



SINTEF Teknologi og samfunn
Sikkerhet

Postadresse: 7465 Trondheim
Besøksadresse: S P Andersens veg 5
7031 Trondheim
Telefon: 73 59 03 00
Telefaks: 73 59 28 96

Foretaksregisteret: NO 948 007 029 MVA

SINTEF RAPPORT

TITTEL

Metode og verktøy for en samlet risikovurdering av kritiske infrastrukturer

**Sluttrapport for DECRIS:
Risk and Decision Systems for Critical Infrastructures**

FORFATTER(E)

Maria B. Line, Dag Bertelsen, Håvard Fridheim, Per Hokstad, Gerd Kjølle, Jon Røstum, Ingrid B. Utne, Gunhild Åm Vatn, Jørn Vatn

OPPDRAGSGIVER(E)

Norges forskningsråd

RAPPORTNR. SINTEF A11636	GRADERING Åpen	OPPDRAGSGIVERS REF. Bjørge Ofstad	
GRADER. DENNE SIDE Åpen	ISBN 978-82-14-04814-8	PROSJEKTNR. 504121	ANTALL SIDER OG BILAG 24/2
ELEKTRONISK ARKIVKODE DECRIS rapport.doc	PROSJEKTLEDER (NAVN, SIGN.) Per R. Hokstad	VERIFISERT AV (NAVN, SIGN.) Lars Bodsberg	
ARKIVKODE	DATO 2009-08-30	GODKJENT AV (NAVN, STILLING, SIGN.) Lars Bodsberg, Forskningsjef	

SAMMENDRAG

Prosjektet DECRIS er finansiert av Norges forskningsråd under SAMRISK-programmet. Det er et samarbeidsprosjekt mellom SINTEF, FFI og NTNU. Prosjektet har utviklet og tilpasset metoder for risikovurdering for kritisk infrastruktur. Metodene skal kunne brukes på tvers av ulike infrastrukturer (vann og avløp, strøm, veg/bane og IKT), og vil ta hensyn til avhengigheter mellom disse som har betydning for uønskede hendelser.

Notater og publikasjoner fra prosjektet er å finne på nettstedet
<http://www.sintef.no/Projectweb/SAMRISK/DECRIS/>

STIKKORD	NORSK	ENGELSK
GRUPPE 1	Sikkerhet	Safety
GRUPPE 2	Risikovurdering	Risk assessment
EGENVALGTE	Kritisk infrastruktur	Critical infrastructures
	Samfunnskritiske funksjoner	Critical societal functions

Forord

Denne rapporten oppsummerer resultater fra prosjektet DECRIS – *Risk and Decision Systems for Critical Infrastructures*, som er finansiert av Norges forskningsråd under SAMRISK-programmet – Samfunnssikkerhet og risikoforskning (2006 – 2010). Totalbudsjettet for DECRIS er på 3 mill NOK, og prosjektet har en varighet på to år; august 2007 – september 2009.

Prosjektpartnerne i DECRIS er SINTEF, NTNU og FFI, og disse miljøene dekker til sammen de relevante fagområdene i prosjektet; risikoanalyse, risikokommunikasjon og fagkunnskap om de utvalgte infrastrukturene.

I DECRIS har vi vært så heldige å kunne samarbeide og utprøve metoder sammen med Oslo kommune og samarbeidende parter. Det å etablere en slik møteplass har vært svært nyttig for prosjektet, men vi håper det også har vært nyttig for de aktuelle parter å delta i dette forumet, der både konkrete case og generelle problemstillinger av felles interesse har vært diskutert.

Vi ønsker å takke alle som har bidratt til DECRIS. Spesielt har det gode samarbeidet med Beredskapsetaten ved Oslo kommune, først og fremst via Jan Egil Bäckmark, vært viktig for prosjektet. Videre har Oslo kommunes samarbeidspartnere; Brann- og redningsetaten, Hafslund Nett AS, Oslo Forsikring AS, Oslo Havn KF, Ruter AS, Samferdselsetaten og Vann- og avløps-etaten bidratt meget konstruktivt under arbeidsmøter og seminarer, og ved å gi innspill til gjennomføring av case. Det samme gjelder Post- og teletilsynet, Telenor Norge, Telenor ASA og Ullevål universitetssykehus. Videre har vi fått gode innspill fra Direktoratet for samfunnssikkerhet og beredskap (DSB), Nasjonal sikkerhetsmyndighet (NSM), samt beredskapssjefer i flere kommuner, blant andre Stavanger og Trondheim. Vi har underveis også hatt godt samarbeid med to andre SAMRISK-prosjekt: AdaptCRVA og CISS.

Per R. Hokstad
SINTEF
Prosjektleder

Sammendrag

DECRIIS-prosjektet har tatt eksisterende metoder for å utføre sektorovergrepene risiko-vurderinger et steg videre. Verktøyet InfraRisk har blitt videreutviklet, spesielt til støtte for den innledende grovanalysen. Grovanalyser med bruk av dette verktøyet har blitt anvendt med Oslo kommune som eksempel, hvor det er sett på infrastrukturene strømforsyning, vannforsyning og trafikk (veg/bane), og til dels IKT.

DECRIIS omfatter også en detaljanalyse av utvalgte uønskede hendelser identifisert i grovanalysen. Årsaksanalyser og avhengighets/konsekvensanalyser er to av metodene som kan inngå i en slik detaljanalyse. Det er dessuten utviklet en egen metode for analyse av avhengigheter, hvor slike klassifiseres som funksjonsavhengigheter og lokasjonsavhengigheter. Ulike metoder for detaljanalysen er eksemplifisert på i alt fire scenarier fra Oslo.

Utfyllende informasjon om metodikk og eksempler er gitt i 10 notater, som ble utarbeidet i prosjektet, se <http://www.sintef.no/Projectweb/SAMRISK/DECRIIS/>.

INNHALDSFORTEGNELSE

Forord	2
Sammendrag	3
1 Innledning	5
2 Oversikt over DECRIS metodikk	7
3 DECRIS: Oppstart	8
4 DECRIS: Grovanalyse	9
4.1 Analyse av uønskede hendelser	9
4.2 Verktøystøtte.....	10
4.3 Grovanalyse utført for Oslo	11
5 DECRIS: Detaljanalyser	12
5.1 Ulike metoder til bruk i detaljanalysene	12
5.2 Case 1: Utfall i strømforsyningen	17
5.3 Case 2: Bortfall av vann i Oset/Maridalsvannet; konsekvenser for Ullevål sykehus ...	18
5.4 Case 3: Leveringssikkerhet av petroleumsprodukter fra Sjursøya til Gardermoen	19
5.5 Case 4: Brann i kabelkulvert på Oslo S	19
6 DECRIS: Vurdering av totalrisiko – ansvar og tiltak	20
7 Diskusjon og videre arbeid	22
Referanser	24
Vedlegg A. Notater og publikasjoner	25
Vedlegg B. Møter og seminarer i regi av DECRIS	26

1 Innledning

Kritiske infrastrukturer som vannforsyningen, strømforsyningen, transport og IKT omtales gjerne som livsviktige forbindelseslinjer (eng: *lifelines*). Disse er helt grunnleggende i et moderne samfunn, og det kan medføre store konsekvenser om de blir satt ut av spill. Oftest er det også sterke avhengigheter mellom ulike infrastrukturer. Et strømbrudd kan for eksempel føre til at ulike elektroniske kommunikasjonssystemer faller ut, som igjen kan føre til svikt i drifts- og styrings-systemer i andre infrastrukturer. Det vil også gi avhengigheter overfor en rekke andre samfunns-kritiske funksjoner, som nødkommunikasjon, finanstransaksjoner og helsetjenester. Disse koplingene gjør det svært utfordrende å vurdere risikoen og effekten av tiltak.

Risikovurderinger¹ 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 beredskapsplikt², 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.

Kompleksiteten øker når man skal se på flere infrastrukturer på en gang. Det fører med seg en rekke metodiske problemstillinger:

- Hvordan avgrense analysesystemet og velge riktig nivå på analysen?
- Hvordan få tilgang til riktig kompetanse og informasjon i analysen?
- Kan man gjenbruke informasjon fra tidligere analyser?
- Hvordan få til en all-hazards³-tilnærming?
- Hvilke tap skal vurderes iht. konsekvenser?
- Hvordan håndtere følgekonskvenser?
- Hvordan behandle sensitiv informasjon?
- Hvordan velge tiltak etter analysen?
- Hvordan kommunisere rundt risiko?

DECRIIS – Risk and Decisions Systems for Critical Infrastructures – er et tverrfaglig prosjekt hvor hovedmålet er å videreutvikle eksisterende metoder for risikovurdering, for å komme fram til en overordnet samling av metoder som fungerer på tvers av sektorer. Hensikten er å kunne analysere flere infrastrukturer under ett, slik at myndigheter kan få den nødvendige beslutningsstøtten, bl.a. for kartlegging av trusler (risiko/sårbarhet), planlegging av beredskap, og prioritering av risiko-reducerende tiltak. Dessuten har prosjektet videreutviklet et verktøy til å støtte risikovurderings-arbeidet; her er som utgangspunkt benyttet et verktøy basert på prosjektet BAS5⁴, kalt InfraRisk.

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

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

³ All-hazards-tilnærming innebærer å kunne vurdere hendelser av både tilfeldig art (naturhendelser, tekniske feil osv.) og viljeshandlinger (terror, sabotasje mm.).

