Trafikstyrelsen
Danish Transport Authority

Vejledning i udformning af systemdefinition

Version 3 / 8. maj 2014

Indhold

1) Indledning

Formål med vejledningen

Bekendtgørelserne om ibrugtagning af infrastruktur og rullende materiel[1] fastsætter, at systemdefinitionen, eller en foreløbig systemdefinition, er obligatorisk dokumentation, når virksomheder søger om ibrugtagningstilladelse eller forelægger ændringer for Trafikstyrelsen.

Vejledningen angiver retningslinjer for, hvad en systemdefinition bør indeholde. Kravene til indholdet i en systemdefinition er fastsat i CSM-RA[2] bilag I.

Vejledningen henvender sig til den personkreds i jernbanevirksomheder, hos infrastrukturforvaltere, vedligeholdelsesansvarlige og fabrikanter, der har ansvar for udarbejdelse af systemdefinitioner. Vejledningen henvender sig desuden til de assessorer, som assesserer anvendelsen af CSM-RA-metoden.

Indhold i vejledningen

Vejledningen afspejler den praktiske anvendelse af systemdefinitionen som redskab i risikostyringsprocessen og godkendelsesprocessen. Vejledningen angiver desuden retningslinjer for, hvad en systemdefinition skal og bør indeholde.

Vejledningen suppleres af tre bilag, som kan finde i *Bilag til vejledning i udformning af systemdefinition,* som udgives samtidig med *Vejledning i udformning af systemdefinition*:

- Bilag 1. Råd om, hvad der bør medtages i en systemdefinition.
- Bilag 2. Inspiration til udfærdigelse af tjekliste, som kan anvendes i forbindelse med forslagsstillers kvalitetssikring af systemdefinitionen.
- Bilag 3. Referenceliste.

Når der i vejledningen skrives *ændring*, menes der følgende med mindre andet fremgår af sammenhængen:

- en ændring af et eksisterende delsystem, eller
- et nyt delsystem/eller element i et nyt delsystem[3]

Formål med systemdefinitionen

Formålet med systemdefinitionen er at beskrive og afgrænse det system (analyse objekt), som er genstand for en risikovurdering. Formålet er også at dokumentere sikkerhedskravene til systemet.

[1] Bekendtgørelse nr. 1187, om ibrugtagningstilladelse for delsystemer i jernbaneinfrastrukturen af 12.12.2012 og bekendtgørelse nr. 56 om godkendelse af køretøjer på jernbaneområdet af 24.1.2013.

[2] Kommissionens forordning (EF) Nr. 352/2009 af 24. april 2009 om vedtagelse af en fælles sikkerhedsmetode til risikoevaluering og -vurdering, også kaldet CSM-RA.

[3] På infrastrukturområdet er det f.eks. anlæggelsen af en perron på et sted, hvor der ikke i dag er en perron.

I systemdefinitionen beskrives det nye delsystem eller de ændringer, der foretages i et eksisterende delsystem. Derudover beskrives grænsefladerne til andre delsystemer i det samlede jernbanesystem, samt, når det er relevant, grænsefladen mellem, hvad der er en del af jernbanesystemet, og hvad der ikke er.

En systemdefinition skal som minimum omhandle følgende områder[4]:

a) *En systemmålsætning, f.eks. det tilsigtede formål*

b) *Systemfunktioner og -elementer, når dette er relevant (herunder eksempelvis menneskelige, tekniske og operationelle elementer)*

c) *Systemafgrænsning, herunder vekselvirkninger med andre systemer*

d) *Fysiske (dvs. vekselvirkende systemer) og funktionelle (dvs. funktionelt input og output) grænseflader*

e) *Systemmiljøet (f.eks. energi- og varmestrømme, stød, vibrationer, elektromagnetisk interferens, operationel anvendelse)*

f) *Eksisterende sikkerhedsforanstaltninger og, efter en iterativ proces, definition af de sikkerhedskrav, der er identificeret i forbindelse med risikovurderingsprocessen*

g) *Antagelser med henblik på at afgrænse risikovurderingen.*

I CSM-RA anvendes betegnelsen *foreløbig systemdefinition* om den systemdefinition, som anvendes, når virksomheden afgør, om en ændring er signifikant. Den foreløbige systemdefinition kan betragtes som en indledende systemdefinition, hvor alle tilgængelige oplysninger om ændringen og det system, som ændringen skal udføres i, beskrives.

I den foreløbige systemdefinition indgår altså en beskrivelse af de samme emner, som i de senere systemdefinitioner. Kun anden del af *f) eksisterende sikkerhedsforanstaltninger og, efter en iterativ proces, definition af de sikkerhedskrav, der er identificeret i forbindelse med risikovurderingsprocessen* må afvente, at risikovurderingsprocessen er gennemført.

I denne vejledning anvendes desuden begrebet *endelig systemdefinition.* Med *endelig* menes den systemdefinition som kan laves for systemet, når ændringen er gennemført.

Læs mere om den *foreløbige* og den *endelige* systemdefinition i bilag 1 i *Bilag til vejledning i udformning af systemdefinition*.

Områderne a) – f) beskrives i kapitel 2.

Systemdefinitionen danner grundlag for bedømmelsen af, hvordan jernbanesikkerheden påvirkes, efter at ændringen er udført.

Systemdefinitionen indeholder de nøgleoplysninger om systemet/delsystemet, der er nødvendige for at få en forståelse af potentielle risici og

[4] jf. CSM-RA, bilag I, § 2.1.2

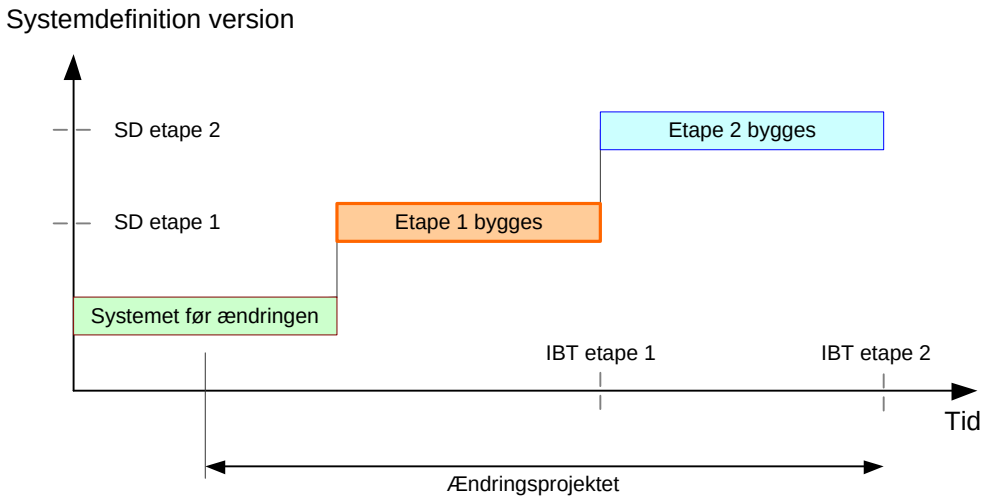
sikkerhedsforanstaltninger. Systemdefinitionen er altså *ikke* en deltaljeret beskrivelse af projektets aktiviteter og dets praktiske gennemførsel.

Bemærk, at systemdefinitionen ikke kun er en *beskrivelse* af systemet og ændringen. Der er et element af analyse i systemdefinitionen. Uden dette ville det f.eks. ikke være muligt at beskrive systemets grænseflader.

Detaljeringsgraden afhænger af ændringens karakter. Systemdefinitionen bør kunne læses som et selvstændigt dokument, gerne suppleret med tegninger, fotografier, lister mv.

Systemdefinitionen skal beskrive baggrunden for den planlagte ændring på følgende måde:

> (a) hvis den planlagte ændring er en ændring af et eksisterende system, skal systemdefinitionen både beskrive systemet inden ændringen og den planlagte ændring.
>
> (b) hvis den planlagte ændring er et nyt system, er beskrivelsen begrænset til definitionen af systemet.



Figur 1: Eksempel på et forløb, hvor et jernbanesystem skal idriftsættes flere gange[5].

