Risikovurdering i en jernbane under endring

Terje Sivertsen

Risiko og pålitelighet i en moderne transportverden, Gardermoen, 27. mars 2019

En jernbane under endring

- Sikkerheten på norsk jernbane er fortsatt i stor grad basert på eldre, relebasert teknologi
- Siden 1990-tallet er ulike typer elektroniske sikringsanlegg innført
- Europeiske standarder er tatt i bruk som basis for RAMS-styringen i systemutviklingen (*Reliability*, *Availability*, *Maintainability*, *Safety*)
- Nye tekniske løsninger har krevd endringer i sikkerhetstenkningen
- Ulike muligheter for digitalisering prøves ut
- Dagens signalsystemer erstattes med ERTMS (European Rail Traffic Management System) og nytt trafikkstyringssystem
- Driftsapparatet endres for å tilpasses den nye teknologien, parallelt med behovet for å vedlikeholde det eksisterende
- Ny kompetanse tilpasset fremtidens signalsystemer rekrutteres, samtidig som kompetansen på dagens systemer må ivaretas

Risikovurdering i jernbanen

- I henhold til EN 50126 er risikovurderingen en del av jernbane-virksomhetens ansvar i forbindelse med RAMS-prosessen
  - skal sikre spesifisering av kravene som må oppfylles for at det skal være sikkerhetsmessig forsvarlig å ta et planlagt system i bruk
  - er del av jernbanevirksomhetens sikkerhetsstyring i forbindelse med fremskaffelsen av systemet
  - Jernbanevirksomhetens myndighet til å ta ansvaret for dette er gitt gjennom sikkerhetsgodkjenningen av jernbanevirksomheten
- Med hensyn til utledningen av sikkerhetskrav, kan risikovurderingsprosessen beskrives som bestående av
  - fareidentifisering
  - identifisering av eventuelle eksisterende eller planlagte eksterne barrierer
  - risikovurdering av de identifiserte farene
  - identifisering av sikkerhetsfunksjoner i det aktuelle systemet som skal håndtere farene, og utledning av sikkerhetskrav til disse (THR)
  - identifisering av andre funksjoner som ved svikt kan føre til fare, og utledning av sikkerhetskrav til disse (THR)

Er risikovurdering vanskelig nok som det er?

Sandvika stasjon, Slependen blokkpost (2005)

- Forsignal til blokksignal viste for lite restriktivt signalbilde

Hva var årsaken?

- Programmeringsfeil i generisk programvare

Hvordan kunne designfeilen oppstå?

- Programmeringsfeilen ble ikke avdekket av leverandøren gjennom eksisterende prosesser for utvikling og sikring av programvare
- Det ble ikke gjennomført nødvendig fareidentifisering og analyser under de tidlige fasene slik EN 50126 krever

Hva indikerer dette av nødvendige tiltak?

- Leverandøren må demonstrere at prosessene for utvikling og sikring av programvare effektivt avdekker mulige sikkerhetsrelaterte feil
- Kunden må utføre en risikovurdering på overordnet jernbanesystemnivå, verifisere at denne har vært tilfredsstillende med hensyn på å kunne etablere eventuelle sikkerhetskrav, og verifisere at sikkerhetskravene har vært håndtert videre i prosessen

BANE NOR

Risikovurderingene utfordres av endringer

- Endringer i
  - relasjonene mellom årsaker, farer og ulykker
  - operasjonelle tilstander, betingelser i omgivelsene, interaksjon
  - forutsetningene for at en fare praktisk kan unngås
  - organisering uten erstatning av eksisterende barrierer, kompetanse, strukturer
- Nye
  - avhengigheter som kan gi svikt av felles årsak
  - sikkerhetsrelaterte grensesnitt
  - sikkerhetsrelaterte funksjoner, eksisterende funksjoner som blir sikkerhetsrelaterte, eller krav til sikkerhetsintegriteten til disse funksjonene
  - fysiske eller informasjonsteknologiske sikringstrusler
  - ledere og medarbeidere med et annet sikkerhetsfokus
  - avhengigheter til informasjon, automatisering og autonome systemer
- Uegnede risikoakseptkriterier eller feil bruk av dem
- Ukjente svakheter i eksisterende kompetanse eller prosesser
- Utilstrekkelig overføring eller innarbeidelse av sikkerhetsprinsipper