⁴ BAS = Beskyttelse av samfunnet, sårbarheter i kritisk infrastruktur; FFI, NTNU/SINTEF, UiS, Proactima og DSB. BAS5: Sårbarhet i kritiske IKT-systemer

Videre er det sett på beslutningsprosesser knyttet til risiko, og hvordan risiko kommuniseres i det offentlige rom.

De sektorene som er 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” [1].

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:
 - 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
- Vitenskapelige publikasjoner. Detaljerte resultater fra prosjektet finnes i egne notater (se vedlegg A).
- Prosjektet har fungert som en møteplass for en rekke aktører som har vært opptatt av problemstillingen rundt risikovurdering av kritisk infrastruktur. Dette gjelder spesielt gjennomføringen av analyseeksemplene for Oslo kommune med samarbeidspartnere. I en slik sammenheng er det essensielt at aktørene fra ulike infrastrukturer møtes for å utveksle erfaringer og samkjøre analyser.

Denne rapporten beskriver analysemetoder som er tilpasset og/eller utviklet i DECRIS, samt konkrete eksempler på bruk av disse. Først gis et raskt overblikk over gangen i en komplett DECRIS-analyse; i de fire neste kapitlene presenteres de ulike trinnene: oppstart, grovanalyse, detaljanalyser og totalvurdering. Til slutt gis en diskusjon av prosjektresultatene og idéer til videre arbeid. Vedleggene omfatter en oversikt over notater og publikasjoner utarbeidet i prosjektet, og oversikt over møter og seminarer som er avholdt i regi av prosjektet.

2 Oversikt over DECRIS metodikk

DECRIS er en samling av metoder for sektorovergripende risikovurdering av kritisk infrastruktur. Den innebærer analyse i to faser; grovanalyse og detaljanalyser. 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 [2]. Dataverktøyet som benyttes, InfraRisk, er også videreutviklet fra BAS5.

Basert på grovanalysen kan en velge ut noen scenarier 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, dessuten er det utviklet en egen metode for å kartlegge 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 risikomatrix; 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 risikomatrix
 - 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, e.g.
 - 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 DECRIS: Oppstart

I oppstartsfasen av en risikovurdering er det viktig å avklare formål, gi en systembeskrivelse og foreta avgrensninger. I en tverrsektoriell analyse som beskrevet i DECRIS, er det også viktig å etablere en møteplass for alle involverte aktører.

Først og fremst må det være helt klart hvem analysen utføres for, og hva formålet med analysen er. Ulike interessenter kan ha ulik motivasjon for å få utført en risikovurdering:

- *Myndigheter*, som kommuner eller fylker, kan være mest opptatt av å få en totaloversikt over sårbarheter og trusler innenfor sitt ansvarsområde. De vil ønske å se flere sektorer under ett, for å planlegge beredskap og prioritere tiltak.
- *Infrastruktureiere*, for eksempel innen vannforsyning, strømforsyning eller kommunikasjon, kan være mest interessert i å få analysert sin egen leveringssikkerhet overfor ulike kunder.
- *Brukere av infrastruktur*, for eksempel større sykehus eller trafikkelskap, kan være mest ute etter å analysere sine sårbarheter og avhengigheter av kritisk infrastruktur, spesielt for å kunne vurdere tilleggs løsninger og reservetiltak, slik at driften ikke må stanse selv om en hendelse inntreffer.

Utformingen av risikovurderingen vil avhenge av hvilke interessenter analysen utføres for og hvilke problemstillinger disse primært er opptatt av.

Deretter må det bestemmes detaljeringsgrad for risikovurderingen. Det må settes tydelige begrensninger for hvilke deler av problemområdet som skal vurderes, og hvilke elementer (årsaker/konsekvenser) som holdes utenfor. Relevante spørsmål i denne sammenhengen kan være:

- Skal man se på infrastrukturen på et overordnet systemnivå, eller skal man se på delsystemer eller enkeltkomponenter?
- Er man interessert i konsekvenser for systemet, for systemeieren, spesifikke brukere eller samfunnet som helhet?
- Hvilke typer konsekvenser skal vurderes; tilgjengelighet, sikkerhet for liv/helse, økonomi, andre?
- I hvilken grad skal man trekke inn menneskelige og organisatoriske bidrag? Er viljes handlinger en del av analysen?

En risikovurdering kan komme til å kreve bruk av sensitiv informasjon, enten kommersielle hemmeligheter for oppdragsgiver eller informasjon som er gradert i henhold til Sikkerhetsloven. Dette vil kunne legge føringer på hvilken informasjon som kan publiseres offentlig og hvilket innhold kommunikasjonen om risikoforholdene kan ha. Dessuten, selv om all informasjon som inngår i analysen i utgangspunktet er åpen, kan sammenstillingen av denne informasjonen likevel være sensitiv. Man må også vurdere om prosjektgruppen har sikkerhetsklarering og om arbeidet foregår i lokaler som tilfredsstillende eventuelle sikkerhetskrav.

I oppstartsfasen bør det også etableres et forum for alle aktørene som er involvert i den aktuelle risikovurderingen. Dette vil typisk inkludere en rekke eksperter på ulike deler av systemene og problemområdet som skal vurderes. Her vil man kunne få fram ulike perspektiv og interesser, og ikke minst klarlegge ansvarsforhold. Videre kan det være aktuelt å etablere akseptkriterier for evaluering av analyseresultater. Men spesielt er det viktig med denne møteplassen for kommunikasjon og kunnskapsutveksling mellom involverte aktører.

For utdypende forklaringer til oppstartsfasen, se notat 1, *DECRIS – Problemstillinger rundt tverrsektorielle risikoanalyser*, og notat 6, *DECRIS – Risikoanalyse av kritisk infrastruktur* [3].

4 DECRIS: Grovanalyse

En grovanalyse brukes for å få en rask oversikt over risikobildet og for å finne enkeltområder som bør vurderes i mer detalj. Den starter ved at man fastsetter konsekvensdimensjoner. I DECRIS brukes dimensjonene liv og helse samt utilgjengelighet av kritisk infrastruktur. Når man vurderer risiko for flere ulike infrastrukturer eller flere sektorer på en gang, er det viktig at konsekvensdimensjonene og kategoriene for sannsynlighet og konsekvens er samkjørte.

DECRIS foreslår å benytte fem kategorier for både sannsynlighet og konsekvens. Videre vil en ha en felles struktur på klassifiseringen av uønskede hendelser. En vil se på både generiske hendelser (uten spesifisering av tid og sted), og helt konkrete hendelser. I DECRIS er det også lagt vekt på å få et strukturert opplegg med hensyn til hvor i hendelseskjeden den uønskede hendelsen inntreffer, og når og på hvilken måte ulike samfunnskritiske funksjoner påvirker eller blir påvirket av hendelsesforløpet.

4.1 Analyse av uønskede hendelser

Uønskede hendelser identifiseres gjerne gjennom en fri idémyldring. Når man har kommet fram til en mengde uønskede hendelser som skal analyseres, er det noen aktiviteter som skal utføres for hver enkelt hendelse.

Hendelsesklassifisering:

I DECRIS klassifiseres hendelsen ut ifra følgende fire årsakskategorier:

1. Naturhendelse (N)
2. Medisinsk/biologisk (B)
3. Teknisk/menneskelig (systemfeil/ulykke) (T)
4. Viljeshandlinger, inkludert destruktive handlinger (V)

Samfunnskritisk funksjon (SKF) som berøres:

Her nevnes samfunnskritiske funksjoner som berøres av den uønskede hendelsen. De SKF som er viktige i DECRIS er bane, veg, strøm, vann og IKT. For hver av de aktuelle SKF angis også *Før*, *Etter* eller *Truet av*, for å vise når denne SKF påvirkes i hendelsesforløpet.

Beskrivelse av hendelsen:

Hendelsen, eventuelt scenariet, beskrives med fritekst.

Sannsynlighet og konsekvens:

Sannsynlighet og konsekvens for den uønskede hendelsen vurderes ut fra de gitte kategoriene, og resultatet presenteres i en risikomatrix, se Fig. 1. Det settes opp en risikomatrix for hver konsekvensdimensjon, og figuren viser matrisen for liv/helse. Når det gjelder utilgjengelighet av infrastruktur, gir DECRIS støtte til å definere konsekvenskategorier ut ifra varighet og antall eksponerte.

En sektorovergrepande risikovurdering vil ofte utføres som et ledd i en beredskapsplanlegging, og da kan det være naturlig å angi "alvorligste konsekvens", og ikke forventet ("gjennomsnittlig") konsekvens i forbindelse med risikoestimeringen. Hvis en velger å se på alvorligste konsekvens, kan en oppgi betinget sannsynlighet for et slik "verste utfall".

	Opp til 5 skadde/alvorlig syke	Opp til 40 skadde/alvorlig syke	1-2 drepte, opp til 100 skadde/alvorlig syke	2-10 drepte, opp til 500 skadde/alvorlig syke	Mer enn 10 drepte, mer enn 1000 skadde/alvorlig syke
Mindre enn en gang pr 1000 år	Svært lav risiko	Svært lav risiko	Svært lav risiko	Lav risiko	Middels risiko
En gang pr 100-1000 år	Svært lav risiko	Svært lav risiko	Lav risiko	Middels risiko	Middels risiko
En gang pr 10-100 år	Svært lav risiko	Lav risiko	Middels risiko	Middels risiko	Høy risiko
En gang pr 1-10 år	Lav risiko	Middels risiko	Middels risiko	Høy risiko	Svært høy risiko
Oftere enn en gang per år	Middels risiko	Middels risiko	Høy risiko	Svært høy risiko	Svært høy risiko

Fig. 1 En risikomatrix for liv/helse med fem kategorier for både sannsynlighet og konsekvens.