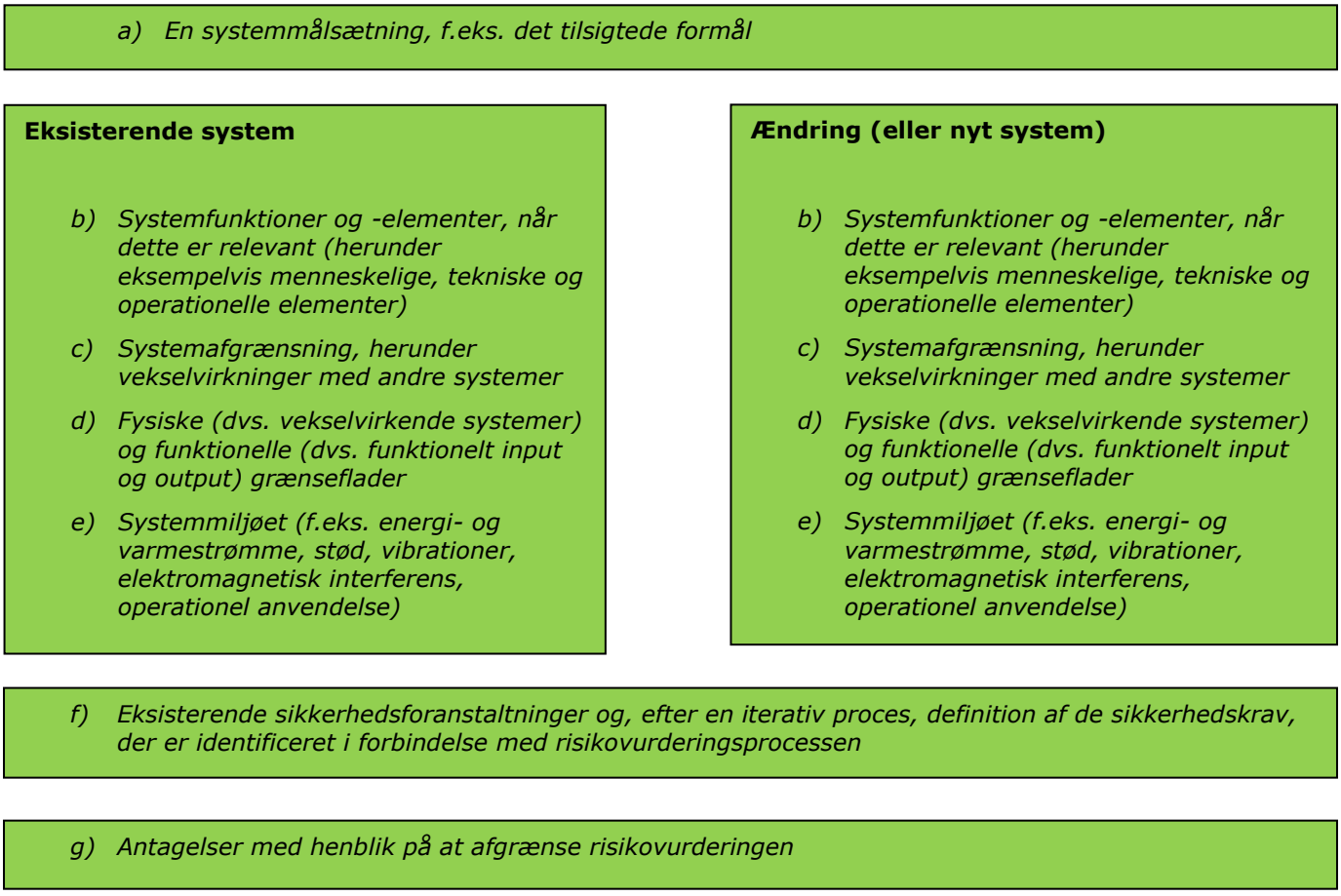
Større ændringer, der ibrugtages etapevis jf. figur 1, bør have en systemdefinition for hver etape. Ved ansøgning om ibrugtagningstilladelse til den enkelte etape vedlægges den relevante systemdefinition. Det bør fremgå af systemdefinitionen, hvordan den aktuelle etape passer ind i den overordnede ændring.

[5] Bemærk, at for f.eks. konstruktionsprojekter og for sikkerhedsmæssige ændringer i trafikafviklingen, er tegningen misvisende, da sådanne ændringer ofte får ibrugtagningstilladelse før en etape igangsættes og ikke efter.

2) Hvad skal beskrives i en systemdefinition?

I dette kapitel beskrives de områder, som skal beskrives i systemdefinitionen. Disse områder er ikke tænkt som en indholdsfortegnelse. I kapitel 3 og i bilag 1 gives vejledning i, hvorledes indholdet i en systemdefinition kan struktureres.

Figur 2 illustrerer de obligatoriske områder, der skal behandles i en systemdefinition.



Figur 2: illustration af de områder, der skal behandles i en systemdefinition og deres indbyrdes forhold

I Figur 2 er punkterne b) til e) vist to gange for at illustrere, at i de tilfælde, hvor et eksisterende system ændres, skal systemdefinitionen både beskrive systemet inden ændringen og den planlagte ændring.

Hvilket delsystem skal der tages udgangspunkt i?

I *system*defintionen beskrives *system*målsætningen, *system*funktioner, *system*elementer, *system*afgrænsningen, samt *system*miljøet.

Det del*system,* som der tages udgangspunkt i, i systemdefinitionen, er "en del af det system, der vurderes, som udgør en specialiseret funktion"[6]. Man kan altså ikke nøjes med at anvende den opdeling i delsystemer, som fremgår af Interoperabilitetsdirektivets bilag II[7], når man afgrænser sit delsystem. Afgrænsningen skal være mere snæver. Man kan f.eks. ikke nøjes med at afgrænse sig til "infrastrukturen", som er et delsystem i Interoperabilitetsdirektivets bilag II, når man ønsker at udføre en ændring i infrastrukturen. Man skal også afgrænse sig fra, om man i forbindelse med ændringen kan komme til at påvirke spor, sporkasse, overkørselsanlæg, konstruktioner eller andre elementer i jernbaneinfrastrukturen.

Der er dog alligevel en fordel i – i forbindelse med systemafgrænsningen – at anvende interoperabilitetsdirektivets opdeling i delsystemer som udgangspunkt. Dette skyldes, at Trafikstyrelsen i forbindelse med en evt. ibrugtagningstilladelse vil tage udgangspunkt i Interoperabilitetsdirektivets opdeling i delsystemer. Det anbefales derfor, at forslagsstiller i systemdefinitionen først afgrænser sit delsystem ved at følge opdelingen i Interoperabilitetsdirektivets bilag II og derefter yderligere afgrænser sit delsystem.

Læs mere om dette ved gennemgangen af område *c) Systemafgrænsning, herunder vekselvirkninger med andre systemer* længere fremme i dette kapitel.

<u>Beskrivelse af delsystemet før og efter</u>

I de tilfælde, hvor der foretages en ændring af et eksisterende system, er beskrivelsen af systemet før ændringen nødvendig, fordi den er grundlag for, at man kan argumentere for, at jernbanesikkerheden ikke påvirkes negativt af ændringen. Har man ikke en beskrivelse af det system, som ændringen foretages i, men blot en beskrivelse af, hvordan ændringen konkret skal foretages, kan man ikke bedømme den sikre integration af ændringen og derved, hvordan jernbanesikkerheden påvirkes af ændringen.

Et simpelt eksempel illustrerer nødvendigheden af en tilstrækkelig systembeskrivelse: Ønsker man f.eks. at forlænge en perron, skal systemdefinitionen inkludere en beskrivelse af den nuværende udformning af perronkant og perronhøjde. Desuden skal den indeholde en beskrivelse af andre forhold, der kan have sikkerhedsmæssig betydning.

Hvis disse forhold ikke er med i beskrivelsen, er det ikke muligt at vurdere, om perronforlængelsen introducerer nye farer, som påvirker jernbanesikkerheden. Det vil f.eks. kunne ske, hvis den nye forlængede perron har en væsentlig anden afstand til spormidten, en væsentlig anden højde, eller en krumning, der vanskeliggør oversigtsforhold i forbindelse med afgang. Herved forøges risikoen for, at passagererne kommer til skade, når de skal ind og ud af toget.

[6] Jf. side 17 i ERA's: *Vejledning i anvendelse af Kommissionens forordning om vedtagelse af en fælles sikkerhedsmetode med hensyn til risikoevaluering og -vurdering som anført i artikel 6, stk. 3, litra a), i jernbanesikkerhedsdirektivet.*

[7] Jf. side 17 i ERA's: *Vejledning i anvendelse af Kommissionens forordning om vedtagelse af en fælles sikkerhedsmetode med hensyn til risikoevaluering og -vurdering som anført i artikel 6, stk. 3, litra a), i jernbanesikkerhedsdirektivet.*

I det følgende uddybes de enkelte emner vist i figur 2:

a) En systemmålsætning, f.eks. det tilsigtede formål

Systemmålsætningen indeholder en beskrivelse af formålet med systemet. Hvad skal det kunne? Systemmålsætningen er f.eks. systemets ydeevne og andre specifikationer.

Er der tale om en ændring, bør det uddybes, hvad formålet med ændringen er. Hvad skal systemet kunne, som det ikke kunne før?

Målsætningen bør omfatte overvejelser om det sikkerhedsmål, der er fastsat. Er det f.eks. ønsket, at ændringen skal forbedre eller bevare sikkerheden?

Et konkret eksempel kunne være, at formålet med en ændring er at gennemføre en perronforlængelse for at kunne betjene længere tog. Sikkerhedsmålet er, at sikkerhedsniveauet bevares.

Er der tale om en ny bane eller strækning, bør forslagsstiller i systemdefinitionen desuden forholde sig til, om/hvordan banen eller strækningens sikkerhedsmål relaterer sig til det nationale sikkerhedsmål.

b) Systemfunktioner og -elementer, når dette er relevant (herunder eksempelvis menneskelige, tekniske og operationelle elementer)