BANE NOR

Risikovurdering er noe av det viktigste jernbanen gjør og enda viktigere under endring

Metodikk for risikovurderinger for en jernbane under endring:

SafeT – Safety Assessment Framework for Efficient Transport

BANE NOR

SafeT-prosjektet (2016-2019)

- Prosjektet SafeT utvikler et rammeverk for system- og risikomodellering i
  - etableringen av sikkerhetskravene til et teknisk system
  - demonstrasjonen av at systemet er sikkert å ta i bruk
- Risikovurderingen er en viktig del av metodikken
- Siktemålet er å gjøre kunden bedre i stand til å forvalte sitt ansvar i den videre digitaliseringen innenfor sin sektor
- Partnere og FoU-leverandører:
  - Bane NOR, prosjekteier og prosjektleder
  - IFE, Safetec, NTNU, Avinor, og Indra Navia (Norge)
  - Solvina (Sverige)
  - VTT (Finland)
  - Beijing Jiaotong University (Kina)
- Sponsorer:
  - Norges forskningsråd (TRANSPORT), Bane NOR

Bruk av modeller i SafeT-rammeverket

- ***Beskrive og analysere***
  - et systems statiske struktur og elementer
  - systemets oppførsel
  - systemets interaksjon med sine omgivelser
- ***Understøtte***
  - aktiviteter i forbindelse med risikovurdering og farekontroll
  - utledning av nødvendige sikkerhetskrav for å håndtere de identifiserte farene
  - demonstrasjon av at systemdesignen er egnet for påkrevd sikkerhetsintegritet
- ***Kommunisere***
  - design og risikoaspekter ved systemet
  - sikkerhetsargumentasjonen som legges til grunn for aksept av systemet

Etablering av SafeT-rammeverket

1. Identifisering av modelleringsbehovene i RAMS-fasene, med fokus på utledning og validering av sikkerhetskravene
2. Etablering av prosesser for modelleringsaktivitetene i RAMS-fasene
3. Etablering av krav til modeller som skal tilfredsstille behovene
4. Identifisering av teknikker basert på evaluering mot kravene
5. Anvendelse på relevante case-eksempler
6. Utvikling av et omforent sett av verktøy for å understøtte modelleringsaktivitetene i sikkerhetsargumentasjonen
7. Integrering av formelle metoder (matematisk baserte teknikker for spesifisering, utvikling og verifisering av programvare og maskinvare)

