

I vejledningsteksten, der følger efter kravet, er der brugt betegnelsen "virksomheden", når et krav gælder alle virksomhedstyper, der kan opnå sikkerhedsgodkendelse og sikkerhedscertifikat.

Der er igennem vejledningen brugt forskellig syntaks for at skelne mellem beskrivelser, som er en uddybning eller forklaring til et ufravigeligt krav og beskrivelser, der er ment som en vejledning i, hvordan kravet kan opfyldes. Formålet med den første type er at sikre forståelse af, hvad kravet indebærer, og ordet "skal" bruges, mens formålet med den anden type er at hjælpe den ansøgende virksomhed på vej i forhold til, hvordan kravene kan opfyldes. Her bruges ordene "bør", "kan" mv. Vejledningen er ikke bindende på disse områder, og kravene kan søges opfyldt på anden måde, men ofte vil beskrivelserne rumme det, der inden for ledelsessystemer regnes som almindeligt accepterede metoder. Beskrivelserne er ikke nødvendigvis udtømmende, så hver enkelt virksomhed er selv forpligtet til at vurdere, hvad der skal til for at opfylde kravene på en tilstrækkelig og dækkende måde for den pågældende virksomhed.

Når der i vejledningen anvendes ordene "Sikkerhedsledelsessystemet skal …" betyder det, at der i sikkerhedsledelsessystemet forventes at være dokumenterede processer eller tilsvarende for at sikre opfyldelse af det pågældende krav.

Når der i vejledningen anvendes ordene "Virksomheden skal…", forventes ikke nødvendigvis at virksomheden har udarbejdet dokumenterede processer, men at ledelsen blot har sikret, at det pågældende krav er opfyldt. Eksempelvis forventes det ikke, at virksomheden har udarbejdet en proces for udarbejdelse af en sikkerhedspolitik, men blot at denne er udarbejdet.

Vejledning

1. Virksomhedens rammer og vilkår

1.1. Forståelse af virksomheden og dens rammer og vilkår

Virksomheden skal identificere og dokumentere sine aktiviteter i forbindelse med den del af driften, som sikkerhedscertifikatet eller sikkerhedsgodkendelsen omfatter, samt identificere og dokumentere eksterne parter uden for og inden for jernbanesystemet samt grænseflader, der er relevante for sikkerheden.

Formålet med dette krav er, at virksomheden skal danne sig et overblik over de aktiviteter som certifikatet/godkendelsen omfatter samt de grænseflader og parter udenfor virksomheden, som kan påvirke jernbanesikkerheden.

Det drejer sig specifikt om at identificere de aktiviteter, som virksomheden udfører i forbindelse med den del af driften, som sikkerhedscertifikatet og/eller sikkerhedsgodkendelsen vedrører.

Således er det f.eks. for entreprenørvirksomheder, der i forbindelse med anlægs- og vedligeholdelsesarbejde for infrastrukturforvaltere udfører kørsel på eget ansvar, kun de aktiviteter, der er forbundet med kørslen (herunder uddannelse af førere samt vedligeholdelse af køretøjer) det drejer sig om, og ikke anlægs- og vedligeholdelsesarbejdet. Dette hører under infrastrukturforvalterens aktiviteter / ansvarsområde.

Støtteaktiviteter, som f.eks. ledelse, intern audit mv. er heller ikke en del af de aktiviteter, der skal identificeres her.

Virksomheden skal ligeledes identificere hvilke grænseflader der er imellem aktiviteter internt i virksomheden og hvilke grænseflader der er til eksterne samarbejdspartnere, andre jernbanevirksomheder eller infrastrukturforvaltere, leverandører mm. samt omgivende miljø (overkørsler, kommuner, borgere der færdes ved jernbanen etc.).

En metodisk fremgangsmåde bør kunne sikre, at alle relevante aktiviteter i organisationen og relevante grænseflader bliver identificeret, og nedbrudt på et relevant operationelt niveau. Ved identifikationen bør virksomheden inddrage medarbejdere med de rette kompetencer bredt fra virksomheden, for at få større sikkerhed for at arbejdet bliver fyldestgørende.

De identificerede aktiviteter mv. kan dokumenteres i skematiske opstillinger (regneark / matricer) og/eller tegninger.

Formålet med at identificere sine aktiviteter er, at virksomheden efterfølgende kan identificere de jernbanesikkerhedsmæssige farer, der er forbundet med driften af virksomheden, og således forstå hvilke risici, den udsætter sig selv og omverdenen for (se krav 1.3).

Den samlede dokumentation danner således grundlag for etablering af risikoprofil og sikkerhedsledelsessystem (se krav 1.3 og 1.4).

1.2. Eksterne krav

1.2.1. Virksomheden skal identificere eksterne krav, som er relevante i forhold til virksomhedens aktiviteter, herunder lovkrav, bekendtgørelser, myndighedsafgørelser, tekniske og driftsmæssige standarder og andre normative krav.

1.2.2. Virksomheden skal kunne dokumentere, at relevante krav er identificeret.

Formålet med dette krav er, at virksomheden opnår en afklaring af den lovgivningsmæssige ramme, som virksomheden skal overholde, mens krav 5.9 handler om den løbende identifikation af lovkrav og andre krav og implementering af disse i sikkerhedsledelsessystemet.

For at sikre sig, at virksomheden ved sine aktiviteter overholder relevant lovgivning, skal virksomheden identificere relevant gældende lov samt andre relevante standarder og forskrifter mm.

Virksomheden skal være opmærksom på, at det ikke kun er myndigheder, der kan stille krav til virksomheden. Eksempelvis stiller en infrastrukturforvalter krav til en jernbanevirksomhed.

Krav fra myndighederne kan f.eks. findes på Trafik-, Bygge- og Boligstyrelsens hjemmeside og / eller Retsinformation, mens krav fra infrastrukturforvaltere kan findes hos disse.

De identificerede love og regler danner sammen med risikoprofilen, jf. nedenfor, grundlag for etablering af sikkerhedsledelsessystem (se krav 1.3 og 1.4).

1.3. Identifikation af farer
1.3.1. På baggrund af virksomhedens identificerede aktiviteter, grænseflader og eksterne krav skal virksomheden udarbejde og vedligeholde en risikoprofil. Virksomheden skal sikre, at alle relevante farer i forhold til jernbanesikkerheden og deres årsager identificeres og håndteres i risikoprofilen
1.3.2. Risikoprofilen samt dens vedligeholdelse skal dokumenteres.

Formålet med dette krav er, at virksomheden får etableret et overblik over de farer og risici, som virksomhedens aktiviteter medfører, således at virksomheden kan prioritere og opstille barrierer, og forvalte sine aktiviteter sikkerhedsmæssigt forsvarligt, med henblik på at forebygge hændelser og ulykker og dermed sikre et højt jernbanesikkerhedsniveau.

Dette krav omhandler identifikation og dokumentation af farer og risici. Opstilling af barrierer beskrives i krav 3.1.

Risikoprofil

En risikoprofil er en optegnelse af de farer, som virksomhedens aktiviteter medfører, farernes estimerede risici samt opstillede barrierer, som er nødvendige for at eliminere / begrænse risici til et acceptabelt niveau. En risikoprofil skal være dokumenteret, f.eks. i et regneark eller en database.

Metodik

Ved udarbejdelse af virksomhedens risikoprofil bør tages udgangspunkt i de aktiviteter der er identificeret, jf. krav 1.1.

For hver aktivitet identificeres de farer, der er forbundet med den pågældende aktivitet. Ligeledes identificeres der årsager for hver fare.

Virksomheden skal også identificere de farer og tilhørende årsager der relaterer til eksterne parter (f.eks. leverandører af sikkerhedsmæssige ydelser, beboelse beliggende tæt op ad spor). Ligesom farer, der er identificeret i gennemførte ændrings- eller etableringsprojekter, og som ikke kan lukkes i projektet, bør inkluderes i arbejdet med risikoprofilen.

Virksomheder, der udfører opgaver for infrastrukturforvaltere eller jernbanevirksomheder skal huske, at de aktiviteter, der skal identificeres farer for, for at opnå sikkerhedscertifikat, er dem der vedrører kørslen (herunder også uddannelse af førere samt vedligeholdelse af det rullende materiel).

Risici for hver fare skal kunne estimeres, således at det er muligt at prioritere indsatsen for hver fare.

Risici kan udregnes ved at estimere værdier for sandsynlighed og konsekvens, og multiplicere disse. Man kan også anvende simple matricer, hvor det med fastsatte kriterier – og uden matematik – kan vurderes om en risiko er acceptabel eller uacceptabel, og om der således skal opstilles barrierer.

For at få et fyldestgørende resultat og en for virksomheden dækkende risikoprofil er det god praksis at inddrage såvel fagspecialister som generalister på tværs af organisationen. Det anbefales at afholde workshops, der faciliteres af en person med kompetencer inden for workshops, facilitering og risikovurdering.

For yderligere vejledning til arbejdet med risikoprofilen henvises til den generelle vejleding til risikovurdering "Introduktion til risikovurdering", der kan findes på Trafik-, Bygge- og Boligstyrelsens hjemmeside.

Risikoprofilen skal udgøre et væsentligt fundament for virksomhedens arbejde med sikkerhed. Risikoprofilen skal kunne give overblikket over virksomhedens jernbanesikkerhedsmæssige risici og de barrierer, der er opstillet for at mindske disse. Risikoprofilen bør løbende konsulteres ved ændringer i risikobilledet, for at vurdere om det giver anledning til nye barrierer. Ligeledes bør risikoprofilen konsulteres ved svigt eller ændringer i barrierer, for at vurdere, om dette medfører et ændret risikobillede.

1.4. Sikkerhedsledelsessystem
1.4.1. For at håndtere alle identificerede farer og eksterne krav samt for at opretholde eller forbedre jernbanesikkerheden skal virksomheden etablere, implementere og vedligeholde et sikkerhedsledelsessystem i overensstemmelse med kravene i denne bekendtgørelse.
1.4.2. Systemet skal dokumenteres og struktureres, så det passer til den enkelte virksomhed.
1.4.3. Systemet kan være integreret med andre ledelsessystemer.

Formålet med et sikkerhedsledelsessystem er at:

- Skabe overblik over organisation og aktiviteter samt opretholde effektive risikostyringsforanstaltninger
- Fastlægge hvor virksomheden vil bevæge sig hen (politikker og mål) og formidle dette, således at alle arbejder i samme retning
- Dokumentere opgaver, ansvar og kompetencer i organisationen, således at det sikres, at alle kender deres ansvarsområder, og at alle har de fornødne kompetencer og beføjelser i forhold til det arbejde de skal udføre
- Dokumentere arbejdsgange, således at det sikres, at de enkelte medarbejdere kender disse
- Kontinuert/periodisk evaluere virksomhedens "tilstand", således at stærke og svage sider identificeres, så passende tiltag herefter kan iværksættes med henblik på at forbedre sikkerheden (/fortsætte arbejdet i den fastsatte retning)

Overordnet skal systemet således sikre:

- Opretholdelse af sikkerheden i den daglige drift (operationelle processer)
- Kontinuerlig forbedring af sikkerheden (ledelsesprocesser)

<u>Sikkerhedsledelsessystemets indhold og struktur</u>

For at opbygge et system, der passer til den enkelte virksomhed skal systemet både adressere relevante farer og være tilpasset virksomhedens størrelse.

Derfor skal systemet adressere de farer, som er identificeret i forbindelse med udarbejdelse af risikoprofilen, jf. krav 1.3. Mange af de barrierer, der skal opstilles for at mindske farerne, eller overvåge disse, vil netop være dokumenterede arbejdsgange i sikkerhedsledelsessystemet.

Sikkerhedsledelsessystemet skal endvidere indeholde de overvågningsprocesser, der skal etableres iht. til krav 6 og 7.

Et sikkerhedsledelsessystem bør være enkelt i sin struktur. Systemet bør struktureres med udgangspunkt i virksomhedens behov, dvs. efter virksomhedens aktiviteter / risikoprofil og ikke efter bekendtgørelsens krav.

I opbygningen af systemet bør der også tages hensyn til virksomhedens størrelse og kompleksitet. Det forventes ikke at små virksomheder, eller virksomheder med begrænset jernbanesikkerhedsmæssig aktivitet har store komplicerede systemer med

flowdiagrammer etc. Et system bestående af word-dokumenter organiseret i en mappestruktur kan være lige så velfungerende og effektivt som større IT-systemer.

Et sikkerhedsledelsessystem må gerne være papirbaseret, såfremt virksomheden finder dette hensigtsmæssigt. I visse tilfælde kan det også være hensigtsmæssigt at have dele af systemet papirbaseret, f.eks. arbejdsinstruktioner i et værksted. Papirbaserede systemer kan dog ofte være mere ressourcekrævende at administrere end elektroniske systemer.

Det væsentligste er, at systemet skal være naturligt at anvende – på lige fod med andre systemer, der anvendes i virksomheden.

Se endvidere mere detaljeret vejledning om sikkerhedsledelsessystemets dokumentation i krav 4.5.

Integration med andre ledelsessystemer

Det kan være hensigtsmæssigt at integrere sikkerhedsledelsessystemet med eventuelle andre ledelsessystemer, der anvendes i virksomheden, eller f.eks. have tilgang til dem fra samme platform eller indgangsbillede, såfremt systemet er elektronisk.

Nogle procedurer/processer, f.eks. afvigelseshåndtering og intern audit er generelle, og kan derfor også være fælles for systemerne.

2. Lederskab

2.1. Lederskab og forpligtelse

Virksomhedens øverste ledelse skal udvise lederskab og engagement ved at tage det overordnede ansvar for sikkerheden. Virksomhedens øverste ledelse skal

1) sikre, at sikkerhedsledelsessystemet er foreneligt med virksomhedens forretningsprocesser,
2) sikre, at sikkerhedsledelsessystemet er implementeret og fungerer efter hensigten,
3) sikre, at nødvendige ressourcer, herunder udstyr og kompetencer, der kræves ved implementeringen og anvendelsen af sikkerhedsledelsessystemet, er tilgængelige,
4) kommunikere værdier og beslutninger vedrørende sikkerhed til organisationen og
5) skabe en sikkerhedskultur i virksomheden, der understøtter løbende forbedringer af sikkerheden.

Med virksomhedens øverste ledelse menes ledere på direktionsniveau.

Hvis den øverste ledelse ikke giver udtryk for et kvalificeret, varigt engagement i sikkerhed som en af de vigtigste forretningsmæssige målsætninger, kan fokus på sikkerhed i driften let flytte sig mod andre forretningsmæssige målsætninger, navnlig i mindre modne organisationer.

Derfor skal ledelsen "gå forrest og vise vejen" i forhold til sikkerhedsledelse. Ledelsens engagement indebærer f.eks. at ledelsen sikrer:

- At sikkerhedsledelsessystemet er foreneligt med virksomhedens forretningsprocesser. Med forretningsprocesser menes de processer, som virksomheden har etableret for at drive sin forretning. Disse processer behøver ikke at være dokumenteret i et system, men sikkerhedsledelsesprocesserne må ikke stride mod disse processer. Et eksempel er, at ledelsen integrerer vurdering af sikkerhed i alle virksomhedens beslutninger, og ikke går på kompromis med sikkerheden ved forretningsmæssige beslutninger.
- At nødvendige ressourcer er til stede og prioriteringer foretages, således at sikkerhedsledelsessystemet bliver implementeret i organisationen, og at der sikres bevidsthed, forståelse og kultur blandt medarbejderne, i forhold til at anvende systemet som en naturlig del af hverdagen og løbende foretage forbedringer.