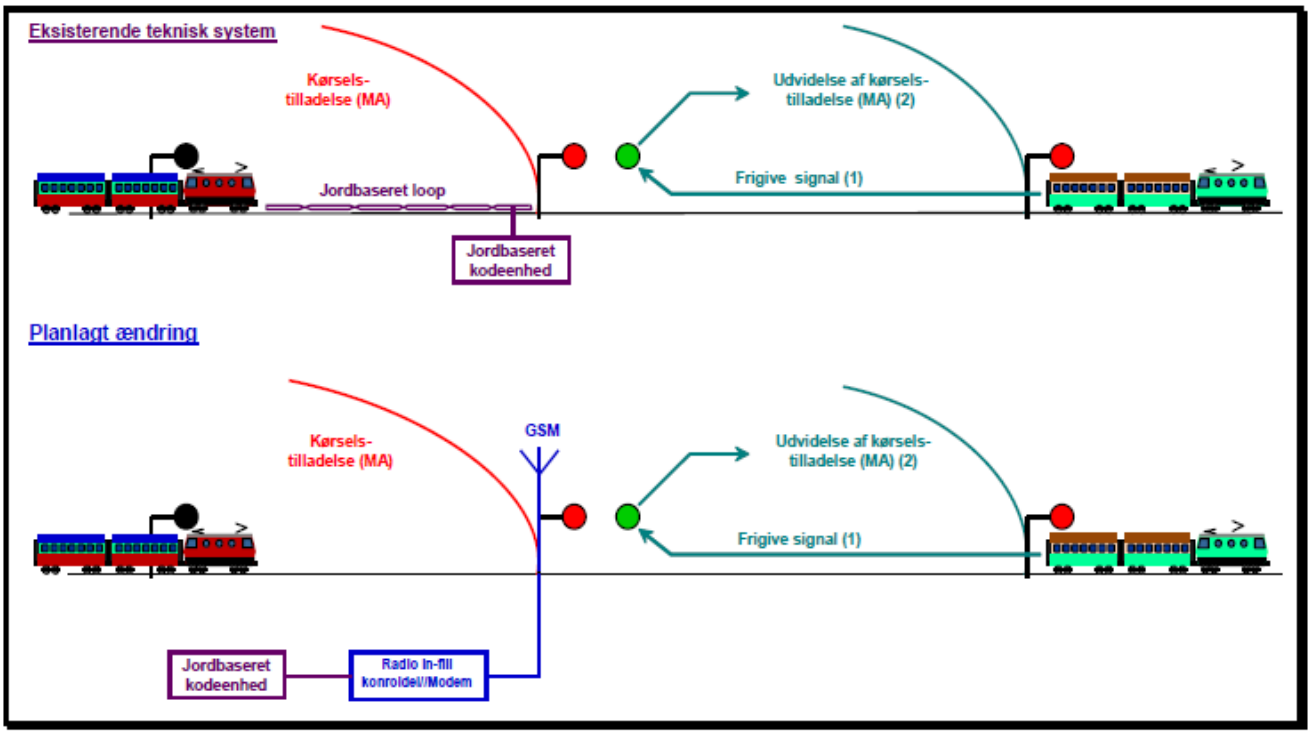
Beskrivelsen af systemets funktioner og elementer bør vedlægges tegninger, som viser systemets elementer og funktioner.

Hvis der er tale om en ændring af et eksisterende system, bør der fokuseres på ændringen, og systemets funktioner og elementer beskrives både før og efter ændringen.

Eksempel: Hvis en ændring f.eks. består i at erstatte et jordbaseret loop placeret før et signal med ”radio infill + GSM”, kan Figur 3 illustrere elementer og funktioner før og efter ændringen.

Sådan en figur bør altid uddybes med en supplerende tekst, der mere detaljeret beskriver funktionaliteten af ændringen[8].

[8] Formålet med denne ændring er bl.a. at opdatere kørtilladelser i førerrummene kontinuerligt i stedet for at være begrænset af den geografisk begrænsede dækning af en jordbaseret kodeenhed.



Figur 3: Eksempel på illustration af systemelementer og systemfunktioner. Ændring af jordbaseret loop til radio infill + GSM[9].

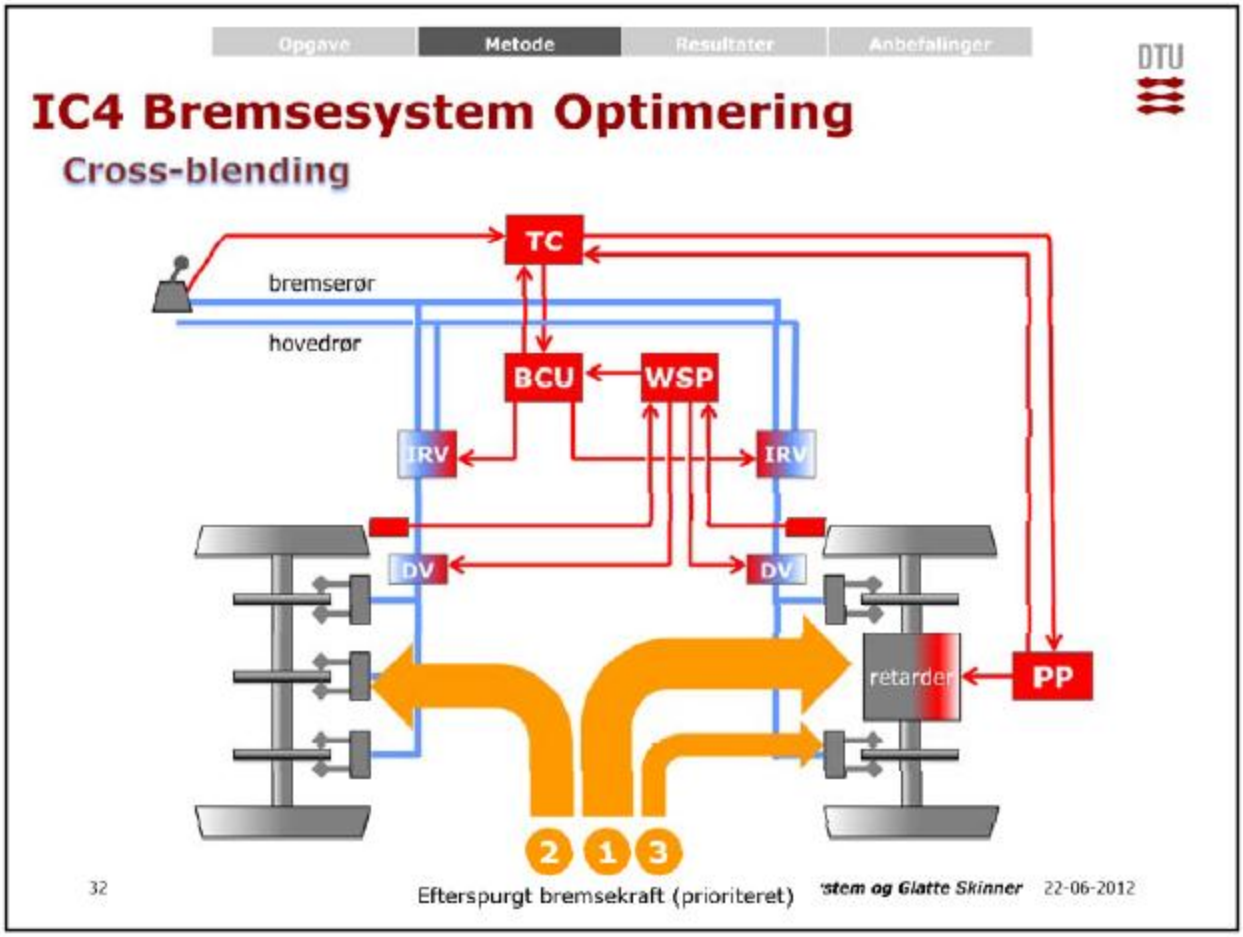
I eksemplet med en perronforlængelse bør den eksisterende perron beskrives, herunder: perronkant, perronhøjde, perronoverflade, afmærkning på perron osv. Hvis der er signaler ved perronen, bør deres eksisterende placering og funktion ligeledes beskrives. Endelig beskrives elementer og funktioner i delsystemet "drift", dvs. den eksisterende driftsafvikling på stationen, herunder hvilke restriktioner der er i forbindelse med anvendelse af den nuværende perron med hensyn til ekspedition af lange tog, f.eks. angivelse af standsningssted, procedurer for ekspedition af lange tog, eller hvilken signalgivning der skal anvendes for lange tog.

Derefter beskrives, hvordan de samme elementer og funktioner vil se ud, når ændringen er gennemført.

Et andet eksempel er IC4 togets bremsesystem, som er analyseret af DTU[10]. Som led i den omfattende analyse af togets bremsesystem har DTU beskrevet, hvilke elementer og funktioner bremsesystemet består af. En motorbogie består af en løbeaksel og en drivaksel. Løbeakslen har 3 bremseskiver og motorakslen har 2 bremseskiver. Se Figur 4:

[9] Figuren er taget fra (ERA) det europæiske jernbaneagenturs *Samling af eksempler på risikovurderinger og nogle mulige værktøjer, der støtter CSM-RA.*

[10] Analyseret i *Undersøgelse af IC4 Bremsesystem og Glatte skinner*. Midtvejsrapportering. DTU. 22.6.2012.



Figur 4: Eksempel på illustration af systemelementer.

Figur 4 viser elementer i togets bremsesystem/motorbogie 1: Togcomputer (TC), Bremsecomputer (BCU), Power Pack (PP), hjulslipsbeskyttelsessystem (WSP) og retarder.

WSP systemet kontrollerer en ”dump valve” (DV) og kan dermed regulere trykket i bremsecylindrene i tilfælde af begyndende blokering. Desuden kobles retarderen ud, hvis der er begyndende blokering på en motoraksel. Bemærk også, at BCUen anvender en såkaldt Integrated Relay Valve (IRV) til at styre trykket i bremsecylinderne.

c) *Systemafgrænsning, herunder vekselvirkninger med andre systemer*

Systemafgrænsningen har til formål at synliggøre, hvad der er med i ”systemet”, og hvad der ligger udenfor.

