DECRIS - Risk and Decisions Systems for Critical Infrastructures

Jørn Vatn
NTNU/SINTEF

ABSTRACT: Kritiske infrastrukturer som vannforsyningen, strømforsyningen, transport og IKT omtales gjerne som livsviktige forbindelseslinjer (eng: *lifelines*). Et moderne samfunn er avhengig av sikker ytelse av disse. Det eksisterer flere typer avhengigheter mellom disse kritiske infrastrukturene, noe som gjør samfunnet ekstra sårbart. Et strømbrudd kan for eksempel føre til at ulike elektroniske kommunikasjonssystemer faller ut, som igjen kan føre til svikt i drifts- og styringssystemer i andre infrastrukturer. Det vil også gi avhengigheter overfor en rekke andre samfunnskritiske funksjoner, som nødkommunikasjon, finanstransaksjoner og helsetjenester. Disse koplingene gjør det utfordrende å vurdere risikoen og effekten av tiltak. I denne presentasjonen fremstiller vi de viktigste elementene av den såkalte DECRIS metoden. En detaljert diskusjon gis av noen få av trinnene, dvs etablering av risikomatriser, en totrinns prosess for å fastsette sannsynlighet og konsekvens i grovanalyen, og håndtering av avhengigheter

1 INNLEDNING

Risikovurderinger[1] innenfor den enkelte infrastruktur, eller deler av den, gjennomføres regelmessig. Derimot er analyser på tvers av infrastrukturer, som også tar hensyn til avhengighetene mellom disse, i svært liten grad utviklet og tatt i bruk. Men sektorovergripende risikoanalyser etterspørres, ikke minst av myndighetene, for eksempel kommuner og fylkesmenn, og slike analyser vil være nødvendig input ved gjennomføring av nasjonale risikovurderinger. Regjeringen har nylig fremmet et lovforslag om kommunal beredskapsplikt[2], som per 16.06. 2009 er vedtatt i Odelsting og Lagting. "Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og sivilforsvaret" er dermed et faktum, og vil innebære at kommunene må gjennomføre sektorovergripende risikovurderinger. Dette understreker ytterligere behov for å videreutvikle eksisterende analysemetoder og -verktøy.

DECRIS – Risk and Decisions Systems for Critical Infrastructures – var et tverrfaglig prosjekt hvor hovedmålet var å videreutvikle eksisterende metoder for risikovurdering, for å komme fram til en overordnet samling av metoder som fungerer på tvers av sektorer. Hensikten var å kunne analysere flere infrastrukturer under ett, slik at beslutningstaker kan få den nødvendige beslutningsstøtten, bl.a. for kartlegging av trusler (risiko/sårbarhet), planlegging av beredskap, og prioritering av risikoreduserende tiltak. Dessuten har prosjektet videreutviklet et verktøy til å støtte risikovurderingsarbeidet; her er som utgangspunkt benyttet et verktøy basert på prosjektet BAS5[3], kalt InfraRisk. Videre er det sett på beslutningsprosesser knyttet til risiko, og hvordan risiko kommuniseres i det offentlige rom.

Denne artikkelen er organisert på følgende måte. Først presenteres hovedelementene i DECRIS metoden. Deretter diskuterer vi noen metodiske utfordringer i detalj.

De sektorene som var valgt ut for prosjektet er vannforsyningen, strømforsyningen, transport (veg og bane) og IKT (som støtte for de andre). Disse er definert som kritiske infrastrukturer i NOU 2006:6 ”*Når sikkerheten er viktigst*” (NOU 2006).

Metodeutviklingen i DECRIS har i stor grad vært knyttet til gjennomføring av eksempelanalyser med Oslo kommune og samarbeidspartnere:

- Grovanalyse av utvalgte infrastrukturer i Oslo
- Detaljanalyser av følgende hendelser:
  - Bortfall av vann i Oset/Maridalsvannet; konsekvenser for Ullevål sykehus
  - Utfall av strømforsyning relatert til transformatorstasjoner i regionalnettet i Oslo
  - Leveringssikkerhet av petroleumsprodukter fra Sjursøya til Gardermoen
  - Brann eller annen skade i kabelkulvert ved Oslo S. Analysen tar utgangspunkt i en hendelse ved Oslo S i november 2007.

Andre viktige resultater fra prosjektet i tillegg til disse eksempelanalysene, er:

- Metodene for grovanalyse fra BAS5 er testet, videreutviklet og tilpasset de nevnte infrastrukturene. Denne sektorovergripende grovanalysen:

[1] Også ofte omtalt som risiko- og sårbarhetsanalyse, ROS-analyse.

[2] http://www.regjeringen.no/nb/dep/jd/pressesenter/pressemeldinger/2009/lovforslag-om-kommunal-beredskapsplikt.html?id=554228 (publ. 03.04.2009, sist aksessert 25.06.2009)

[3] BAS = Beskyttelse av samfunnet, sårbarheter i kritisk infrastruktur; FFI, NTNU/SINTEF, UiS, Proactima og DSB. BAS5: Sårbarhet i kritiske IKT-systemer

- Håndterer ulike konsekvenstyper, som tapte liv, utilgjengelighet (f.eks. ved strømutfall) og kvalitet (f.eks. forurenset drikkevann)
- Gir en systematikk for å definere trusler og samfunnskritiske funksjoner
- Benytter en videreutviklet versjon av verktøyet InfraRisk for beslutningsstøtte og dokumentasjon

– Metoder for detaljanalyser av kritiske infrastrukturer er utviklet og illustrert; spesielt er det sett på:
  - Analyse av avhengigheter
  - Årsaks- og konsekvensanalyser

Merk at DECRIS prosjektet i hovedsak har vært et metodeutviklingsprosjekt. Det har i begrenset omfang vært rom for mer teoretiske betraktninger.

2 OVERSIKT OVER DECRIS METODIKK

DECRIS er en samling av metoder for sektorovergripende risikovurdering av kritisk infrastruktur. Den metodiske tilnærmingen som setter disse analysene i et system tar utgangspunkt i at det først gjennomføres en grovanalyse for å identifisere, og rangere de viktigste risikoforhold. Formålet med en slik grovanalyse er å få oversikt, og kunne velge ut områder hvor en mer detaljert risikoanalyse er påkrevd.