- At der etableres kommunikationsveje op og ned i organisationen, så det sikres at væsentlig information om sikkerhedsmæssige forhold tilgår ledelsen, således at den kan træffe de rette beslutninger. Ligeledes at information om sikkerhedsmæssige beslutninger tilgår de relevante medarbejdere, således at de kan handle i overensstemmelse hermed.

2.2. Sikkerhedspolitik

2.2.1. Virksomhedens øverste ledelse skal godkende, implementere og vedligeholde en dokumenteret sikkerhedspolitik og sikre, at sikkerhedspolitikken

1) er tilpasset virksomhedens drift og
2) fokuserer på at forbedre sikkerheden samt at overholde sikkerhedsledelsessystemet.

2.2.2. Sikkerhedspolitikken skal være kommunikeret til og forstået af hele organisationen og andre, der – på vegne af virksomheden – udfører arbejde, som kan påvirke sikkerheden.

Virksomhedens sikkerhedspolitik skal udtrykke den holdning virksomhedens ledelse vil forvalte jernbanesikkerheden efter. Sikkerhedspolitikken skal udtrykke ledelsens engagement, forpligtigelse og strategiske syn på jernbanesikkerhed.

Sikkerhedspolitikken kan også opridse de væsentligste overordnede principper og værdier, som organisationen og medarbejderne skal arbejde efter og på den måde vise ledelsens engagement i forhold til at forbedre sikkerheden og styrke sikkerhedskulturen.

Sikkerhedspolitikken kan med fordel være afledt af (eller integreret med) virksomhedens øvrige politikker samt mission og vision. Dette for at sikre, at sikkerhedsledelsen er en integreret del af virksomhedens samlede ledelsessystem (forretning).

Sikkerhedspolitikken skal formidles, således at den enkelte medarbejder forstår politikken, og hvad den betyder for ham/hende og hans/hendes egen rolle og bidrag i forbindelse med sikkerhedsledelsessystemet. Også eksterne som arbejder under virksomhedens sikkerhedsledelse, herunder indlejet personale, skal være bekendt med sikkerhedspolitikken. Dette kan evt. sikres via den kontrakt eller aftale, der indgås med den eksterne samarbejdspartner.

Politikken skal ikke "læres udenad" af medarbejderne, men skal "ligge i baghovedet", således at sikkerhedsbevidstheden styrkes, og alle arbejder efter de fælles værdier.

Der er ikke krav om, at virksomheden skal etablere en dokumenteret proces for udarbejdelse af sikkerhedspolitikken, men sikkerhedspolitikken skal evalueres mindst en gang årligt for at sikre, at den stadig er relevant og egnet for virksomheden (se krav 7.2).

2.3. Roller, ansvar og beføjelser i organisationen

2.3.1. Virksomhedens øverste ledelse skal sikre, at identificerede funktioner (jf. 4.1) bestrides af personale med de fornødne kompetencer og ressourcer.

2.3.2. Virksomhedens øverste ledelse skal sikre, at ansvar og beføjelser tildeles og kommunikeres til det personale, der bestrider en funktion i sikkerhedsledelsessystemet.

2.3.3. Virksomhedens øverste ledelse skal udpege en funktion, der har ansvar for og beføjelser til at:

1) sikre, at sikkerhedsledelsessystemet er i overensstemmelse med kravene i denne bekendtgørelse,
2) sikre koordinering af aktiviteterne i sikkerhedsledelsessystemet på tværs af organisationen og
3) rapportere om systemets effektivitet og egnethed til virksomhedens øverste ledelse.

Det er virksomhedens øverste ledelse, der har det overordnede ansvar for at sikre, at personalet har de fornødne kompetencer og ressourcer. Ansvar og tildelte beføjelser skal stå i forhold til de opgaver, der skal varetages.

Ledelsen skal endvidere sikre, at organisationen tilføres de ressourcer, der er nødvendige for gennemførelsen af alle sikkerhedsmæssige aktiviteter.

Det skal understreges, at uddelegering af ansvar og sikkerhedsmæssige opgaver ikke fritager organisationens øverste ledelse fra det overordnede ansvar og pligter i relation til jernbanesikkerheden.

Både for ledere og medarbejdere gælder, at ansvar og beføjelser skal være kommunikeret og forstået. Virksomheden skal sikre, at alle ved hvad de forventes at gøre (ansvar) og hvad de må tage beslutninger om (beføjelser), og at de forstår hvordan ansvar og beføjelser hænger sammen.

For at arbejdet med sikkerhedsledelsessystemet sikres tilstrækkelig fokus, er der krav om, at virksomhedens øverste ledelse skal udpege en funktion, der har ansvar for og fokus på arbejdet med sikkerhedsledelsessystemet. Typisk varetages denne funktion af en sikkerhedschef (tidligere har begrebet "Ledelsens Repræsentant" været brugt – og i praksis er intet ændret).

Funktionen skal tildeles de nødvendige beføjelser og ressourcer til løfte dette ansvar.

Funktionen bør være uafhængig i forhold til andre ansvarsområder, således at der ikke opstår interessekonflikter i forhold til udførelsen af det sikkerhedsmæssige hverv.

Se afsnit 4.1 vedr. kompetencekrav til denne funktion.

3. Planlægning

3.1. Håndtering af farer
3.1.1. Med udgangspunkt i risikoprofilen, skal virksomheden identificere og opstille barrierer til at håndtere de identificerede farer og årsagerne til disse.
3.1.2. Virksomheden skal sikre sporbarhed mellem identificerede barrierer, og de farer og årsager de håndterer.

For alle farer, som jf. risikoprofilen er identificeret, og som virksomheden har vurderet ikke at være acceptable, skal virksomheden opstille barrierer.

En "barriere" er her en betegnelse for de forskellige risikoreducerende tiltag som groft kan grupperes i følgende:

- Tekniske / fysiske barrierer, der forhindrer/begrænser farlige situationer ved fysiske eller tekniske løsninger (som hegn, bomme, togkontrolsystemer etc.)
- Processer, arbejdsgange, regler mv. i virksomheden, der sikrer, at personalet foretager de korrekte dispositioner ved at følge disse
- Organisatoriske barrierer, i form af organisering og kompetencer hos personale, der sikrer korrekt vurdering, valg og udførelse at sikkerhedsmæssige aktiviteter

Der kan opstilles flere barrierer for hver fare. Det drejer sig primært om at eliminere alle årsagerne til en fare, således at faren nedbringes til et for virksomheden acceptabelt niveau.

Barrierer kan både opstilles for at forhindre en fare i at opstå, men også for at begrænse den i at udvikle sig, såfremt den alligevel skulle opstå. Yderligere information om at opstille barrierer kan findes i vejledningen "Introduktion til risikovurdering" på Trafik-, Bygge- og Boligstyrelsens hjemmeside.

Såfremt en risiko ikke kan nedbringes til at acceptabelt eller ønsket niveau, f.eks. hvis barriererne ikke anses som tilstrækkeligt stærke (tekniske barrierer anses normalt som værende stærkere end barrierer, der består af instruktion eller uddannelse), kan barriererne suppleres med overvågning, f.eks. ved at gennemføre inspektioner af medarbejdernes kendskab til og efterlevelse af regler, og at de til stadighed har opdateret viden.

Overvågningen er altså ikke en barriere i sig selv, men et middel til at sikre, at barrieren ikke svigter. For yderligere omkring overvågning, se krav 6.

Sporbarhed

Virksomheden skal sikre, at der er sporbarhed fra hver fare til hver barriere, der er opstillet for faren eller dens årsager. Ligeledes skal der være sporbarhed fra hver barriere til den fare / de farer, den er opstillet for.

Disse referencer kan med fordel synliggøres ved angivelse i risikoprofilen, så denne, udover at være en oversigt over farerne ved virksomhedens aktiviteter, også bliver en oversigt over samtlige barrierer, og de farer (og årsager til farer) de er opstillet for.

Ved at synliggøre disse sammenhænge, kan virksomheden lettere vurdere konsekvensen af ændringer i risikobilledet. F.eks. hvis der ændres i en barriere, kan der hurtigt etableres et overblik over hvilke farer, dette kan få indflydelse på. Ligeledes, hvis risikoen for en fare vurderes ændret, kan der etableres et overblik over, hvilke barrierer der allerede er opstillet.

3.2. Sikkerhedsmål og handlingsplaner

3.2.1. Med afsæt i sikkerhedspolitikken og med udgangspunkt i risikoprofilen, resultaterne af overvågningen jf. 6 og konklusionen fra evalueringen jf. 7.2 skal virksomhedens øverste ledelse fastlægge relevante kvantitative og kvalitative mål for fastholdelse eller forbedring af sikkerheden.

3.2.2. For hvert opstillet mål skal defineres kriterier for, hvornår målet er opfyldt.

3.2.3. For hvert opstillet mål skal udarbejdes handlingsplaner for opfyldelse af målet.

3.2.4. Sikkerhedsmål og tilhørende handlingsplaner skal kommunikeres til de medarbejdere, som skal bidrage til målopfyldelsen.

3.2.5. Virksomheden skal følge op på gennemførelse af handlingsplanerne.

3.2.6. Sikkerhedsledelsessystemet skal sikre, at mål, handlingsplaner og løbende opdatering dokumenteres.

Formålet med at opstille mål er at opnå forbedringer. Et mål skal udtrykke, hvor ledelsen ønsker, at virksomheden skal hen.

Mål skal således opstilles på områder, hvor virksomheden ønsker at forbedre sig, eller hvor overvågningen viser at præstationen bør kunne forbedres. Det kan være hvor en aktivitet indebærer store risici, jf. risikoprofilen, eller hvor evaluering af målinger / trends viser, at sikkerhedsniveauet går den forkerte vej.

Mål er et styrende værktøj, og virksomhedens ledelse skal være bevidst om, hvorfor netop de pågældende mål er opstillet.

Mål contra sikkerhedsindikatorer

Sikkerhedsindikatorer er ikke det samme som sikkerhedsmål.

Sikkerhedsindikatorer er "blot" værdier, der kontinuert overvåges for at følge udviklingen i sikkerhedsniveauet. Ledelsen vælger, hvilke sikkerhedsindikatorer, virksomheden skal overvåges. Det anbefales f.eks. at overvåge dem, som via risikoprofilen er vurderet til at udgøre en særlig risiko, eller dem der ikke kan nedbringes til et acceptabelt niveau (se også krav 1.3 og krav 6).

Eksempler på sikkerhedsindikatorer kan findes under krav 6.3.

Hvis en indikator omhandler et særligt risikofyldt emne; hvis den viser en negativ trend, eller hvis ledelsen ønsker at forbedre det acceptable niveau for indikatoren, kan denne gøres til et sikkerhedsmål.

Opstilling af sikkerhedsmål

Virksomheden skal opstille og dokumentere kvantitative og kvalitative mål. For alle mål skal virksomheden opstille kriterier for, hvornår målet er opfyldt, således at det kan måles, om målet er nået.

Det er virksomhedens ledelse, der beslutter målene. Målene skal være realistiske og harmonere med virksomhedens sikkerhedspolitik, således at virksomheden ikke arbejder i "forskellige retninger" mht. sikkerheden.

Kvantitative mål er mål, der direkte kan måles, faktuelle værdier, som f.eks. "reduktion af antal signalforbikørsler af en bestemt type med 10 %" eller "10 % reduktion af antallet af hændelser som følge af løse stropper pr. mio. tog km."

Kvalitative mål er mål, der baserer sig på en subjektiv vurdering, som f.eks. "kompetenceudvikling af personalegruppe vedr. konkret emne, svarende til 8 på en skala fra 1 til 10".

Virksomheden skal være opmærksom på forskellen mellem et mål og en handling. Det er som udgangspunkt ikke et sikkerhedsmål at gennemføre nogle bestemte handlinger, som f.eks. et antal tilsyn. Handlingerne er ikke målet i sig selv, men bidrager til at opnå et andet mål om forbedret sikkerhed.

Opstilling af handlingsplaner

For hvert mål skal der opstilles en (eller flere) handlingsplan(er) for opnåelse af målet. Det er vigtigt at en handlingsplan konkret specificerer følgende:

- Formålet med handlingsplanen (hvilket mål skal opnås)
- Planlagte aktiviteter for opnåelse af målet
- Anførelse af ansvaret for gennemførelsen af hver aktivitet i handlingsplanen
- Tidsplan for gennemførelse af aktiviteterne

Handlingsplanerne skal kommunikeres til de medarbejdere, der skal gennemføre aktiviteter beskrevet i handlingsplanerne.

Tidspunkt for fastsættelse af sikkerhedsmål og handlingsplaner

Mål og tilhørende handlingsplaner fastsættes som udgangspunkt én gang årligt ved ledelsens evaluering.

Løbende opfølgning på mål og handlingsplaner

Se krav 6.2.

Proces for mål og handlingsplaner

Virksomheden bør i sit sikkerhedsledelsessystem beskrive proces og ansvar for arbejdet med sikkerhedsmål og handlingsplaner, inkl. opfølgning på disse. Det skal ligeledes her fastsættes, hvorledes mål, handlingsplaner og den foretagne opfølgning skal dokumenteres.

Denne beskrivelse kan være en del af processen for ledelsens evaluering.

4. Støtteaktiviteter og -funktioner

4.1. Organisering
4.1.1. Virksomheden skal identificere alle funktioner, der udfører aktiviteter i forbindelse med den del af driften, som sikkerhedscertifikatet eller sikkerhedsgodkendelsen omfatter, jf. 1.1, samt funktioner, der udfører aktiviteter i forbindelse med etablering, implementering, overvågning, evaluering og forbedring af sikkerhedsledelsessystemet. 4.1.2. Sikkerhedsledelsessystemet skal indeholde beskrivelser af ansvar, beføjelser og kompetencekrav for alle identificerede funktioner.

Identifikation af funktioner / roller

Virksomheden skal på baggrund af den udarbejdede risikoprofil fastlægge de organisatoriske barrierer, dvs. den organisation, der kan "løfte opgaven".

Organisationen kan beskrives ved at identificere og beskrive de funktioner / roller:

1. Der har ansvaret for - eller udfører de sikkerhedsmæssige aktiviteter, som sikkerhedscertifikatet eller -godkendelsen omfatter.

Dette drejer sig f.eks. om de funktioner, der har ansvaret for, eller gennemfører de processer, der er opstillet i sikkerhedsledelsessystemet som barrierer.

2. Der udfører aktiviteter i forbindelse med etablering og implementering af sikkerhedsledelsessystemet.

   Dette drejer sig om de funktioner, der arbejder med selve systemet, definerer hvorledes systemet skal opbygges, skriver processer og instruktioner, vedligeholder systemet, uddanner medarbejderne i systemet etc.

3. Der udfører aktiviteter i forbindelse med overvågning, evaluering og forbedring af sikkerhedsledelsessystemet.

   Dette drejer sig f.eks. om de funktioner, der overvåger og evaluerer systemet ved intern audit, inspektioner samt de funktioner der overvåger målopfyldelse og gennemfører ledelsens evaluering.

En funktion kan bestrides af flere personer.