Forslagsstiller bør tage udgangspunkt i interoperabilitetsdirektivets[11] opdeling af jernbanesystemet i strukturelle og funktionelle delsystemer:

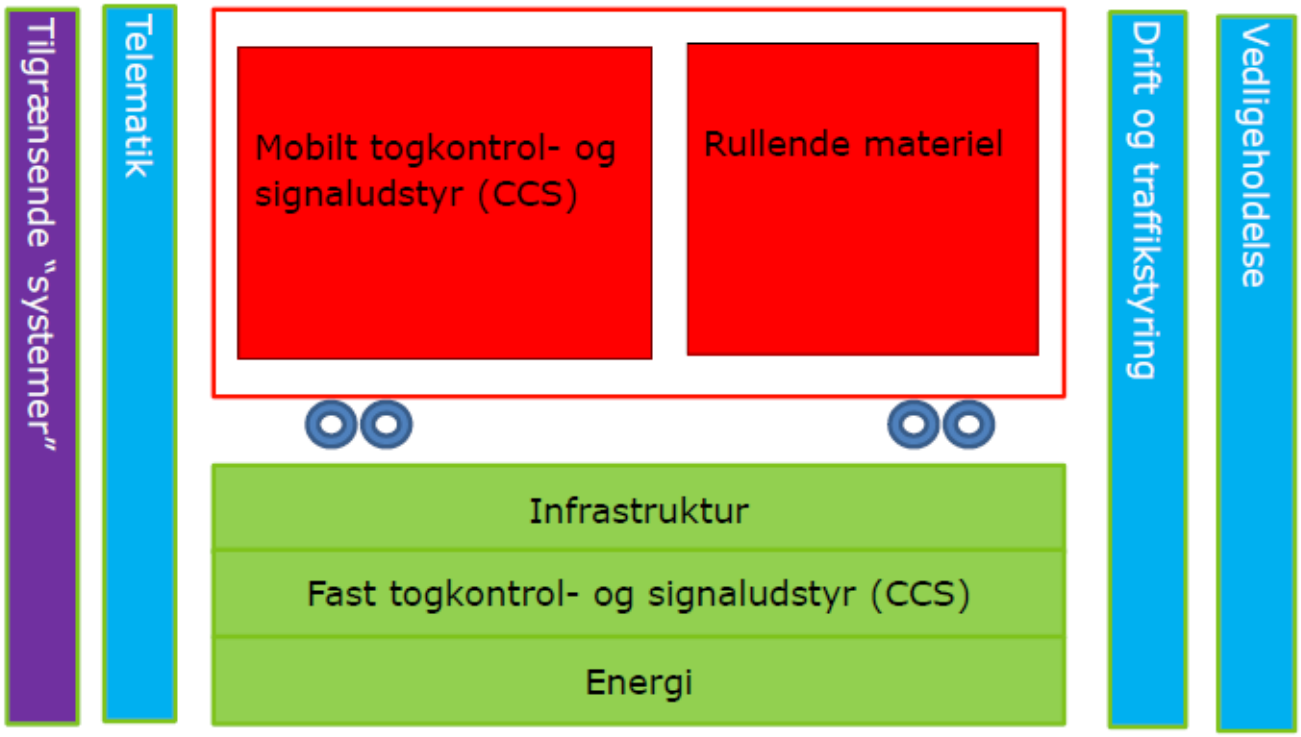
Strukturelle delsystemer:

- infrastruktur
- energi
- fast togkontrol- og signaludstyr
- mobilt togkontrol- og signaludstyr
- rullende materiel

Funktionelle delsystemer:

- drift og trafikstyring
- vedligeholdelse
- trafiktelematik for person- og godstrafikken.

Delsystemerne kan også illustreres, så grænsefladerne mellem et køretøj og de faste anlæg tydeliggøres:



Figur 5: Jernbanesystemets opdeling i strukturelle og funktionelle delsystemer

"Grønne" delsystemer i Figur 5 godkendes iht. infrastrukturbekendtgørelsen[12].

[11] I Interoperabilitetsdirektivet er en overordnet opdeling af jernbanesystemet i funktionelle og strukturelle delsystemer. Delsystemerne kan igen nedbrydes i dele af delsystemer i form af komponenter eller afgrænsede dele af delsystemet. Læs nærmere i Interoperabilitetsdirektivet (2011/18/EU) Annex II.

[12] I overensstemmelse med bekendtgørelse nr. 1187, om ibrugtagningstilladelse for delsystemer i jernbaneinfrastrukturen af 12.12.2012.

Røde delsystemer godkendes iht. Køretøjsbekendtgørelsen[13]. "Blå" delsystemer er funktionelle delsystemer, som sikrer, at de strukturelle delsystemer betjenes og vedligeholdes korrekt, og at information udveksles på fornuftig vis.

De funktionelle delsystemer inddrages i systemdefinitionen for at afdække, om ændringerne i de strukturelle delsystemer kræver ændringer i de funktionelle dele af jernbanesystemet f.eks. i organisation, driftsafvikling eller procedurer[14].

Det "lilla" delsystem dækker de tilgrænsende systemer, som kan påvirke jernbanesystemet. Det kan f.eks. være en gasledning, som er ført under sporet, eller en vejbro over banen.

Systemdefinitionen bør altid beskrive, hvilke af delsystemerne i figur 5, som systemdefinitionen vedrører. Hvis systemdefinitionen vedrører flere delsystemer, skal de beskrives hver for sig. Dette skyldes at EF-verifikationsproceduren (og Trafikstyrelsens godkendelsesbekendtgørelser) retter sig mod godkendelse af delsystemerne vist i figur 5. Grænsefladen mellem de enkelte delsystemer (og deres vekselvirkning/integration) skal ligeledes beskrives.

I eksemplet med perronforlængelsen er det system, som ændringen foretages i, *infrastrukturen.* I afgrænsningen skal forslagsstiller beskrive vekselvirkningen med delsystemet rullende materiel og med procedurerne for drift og trafikstyring.

Bemærk dog, at såfremt der er tale om en ændring af et eksisterende delsystem, er en inddelingen i delsystemer jf. figur 5 ikke alene tilstrækkeligt til at afgrænse ændringen[15]. I det tilfælde bør systemdefinitionen også beskrive de interne grænseflader i det delsystem som ændres.

De interne grænseflader kan f.eks. være mellem spor og sporbærende bro i delsystemet infrastruktur og mellem vognkasse og bogie i delsystemet rullende materiel.

Afgrænsning af ændringen ift. aktiviteter, der ikke påvirker jernbanesikkerheden

Indgår der aktiviteter ifm. ændringen, som ikke påvirker jernbanesikkerheden – f.eks. arbejde med flytning af vejanlæg i nærheden af et areal, hvor der skal etableres en ny bane, så vil en kort beskrivelse af disse aktiviteter hjælpe til at give læseren overblik over hele ændringen. Den tydelige opdeling i aktiviteter, der har betydning for jernbanesikkerheden, og aktiviteter, der ikke har betydning for jernbanesikkerheden, hjælper desuden forslagsstiller, hvis

[13] I overensstemmelse med bekendtgørelse nr. 56 om godkendelse af køretøjer på jernbaneområdet af 24.1.2013.

[14] Bemærk dog, at telematik normalt ikke betragtes som sikkerhedsbærende. Forslagsstiller behøver derfor ikke beskrive dette delsystem i systemdefinitionen.

[15] Jf. side 17 i ERA's: *Vejledning i anvendelse af Kommissionens forordning om vedtagelse af en fælles sikkerhedsmetode med hensyn til risikoevaluering og -vurdering som anført i artikel 6, stk. 3, litra a), i jernbanesikkerhedsdirektivet.*

der skal tilknyttes assessor på ændringen til at tydeliggøre, hvilke dele af et projekt, som er med i assessors scope of work, og hvilke der ikke er.

d) Fysiske (dvs. vekselvirkende systemer) og funktionelle (dvs. funktionelt input og output) grænseflader

Grænseflader mellem det nye eller ændrede delsystem og de andre delsystemer bør være veldefinerede, da det særligt er i grænsefladerne, at der kan opstå farer, som forslagsstiller skal håndtere.

I eksemplet med perronforlængelsen er grænsefladen mellem det rullende materiel og infrastrukturen interessant, og hermed også grænsefladen til de procedurer, der anvendes i forbindelse med drift og trafikstyring.

Ofte vil en ændring ikke bare påvirke ét system, men flere. I sådanne tilfælde er det vigtigt, at man beskriver alle de berørte systemer/delsystemer og deres grænseflader til hinanden.

I eksemplet med perronforlængelsen er det delsystem, som ændringen foretages i, *infrastrukturen*. Indgår flytning af signaler i ændringen, vil ændringen påvirke tre delsystemer: *infrastruktur*, *sikringsanlæg* og *drift*:

- *Infrastruktur* påvirkes, fordi perronen forlænges. Ændres placeringen af togdetekteringsafsnittet, bør denne aktivitet også fremgå af systemdefinitionen.

- *Sikringsanlæg* påvirkes, fordi signaler flyttes. Grænsefladen mellem de tre systemer i form af f.eks. overvejelser omkring placering af signaler ift. perronens endepunkt bør medtages i systemdefinitionen.

- *Drift* påvirkes, hvis signalflytningen betyder, at strækningsoversigt skal opdateres. Hvis perronforlængelse samtidig medfører ændringer i personalets procedurer i forbindelse med standsning ved perron f.eks. omkring aflåsning af døre, bør det også medtages i systemdefinitionen.

Fysiske og funktionelle grænseflader

Der skelnes i CSM-RA imellem fysiske og funktionelle grænseflader. Disse kan være interne i det system der ændres, eller det kan være en grænseflade mellem to af delsystemerne vist i Figur 5.

