NTNU FFI Forsvarets forskningsinstitutt SINTEF

DECRIS ARBEIDSNOTAT 1

TITTEL

DECRIS – Problemstillinger rundt tversektorielle risikoanalyser. Kritisk infrastruktur

FORFATTERE

Håvard Fridheim, Jon Røstum, Gerd Kjølle, Dag Bertelsen, Inger Anne Tøndel, Jørn Vatn, Gunhild Åm Vatn, Ingrid Utne

SAMMENDRAG

Hensikten med notatet er å dokumentere kjent kunnskap i prosjektet ifm. problemstillinger rundt tverrsektorielle risikoanalyser og risikokommunikasjon. Dokumentet har flere målsettinger:

- Gi grunnleggende beskrivelse av infrastruktur behandlet i DECRIS
- Bidra til å avklare problemstillingene for arbeidet i DECRIS

ISBN	DATO
	2009-03-23
GRADERING	ANTALL SIDER
ÅPEN	22
KONTAKT DETTE NOTAT	ADRESSE
Håvard Fridheim	Havard.Fridheim@ffi.no, FFI
NØKKELORD NORSK	NØKKELORD ENGELSK
Kritisk infrastruktur, tverrsektoriell risikoanalyse	

Innhold

1 Innledning

Prosjektet "Risk and Decision Systems for Critical Infrastructures" (DECRIS) er finansiert av Norges forskningsråd gjennom SAMRISK[1]-programmet. Tema for prosjektet er å studere beslutningsprosessen i forbindelse med tverrsektorielle risikoanalyser, med formål å utvikle en metode for risikoanalyse som er anvendbar på tvers av sektorer. Dette inkluderer en analyse av relevante aspekter ved risikokommunikasjon i tilknytning til beslutningsprosessen.

Prosjektet vil, etter en innledende kartlegging av metoder og praktiske erfaringer, gjennomføre en risikoanalyse ("case") med henblikk på tverrsektorielle risikovurderinger. Metodeutvikling vil skje i forbindelse med denne analysen.

Prosjektarbeidet gjennomføres i perioden august 2007 – september 2009. Deltakere i prosjektet er SINTEF, NTNU og FFI. Oslo kommune er invitert inn som samarbeidspartner i selve risikoanalysen, mens personer fra DSB, NSM, NVE og Stavanger kommune er invitert med som deltakere i en referansegruppe for prosjektet.

Dette notatet har flere målsettinger. Primært skal notatet identifisere viktige problemstillinger ved risikoanalyser av kritisk infrastruktur som metodeutviklingen i prosjektet må ta høyde for. Sekundært skal den gi et generelt kunnskapsgrunnlag for deltakerne i prosjektet om prosjektets hovedproblemstillinger og de infrastrukturene som skal analyseres. Dette vil gi bidrag inn til planleggingen av risikoanalysen for Oslo kommune.

Notatets disposisjon er som følger:

- Kapittel 2 presenterer noen begreper som er brukt i notatet.
- Kapittel 3 gir enkle systembeskrivelser for de infrastrukturene som er aktuelle å analysere i prosjektarbeidet: transport, vannforsyning og kraftforsyning.
- I kapittel 4 presenteres noen viktige metodiske og praktiske utfordringer med gjennomføring av risikoanalyser for kritisk infrastruktur
- Kapittel 5 reiser problemstillinger knyttet til tverrsektorielle risikoanalyser, herunder aspekter ved beslutningsprosess og risikokommunikasjon
- Kapittel 6 oppsummerer rapporten kort.

2 Begrepsavklaringer

Kritisk infrastruktur omfatter de infrastrukturer som er mest sentrale for å holde samfunnet i gang, for eksempel elektrisk kraft, telekommunikasjoner, vann og avløp, olje- og gassforsyning, transport, og bank og finans. Infrastrukturutvalget definerer begrepet slik[2]

- "Kritisk infrastruktur er de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse."

I forlengelsen av dette er **kritiske samfunnsfunksjoner** alle funksjoner som samfunnet er avhengig av for å dekke befolkningens grunnleggende behov.

[1] Samfunnssikkerhet og risikoforskning
[2] Justis- og politidepartementet (2006): NOU 2006:6. *Når sikkerhet er viktigst*

Risiko uttrykker fare for tap av viktige verdier som følge av uønskede hendelser. En vanlig tilnærming er å se på risiko som en kombinasjon av sannsynlighet og konsekvens for en gitt hendelse. En annen tilnærming er at risiko er en kombinasjon av mulig konsekvens og tilhørende usikkerhet.

Sårbarhet er et uttrykk for et systems evne til å fungere og oppnå sine mål når det utsettes for påkjenninger. Sårbarhetsutvalget definerer på sin side sårbarhet på følgende måte:[3]

- "Sårbarhet er et uttrykk for de problemer et system vil få med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet."

En **risiko- og sårbarhetsanalyse** (eller bare risikoanalyse) er en prosess for å kartlegge og dokumentere risiko og sårbarhet i et gitt system. Målet med analysen er som regel å gjøre systemet mer robust mot ulike farer og trusler. Ved å kombinere kunnskap fra eksperter, ledelse og/eller brukere i en strukturert prosess, identifiseres og rangeres uønskede hendelser ut i fra risiko, og det gis en beskrivelse av risikobildet knyttet til systemet som analyseres. Dette gir et grunnlag for å komme frem til risiko- og sårbarhetsreduserende tiltak knyttet opp mot de identifiserte hendelsene.[4]

Med **risikokommunikasjon** menes her all språklig kommunikasjon relatert til kritiske eller farlige situasjoner, mellom eksperter og beslutningstakere i forvaltningen (intern kommunikasjon med fokus på beslutningsprosesser, og kommunikasjon ut til allmennheten). Risikokommunikasjon har et sterkt strategisk tilsnitt: hensikten er ofte å påvirke beslutninger eller å påvirke allmennheten til å handle på en bestemt måte eller å påvirke allmennhetens oppfatning av en situasjon eller et fenomen.

3 Systembeskrivelser

Kapittelet gir overordnede beskrivelser av infrastrukturene som skal analyseres i prosjektets case.

3.1 Transport

Transportsystemet i Norge er satt sammen av fire svært ulike transportnettverk: Veg, bane, luft og sjø. Disse nettverkene er ulike både med hensyn til egenskaper som transportbærere og fysisk utforming, men skal like fullt utgjøre et samlet nasjonalt transportsystem.

I det videre beskrives veg- og banetransport generelt. Disse nettverkene er mest aktuelle for vurdering i ROS-caset som er beskrevet i kapittel **Error! Reference source not found.**.

3.1.1 Vegtransport

Infrastruktur
Det offentlige vegnettet har en total lengde på nesten 93.000 km; ca 27.000 km riksveg, 27.000 km fylkesveg og 39.000 km kommunal veg. [5] Inkludert i vegnettet, spesielt i riksvegnettet på

[3] Justis- og politidepartementet (2000): NOU 2000:24. *Et sårbart samfunn*
[4] T K Sivertsen (2007): Risikoanalyse av samfunnskritiske IKT-systemer – teknologiske ergaringer, FFI/RAPPORT-2007/00910
[5] Statens vegvesen (2006): Nøkkeltall

Vestlandet og i Nord-Norge, er tunneler, bruer og ferjer. De siste årene har flere ferjesamband blitt erstattet av fastlandsforbindelser i form av bruer eller undersjøiske tunneler.

På veginfrastrukturen gjennomfører en rekke aktører person- eller godstransport. For persontransport på veg er bussterminaler i de store byene viktige knutepunkter. Imidlertid kan bussen stoppe på alle typer holdeplasser, og persontransport på veg avhenger derfor ikke av terminaler på samme måte som for fly-, tog- og sjøtransport.

Godsterminaler er sentrale for sortering og omlasting av varer for godstransporten. Disse er i hovedsak eid av speditører og transportører. De store speditørene og transportørene på vegsiden har alle utbygd omfattende nett av terminaler rundt om i landet. Flere har lokalisert samlastterminaler på Alnabru i Oslo, i nær tilknytning til jernbanens hovedgodsterminal.