Spesielle forhold:

En del spesielle forhold rundt hendelsen vurderes:

- Har den storulykkespotensiale?
- Er det avhengigheter mellom SKFer i dette scenariet?
- Er hendelsen generisk eller spesifikk (med konkret stedsangivelse)?
- Representerer hendelsen spesielle interne/eksterne kommunikasjonsproblemer?

Dette er informasjon som er relevant når en skal velge ut uønskede hendelser til detaljanalyse.

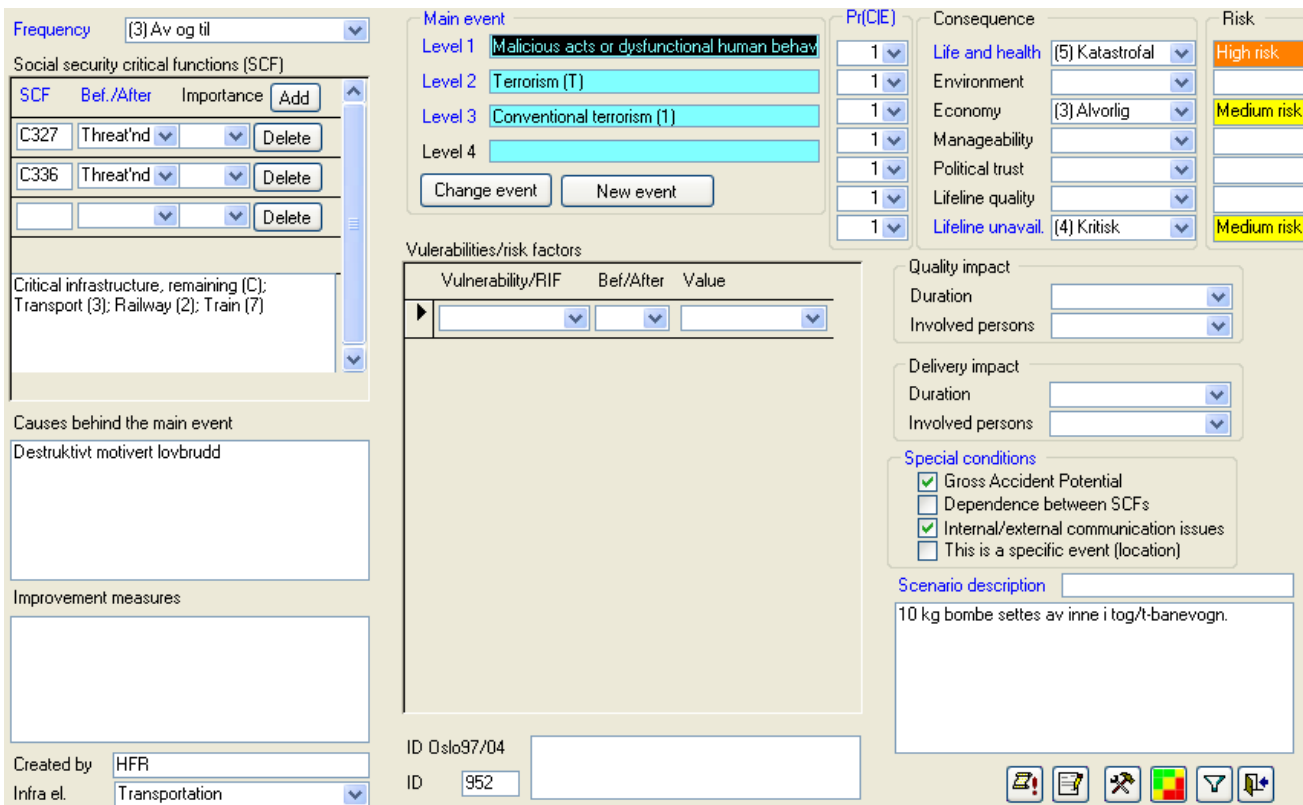
Grovanalysen avsluttes med en oppsummering av de viktigste sårbarhetene og truslene, samt en vurdering og prioritering av risikoreduserende tiltak.

4.2 Verktøystøtte

InfraRisk er et verktøy som gir støtte i arbeidet med risikovurderinger, hovedsakelig i grov-analysefasen. Det er utviklet i BAS5 og videreutviklet i DECRIS. For en grovanalyse kan alle punktene som er nevnt i forrige avsnitt utføres i InfraRisk. For hver uønskede hendelse kan man lenke til samfunnskritiske funksjoner som berøres og legge inn sannsynlighet og konsekvens. Risiko beregnes direkte som en funksjon av disse, og man får generert en risikomatrix som viser hvor den enkelte hendelsen blir plassert.

InfraRisk støtter enkle FTA og ETA, og det er en intensjon å lage grensesnitt mellom InfraRisk og mer avanserte verktøy som også støtter nettverksstrukturer (videre arbeid).

Fig. 2 viser et skjermbilde fra InfraRisk.



The screenshot displays the InfraRisk software interface for a risk analysis. Key sections include:

- Frequency:** [3] Av og til
- Social security critical functions (SCF):** A table with columns for SCF, Bef./After, and Importance. Two entries are visible: C327 (Threat'nd) and C336 (Threat'nd).
- Main event:** A hierarchical list of event levels:
 - Level 1: Malicious acts or dysfunctional human behav
 - Level 2: Terrorism (T)
 - Level 3: Conventional terrorism (1)
 - Level 4: [Empty]
- Vulnerabilities/risk factors:** A table with columns for Vulnerability/RIF, Bef./After, and Value.
- Pr(CIE):** A vertical list of probabilities, all set to 1.
- Consequence:** A list of consequence categories with dropdown menus:
 - Life and health: (5) Katastrofal
 - Environment: [Empty]
 - Economy: (3) Alvorlig
 - Manageability: [Empty]
 - Political trust: [Empty]
 - Lifeline quality: [Empty]
 - Lifeline unavail.: (4) Kritisk
- Risk:** A vertical list of risk levels: High risk (orange), Medium risk (yellow), and Medium risk (yellow).
- Quality impact:** Fields for Duration and Involved persons.
- Delivery impact:** Fields for Duration and Involved persons.
- Special conditions:** Checkboxes for Gross Accident Potential, Dependence between SCFs, Internal/external communication issues, and This is a specific event (location).
- Scenario description:** A text box containing "10 kg bombe settes av inne i tog/t-banevogn."
- Metadata:** Created by HFR, Infra el. Transportation, ID Oslo97/04, ID 952.

Fig. 2 Skjerm bilde fra InfraRisk; grovanalyse av en uønsket hendelse.

Nærmere beskrivelser av grovanalysen og InfraRisk finnes i notat 3, *DECRIS – Beskrivelse av verktøy InfraRisk* og notat nr. 4, *DECRIS – Beskrivelse av grovanalysemetodikken*, [3]. Notat nr. 2, *DECRIS – Sammendrag ROS-analyser*, [3], gir et sammendrag av en del tidligere risikovurderinger utført for fylker og bykommuner; her er altså ikke DECRIS metodikken benyttet.

4.3 Grovanalyse utført for Oslo

Som en del av metodeutviklingen ble det utført en grovanalyse av de aktuelle infrastrukturene for Oslo kommune. Flere møter ble avholdt med Oslo kommune (Beredskapssetaten) og en rekke av deres samarbeidspartnere.

Viktige uønskede hendelser ble identifisert for

- Vannforsyning
- Strømforsyning
- Transport, (bane, veg)

Videre ble IKT som samfunnskritisk funksjon trukket inn i analysen.

Analysen dekket en rekke tekniske (T) hendelser og viljeshandlinger (V), samt en del naturhendelser (N), men ingen medisinske/biologiske (B) hendelser.

En kort oppsummering av analysen er gitt i notat 5, *DECRIS – Oppsummering av grovanalysen for Oslo*, [3]. I alt fire hendelser ble valgt ut til nærmere, detaljert analyse, se neste kapittel.

5 DECRIS: Detaljanalyser

Ulike prinsipper kan legges til grunn for utvelgelse av hvilke hendelser som skal vurderes nærmere. Ofte benyttes risikomatriisen til å identifisere hendelser med størst risiko. En kan også se på hendelser med storulykkespotensial, hendelser med sterke avhengigheter mellom infra-strukturer, spesielle årsakstyper (viljeshandlinger), eller spesielle konsekvenskategorier (utilgjengelighet av infrastruktur). Det er viktig at formålet med detaljanalysen først klargjøres.

Når et sett av hendelser er valgt, gis en detaljert scenaribeskrivelse av disse. Ut fra en generisk hendelse beskrives et konkret scenario (spesifikt sted) som analyseres. Når scenariet er ferdig analysert, foretas det en oppsummering med hensyn til risikoen knyttet til det den generiske hendelsen (for eksempel innen Oslo).

Ofte vil resultater fra detaljanalysen måtte håndteres som sensitiv informasjon. Det må derfor gjøres en vurdering på hvem som skal ha tilgang til dem.

I dette kapitlet gis først en kort oversikt over detaljanalyser. Deretter beskrives fire "case", der ulike detaljanalyser inngår, se også notatene, 6-10, [3].