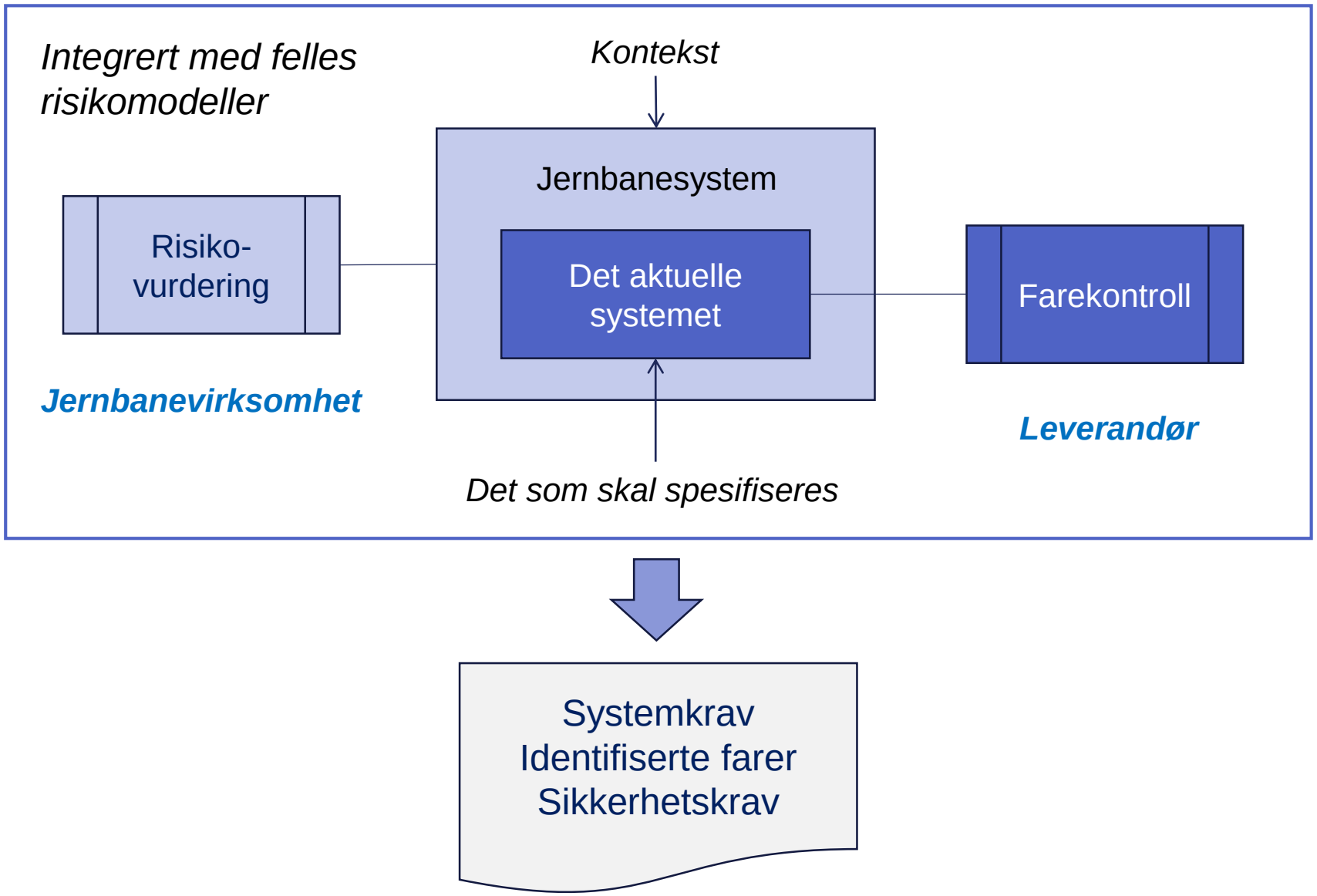
SafeT har fokusert spesielt på RAMS-fasene 2 til 4:

- Systemdefinisjon og operasjonell kontekst
- Risikoanalyse og evaluering
- Spesifikasjon av systemkrav

Forberede risikovurderingen:
Systemdefinisjon og operasjonell kontekst
(RAMS-fase 2)

Systemdefinisjon og operasjonell kontekst

- Utgangspunktet er at det skal fremskaffes et jernbaneteknisk system som skal innføres i infrastrukturen eller om bord på tog
  - Det skal etableres krav til *pålitelighet*, *tilgjengelighet*, *vedlikeholdbarhet* og *sikkerhet* (RAMS)
  - Sikkerhetskravene forutsettes etablert gjennom en risikoanalytisk prosess og oppfylt i systemet gjennom bruk av prosesser, metoder, teknikker og verktøy tilpasset risikonivået
- Systemdefinisjonen må ligge på overordnet jernbanesystemnivå:
  - Risikovurderingen utføres på dette nivået
  - Mer enn det aktuelle systemet berøres
- Systemdefinisjonen brukes som basis for
  - identifisering av eksterne risikoreduserende tiltak
  - risikovurdering
  - utledning av RAMS-krav (inngår i systemkravene)
  - spesifisering av sikkerhetsrelaterte anvendelsesbetingelser


Integrert med felles risikomodeller
Kontekst
Jernbanesystem
Risiko-vurdering
Det aktuelle systemet
Farekontroll
Jernbanevirksomhet
Leverandør
Det som skal spesifiseres
Systemkrav
Identifiserte farer
Sikkerhetskrav

Bruk av modellering i fase 2

- Oppgave:
  - Produsere systemdefinisjonen, sammen med en RAMS-plan og sikkerhetsplan
- Modellering:
  - Understøtte systemdefinisjonen med modeller som beskriver de forskjellige systemaspektene
- Eksempel på krav til modellene:
  - Vise hvordan et system i interaksjon med omgivelsen responderer på input for å produsere spesifiserte output
- Eksempel på teknikk:
  - Prosess-simulering kan bidra gjennom å lage et system som etterlikner oppførselen til omgivelsene som skal kontrolleres av systemet som skal testes