Av hensyn til trafikksikkerhet og effektiv avvikling av transport er trafikkstyring viktig. Statens Vegvesen har fem regionale vegtrafikksentraler (VTS) som står for den kontinuerlige strømmen av informasjon i vegsystemet på riks- og fylkesvegnivå. Fra disse sentralene styres eksempelvis lyskryss, bomstasjonssignaler, datastyrte fritekstavler og fjernstyrte skilt via fjernstyringssystemer. Kameraovervåking av enkelte vegstrekninger (inkludert tunneler og bruer) skjer også herfra. I tillegg har Vegtrafikksentralen i Oslo ansvaret for Vegmeldingssentralen som formidler veg- og trafikkinformasjon ut til publikum via tekst-TV, RDS-meldinger på radio, Internett osv. Kommunene har ansvar for trafikklys og skilting på kommunal veg.[6]

Figur 3.1 Vegtrafikksentralen i Oslo. Illustrasjon: Statens Vegvesen.

Aktører, beredskap og lovverk
Samferdselsdepartementet er det overordnede departementet med ansvar for vegtransport. Statens vegvesen/Vegdirektoratet, et forvaltningsorgan under Samferdselsdepartementet, har ansvaret for planlegging, bygging, drift og vedlikehold av riks- og fylkesvegnettet. Selve produksjonsdelen ble i 2003 skilt ut i et eget selskap, Mesta. Øvrige oppgaver gjøres i hovedsak av fylkesvise Vegkontor under direktoratet. Kommunale samferdselsetater har tilsvarende ansvar for kommunale veger.

[6] S K Rodal (2002): Systembeskrivelse av norsk vegtransport, FFI/RAPPORT-2002/00807.

Det er mange instanser som har tilsyns- og kontrolloppgaver når det gjelder sikkerhet i transportsektoren. Statens vegvesen fører tilsyn og kontroll med trafikanter, kjøretøy, transportører, trafikkskoler og infrastruktur. Politiet har kontrolloppgaver mot trafikantene. Direktoratet for samfunnssikkerhet og beredskap har flere tilsynsoppgaver knyttet til transport av farlig gods på veg og jernbane. Lokale brannkorps har tilsynsoppgaver knyttet til brannsikring i norske vegtunneler og andre underjordiske veganlegg. Sjøfartsdirektoratet har ansvar for tilsyn med trygghet og miljø ved ferjedriften, i tillegg til at kommunene har tilsyns- og kontrolloppgaver knytt til parkering og tollvesenet. Statens forurensningstilsyn har også enkelte tilsynsoppgaver. [7]

Viktige lovverk innenfor vegtransportområdet er Vegtrafikkloven og generelle trafikklover. I tillegg finnes en rekke lover og forskrifter som kan knyttes til tilsynsoppgavene som er skissert i avsnittet over.

Problemområder
Et generelt problem for veginfrastrukturen er manglende vedlikehold. Standarden på vegnettet har lenge vært karakterisert som for dårlig. I tillegg har mye fokus det siste året vært rettet mot sikkerheten i vegtunneler, spesielt etter raset i Hanekleivtunnelen 1. juledag 2006.

Vegtransport er mer fleksibel enn banetransport, i den forstand at det som regel finnes omkjøringsmuligheter dersom en strekning faller ut. Likevel er belastningen på vegnettet stor, spesielt i sentrale byområder, slik at enkeltfeil ofte vil skape problemer for trafikkavviklingen. Hovedfartsårer inn og ut av de store byene er viktige i så måte.

Når det gjelder sikkerheten for trafikantene finnes flere områder som er verdt å se nærmere på:

- Tunneler ifm. brann, ras eller oversvømmelse
- Bruer eller ferjesamband ifm. kraftig uvær
- Terminaler/bygninger med mange mennesker eller tunneler ifm. viljeshandlinger
- Ulykker med farlig gods involvert

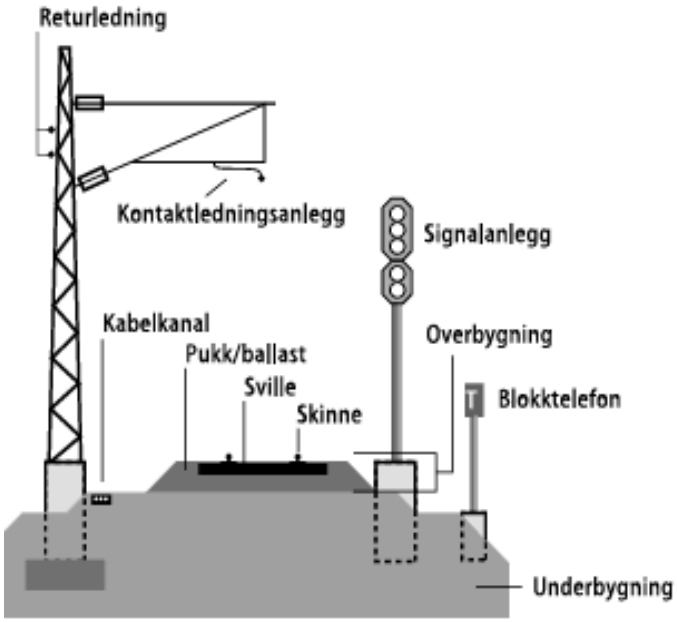
3.1.2 Banetransport

Infrastruktur
Banetransport kan skilles i tre hovedområder: jernbane, trikk og T-bane. Teknisk sett har disse områdene mye til felles med hverandre. De vil alle ha tre hovedelementer:

- Sporene som tog, trikk og t-banevogner kan kjøre på.
- Under- og overbygning, som sørger for at sporet ligger stabilt og at krav til sikkerhet, komfort, hastighet osv. kan ivaretas.
- Elektrotekniske anlegg – dette inkluderer strømforsyning for kjørestrøm til vognene, signalsystemer for trafikkstyring og teleanlegg for kommunikasjon.

Dette er prinsipielt skissert for jernbane i Figur 3.2.

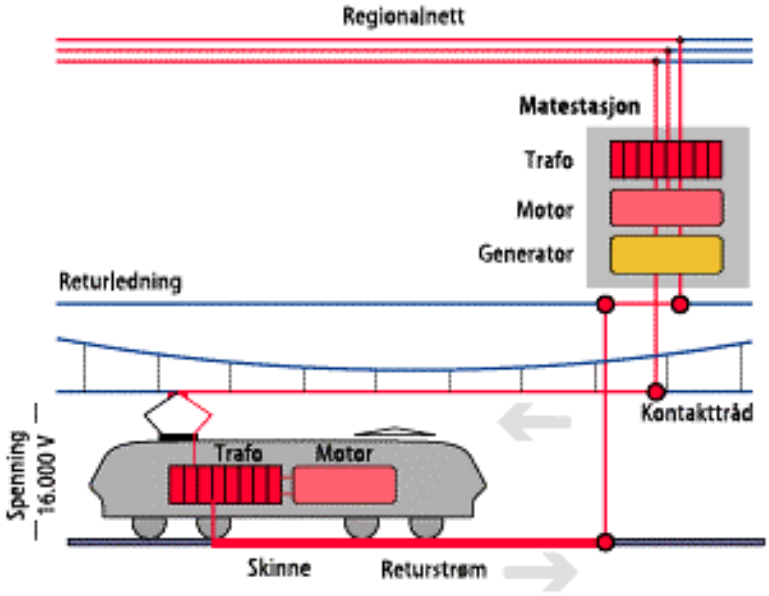
[7] Samferdselsdepartementet (2006): Om ein del saker på Samferdselsdepartementets område, St.prop. nr 68 (2006-2007)



Figur 3.2 Jernbanens kjøreveg[8]

Jernbanenettet i Norge er i hovedsak enkeltsporet, med unntak at sentrale deler av Østlandet (dobbeltspor) og jernbanestasjonene (krysningsspor). Trikk- og t-banesystemer er for det meste dobbeltsporet.

På jernbanenettet finnes både elektriske og dieseldrevne lokomotiver, mens trikk og t-bane er elektrisk drevet. Kjørestrøm hentes ut av det vanlige kraftforsyningsnettet i Norge, men konverteres til egnet frekvens og spenning i egne matestasjoner før de sendes ut på kontaktledningene langs sporene (se Figur 3.3). Det er montert fjernkontrollerte brytere som gjør det mulig å koble ut spenning i ulike seksjoner av banenettet.