5.1 Ulike metoder til bruk i detaljanselysene

Det finnes en rekke metoder som er aktuelle for detaljanalysen. Vi kan skille mellom noen hovedtyper: årsaksanalyser, barriereanalyser, avhengighetsanalyser og konsekvensanalyser. Det kan dessuten være en egen analyse knyttet til beredskap og krisehåndtering. Analysene kan gjerne knyttes opp til ulike aspekter ved det såkalte "Bow tie"-diagrammet, se Fig. 3. Det trenger imidlertid ikke være et skarpt skille mellom disse hovedtypene av analyser. Formålet med analysen må være førende for hvilke metoder man velger å benytte.

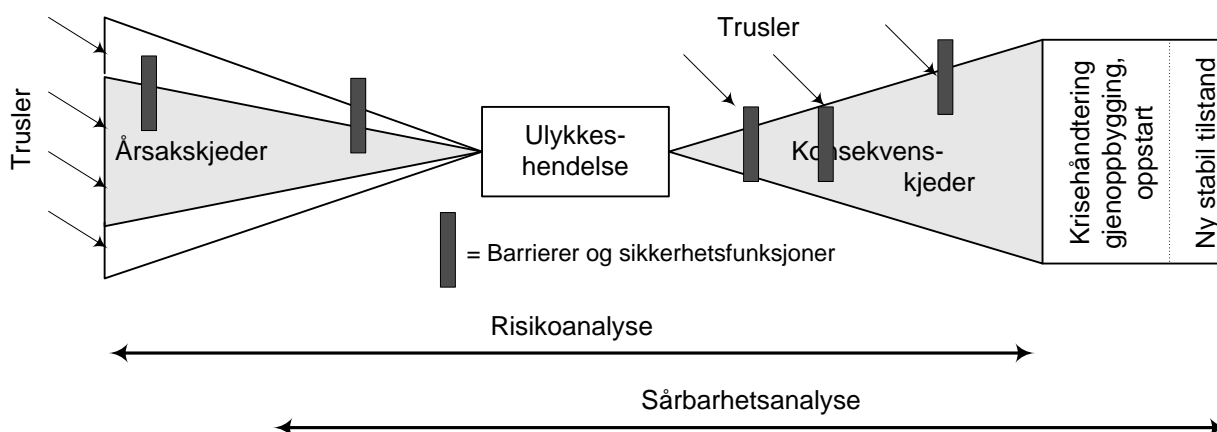


Fig. 3 Bow tie-diagram.

Barriereanalyse

Hensikten er å identifisere eksisterende barrierer og status for disse. Eksempler på slike er fysisk beskyttelse, adgangskontroll og redundans. Barrierer bør kategoriseres etter hvilke årsaker de skal forhindre. Svikt i barrierer kan analyseres ved hjelp av feiltre.

Årsaksanalyse

Hensikten er å identifisere alle mulige årsaker til den uønskede hendelsen. Til dette brukes gjerne feiltreanalyse (Fault Tree Analysis, FTA) som metode. Fig. 4 er et eksempel på en type årsaks-/konsekvensanalyse. Dette diagrammet gir på et overordnet nivå en oversikt over årsaker til tre ”hovedhendelser” (grønt i figuren): *Lagrene tømmes*, *luke/pumpe-problem*, *brann på kaiområdet*, og gir samtidig tre mulige konsekvenser (rødt) med hensyn til leveringssikkerhet, som følge av disse tre hendelsene.

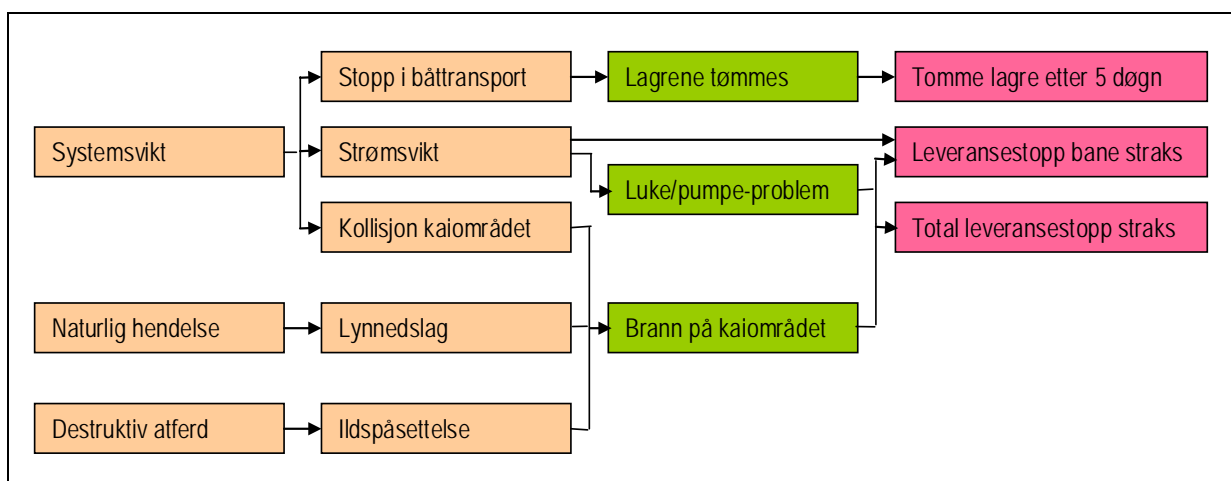


Fig. 4 Overordnet årsaks-/konsekvensdiagram for leveringssikkerhet fra oljeterminalen på Sjursøya, (Notat 9)

Fig. 5 er et eksempel på et feiltre, som gir en strukturert nedbryting av årsaker til hendelsen ”Vann leveres ikke fra Oset Vannverk”. Av dette feiltreet finnes alle kombinasjoner av hendelser som kan gi denne uønskede hendelsen. Feiltreet gir også mulighet til å beregne frekvens eller sannsynlighet for den uønskede hendelsen.

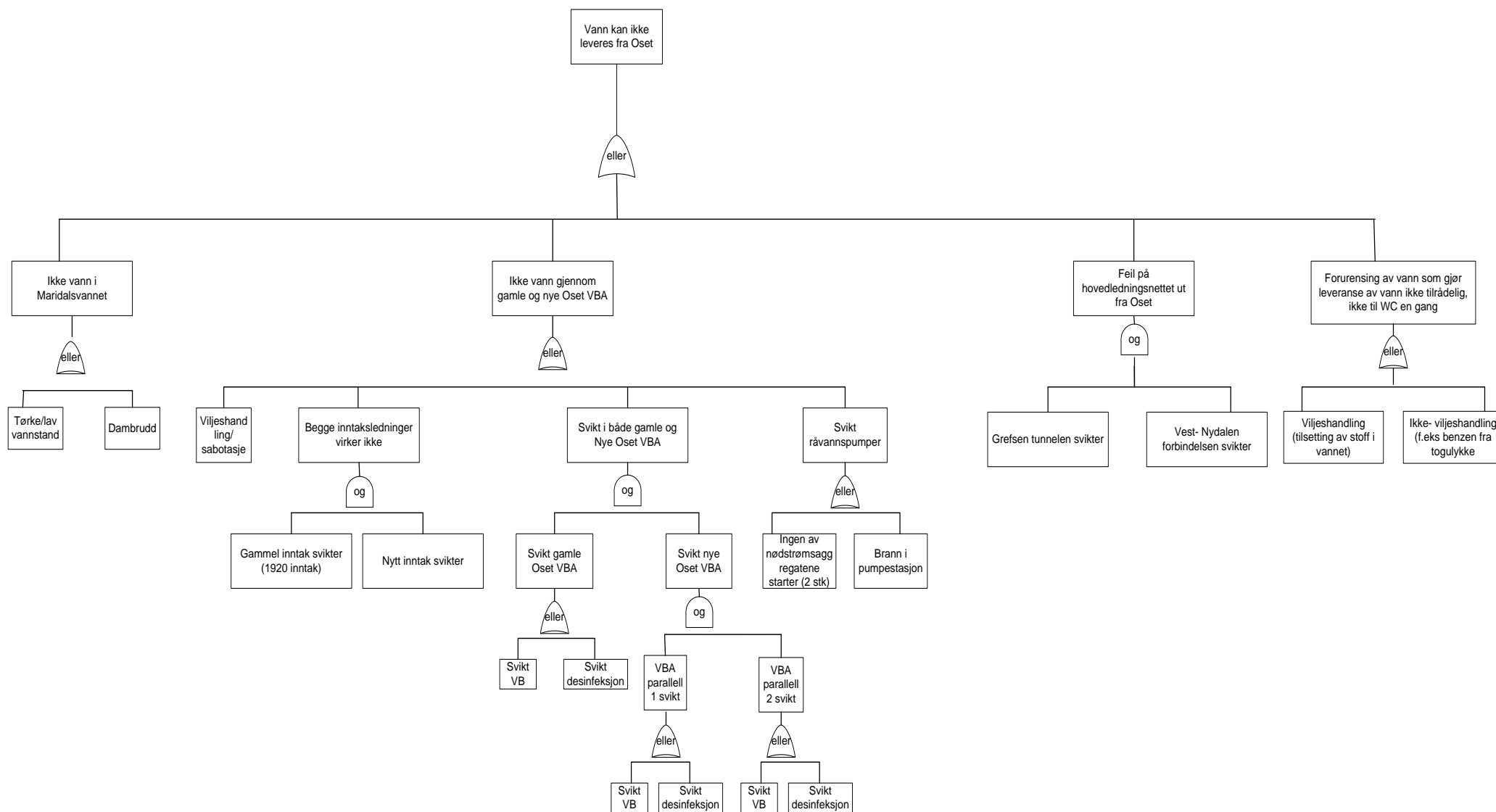


Fig. 5 Feiltre for hendelsen "Vann kan ikke leveres fra Oset", (Notat 8)

Avhengighetsanalyse

Avhengigheter mellom samfunnskritiske funksjoner kan føre til at konsekvensene for samfunnet blir langt mer alvorlige enn det som framkommer ved kun å se på en enkelt SKF. I DECRIS har en derfor utviklet en egen metode for avhengighetsanalyse, som består av følgende trinn:

- 1) Detaljert beskrivelse av ulykkescenariet; alle faktorer som sted, tid, fysiske objekter, funksjoner, samt mulige årsaker beskrives.
- 2) Avdekke ulike avhengigheter, ved hjelp av systematiske kontrollspørsmål.
- 3) Kvalitativ identifisering og kartlegging av avhengighetene.
- 4) Semikvantitativ analyse for å estimere totalrisiko; (basert på vurderinger av sannsynlighet/frekvens, og omfang/varighet av hendelse).
- 5) Kvantitativ analyse av totalrisiko; kan bruke feiltreanalyse, hendelsestreanalyse, og evt. nettverksmodeller av kapasiteten til en infrastruktur.
- 6) Evaluere resultat og angi tiltak for å redusere kritiske avhengigheter; vurdere om tilsvarende hendelser også kan skje andre steder.