Eksempler på funktioner kan være den:

- Der har det overordnede og totale ansvar for jernbanesikkerheden i virksomheden
- Der har ansvaret for sikkerhedsledelsessystemet samt funktioner, der er direkte involveret i arbejdet omkring sikkerhedsledelsessystemet
- Der har det overordnede ansvar for at virksomheden følger gældende lovgivning og virksomhedsregler indeholdende jernbanesikkerhed
- Der udfører intern audit
- Der udfører operationelle inspektioner
- Der undersøger og følger op på sikkerhedsmæssige hændelser
- Der udfører sikkerhedsklassificeret arbejde
- Der har personaleansvar for medarbejdere, der bestrider en funktion i sikkerhedsledelsessystemet
- Der sikrer, at virksomheden har nødvendige og fyldestgørende regler vedrørende jernbanesikkerhed
- Der har ansvar for at køretøjer og/eller infrastruktur er godkendt og at det vedligeholdes efter forskrifterne
- Der udfører vedligeholdelsesarbejde, som kan have indflydelse på jernbanesikkerheden
- Der frigiver køretøjer eller infrastruktur til drift
- Der gennemfører signifikans- og risikovurderinger
- Der indgår aftaler med sikkerhedsmæssigt indhold
- Der uddanner driftspersonale

<u>Beskrivelse af funktioner / roller</u>

Form

Der er ingen formkrav til en funktions- eller rollebeskrivelse. I det følgende benyttes ordet ”funktion”, idet begreberne dækker det samme.

Funktioner vil typisk kunne beskrives i funktionsbeskrivelser. Afhængig af virksomhedens størrelse kan det være et samlet dokument, eller et dokument pr. funktion.

Nogle virksomheder anvender skemaer (krydsmatricer), hvor det anføres hvilke beføjelser eller kompetencer (jf. nedenfor), der er krævet for en given aktivitet / opgave. (F.eks. at der i værkstedet kræves svejsecertifikat for at udføre svejseopgaver). I dette tilfælde er kompetencekravene knyttet direkte til opgaven.

Indhold

Beskrivelsen af hver funktion bør tage udgangspunkt i de opgaver funktionen skal udføre, og ikke i den person, som evt. bestrider funktionen.

For hver funktion skal som minimum defineres og beskrives:

- Den pågældende funktions ansvarsområder
- Funktionens beføjelser i relation til sikkerhedsarbejdet
- Kompetencekrav til den medarbejder / de medarbejdere, der skal bestride funktionen

For hver funktion bør der endvidere i beskrivelsen være sporbarhed (f.eks. henvisning) til de aktiviteter / opgaver som er beskrevet i sikkerhedsledelsessystemets dokumentation, og som den pågældende funktion har ansvaret for.

Særligt om kompetencekrav

For at virksomhedens personale kan gennemføre aktiviteterne / opgaverne på den korrekte og sikre måde, er det vigtigt, at virksomheden gør sig klart hvilke kompetencer, der er nødvendige for at udføre en given opgave / aktivitet, jf. ovenfor.

Alle de kompetencer, som er nødvendige i forhold til de opgaver / aktiviteter, som funktionen skal kunne udføre, er relevante i kompetencebeskrivelsen. Dette kan både være faglige kompetencer, som kendskab til regler, materiel eller infrastruktur og kompetencer vedrørende ledelsessystemer, som f.eks. intern audit eller årsagsanalyse.

Kompetence kan angives ved uddannelseskrav, eller ved erfaring inden for et givet område. Kompetencekrav bør beskrives så præcist som muligt. (Hvad skal de enkelte kunne?) Således vil det være lettere at vurdere, om kompetencekravet er opfyldt (se krav 4.2).

Kompetencekrav kan også gradueres ved en skala. Et eksempel er 4-trinsskalaen: Kende, kunne, beherske og mestre. Det er blot vigtigt, at virksomheden definerer de enkelte niveauer i skalaen, inden den tages i brug.

Krav til kompetencer i.f.m. arbejdet med sikkerhedsledelsessystemet (jf. punkt 2.3)

Det vurderes som afgørende for at kunne sikre et velfungerende sikkerhedsledelsessystem, at organisationen råder over kompetence, der har et indgående kendskab til ledelsessystemer. Det anbefales derfor, at den eller de personer, der varetager arbejdet med sikkerhedsledelsessystemet, har en uddannelse i og erfaring med udvikling og vedligeholdelse af ledelsessystemer. Det vil normalt ikke være tilstrækkeligt kun at have erfaring som bruger af ledelsessystemer (uanset om dette suppleres med en uddannelse som lead auditor).

Det vil yderligere være væsentligt at have evner til at kommunikere og formidle, og besidde en gennemslagskraft således, at ledelsessystemet kan udbredes og implementeres i virksomheden på en hensigtsmæssig måde.

Principperne i ledelsessystemer er ens, således at erfaring med f.eks. kvalitets-, miljø- eller arbejdsmiljøledelsessystemer i vid udstrækning vil kunne kvalificere til at arbejde med sikkerhedsledelsessystemer.

4.2. Sikring af kompetencer

4.2.1. Sikkerhedsledelsessystemet skal sikre, at relevant behov for uddannelse og træning bliver identificeret, samt at uddannelsen hhv. træningen gennemføres, således at medarbejderne opnår de kompetencer, der er krævede for udførelsen af deres funktioner, jf. 4.1.

4.2.2. Virksomheden skal sikre specifik uddannelse i sikkerhedsledelsessystemet til alt personale, der har indflydelse på sikkerhedsledelsessystemets indhold og funktionalitet.

4.2.3. Opnåelse af krævede kompetencer skal dokumenteres.

4.2.4. 4.2.1 – 4.2.3 gælder såvel egne, som indlejede medarbejdere.

Virksomheden skal gennem processer / systemer i sikkerhedsledelsessystemet sikre, at de kompetencekrav, der er identificeret i forbindelse med organiseringen af sikkerhedsarbejdet, jf. krav 4.1 ovenfor bliver opfyldt, således at personalet er kvalificeret til at udføre aktiviteterne.

Virksomheden skal i sikkerhedsledelsessystemet fastlægge processer, der sikrer, at

- Kompetenceniveauet for alle medarbejdere, der skal bestride de pågældende funktioner bliver vurderet, og eventuelt manglende kompetence (kompetencegab) bliver identificeret.

  Dette skal både ske som indledende vurdering ved nye aktiviteter, nye medarbejdere, medarbejderrotation eller lignende samt løbende, f.eks. ved årlige personalesamtaler eller periodisk efteruddannelse og kontrol (f.eks. i forbindelse med sikkerhedsklassificeret arbejde).

- Medarbejderne opnår den kompetence, der er krævet enten ved eksterne kurser, interne kurser, sidemandsoplæring eller tilsvarende.

  Dette ved såvel indledende oplæring som ved løbende vedligeholdelse af kompetencer.

Indlejet personale

Virksomheden skal sikre, at kompetencekrav vurderes og opfyldes løbende både for eget personale og for eventuelt indlejet personale.

Ved indlejet personale forstås personale, der ikke er ansat af virksomheden, men er indlejet således, at personalet arbejder direkte under virksomhedens ledelsesansvar på lige fod med virksomhedens eget personale. Kravet er således, at kompetencer for indlejet personale styres på samme måde, som for virksomhedens egne medarbejderes kompetencer.

Specifikt vedr. kompetencer i sikkerhedsledelsessystemet

Virksomheden skal ligeledes sikre specifik uddannelse i sikkerhedsledelsessystemet til alt personale, der har indflydelse på sikkerhedsledelsessystemets indhold og funktionalitet og udfører opgaver direkte i forbindelse hermed.

Dette krav er ikke møntet på brugerne af systemet, men på dem der udvikler og vedligeholder systemets dokumentation og evt. IT-platform.

Myndighedsgodkendelse af uddannelse

Virksomheden skal sikre, at uddannelser, der skal godkendes af myndigheder, fremsendes til disse i henhold til gældende lovkrav.

Det anbefales at fremsende materialet i god tid inden uddannelsen skal påbegyndes, både for at sikre tid til sagsbehandling og for at sikre, at eventuelle kommentarer fra myndigheden kan indarbejdes i uddannelsesmaterialet.

Virksomheden skal ligeledes være opmærksom på de specifikke krav omkring uddannelse af lokomotivførere, f.eks. om godkendelse som uddannelsescenter.

Dokumentation af kompetencer

Virksomheden skal opbevare dokumentation for de kompetencer virksomhedens medarbejdere, inkl. indlejet personale har opnået. Virksomheden skal kunne dokumentere, at de medarbejdere, der bestrider en given funktion, har de kvalifikationer, der kræves jf. krav 4.1 ovenfor.

Dette kan være:

- Uddannelsesbeviser
- Certifikater
- Godkendelser (herunder helbredsgodkendelser)
- Dokumenterede udtalelser eller vurderinger (f.eks. i forbindelse med medarbejderudviklingssamtaler)

Det bemærkes, at et CV ikke alene kan betragtes som dokumentation for opnået kompetence.

Skriftlige udtalelser eller vurderinger kan være en måde at dokumentere, at en kompetence er opfyldt, hvor dette ikke kan gøres ved uddannelsesbeviser eller tilsvarende. Således beskriver og kvitterer f.eks. medarbejderens chef for, at det er vurderet, at medarbejderen har de krævede kompetencer (f.eks. på baggrund af erfaring) i forhold til den funktion, der skal bestrides.

Såfremt det er vurderet, at et kompetencekrav ikke er opfyldt, skal virksomheden kunne dokumentere, at der er planlagt aktiviteter for, at medarbejderen skal opnå den manglende kompetence inden de givne opgaver udføres på eget ansvar. Dette kan f.eks. gøres ved dokumenterede uddannelsesplaner, dokumentation for tilmelding til kurser eller dokumentation for planlagt sidemandsoplæring (det kan være en mail eller booking i kalendersystemet).

4.3. Bevidsthed

4.3.1. Virksomheden skal sikre, at medarbejdere, der udfører arbejde med betydning for sikkerheden, anerkender og forstår alle relevante dokumenter og systemer til udførelse af deres arbejde.

4.3.2. Virksomheden skal sikre, at medarbejderne er bevidste om deres indflydelse på sikkerheden og den sikkerhedsmæssige konsekvens af ikke at udføre arbejdet i overensstemmelse med sikkerhedsledelsessystemet.

Bevidsthed handler om, at medarbejderne, udover at følge systemet, også forstår og anerkender hvorfor de gør det. Det drejer sig således ikke kun om, at systemet er implementeret. Bevidsthed går længere end dette.

Beslægtet hermed er systemforståelse. Systemforståelse medfører, at systemet anvendes helt naturligt, fordi medarbejderne forstår, at det er måden at gøre tingene på, og at det selvfølgelig er systemet, der er rygraden i arbejdet. Således anvendes ikke skuffesystemer og hjemmelavede processer, som ikke er en del af det samlede system.

Det er ligeledes vigtigt, at medarbejderne forstår, hvilken indflydelse de har på sikkerheden både i positiv og negativ retning.

Bevidsthed vil typisk komme fra ledelsen og have afsmitning ned gennem organisationen.

Bevidsthed måles ikke nødvendigvis på en skala, men ofte kan det fornemmes om den er til stede. Det forventes således ikke, at virksomhederne "sætter hak" ud for "bevidsthed" på en tjekliste, men det kan f.eks. indgå som en parameter, der vurderes ved intern audit eller medarbejderudviklingssamtaler.

4.4. Kommunikation

4.4.1. Virksomheden skal sikre, at nødvendig sikkerhedsrelevant kommunikation fra og til interne og eksterne parter identificeres, registreres og behandles.

4.4.2. Relevant kommunikation skal dokumenteres.

Et af de afgørende forhold for at opretholde et højt sikkerhedsniveau er, at der foregår en effektiv kommunikation mellem alle relevante parter.

Kommunikation findes i alle virksomhedens arbejdsprocesser, og dette krav skal ikke tolkes som at virksomheden skal udarbejde en specifik proces for kommunikation, men at den kommunikation, der foregår, skal identificeres og indarbejdes i de forskellige processer, som virksomheden anvender, jf. nedenfor.

<u>Intern kommunikation</u>

Dette gælder f.eks. intern kommunikation mellem medarbejdere på samme niveau, kommunikation af ledelsesbeslutninger mv. "ned" i organisationen eller kommunikation fra organisationen til ledelsen. Eksempler er:

- Kommunikation i forbindelse med ændringer i sikkerhedsledelsessystemet, herunder både høring af relevante medarbejdere og uddannelse af personale efter ændringer
- Kommunikation i en driftssituation om sikkerhedsmæssige forhold ved lokomotivførerskift
- Klarmelding af køretøjer eller infrastruktur efter vedligeholdelse

- Rapportering af hændelser
- Beslutninger, politikker, mål og processer/procedurer mv. fra ledelsen
- Information til ledelsen som beslutningsgrundlag i forbindelse med f.eks. ledelsens evaluering
- Den kommunikation, der finder sted mellem de forskellige funktioner, der arbejder sammen i de processer / aktiviteter, der foregår i virksomheden

Denne kommunikation bør være en implicit del af processerne for de enkelte aktiviteter. F.eks. indeholder processen for håndtering af hændelser en beskrivelse af den kommunikation og det informationsflow, der skal foregå ved indmelding og håndtering af en ulykke.

Processerne skal således også sikre, at information er relevant og gyldig, at informationen er tilgængelig for personalet, og at personalet er bekendt med informationen, inden den skal anvendes.

Andre typer af kommunikation kan mere hensigtsmæssigt dokumenteres ved beskrivelser af mødestrukturer (frekvens, ansvarlig, formål, dagsorden, referater mm.)

Ekstern kommunikation

Kommunikation med eksterne parter er af lige så stor betydning som intern kommunikation. Eksempler på ekstern kommunikation er:

- Kommunikation mellem jernbanevirksomhed mv. og jernbaneinfrastrukturforvalter i forbindelse med trafikstyring, f.eks. information om hastighedsnedsættelse
- Kommunikation mellem jernbanevirksomhed mv. og infrastrukturforvalter i forbindelse med ulykker
- Kommunikation mellem to jernbanevirksomheder i forbindelse med overdragelse af jernbanevogne (gods- eller passagervogne)
- Kommunikation mellem infrastrukturforvaltere om overkørsler
- Kommunikation mellem virksomhed og leverandører af sikkerhedsmæssige ydelser
- Kommunikation med myndigheder
- Kommunikation med eksterne parter, som f.eks. kommuner i forbindelse med udvikling af byområder eller ny jernbaneinfrastruktur

Virksomheden bør sikre, at den eksterne kommunikation, der skal foregå, er fastlagt i regler eller aftaler, og det bør sikres at det relevante personale har adgang til og er bekendt med disse.

Dokumentation af kommunikation

De udarbejdede processer, jf. ovenfor, skal indeholde krav til hvorledes og hvor gennemført kommunikation skal dokumenteres.

Hvor der ikke eksplicit stilles krav om det i regler og lovgivning, er det virksomheden selv, der vurderer hvilken kommunikation, der skal dokumenteres.

Kommunikation kan f.eks. dokumenteres i form af arkiverede mails, mødereferater, båndede samtaler, udfyldte skemaer, der evt. er kvitteret af de kommunikerende parter mv.

4.5. Sikkerhedsledelsessystemets dokumentation
4.5.1. Sikkerhedsledelsessystemet skal indeholde beskrivelser, der fastlægger, 1) hvordan sikkerhedsledelsessystemet er opbygget og dokumenteret, herunder hvilke dokumenttyper, der indgår, 2) hvordan de enkelte dokumenter i sikkerhedsledelsessystemet entydigt identificeres,

3) hvordan ansvaret for de enkelte dokumenter i sikkerhedsledelsessystemet entydigt identificeres,

4) hvordan det sikres, at dokumenter i sikkerhedsledelsessystemet til hver en tid er fyldestgørende, korrekte og godkendte,

5) hvordan dokumenter i sikkerhedsledelsessystemet udarbejdes/ændres, granskes, godkendes og publiceres, og

6) hvordan dokumenter, der ikke længere er gyldige i sikkerhedsledelsessystemet, håndteres.