Figur 3.3 Kjørestrøm til banebasert transport[9]

[8] Jernbaneverket (1999): Slik fungerer jernbanen. Webutgave oppdatert 23. mai 2007 - http://www.jernbaneverket.no/jernbanenettet/slik_fungerer_jernbanen/

Signalanleggene er viktige for sikker og effektiv trafikkavvikling. I prinsippet håndteres dette gjennom trafikklys som vognførerne må etterleve under reisen. Men for t-bane og spesielt jernbane ligger det komplekse datanettverk bak de skiftende trafikklysene. Her er banenettet oppdelt i blokker/sporavsnitt, og gjennom signalsystemene er det mulig å registrere hvilket sporavsnitt et vognsett befinner seg på og hvilken retning det kjører. Denne informasjonen brukes for å hindre at to forskjellige vognsett kjører inn på samme sporavsnitt samtidig. Dette muliggjør også systemer for automatisk togstopp, som stopper vognsettene automatisk i farlige situasjoner.[10]

Teleanlegg gir nødvendig samband (kommunikasjon) for vognframføring, og sørger for at de tekniske anleggene fungerer som de skal. Dette gjelder også for tele- og informasjonssystemer for de reisende og interne telefoni- og dataoverføringer.

Terminaler for persontransport på bane inkluderer jernbanestasjoner, trikkeholdeplasser og t-banestasjoner. Disse varierer mye i størrelse og omfang, hvorvidt de ligger i dagen eller under bakken osv. Generelt vil alle terminalene som er tilrettelagt for persontrafikk samle mange mennesker og legge få hindringer i veien for passasjerene, slik at de skal kunne kjøpe billett og komme seg ombord i vognene i løpet av få minutter. Jernbanen benyttes i tillegg til godstransport, ikke minst fra egne godsterminaler som tar inn, sorterer og distribuerer gods.

Aktører, beredskap og lovverk
Innenfor banetransport er Jernbaneverket statens forvaltnings- og fagorgan for jernbanevirksomheten. Jernbaneverket eier mesteparten av infrastrukturen knyttet til fremføring av togene, og i tillegg har de et overordnet ansvar for jernbanetrafikk i Norge.

Myndighets- og tilsynsoppgavene ligger hos Jernbanetilsynet. Dette forvaltningsorganet fører tilsyn med transportørene og Jernbaneverket.

Blant transportoperatørene er NSB AS den største på jernbanesiden, men aktører som Flytoget, Cargonet osv. opererer også på norske spor. NSB eier mesteparten av stasjonsbygningene i Norge (gjennom underselskapet ROM Eiendom).

Trikk og t-bane i Oslo drives av hhv. Oslo Sporvognsdrift AS og Oslo T-banedrift A/S, datterselskaper av Kollektivtransportproduksjon AS.[11] I Trondheim drives en trikkelinje av AS Gråkallbanen.

Lovmessig er banedrift underlagt Jernbaneloven, i tillegg til Vegtrafikkloven og de generelle trafikkreglene for alle vegfarende. Driftstillatelser og tekniske godkjenninger utstedes av Statens jernbanetilsyn, som også fører løpende tilsyn og kontroll med virksomheten.

Problemstillinger
Som for de fleste andre infrastrukturer er aldring pekt på som et problem for banetransport. Manglende vedlikehold på flere strekninger og gammelt vognmateriell kan gi problemer for trafikkavvikling. Enkeltsporede strekninger er spesielt utsatte for feil på ledningsnettet, det samme gjelder høyt trafikkerte strekninger med dobbeltspor (eksempelvis Oslotunnelen mellom Oslo S og Skøyen, som kobler sammen de gamle vestlige og østlige linjene i hovedstadsområdet).

---

[9] Jernbaneverket (1999): Slik fungerer jernbanen. Webutgave oppdatert 23. mai 2007 - http://www.jernbaneverket.no/jernbanenettet/slik_fungerer_jernbanen/
[10] Rodal, S (2003): Systembeskrivelse av den norske jernbanen, FFI/RAPPORT-2002/00808.
[11] Selskapet som ivaretar de operative funksjonene fra tidligere Oslo Sporveier. Oslo Sporveier er likevel den administrative overbygningen for mesteparten av kommunal kollektivtransport i Oslo.

I tett trafikkerte byer vil trikketransport kjøre i gater som også er åpne for normal biltrafikk. Ved feil på veginfrastrukturen vil dette også kunne forplante seg slik at trikketransporten får problemer.

Feil på signalsystemer kan gi utfordringer både for trafikkgjennomføring og personsikkerhet. Normalt vil feil på signalsystemet føre til stopp i banetransport, evt. manuell drift med redusert kapasitet. I verste fall kan dette føre til at to vognsett kjører inn på samme strekning samtidig og kolliderer.

Elektrisk dreven banetransport er kritisk sårbar overfor svikt i kraftforsyningen. Kraftforsyningsbrudd vil medføre umiddelbar stopp i t-bane- og trikkesystemer.

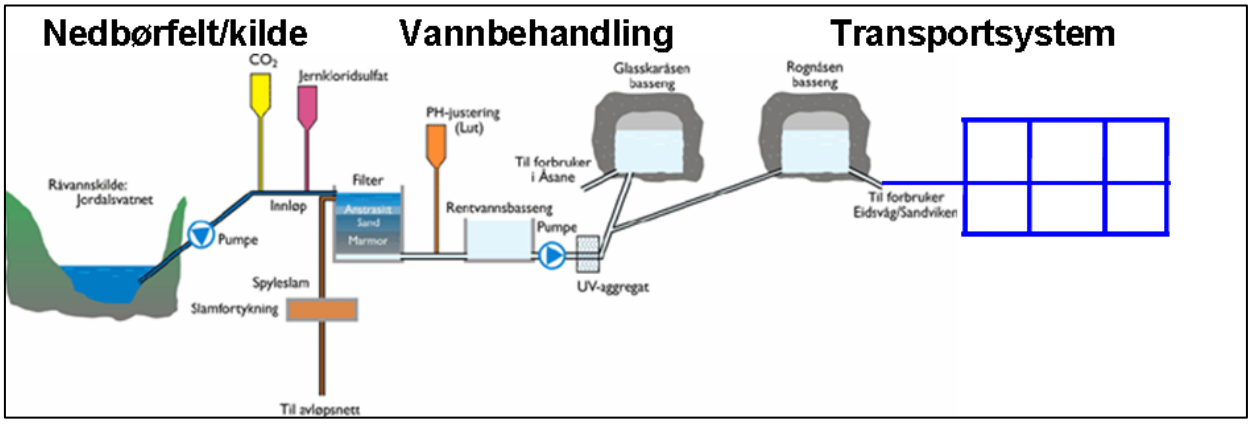
Deler av jernbaneinfrastrukturen ligger i værharde og rasutsatte områder. Dette kan føre til forsinkelser i trafikken, i verste fall personskade ved avsporinger og ras på linjen.

De siste årene har banetransport vist seg som en attraktiv arena for viljeshandlinger. Utover tradisjonelt hærverk og kriminalitet (lommetyveri) har flere store terrorhandlinger blitt gjennomført enten mot vogner i trafikk eller stasjonsområder. Kjente eksempler er bl.a. angrepene mot pendlertog i Madrid i 2004 og aksjonene mot t-bane og buss i London i 2005.

3.2 Vann

Infrastruktur

Vannforsyningssystemet omhandler alt fra nedbørfelt, kilde, vannbehandlingsanlegg og transportsystem.



Figur 3.4 Prinsippskisse av vannforsyningssystemet

NORVAR har utgitt en rapport som omhandler gjenanskaffelseskostnader for norske VA-anlegg, tallene under er gjengitt fra denne rapporten.[12] Om lag 20 % av all kommunal infrastruktur er knyttet til vannforsyning. Oversikt over verdiene for vann er (milliarder NOK):

[12] NORVAR (2004): Gjenanskaffelsekostnader for norske vann- og avløpsanlegg, NORVAR-rapport 130.

Råvannstransport	7.9
Grunnvannsanlegg	0.9
Vannbehandling	5.1
Transport og distribusjon	184.1
Stikkledninger	21.0
Anlegg for enkelthus/husgrupper	9.0
Sum	**228.0**

De største verdiene ligger i transportsystemet. Samlet er det i Norge 46.000 km hovedvannledninger.

Aktører, beredskap og lovverk
De største eierne av vannverk er kommuner. Det finnes en del private vannverk, i hovedsak mindre vannverk. I tillegg finnes det en del interkommunale vannverk som typisk er engros-leverandører. Noen kommuner har organisert vannverkene som egne foretak (KF) eller selskap (AS). For de kommunale vannverk er kommunene både eier av infrastruktur, utfører egenkontroll/internkontroll (IK Mat) og tilsynsmyndighet. Samlet er det om lag 1600 vannverk som leverer vann til mer enn 50 personer (og som da er rapporteringspliktige).