I den første fasen er hovedmålet å kartlegge risiko ved hjelp av en relativt grundig grovanalyse, og videre identifisere uønskede hendelser (scenarier) som kan analyseres i mer detalj. I DECRIS er det lagt opp til å benytte flere ulike konsekvensdimensjoner, som sikkerhet (tap av liv), økonomiske konsekvenser og utilgjengelighet av tjenester (infrastruktur).

En rekke samfunnskritiske funksjoner (SKF) defineres og knyttes til de uønskede hendelsene i en prosedyre som er basert på ideer fra BAS5. Dataverktøyet som benyttes, InfraRisk, er også videreutviklet fra BAS5.

Basert på grovanalysen kan en velge ut noen scenarioer for mer detaljert analyse. I denne andre fasen kan det være et mål å få mer detaljert innsikt i risiko for omfattende hendelser, gjerne med store avhengigheter mellom ulike infrastrukturer. Feiltreanalyser (FTA) og hendelsestreanalyser (ETA) er to metoder for dette. Det er også utviklet en egen metode for å analysere avhengigheter.

En komplett DECRIS-analyse består av følgende trinn:

1 Oppstart
  a. Klargjøre mål: Hvem utføres analysen for, og hva er formålet?
  b. Bestemme avgrensning/systemdefinisjon
  c. Etablere forum/møteplass for aktørene
2 Grovanalyse
  a. Fastsette konsekvensdimensjoner
  b. Kalibrere risikomatrise; etablere kategorier for sannsynlighet og konsekvens
  c. Identifisere uønskede hendelser
  d. Klassifisere uønskede hendelser
  e. Angi frekvens (1-5)
  f. Identifisere hvilke samfunnskritiske funksjoner (SKF) som berøres
  g. Vurdere konsekvenser for de ulike konsekvensdimensjonene, hver gis en verdi 1-5
  h. Etablere risikomatrise
  i. Oppsummere sårbarheter og trusler
  j. Vurdere og prioritere tiltak
3 Detaljanalyse
  a. Velge hendelser for detaljanalyse (med utgangspunkt i resultatet fra grovanalysen)
  b. System/scenario-beskrivelse
  c. Detaljanalyser, f eks
    - Avhengighetsanalyse
    - Årsaksanalyse
    - Konsekvensanalyse
4 Totalvurdering og tiltak
  a. Totalvurdering av risiko; viktige sårbarheter og trusler
  b. Plan for tiltak, ansvarsplassering
  c. Evt. behov for ytterligere analyser

3 GROVANALYSE

DECRIS tilnærmingen tar utgangspunkt i at det først gjennomføres en grovanalyse for å få oversikt over risikobildet. En viktig del av innledningen til grovanalyen er å definere hvilke konsekvensdimensjoner som skal inngå i analysen. I DECRIS har vi valgt å forhåndsdefinere sju dimensjoner, men det er opp til brukeren å avgjøre hvorvidt alle dimensjoner skal inngå i analysen. Følgende dimensjoner inngår i DECRIS:

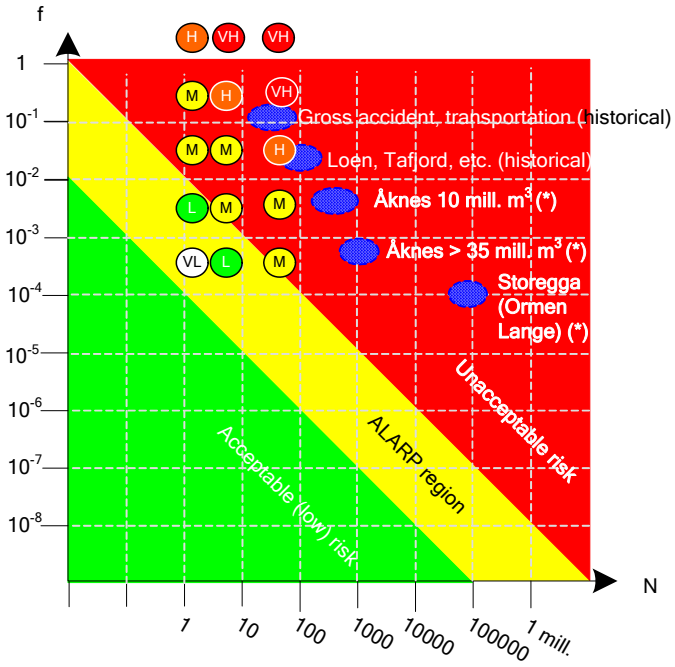
– Liv og helse
– Miljø
– Økonomi
– Styrbarhet
– Politisk tillit
– Kvalitet av infrastrukturtjenester
– Tilgjengelighet av infrastrukturtjenester

De fem første dimensjonene er videreført fra BAS5, mens vi har valgt å legge til kvalitet og tilgjengelighet av infrastruktur.

Videre må det etableres kategorier både for sannsynlighets- og konsekvensdimensjonen. Verdiområdet må defineres slik at hele skalaen både for sannsynlighet og konsekvens blir benyttet. Videre er det i DECRIS foreslått at en gitt sannsynlighet/konsekvens på tvers av dimensjonene skal være tilnærmet lik med hensyn på ”alvorlighet”. Det vil si at ved såkalt kalibrering av risikomatrisene må en vurdere alle dimensjoner opp mot hverandre. Dette kan da også gi en utfordring med hensyn på å ”bruke” ska-

laen dersom dimensjonene i en gitt analyse har svært ulik "alvorlighetsgrad". I DECRIS har vi valgt å forhåndskalibrere risikomatrisene for alle dimensjoner. En slik kalibrering er foretatt med hensyn på en typisk norsk storby. Utgangspunkt for kalibreringen har vært tidligere analyser gjennomført i Oslo, Stavanger, og en del fylkesvise risiko- og sårbarhetsanalyser. Merk at en kalibrering av risikomatrisene representerer verdiutsagn. Ved uttesting av metoden for Oslo forsøkte vi å få i gang en diskusjon om foreslått kalibrering reflekterer verdiforhold som eventuelt uttrykkes i Oslo. Det viser seg vanskelig å få til en reel diskusjon på dette området. Det er ikke åpenbart hvem som bør delta i en slik diskusjon, for eksempel er det byråkrater, enhetsledere, eller politikere som bør delta? Det ble ikke gjennomført noen studie for å dokumentere hvordan slike kalibreringsprosesser arter seg. Erfaring fra andre studier, f eks krav til vannforsyning, planlegging med hensyn til dimensjonering av avløpsnett osv, viser etter vår erfaring at det er lettere å få til en reell diskusjon her, enn dersom man diskuterer liv og helse. Dette skyldes etter vår vurdering at ansvarlige for infrastrukturelementer er mer vant til å formulere eksplisitte krav til infrastrukturen enn hva situasjonen er for liv og helse.