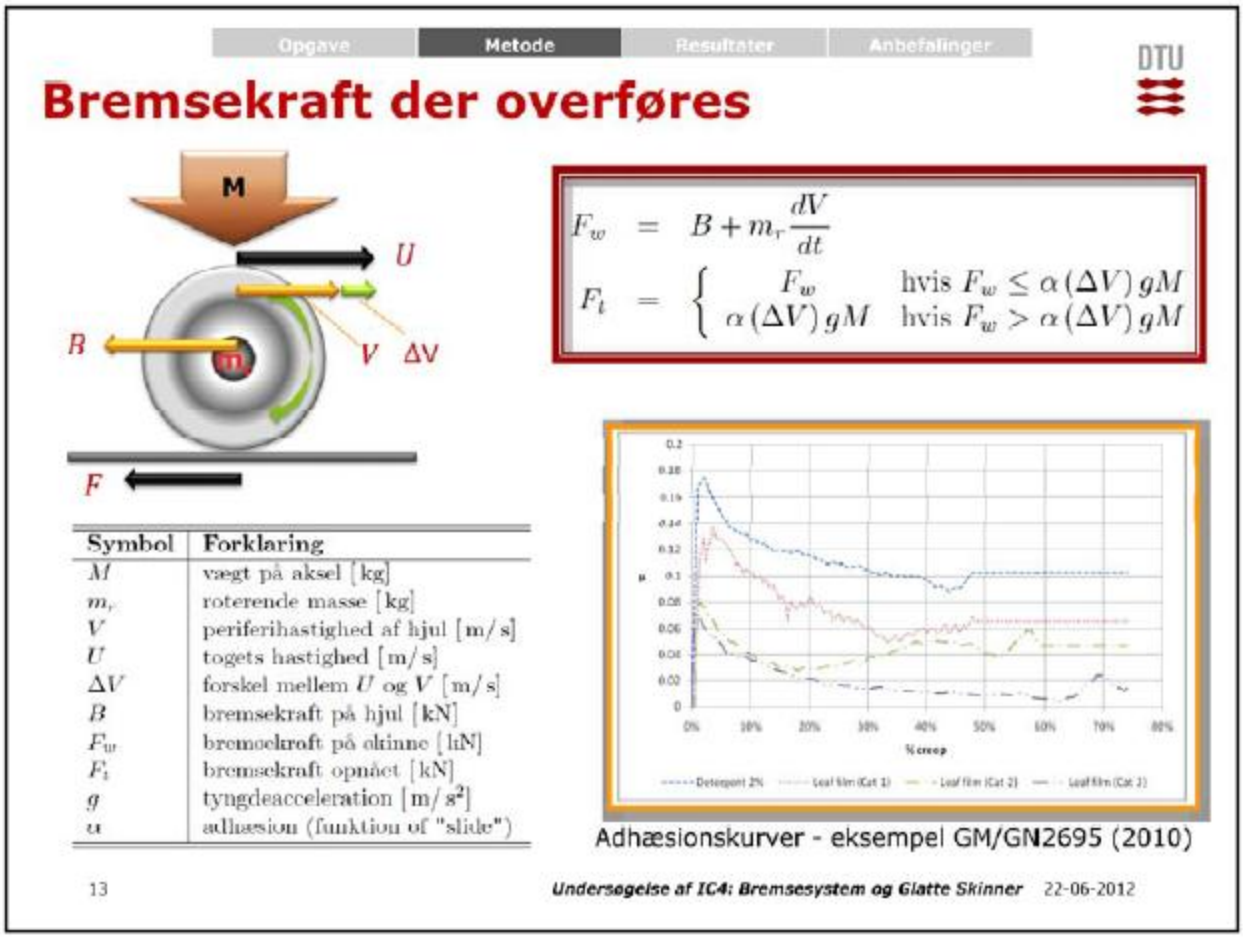
Fysiske grænseflader er grænseflader, hvor to strukturelle delsystemer, eller elementer indenfor et delsystem, fysisk støder op til hinanden. Det kan f.eks. være mellem spor (infrastruktur) og rullende materiel eller mellem et spor og dets nabospor.

Funktionelle grænseflader er grænseflader, hvor der udveksles information, energi eller lignende mellem to delsystemer eller mellem et jernbanesystem og det omgivende system.

Grænsefladerne mellem strukturelle delsystemer og funktionelle delsystemer vil ofte være funktionelle. F.eks. vil køreplan og infrastruktur på en strækning have en funktionel grænseflade ligesom operatørens driftsinstruktion til en bestemt køretøjstype har en funktionel grænseflade til køretøjstypen.

Nogle gange er en grænseflade en funktionel grænseflade såvel som en fysisk grænseflade.

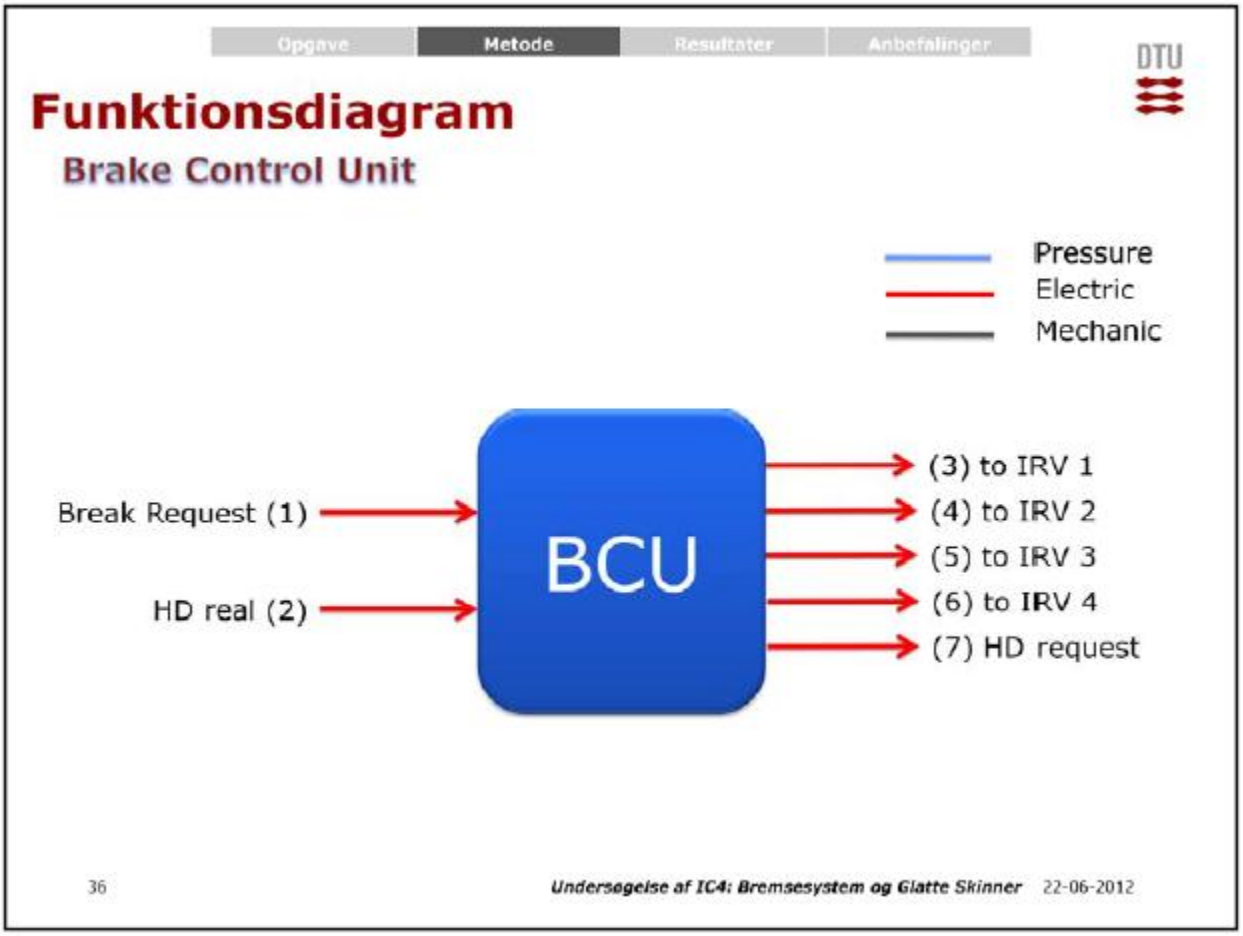
Figur 6 illustrerer grænsefladen mellem hjul og skinne. Grænsefladen er både fysisk, da hjul og skinne rører hinanden, og funktionel, da der overføres bremsekraft mellem hjul og skinne for at bremse toget.



Figur 6: Illustration af et hjul, der nedbremses på skinnen.

Det anbefales, at forslagsstiller laver en eller flere systemtegninger for at illustrere delsystemet/delsystemerne og systemgrænserne. Såfremt der er tale om en ændring, bør ændringen illustreres i forhold til det system der ændres.

Et eksempel på en systemtegning er et funktionsdiagram. Figur 7 viser, hvorledes DTU har illustreret den funktionelle grænseflade for en bremsecomputer (BCU). På tilsvarende vis har DTU beskrevet grænsefladen for de øvrige elementer i systemet vist i Figur 4. Funktionsdiagrammet vist i figur 7 er i DTU's rapport ledsaget af en tekst, der beskriver input/output.



Figur 7: Eksempel på et simpelt funktionsdiagram som viser input- outputsignaler til en bremsecomputer (BCU). HD er en forkortelse for hydrodynamisk bremse. Se også Figur 4

e) Systemmiljøet (f.eks. energi- og varmestrømme, stød, vibrationer, elektromagnetisk interferens, operationel anvendelse)

Systemmiljøet bør beskrives for hvert delsystem, der påvirkes af ændringen.

Systemmiljøet bør beskrives med tanke for systemets livscyklus: design, installation, drift, beredskab, vedligeholdelse og evt. afvikling af systemet.

I beskrivelsen af systemmiljøet angives, hvem der kommer i kontakt med systemet, f.eks. personale, passagerer, håndværkere og brugere af overkørsler, og hvordan denne interaktion skal foregå[16].