Drift utføres enten i egen regi eller er utsatt til private. Kommunale selvkostregimer gjør at kostnader til drift og investeringer kan dekkes inn via vann- og avløpsgebyr. Forskrift om kommunale vann- og avløpsgebyrer[13] bestemmer at de samlede gebyrinntektene for vann og avløp ikke kan være større enn utgiftene (selvkostprinsippet). Med utgangspunkt i dette kan lokale politikere bestemme hovedlinjene i vannforsyningen, gjennom å godkjenne hovedplaner, fastsette gebyrnivå etc.

Relevante lovverk er regulert av en rekke departementer. Kommunal- og regionaldepartementet, Miljøverndepartementet, Helse- og omsorgsdepartementet, Justisdepartementet er blant de viktigste, men totalt er vannforsyningen underlagt et lov- og forskriftsregime som impliserer minst ni forskjellige departementer. NORVAR har laget en egen oversikt over dette regimet i den såkalte VA-jusdatabasen på http;/www.norvar.no.

Et utvalg av lovene/forskriftene som gjelder for vann og avløp er angitt under, som illustrasjon over mangfoldet innen VA:

Plan- og bygningsloven, Lov om arbeidervern og arbeidsmiljø m.v. – Arbeidsmiljøloven, Forskrift om vannforsyning og drikkevann (Drikkevannsforskriften), Lov om vassdrag og grunnvann (vannressursloven), Lov om vern mot forurensninger og om avfall (Forurensningsloven), Produktkontrolloven, Kommunehelsetjenesteloven, Helse- og sosialberedskapsloven, Næringsmiddelloven, Lov om brann og eksplosjonsvern, Lov om sivilforsvar, Lov om vass- og kloakk-avgifter, Lov om tilsyn med elektriske anlegg og elektrisk utstyr, Forvaltningsloven, Oreigningsloven, Gjødselvareloven, Matloven, Lov om offentlige anskaffelser, Kjøpsloven, Forbrukerkjøpsloven.

NOU 2006:6 ”Når sikkerheten er viktigst” anbefalte at lovverket knyttet til VA ble organisert under en ny sektorlov for vann og avløp (”VA-lov”). Dette er et naturlig forslag, med tanke på alle de små kommuner og vannverker, med relativt små ressurser, som har et relativt omfattende lovverk og mange offentlige etater å forholde seg til.

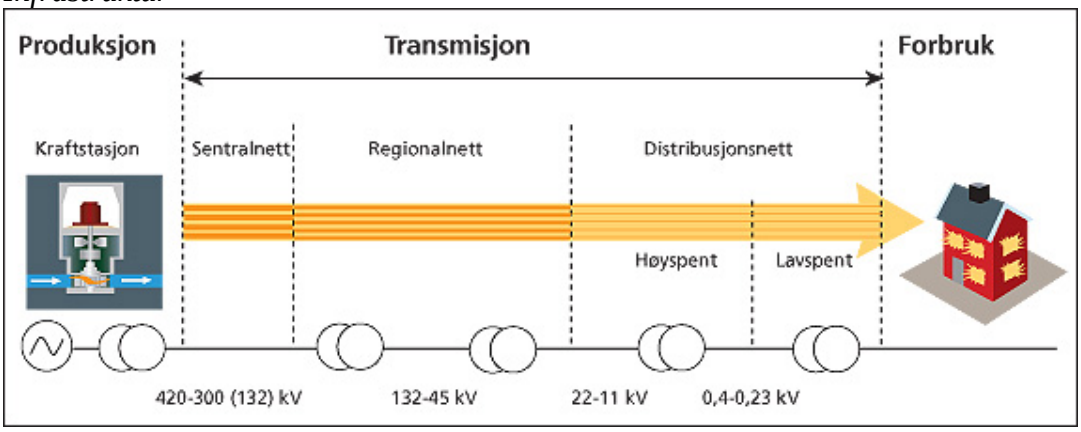
[13] Miljøverndepartementet (2000): Forskrift om kommunale vann- og avløpsgebyrer.

Mattilsynet har tilsynsroller innenfor drikkevann, og Folkehelseinstituttet har en rolle som nasjonal rådgiver.

Ufordringer
Blant utfordringene for vann- og avløpssystemene er en generelt aldrende infrastruktur og klimapåvirkninger. Klimaendringer kan gi endret vannkvalitet, for eksempel gjennom introdusering av nye patogener i drikkevannet, utfordringer knyttet til ekstremnedbør og avrenning etc. Kundeforventningene til rent og godt drikkevann blir også større. Samtidig sliter mange kommuner i dag med å fremskaffe kvalifiserte VA-ingeniører.

3.3 Kraftforsyning

Infrastruktur



Figur 3.5 Kraftsystemet (fra http://www.nve.no)[14]

Elektrisk kraft produseres i kraftstasjoner og leveres ut på overføringsnettet, for deretter å bli transportert til den enkelte sluttbruker. Overføringssystemet omfatter mange ulike komponenter: Kraftledninger, jord- og sjøkabler, transformatorer, brytere mm. på ulike spenningsnivå osv. Figuren over viser en skjematisk framstilling av det norske kraftsystemet fra produksjon til forbruker. Flere forbrukere og kraftstasjoner er også tilknyttet andre nettnivåer enn det som figuren viser.

Norsk kraftforsyning er hovedsakelig basert på vannkraft (utgjorde 99% av produsert elektrisk kraft i 2005). I tillegg er det noe vindkraft og gasskraft i drift, og det foreligger mange planer og konsesjonssøknader for utbygging av både vind- og gasskraftanlegg. Overføringsnettet deles inn i sentralnett (”hovedveiene i kraftforsyningen”), regionalnett som binder sentralnettet og distribusjonsnettet sammen, og distribusjonsnett som er det lokale nettet for distribusjon fram til sluttbrukerne. Mens elektrisitetsproduksjon er underlagt konkurranse gjennom energiloven, er elektrisitetsnett å betrakte som naturlige monopol. Som følge av dette er nettvirksomheten monopolregulert og nettselskapene får fastsatt en øvre ramme for tillatte årlige inntekter. Reguleringen – som omtales som monopolkontroll – skal sikre brukernes rettigheter, legge til rette for et velfungerende kraftmarked og en effektiv drift og utvikling av nettet.

Aktører, lovverk og beredskap
Olje- og energidepartementet er ansvarlig departement for kraftforsyningen i Norge. Tilsynsvirksomhet for kraftforsyningen er i hovedsak lagt til Norges vassdrags- og

[14] Mer info om kraftsystemet og kraftforsyning finnes på www.nve.no og i OEDs faktahefter om energi og vannressurser i Norge (www.regjeringen.no/en/dep/oed/)

energidirektorat (bl.a. generell kraftberedskap, damsikkerhet, monopolregulering osv.), men DSB har tilsynsoppgaver overfor elektriske anlegg.

Det er 175 selskaper som produserer elektrisk kraft i Norge. Staten, gjennom Statkraft, eier ca 37 % av produksjonskapasiteten i Norge. Kommuner og fylkeskommuner eier ca 50 %, mens resten er i private hender.[15]

Totalt er det 176 selskaper som har nettvirksomhet på ett eller flere nivå. Kommuner og fylkeskommuner eier det meste av regionalnettene og lokale distribusjonsnett. Staten, gjennom Statnett, eier størsteparten (87%) av Sentralnettet.

Statnett er gjennom egen konsesjon utpekt til å utøve systemansvaret i det norske kraftsystemet. Systemansvaret skal legge til rette for et effektivt kraftmarked og en tilfredsstillende leveringskvalitet i kraftsystemet. I praksis innebærer dette at Statnett skal sikre momentan balanse mellom samlet produksjon og forbruk, hensyn tatt til kraftutveksling med omkringliggende kraftsystemer og eventuelle flaskehalser i nettet. Rent operativt håndteres dette ansvaret fra Statnetts Landssentral i Oslo. I tillegg har Statnett tre regionssentraler, Sør, Midt og Nord, med ansvar for direkte fysiske driftsoppgaver (inn- og utkoblinger av stasjonene via fjernstyring, vedlikehold o l) innenfor sitt geografiske område. Produksjonsselskaper og øvrige nettselskaper vil også ha egne driftssentraler som ivaretar tilsvarende oppgaver innenfor sitt ansvarsområde (f.eks. Hafslunds driftssentral for Østlandsområdet).