3.1 *Kalibrering av matrise for liv og helse*



Figur 1Sammenligning av risikomatriser for liv og helse

I DECRIS prosjektet er både sannsynlighet og konsekvens definert på en 5 punkts skala, og fargene i risikomatrisen representerer også 5 nivå, svært lav (VL=hvit), lav (L=grønn), middels (M=gul), høy (H=orange), og svært høg (VH=rød). I Figur 1 har vi sammenholdt risikomatrisene for DECRIS med en såkalte f-N kurver som benyttes ved risikovurderinger for industrianlegg. f-N kurvene her svarer til risikoakseptkriterier benyttet av Lyse i forbindelse med bygging av en LNG fabrikk i Risavika. Se Vatn (2009) for en grundig diskusjon om valg av risikoakseptkriterier, hvor også bakgrunnen for "erfarte/vurderte" naturhendelser (skraverte ellipser) er diskutert.

Den delen av risikomatrisa som angår død for DECRIS matrisene er lagt inn som sirkler i Figur 1, hvor VL betyr svært lav, L betyr lav osv. Noen refleksjoner ut fra denne framstillingen er:

- Et "høyt" risikonivå i DECRIS svarer grovt sett til erfarte storulykker på landsbasis i Norge
- Bruk av risikomatriser i grovanalyse slik man gjør i DECRIS metoden tilsier at man ofte har mange hendelser (>10) som kan ha høgt risikonivå. Sammen med det faktum at kun om lag en tiendedel av Norges befolkning bor i Oslo, betyr dette at man implisitt aksepterer en risiko som er høyere enn "erfart storulykkesrisiko".
- f-N kurvene som er lagt til grunn for Risiavika representerer kun ett anlegg, hvor befolkningsmengden kun svarer til om lag en prosent av Oslo's befolkning. Ved å justere for denne forskjell i eksponering, er DECRIS matrisene i rimelig overensstemmelse med f-N kurvene som benyttes i Risavika.

Selv om vi ved uttestingen av DECRIS metoden ikke la opp til en forskningstilnærming med hensyn til å studere prosessene som man må gå gjennom mht å kalibrerer risikomatriser, velger vi likevel å konkludere med følgende påstander:

- Det er en utfordring å få til en reel diskusjon om verdiinnholdet som ligger implisitt i valg av risikomatriser
- Det er lettere å kalibrere risikomatriser for ytelse av kritisk infrastruktur slik som vann og strømforsyning enn det er for liv og helse
- Ved diskusjon av risikomatriser i en konkret situasjon slik som Risavika (see Vatn m.fl., 2008) oppnås etter vår mening en viss forståelse av valg av risikomatriser ved diskusjoner på folkemøter osv hvor viktige interessenter er til stede.
- Ved å foreta en diskusjon slik den som følger i forlengelsen av Figur 1 ovenfor, kan man også bli rimelig konkret på hva verdivalgene faktisk representerer.
- Ved innføring av internkontroll i Norge på slutten av åttitallet var det et poeng at virksomhetene selv skulle fastsette risikoakseptkriterier. Erfaring fra f eks Risavika (see Vatn, 2009) viser at dette skaper legimitetsproblemer. Når vi også erfarer at det er vanskelig å få forvaltningen og politikerne til å fastsette risikoakseptkriterier, er det grunn til å vurdere om sentrale myndigheter slik som f eks direktoratet for samfunnssikkerhet og beredskap (DSB) burde gi sterkere føringer.
- Det må også understrekes at bruk av risikoakseptkriterier medfører en del utfordringer, uten at vi går inn på dette her.

3.2 *To trinns prosess for å fastsette sannsynlighet og konsekvens*

I standard grovanalysemetodikk fastsettes i regelen sannsynlighet og konsekvens i ett trinn. Det betyr at for en hendelse som vurderes, f eks brann, fastsettes sannsynligheten for brann og konsekvensen av brann ved å foreta en konkretisering av branntype, f eks en alvorlig brann. Her ligger det vanligvis en stor utfordring mht å bli prinsipiell. Ideelt sett ønsker man å angi sannsynlighet for brann, men også å angi sannsynlighet for de *ulike* konsekvensene av brann. En slik vurdering av ulike konsekvenser vurderes imidlertid til å være for arbeidskrevende. Derfor velges ofte en pragmatisk tilnærming hvor man forsøker å tenke seg en ”alvorlig realisasjon” av hendelsen, slik at den ene konsekvensen man gir uttrykker et ”verst tenkelig” utfall. Her legges ofte en begrensning i ’verst tenkelig’ ved at man ikke ser på (teoretiske) ekstremsituasjoner. Det sier seg imidlertid selv at man i en analyse sjelden blir helt eksplisitt på hva som er tenkningen.

I DECRIS prosjektet har vi identifisert en stor metodisk utfordring med denne vanlige praksisen når vi betrakter flere dimensjoner samtidig. Et eksempel på dette er brann i T-bane tunell. Slike branner oppstår ofte som følge av at f eks en avis kan antennes fra varmen som togene produseres. Frekvensen av slike branner kan være ganske høg. Konsekvensen av en slik brann mht tilgjengelighet av infrastrukturen (T-bane driften) er stor. Derfor er det naturlig når man skal fastsette frekvens/sannsynlighet av branner at man tar høyde for disse hendelser. Men dersom man har en slik hendelse i tankene når man skal fastsette konsekvens for liv og helse, blir det forholdsvis uinteressant. Det er vanskelig å se for seg noen dramatiske konsekvenser ved en slik hendelse.

I DECRIS prosjektet har vi derfor valgt en totrinns tilnærming når vi skal fastsette sannsynlighet og konsekvens for flere dimensjoner samtidig. Først fastsettes sannsynlighet for hendelsen som da ofte forstås som en begrenset alvorlighet av hendelsen. Det kan være branner, eller branntilløp generelt. Deretter vurderes for hver konsekvensdimensjon hva som kan være typiske alvorlige konsekvenser. For hver dimensjon angir vi da i tilegg *sannsynligheten* for at hendelsen gir denne alvorlighetsgraden. Brukeren av metoden, eller InfraRisk verktøyet, må da angi sannsynlighet som er felles for alle konsekvensdimensjoner, og så supplere med en ny sannsynlighetsvurdering svarende til valgt alvorlighet for hver av konsekvensdimensjonene. InfraRisk verktøyet håndterer beregningene som da blir nødvendig for å kunne vise resultatet i matrisene for de ulike dimensjonene. Det betyr i praksis at sannsynlighetene for hver hendelse justeres ned.