Også sammenhængen mellem systemet og systemmiljøet beskrives. F.eks. forholdet mellem trafikbelastning og det elektriske, termiske og mekaniske miljø.

[16] Sammenhængen mellem de funktionelle delsystemer (procedurer, kompetencer, drift og organisation) og de strukturelle delsystemer beskrives i forbindelse med emnet: d) fysiske og funktionelle grænseflader.

Eksempel: Operatøren "gode lyntog" kører nonstop på hovedstrækningen mellem landets største byer. Grundet sporarbejde omlægges driften i en periode, så togene også skal anvendes til regionaltogskørsel med stop ved alle byer på strækningen. Den nye køreplan betyder således, at den operationelle anvendelse af køretøjet ændres, idet der skal bremse mere pr. tur, hvilket igen betyder, at bremseklodserne på toget oftere skal skiftes. Dette forhold vil skulle beskrives i systemdefinitionen.

I eksemplet med perronforlængelsen er det f.eks. relevant, om forlængelsen gør, at perronen nu kan anvendes på en anden måde end før ændringen. Hvis forlængelsen medfører, at perronen får ændrede adgangsveje, og at f.eks. en eksisterende perronovergang derfor vil blive anvendt anderledes end før, er det en ændring i systemmiljøet, som bør beskrives i systemdefinitionen.

f) Eksisterende sikkerhedsforanstaltninger og, efter en iterativ proces, definition af de sikkerhedskrav, der er identificeret i forbindelse med risikovurderingsprocessen

Sikkerhedsforanstaltninger er tiltag, der enten mindsker den relative hyppighed af en fare eller afbøder dens konsekvenser med henblik på at nå frem til eller bibeholde et acceptabelt risikoniveau.[17]

Hvis der er tale om en ændring af et eksisterende system, skal alle relevante eksisterende sikkerhedsforanstaltninger, der findes ved systemet før ændringen, dokumenteres i den første udgave af systemdefinitionen. F.eks. beskyttelsesskinner, sporstoppere, røgalarmer, driftsinstruktionen osv.

Nye sikkerhedsforanstaltninger, som identificeres i forbindelse med risikovurderingsprocessen, skal fremgå af fareregisteret.[18]

Sikkerhedskrav er de nødvendige sikkerhedsegenskaber (kvalitative eller kvantitative) for et system og driften heraf (herunder driftsforskrifter) med henblik på at opfylde lovbestemte eller virksomheders sikkerhedsmål.[19]

Sikkerhedskrav der identificeres i forbindelse med risikovurderingsprocessen, skal dokumenteres, enten som en del af en opdaterede systemdefinition, eller ved en henvisning til relevante dokumenter. Sikkerhedskrav er f.eks.: minimumskrav til hjulmål, afstandskrav mellem perronkant og spor og krav til signalsynlighed.

Det bør tydeligt fremgå af systemdefinitionen, hvilke sikkerhedskrav der er almindeligt kendte i virksomheden, og hvilke sikkerhedskrav der er særlige for ændringen og derfor må forventes at skulle være særlig opmærksomhed omkring for at blive overholdt.

Det anbefales desuden, at der argumenteres tydeligt for afvigelser fra de almindeligt kendte sikkerhedskrav.

[17] Definition, jf. CSM-RA art. 3 (10)
[18] CSM-RA bilag I. 4. 1. 2
[19] Definition, jf. CSM-RA art. 3 (9)

Sikkerhedsrelaterede anvendelsesbetingelser[20] er en variant af sikkerhedskrav. En ændring kan give anledning til nye anvendelsesbetingelser relateret til systemets drift og vedligehold. I tilfælde hvor anvendelsesbetingelser har sikkerhedsmæssig betydning, skal disse betingelser for systemets anvendelse iagttages, for at systemet kan drives på en sikker måde.

I forbindelse med ibrugtagning til drift har driftsorganisationen derfor brug for at kende disse betingelser. Styrelsen forudsætter derfor, at alle sikkerhedsrelaterede anvendelsesbetingelser er identificeret på tidspunktet for ansøgning om ibrugtagningstilladelse. Sikkerhedsrelaterede anvendelsesbetingelser forventes indarbejdet i den version af systemdefinitionen, som medsendes med ansøgningen. Forhold som i forvejen er indarbejdet i driftsinstruktioner og/eller vedligeholdelsesforskrifter jf. virksomhedens sikkerhedsledelsessystem, og derfor i forvejen er kendt af drifts- og vedligeholdelsesorganisationen betragtes ikke i denne sammenhæng som værende 'identificeret i forbindelse med risikovurderingsprocessen'.

Indarbejdelse af disse anvendelsesbetingelser i systemdefinitionen tjener især to formål:

- Struktureret overdragelse af disse betingelser til drifts- og vedligeholdelsesorganisationen
- Assessor kan tage stilling til, om betingelserne er håndteret

Det vil i nogle tilfælde være hensigtsmæssigt at skelne mellem betjeningsmæssige anvendelsesbetingelser og anvendelsesbetingelser relateret til vedligehold.

Et eksempel: En perronforlængelse introducerer en ny type afmærkning af fareområdet (sikkerhedszonen). Der kunne i forbindelse med indførelsen af det nye materiale være identificeret den fare, at afmærkningen ikke længere er synlig grundet afmærkningens manglende holdbarhed eller vaskbarhed. For at reducere risikoen ved denne fare stilles som betingelse for perronens anvendelse, at den ny type afmærkning skal efterses hver tredje måned det første år og derefter en gang årligt for at sikre, at afmærkningen fortsat er synlig. I dette tilfælde er vedligeholdelseskravet ny for vedligeholdelsesorganisationen, og det har sikkerhedsmæssig betydning, at kravet overholdes. Denne *sikkerhedsrelaterede anvendelsesbetingelse* for perronen skal derfor tydeligt fremgå af systemdefinitionen.

g) Antagelser med henblik på at afgrænse risikovurderingen.

Systemdefinitionen bør indeholde argumentation for en passende afgrænsning af selve risikovurderingen. Her bør angives de elementer, der ikke bliver taget højde for eller der er usikkerhed omkring.

Overvejelser vedr. pålidelighed af testresultater, målinger og datakvalitet til beskrivelse af systemet kan indgå i antagelserne.

[20] Svarer til driftsforskrifter

De antagelser, der afgrænser risikovurderingen, skal anføres udtømmende. Antagelserne indgår i risikovurderingens fareregister på samme måde som sikkerhedskravene og sikkerhedsforanstaltningerne. Forslagsstiller bør vurdere, hvordan antagelserne bidrager til usikkerhed på risikovurderingen.

Da systemantagelserne bestemmer afgrænsningen og gyldigheden af risikovurderingen, skal risikovurderingen ajourføres eller erstattes af en ny risikovurdering, hvis disse antagelser ændres eller revideres.

3) Hvordan bør en systemdefinition struktureres?

I kapitel 2 er det gennemgået, hvilke obligatoriske områder, punkt a) – g), der skal indgå i en systemdefinition i overensstemmelse med CSM-RA. Emneopdelingen er, som tidligere nævnt, ikke tænkt som en indholdsfortegnelse til en systemdefinition.

Systemdefinitionen indgår i forskellige sammenhænge f.eks. i forbindelse med assessering ved CSM assessor og ved sagsbehandling i Trafikstyrelsen. Alt efter omstændighederne kan systemdefinitionen derfor struktureres på forskellig vis. I bilag 1 gives der eksempler herpå. Se *Bilag til vejledning i udformning af systemdefinition.*

Det står forslagsstiller frit for, om han vil lave systemdefinitionen som et selvstændigt dokument, eller om han vil lade systemdefinitionen være en del af et større dokument. Vælger forslagsstiller at lade systemdefinitionen være en del af et større dokument bør det klart fremgå af indholdsfortegnelsen, hvilke afsnit der udgør systemdefinitionen. Disse afsnit bør kun indeholde forhold, der er relevante ift. systemdefinitionen.

Alt efter omstændighederne kan følgende afsnit medtages i systemdefinitionen som supplement til punkterne a) – g):

Indledning.

En systemdefinition bør altid have en indledning. Denne kan dog godt deles med f.eks. en signifikansvurdering eller med en risikovurderingsrapport.

En beskrivelse af projektet

Her gives generelle oplysninger om projektets omfang, aktører, evt. etapeopdeling mm.

Systemidentifikation

Såfremt det nye eller ændrede delsystem er omfattet af typeafprøvningsattester og verifikationsattester/-rapporter, udarbejdet af NoBo eller DeBo i henhold til TSI'er eller nationale regler, bør der refereres til disse.

Risikostyringsprocessen

Her gennemgås risikostyringsprocessen, som har været anvendt, ved at beskrive faser, involverede parter (og deres kompetencer), og resultater. Herunder:

- fareidentifikation og klassifikation
- valg af risikoacceptprincippet
- valg af risikoacceptkriterierne
- risikoevalueringen
- fastlæggelse af sikkerhedskrav
- fastlæggelse af sikkerhedsforanstaltninger
- at det er dokumenteret, at de identificerede sikkerhedskrav er opfyldt og dokumentation herfor

- assessors involvering
- kompetencer hos personale, som har foretaget risikovurderingen
- såfremt risikostyringen følger EN 50156, bør der være en henvisning til safety case (jf. EN 50129)
- der bør også indgå en henvisning til systemets fareregister

Konklusion

I konklusionen begrunder forslagsstiller, hvorfor delsystemet kan accepteres. Det skal beskrives, hvordan antagelserne bidrager til usikkerhed på resultatet.

Tjekliste

I bilag 3 findes et forslag til en tjekliste, der kan anvendes i forbindelse med forslagsstillers kvalitetssikring og godkendelse af systemdefinitionen.