Kraftmarkedet håndteres av den nordiske kraftbørsen Nord Pool, som driver handel og clearing av fysiske og finansielle kraftkontrakter i Norden. Det er i dag om lag 330 aktører som handler i ett eller flere av Nord Pools markeder. Aktørene på Nord Pools spotmarked er foruten kraftprodusenter og industrien også distribusjonsselskaper, strømleverandører og kraftmeglere.

Den sentrale loven ift. kraftforsyningen er Energiloven. Andre relevante lovverk er Vannressursloven, Vassdragsreguleringsloven, Industrikonsesjonsloven, Oreigningsloven, Naturgassloven, Produktkontrolloven, Lov om merking av forbruksvarer, Sikkerhetsloven, Kraftledningsregisterloven, Plan- og bygningsloven (KU-forskriften) og Lov om tilsyn med elektriske anlegg og elektrisk utstyr.

Problemområder
Som for øvrige infrastrukturer karakteriseres kraftforsyningen av økende alder på komponentene og reduserte investeringer. Reinvesterings- og vedlikeholdstakten er relativt lav, og det er bekymring om aldrende komponentene takler en generelt økende belastning og et endret driftsmønster. En annen utfordring som kraftbransjen står overfor er forhold knyttet til bemanning og kompetanse. Siden midt på 1990-tallet har det vært en betydelig nedbemanning og omstrukturering i kraftbransjen (omorganisering, utskillelse av entreprenørvirksomhet mm), og særlig innenfor nettvirksomheten har det kommet til mange nye oppgaver som følge av nye forskrifter og reguleringer.

Overføringsnettet ligger til dels i værharde områder. Selv om sentralnettet i stor grad er dimensjonert for å takle langt kraftigere belastninger enn man normalt vil se, vil regionale nett og spesielt distribusjonsnett ofte være designet etter mindre ambisiøse krav. Utfall i nettet som følge av kraftige vindkast, nedising av linjer, trefall e.l. kan gi omfattende avbrudd i kraftforsyningen. Det er usikkert hvilken betydning forventede klimaendringer vil få for påkjenningene på kraftsystemet.

[15] Justisdepartementet (2006): Når sikkerhet er viktigst, NOU 2006:6. OEDs faktahefte 2008.

Kraftbransjen er i økende grad avhengig av robuste informasjonssystemer. Feil i drifts- og kontrollsystemene vil i beste fall føre til mindre optimal utnyttelse av kraftsystemet, i verste fall føre til et fullstendig systemsammenbrudd. Eksterne angrep mot driftssystemer via Internett er også en mulighet.

3.4 IKT i kritisk infrastruktur

IKT-systemer blir stadig viktigere innen kritisk infrastruktur. Eksempel er signalsystemer for togtrafikk og driftssystemer for elektrisitetsproduksjon. Trenden er at slike systemer i større og større grad utvikles basert på hyllevare (f.eks. MS Windows) i stedet for rene spesiallagede systemer. Man ser også oftere at slike systemer kobles mot for eksempel administrasjonsnett, som igjen gjerne er koblet mot Internett.

Den økende bruken av IKT sammen med økt bruk av hyllevare og økt sammenkobling mot andre nett gjør at sårbarheten når det gjelder IKT-trusler er større enn før. Innenfor mange kritiske infrastrukturer er man imidlertid lite vant til å tenke på denne typen trusler.

Når det gjelder sikring av IKT-systemer og den informasjonen som ligger i disse systemene snakker man gjerne om sikring av[16]:

- **Konfidensialitet;** "det å sikre at informasjonen er tilgjengelig bare for dem som har autorisert tilgang"
- **Integritet;** "det å sikre at informasjonen og behandlingsmetodene er nøyaktige og fullstendige" – innebærer at uvedkommende ikke kan endre informasjon eller systemet som behandler informasjonen
- **Tilgjengelighet;** "det å sikre autoriserte brukeres tilgang til informasjon og tilhørende ressurser ved behov"

Når det gjelder drifts- og styringssystemer vil ofte integritet og tilgjengelighet være vel så viktig som konfidensialitet – man er avhengig av at systemet er tilgjengelig og gjør de oppgavene det er satt til basert på riktig informasjon.

Typiske trusler kan være[17]:

- **Utilsiktede menneskelige feil:** Brukerne av IKT-systemer, og de som bygger, drifter og vedlikeholder systemene, er mennesker; den menneskelige faktor er derfor noe man må ta hensyn til ved design av systemer og utforming av regler og rutiner for bruk.
- **Utro tjenere:** Egne ansatte eller innleide som er misfornøyde, har mistet jobben, har egen agenda, etc.
- **Misbruk av ressurser:** Ansatte benytter dataressurser til privat og/eller ulovlig bruk, noe som kan føre med seg økt sårbarhet.
- **Single-point-of-failure;** Avhengighet av enkeltkomponenter gjør at man blir svært sårbar dersom disse skulle falle bort.
- **Tjenestenekting:** Oppstår når en tjeneste blir utilgjengelig uten at dette er planlagt, for eksempel som følge av et målrettet angrep i form av store mengder nettverkstrafikk. Skjer ofte som et resultat av virus-/orm-angrep.
- **Datainnbrudd:** En person oppnår uautorisert tilgang til et system. Det er typisk to typer angripere: Såkalte "script kiddies" som benytter verktøy utviklet av andre, og de profesjonelle crackerne. Begge grupper utgjør en stor trussel og kan utføre handlinger som vil påføre virksomheten store tap.

[16] Definisjonene under er hentet fra NS 7799:2003
[17] Basert på SIS trusselrapport oktober 2005: http://www.norsis.no/trusler/Manedsrapporter/213.html

- **Virus og ormer:** Tiden fra en sårbarhet oppdages til det dukker opp et virus eller en orm som utnytter denne, blir stadig kortere. Det er derfor en stor utfordring å sørge for å holde systemer oppdatert med siste sikkerhetspatch og ha oppdaterte virusfiltre.
- **Sikkerhetshull i standard programvare:** Ingen programmer leveres feilfrie, men når feilene utgjør en sikkerhetsrisiko, kan de utgjøre en stor trussel mot virksomhetens IKT-systemer. Sikkerhetsoppdateringer bør anvendes så snart som mulig, men helst etter at de er blitt testet ut først.
- **Sikkerhetshull i spesialutviklet programvare:** Virksomheter som selv administrerer eller utfører programvareutvikling, er i stor grad eksponert for risiko ved at utilsiktede feil eller tilsiktet ondsinnet kode legges inn i programvaren.

Ofte har man et fokus på viljeshandlinger innen IKT-sikkerhet, selv om hendelser også kan inntreffe på grunn av teknisk svikt eller menneskelig feil. Viljeshandlinger trenger imidlertid ikke å være rettet mot et enkeltsystem, men kan være en del av generelle angrep, for eksempel virus/ormer og lignende, og datainnbrudd som har som mål å få tilgang til dataressurser.

I tillegg til IKT-systemene som er viktige innen en infrastruktur vil man ofte være avhengig av IKT-systemer for samband. Dette ligger litt på siden av de IKT-systemene vi har fokus på i DECRIS-prosjektet, men er likefullt noe det er viktig å ha i bakhodet.

4 Prinsipielle problemstillinger i vurderinger av risiko og sårbarhet for kritisk infrastruktur

Dette kapittelet skal i første rekke presentere viktige metodiske og praktiske utfordringer ved å gjennomføre risikoanalyser av kritisk infrastruktur.

4.1 Avgrensning av analysesystemet og valg av nivå

I DECRIS-arbeidet inkluderes kritiske infrastrukturer som kraftforsyning, transportsystemer og vannforsyning. Selv innenfor et avgrenset område, f.eks. en kommune, kan dette være store og komplekse systemer. Typisk vil infrastrukturen innebære:

- En produsent eller leverandør av tjenester over infrastrukturen
- En kunde som får levert tjenester via infrastrukturen
- Et fysisk nettverk som bringer produkter fra leverandør til kunde
- Drifts, styrings- og kontrollsystemer som sørger for en effektiv og sikker tjenesteleveranse over nettverket.

Med andre ord innebærer systemet så vel teknologiske som menneskelige og organisatoriske aspekter, både tunge mekaniske innretninger og logiske IKT-infrastrukturer, med et spenn i nivå fra (inter)nasjonale nettverk til komponenter i den enkeltes husstand. Innenfor dette spennet er det mange ulike analyser som kan gjøres, og avgrensninger og valg av nivå på analysen blir derfor avgjørende.

Noen forhold å vurdere i denne sammenheng er:

- Skal analysen konsentrere seg om teknologi, eller skal man også inkludere menneskelige og organisatoriske aspekter?