4.5.2. Sikkerhedsledelsessystemet skal sikre, at relevante funktioner bliver hørt på passende vis i forbindelse med fastlæggelse og ændring af processer, som måtte vedrøre dem.

4.5.3. Relevante dele af sikkerhedsledelsessystemet skal til hver en tid være tilgængelige for alle medarbejdere, der udfører aktiviteter i forbindelse med den del af driften, som sikkerhedscertifikatet eller sikkerhedsgodkendelsen omfatter.

4.5.4. Processer og/eller systemer i sikkerhedsledelsessystemet skal sikre arkivering og relevant sporbarhed af dokumentation genereret ved anvendelsen af sikkerhedsledelsessystemet. Formater og periode for arkivering skal specificeres i sikkerhedsledelsessystemet.

Dette krav handler som udgangspunkt om, at virksomheden skal beskrive, hvordan dens sikkerhedsledelsessystem er opbygget, hvilke dokumenter der indgår, og hvorledes dokumenterne styres mv.

Dokumenter i sikkerhedsledelsessystemet

Et sikkerhedsledelsessystem kan indeholde flere forskellige typer af dokumenter:

- Dokumenter, der fastsætter de overordnede rammer, f.eks. sikkerhedspolitik og risikoprofil.
- Dokumenter, der beskriver aktivitetsforløb i virksomheden, dvs. hvem gør hvad og i hvilken rækkefølge – herunder informations-/kommunikationsflowet, samt hvad der skal dokumenteres. Disse dokumenter skal illustrere aktiviteter, sammenhænge og ansvarsskift og skal sikre en fælles forståelse af arbejdsgangen, så alle kender deres roller og ved hvad de skal gøre.
- Dokumenter med detaljeret information, som f.eks. arbejdsinstruktioner, skemaer, regler og de dokumenter, der specificerer beføjelser og kompetencekrav.

Der er ikke krav om, at forskellige dokumenttyper kaldes noget bestemt. Virksomheden vælger f.eks. selv om dokumenter kaldes processer eller procedurer eller noget helt tredje.

Der er heller ikke krav om bestemte formater. Virksomheden vælger selv om den vil anvende flowdiagrammer, tekstbeskrivelser, skematiske opstillinger, elektroniske eller papirbaserede systemer, jf. også krav 1.4.

Det anbefales at anvende så korte og klare tekster som muligt.

Det væsentligste er, at der vælges et system, der er hensigtsmæssigt for virksomheden at anvende.

Dokumentstyring

Virksomheden skal fastsætte rammer for og beskrivelser af hvorledes alle typer af dokumenter styres og arkiveres.

Dokumenter i sikkerhedsledelsessystemet skal dokumentstyres, således at det sikres, at indholdet er korrekt og fyldestgørende og således, at det altid er muligt at se, hvilken version, der er den gældende.

Et dokument skal være entydigt identificeret, og dato samt ansvarlig for dokumentet skal være anført på dokumentet eller skal kunne henføres direkte fra dokumentet.

Virksomheden skal udarbejde en beskrivelse, der fastlægger:

- Sikkerhedsledelsessystemets struktur / opbygning, herunder de forskellige dokumenttyper (/niveauer hvis relevant) der arbejdes med (f.eks. processer eller procedurer og instruktioner)

- Ansvaret for de enkelte dokumenter (processer, instruktioner mv.)
- Formater og indhold af de forskellige dokumenttyper, herunder:
    - Dokumentdata i dokumenthovede eller dokumentfod (eller via 1:1 reference i IT-system):
        - Titel (som er sigende for formål/indhold)
        - Unik dokumentidentitet, f.eks. dokumentnummer (syntaks skal defineres, f.eks. "SLS 12.05" eller lignende)
        - Dato for udgivelse og evt. versionsnummer
        - Forfatter (typisk fagansvarlig)
        - Evt. gransker (fagligt input eller input fra sikkerhedsledelse)
        - Godkender (typisk chef/ansvarlig for ressourcer)
    - Indhold af den pågældende dokumenttype (eksempler):
        - Formål
        - Gyldighedsområde (hvor og hvornår skal dokumentet anvendes)
        - Proces-/instruktionstrin m. ansvar hvis relevant. Det anbefales, at teksten er kort og præcis, gerne skemaer, tjeklister eller flowdiagrammer.
        - Input (hvad initierer proceduren)
        - Output (hvad er resultatet af proceduren)
        - Links til andre dokumenter og systemer, indsat hvor relevant (f.eks. instruktioner, skabeloner, databaser etc.)
        - Registrering og arkivering (hvilke data genereres evt. og hvor, og hvor længe arkiveres disse)
    - Format og indhold kan opsættes i en skabelon, som der kan arbejdes ud fra
- Arbejdsgang for udarbejdelse og ændring af dokumenterne i sikkerhedsledelsessystemet:
    - Udarbejde / revidere dokument (herunder bør der opstilles krav til dem, der må udarbejde)
    - Granske dokument / høring (herunder bør der opstilles krav til dem, der må granske)
    - Evt. revidere dokument
    - Godkende dokument (herunder bør der opstilles krav til dem, der må godkende, f.eks. at det er en afdelingsansvarlig)
    - Publicere dokument i sikkerhedsledelsessystemet
    - Implementere dokumentet i organisationen (Dette bør være den ansvarlige for dokumentets ansvar)
    - Håndtering af dokumenter, der ikke længere er gyldige

Beskrivelsen skal sikre, at relevante medarbejdere bliver involveret på passende vis under udarbejdelsen af dokumenterne, og feedback fra høringer skal opbevares.

Det anbefales, at den relevante fagchef/afdelingsansvarlige godkender processer / instruktioner, for at sikre ejerskab af disse. Godkendelse af et dokument skal kunne dokumenteres. Dette kan f.eks. gøres via et IT-system, der dokumenterer det eller ved at godkenderen har sendt en mail om dette, som arkiveres.

Hvor dette ikke er sikkerhedschefen, bør denne (eller tilsvarende) være gransker for at sikre, at der bliver taget højde for sikkerhedsmæssige aspekter og systemmæssige krav ved processen / instruktionen.

Det bør være den enkelte fagchef, der sikrer at relevante processer implementeres i den pågældendes del af organisationen. Såfremt det drejer sig om mere generelle processer, hvor sikkerhedschefen har godkendt dokumentet, kan implementering ske i samarbejde mellem fagchefen og sikkerhedschefen.

Det anbefales at have et system, hvor det er muligt at se hvilke ændringer der er foretaget i dokumentet siden seneste revision, evt. ved en ændringslog, hvor væsentlige ændringer og årsag til ændringen anføres. Dette for at sikre sporbarhed mellem ændring og beslutningsgrundlag.

Virksomheden skal sikre, at der kun er ét gældende system. Såfremt der, af en eller anden årsag, skal produceres dubletter, skal det tydeligt angives på disse, at de er kopier eller lignende.

Såfremt virksomheden anvender et papirbaseret system (enten helt eller delvist) skal virksomheden endvidere udarbejde procedurer, for at sikre distribution af nyeste versioner herunder kontrol af, at gamle versioner fjernes.

Tilgængelighed

Sikkerhedsledelsessystemet skal altid være tilgængeligt for det personale, der skal anvende det. Dette gælder både for virksomhedens egne medarbejdere såvel som indlejede medarbejdere. Det skal sikres, at alle relevante medarbejdere ved, hvor det gældende system kan findes.

Dette betyder ikke, at rutinerede medarbejdere altid skal læse i systemet før en given opgave udføres. Men medarbejderne skal altid have mulighed for at søge information i systemet, enten direkte eller evt. via telefonopkald til lederen eller andre kollegaer.

Endvidere skal blanketter og lignende, der skal anvendes til arbejdet, altid være tilgængelige for de pågældende medarbejdere i den form, de skal anvendes (f.eks. papir eller elektronisk).

Hvis det vurderes relevant og hensigtsmæssigt, skal eksterne parter, som skal arbejde iht. virksomhedens sikkerhedsledelsessystem også have adgang til dette. Alternativt kan processer mv. beskrives i den aftale, der indgås med den eksterne part.

Arkivering og styring af dokumentation genereret ved anvendelse af sikkerhedsledelsessystemet

Den dokumentation, der genereres ved anvendelse af sikkerhedsledelsessystemet kan i princippet registreres / arkiveres på mange måder, og det er ikke nødvendigvis hensigtsmæssigt, at forskellige typer af dokumentation håndteres ens.

Noget dokumentation skal blot arkiveres for at bevares, mens anden dokumentation skal registreres for at blive anvendt i et videre forløb eller i en anden proces. Nogle registreringer er statiske, f.eks. mødereferater, mens andre registreringer er dynamiske og skal løbende vedligeholdes, som f.eks. registreringer om en medarbejders kompetencer.

Det anbefales, at der ikke udarbejdes deciderede arbejdsgange for registrering / arkivering alene. Hvorledes data håndteres, anvendes og arkiveres bør derimod være en implicit del af processerne for de enkelte aktiviteter. F.eks. skal processen om hændelser / ulykker indeholde en beskrivelse af hvilke data, der skal rapporteres, i hvilket system disse data skal registreres og hvad registreringerne skal bruges til.

Processerne og registreringssystemerne skal også sikre, at data altid er korrekte og gyldige, at data er tilgængelige for relevant personale, og at personale er bekendt med data, inden de evt. skal anvendes.

Hvor regler og lovgivning ikke eksplicit stiller krav om arkiveringsperiode, skal virksomheden selv vurdere og beskrive, hvor længe data bør opbevares.

5. Godkendelse og drift

5.1. Godkendelse af infrastruktur og køretøjer
5.1.1. Sikkerhedsledelsessystemet skal sikre, at de forskellige typer køretøjer, der anvendes til driften, og infrastruktur, som virksomheden er ansvarlig for, overholder relevante krav og normer og er behørigt godkendt.
5.1.2. Sikkerhedsledelsessystemet skal sikre, at køretøjer overholder driftsmæssige begrænsninger og netspecifikke krav.

5.1.3. Virksomheden skal opbevare dokumentation for, at infrastruktur og køretøjer er godkendt.

Alle køretøjer, der anvendes til driften, eller til vedligeholdelse af infrastruktur skal være godkendt og opfylde relevante gældende krav. Kravet gælder for alle køretøjer, således også for lejede og lånte køretøjer eller køretøjer, der på anden måde er stillet til rådighed for den, som har ansvaret for kørslen.

Ligeledes skal den forvaltede infrastruktur være godkendt. Det er den infrastrukturforvalter, der har ansvaret for den specifikke infrastruktur, som skal sikre dette.

Sikkerhedsledelsessystemet skal indeholde dokumenterede processer eller tilsvarende, der sikrer:

- Ansøgning til myndigheder om opnåelse af godkendelser / ibrugtagningstilladelser
- Overholdelse af evt. midlertidige godkendelser eller betingelser/vilkår i ibrugtagningstilladelser
- Sikring af, at køretøjer udelukkende benyttes på infrastruktur, de er kompatible med
- Håndtering af godkendelser fra andre parter for køretøjer, der f.eks. er lejet eller lånt

5.2. Drift

5.2.1. Sikkerhedsledelsessystemet skal sikre, at der udarbejdes og implementeres interne sikkerhedsregler, operationelle instrukser og systemer, der er nødvendige for at opretholde en sikker drift under både normale og unormale driftsforhold.

5.2.2. De interne sikkerhedsregler, operationelle instrukser og systemer skal være dokumenterede og være en del af sikkerhedsledelsessystemet.

5.2.3. Sikkerhedsledelsessystemet skal sikre, at sikkerhedsregler og trafikale sikkerhedsregler håndteres i henhold til jernbaneloven.

Sikkerhedsledelsessystemet skal indeholde de nødvendige barrierer for at sikre en sikker drift. Barrierer fastlægges gennem arbejdet med risikoprofilen (se krav 3.1) og håndtering af ændringer (se krav 5.10). Kravet i 5.2 vedrører de barrierer, som virksomhedens egne sikkerhedsregler, instrukser, systemer mv. udgør.

Eksempler på dokumentation, der hører under denne kategori, kan være

- Virksomhedens trafikale sikkerhedsregler (f.eks. SR, SIN, cirkulærer og supplerende sikkerhedsbestemmelser) og nødprocedurer
- Dokumentation til brug for gennemførelse af vedligeholdelse (f.eks. instruktioner, tjekskemaer, mv.), der viser hvorledes vedligeholdelsesgrundlaget fra leverandøren er implementeret på køretøjer eller infrastruktur og eventuelle systemer til brug for styring og registrering af vedligeholdelse
- Dokumentation, som lokomotivførere og/eller andet togpersonale medbringer under driften (information om hastighedsnedsættelse, regler og lignende)

Sådanne regler, instrukser og systemer skal betragtes som en del af sikkerhedsledelsessystemet, og ligesom for resten af sikkerhedsledelsessystemet skal der defineres krav til, hvordan dokumenthåndtering skal foregå. Dvs. at sikkerhedsledelsessystemet skal indeholde beskrivelser af f.eks. format for sådanne dokumenter, processer for ændringer og ansvar for dokumenter mv., jf. krav 4.5.

For nogle typer af sikkerhedsregler er der i jernbaneloven krav om, at disse godkendes hos Trafik-, Bygge- og Boligstyrelsen. Sikkerhedsledelsessystemet skal have skriftlige processer for, hvorledes det sikres, at den krævede godkendelse opnås.

5.3. Vedligehold af infrastruktur og køretøjer

5.3.1. Sikkerhedsledelsessystemet skal sikre, at køretøjer og infrastruktur bliver vedligeholdt i henhold til krav og normer og til enhver tid overholder disse.

5.3.2. Virksomheden skal opbevare dokumentation for, at vedligehold af infrastruktur og køretøjer er gennemført, og at infrastruktur og køretøjer lever op til krav og normer.

5.3.3. Sikkerhedsledelsessystemet skal sikre information til kendte interessenter om driftsmæssige farer som følge af konstruktions- eller funktionsmæssige fejl.

Køretøjer og infrastruktur skal vedligeholdes regelmæssigt i henhold til normer, vedligeholdelsesforskrifter og -planer.

Sikkerhedsledelsessystemet skal have skriftlige processer eller tilsvarende for at sikre, at køretøjer og infrastruktur vedligeholdes som krævet.

Virksomheden skal sikre og have adgang til dokumentation for, at vedligeholdelse planlægges, styres og gennemføres. Dette kan f.eks. være:

- Procedurer for vedligeholdelse
- IT-system hvor vedligeholdelse styres
- Vedligeholdelsesplaner og instrukser
- Tjekskemaer til sikring af at alle krav i vedligeholdelsesgrundlag overholdes
- Udfyldte tjekskemaer fra gennemført vedligeholdelse
- Dokumentation for vedligeholdelsesintervallet/-tidspunkt er overholdt
- Dokumentation for kalibrering af værktøj (mærkater, skemaer, procedurer mv.)
- Dokumentation for at sporbare komponenter er vedligeholdt (på samme måde som ”hele” lokomotiver/togsæt/vogne etc.)
- Dokumentation for at køretøjer/infrastruktur er frigivet til drift
- Dokumentation for, at det er personale med de rette kvalifikationer, der har gennemført vedligeholdelsen eller har frigivet materiellet til drift

Brug af leverandører til vedligeholdelsesydelser

Hvis vedligehold udføres af andre end virksomheden selv, skal virksomheden fortsat kunne dokumentere, at køretøjer/infrastruktur er vedligeholdt. Dette kan være via dokumentation for ”indgangskontrol”, eller dokumentation for tilsyn hos leverandøren (og evt. underleverandører) vedr. om de opfylder kontraktens krav (se også krav 5.8).