4) Kompetencer

Fagkompetencer hos de personer, der laver systemdefinitionen

De personer, som skriver systemdefinitionen, skal have tilstrækkelige fagkompetencer inden for det område, de skal analysere og beskrive. Virksomhedernes sikkerhedsledelsessystem bør indeholde procedurer for valg af kompetente personer, så disse udvælges på en systematisk måde.

De kompetente personer bør også selv forholde sig kritisk til, om de har de fornødne kompetencer til de opgaver, de gives. F.eks. bør afgrænsningen af et projekt i forhold til, hvilke fagområder der ikke berøres af en ændring, ske af personer med de fornødne kompetencer.

Helt lavpraktisk medfører dette, at det f.eks. ved et sporprojekt ikke bør være den ansvarlige indenfor spor som afgør, om der er en grænseflade til sikringsanlægget, som bør håndteres. En person med kompetencer indenfor sikringsanlæg bør afgøre dette.

Et andet eksempel er ændring af fjernstyringen af et sikringsanlæg. Her er det ikke tilstrækkeligt kun at se på den tekniske ændring, men også på hvilke konsekvenser det får for den, der betjener anlægget og den organisatoriske enhed, vedkommende indgår i. Derfor bør der også tilknyttes en person med de tilstrækkelige kompetencer inden for samspillet mellem teknik, drift og trafikstyring til at foretage afgrænsningen.

Hvem udpeger, hvem der laver systemdefinitionen?

Forslagsstiller er ansvarlig for skriftligt at dokumentere, hvem der er ansvarlig for at varetage hvilke opgaver i forbindelse med risikostyringen jf. CSM-RA bilag 1 (1.1.6) allerede i den første fase af risikovurderingen. Formålet med dokumentet er at styre arbejdsfordelingen og derved sikre, at systemet kommer til at opfylde de specificerede sikkerhedsniveauer og sikkerhedskrav. Forslagsstiller kan vælge at gøre dokumentet til en del af systemdefinitionen.

Forslagsstillers koordinering af sikkerhedsaktiviteterne ved grænsefladen mellem de samarbejdende aktører er afgørende for jernbanesystemets sikkerhedsniveau.

I tråd hermed er det også forslagsstillers ansvar at udpege den eller de kompetente personer, som skal skrive og udvikle systemdefinitionen. Det er derfor vigtigt, at virksomhedernes sikkerhedsledelsessystem indeholder kompetencekrav til forslagsstiller, så opgaverne fordeles på en kompetent måde. Forslagsstiller kan vælge at anvende egne kompetente personer eller eksterne kompetente personer – valget bør dog dokumenteres som beskrevet i indledningen.

Da forslagsstiller er ansvarlig for, at CSM-RA processen følges, bør det fremgå af virksomhedens sikkerhedsledelsessystem, hvem der kan være

forslagsstiller og på virksomhedens vegne være ansvarlig for systemdefinitionen[21].

Versionsstyring og forslagsstillers påtegning bør fremgå af systemdefinitionen.

Hvem kan være forslagsstiller?

Forslagsstiller er jf. den udgave (352/2009) af CSM-RA[22]som skal anvendes til og med 20. maj 2015:

- jernbanevirksomheder eller jernbaneinfrastrukturforvaltere inden for rammerne af de risikokontrolforanstaltninger, de skal gennemføre i henhold til artikel 4 i direktiv 2004/49/EF,

- ordregivere eller fabrikanter, når de opfordrer et bemyndiget organ til at anvende »EF«-verifikationsproceduren i overensstemmelse med artikel 18, stk. 1, i direktiv 2008/57/EF,

- eller den, der ansøger om tilladelse til at tage et køretøj i brug.

[21] Dette er i overensstemmelse med § 18 i BEK 14 og § 17 i BEK 13 af 4. januar 2007: *Virksomheden skal udforme og vedligeholde procedurer, der sikrer, at relevante behov for uddannelse og træning bliver identificeret, og at medarbejderne opnår de nødvendige færdigheder, der er hensigtsmæssige eller krævede for udførelsen (/gennemførelsen) af deres arbejde.*

[22] CSM-RA art 3(11)

5) Sammenhæng med virksomhedens sikkerhedsarbejde

I dette kapitel beskrives, hvordan arbejdet med systemdefinitionen kan bruges som et redskab i forbindelse med virksomhedens sikkerhedsarbejde.

Hvornår skal der laves en systemdefinition?

Systemdefinitionen er et element i CSM-RA[23]. Systemdefinitionen skal løbende opdateres, når risikostyringsmetoden i CSM-RA anvendes. Processen styres af forslagsstiller.

For at afgøre, om risikostyringsmetoden i CSM-RA skal anvendes, starter forslagsstiller med at udpege den eller de kompetente personer, som skal lave en *foreløbig systemdefinition* for den ændring, som ønskes gennemført. Den foreløbige systemdefinition danner udgangspunkt for en signifikansvurdering.

Signifikansvurderingen anvendes til at afgøre, om CSM-RA-metoden skal anvendes til risikostyring. CSM-RA-metoden skal følges, når:

- det kræves i en TSI (art 5(1) i CSM-RA)
- et nyt eller signifikant ændret delsystem, eller et nyt element i et delsystem skal integreres i det samlede jernbanesystem[24],
- et nyt eller signifikant ændret delsystem ikke er fuldt dækket af TSI'er eller nationale regler[25]

Når en ændring ikke er signifikant og ingen af de andre ovenstående krav er relevante, er der ikke krav om, at CSM-RA-metoden anvendes. Forslagsstiller er forpligtet til at kunne dokumentere sin vurdering af signifikans.

Risikostyringsprocessen

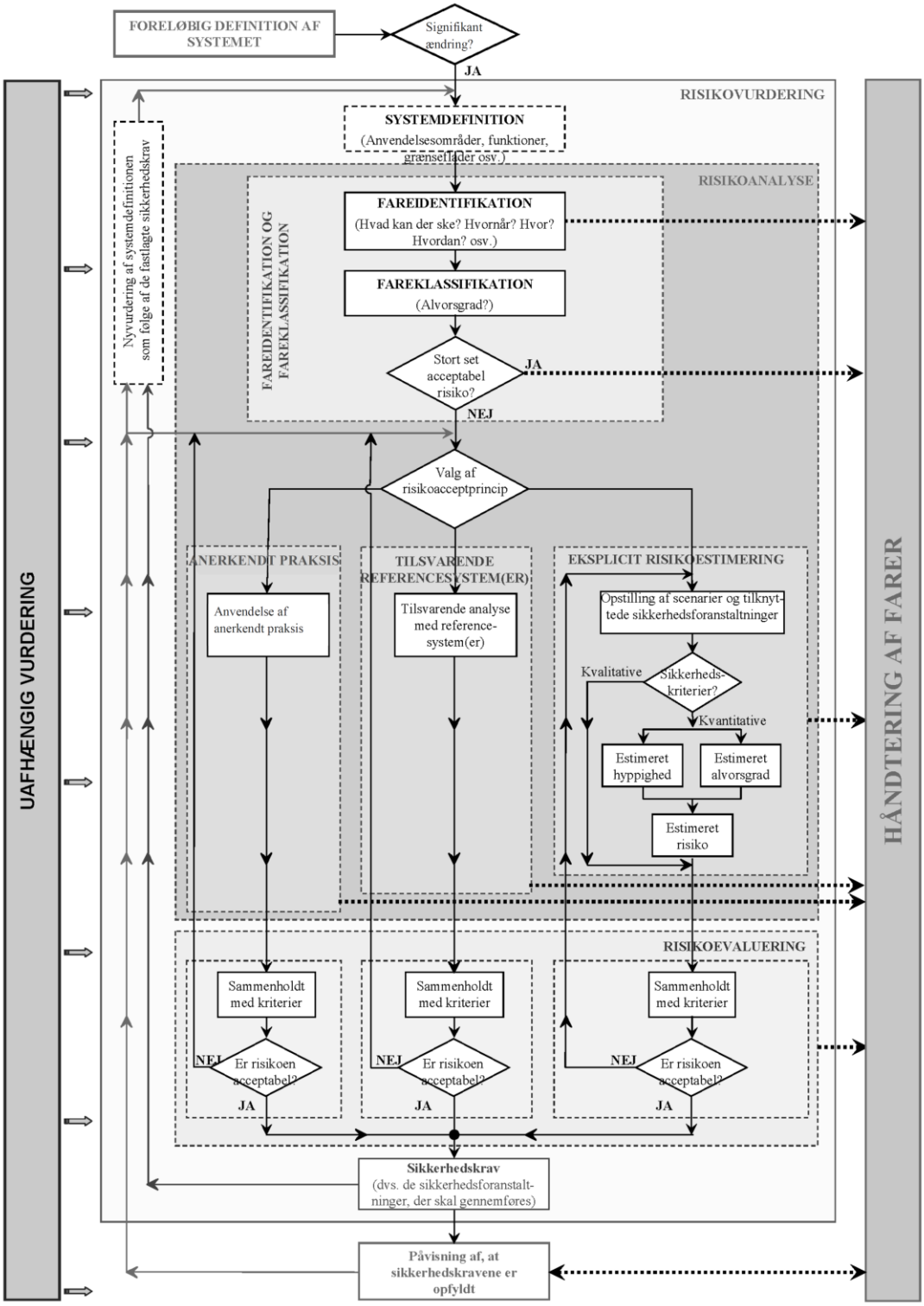
I det følgende gennemgås risikostyringsprocessen ifølge CSM-RA med fokus på de sammenhænge, hvor systemdefinitionen indgår. For en mere detaljeret gennemgang af risikostyringsprocessen henvises til ERA's vejledninger om emnet[26].