Bruk av formelle metoder i fase 2

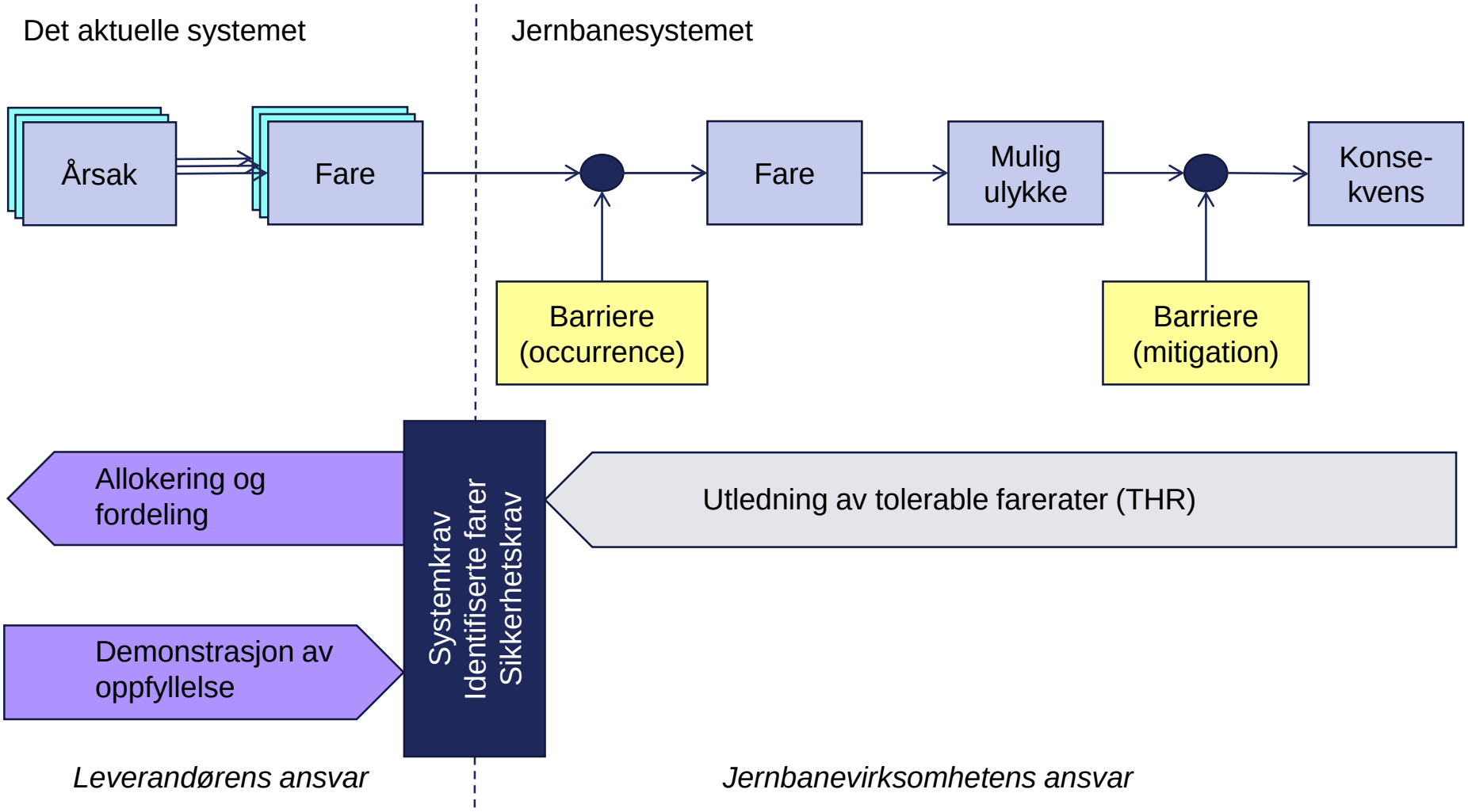
- Beskrive systemresponsen i en formell notasjon, med innebygde muligheter til å identifisere alle funksjoner som responderer på en gitt input
- Knytte systemet og omgivelsene sammen gjennom å spesifisere systemets og omgivelsenes funksjoner og egenskaper på basis av hverandre
- Beskrive vekselvirkningen mellom systemet og dets omgivelser gjennom spesifikasjonene av funksjonene og egenskapene til systemet og andre systemer, delsystemer og komponenter det kommuniserer med
- Integrere de ulike stegene i systemets livsløp gjennom bruk av samme formelle notasjon