4 AVHENGIGHETER

I DECRIS prosjektet er det gjennomført en omfattende litteratur hvor ulike avhengighetsmodeller i forbindelse med kritisk infrastruktur er gjennomgått. Det er i hovedsak tre aspekter som ofte tematiseres. Det første punktet er såkalte avhengighetsmatriser hvor man for par av infrastrukturer angir styrken på avhengigheter (påvirkninger). Slike avhengighetsmatriser kan benyttes for å justere verdiene fra uavhengige vurderinger av hver enkelt infrastruktur. Videre presenteres ofte såkalte spagettimodeller hvor man grafisk illustrerer påvirkninger. Videre er det mange som forsøker å definerer, og kategorisere ulike typer avhengighet. Nedenfor presenteres noen av de mer teoretiske betraktningene fra litteraturstudien.

Rinaldi et al. (2001) definere avhengighet mellom infrastrukturer som et toveis forhold der tilstanden i hver av infrastrukturene påvirker eller er korrelert til tilstanden i den andre. Det skilles altså mellom ”dependencies” som enveis avhengigheter og ”interdependencies” som toveis avhengigheter. Hos Rinaldi et al. (2001) er hovedfokuset på toveis avhengigheter, og det betyr at man ser på avhengigheter i et makroperspektiv og ikke som noe som eksisterer mellom systemkomponenter. Andre skiller ikke spesifikt mellom enveis og toveis avhengigheter, for eksempel Peerenboom et al. (2002).

Avhengigheter kan også være direkte (av første orden) og indirekte (av høyere orden) (Johansson and Jönsson, 2008).

Rinaldi et al. (2001) bruker et rammeverk bestående av seks dimensjoner til å beskrive og analysere avhengigheter mellom infrastrukturer. Disse dimensjonene er (1) type avhengigheter, (2) miljø, (3) koblinger og reaksjonsmåte, (4) infrastrukturkarakteristikker, (5) type svikt og (6) operasjonsmodus.

Zimmerman (2001) beskriver tre viktige faktorer knyttet til avhengigheter mellom infrastrukturer, nemlig sammenkobling, redundans og systemkunnskap. Sammenkobling har effekt på hvordan svikt forplanter seg i systemene, redundans har betydning for eventuelle alternative muligheter for å opprettholde drift av systemet, og kunnskap gir mulighet for å oppdage og gjenkjenne trusler.

Zimmerman (2001; 2004) skiller mellom romlige og funksjonssammenkoblinger (avhengigheter). Romlige avhengigheter er knyttet til nærhet mellom infrastrukturer. Funksjonsavhengighet refererer til en situasjon der en type infrastruktur er nødvendig for drift av en annen, for eksempel at pumpene i et vannbehandlingsanlegg trenger strøm for å fungere. Zimmerman (2001) beskriver også tilfeller hvor man har både romlig og funksjonell avhengighet, for eksempel i trådløs kommunikasjon.

Nedenfor beskrives DECRIS metodikken for å analysere avhengigheter mellom infrastrukturene og konsekvenser av disse avhengighetene.

4.1 *Metoden i trinn*

Som diskutert ovenfor har DECRIS' risiko- og sårbarhetsanalyse to hovedfaser; en grovanalyse og en detaljanalyse. I detaljanalysene er det ulike forhold man kan forsøke å belyse nærmere, og vi vil nå se på aspekter av avhengigheter hvor DECRIS tilnæringen inkluderer følgende (del)trinn:

1 Avdekk avhengigheter
2 Gjennomfør en kvalitativ kartlegging og analyse av avhengighetene
3 Gjennomfør en semikvantitativ analyse; dvs. sannsynligheter og konsekvenser er kvantifisert ved å angi ulike kategorier (lav, middels, høy osv), og så estimere totalrisikoen knyttet til scenariet
4 Ved behov, gjennomfør en ren kvantitativ analyse av totalrisiko
5 Evaluer analyseresultat og angi tiltak for å redusere kritiske avhengigheter og dermed totalrisikoen.

Disse trinnene beskrives nærmere under. Først kommenteres beskrivelsen av ulykkesscenarioet

4.2 *Beskriv ulykkesscenario*

Basert på grovanalysen i fase 1, velger vi ut kritiske uønskede hendelser for mer detaljert analyse.

Grunnlaget for analysen av avhengigheter baseres på en systembeskrivelse. Det betyr at den uønskede hendelsen må detaljeres som et ulykkesscenario med en fysisk stedsbeskrivelse, beskrivelse av omgivelser, rammebetingelser og begrensninger, samt tidsrom. Tekniske og organisatoriske systemer må beskrives, viktige driftsmessige faktorer, og fysiske objekter som rammes umiddelbart av hendelsen, må også inkluderes. De seks dimensjonene til Rinaldi et al. (2001), kan brukes som innspill til scenariobeskrivelsen. Deretter må funksjonene i scenariet beskrives, i forhold til de fysiske objektene, organisasjonene, og sosiale strukturene, og ikke minst, knyttet til de samfunnskritiske funksjonene (SKF) og deres driftssituasjon før, i løpet av, og etter den uønskede hendelsen. I DECRIS har vi tatt utgangspunkt i en generisk liste med SKF'er som kan brukes som utgangspunkt for funksjonsbeskrivelsen. Scenariobeskrivelsen må også inkludere mulige årsaker til den uønskede hendelsen. Dersom omfang/type konsekvenser avhenger av årsak, må man ta hensyn til dette i analysen.

4.3 *Trinn 1: Avdekk avhengigheter*

Vi innfører først ulike *kategorier* av avhengigheter som blir behandlet i DECRIS. Disse kategoriene hjelper oss med å avdekke avhengighetene i analysen.

Ovenfor diskuterte vi ulike typer avhengigheter, blant annet bruken av begrepene "interdependencies" og "dependencies". I DECRIS brukes *avhengigheter* om både enveis eller flerveis avhengigheter, (dvs. uavhengig av årsaksretningen på avhengigheten). Eventuelle gjensidige avhengigheter (interdependencies) fanges opp ved den grafiske fremstillingen.