[23] Værktøjet "systemdefinition" anvendes i CSM-RA, men blev introduceret i cenelec-standarden EN 50126. EN 50126 er en metode, som anvendes til at fastsætte RAMS-krav (reliability, availability, maintainability og safety) vha. en analyse af produktet/projektet fra koncept til systemaccept, drift og vedligehold og senere nedlukning og bortskaffelse – altså hele systemets livscyklus.
Der er ikke modstrid mellem EN 50126 og CSM-RA, derfor vælger mange projekter at anvende CSM-RA suppleret med EN 50126.

[24] art 2(2b) i CSM-RA

[25] I bekendtgørelse nr. 56 om godkendelse af køretøjer på jernbaneområdet af 24.1.2013.

[26] *Samling af eksempler på risikovurderinger og nogle mulige værktøjer, der støtter CSM-forordningen*. ERA. 06/01/2009 og *Vejledning i anvendelse af Kommissionens forordning om vedtagelse af en fælles sikkerhedsmetode med hensyn til risikoevaluering og-vurdering som anført i artikel 6, stk. 3, litra a), i jernbanesikkerhedsdirektivet* ERA. 06/01/2009



Figur 8: Tegning fra CSM-RA over risikostyringsprocessen og den uafhængige vurdering

Figur 8 viser risikostyringsprocessen og den uafhængige vurdering jf. CSM-RA. Processen starter øverst til venstre i figuren med en ”foreløbig definition af systemet” også kaldet en foreløbig systemdefinition.

På baggrund af den foreløbige systemdefinition laves signifikansvurderingen.

Systemdefinitionen færdiggøres trinvis. Dette er årsagen til, at kassen "systemdefinition" er vist med stiplet kant i figuren.

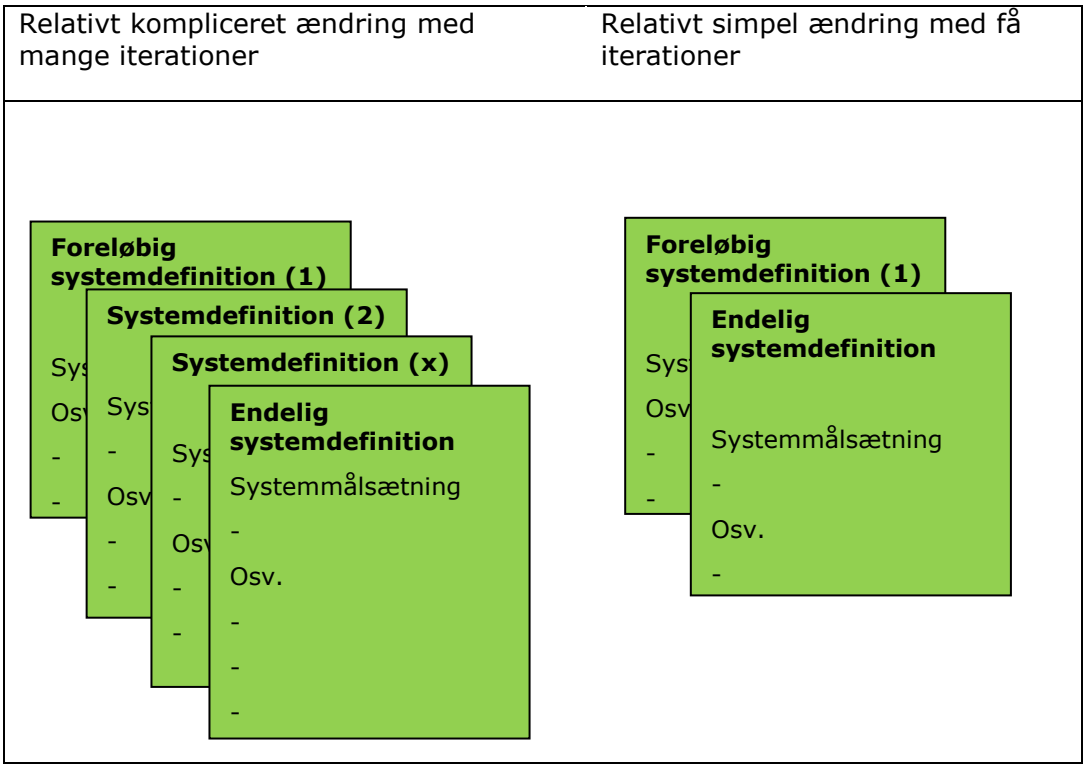
Efter at have færdiggjort den første systemdefinition fortsætter forslagsstiller med "risikoanalysen", derefter evalueres de identificeres risici (risikoevaluering), og på baggrund heraf formuleres sikkerhedskrav. Fra "sikkerhedskrav" går en pil tilbage op igen langs venstre side af figuren og op til kassen med "nyvurdering af systemdefinitionen". Derfra går pilen videre til "systemdefinition". Pilen laver altså en cirkelbevægelse igennem figuren.

Bevægelsen gennem modellen symboliseret med pile viser den *iterative proces*, hvor systemdefinitionen hele tiden opdateres, efterhånden som farer identificeres, og der opstilles nye sikkerhedskrav.

Systemdefinitionen er altså ikke bare første led i en risikostyringsproces, men også der, hvor resultatet af risikostyringsprocessen – i form af sikkerhedskrav – oplistes. Systemdefinitionen rettes desuden hele tiden til, hvis man opdager, at nogen af de antagelser, som man har om det delsystem, som ændringen foretages i, er forkerte eller ændrer sig.

Den iterative proces for udvikling og opdatering af systemdefinitionen er illustreret i figur 9. For hver iteration udvikles systemdefinitionen og bliver mere detaljeret og omfattende. Antallet af iterationer er afhængig af hvor omfattende og komplekst projektet er[27]:

[27] Noget, som kan være med til at gøre et projekt mindre kompliceret og omfattende, er, hvis mange af de identificerede risici er "stort set acceptable" Jf. afsnit 2.2.2 i CSM-RA. Som vist i CSM-RA flowdiagrammet, figur 8, er det tilstrækkeligt at registrere sådanne risici i fareregisteret (Læs evt. mere i afsnit 2.2.2 i: *Samling af eksempler på risikovurderinger og nogle mulige værktøjer, der støtter CSM-forordningen*. ERA. 06/01/2009)



Figur 9: eksempler på to typer ændringer som har et forskelligt antal iterationer og derfor et forskelligt antal systemdefinitioner

Fordi systemdefinitionen opdateres løbende, er det svært at opstille entydige krav til, hvad der skal stå i en systemdefinition. Indholdet af en systemdefinition er afhængig af, hvor langt fremskreden risikostyringsprocessen er, og hvor meget forslagsstiller derfor kan vide om ændringen og det delsystem, som ændringen foretages i. Indholdet af en systemdefinition er desuden afhængig af omfanget af ændringen.

Den endelige systemdefinition kan først færdiggøres, når alle sikkerhedskrav til systemet er identificeret og er opfyldt.

Uafhængigt af, om man skal anvende CSM-RA-metoden til risikostyring, eller om man bruger en risikostyringsmetode beskrevet i eget sikkerhedsledelsessystem, er anvendelsen af en systemdefinition et hensigtsmæssigt værktøj til at beskrive ændringen og til at dokumentere sikkerhedskrav.

Involvering af Trafikstyrelsen

Systemdefinitionen udvikles iterativt som en del af risikostyringsprocessen. Nogle af disse iterationer involverer Trafikstyrelsen eller en assessor.

I de tilfælde, hvor der skal indsendes en systemdefinition til Trafikstyrelsen, anvendes den seneste opdaterede version f.eks. som bilag til ansøgning om assessorgodkendelse, eller som bilag til en ansøgning om ibrugtagningstilladelse.

Involvering af Assessor

Assessor skal involveres så tidligt som muligt i projektet, f.eks. umiddelbart efter virksomheden har afgjort, at ændringen er signifikant

Forslagsstiller bør altid udarbejde en skriftlig opgavebeskrivelse for assessor, uanset om assessor er intern eller ekstern. Systemdefinitionen er et vigtigt element i denne beskrivelse, idet den afgrænser det system, som skal risikovurderes og assesseres. I forbindelse med assessors accept af opgaven, bør assessor forholde sig kritisk til systemdefinitionen.

Efter assessor er godkendt, skal alle versioner af systemdefinitionen, som indsendes til Trafikstyrelsen, være assesseret.

I starten af større projekter kan det være vanskeligt at gennemskue det detaljerede indhold i alle projektets faser. I sådanne projekter bør assessors opgavebeskrivelse herunder systemdefinitionen, opdateres ved hvert faseskift. Dette vil under alle omstændigheder være et krav, såfremt den enkelte fase skal have ibrugtagningstilladelse. Her bør assessor igen forholde sig kritisk til systemdefinitionen.

I et projekt med flere faser/etaper kan det være hensigtsmæssigt at lave en AAPP (Authority Approval Proces Plan) for projektet. Herved sikres en oversigt over, hvornår Trafikstyrelsen skal involveres med enten en tilkendegivelse eller en ibrugtagningstilladelse. Dette kan være en hjælp for både forslagsstiller og assessor til at tilrettelægge deres arbejde.

N.B. Vejledningen suppleres af tre bilag. Se særskilt dokument: Bilag til vejledning i udformning af systemdefinition*. Dokumentet kan findes på Trafikstyrelsens hjemmeside.*

Trafikstyrelsen
Edvard Thomsens Vej 14
DK-2300 København S

info@trafikstyrelsen.dk
www.trafikstyrelsen.dk

Vejledning i udformning af systemdefinition