En infrastrukturforvalter kan ikke lægge ansvaret for vedligeholdelsen af infrastrukturen over til en anden virksomhed, men kan købe sig til vedligeholdelsesydelser.

For køretøjer kan virksomheden med sikkerhedscertifikat godt entrere med en anden virksomhed, som vedligeholdelsesansvarlig, men det ændrer ikke ved, at det er virksomheden med sikkerhedscertifikat, der er ansvarlig for en sikker drift. Hvis den ansvarlige for vedligeholdelsen f.eks. er indehaver af et sikkerhedscertifikat eller er certificeret vedligeholdelsesansvarlig, bør man ved aftaleindgåelsen kunne gå ud fra, at processerne for vedligeholdelse overholdes, og opfølgning på kontrakt og ydelser kan tilpasses herefter.

Hvis der til driften benyttes lejede eller lånte køretøjer, eller køretøjer, der på anden måde er sat til rådighed, er det stadig den der benytter køretøjet, der er ansvarlig for, at køretøjet er vedligeholdt. Der vil stadig skulle indgås en aftale (kontraktligt forhold), og denne skal der følges op på.

Underretning i tilfælde af fejl

Hvis der i forbindelse med vedligeholdelse af køretøjer og infrastruktur konstateres fejl (konstruktions- eller funktionsmæssige), som kan resultere i driftsmæssige farer, skal virksomheden sikre, at relevante interessenter får oplysning om dette. Interessenter kan være andre brugere af køretøjer eller infrastrukturelementer, producenter samt Trafik-, Bygge- og Boligstyrelsen. For yderligere information om straksindberetning af sikkerhedsmæssige fejl, se Trafik-, Bygge- og Boligstyrelsens hjemmeside.

Sikkerhedsledelsessystemet skal indeholde processer eller procedurer for behandlingen af fejl, så den rette kommunikation sikres (se også krav 5.6).

5.4. Nødberedskab og afværgeforanstaltninger
5.4.1. Virksomheden skal identificere mulige nødsituationer og i relevant omfang beskrive disse. 5.4.2. Virksomheden skal i sikkerhedsledelsessystemet fastlægge nødvendige planer, processer, procedurer eller systemer for opretholdelse af et tilstrækkeligt sikkerhedsniveau i forbindelse med en nødsituation.
5.4.3. Sikkerhedsledelsessystemet skal endvidere sikre nødvendig information til interne og eksterne parter før, under og efter en nødsituation. 5.4.4. Sikkerhedsledelsessystemet skal ligeledes sikre, at genoprettelse af normal drift foretages på en sikkerhedsmæssig forsvarlig måde. 5.4.5. Planer, processer, procedurer og systemer skal evalueres, og virksomheden skal opbevare dokumentation for disses effektivitet.

Virksomhedernes identifikation af mulige nødsituationer kan afledes af de farer, som er beskrevet i virksomhedens risikoprofil (se krav 1.3 og 3.1). Planerne for hvordan nødsituationer håndteres bør derfor udformes med udgangspunkt i risikoprofilen.

Virksomhedens samlede planer for nødberedskab og afværgeforanstaltninger omfatter planer, procedurer, instrukser mv. til at håndtere nødsituationer under følgende faser:

- Forebyggelsesfase: Planer/procedurer/instrukser til at forebygge at en nødsituation opstår. Kan også betegnes "sikringsplaner" (begrebet Security omhandler dette område).
- Indsatsfase: Planer/procedurer/instrukser for hvordan en nødsituation håndteres fra det øjeblik den indtræffer, og indtil situationen ikke længere udgør en trussel. Kan også betegnes "indsatsplaner".
- Genopretningsfase: Planer/procedurer/instrukser for hvordan der returneres til normaltilstand efter en nødsituation har været opstået. Kan også betegnes "genopretningsplaner".

Følgende er eksempler på henholdsvis sikringsplaner, indsatsplaner og genopretningsplaner:

- En sikringsplan kan være en infrastrukturforvalters procedure for at udtynde og evt. nedlukke trafikken ved varslinger om ekstremt vejr, som kan have indvirkning på togdriften og bringe passagererne i fare.
- En indsatsplan i tilfælde af, at ekstremt vejr er indtruffet, kan være infrastrukturforvalterens plan for indkaldelse og placering af ekstra personale og materiel til udbedring af eventuelle skader, samt overvågning og kommunikation om de faktiske forhold med henblik på at vurdere, hvornår driften kan genoptages.
- Endelig kan en genopretningsplan ved ekstremt vejr være en infrastrukturforvalters procedure for i samarbejde med jernbanevirksomhederne at genoprette trafikken til normal drift, når dette kan gøres på en sikker måde.

Virksomheden skal endvidere være opmærksom på, at der i bekendtgørelse 1312 af 16/12/2008 om jernbanevirksomheders og jernbaneinfrastrukturforvalteres beredskabsarbejde yderligere er beskrevet:

- Hvordan den overordnede planlægning og koordinering af beredskabsarbejdet skal foregå, samt
- Krav til forebyggelse og håndtering af visse ekstraordinære situationer

Trafik-, Bygge- og Boligstyrelsen vurderer som udgangspunkt, at de ekstraordinære situationer som er omfattet af bekendtgørelse 1312, vil være hændelser af et omfang, hvor enten den lokale beredskabsstab (LBS) eller nationale operative stab (NOST) aktiveres.

Koordinering og kommunikation

Det er infrastrukturforvalteren som er ansvarlig for at koordinere beredskabsarbejdet med de jernbanevirksomheder, som anvender infrastrukturen. Banedanmark er endvidere ansvarlig for den overordnede koordinering på statens jernbanenet og mellem de tilstødende infrastrukturforvaltere.

Virksomheden skal sikre at dennes planer mv. for nødberedskab er koordinerede og evt. godkendt af relevante offentlige instanser, f.eks. brand- og redningstjenester samt politiet. Virksomheden skal herunder sikre, at de øvrige aktører der kan blive berørt af en nødsituation (herunder brand- og redningstjenester samt politiet) på forhånd har adgang til relevante oplysninger, så de kan forberede deres indsats.

Virksomheden skal overveje hvilken kommunikation, der under og efter en nødsituation, er nødvendig til hhv. interne og eksterne parter. Dette kan f.eks. være:

- Alarmering af brand- og redningstjenester, politi samt øvrigt personale med ansvar for håndtering af en nødsituation
- Information til passagerer, pårørende, presse og andre eksterne interessenter
- Oplysninger om kontaktpunkt, så jernbanevirksomheder og infrastrukturforvaltere effektivt kan komme i kontakt med hinanden i en nødsituation

Organisering, kompetencer og uddannelse

Virksomheden skal have beskrevet roller, ansvar og beføjelser i nødsituationer under både forebyggelses-, indsats- og genopretningsfasen. Virksomheden skal i den forbindelse identificere de kompetencer og uddannelseskrav, der er nødvendige for, at personalet kan agere hensigtsmæssigt og sikkerhedsmæssigt forsvarligt i forbindelse med nødsituationer (se også krav 4.1 og 4.2).

Evaluering og øvelser

Virksomheden skal løbende evaluere de enkelte dele af sine beredskabsplaner (f.eks. sikringsplaner, indsatsplaner og genopretningsplaner) for at sikre, at planernes indhold og deres efterlevelse er hensigtsmæssig. For at opnå bedst mulig læring, skal virksomheden evaluere de relevante dele af beredskabsplanerne, når disse har været i anvendelse, enten i forbindelse med øvelser eller konkrete nødsituationer (se endvidere krav 6.1).

Virksomhedens evaluering af beredskabsplanerne skal indeholde en stillingtagen til hvorvidt disse fungerer effektivt, og om der er behov for eventuelle justeringer i planer, procedurer, instrukser samt om nødvendigt fysiske eller organisatoriske forhold. Virksomheden skal opbevare dokumentation for denne evaluering.

Virksomheden skal identificere de scenarier, hvor det er nødvendigt at gennemføre øvelser for at afprøve nødberedskabet. Bekendtgørelse 1312 stiller krav om, at der afholdes beredskabsøvelser for de ekstraordinære situationer, som er omfattet af bekendtgørelse 1312.

Øvelser skal gennemføres i samarbejde med relevante parter (f.eks. andre infrastrukturforvaltere og jernbanevirksomheder, brand- og redningstjenester samt politiet) med henblik på at identificere udfordringer i den koordinerede indsats samt verificere, at nødsituationer håndteres korrekt.

5.5. Registrering og håndtering af ulykker og forløbere til ulykker
5.5.1. Sikkerhedsledelsessystemet skal sikre, at ulykker og forløbere til ulykker bliver afhjulpet og registreret.
5.5.2. Sikkerhedsledelsessystemet skal sikre, at undersøgelse, analyse og korrigerende handlinger herefter gennemføres iht. 7.3.

Begreberne ulykker og forløbere til ulykker er nærmere beskrevet i bekendtgørelsen om indberetning af ulykker mv. med tilhørende vejledning. Observationer af denne type knytter sig til kørsel med jernbanekøretøjer. Hvis der ikke er kørsel involveret vil der blot være tale om fejl og mangler, som ikke er farlige, så lang tid, der ikke køres (se krav 5.6 og 5.7).

Dette krav omhandler alle typer af hændelser, som virksomheden skal registrere. Hændelser er her fælles begreb for alle typer af ulykker og forløbere til ulykker, og ikke blot dem, som skal indberettes til myndigheden.

Sikkerhedsledelsessystemet skal indeholde processer / instruktioner for at afhjælpe og evt. begrænse hændelser, når de er sket.

Ligeledes skal sikkerhedsledelsessystemet indeholde processer / instruktioner og systemer til at registrere hændelser. Det er væsentligt, at det tydeligt er præciseret i f.eks. en instruktion eller et selvforklarende registreringssystem, hvilke data der skal registreres.

Forholdene bør beskrives så præcist som muligt med fakta som f.eks. tid, sted, involverede køretøjer, involverede personer, hændelsesforløb samt andet, der kan være relevant for den videre behandling.

Virksomheden skal sikre, at processerne/systemerne for registrering er kendt af alle relevante medarbejdere, der skal kunne registrere en ulykke eller en forløber til en ulykke. Virksomheden bør afgrænse, hvilke typer af medarbejdere, der skal registrere hændelser. Disse medarbejdere bør oplæres i processerne / systemerne, således at alle får en fælles opfattelse af hvad der skal registreres, i hvilke systemer og i hvilke situationer, der skal registreres.

Formålet med at registrere hændelser, er at opsamle data og dermed få viden til at kunne analysere årsagen til hvad der gik galt, og således kunne opstille korrigerende handlinger for at forebygge gentagelse.

Processen for registrering af hændelser skal lede til proces for undersøgelse, analyse og korrigerende handlinger, jf. krav 7.3.

5.6. Opsamling af data om fejl og mangler opstået under driften
5.6.1. Sikkerhedsledelsessystemet skal sikre, at fejl og mangler, der opstår på køretøjer eller infrastruktur under den daglige drift, bliver afhjulpet og registreret.
5.6.2. Sikkerhedsledelsessystemet skal sikre, at undersøgelse, analyse og korrigerende handlinger herefter gennemføres iht. 7.3.

Drift skal her forstås i den brede forstand, således at alt hvad der hører med til at drive virksomhed (som jernbanevirksomhed eller infrastrukturforvalter eller den del af en virksomhed med sikkerhedscertifikats drift, som hører til kørsel på jernbanen) indgår. Således er det både fejl ved køretøjer, som lokomotivføreren / togpersonalet konstaterer og de fejl og mangler, der konstateres på værkstedet i forbindelse med vedligeholdelse, der skal registreres. Ligeledes for infrastruktur skal både fejl rapporteret i forbindelse med kørslen på denne og fejl konstateret i forbindelse med vedligeholdelsesarbejde registreres.

Data fra vedligeholdelse af køretøjer og/eller infrastruktur kan afsløre potentielle risici, men potentielt anses risici for at være endnu større, hvis fejl eller mangler først opdages under kørslen.

Sikkerhedsledelsessystemet skal indeholde processer og systemer for registrering og afhjælpning af de ovennævnte forhold. Forholdene bør beskrives så præcist som muligt med fakta om fejlen samt andet, der kan være relevant for den videre behandling.

Processen for opsamling af data om fejl og mangler opstået under driften skal lede til proces for analyse og korrigerende handlinger, jf. krav 7.3.

5.7. Afvigelser fra sikkerhedsledelsessystemet, som identificeres løbende
5.7.1. Sikkerhedsledelsessystemet skal sikre, at afvigelser fra sikkerhedsledelsessystemet, som identificeres løbende, bliver afhjulpet og registreret.
5.7.2. Sikkerhedsledelsessystemet skal sikre, at undersøgelse, analyse og korrigerende handlinger herefter gennemføres iht. 7.3.

Dette krav vedrører de fejl og afvigelser fra sikkerhedsledelsessystemet, der opdages løbende og ikke i forbindelse med systemaudit, jf. krav 6.5.

Ved afvigelse fra sikkerhedsledelsessystemet menes enhver situation, hvor sikkerhedsledelsessystemets retningslinjer ikke er fulgt. Virksomheden bør dog selv definere et niveau for, hvornår afvigelser skal registreres, så håndteringen af afvigelser giver værdi for virksomheden. Afvigelse kan dække mange forskellige situationer, f.eks. hvis en medarbejder ikke får brugt den korrekte instruktion eller skabelon, eller ikke følger processen ved udførelsen af sit arbejde.

Sikkerhedsledelsessystemets procedurer jf. ovenstående bør sikre, at situationen om nødvendigt afhjælpes. Ligeledes bør procedurerne beskrive hvem der skal inddrages og/eller have ansvar for den videre behandling af observationerne. F.eks. bør ansvarlige ledere, procesejere eller lignende inddrages.

Formålet med at registrere afvigelser er læring med det formål at forbedre systemet eller f.eks. implementeringen af dette – ikke at bebrejde medarbejderne.

Processen vedr. afvigelser fra sikkerhedsledelsessystemet, som identificeres løbende skal lede til proces for analyse og korrigerende handlinger, jf. krav 7.3.

5.8. Styring af eksterne leverancer

5.8.1. Sikkerhedsledelsessystemet skal sikre, at leverandører af ydelser med sikkerhedsmæssigt indhold udvælges på baggrund af opstillede kriterier til ydelsen, herunder eventuelle kompetencekrav til det anvendte personale hos leverandøren.

5.8.2. Sikkerhedsledelsessystemet skal sikre, at aftaler med leverandører om samarbejde om eller køb af ydelser med et sikkerhedsmæssigt indhold er fastsat i en skriftlig aftale, som definerer krav til ydelsernes indhold samt krav til ansvar, dokumentation, kommunikation, kompetencer og overvågning.

5.8.3. Sikkerhedsledelsessystemet skal sikre, at aftalen godkendes af en medarbejder med de rette beføjelser.

5.8.4. Sikkerhedsledelsessystemet skal med udgangspunkt i det sikkerhedsmæssige indhold sikre, at aftalen er beskrevet i en detaljeringsgrad, der muliggør, at leverancerne kan overvåges.

Dette krav omhandler alt det arbejde, der har indflydelse på sikkerheden, som udføres af eksterne parter. Det kan være ydelser omkring vedligeholdelse af køretøjer eller infrastruktur, men også ydelser af sikkerledelsesmæssige opgaver, som f.eks. intern audit og gennemførelse af risikovurderinger mv.