En kan både ha (i) avhengigheter mellom årsakene til en uønsket hendelse, ("sammenfall av uheldige omstendigheter") og (ii) avhengigheter mellom infrastrukturene, som følge av at konsekvensene til den uønskede hendelsen forplanter seg ("dominoeffekter") eller at flere infrastrukturer rammes "samtidig". I dette notatet fokuserer vi på de sistnevnte typer (ii), det vil si:

1 Lokasjonsspesifikke (fysiske) avhengigheter
2 Funksjonsavhengigheter

De lokasjonsspesifikke avhengighetene tilsvarer de geografiske og fysiske gruppene til Rinaldi et al. (2001) og den romlige koblingen til Zimmerman (2001). Disse avhengighetene er i hovedsak knyttet til fellessvikt. Lokasjonsspesifikke avhengigheter kan for eksempel være at en kortslutning i en strømkabel fører til brann, hvorav røyken fra brannen gjør at jernbanestasjonen må stenge slik at togtrafikken dermed ikke kan gå.

Funksjonsavhengigheter fokuserer på funksjonene involvert i et scenario og likner cyber- og logiske avhengighetskategorien til Rinaldi et al. (2001) og funksjonskoblingen til Zimmerman (2001). Disse avhengighetene er i hovedsak knyttet til kaskadesvikt. Funksjonsavhengigheter kan for eksempel være at et strømbrudd fører til utfall av internett.

For å avdekke lokasjonsspesifikke avhengigheter mellom SKF'ene i scenarioet kan vi systematisk stille flere spørsmål:

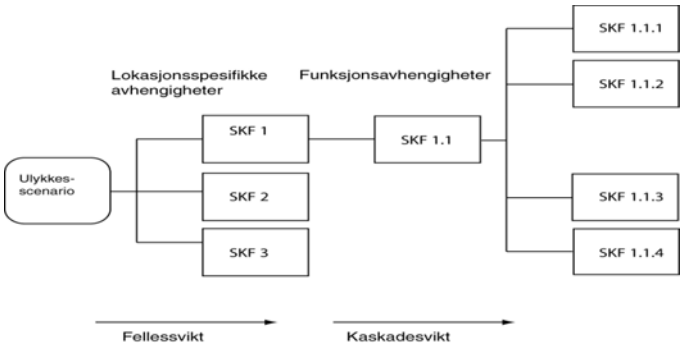
– Kan scenarioet forårsake tap av en SKF på grunn av den fysiske lokasjonen til systemet eller utstyret?
– Er det lokasjoner som, for eksempel, kan trues på grunn av brann?

For å avdekke funksjonsavhengigheter mellom SKF'ene i scenarioet kan vi spørre:

– Hva er de funksjonelle avhengighetene mellom SKF'ene avdekket i spørsmålene over og andre berørte SKF'er?

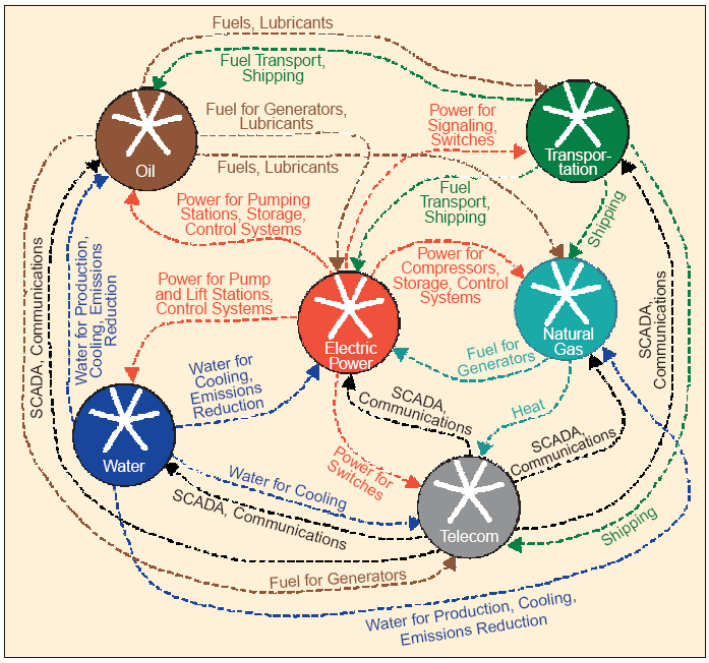
Videre undersøker vi de funksjonelle avhengighetene mellom SKF'ene, og ulike typer konsekvenser, ved å spørre:

– Forårsaker avhengigheten en total eller delvis svikt i SKF'en?
– Finnes det barrierer som kan motvirke fellessvikt eller kaskadesvikt?
– Hvilke konsekvensdimensjoner er sannsynlige som følge av tap av de ulike SKF'ene?



Figur 2 Eksempel på et kaskadediagram

Et kaskadediagram illustrerer avhengigheter og forholdene dem i mellom. Et slikt diagram gjør det enklere å få oversikt over avhengighetene i ulykkesscenarioet. Til forskjell fra spaghetti-diagrammet til Rinaldi et al. (2001), vist i Figur 3, er kaskadediagrammet mer strukturert og oversiktlig. På mange måter likner et kaskadediagram et hendelsestre, men det er noen forskjeller som diskuteres senere.



Figur 3 Eksempel på "spaghetti-diagram", hentet fra Rinaldi et al. (2001)

Når vi lager et kaskadediagram, starter vi med ulykkesscenarioet lengst til venstre, og modellerer deretter de lokasjonsspesifikke (førsteordens) avhengighetene til høyre for ulykkesscenarioet. Dersom vi velger å ikke forfølge en konsekvens videre, merker vi av boksen med et "stopp"-symbol, vist i Figur 4 på neste side. Sluttnodene, det vil si de nodene som ikke har noen påfølgende noder til høyre i diagrammet, kalles *løvnoder*

Funksjonsavhengighetene følger deretter, som høyere ordens avhengigheter. Avhengighetene i diagrammet visualiseres ved hjelp av linjer. Boksene illustrerer konsekvensene av avhengighetene, for eksempel "utfall av strømforsyning". Disse boksene kalles *noder*.

4.4 *Trinn 2: Kvalitativ analyse*

Etter å ha avdekket avhengighetene på et nivå som passer i forhold til analysens formål, kan vi velge å gjennomføre en ren kvalitativ analyse ved å diskutere avhengighetene som fremkommer i kaskadediagrammet og avdekke koblinger med stort ulykkespotensial. Deretter må det vurderes om det er behov for avhengighetsreduserende- eller risikoreduserende tiltak. I noen tilfeller kan det være aktuelt å grovt forfølge de avhengighetene som har størst sannsynlighet for å inntreffe, og dermed forenkle diagrammet.