Utføre risikovurderingen:
Risikoanalyse og evaluering
(RAMS-fase 3)

Risikoanalyse og evaluering

- Forhold som bidrar til risiko identifiseres som *farer* som trigges av *årsaker* og kan lede til *ulykker*
- Ulykkenes omfang vurderes på grunnlag av ulykkenes *konsekvenser*, som analyseres i en *konsekvensanalyse*
- Konsekvensanalysen utføres gjennom å definere en *risikomodell* som visualiserer de forskjellige *ulykkesscenariene*
- Hensikten med risikomodellen er å vise hvordan årsaker, farer, barrierer og ulykker er relatert
- Risikomodellen
  - tar utgangspunkt i fareidentifiseringen på overordnet jernbanesystemnivå
  - brukes som basis for utledning av tolerable farerater
  - utvides gjennom å trekke inn resultatene fra fareidentifiseringen for det aktuelle systemet
- Det kan dermed refereres til en enhetlig modell som inkluderer resultatene fra fareidentifiseringene på de ulike systemnivåene

Generisk risikomodell



Bruk av modellering i fase 3

- Oppgave:
  - Utføre risikovurdering
  - Etablere fareloggen
  - Oppdatere sikkerhetsplanen og RAM-planen
  - Etablere planen for uavhengig sikkerhetsvurdering
- Modellering:
  - Understøtte risikovurderingen med risikomodeller som representerer relasjonene mellom farer, årsaker, ulykker, etc.
- Eksempel på krav til modellene:
  - Legge til rette for identifisering av farer assosiert med systemet og hendelser som leder til disse farene, fastsettelsen av risikoen assosiert med farene, og identifisering av mulige ytterligere sikkerhetskrav som er nødvendige for å redusere risikoen til et akseptabelt nivå, på et vilkårlig systemnivå
- Eksempel på teknikk:
  - Designgransking, understøttet med sjekklister, kan bidra gjennom gjennomgang av spesifikasjoner, design og programmer med mål om å identifisere mulige farer

Bruk av formelle metoder i fase 3

- Kombinere formelle metoder med teknikker for fareidentifisering og risikoanalyse
- Identifisere kombinasjoner av betingelser som kan lede til en topphendelse og formelt utlede sikkerhetskrav som forhindrer at disse kombinasjonene oppstår
- Bruke feiltrær for å knytte topphendelsene til sikkerhetskrav til systemets funksjoner og gjennom den formelle verifiseringen videre ned til påkrevde relasjoner mellom systemvariablene
- Understøtte feiltreanalysen gjennom å formalisere relasjonen mellom feiltre og sikkerhetskrav og bruke dette som basis for formell verifisering av komplettheten av sikkerhetskravene

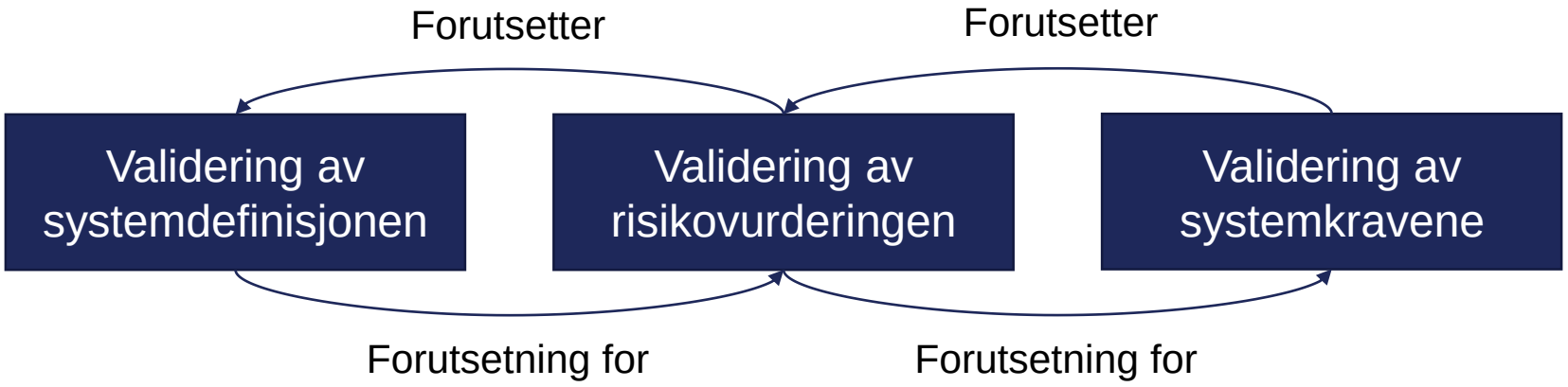
Bruke risikovurderingen:
Spesifikasjon av systemkrav
(RAMS-fase 4)