Sikkerhedsledelsessystemet skal indeholde skriftlige processer eller tilsvarende, der beskriver hvordan leverandører udvælges. Processerne kan med fordel fastholdes gennem udarbejdelse af tjeklister/-skemaer og kontraktstandarder eller -skabeloner, der sikrer, at virksomheden forholder sig til alle relevante sikkerhedsmæssige aspekter ved indgåelse af aftaler/kontrakter. Det vil endvidere være naturligt at inddrage virksomhedens jurister/en juridisk vurdering i dette arbejde.

Der skal være processer i sikkerhedsledelsessystemet der sikrer, at der udarbejdes en skriftlig aftale for leverance af ydelser med sikkerhedsmæssigt indhold, og virksomheden skal kunne fremvise gyldige skriftlige kontrakter for alle sådanne ydelser.

Af kontrakterne skal det fremgå:

- Hvilke opgaver/leverancer, der er aftalt
- Ansvarsfordeling
- Eventuelle krav til leverancer og/eller kompetencer
- Hvilke parametre, der skal overvåges
- Aftaler om adgang til leverandøren, evt. i forbindelse med audit
- Hvornår kontrakten er indgået og evt. hvornår den er gyldig til

Kontrakten skal være så specifik, at det er muligt for virksomheden at følge op på, om den aftalte ydelse leveres.

Kontrakter skal være gennemgået og underskrevet af begge parter, af personale med dokumenterede beføjelser hertil.

Virksomheden skal gennemføre kontrol med kontraktens overholdelse. Denne kontrol kan være i form af "indgangskontrol", eller tilsyn hos leverandøren (og evt. underleverandører) vedr. om de opfylder kontraktens krav. Gennemført kontrol skal dokumenteres. Virksomheden bør ligeledes have processer for sikring af eventuelle korrigerende handlinger hos leverandøren.

5.9. Eksterne krav
5.9.1. Sikkerhedsledelsessystemet skal sikre, at eksterne krav i form af lovkrav, bekendtgørelser, myndighedsafgørelser, tekniske og driftsmæssige standarder, andre normative krav m.v. kontinuerligt bliver identificeret og implementeret i sikkerhedsledelsessystemet.
5.9.2. Sikkerhedsledelsessystemet skal sikre overholdelse af eksisterende, nye og ændrede eksterne krav.
5.9.3. Virksomheden skal kunne dokumentere implementering af eksterne krav.

Dette krav handler om den løbende identifikation af lovkrav og andre krav og implementering af disse i sikkerhedsledelsessystemet, mens krav 1.2 handler om den indledende afklaring af den lovgivningsmæssige ramme, som virksomheden planlægges at skulle fungere i.

Virksomheden skal identificere og sætte sig ind i de gældende love og andre relevante standarder og forskrifter og indføre et system, der sikrer, at de overholdes.

Sikkerhedsledelsessystemet skal have dokumenterede processer eller tilsvarende for, hvorledes identifikation og efterlevelse af relevant lovgivning, bekendtgørelser, forordninger og andre EU-regler (herunder TSI'er), forskrifter, og krav fra f.eks. infrastrukturforvaltere til jernbanevirksomheder mv. sikres.

Sikkerhedsledelsessystemet skal specificere ansvaret for dette arbejde og angive en metode, hvorpå det sikres at ny/ændret lovgivning samt nye/ændrede regler implementeres rettidigt inden ikrafttræden.

Sikkerhedsledelsessystemet bør således specificere ansvar og opgaver i forbindelse med:

- Identifikation af ny eller ændret lovgivning eller nye/ændrede regler. Dette kan f.eks. gøres via regelmæssig screening af relevante hjemmesider og suppleres med abonnement, deltagelse i udvalg, høringsrunder og lignende.
- Implementering af ny eller ændret lovgivning eller nye/ændrede regler i sikkerhedsledelsessystemet. Der skal foretages en gennemgang af relevante dele af sikkerhedsledelsessystemet, for at sikre at ændringer i love og regler implementeres i processer/procedurer, hvor dette er påkrævet.

Det forventes, at virksomheden kan fremvise et overblik over gældende love og regler, evt. i form af en liste eller et register. Følgende bør fremgå:

- Hvor i sikkerhedsledelsessystemet de enkelte love og regler er indarbejdet
- Hvilke dele af lovgivningen, der er implementeret (f.eks. kan der være TSI'er, hvor kun dele af dem er relevante for virksomheden)

Virksomheden bør selv f.eks. ved intern audit følge op på, om lovgivning mv. er implementeret. Til brug for planlægning af sådanne audits vil ovennævnte overblik kunne være til nytte.

5.10. Håndtering af ændringer

5.10.1. Sikkerhedsledelsessystemet skal sikre risikovurdering og implementering af risikostyringsforanstaltninger, hvis en ændring i organisation, driftsvilkår, infrastruktur eller køretøjer indebærer nye og/eller ændrede risici i relation til driften. Sikkerhedsledelsessystemet skal sikre, at

1) alle ændringer identificeres,
2) ændringens sikkerhedsmæssige betydning, herunder også risici der er ved ændringens gennemførelse, vurderes og
3) metode for håndtering af ændringer vælges.

5.10.2. Identificerede ændringer, vurderinger og valg af metode skal dokumenteres.

5.10.3. Sikkerhedsledelsessystemet skal sikre, at alle ændringer vurderes af repræsentanter for relevante interne og eksterne parter, der påvirkes af ændringen. Vurderingen skal dokumenteres.

5.10.4. For alle ændringer skal det vurderes, om ændringen har indflydelse på virksomhedens risikoprofil jf. 3.1. Vurderingen skal dokumenteres.

Ændringer kan forekomme som følge af udefra kommende forhold eller interne forhold. Udefra kommende ændringer kan f.eks. initieres af påkrævet ny teknologi (f.eks. ERTMS) eller ny lovgivning. Ændringer som følge af interne forhold kan f.eks. være planlagte investeringer i køretøjer, infrastruktur, styresystemer (f.eks. SAP), ønske om drift på nye strækninger, ændringer i organisationen, udskiftning af leverandører eller korrigerende handlinger som følge af fejl, ulykker, intern audit eller ledelsens evaluering.

Alt, der ikke er 1:1 udskiftninger, skal som udgangspunkt betragtes som en ændring. Virksomheden skal definere, hvornår noget er en ændring / hvad en ændring er, og sikre, at alle medarbejdere, der arbejder inden for områder, der kan blive berørt af ændringer, er bekendt med definitionen, og hvordan ændringer skal håndteres jf. nedenfor. Specielt for medarbejdere, der arbejder med vedligeholdelsesopgaver er det vigtigt, at de har en korrekt opfattelse af, hvad der er en ændring (og skal behandles som sådan), og hvad der blot er almindelig vedligeholdelse.

Sikkerhedsledelsessystemet skal have dokumenterede processer eller tilsvarende, som sikrer, at alle ændringer håndteres efter følgende fremgangsmåde:

1. Enhver ændring skal vurderes med henblik på, om den har betydning for jernbanesikkerheden. Ved denne vurdering er det vigtigt at vurdere ændringen isoleret set, og således ikke allerede her tænke barrierer ind i vurderingen. Dvs. det skal vurderes om ændringen i sig selv ville have indflydelse på sikkerheden, hvis man implementerede den, uden at opstille barrierer for at imødekomme evt. øgede risici. Kun hvis det vurderes, at ændringen i sig selv ikke har indflydelse på sikkerheden, skal den ikke risikovurderes yderligere inden gennemførelse. Risikoprofilen skal inddrages ved dette arbejde.
2. Vurderes det, at en ændring har betydning for sikkerheden, skal det efterfølgende vurderes om ændringen er signifikant.
3. Signifikansvurdering og håndtering af signifikante ændringer behandles ikke yderligere her, der henvises til Trafik-, Bygge- og Boligstyrelsens bekendtgørelser og vejledninger specifikt om dette emne.
4. Ændringer, der vurderes ikke-signifikante skal håndteres efter processer eller tilsvarende i virksomhedens sikkerhedsledelsessystem, som skal sikre vurdering af det ændrede risikobillede og opstilling af barrierer, jf. nedenfor.

Ændringer skal håndteres som et samarbejde mellem personale, der har passende faglige kompetencer til at vurdere risici mv. og personale, der har ledelsesmæssige beføjelser til at gennemføre nødvendige ændringer. Det er ligeledes væsentligt at inddrage medarbejdere og eventuelle eksterne parter, som har indflydelse på eller påvirkes af ændringen for at sikre, at alle relevante forhold er taget i betragtning.

Alle ændringer samt beslutninger taget og resultater fremkommet i løbet af processen med håndtering af ændringen skal dokumenteres.

5.11. Dispensationer

5.11.1. Sikkerhedsledelsessystemet skal sikre, at sikkerhedsmæssige konsekvenser ved eventuelle dispensationer fra krav og/eller processer i sikkerhedsledelsessystemet vurderes af funktioner med de rette kompetencer og beføjelser.

5.11.2. Virksomheden skal opbevare dokumentation for udstedte dispensationer med tilhørende vurderinger.

Som udgangspunkt skal sikkerhedsledelsessystemet altid følges. Der vil dog kunne forekomme tilfælde, hvor dette ikke kan lade sig gøre, det ikke er hensigtsmæssigt, eller at der i forbindelse med ændringer vil være behov for midlertidigt at gøre noget andet, end det som systemet foreskriver.

Det kan for eksempel være i en situation, hvor virksomheden arbejder henimod en ændret metode eller indførelsen af et nyt system til f.eks. vedligeholdelse, og hvor implementeringen ikke kan ske for hele organisationen på en gang – eller det af hensyn til afprøvningsfasen er hensigtsmæssigt, at dele af virksomheden følger nye processer, mens resten af virksomheden stadig skal bruge de eksisterende.

I sådanne tilfælde kan virksomheden vælge at dispensere fra krav eller processer i systemet og på den måde acceptere "planlagte afvigelser". Det bemærkes at virksomheden kun kan dispensere fra egne krav, og ikke lovgivning og andre eksterne krav.

Det er dog altid vigtigt, at dispensationer gives på et korrekt og oplyst grundlag, og at eventuelle sikkerhedsmæssige konsekvenser er vurderet. Vurderingen bør principielt ligne vurderingen, der skal gennemføres ved håndering af ændringer jf. krav 5.10, men der er ikke et formelt krav om, at metodikken her skal følges. Dog skal det altid sikres, at der foretages en vurdering af dispensationens indflydelse på sikkerheden, og at de rette kompetencer og beføjelser inddrages.

Ofte kan det være hensigtsmæssigt at kræve, at en central person i forhold til sikkerhedsledelsessystemet (f.eks. sikkerhedschefen) skal inddrages af hensyn til sammenhængen i systemet, mens det ligeledes forventes, at berørte medarbejdere og ansvarlige ledere for det berørte område deltager i vurderingen.

Virksomheden skal definere, hvorledes dispensationer med tilhørende vurderinger skal dokumenteres.

6. Overvågning

6.1. Overvågning, måling, analyse og evaluering

6.1.1. Virksomheden skal med udgangspunkt i risikoprofilen udarbejde en dokumenteret overvågningsstrategi, som identificerer områder og prioriteringer for overvågning af det sikkerhedsmæssige niveau og sikkerhedsledelsessystemets effektivitet.

6.1.2. Overvågningsstrategien skal i relevant omfang indeholde overvågning af leverandørers sikkerhedsmæssige formåen.

6.1.3. Overvågningsstrategien skal omsættes til en eller flere dokumenterede overvågningsplaner for sikkerhedsmål, sikkerhedsindikatorer, inspektioner og systemaudit.

Sikkerhedsniveauet og sikkerhedsledelsessystemets effektivitet skal overvåges, således at virksomheden så tidligt som muligt har mulighed for at identificere de sikkerhedsmæssige forhold samt trends, som kan resultere i hændelser eller andre (potentielt) farlige situationer. Formålet er at kunne gennemføre korrigerende handlinger inden en farlig situation opstår.

Overvågningsstrategi

En overvågningsstrategi skal dokumentere de forskellige typer af overvågning, som virksomheden har prioriteret og besluttet at gennemføre. Herunder skal strategien kunne dokumentere, de kriterier prioriteringerne er foretaget ud fra.

Det forventes ikke, at en overvågningsstrategi er et stort og omfattende dokument, men at virksomheden i overvågningsstrategien på en kort og klar måde kan redegøre for valgene og deres baggrund. Virksomheden kan anvende skematiske opstillinger med kort og klar tekst.

Beslutningen om, hvad der skal overvåges, skal træffes ud fra vurderinger af, hvad der giver anledning til de største risici, og hvor det kan have negative konsekvenser for sikkerheden, hvis der ikke overvåges effektivt. Virksomheden skal med udgangspunkt i risikoprofilen samt ledelsens evaluering identificere og beslutte hvilke områder, der skal overvåges og således indsamles oplysninger om. Ligeledes skal kravene i denne bekendtgørelse sikres opfyldt.

Overvågningsstrategien skal således sikre overvågning af:

- Målopfyldelse (jf. krav 3.2 og 6.2)
- Egne udvalgte sikkerhedsindikatorer (jf. krav 6.3)
- Data fra operationelle inspektioner (jf. krav 6.4)
- Data opsamlet ad hoc fra driften, herunder data fra vedligeholdelse af rullende materiel og/eller infrastruktur (jf. krav 5.5, 5.6 og 5.7)
- Afholdte beredskabsøvelser (jf. krav 5.4)
- Om procedurer mv. i sikkerhedsledelsessystemet er korrekte og anvendes korrekt, og om systemet er dækkende i forhold til virksomhedens risici og aktiviteter (jf. krav 6.5)
- Leverandørers ydelser iht. de aftaler, der er indgået med leverandøren (jf. krav 5.8)

Mindre virksomheder, som kun genererer få data, kan her overveje muligheden for dialog med branchen, for bedre at kunne vurdere om der kan identificeres eventuelle relevante trends eller andre sikkerhedsmæssige forhold af betydning for virksomheden.

For virksomheder, der udfører opgaver for jernbanevirksomheder eller infrastrukturforvaltere, er det udelukkende et krav, at overvågningsstrategien vedrører overvågning af aktiviteterne ifm. kørslen (jf. krav 1.1).

Overvågningsstrategien skal godkendes af virksomhedens øverste ledelse, som også bør inddrages i udarbejdelsen af strategien. Det anbefales, at overvågningsstrategien indgår som et fast punkt ved ledelsens evaluering (se krav 7.2.)

Overvågningsplaner

For hver af de besluttede overvågningstyper, skal virksomheden opstille overvågningsplaner. Overvågningsplanerne skal definere ansvar, frekvens og evt. metode for opsamling af data.

Planerne kan med fordel kobles til risikoprofilen, således at det af risikoprofilen fremgår hvilke barrierer, der overvåges på hvilken måde.

Overvågninger, som er kontinuerte/en fast del af sikkerhedsledelsen, kan evt. beskrives i sikkerhedsledelsessystemets processer / instruktioner.

Overvågningsplaner inden for områderne sikkerhedsmål, sikkerhedsindikatorer, operationelle inspektioner og systemaudit behandles i krav 6.2 – 6.5.

6.2. Sikkerhedsmål
6.2.1. Sikkerhedsledelsessystemet skal sikre overvågning af virksomhedens sikkerhedsmål med henblik på vurdering af målopfyldelse.
6.2.2. Gennemført overvågning og resultatet af denne skal dokumenteres.

Virksomheden skal følge sin overvågningsplan for området sikkerhedsmål. Virksomheden skal løbende følge op på gennemførelse af handlingsplaner for mål, men bør også løbende – hvis muligt - følge op på målopfyldelse (jf. krav 3.2).