- Skal man kun se på infrastrukturen på overordnet systemnivå, eller må man også gå inn og gjøre detaljerte sårbarhetsvurderinger av enkeltkomponenter i infrastrukturen? Parallelt med dette blir det et spørsmål om man skal velge en top-down eller bottom-up tilnærming i analysen.
- Hvilke konsekvenser ser man på i analysen: for systemet, for systemeieren eller for samfunnet?
- Inkluderer man alle relevante fare- og trusselsituasjoner, eller fokuserer man bare på noen spesielle?
- Skal IKT-løsninger og drifts- og styringssystemer inkluderes i analysen?

Et beslektet spørsmål er muligheten for å lage en modell av systemet som skal analyseres. En form for modellering av systemet som skal analyseres er som regel nødvendig, selv om selve risikoanalysemetoden som benyttes ikke er modellbasert. En god felles modell er viktig både for å kunne diskutere risiko i analysegruppen og for å kunne kommunisere resultatene av analysen videre. Som diskusjonen over viser vil imidlertid kompleksiteten i kritiske infrastrukturer være stor, kanskje så stor at det kan vise seg vanskelig å utvikle gode modeller som tar inn over seg alle relevante forhold ved systemet som skal analyseres.

4.2 Tilgang på kompetanse og informasjon

Risikoanalyser krever god oversikt over systemet som skal analyseres. Her ligger en av hovedutfordringene ved analyser av kritisk infrastruktur.

I tillegg til å forstå de funksjonene som infrastrukturen skal utføre, må man ha kompetanse om systemets arkitektur, komponentene som inngår, eksisterende sikkerhetsløsninger, brukerne av systemet og organisatoriske rammebetingelser. Man må også ha kunnskap om mulige sårbarheter systemet kan ha og hvilke farer og trusler det kan utsettes for.

Informasjonsinnsamlingen for analysen blir derfor raskt en krevende oppgave. For det første er det svært mange forhold som må forstås, og i tillegg vil dokumentasjon av relevante forhold ofte være mangelfull, utdatert eller ikke-eksisterende. Alternativet vil være å bruke eksperter på systemet for å få informasjon, kanskje også for å få risikovurderinger direkte. Uansett vil en klar målsetting med analysen og hensiktsmessige avgrensinger av oppgaven være viktig for å styre informasjonsinnhentingen i riktig retning.

4.3 Gjenbruk av resultater

Et interessant spørsmål er i hvilken grad det er mulig å gjenbruke informasjon fra risikoanalyser på et «lavere» nivå i systemet som skal analyseres. Dette er en fristende tanke, siden resultater fra eksisterende analyser kan avhjelpe informasjonsinnhenting og gi innspill til vurderinger av sannsynlighet og konsekvens av ulike hendelser. Innenfor en sektor kan analyser av delsystemer benyttes som innspill til hele sektoranalyser, mens tverrsektorielle analyser kan anvende resultatene fra rene sektoranalyser. BAS5-metode for nasjonal prioritering legger opp til en slik tilnærming.[18]

I den grad dette faktisk er mulig avhenger av en rekke forhold, bl.a.:

[18] S. Henriksen, K. Sørli, and L. Bogen, "Metode for identifisering og rangering av kritiske samfunnsfunksjoner," FFI/RAPPORT 2007/00784, 2007

- Hvorvidt systemet har endret seg så mye at resultatene fra gamle analyser fremdeles er gyldige
- Hvorvidt analysene tar utgangspunkt i tilsvarende fare- og trusselsituasjoner
- Hvorvidt konsekvenser for ulike hendelser vurderes på samme nivå
- Hvorvidt tidligere risikovurderinger kan plugges rett inn i sannsynlighets- og konsekvensskalaene som anvendes i analysen

Med andre ord er det en fare for at tidligere analyser kan være gjennomført med et annet formål og en annen innretning enn det man planlegger i den kommende analysen. I så fall vil tidligere analyser i beste fall være en indikator på relevante risikoforhold, uten at resultatene kan anvendes direkte.

4.4 Fare- og trusselidentifikasjon: hvordan inkludere både safety og security i analysene?

I Norge er det en tradisjon for å skille mellom begrepene safety og security, der safety brukes om vern mot ikke-villede hendelser og security om vern mot viljeshandlinger. Ingen etablerte norske begrep skiller mellom disse to. Dette viser seg i praksis også vanskelig å etablere, siden noen miljø utelukkende bruker sikkerhet om security, mens andre miljø utelukkende bruker sikkerhet om safety.[19] I forlengelsen av dette vil flere benytte begrepet farer om ulykker og teknisk svikt, mens trusler er hendelser som forutsetter en bevisst angriper med intensjon og kapasitet til å gjennomføre en uønsket handling. Uansett er terminologien på området fremdeles uklar.[20]

Uavhengig av begrepsbruken er det flere metodiske utfordringer ved å inkludere begge disse aspektene i samme risikoanalyse. Risikoanalysene har sitt utspring i prosessbasert industri, som f.eks. kjernekraft og petroleum, med formål å vurdere konsekvenser av ulike tekniske feilsituasjoner og tilhørende sannsynligheter. Sannsynlighetsvurderinger ble her ofte angitt som frekvenser, basert på tilgjengelig statistikk for feilraten til ulike komponenter, hvor ofte ulike ulykker har inntruffet osv.

Tilnærmingen med frekvensvurderinger vil imidlertid være problematisk når det gjelder viljeshandlinger, ikke minst fordi tilgjengelig statistikk er både begrenset og usikker. Samtidig er trusselbildet knyttet til viljeshandlinger stadig i endring, og det er vanskelig å finne god og balansert informasjon om temaet (spesielt informasjon som er offentlig tilgjengelig). Alternativet kan være rene kvalitative, subjektive vurderinger, hvor eksperter gir en sannsynlighetsverdi basert på hvor mye de tror på at ulike hendelser kan inntreffe. Uansett må sannsynlighetsvurderingene gis iht. samme skala for både fare- og trusselhendelser dersom de skal kunne sammenlignes i en analyse.

4.5 Hvilke tap skal vurderes iht. konsekvenser?

For å kunne vurdere risiko for ulike uønskede hendelser opp mot hverandre, må en kunne måle konsekvens med en felles metrikk. Det å lage og på en god måte anvende en slik felles metrikk, er ofte en av hovedutfordringene i en risikoanalyse.

Det finnes flere ulike tap som konsekvenser kan måles mot, f.eks.:

- Helse, miljø og sikkerhet; tap av liv og personskade samt skade på miljø og omgivelser.

[19] Det er gjort et forsøk på avklaring i et vedlegg til Infrastrukturutvalgets rapport, "Når sikkerhet er viktigst" (NOU 2006:6). Sikkerhet omfatter der både security (kalt sikring) og safety (kalt trygghet).

[20] T K Sivertsen (2007): Risikoanalyse av samfunnskritiske IKT-systemer – teknologiske ergaringer, FFI/RAPPORT- 2007/00910

- Økonomiske tap; tapt eller forsinket produksjon, skade på utstyr og eiendom, svindel og tyveri, erstatningsansvar, tapt arbeidstid
- Skader på tillit og anseelse; tillit hos kunder, marked, samfunn, ansatte og eventuelt regulerende organ (offentlig tilsyn, konsesjonsutstedere osv) (kan også sees på som langsiktige økonomiske verdier)
- Redusert trygghetsfølelse i befolkningen som følge av ulike hendelser
- Stans i tjenesteleveranser

I utgangspunktet er det ikke trivielt å sette opp en konsekvensklasse som ivaretar alle disse mulige tapene. Noen alternativer kan være å benytte flere skalaer i analysen, en for hvert verditap. En utfordring vil være å avstemme de ulike konsekvensskalaene mot hverandre, slik at tapene er sammenlignbare. Har man først kommet så langt, kan man kanskje vurdere en felles konsekvensklasse likevel, hvor f.eks. alle konsekvenser omregnes til økonomiske verdier. Imidlertid er det vanskelig å fastsette hva f.eks. en redusert trygghetsfølelse skal innebære i kroner og øre. I tillegg er det ikke nødvendigvis slik at tapene kan vurderes til å ha samme verdi på tvers av hele spekteret av fare- og trusselsituasjoner (et menneskeliv kan f.eks. verdsettes forskjellig i en trafikkulykke sammenlignet med et terrorangrep).