I analysen tar en utgangspunkt i de(n) primær(e) SKF, som direkte berøres av den uønskede hendelsen.

DECRIS benytter to kategorier for avhengigheter: funksjonsavhengigheter og lokasjonsspesifikke avhengigheter. Med funksjonsavhengigheter menes at en hendelse i én SKF også kan sette andre SKFer ut av spill; noe som skjer for eksempel ved et strømutfall. Med lokasjonsspesifikke avhengigheter menes at den rammede SKF er fysisk i nærheten av andre SKF, og at dette kan forårsake at også disse også rammes av hendelsen. Et eksempel på dette er brann, hvor brannen eller tilhørende røyk kan spres og gjøre tilgrensende SKF utilgjengelig for publikum, eventuelt påføre skade på personer som benytter den tilgrensende SKF. Graden av denne type avhengighet er dermed knyttet til ”styrken” til de (fysiske) skiller/barrierer mellom aktuelle SKF.

En spesiell form for avhengighet oppstår når det er mangelfulle barrierer mellom sårbare objekter, slik at dersom en person med uhederlige hensikter får tilgang til ett objekt, får han samtidig tilgang til en rekke andre. Denne formen for avhengighet åpner for meget alvorlige hendelser.

For å illustrere og analysere ulike avhengigheter er det i DECRIS utviklet et såkalt kaskadediagram. Fig. 6 er et eksempel på dette, der man følger hendelsen ”svikt i strømforsyning”, (som følge av ”brann i kulvert”).

Notat nr. 10, *Avhengighetsanalyse for kritisk infrastruktur*, [3], beskriver avhengighetsanalysen nærmere.

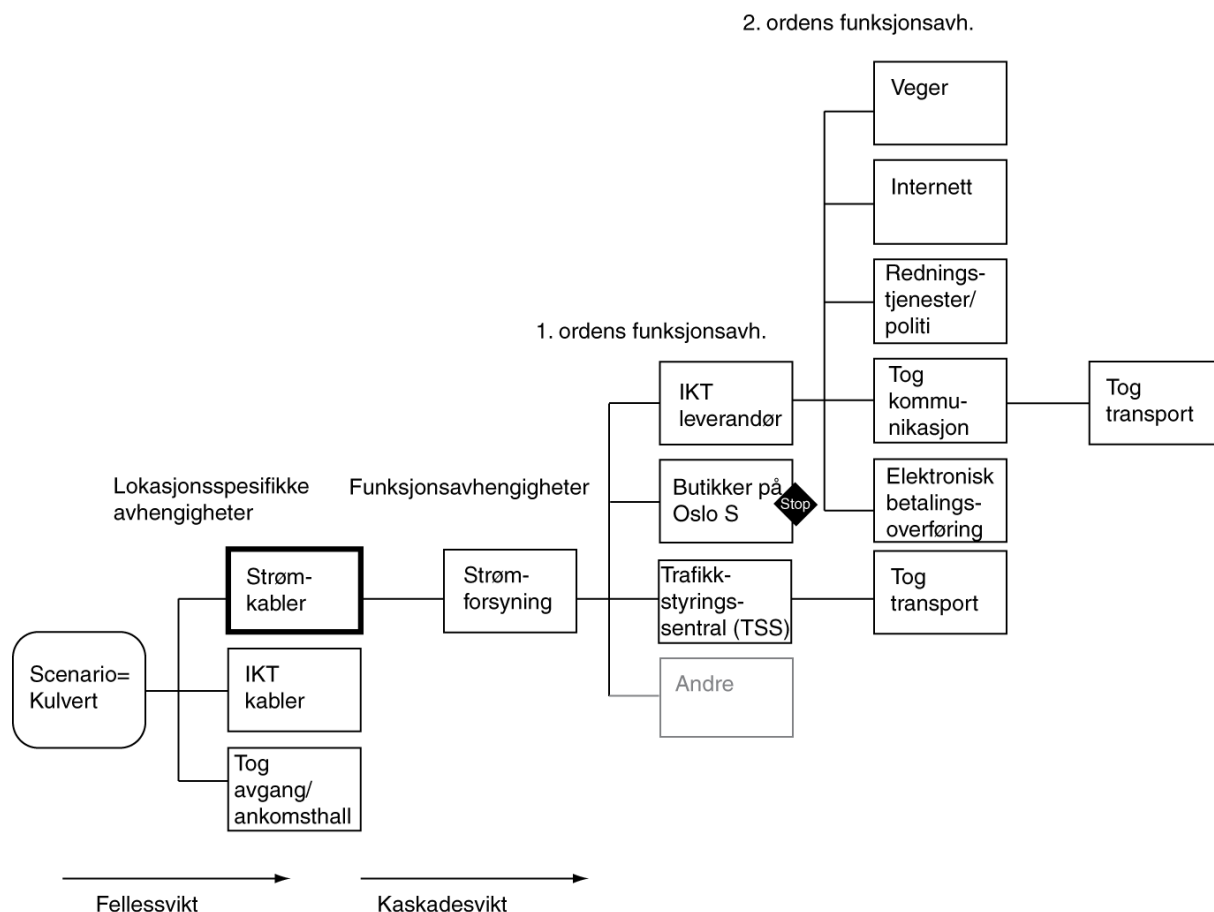


Fig. 6 Kaskadediagram for scenariet "Brann i kulvert" med hovedvekt på svikt i strømforsyning, (Notat 10)

Konsekvensanalyse

Det er viktig å identifisere alle mulige konsekvenser av en uønsket hendelse. Konsekvensdimensjoner som drepte og skadde, miljøkonsekvenser, materielle skader og omdømmetap kan typisk inkluderes. Til dette brukes ofte hendelsestreanalyse (Event Tree Analysis, ETA). Ved en slik analyse kan man beregne sannsynligheter for de ulike konsekvensene. Fig. 7. viser et eksempel på et ETA-diagram.

Her vil første oppgave være å definere selve hendelsen. Det er funnet at "En ukes bortfall av vannforsyning" er en interessant hendelse, som har spesielle beredskapsutfordringer. Tilsvarende kan det være interessant å analysere for eksempel konsekvenser av "En dags bortfall av vannforsyning", osv.

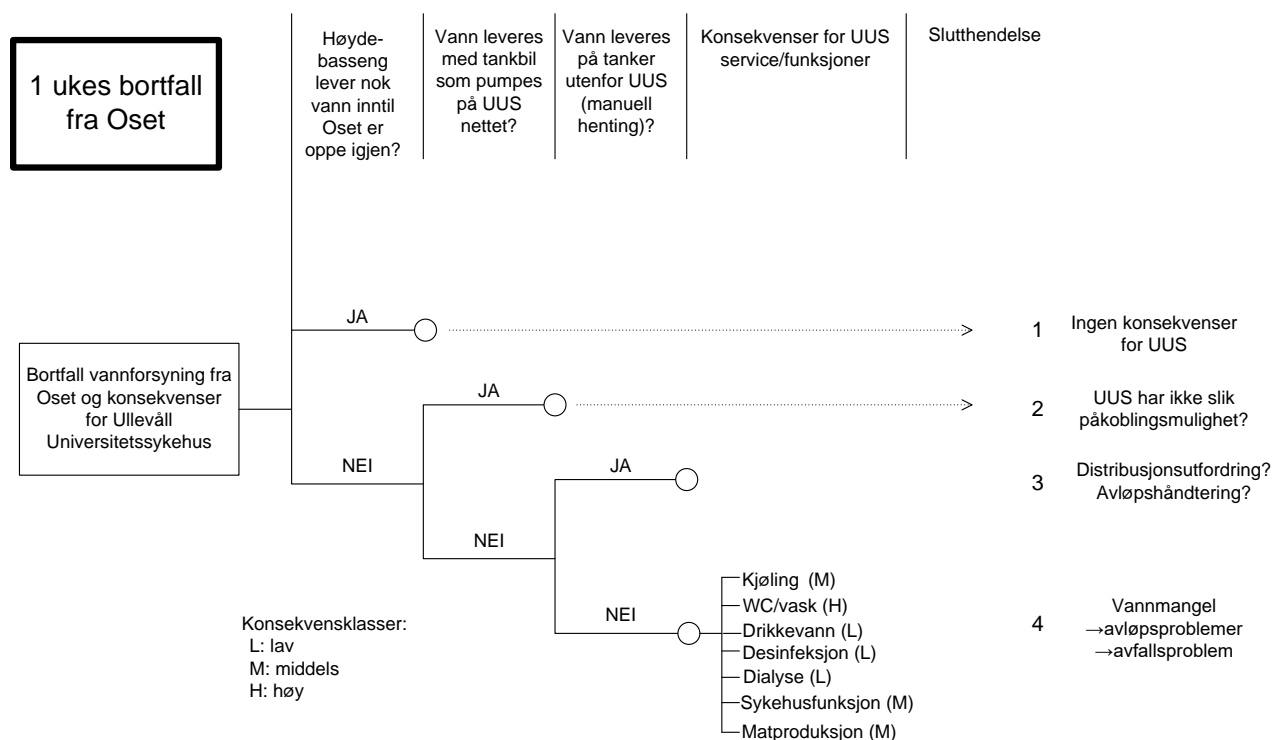


Fig. 7 Hendelsestre for scenariet "En ukes bortfall av vannforsyning fra Oset", (Notat 8)