Overvågningen skal sikre, at der er grundlag (data/informationer) for at foretage løbende evalueringer i forhold til målopfyldelse, således at en evt. trend, der går i den forkerte retning, opdages så tidligt som muligt og der kan foretages de fornødne justeringer.

Endvidere kan ændringer i virksomhedens aktiviteter, organisationen eller omverdenen ændre risikobilledet, hvorefter målene ligeledes bør revurderes og justeres.

Som minimum skal målopfyldelsen evalueres af ledelsen ved den årlige ledelsens evaluering (jf. krav 7.2).

Det vil være naturligt, at det er ledelsen der overvåger den løbende fremdrift i virksomhedens fastsatte sikkerhedsmål over året.

Det forventes, at virksomheden kan dokumentere overvågningen f.eks. i form af mødereferater, opsamlede data i regneark, databaser eller tilsvarende.

6.3. Sikkerhedsindikatorer

6.3.1. Sikkerhedsledelsessystemet skal sikre identifikation og overvågning af relevante sikkerhedsindikatorer i henhold til overvågningsplanerne.

6.3.2. Gennemført overvågning og resultatet af denne skal dokumenteres.

6.3.3. Sikkerhedsledelsessystemet skal sikre, at tendenser bliver identificeret, og at der, når relevant, iværksættes analyse og korrigerende handlinger jf. 7.3.

Sikkerhedsindikatorer er værdier, der kontinuert skal måles på for at følge udviklingen i virksomhedens sikkerhedsmæssige niveau. Ledelsen vælger i forbindelse med udarbejdelse af overvågningsstrategien (jf. krav 6.1), hvilke sikkerhedsindikatorer, der skal måles på.

Eksempler på sikkerhedsindikatorer er "antal skinnebrud pr. tusind spor-km pr. år", "antal signalforbikørsler forbi farepunkt pr. million tog-km pr år" og "antal knækkede aksler pr. million tog-km pr år".

Når der måles på sikkerhedsindikatorer, er det vigtigt for at kunne udlede en evt. trend, at data opsamles over tid, og gerne over flere år. Hvis ikke der opsamles data over tid, er det ikke muligt at følge udviklingen, og evt. forhindre en negativ sikkerhedsmæssig tendens, jf. nedenfor.

Det forventes, at virksomheden kan dokumentere overvågningen f.eks. i form af mødereferater, opsamlede data i regneark, databaser eller tilsvarende.

Overvågningen skal sikre at en evt. trend, der går i den forkerte retning, opdages så tidligt som muligt, så virksomheden kan foretage de fornødne tiltag. Hvis en indikator viser en negativ trend, så skal årsagen til dette undersøges nærmere jf. krav 7.3.

6.4. Operationelle inspektioner

6.4.1. Sikkerhedsledelsessystemet skal sikre planlægning og periodevis udførelse af operationelle inspektioner i henhold til overvågningsplanerne for at undersøge, hvorvidt sikkerhedsledelsessystemet genererer de tilsigtede resultater.

6.4.2. Metoderne for operationelle inspektioner skal defineres og dokumenteres.

6.4.3. Planer for inspektioner skal dokumenteres og ajourføres, således at status til hver en tid fremgår.

6.4.4. Gennemførte inspektioner og deres resultater skal dokumenteres.

6.4.5. Sikkerhedsledelsessystemet skal sikre, at der sker en effektiv opfølgning på resultaterne af inspektionerne, herunder identifikation af tendenser, og at der, når relevant, iværksættes analyse og korrigerende handlinger jf. 7.3.

Operationelle inspektioner er periodiske kontroller af sikkerhedsledelsessystemets output. Det er ikke den kontrol, der foretages i den daglige drift, som f.eks. kontrol af

personalets kompetencer i forbindelse med tildeling af opgaver i værkstedet eller ved vagtplanlægning.

Det er derimod kontroller, der foretages med givne mellemrum, for at kontrollere om f.eks. en lokomotivfører foretager de rette dispositioner, når han/hun fremfører tog (førerrumstilsyn) eller en stikprøvekontrol, som f.eks. en produktionsleder kan foretage i vedligeholdelsesværkstedet, hvor et netop vedligeholdt tog bliver udtaget til en ekstra 100 % kontrol af, om vedligeholdelse er foretaget fyldestgørende og korrekt.

Operationelle inspektioner adskiller sig fra intern audit (jf. krav 6.5) ved primært at være kontrol af output, mens intern audit primært er kontrol af processen.

Ledelsen vælger i forbindelse med udarbejdelse af overvågningsstrategien (jf. krav 6.1), hvilke operationelle inspektioner, der skal foretages. Det anbefales også her at konsultere risikoprofilen, samt resultaterne af ledelsen evaluering for at identificere evt. problemområder.

Operationelle inspektioner foretages normalt som en kontinuert tilbagevendende opgave i virksomheden. For hver inspektionstype skal ansvar, metode (instruktioner, skabeloner mv.), planlægning og dokumentation af gennemførte inspektioner beskrives i sikkerhedsledelsessystemet i et omfang, der er passende for virksomheden.

Virksomheden skal udarbejde årlige planer for de operationelle inspektioner. Planerne skal sikre, at hele det valgte område for inspektionerne er dækket over en passende periode, som virksomheden selv definerer. Status på gennemførelse af inspektionerne skal fremgå af planen. Regneark eller databaser er velegnede til dokumentation af disse planer.

Resultaterne af inspektionerne skal dokumenteres. Det anbefales som minimum at dokumentere følgende:

- Inspektionens formål, emne og omfang
- Fakta (dato, deltagere etc.)
- Resultater, konklusioner (som også kan være, at der ikke er fundet afvigelser)
- Afvigelser / forhold til opfølgning

Processerne for operationelle inspektioner skal sikre, at der følges op på identificerede afvigelser / forhold til opfølgning og at disse i relevant omfang håndteres iht. krav 7.3.

6.5. Intern audit (systemaudit)

6.5.1. Sikkerhedsledelsessystemet skal sikre periodevis udførelse af intern audit af sikkerhedsledelsessystemet i henhold til overvågningsplanerne for at undersøge, hvorvidt systemet er udformet og fungerer tilfredsstillende.

6.5.2. Metoderne for intern audit skal defineres og dokumenteres.

6.5.3. Planer for intern audit skal dokumenteres og ajourføres, således at status til hver en tid fremgår.

6.5.4. Gennemførte interne audits og deres resultater skal dokumenteres.

6.5.5. Sikkerhedsledelsessystemet skal sikre, at der sker en effektiv opfølgning på resultaterne af de interne audits, herunder identifikation af tendenser, og at der, når relevant, iværksættes analyse og korrigerende handlinger jf. 7.3.

6.5.6. Sikkerhedsledelsessystemet skal sikre, at intern audit udføres af auditorer, der er uafhængige af den funktion eller aktivitet, der auditeres, samt at der stilles krav om kompetencer for auditorer.

Formålet med intern audit (systemaudit) er:

- At afdække hvorvidt hele sikkerhedsledelsessystemet er retvisende, implementeret og fungerer effektivt
- At afdække om ledelsessystemet er dækkende i forhold til virksomhedens aktiviteter og risici

- At afdække om alle relevante krav er implementeret i virksomhedens sikkerhedsledelsessystem
- På baggrund heraf, at opstille korrigerende handlinger for at forbedre systemet

Ved intern audit undersøges hvorvidt virksomhedens sikkerhedsledelsessystem er udformet tilfredsstillende og fungerer efter hensigten. Derfor afdækkes det ved intern audit hvorvidt processerne mv. i systemet er fulgt. Eksempelvis om de enkelte trin i processen eller instruktionen er fulgt, om eftersynsskemaer er udfyldt som angivet, om fejlhåndtering er sket korrekt i forhold til det beskrevne, om det er personer, der har de rette kompetencer, der f.eks. klarmelder materiel til drift etc. Det afdækkes også, om der evt. mangler processer, instruktioner, skabeloner mv.

Intern audit må ikke forveksles med kontrol af resultatet eller output, idet et korrekt resultat eller output ikke nødvendigvis betyder, at systemet er fulgt. Kontrol af resultatet eller outputtet kan både foregå som en del af driften, eller som operationelle inspektioner (se krav 6.4), men vil også typisk indgå som stikprøver ved intern audit.

Virksomheden skal i sikkerhedsledelsessystemet etablere dokumenterede metoder / processer og systemer til at udforme auditplan samt planlægge og gennemføre de enkelte interne audit (inkl. registrering og opfølgning).

Denne vejledning indeholder ikke vejledning i specifikke metoder til gennemførelse af intern audit. Her henvises til anden litteratur om emnet.

Plan for intern audit (overvågningsplan for systemaudit)

Virksomheden skal udarbejde en plan for intern audit. Planen skal sikre, at der bliver gennemført intern audit med hele systemet over en periode, som virksomheden selv definerer. Perioden må maksimalt være 5 år, men en periode på 2-3 år anbefales.

Virksomheden skal med udgangspunkt i risikoprofilen vurdere, om nogle aktiviteter skal auditeres oftere end andre. Dette kan være de processer, der er opstillet som barrierer for farer som indebærer stor sikkerhedsmæssig risiko.

Planen bør fastsætte ca. tidspunkt og auditorer for de enkelte audit. Planen kan opdeles efter organisationen eller systemet eller en kombination, alt efter hvad virksomheden finder mest hensigtsmæssigt. Det frarådes at planlægge intern audit udelukkende efter bekendtgørelsens krav, da udgangspunktet bør være virksomheden og dens risikoprofil.

Det skal bemærkes, at det normalt ikke er muligt at gennemføre intern audit med hele sikkerhedsledelsessystemet på en enkelt dag (med mindre der anvendes mange auditorer samtidig). En så begrænset tid til audit vil næppe kunne give et retvisende billede, jf. formålet med intern audit ovenfor.

Det er normalt sikkerhedschefens ansvar at udarbejde planen for intern audit. Planen for intern audit bør godkendes af virksomhedens øverste ledelse.

Planen for intern audit skal opdateres løbende, således at den aktuelle status fremgår, og at det af planen er muligt at se om planlagte audit er gennemført, flyttet i forhold til den oprindelige plan, ændret indholdsmæssigt eller helt udgået. Det bør i sikkerhedsledelsessystemet fremgå hvorledes opdateringen skal foregå og dokumenteres. Det er normalt sikkerhedschefens ansvar at holde planen opdateret. Relevante ændringer i forhold til den oprindelige godkendte plan bør godkendes af virksomhedens øverste ledelse.

Dokumentation for gennemført audit

Resultaterne af gennemført audit skal dokumenteres. Det anbefales som minimum at dokumentere følgende:

- Hvad der er udført intern audit med (gennemgåede processer mv.)
- Fakta (dato, deltagere etc.)
- Resultater, konklusioner (som også kan være, at der ikke er fundet afvigelser)
- Afvigelser / forhold til opfølgning

Virksomheden bør udarbejde procedurer, relevante tjeklister, skemaer samt systemer til registrering af resultater af gennemførte audit, som auditorerne skal anvende ved gennemførelsen. Det vil typisk være sikkerhedschefen, der har ansvaret for denne dokumentation.

Opfølgning på afvigelser

Afvigelser skal håndteres og følges op. Det skal derfor klart beskrives i sikkerhedsledelsessystemet hvordan f.eks. konstaterede fejl, uoverensstemmelser, afvigelser ol. fundet ved de gennemførte audit, registreres. Det anbefales at registrere afvigelser separat, for bedre at kunne håndtere og følge op på disse.

Ansvaret for opfølgning skal fastlægges i sikkerhedsledelsessystemet, og det skal sikres, at der sker den fornødne opfølgning iht. krav 7.3.

Auditorer

Intern audit skal foretages af personer, der er organisatorisk uafhængige af det arbejde eller de personer, der skal udføres intern audit med. Det må således ikke være chefen for området, eller en person, der arbejder i samme procesforløb eller på anden måde har interesser i det, der bliver udført intern audit med.

I meget små virksomheder kan det være svært at opretholde princippet om uafhængighed, og det vil ofte ikke være muligt at gennemføre i praksis. I sådanne tilfælde bør virksomheden gøre brug af eksterne auditorer.

Virksomheden skal opstille kompetencekrav til auditorer. Nødvendige krav er kendskab til sikkerhedsledelsessystemet samt til relevant lovgivning, men det forventes, at virksomhederne også stiller krav om specifik auditoruddannelse på et passende niveau, således at der opnås en vis grad af systemforståelse, samt kendskab til spørgeteknik, begreber som objektivt vidnesbyrd, afvigelser, korrigerende handlinger mv.

7. Forbedring

7.1. Generelt

7.1.1. På baggrund af overvågningen, jf. 6.1–6.5 skal virksomheden løbende fastlægge muligheder for forbedringer og implementere nødvendige handlinger for at nå de resultater, der tilsigtes med sikkerhedsledelsessystemet.

Resultaterne af virksomhedens samlede overvågning (jf. krav 6) giver viden om virksomhedens sikkerhedsmæssige niveau, herunder viden om den aktuelle udvikling i de parametre der overvåges samt viden om effektiviteten af sikkerhedsledelsessystemet.

Denne viden skal omsættes til fastlæggelse af muligheder for forbedringer. Dette arbejde skal ske løbende via processer i sikkerhedsledelsessystemet.

Krav 7.1 handler om at sikre sammenhæng mellem resultaterne af virksomhedens overvågning og beslutninger om sikkerhedsmæssige forbedringer. Man kan omvendt sige, at virksomhedens beslutninger om sikkerhedsmæssige forbedringer skal være baseret på databaseret viden om dens sikkerhedsniveau og effektiviteten af dens sikkerhedsledelsessystem. Ligeledes handler det om, at virksomheden kontinuert har fokus på muligheder for forbedring.

Det forventes ikke at virksomheden opstiller særskilte processer vedr. dette krav. Det bør kunne sikres gennem implementering af krav 6, 7.2 og 7.3. Implementeringen af dette krav vil ligeledes kunne afspejles i virksomhedens sikkerhedskultur.

7.2. Ledelsens evaluering

7.2.1. På baggrund af virksomhedens opnåede resultater i forhold til de opstillede sikkerhedsmål, resultaterne af overvågningen, analyse af hændelser, afvigelser, fejl og mangler opstået i forbindelse med driften samt andre relevante informationer skal virksomhedens øverste ledelse mindst en gang om året evaluere virksomhedens overordnede sikkerhedsmæssige niveau og sikkerhedsledelsessystemet for at sikre, at sikkerhedsledelsessystemet fortsat er hensigtsmæssigt.

7.2.2. Evalueringen skal behandle eventuelle behov for ændringer i risikoprofil, sikkerhedspolitik, sikkerhedsmål og handlingsplaner samt processer m.v. i sikkerhedsledelsessystemet.

7.2.3. Evalueringen, grundlaget for denne og de beslutninger, der tages i forbindelse med ledelsens evaluering, skal dokumenteres.

Ledelsens evaluering er topledelsens evaluering af sikkerhedens overordnede tilstand i virksomheden.

Formål

Formålet med ledelsens evaluering er at evaluere det overordnede billede af, hvorledes det går med sikkerheden i virksomheden. Er mål nået, er nye risici identificeret, hvilken vej går trends, er sikkerhedsledelsessystemet hensigtsmæssigt, etc.

På baggrund heraf skal der identificeres og iværksættes handlinger for at opretholde eller forbedre sikkerhedsniveauet. Eksempelvis opstilling af nye mål og handlingsplaner, ny politik, justering af sikkerhedsledelsessystemet etc.

Ledelsens evaluering skal som udgangspunkt ikke håndtere enkeltsager, men vurdere det overordnede billede af hvad vej sikkerheden går.