For å vurdere risikoen, innfører vi for hver "følgehendelse"[4] (eller node i kaskadediagrammet) mål på:

- Sannsynlighet (*P*), evt frekvens (*F*)
- Omfang (*E*)[5]
- Varighet (*D*)[6]

For den uønskede hendelsen (selve ulykkesscenarioet) angir vi en frekvens, *F*, (for eksempel antall hendelser per 100 år eller lignende). For de etterfølgende hendelsene i kaskadediagrammet, angir vi en betinget sannsynlighet, *P*, for hendelsen, gitt at den forutgående hendelse i diagrammet (dvs. årsaken) har inntruffet. For å vurdere slike betingede sannsynligheter, må analytikeren vurdere verdiene av omfang (*E*) og varighet *(D)* for den forutgående hendelsen.

Dersom en slik kvalitativ vurdering ikke er tilstrekkelig, kan vi analysere og vurdere risikoen knyttet til avhengighetene på en semi- kvantitativ måte.

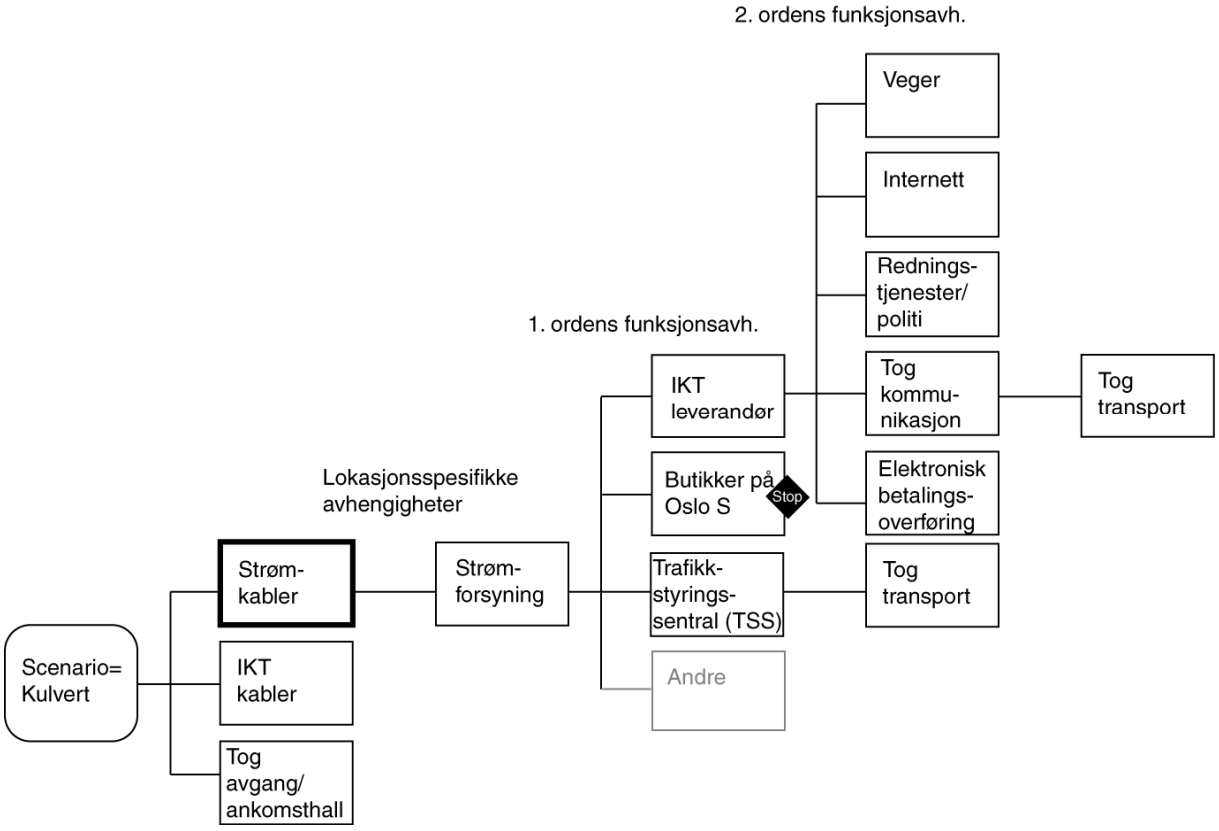
4.5 *Trinn 3: Semi-kvantitativ analyse*

I en semi-kvantitativ analyse, angir en *kategorier* for *F*, *P*, *E* og *D*. Tabell 1 frekvenskolonnen som benyttes. Det henvises til DECRIS hovedrapport for *P*, *E* og *D*. I (Utne et al., 2009) har vi forenklet noen av kategoriene, fra intervall til punktestimater, fordi beregningsalgoritmene da blir mer intuitive og enklere å forstå.

I det følgende, bruker vi kategorier som er konsistente med DECRIS- verktøyet InfraRisk, noe som gjør beregningene litt mer kompliserte. For enklere forklaring av beregningene, se (Utne et al., 2009).

Kategori 1 omfatter hendelser med frekvens sjeldnere enn hvert 1000 år. Tilsvarende vil man for "P", "E" og "D" ha at kategori 1 svarer til en sannsynlighet på 10^{-4}, omfanget til å være uvesentlig og varigheten til å være mindre enn en time.

[4] En "følgehendelse" er en konsekvens av forutgående hendelser i kaskadediagrammet.
[5] E- Engelsk for "extent".
[6] D- Engelsk for "duration".



Figur 4 Kaskadediagram for kulverteksempelet med fokus på svikt i strømforsyning

Tabell 1Kategorier for sikkerhet

Kat.	Frekvens
1	Mindre enn en gang pr 1000 år
2	En gang pr 100-1000 år
3	En gang pr 10-100 år
4	En gang pr 1-10 år
5	En gang eller mer pr år

Kategori 1 inkluderer altså de mest trivielle hendelsene. I motsatt ende av skalaen har vi kategori 5, altså de hendelsene med en frekvens på en gang eller mer per år osv. Bruk av kategorier som vist i Tabell 1 forenkler risikoberegningene..