For komplekse infrastrukturer som for eksempel strømforsyning, kan det være mer hensiktsmessig å bruke nettverksanalyse for å kartlegge konsekvenser. Om utfall i strømforsyning vil medføre utilgjengelig strømforsyning til de enkelte leveringspunktene, må ofte kartlegges ved å analysere elektriske konsekvenser som følge av utfall av kraftledninger, kabler, transformatorer osv. Dette kan gjøres ved å benytte metoder for utfallsanalyse der en også kan ta hensyn til reserve- og omkoplingsmuligheter. Det finnes forskjellige teknikker og verktøy for å gjennomføre slike konsekvensanalyser av strømforsyningssystemet (nettverket), se notat nr. 7, *Utfall i strømforsyningen – analysemetodikk og case* [3].

Analyse av krise- og redningsledelse

Det kan være avhengigheter i beredskap og krisehåndtering for ulike samfunnskritiske funksjoner. Elementer som kan studeres, er samhandling i krisesituasjonen og kommunikasjon både internt og ut til berørte parter og media. I en slik analyse kan bl.a. et STEP-diagram benyttes. Krise- og redningsledelse er nærmere omtalt i notat nr. 6, *DECRIS – Risikoanalyse av kritisk infrastruktur: Komplette risikoanalyse og gjennomføring av detaljanalyse* [3].

5.2 Case 1: Utfall i strømforsyningen

I grovanalysen ble det vurdert hvilke av hendelsene med utfall i strømforsyningen som vil kunne medføre at minst en bydel i Oslo får avbrudd i strømforsyningen over en viss varighet. Analysen viste at slike uønskede hendelser dreier seg om utfall av transformatorstasjoner og kraftledninger eller kabler i sentral- og regionalnettet. Hendelsene antas å være mest kritiske dersom de inntrer i situasjoner med maksimal belastning i nettet, vanligvis om vinteren når det er kaldt. I slike situasjoner er det relativt lav reservekapasitet tilgjengelig ved utfall.

Uønskede hendelser som vil gi konsekvenser i det omfanget vi her snakker om, vil i hovedsak dreie seg om flere samtidige feil. Noen steder er det *avhengigheter* mellom hovedkomponentene i nettet i form av fysisk nærhet (fellesføringer), felles komponenter eller funksjonsavhengigheter. Eksempler på kombinasjoner av hendelser (feil og utfall) i kraftsystemet som kan gi større konsekvenser, er feil på to kraftledninger på samme mastepunkt eller flere kabler i samme grøft eller kulvert.

Detaljanalysen fokuserte på å identifisere kombinasjoner av utfall som medfører leveringsvikt for leveringspunkter i regionalnettet i Oslo. Det ble benyttet utfallsanalyse for å kartlegge elektriske konsekvenser i nettet og konsekvenser for leveringspunkter i regionalnettet. Leveringssvikt skjer typisk hvert annet år, og er som oftest kortvarig (under 1 time) fordi driften i de fleste tilfeller kan gjenopprettes ved omkopling.

Infrastruktureieren, i dette tilfellet nettselskapet, har kun mulighet til å kartlegge konsekvensene på et aggregert nivå til de enkelte leveringspunkter ettersom den detaljerte analysen av konsekvensene fordrer detaljert kunnskap om den enkelte sluttbruker. Konsekvensene må derfor kartlegges separat hos de øvrige infrastrukturere som er avhengige av strømforsyning, evt. hos den enkelte sluttbruker.

Dette case er beskrevet nærmere i notat nr. 7, *Utfall i strømforsyningen – analysemetodikk og case*, [3].

5.3 Case 2: Bortfall av vann i Oset/Maridalsvannet; konsekvenser for Ullevål sykehus

I grovanalysen for vannforsyningen i Oslo ble hendelsen at det blir helt bortfall av vann fra hovedvannkilden Oset/Maridalsvannet valgt ut som en hendelse en ønsker å gå videre med i en detaljanalyse. Store deler av vannforsyningen til Oslo forsynes fra Maridalsvannet/Oset og konsekvensene vil bli merkbare allerede etter kort tid for de fleste forbrukere/kunder. I dette case har en valgt å fokusere på de konsekvensene et slikt bortfall vil ha for et sykehus, og det aktuelle sykehuset er Ullevål Universitetssykehus (UUS). Den aktuelle uønskede hendelsen har så langt ikke vært observert i Oslo.

For å analysere og illustrere hendelsen benyttes et ”bow-tie”-diagram (Fig. 3) for å se på både årsakssiden og konsekvenssiden av den uønskede hendelsen. Årsakssammenhengen er modellert ved hjelp av en feiltreanalyse, (Fig. 5). En detaljert beskrivelse av de enkelte hendelsene som inngår i feiltreet, er utelatt fra analysen. Konsekvenskjeden er modellert ved hjelp av en hendelsestreanalyse, (Fig. 7), hvor en ser på bortfall av ulik varighet.

En av hovedkonklusjonene fra analysen er at det er problemeier (dvs sykehuset) som selv må definere hvilke behov de har og vurdere om dagens leveringssikkerhet for vann er god nok for dem. Hvis forsyningssikkerheten ansees som ikke tilfredsstillende, må problemeier iverksette nødvendige tiltak. Det er utarbeidet et forslag til ”kokebok”/roadmap som viser hvordan vannverk i samarbeid med sykehus/helseinstitusjon kan planlegge for beredskapssituasjon hvor en får bortfall av vannforsyningen inn på anlegget og det må leveres nødvann. Denne metoden vil bli videreutviklet i samarbeid med UUS og Vann og avløpsetaten i et annen prosjekt.

Dette case er beskrevet nærmere i notat nr. 8, *Detaljering av hendelser i vannforsyning – Case: bortfall av vann Oset/Maridalsvannet – konsekvenser for Ullevål sykehus*, [3].

5.4 Case 3: Leveringssikkerhet av petroleumsprodukter fra Sjursøya til Gardermoen

Innledningsvis ble det gjort en generell vurdering av hvilke kritiske hendelser som kan inntreffe ved havneanlegget på Sjursøya i Oslo, herunder brann- og eksplosjonsfare, alvorlig miljøforurensning, blokkering av vitale transportårer, langvarig bortfall av strøm osv. Diverse analyser er gjennomført tidligere, men resultatene er ikke offentlig tilgjengelig, dels av hensyn til samfunnssikkerheten, dels for å beskytte bedriftsinterne opplysninger.

Anleggene på Sjursøya omfatter et sentrallager for petroleumsprodukter med daglige leveranser av flydrivstoff til Gardermoen. Stopp i disse leveransene vil skape problemer for flytrafikken allerede etter 1-2 døgn. Leveranseproblemer kan oppstå i tilknytning til anleggene på Sjursøya, men kan også skyldes problemer med leveransene til Sjursøya eller togtransporten mellom Sjursøya og Gardermoen. Blant aktuelle kriseløsninger kan være transport med bil fra Sjursøya, Fredrikstad eller Slagentangen, men dette forutsetter at nødvendige forberedelser er gjort for å iverksette riktig tiltak når krisen er et faktum.

Det er mange ulike aktører, både offentlige, halvoffentlige og private, som har ulike interesser og ansvar når slike kriser inntreffer. Derfor er det en stor utfordring å finne frem til aktuelle forebyggende tiltak og krisetiltak som er tilpasset de mest aktuelle krisesituasjonene. Notat nr. 9, *Leveringssikkerhet for petroleumsprodukter fra Sjursøya i Oslo*, [3], går nærmere inn på disse problemstillingene og konkluderer med at det fremdeles er mange metodiske og faglige utfordringer for å kunne gjennomføre ROS-analyser for slike komplekse problemstillinger på en fullgod måte.

5.5 Case 4: Brann i kabelkulvert på Oslo S

Utgangspunktet er en generisk hendelse, som har stort potensial for omfattende konsekvenser, spesielt med hensyn på tilgjengelighet av viktige samfunnsfunksjoner:

Ødeleggelse i felles framføringstrasé for elektrisitet, IKT/samband, evt. vann/avløp, i sentralt byområde. Framføringstraséen er fysisk plassert under bakkenivå (kulvert e.l.) eller på bro.

Selve detaljanalysen behandler et spesifikt scenario, en konkret hendelse på Oslo S, [4]:

Utfall av/skade på deler av strømforsyning og/eller IKT-nett i en kulvert nær Oslo S; med følgekonskvenser for annen SKF.