Systemkravenes utvikling

- Initiale systemkrav
  - input til kravetableringsprosessen, fra et gitt systembehov
- Fase 1: Ulike muligheter utredes og sammenliknes
- Fase 2: Kravene bearbeides ytterligere
- Fase 3: Konkretisering av krav til systemets håndtering av identifiserte farer
- Fase 4: Etableringen av selve systemkravspesifikasjonen, basert på input fra tidligere faser
- Fase 5: Systemkravene fordeles på delsystemene i den valgte systemarkitekturen

Spesifisering, verifisering og validering av sikkerhetskrav

- Risikovurderingen leder frem til et omforent sett av sikkerhetskrav
- Verifisering av risikomodellen skal vise at alle identifiserte årsaker, farer, barrierer og ulykker er satt i sammenheng med hverandre
- Valideringen skal vise at modellen reflekterer de faktiske forholdene og gir et tilfredsstillende grunnlag for å identifisere sikkerhetskrav
- Når sikkerhetskravene er etablert, skal verifiseringen vise at
  - alle farer kan spores til sikkerhetskrav
  - alle sikkerhetskrav kan spores tilbake til risikomodellen
- Valideringen bruker verifiseringsresultatene for å avgjøre om de riktige sikkerhetskravene er spesifisert



Bruk av modellering i fase 4

- Oppgave:
  - Produsere RAMS-systemkravspesifikasjonen
  - Sikkerhetsrelaterte anvendelsesbetingelser
  - Oppdatert farelogg, sikkerhetsplan og RAM-plan
  - Valideringsrapport som dekker de fire første fasene
  - RAM- og sikkerhetsvalideringsplan for de påfølgende fasene
- Modellering:
  - Understøtte spesifiseringen av krav og anvendelsesbetingelser for det aktuelle systemet, på basis av modellene fra systemdefinisjonen og risikovurderingen
- Eksempel på krav til modellene:
  - Legge til rette for identifiseringen av sikkerhetskrav
- Eksempel på teknikk:
  - Prototyping og animering kan bidra gjennom å demonstrere den tiltenkte funksjonaliteten av sikkerhetsfunksjonen, for derved å gi et grunnlag for å analysere og spesifisere sikkerhetskravene assosiert med funksjonen

Bruk av formelle metoder i fase 4 og videre

- Utlede sikkerhetskravene formelt fra resultatene av risikovurderingen
- Vedlikeholde sporbarheten av kravene som en iboende del av metodikken
- Sikre sporbarheten mellom sikkerhetskravene og programvaren for det enkelte anlegg gjennom formell verifisering opp mot sikkerhetskravene
- Bruke automatisk bevisføring for å sikre komplett verifisering og automatisk identifisering av tilfeller der sikkerhetskravene ikke er oppfylt
- Legge til rette for formell verifisering av design og implementering
- Bevise at spesifiserte sikkerhetsegenskaper er invariante funksjonelle egenskaper ved systemet eller programvaren

Oppsummering

- Risikovurdering er noe av det viktigste jernbanen gjør og enda viktigere under endring
- System- og risikomodeller som utvikles gjennom livsløpsfasene tilrettelegger for etableringen og valideringen av sikkerhetskravene
- Formelle metoder legger ytterligere til rette for valideringen av systemkravene og et gir et godt grunnlag for design, implementering, validering og aksept av det endelige systemet

Risikovurdering

Modeller

Formelle metoder

I en tid med endring kan det viktigste vi gjorde i går bli enda viktigere i morgen

BANE NOR