4.6 Hvordan håndtere følgekonsekvenser?

Konsekvenser kan måles på ulike nivåer, f.eks.:

- For systemet selv (f.eks. nedetid)
- For systemeier (f.eks. skade på egne ansatte, egne økonomiske tap)
- For kunder og «samfunnet» forøvrig (f.eks. andres økonomiske tap)

Et avklart forhold til hvilket nivå av konsekvenser som vurderes er derfor viktig. Her er det også viktig å bestemme hvorvidt kjeder av konsekvenser skal tas hensyn til.

De fleste kritiske infrastrukturer er såpass sentrale for samfunnet at feilsituasjoner raskt vil ramme andre samfunnsfunksjoner. Dette kan igjen føre til ytterligere konsekvenser på lengre sikt. For eksempel vil et strømbrudd av en viss varighet kunne føre til at ulike elektroniske kommunikasjonstjenester slås ut, som igjen kan medføre at man ikke får varslet nødetatene i forbindelse med ulykker osv. Sammenbruddet i kommunikasjonstjenestene kan på sin side medføre økte reparasjonstider for å utbedre strømbruddet. Slike konsekvenskjeder og gjensidige avhengigheter er en viktig del av sårbarheten i et moderne samfunn. Dette er også meget vanskelig å behandle på en helhetlig måte i risiko- og sårbarhetsanalyser.

En mye brukt teknikk for å illustere slike forhold er bruk av konsekvensmatriser, der ulike infrastrukturer og samfunnsfunksjoner settes langs begge akser i en todimensjonal matrise. Et kryss mellom f.eks. kraftforsyning og elektronisk kommunikasjon vil da angi at funksjonene er avhengige av hverandre. Selv om dette gir en generell illustrasjon av gjensidige avhengigheter, er det vanskelig å benytte dette som utgangspunkt for gode analyser (i praksis vil man ofte se at «alt er avhengig av alt»). Et steg videre er å tegne kausaldiagrammer eller hendelsestrær, hvor konsekvensene av en innledende hendelse tegnes systematisk. Imidlertid vil slike diagrammer raskt kunne bli svært store.

4.7 Sensitive resultater

Risikoanalysen kan komme til å kreve bruk av sensitiv informasjon, enten kommersielle hemmeligheter for oppdragsgiver eller informasjon som er gradert iht. Sikkerhetsloven. Dette må kunne håndteres løpende av gruppen som gjennomfører analysen. I tillegg vil dette legge føringer

på hvilken informasjon fra analysene som kan publiseres offentlig og hvilket innhold kommunikasjon om risikoforholdene kan ha.

4.8 Valg av tiltak - beslutning

Selv om man har en prioritert liste over relevante risikoforhold og tilhørende tiltak, er det ikke enkelt å bestemme hvilke av tiltakene som skal implementeres. I utgangspunktet vil mange velge en optimaliseringstilnærming basert på kosteffektivitet eller kost-nytte, men i mange tilfeller vil det være vanskelig å estimere kostnad, effektivitet og nytte. Det kan også være at beslutningsprosessen ikke legger til rette for en slik "optimal" løsning.

Beslutninger om tiltak vil avhenge av beslutningstakernes forståelse av problemstillingen og aksept overfor ulike risikoforhold. I praksis vil tiltak innenfor kritisk infrastruktur være politiske beslutninger (f.eks. om det skal bygges infrastruktur gjennom naturskjønne områder, hvor omfattende terrorsikringstiltak som skal implementeres etc.), og her vil det være mange hensyn å ta utover ren sikring av infrastrukturene. Körte et al. (2002) peker i retning av at slike avgjørelser ofte først tas etter at konsensus er oppnådd blant beslutningstakerne, og slike avgjørelser vil ikke nødvendigvis være optimale sett fra en analytikers ståsted.[21] Oppfølgingsarbeidet etter stormen Gudrun i januar 2005 kan underbygge dette. På grunn av de store konsekvensene for svensk kraftforsyning mente politikerne at dette var en uakseptabel hendelse, og det ble besluttet ved lov at etter 2011 skulle ingen utfall i svensk kraftforsyning vare i mer enn 24 timer. I ettertid har kostnadene for å implementere nødvendige tiltak blitt beregnet til ca 60 milliarder svenske kroner. Konsekvensene av Gudrun var på sin side beregnet til ca 4 milliarder kroner, og stormen ble vurdert til å være en 100-årsstorm.[22] En beslutning med enorme investeringskrav ble tatt etter at politisk konsensus ble oppnådd, men løsningen kan knapt kalles optimal. Eksempelet underbygger behovet for at risikoanalysen må tilpasses beslutningsprosessen den skal understøtte.

5 Tverrsektoriell risikoanalyse, metodikk, beslutningsprosess og risikokommunikasjon

5.1 Utfordringer med tverrsektoriell risikoanalyse

Som diskusjonen i kapittel 4 vil vise, er det flere utfordringer som må håndteres for å kunne gjennomføre en risikoanalyse av en kritisk infrastruktur. Disse utfordringene vil bare bli større når man skal se på risiko på tvers av sektorer.

DECRIS vil se spesielt på to problemstillinger med tverrsektorielle risikoanalyser.

- Hvilken metode kan understøtte slike analyser?
- Er det aspekter rundt beslutningsprosess og risikokommunikasjon som må ivaretas i analysen og ved metodeutviklingen?

Knyttet til metode har gjerne aktørene innenfor en sektor sin egen metodiske tilnærming for risikoanalyser (eksempler er HelseRos, SamRos osv). Per i dag finnes det få (om noen) omforente

[21] Kørte, J., Aven, T. and Rosness, R. (2002): On the use of risk analysis in different decision settings. Paper presented at ESREL 2002, Lyon, March 19-21, 2002.
[22] Risk and Decision Systems for Critical Infrastructures (DECRIS) - Prosjektbeskrivelse

tverrsektorielle metodikker. Enhver tverrsektoriell risikoanalyse må derfor regne med noe metodeutvikling, som også svarer på problemstillingene som er skissert i avsnitt 2.2.

I BAS5-prosjektet er det foreslått en metode for identifisering og rangering av kritiske samfunnsfunksjoner.[23] En hypotese fra dette arbeidet er at det knapt er mulig å prioritere kritiske samfunnsfunksjoner uten samtidig å gjøre seg opp en grunnleggende mening om hvilke risiko de er utsatt for eller utsetter andre for. Det vil si at det må forutsettes at det foretas risiko- og sårbarhetsvurderinger på sektor- og virksomhetsnivå, og den foreslåtte tilnærmingen har derfor store likhetstrekk med en tverrsektoriell risikoanalyse. Denne kan fungere som utgangspunkt for arbeidet i DECRIS. I tillegg er det gjennomført flere større risikoanalyser innenfor kommuner og fylker de siste årene, som dokumentert i et eget DECRIS-arbeidsnotat.[24] Inspirasjon fra disse bør brukes som et ledd i metodeutviklingen i DECRIS.

Imidlertid vil en ny metodisk tilnærming bare finne aksept blant brukerne dersom den er tilpasset de miljøene og de oppgavene den skal anvendes til. Det er derfor nødvendig å studere beslutningsprosessen knyttet til tverrsektorielle risikoanalyser som en del av DECRIS-prosjektet. Relevante problemstillinger i så måte er:

- Hvordan presentere resultater fra risikoanalysene slik at de blir forstått av oppdragsgiver
- Hvordan publisering av informasjon fra risikoanalyser, kanskje spesielt gjennom media, påvirker opinionen.

5.2 Hovedtrinn i en beslutningsprosess

En risikoanalyse skal normalt danne et beslutningsgrunnlag for oppdragsgiver, i form av at han får en prioritert liste over tiltak som kan redusere identifiserte risikoforhold. Når det skal utvikles en metodikk for tverrsektorielle risikoanalyser er det derfor nødvendig å forstå hvordan selve beslutningsprosessen i analysen vil foregå.

Aven (2007) foreslår følgende hovedtrinn i en generell beslutningsprosess:

1. Beslutningssituasjon og stakeholders/interessenter
    a. Hva er problemstillingen?
    b. Hva er alternativene?
    c. Hva er rammebetingelsene?
    d. Hvem berøres av beslutningen?
    e. Hvem skal ta beslutningen?
    f. Hva slags strategier brukes for å komme fram til en beslutning?
2. Målsettinger, preferanser, godhetsmål
    a. Hva ønsker de ulike interessenter?
    b. Hvordan vektlegge de ulike goder og ulemper?
    c. Hvordan uttrykkes og kartlegges godheten av de ulike alternativer?
3. Bruk av ulike former for virkemidler, herunder ulike former for analyser som skal gi beslutningsunderlag
    a. Risikoanalyser
    b. Kost-nytteanalyser
    c. Kost-effektivitetsanalyser
4. Gjennomgang og vurderinger av beslutningstaker. Beslutning

[23] S Henriksen, K Sørli, L Bogen (2007): Metode for identifisering og rangering av kritiske samfunnsfunksjoner, FFI/RAPPORT-2007/00874.
[24] I Bouwer Utne, P Hokstad, J Vatn (2007): DECRIS – Sammendrag ROS-analyser.