Det er ikke utført en ulykkesgransking, men en analyse av hvilke konsekvenser en ødeleggelse av denne kulverten kan gi.

Det utføres en avhengighetsanalyse for dette scenariet, der det altså inntreffer umiddelbar skade på strømforsyning og IKT. Funksjonsavhengigheter og lokasjonsspesifikke avhengigheter analyseres som skissert over (Fig. 6). Med utgangspunkt i kaskadediagrammet gjennomføres også en kvantifisering for å angi totalrisiko knyttet til scenariet. Analysen er ikke komplett, og må oppfattes som en ren illustrasjon av metoden for avhengighetsanalyse som er utviklet i DECRIS.

Dette case er nærmere beskrevet i notat nr. 10, *Avhengighetsanalyse for kritisk infrastruktur*, [3].

6 DECRIS: Vurdering av totalrisiko – ansvar og tiltak

Etter å ha analysert et konkret, lokasjonsspesifikt scenario (knyttet til spesifikk kritisk enhet) foretas det en ”generalisering” ved at en vurderer totalrisikoen knyttet til denne type hendelser i det aktuelle området (f. eks. Oslo). En slik generalisering må basere seg på opplysninger om hvor mange enheter av denne typen som finnes i det aktuelle området, og om den analyserte enheten vurderes å ha høyere eller lavere risiko enn andre slike enheter i området.

Det avsluttende trinnet i en komplett analyse omfatter en oppsummering og vurdering av risiko-reducerende tiltak. Slike tiltak går typisk ut på å innføre nye barrierer og forsterke eksisterende barrierer, samt forbedre beredskap og krisehåndtering. Både på årsakssiden og konsekvenssiden må en vurdere hvilken effekt de identifiserte tiltakene vil ha på risikoen.

Et sentralt punkt er å klargjøre ansvar for oppfølging av tiltak. Tabell 1 (Notat 9) viser eksempel på en ”ansvarsmatrise”, med oversikt over aktuelle aktører og hvilket ansvar hver av dem har. Det er viktig å ha diskusjoner i dialog-/fokusgrupper med de ulike aktørene. Det knytter seg særlig store utfordringer til analyser av problemstillinger med mange offentlige og private aktører med uklare ansvars- og myndighetsforhold. Aktuelle interesser kan knytte seg til:

- Direkte økonomiske interesser
- Indirekte kortsiktige interesser
- Indirekte langsiktige interesser
- Betalingsvillighet for å unngå ulemper
- Sektorinteresser
- Samfunnsmessig helhetssyn

Ved vurdering av tiltak for å redusere risikoen, vil flere aktører kunne komme inn i bildet. Mange eksterne aktører kan sitte med viktig eller nødvendig kompetanse på spørsmål knyttet til å finne frem til et riktig nivå på krav til tilgjengelighet av ulike SKF.

Tabell 1: Rolle/ansvar-matrise for leveringssikkerhet for flydrivstoff, (Notat 9)

Aktør	Økonomi direkte	Indirekte kortsiktig	Langsiktig renomme	Betalingsvilje	Begrenset samf.ansv.	Totalansvar	Politisk betydning
Oljeselskap; Statoil	X	x	x				
Oslo lufthavns tankanlegg	X	x					
Transportør CargoNet	X		x				
Transportsystem Jernbaneverket	X		x				
Oslo havn					x		
Felles HMS-organ på Sjursøya		x	x				
Norsk petroleumsinstitutt		x	x				
Oslo lufthavn	X	x	x		x		
Flyselskapene, rute og charter	X	x	x	x			
Flytrafikanter Tjenestereiser	X			x			
Flytrafikanter Privatreiser	X			x			
Avinor			x		x		
Kystverket					x		
DSB og NSM			x		x	x	
Fylkesmannen					x		
Kommuner, fylker					x		
Rettsapparatet					x		
Departementene					x		x
Regjeringen						x	x
Stortinget						x	
Konsulenter og forskningsinstitutt							

7 Diskusjon og videre arbeid

DECRIIS-prosjektet har kommet et godt stykke på vei med å samle/utvikle viktige metoder for en total risikovurdering av kritisk infrastruktur. Infrastrukturene strømforsyning, vannforsyning, trafikk (veg/bane) og IKT er benyttet som eksempler, hvor IKT primært har blitt sett på som støtte til de øvrige. I DECRIIS er det gjort den begrensning at IKT mest omtales som samband; mobilnett og kommunikasjon; i mindre grad som styringssystem og administrative system. For de utvalgte infrastrukturene er det videreutviklet metoder for grovanalyse, basert på prosjektet BAS5; blant annet med en felles hendelses- og konsekvensklassifisering. Verktøyet InfraRisk er også utvidet med noe ny funksjonalitet, og det er testet ut og tilpasset de aktuelle infrastrukturene.

Ulike metoder til bruk i detaljanalysen er beskrevet og eksemplifisert på utvalgte uønskede hendelser. Det er også presentert en ny metode for analyse av avhengigheter på tvers av infrastrukturene. Dette muliggjør analyse av følgekonsekvenser, men metoden er i beskjeden grad uttestet, og det er behov for videre bearbeiding av denne.

Innenfor detaljanalyse av infrastruktur vil nettverksanalyser være et viktig verktøy. Her finnes det allerede relevante metoder og verktøy for analyse innen de enkelte infrastrukturene, men det er et behov for å integrere slike infrastrukturens spesifikke analyser som del av en risikovurdering på tvers av infrastrukturene.

Når det gjelder årsaker, ville det vært nyttig å ha et generelt feiltre for hver infrastruktur, dvs. ett for bortfall av strøm, ett for bortfall av vann osv. Som utgangspunkt kan man ha en generell årsaksliste, som inkluderer teknisk og menneskelig svikt, brann, sabotasje og naturhendelser. Disse feiltrærne kunne være underlag ved analyse av spesifikke hendelser innenfor infrastrukturene. Dette er et mulig tema for videre arbeid. Et slik hjelpemiddel kunne også samkjøres med verktøyet InfraRisk. Som tidligere nevnt kan et grensesnitt mellom InfraRisk og et mer avansert verktøy som støtter avanserte analyser (e.g. nettverksstrukturer), være en annen videreutvikling.

Kompleksiteten i en tverrsektoriell risikovurdering er åpenbart en utfordring. Det er svært ressurskrevende å gjennomføre flere detaljanalyser og sammenfatte disse til en totalvurdering (f.eks. for Oslo-området), som underlag for en helhetlig prioritering av tiltak. Det gjelder å velge et fornuftig detaljeringsnivå ut fra definerte mål for analysen. På dette området gjenstår det arbeid.

Oppdragsgiver, som ofte er "problemeieren", må klargjøre mål for analysen, spesifisere akseptkriterier og være tydelig på hvem som har ansvar for gjennomføring og oppfølging av tiltak. Det må spesifiseres hvordan samarbeidet mellom alle aktører skal organiseres. Det er spesielt viktig å klargjøre ansvar for oppfølging. Det kan være store utfordringer i problemstillinger med mange offentlige og private aktører med til dels uklare ansvars- og myndighetsforhold, og der det ikke alltid er like klart hvem som egentlig er "problemeieren".

Grenseoppgang mellom ulike infrastruktureiere er vanskelig. En infrastruktureier behøver ikke å ha full oversikt og kontroll over "sin" infrastruktur. Dette kan komplisere arbeidet med å kartlegge konsekvenser, samtidig som eier kan ha begrensede muligheter for å gjennomføre tiltak. Et eksempel er ved utfall i strømforsyning og feil i telenett, hvor nettselskapet ikke har mulighet til å kartlegge konsekvensene fullt ut, kun på et aggregert nivå. Detaljanalyse av konsekvensene må skje hos de øvrige infrastrukturene som er avhengige av strømforsyning, eventuelt hos den enkelte sluttbruker.

Den enkelte sluttbrukers vil også ha ansvar for å kartlegge egen avhengighet og sårbarhet, som er et viktig moment mht det kollektive samfunnsikkerhetsarbeidet.

En komplett risikovurdering vil kreve kunnskap og informasjon om en rekke objekter. Man må samle riktig kompetanse og informasjon, samt sørge for kommunikasjon mellom alle relevante aktører, og mulig gjenbruk av informasjon fra tidligere analyser bør vurderes.

Det kan da være et problem å definere hvor grensen går mellom åpen og sensitiv informasjon. Selv om alle opplysninger i seg selv er åpne, kan likevel den totale mengden være sensitiv. Her er det utfordringer å løse med hensyn på hvem som skal få tilgang til informasjon og hvordan man kan unngå spredning. Resultatet fra risikovurderingen kan i mange tilfeller være sensitiv informasjon og bør dermed unndras offentligheten. På samme tid kan den inneholde mange elementer som i utgangspunktet burde gjøres kjent for allmennheten.

DECRIS gir i prinsippet en "all hazards"-tilnærming. Det gjenstår imidlertid arbeid med hensyn til hvordan en skal integrere og håndtere viljeshandlinger i analysen. Spesielt er det i DECRIS ikke vurdert hvorvidt en skal angi sannsynligheter for disse, på samme måte som for tekniske og menneskelige feil.

Bruk av geografiske informasjonssystemer (GIS) er i senere år blitt et nyttig verktøy for analyse av infrastruktur. Spesifikke detaljanalyser der GIS-verktøy er en del av analysen, er kun diskutert i prosjektet, og det er ikke gitt noe bidrag til utvikling av slike analyser. Det samme gjelder metoder og verktøy for beregning av leveringssikkerhet.