Første trinn i den semi-kvantitative analysen er å fastsette parameterne <*F, E, D*> for den uønskede hendelsen (ulykkesscenarioet) og <*P, E, D*> for hver følgehendelse (node). Vi må ta i betraktning *E* og *D* på en kvalitativ måte når vi beregner sannsynligheter på neste nivå: Et stort omfang og lang varighet kan påvirke sannsynligheten til en følgekonsekvens. Som et eksempel kan vi se på en UPS. En UPS er en reservestrømskilde som får strøm fra et batteri. Batteriet har typisk en varighet på et par timer. Dersom vi lar UPSen representere en node i diagrammet, vil sannsynligheten for at UPSen svikter primært være avhengig av omfang (hvor stor del av strømnettet som har falt ut), og varigheten av utfallet. Dette vil da typisk være en hendelse til venstre for UPSen i diagrammet. Da vi her arbeider på et skjematisk semi-kvantitativt nivå er det vanskelig å foreta noen modellering av sannsynligheten for at UPSen svikter. Til en viss grad vil det imidlertid være mulighet for å gi en vurdering av sannsynligheten basert på varighet og omfang av hendelsen til venstre i diagrammet. Merk ved bruk av mer avanserte tilnærminger, f eks systemdynamikk og agentbaserte teknikker (Balducellli m.fl., 2005) kunne man foretatt slike eksplisitte vurderinger.

Siden alle kategoriene i Tabell 1 er gitt på en logaritmisk skala, er det naturlig å foreta en eksponensiell transformasjon for å finne verdier som svarer til ”virkelige” verdier. For å finne frekvensen for selve ulykkesscenarioet benyttes følgende transformasjon:

$$f = 10^{F-4.5} \quad (1)$$

Ligning (1) viser at dersom en hendelse for eksempel har $F = 2$, er et frekvensmål i betydningen forventet antall forekomster per år gitt ved det geometriske snittet av intervallene i Tabell 1, det vil si $f = 316$ år.

Den betingete sannsynligheten for at følgehendelsene vil inntreffe finnes ved:

$$p = 10^{P-5} \quad (2)$$

Tilsvarende får en for P=3 en tilhørende sannsynlighet på $p= 10^{-2}$.

Transformasjon for omfanget er gitt ved:

$$e = 10^{E} \quad (3)$$

Ved å bruke ligning (3) tilsvarer kategori 1 (uvesentlig) at 10 personer blir berørte, mens kategori 4 (katastrofalt omfang) tilsvarer 100 000 personer.

For varighet bruker vi

$$d = 6^{D - 1.5} \quad (4)$$

Ved for eksempel $D = 4$ blir $d = 88.5$ t, som ligger mellom 48 timer og 1 uke (intervaller for varighet i definisjonen gitt i DECRIS metoden).

Deretter gjennomfører vi beregningene av risikoen knyttet til scenarioet og følgehendelsene. Siden vi til nå har konsentrert oss om frekvensen og sannsynlighetene, gjenstår beregningene av konsekvensene for å kunne fastsette risikoen. Konsekvensberegningene begynner med å studere nodene til høyre i kaskadediagrammet, det vil si *løvnodene*. Løvnodene har ingen noder til høyre for seg, og er markert med en stiplet linje. Når konsekvensene for hver løvnode er beregnet, må vi fusjonere konsekvensene for løvnodene sammen i en konsekvens for hver gren, eller *fusjonsnode*. Vi bruker ikke *E* og *D* i disse beregningene (unntatt for løvnodene), for å unngå å ta varighet og omfang i betraktning flere ganger for en SKF.

Når vi har beregnet konsekvensene for hver fusjonsnode, kan vi beregne risikoen for ulykkesscenarioet. I praksis betyr det at vi beveger oss fra venstre til høyre når vi vurderer frekvens og sannsynligheter (ved hjelp av omfang og varighet), og fra høyre til venstre når vi beregner konsekvensene, noe som er forskjellig fra hendelsestreanalyse (ETA). Til slutt kan vi sammenstille totalrisikoen.

Beregningene gjennomføres altså som følger:

1 For løvnoder er den forventede konsekvensen:

$$C_j = 10^{Pj - 5} \times 10^{Ej} \times 6^{Dj - 1.5} \quad (5)$$

2 Når vi beregner risikoen for ulykkesscenarioet, "fusjonerer" vi altså flere noder fra høyre til venstre. Først summerer vi konsekvensbidraget fra hver gren, og deretter multipliserer vi med det transformerte sannsynlighetsmålet. Det vil si at for fusjonsnode *i* er (forventet) konsekvens gitt ved:

$$C_i = 10^{Pi - 5} \times \Sigma_j C_{j.} \quad (6)$$

Der summasjonen går over de noder, *j*, som er direkte til høyre for node i, og som "fusjonerer" i denne.

3 Når vi kommer til noden lengst til venstre, altså selve ulykkeshendelsen, kan totalrisikoen beregnes ved:

$$R = 10^{F - 4.5} \times \Sigma_j C_j \quad (7)$$

der summasjonen nå er over alle noder, *j*, direkte til høyre for ulykkeshendelsen, og vi har at $C = \Sigma_j C_j$ er total konsekvens, gitt som antall forventede persontimer tapt eller berørt (som følge av svikt i infrastrukturtjenester). Frekvensen til scenarioet er gitt i ligning (1), og som vi ser av ligning (7) er risikoen gitt som $R = f \times C$.

4.5.1 *Vekting og interaksjonseffekter*

I fremgangsmåten beskrevet over, behandles alle SKF'ene som like viktige. I noen tilfeller kan det være at vi ønsker å vektlegge at svikt i noen SKF'er er verre enn i andre. Da kan vi bruke en vektingsprosedyre ved:

$$C_j = w_j \times 10^{Pj - 5.0} \times 10^{Ej} \times 6^{Dj - 1.5} \quad (8)$$

C_j er forventet konsekvens, mens w_j er en vektfaktor som gjenspeiler viktigheten til SKF_j . I figur 7 har vi brukt vektfaktorer for å illustrere at noen noder er mer kritiske enn andre.

Vi kan også ta hensyn til interaksjonseffekter som gjenspeiler at konsekvensen av å miste to SKF'er som følge av en fellesfeil, er mer alvorlig enn simpelthen bare å summere SKF'ene (når de svikter individuelt): Tap av jernbanetransport er for eksempel verre dersom vegtransporten også svikter. En måte å integrere slike interaksjonseffekter på kan være å øke omfangsmålet, *E*. En grov måte kan være å øke alle E_j med en enhet når det er kombinerte effekter. Dersom effektene er sterke, kan vi øke E_j med to enheter, og så videre.