I arbeidet med å utvikle en metodikk for ROS-analyser og som basis for empiriske studier vil det være hensiktsmessig å diskutere interessentene i detalj. Det skilles mellom:

- De som aktivt er med i formelle og uformelle arenaer der beslutninger fattes (involverte)
- De som kun blir berørt av beslutningene som er fattet (berørte)

Formatet på risikoanalysen og måten vi kommuniserer om risiko på vil være forskjellig for de involverte i beslutningen kontra de som er berørte.

En videre analyse av direkte involverte parter i beslutningsprosessen indikerer følgende hovedaktører:

- Analytiker og/eller fasilitator
- Fagekspertise
- Formelle beslutningstakere
- Representanter for de som berøres av beslutningen. Her er det snakk om både de som berøres av risiko involvert, men også de som skal realisere risikoreduserende tiltak, jobbe med beredskap osv.

I forhold til punktene Aven (2007) presenterer ovenfor er hovedelementene kjente, og den indikerte prosessen følges i stor grad for eksempel i offshorenæringen, i transportsektoren osv. Når det gjelder samfunnssikkerhet er prosessen i mindre grad etablert, og noen nye utfordringer dukker opp. Spesielt er det mindre åpenbart hvem som er beslutningstaker. De politiske prosesser som ofte legges til grunn følger andre prinsipper. Vi må derfor kanskje omdefinere punktene til Aven (2007) ved at punkt 4 kanskje blir mer ”flytende”, og dermed vanskeligere å skille ut.

På dette området er det mulig å hente innspill fra prosesser som har løpt de siste årene. I NOKAS-saken vil mange hevde at den reelle beslutningstakeren var saksutrederen, fordi det var han som utformet forslag til vedtak. Ofte ligger selve verdiavveiningen i saksdokumentene uten at de formelle beslutningstakerene (politikerene) egentlig har oversikt over verdivalgene. En studie av risikokommunikasjonen i case som NOKAS-saken vil gi større innsikt i beslutningsprosessen for samfunnssikkerhetsarbeid generelt.

Modellen til Aven (2007) skiller ikke på tidsaspektet for beslutninger. Ofte skiller man på:

1. *Operative* beslutninger som fattes som en direkte respons på risikoutvikling, faresituasjon osv. Her er det svært begrenset mulighet til å utføre omfattende risikoanalyser. Man kan imidlertid benytte seg av forhåndsdefinerte skjematikker for beslutninger.
2. *Taktiske* beslutninger som fattes på mellomlang sikt. Dette kan typisk være vedlikeholdsplanlegging, mindre fornyelsesprosjekter osv. Her er det tid og rom til å utføre nødvendige risikoanalyse.
3. *Strategiske* beslutninger som fattes på høyt politisk nivå og har et langsiktig perspektiv. For eksempel en beslutning om å etablere en reservevannkilde vil være en slik beslutning. Også her er det tid og rom til å utføre risikoanlayser.

Typiske ROS-analyser som er gjennomført er i dag på et format som støtter taktiske og strategiske beslutninger. ROS analysene gir i liten grad støtte til operative beslutninger. Et forskningsmål for DECRIS er derfor å studere punktene til Aven (2007) i lys av de tre nivåene for beslutning listet ovenfor.

5.3 Utfordringer ved risikokommunikasjon (spesielt ved tverrsektorielle risikovurderinger)

Eksisterende ROS-metodikker tar ikke inn over seg begrepet risikokommunikasjon i særlig grad. For analytikeren er ofte problemet løst når en prioritert tiltaksliste er utviklet på bakgrunn av en utfylt risikomatrise. Hva som deretter skjer med analysen er opp til oppdragsgiver.

For DECRIS vil det være naturlig å fokusere på de to feltene interne og eksterne kommunikasjonsprosesser, og på samspillet mellom dem. I den interne prosessen vil det være spennende å studere kommunikasjonen mellom ekspertene og beslutningstakerne. Hvordan beskrives situasjonen mht risikonivå og omfang, hvilken informasjon prioriteres, hvordan skal informasjonen brukes, hvem skal varsles, på hvilken måte etc?

I den eksterne kommunikasjonen vil det være spennende å gjøre retoriske analyser av tekstene mht utforming og innhold, og se på hvordan allmennheten posisjoneres i tekstene. I både intern og ekstern kommunikasjon er det nødvendig å undersøke hele meningsskapingsprosessen, dvs undersøke både hvordan den som utformer tekstene og den som leser/hører tekstene tolker tekstene og forstår situasjonen (jfr Temporarily Shared Social Reality TSSR eller Shared situational awareness SSA).

6 Oppsummering

Rapporten oppsummerer overordnet kunnskap om kritiske infrastrukturer som det er naturlig å se på i DECRIS-prosjektet:

- Transport, inklusive veg- og banetransport
- Vann og avløp
- Kraftforsyning
- IKT-systemer innenfor infrastrukturene

Enkle beskrivelser av system, aktører, beredskap og lovverk innen de ulike infrastrukturene er gitt. På tvers av infrastrukturene er prinsipielt vanskelige forhold i gjennomføring av risikoanalyser identifisert, herunder:

- Avgrensning av system og valg av nivå
- Tilgang på kompetanse og informasjon
- Gjenbruk av informasjon
- Fare- og trusselidentifisering, ikke minst hvordan forhold til både safety og security kan håndteres i analysene
- Hvilke tap som skal vurderes i forhold til konsekvenser
- Hvordan følgekonsekvenser skal håndteres
- Hvordan sensitiv informasjon kan håndteres i analysen
- Hvordan tiltak skal velges og beslutninger tas

I tillegg inneholder rapporten noen betraktninger rundt problemstillinger med risikokommunikasjon. Kommunikasjon av vurderinger og beslutninger knyttet til risiko er en betydelig problemstilling når det gjelder tverrsektorielle risikoanalyser.

Referanser

Aven, T. (2007) Risikostyring. Prinsipper og ideer. Universitetsforlaget.

Henriksen, S. Sørli, K. Bogen, L. (2007) "Metode for identifisering og rangering av kritiske samfunnsfunksjoner," FFI/RAPPORT 2007/00784, 2007

Jernbaneverket (1999): Slik fungerer jernbanen. Webutgave oppdatert 23. mai 2007 - http://www.jernbaneverket.no/jernbanenettet/slik_fungerer_jernbanen/

Justis- og politidepartementet (2006): NOU 2006:6. Når sikkerhet er viktigst

Justis- og politidepartementet (2000): NOU 2000:24. Et sårbart samfunn

Kørte, J., Aven, T. and Rosness, R. (2002): On the use of risk analysis in different decision settings. Paper presented at ESREL 2002, Lyon, March 19-21, 2002.

Miljøverndepartementet (2000): Forskrift om kommunale vann- og avløpsgebyrer.

Norsk standard 7799:2003. Styringssystem for informasjonssikkerhet

NORVAR (2004): Gjenanskaffelsekostnader for norske vann- og avløpsanlegg, NORVAR-rapport 130.

Olje- og energidepartementet (2008): Energi- og vannressurser i Norge.

Rodal, S (2002): Systembeskrivelse av norsk vegtransport, FFI/RAPPORT-2002/00807.

Rodal, S (2003): Systembeskrivelse av den norske jernbanen, FFI/RAPPORT-2002/00808.

Samferdselsdepartementet (2006): Om ein del saker på Samferdselsdepartementets område, St.prop. nr 68 (2006-2007)

Senter for informasjonssikkerhet - Trusselrapport oktober 2005: http://www.norsis.no/trusler/Manedsrapporter/213.html

Sivertsen, T. (2007): Risikoanalyse av samfunnskritiske IKT-systemer – teknologiske erfaringer, FFI/RAPPORT- 2007/00910

Statens vegvesen (2006): Nøkkeltall

Notat 2: Utne, I. Hokstad, P. Vatn, J. (2007): DECRIS – Sammendrag ROS-analyser.