Ledelsens evaluering erstatter ikke den daglige / løbende kontakt mellem driften og den øverste ledelse, men er det forum, hvor de overordnede linjer behandles. Problemer, der opstår i det daglige skal naturligvis håndteres løbende.

Deltagere

Evalueringen skal som minimum foretages af den øverste ledelse, dvs. med deltagelse af direktionen. Det engagement den øverste ledelse forventes at udvise (jf. krav 2.1), udvises bl.a. ved aktiv deltagelse i ledelsens evaluering.

Frekvens for afholdelse af ledelsens evaluering

Ledelsens evaluering skal foretages minimum én gang årligt, men såfremt virksomheden finder det hensigtsmæssigt, kan den afholdes oftere.

Procedure/Metode

Ledelsens evaluering består grundlæggende af 3 trin:

1. Input / Forberedelse
2. Møde
3. Output / Beslutninger og handlinger

1. Input / Forberedelse

Ledelsens evaluering skal baseres på en præsentation / fremstilling af data, som skal give et statusbillede af, hvordan det går med sikkerheden i virksomheden. Det er typisk sikkerhedschefen, der forbereder input, fremsender det, og gennemgår det på mødet for ledelsens evaluering.

Inputtet til ledelsens evaluering skal være dokumenteret, og det bør udsendes til ledelsen i god tid inden mødet, således at ledelsen kan sætte sig ind i materialet som forberedelse til mødet. Ledelsen evaluering skal ikke være "et digert værk", men bør være kortfattet og overskuelig. Det anbefales at anvende tabeller og grafer til f.eks. at illustrere trends.

Som minimum skal evalueringen baseres på følgende grundlag/input:

- **Sikkerhedsmålenes status**. Er sikkerhedsmålene nået? Såfremt målene ikke er nået, evt. en status på handlingsplanerne for sikkerhedsmålene, er handlingsplanerne gennemført som planlagt, eller er der udeståender, og hvilke årsager har der været som forhindrede at målene blev nået.
- **Resultaterne af overvågningen**. Dette drejer sig om målte sikkerhedsindikatorer, resultater af gennemførte operationelle inspektioner samt interne audits. Dette skal være præsentation af samlede data grupperet i kategorier, herunder årsager. Data fra de foregående år medtages, således at eventuelle trends og generelle / større problemer og risici kan udledes. Enkeltsager skal kun gennemgås, hvis de er af en hvis størrelse eller hvis sagen kan være relevant af anden årsag, f.eks. hvis dens konsekvenser har stor betydning for sikkerheden.

- **Analyse af hændelser, fejl og mangler mv**. Forberedelse hertil bør være en gennemgang af udviklingen i hændelser samt alle afvigelser, fejl og mangler der er registreret løbende i drift og vedligeholdelse mv. Dette skal ligeledes være præsentation af samlede data grupperet i kategorier, herunder årsager. Data fra de foregående år medtages, således at eventuelle trends og generelle / større problemer og risici kan udledes. Enkeltsager skal kun gennemgås, hvis de er af en hvis størrelse eller hvis sagen kan være relevant af anden årsag, f.eks. hvis dens konsekvenser har stor betydning for sikkerheden.

Hvis der i ovenstående viser sig trends, der går i den forkerte retning, bør der foretages en analyse af disse trends, således at årsagerne kan afdækkes og præsenteres i inputtet.

Andre relevante informationer**,** som bør evalueres, er:

- Et samlet billede af ændringer i risikoprofilen. Information om ændringer i risikoprofilen er især relevant, hvis disse er afstedkommet af ændringer i virksomhedens aktiviteter. Ændringer i risikoprofilen bør foretages løbende, så her skal blot gives et samlet billede til brug for vurderingerne på ledelsens evaluering.
- Vurdering af overvågningsstrategien. For at sikre den bedst mulige sammenhæng mellem datagrundlag og sikkerhedsrelaterede beslutninger, bør ledelsen forholde sig til om virksomhedens overvågningsstrategi er velegnet som grundlag for generering af relevante data.

Små virksomheder kan sagtens opsamle data og udlede trends, selvom de ikke har mange data. Få data kan også give et fingerpeg om, hvor eventuelle problemer findes og hvilken vej eventuelle trends går. For virksomheder, der udfører opgaver for jernbanevirksomheder eller infrastrukturforvaltere, er det kun et krav, at ledelsens evaluering vedrører aktiviteterne ifm. kørslen (jf. krav 1.1), og den vil ikke nødvendigvis være særlig omfattende.

2. Møde

På mødet gennemgås materialet, der danner grundlaget for evalueringen. På baggrund af materialet og input fra deltagerne evalueres virksomhedens overordnede sikkerhedsmæssige tilstand, herunder om der er eventuelle større eller ændrede problemer og risikoområder samt om sikkerhedsledelsessystemet er hensigtsmæssigt.

Formålet er at vurdere og beslutte hvordan sikkerhedsniveauet fastholdes eller forbedres.

Der skal som minimum tages beslutninger om behov for ændringer i:

- **Risikoprofil**. Giver identificerede trends anledning til et fornyet risikobillede, eller lignende?
- **Sikkerhedspolitik**. Er den fortsat relevant, og udtrykker ledelsens holdning? Er der identificeret problem-/risikoområder, der vil kunne imødegås ved ændringer i sikkerhedspolitikken?
- **Sikkerhedsmål og handlingsplaner**. Hvis f.eks. nye problemer / risikoområder er identificeret, bør der opstilles nye mål og handlingsplaner, eller hvis eksisterende mål er nået, kan virksomheden måske blive endnu bedre?
- **Sikkerhedsledelsessystemet**. Dette kan både være ændringer i enkeltprocedurer eller i hele systemstrukturen, tilgangen for brugerne eller andet hvis f.eks. intern audit har fundet, at systemet ikke anvendes i virksomheden fordi det er for komplekst.

3. Output / Beslutninger og handlinger

Beslutningerne taget ved ledelsens evaluering skal dokumenteres i et referat eller tilsvarende. Såfremt der i inputtet til ledelsens evaluering er anbefalinger til ledelsen, som det vælges ikke at gennemføre, skal dette også dokumenteres med en begrundelse for fravalget.

Alle beslutninger om ændringer skal dokumenteres, f.eks. i handlingsplaner, herunder med angivelse af hvem der har ansvaret for, at ændringerne gennemføres.

Proces (/skabelon)

Det anbefales, at virksomheden udarbejder en tjekliste eller skabelon til det input, der skal anvendes ved ledelsens evaluering, således at det sikres, at alle relevante data medtages. Ansvaret for at forberede præsentationen skal ligeledes fremgå.

Endvidere bør virksomheden udarbejde en fast dagsorden til mødet, for at sikre, at alle punkter bliver behandlet under mødet.

Endelig skal virksomheden sikre, at de handlinger, der skal foregå efter ledelsens evaluering, bliver gennemført. Såfremt, der ved ledelsens evaluering er identificeret forhold, som der skal undersøges nærmere og evt. opstilles korrigerende handlinger for, skal virksomheden sikre, at disse i relevant omfang håndteres iht. krav 7.3.

7.3. Afvigelser og korrigerende handlinger

7.3.1. Sikkerhedsledelsessystemet skal sikre, at fejl og uoverensstemmelser identificeret af virksomheden selv iht. 5.5, 5.6, 5.7, 6.2, 6.3, 6.4 og 6.5, såvel som uoverensstemmelser identificeret af myndigheder og andre relevante eksterne parter analyseres med henblik på at finde årsagen til forholdet.

7.3.2. Herunder skal det fastlægges, om der er lignende forhold, eller om sådanne vil kunne opstå andre steder i systemet eller organisationen.

7.3.3. Sikkerhedsledelsessystemet skal sikre, at korrigerende handlinger planlægges og gennemføres for at eliminere årsagen og undgå gentagelse.

7.3.4. Sikkerhedsledelsessystemet skal sikre, at effektiviteten af de korrigerende handlinger evalueres.

7.3.5. Sikkerhedsledelsessystemet skal sikre, at årsagsanalyser, handlingsplaner, korrigerende handlinger og opfølgning på disse er dokumenteret.

Alle identificerede fejl og uoverensstemmelser, jf. de foregående krav, skal analyseres med henblik på at finde årsagen til forholdet. Dette omfatter alle fejl og uoverensstemmelser identificeret af virksomheden selv, samt uoverensstemmelser identificeret af myndigheder og andre relevante eksterne parter.

Det anbefales, at virksomheden etablerer et system til registrering og håndtering af disse forhold. Dette kan f.eks. være i form af en database, et regneark, eller blanketter / skabeloner, der udfyldes og lægges på et bestemt drev eller lignende. Således vil det være lettere at skabe et overblik over åbne forhold, og det kan sikres og dokumenteres, at alle forhold behandles, og efterfølgende korrigerende handlinger gennemføres og evalueres.

Virksomheden kan overveje at udarbejde en samlet proces, som gælder generelt for alle typer af identificerede forhold. Uanset hvor et forhold er konstateret, er principperne for analyse og korrigerende handlinger etc. de samme. (Denne proces vil med stor sandsynlighed kunne gælde så bredt, at den også kan bruges i virksomhedens kvalitetsstyringssystem og/eller miljøledelsessystem, hvis det er relevant).

Processen skal som minimum indeholde følgende trin:

1. Undersøgelse / Årsagsanalyse

Forholdet undersøges og analyseres med henblik på at finde årsagen – eller årsagerne – til forholdet. Inputtet til analysen er de data, der er registreret i forbindelse med et observeret forhold.

Først bør problemets omfang undersøges. Det skal afdækkes, hvorvidt de registrerede forhold kan opstå / er opstået andre steder i virksomheden eller dens omgivelser end der, hvor det umiddelbart er registeret. Med dette menes, at hvis der f.eks. er konstateret en bestemt fejl på et tog, kan det være at den samme fejl også findes på andre tog af samme type, eller evt. på tog af en anden type.

Når årsagen til et givet forhold skal findes, er det væsentligste at spørge hvorfor det er sket. Det kan være nødvendigt at stille spørgsmålet flere gange, således at man kommer ned til den reelle/bagvedliggende årsag. Det kan her også være nødvendigt at indsamle flere data, hvis datagrundlaget ikke er tilstrækkeligt til at drage konklusioner.

Vær opmærksom på, at der kan være flere årsager samtidig, og disse kan have forskellig betydning / vægtning for forholdet.

Det er vigtigt at "gå efter bolden – og ikke efter manden". Årsager vil ofte ikke bunde i personlige forhold, men i andre forhold hos virksomheden.

I nogle tilfælde kan årsagen skyldes forhold, som virksomheden ikke har indflydelse på, f.eks. en uheldig placering af et signal, så det er svært at se. Hvor det vurderes relevant bør virksomhederne således samarbejde om at eliminere årsager til disse forhold.

Metode til årsagsanalyse skal fastsættes af virksomhedens selv og metoden skal forankres i sikkerhedsledelsessystemet. Virksomheden bør udarbejde f.eks. instruktioner, skabeloner og hjælpeværktøjer, til brug for udarbejdelse af årsagsanalyser.

2. Korrigerende handlinger

Korrigerende handlinger skal gennemføres for at sikre, at årsagen til et givet forhold elimineres og samme forhold ikke vil opstå igen.

Bemærk, at hvis man blot afhjælper et forhold, ved f.eks. at kalibrere et værktøj, der er fundet "ikke kalibreret", har man ikke foretaget korrigerende handlinger. Her skal man ved hjælp af årsagsanalyse finde årsagerne til, at værktøjet ikke var kalibreret; måske er proceduren ikke hensigtsmæssig eller ikke implementeret. Den korrigerende handling kan så være at rette proceduren eller sørge for at medarbejderne kender til den.

For alle korrigerende handlinger er det vigtigt at opstille handlingsplaner eller lignende, hvor aktiviteter og ansvaret for disse er fastlagt. Det vil typisk være en fagchef, der har ansvaret for at gennemføre korrigerende handlinger. Dvs. ikke sikkerhedschefen, med mindre det er konstateret inden for dennes område.

En handlingsplan skal dokumenteres og som minimum indeholde:

- Formål (hvad skal opnås med handlingsplanen)
- Aktiviteter med tilhørende tidsplan og ansvarlige for gennemførelse af de enkelte aktiviteter
- Ansvar for opfølgning på handlingsplanen, jf. nedenfor

Hvor eksterne parter er involveret i gennemførelse af handlingsplanen, skal parterne aftale skriftligt, hvem der har ansvaret for gennemførelse af de enkelte handlinger.

Ved ændringer i handlingsplaner skal relevante interne og eksterne parter informeres.

3. Opfølgning på korrigerende handlinger

Virksomheden skal følge op på de korrigerende handlinger. Opfølgningen skal dokumenteres og som minimum omfatte:

- Opfølgning på korrigerende handlinger for at sikre, at de gennemføres.
- Opfølgning på om handlingsplanen gennemføres korrekt og indenfor den fastlagte tidsplan.
- Opfølgning på om det forventede resultat er opnået og kan fastholdes. Dette kan gøres ved at overvåge, om det forhold man har søgt at fjerne, kommer igen inden for en given tidshorisont.
- Vurdering af om de oprindelige forhold i mellemtiden har ændret sig, og om de aktiviteter, der er fastlagt i handlingsplanen stadig er hensigtsmæssige eller om andre korrigerende handlinger er nødvendige.

Opfølgning på korrigerende handlinger er normalt sikkerhedschefens ansvar.

Bilag

Krydsreferencetabel: Bek. 712, Bek. 147, Bek. 13/14 og ISO 9001:2015

Bek. 712/147	Bek. 13	Bek. 14	ISO 9001:2015
1.1	§ 11, § 18	§ 12, § 19	4.1
1.2	§ 13, Krav 1 og 5	§ 14, Krav 1 og 5	4.2
1.3	§ 11	§ 12	4.3, 6.1
1.4	§ 9	§ 10	4.4
2.1	(§ 14)	(§ 15)	5.1, 7.1
2.2	§ 10	§ 11	5.2
2.3	§ 14, § 15	§ 15, § 16	5.3
3.1	(§ 11, § 18)	(§ 12, § 19)	6.1
3.2	§ 12	§ 13	6.2
4.1	§ 14	§ 15	7.2
4.2	§ 17, Krav 3 og 4	§ 18, Krav 3 og 4	7.2
4.3	—	—	7.3
4.4	§ 16	§ 17	7.4
4.5	§ 21	§ 22	7.5, 6.3
5.1	Krav 6	Krav 6	8.5, 8.6
5.2	§ 18, Krav 2	§ 19, Krav 2	8.1, 8.5
5.3	Krav 7	Krav 7	8.5, 8.6
5.4	§ 20	§ 21	8.2
5.5	§ 22	§ 23	8.7
5.6	§ 22	§ 23	8.7
5.7	(§ 22)	(§ 23)	8.7
5.8	Krav 8	Krav 8	8.4
5.9	§ 13, Krav 1 og 5	§ 14, Krav 1 og 5	8.2
5.10	§ 19	§ 20	8.2, 8.3, 8.5
5.11	—	—	8.6
6.1	—	—	9.1
6.2	(§ 24)	(§ 25)	9.1
6.3	(§ 24)	(§ 25)	8.2, 8.3
6.4	(§ 23)	(§ 24)	9.2
6.5	§ 23	§ 24	9.2
7.1	§ 22	§ 23	10.1, 10.3
7.2	§ 24	§ 25	9.3
7.3	§ 22, § 23	§ 23, § 24	10.2

Trafik-, Bygge- og Boligstyrelsen
Carsten Niebuhrs Gade 43
DK-1577 København V

tilsyn@tbst.dk
www.tbst.dk

Vejledning i Sikkerhedsledelse