For å finne et kvantitativt uttrykk for effekten av interaksjonseffekter kan man beregne risikoen ved ligning (7) med og uten interaksjonseffekter, og for eksempel beregne et forholdstall, eller en prosentvis økning.

I noen tilfeller kan det være at vi avdekker at mer enn en SKF berører en annen SKF, for eksempel at tap av IKT og strømforsyning begge forårsaker svikt i jernbanetransporten. Ved å bruke vekter kan man ta i betraktning at dette er en mer kritisk situasjon enn tap av én SKF og at en mer detaljert analyse er nødvendig, for eksempel feiltreanalyse.

I de tilfellene hvor vi finner at vi trenger mer informasjon, kan vi gjøre en mer detaljert kvantitativ analyse. Hvis ikke, hopper vi direkte til trinn 5.

4.6 *Trinn 4: Kvantitativ analyse*

I en kvantitativ analyse kan vi bruke feiltreanalyse (FTA), hendelsestreanalyse (ETA) og nettverkmodeller av kapasiteten til en infrastruktur. Som nevnt av Kröger (2008), har metoder som FTA ulemper i forhold til analyse av komplekse avhengigheter. Like fullt, for å undersøke noder i kaskadediagrammet i detalj, påstår vi at bruk av FTA og ETA ikke er mer komplisert enn i de fleste andre situasjoner der FTA er nyttig. FTA er for eksempel brukt i en studie av (Volkanowski et al., 2009) til å beregne pålideligheten til kraftforsyning.

4.7 *Trinn 5: Vurder analyse og angi risikoreduserende tiltak*

Når risikoen til ulykkesscenarioet har blitt analysert, kan vi vurdere i hvilken grad scenarioet kan oppstå på andre steder, og om risikoen for alternative steder også bør analyseres. Behov for eventuelle risikoreduserende tiltak må også vurderes, for eksempel behov for nye eller flere barrierer som redundans.

4.8 *Diskusjon av DECRIS avhengighetsmodell*

Vi indikerte innledningsvis at vi i litteraturen primært finner to typer modeller for avhengighet, den første tilnærmingen baserer seg på at det etableres avhengighetsmatriser, mens den andre tilnærmingen baserer seg på at man ved spaghetti-diagrammer kan synliggjøre komplekse avhengighetsstrukturer. Ingen av disse tilnærmingene gjør det mulig på en hensiktsmessig måte å diskutere avhengigheter i forhold til et konkret ulykkesscenario. Ved svært detaljerte analyser slik som bruk av flytnettverk vil det være mulig å foreta slik eksplisitt avhengighetsmodellering for et konkret eksempel.

Styrken i DECRIS tilnærmingen er at man kan foreta en eksplisitt vurdering av avhengigheter for et gitt ulykkesscenario uten å foreta en detaljert kvantitativ modellering. Ved en grafisk visualisering, og en etterfølgende semi-kvantitativ modellering er det mulig både å synliggjøre avhengighetene og vurdere styrken av disse kvantitativt. Det er mulig å definere en rekke avhengighetsmål som man ved en slik tilnærming kan fastsette. Dette gjør det mulig å bli mer eksplisitt på å vurdere effekt av tiltak som kan redusere avhengigheter i systemet.

I DECRIS tilnærmingen kan man synliggjøre gjensidig avhengighet mellom infrastrukturelementer ved å tegne ”tilbakeføringssløyfer”. Per i dag har vi ikke utviklet noen beregningsformler for dette. Ved slike beregninger vurderes det som naturlig å benytte seg av teknikker for analyse av systemdynamikk (system dynamics).

5 OPPSUMMERING

Vi har i denne artikkelen presentert hovedtrekkene i DECRIS metoden. Dette er en totrinnsmetode hvor det først gjennomføres en grovanalyse for å få en grov oversikt over risikobildet. Deretter velges det ut områder for detaljert analyse. Metoden er testet ut med Oslo som kasusstudie. I artikkelen har vi diskutert tre forhold:

1 Elementer av kalibrering av risikomatriser.
2 En totrinns tilnærming for å fastsette sannsynlighet og konsekvens som er konsistent dersom flere konsekvensdimensjoner er relevant for en hendelse
3 En avhengighetsmodell som grafisk illustrerer ulike typer avhengighetsforhold ved et ulykkesscenario, og som ved hjelp av en semi-kvantitativ tilnærming gjør det mulig å fastsette styrke på avhengigheter, interaksjonseffekter osv.

6 REFERANSER

Balducelli, C., Bologna, S., Di Pietro, A. and Vicoli, G. (2005) Analysing interdependencies of critical infrastructures using agent discrete event simulation. *International Journal of Emergecy Management*, 2, pp 306-318.

Kröger, W. (2008) Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools. *Reliability Engineering and System Safety*, 93, pp 1781-1787.

NOU (2006) Norges offentlige utredninger 2006:6. Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner in: Justis- og politidepartementet (ed) Oslo.

Peerenboom, J. P., Fisher, R. E., Rinaldi, S. M. and Kelly, T. K. (2002) Studying the chain reaction. *Electric perspectives*, 27, pp 22-35.

Rinaldi, S. M., Peerenbom, J. P. and Kelly, T. K. (2001) Identifying, Understanding and Analyzing Critical Structures Interdependencies. *IEEE Control Systems Magazine*, pp 11-25.

Utne, I. B., Hokstad, P. and Vatn, J. (2009) A structured approach to modeling interdependencies in risk analysis of critical infrastructures, *ESREL 2009*, Praha, Tsjekkia.

Vatn, J., Vatn, G.Å. and Drottz-Sjöberg, B-M. Societal Security – A case study related to an LNG facility. The first SAMRISK conference. 1-2 September, 2008. Oslo.

Vatn, J. (2009) Issues related to localization of an LNG facility. *ESREL 2009*, Praha, Tsjekkia.

Volkanowski, A., Cepin, M. and Mavko, B. (2009) Application of the fault tree analysis for assessment of power system reliability. *Reliability Engineering and System Safety*, 94, pp 1116-1127.

Zimmerman, R. (2001) Social Implications of Infrastructure Network Interactions. *Journal of Urban Technology*, 8, pp 97-119.

Zimmerman, R. (2004) Decision-making and the Vulnerability of Interdependent Critical Infrastructure, *IEEE International Conference on Systems, Man and Cybernetics*.