Andre viktige tema der det er behov for å gå mer i dybden, er krise- og redningsledelse, samt hvordan en kan og bør kommunisere rundt risiko.

Når vi ser framover, er det utfordringer knyttet til det nye EU-direktivet: *Vern av europeisk kritisk infrastruktur*, som mest sannsynlig blir tatt inn i EØS-avtalen. Dette direktivet gjelder i første omgang energi (strøm, olje og gass) og transport (veg, jernbane, luft og sjø). Direktivet fokuserer på sårbarhet som kan gi konsekvenser utenfor moderlandet og krever innmelding av sårbarhet og tiltak i løpet av to år. Her må det på nasjonalt plan bestemmes hvem skal ha ansvaret for disse analysene, og hvordan skal de gjennomføres.

Som belyst ovenfor, er det gjennom arbeidet med risikoanalyse i DECRIS-prosjektet identifisert en rekke metodiske utfordringer som det ikke har vært rom for å arbeide videre med innenfor rammene av DECRIS. Listen nedenfor kan tjene som en oppsummering av tema der det er behov for videre forskning og utvikling innenfor risikovurdering av kritiske infrastrukturer:

- Videreutvikle en hensiktsmessig hendelses- og konsekvensklassifisering for tverrsektorielle risikoanalyser av kritiske infrastrukturer
- Etablere generelle feiltrær for de enkelte infrastrukturer basert på felles årsakslister
- Integrere infrastrukturens spesifikke analyser (f.eks. nettverksanalyser) i tverrsektorielle risikoanalyser
- Integrere viljeshandlinger i risikoanalysen (all-hazards approach)
- Klimaendringers betydning for kritiske infrastrukturer: Hvilke typer klimadata er nødvendige i tverrsektorielle risikoanalyser og hvordan bruke disse i analysene
- Hvordan utnytte GIS-verktøy i risikoanalysene (kartlegge avhengigheter mm)
- Risikovurderinger av kritiske infrastrukturer med lange levetider: Hvordan håndtere aldring, reinvesteringer (nye komponenter), økende kompleksitet og avhengighet osv.
- Identifikasjon tiltak: Hvordan vurdere og prioritere tiltak på tvers av infrastrukturer

Referanser

1. NOU 2006:6 “*Når sikkerheten er viktigst*”. Justis- og politidepartementet.
2. Henriksen, S., Sørli, K. and Bogen, L.: *Metode for identifisering og rangering av kritiske samfunnsfunksjoner*, FFI/RAPPORT-2007/00874, 2007.
<http://rapporter.ffi.no/rapporter/2007/00874.pdf> (sist aksessert 27. mai 2009)
3. DECRIS’ nettside, inkludert alle notater:
<http://www.sintef.no/Projectweb/SAMRISK/DECRIS/> (sist aksessert 27. mai 2009)
4. Direktoratet for samfunnsikkerhet og beredskap: *Brann i kabelkulvert – Oslo sentralstasjon 27.11.2007*, januar 2008.

Vedlegg A. Notater og publikasjoner

Notater

1. *DECRIIS – Problemstillinger rundt tverrsektorielle risikoanalyser. Kritisk infrastruktur*; Håvard Fridheim, Jørn Vatn, Gunhild Åm Vatn, Per Hokstad, Jon Røstum, Ingrid B. Utne, Gerd Kjølle, Inger Anne Tøndel.
2. *DECRIIS – Sammendrag av noen tidligere ROS-analyser utført for fylker og bykommuner*; Ingrid B. Utne, Per Hokstad, Jørn Vatn.
3. *DECRIIS – Beskrivelse av verktøyet InfraRisk (engelsk)*; Jørn Vatn.
4. *DECRIIS – Beskrivelse av grovanalyse-metodikken*; Jørn Vatn, Ingrid B. Utne, Gunhild Åm Vatn, Per Hokstad.
5. *DECRIIS – Oppsummering av grovanalysen for Oslo*; Ingrid B. Utne, Per Hokstad.
6. *DECRIIS – Risikoanalyse av kritisk infrastruktur: Komplett risikoanalyse og gjennomføring av detaljanalyse*; Per Hokstad, Jørn Vatn, Ingrid B. Utne.
7. *Utfall i strømforsyningen – analysemetodikk og case*; Gerd Kjølle.
8. *Detaljerings av hendelser i vannforsyning – Case: bortfall av vann Oset/Maridalsvannet – konsekvenser for Ullevål sykehus*; Jon Røstum.
9. *Leveringssikkerhet for petroleumsprodukter fra Sjursøya i Oslo*; Dag Bertelsen.
10. *Avhengighetsanalyse for kritisk infrastruktur*; Ingrid B. Utne, Per Hokstad, Jørn Vatn.

Publikasjoner

1. I. B. Utne, P. Hokstad, G. Kjølle, J. Vatn, I. A. Tøndel, D. Bertelsen, H. Fridheim, J. Røstum; *Risk and Vulnerability Analysis of Critical Infrastructures – The DECRIIS Approach*; presented at the SAMRISK conference, Sept 2008, Oslo.
2. J. Vatn, B.-M. Drott Sjöberg, G. Å. Vatn Societal Security – A case study related to an LNG facility. presented at the SAMRISK conference, Sept 2008, Oslo.
3. D. Bertelsen; *Sårbarhet i kommunal infrastruktur*, Kommunalteknikk nr. 9/2008.
4. G. Kjølle; *Kritiske infrastrukturer og samfunnssikkerhet*, Xergi nr 3-2008, SINTEF Energiforskning, februar 2009.
5. I. B. Utne, P. Hokstad, J. Vatn; *A structured approach to modelling interdependencies in risk analysis of critical infrastructures*, accepted for ESREL 7.-10. september 2009, Praha.
6. I. B. Utne, P. Hokstad, J. Vatn; *Risk Analysis of critical Infrastructure Interdependencies*, submitted for publication.
7. J. Røstum et al; *Risikoanalyse, bortfall av vann*. Innsendt journalen VANN.
8. G. Kjølle, I.B. Utne, P. Hokstad; *Critical infrastructures and risk analysis of electric supply*, under arbeid.

Vedlegg B. Møter og seminarer i regi av DECRIS

19. november 2007 – Trondheim:

Møte mellom prosjektgruppen og Beredskapetsetaten fra Oslo kommune. Etablering av referansegruppe for case-studier og planlegging av arbeidsprosessen videre.

9. januar 2008 – Oslo:

Møte mellom prosjektgruppen og Ressursgruppa fra Oslo kommune. Presentasjon av deltakere, prosjektet, kommunen, verktøyet InfraRisk og aktuelle arbeidsprosesser.

2. april 2008 – Oslo:

Møte mellom prosjektgruppen og Ressursgruppa fra Oslo kommune. Presentasjon av grovanalysen av infrastrukturene. Diskusjon rundt hendelser som kan tas med videre til en detaljanalyse.

12. juni 2008 – Oslo:

Seminar arrangert av DECRIS og Oslo kommune: *Sårbarhet og avhengigheter i kritisk infrastruktur*. Agenda og deltakere er listet nedenfor.

13. juni 2008 – Oslo:

Møte mellom prosjektgruppen og Ressursgruppa fra Oslo kommune. Presentasjon og diskusjon rundt hendelsene som ble valgt ut for detaljanalyse.

19. september 2008 – Oslo:

Møte mellom prosjektgruppen og Beredkapsgruppa fra Oslo kommune.

12. februar 2009 – Trondheim:

Seminar med prosjektets samarbeidspartnere og andre relevante interessenter. Presentasjoner og diskusjoner rundt resultatene fra prosjektets case-studier. Agenda og deltakere er listet nedenfor.

13. juni 2008: Sårbarhet og avhengigheter i kritisk infrastruktur

Agenda

SAS Plaza Hotel, Oslo

- 0930 **Åpning**
- 0935 *Hendelsen på Oslo S i november 2007. Hva gikk feil, og hva kan en lære*
Birger Hestnes, DSB.
- 1015 *Forskning rörande risk- och sårbarhetsanalys för kritisk infrastruktur vid Lunds universitet. Inkl. analys av konsekvenser av skadad infrastruktur och analyser av beroenden mellan olika infrastruktursystem och olika aktörer som skall hantera en kris.*
Henrik Johansson, LUCRAM (Lund Universitet).
- 1055 *DECRIS-prosjektet og ROS-analyser i Oslo kommune. Kort presentasjon av DECRIS-prosjektet og arbeidet med ROS-analyser i Oslo kommune. Problemstillinger og utfordringer i videre arbeid.* Jan Egil Bäckmark, Oslo Kommune; Per Hokstad, SINTEF.
- 1130 **Lunsj**
- 1230 *From regular threats to unexampled events: Risk, vulnerability and complex systems.*
(presenteres på dansk/norsk)
Erik Hollnagel, Ecole des Mines de Paris – Centre for Research in Risk and Crises.
- 1315 *Utfordringer ifm beredskapsplanen på Nivå 3 (alvorlige hendelser som krever ekstern hjelp for å håndteres). Også om informasjonsflyten mellom etater.*
Kjartan Reksten, Oslo kommune.
- 1400 **Kaffe**
- 1430 *Er Norge forberedt på en pandemisk influensa? Kartlegging av mulige konsekvenser av en pandemisk influensa, og vurdering av tverrsektorielle avhengigheter og utfordringer.*
Elisabeth Longva, DSB.
- 1505 *Sikkerhetsmessig verdivurdering. Hva er det en ikke har 'råd til' å miste, særlig med hensyn til konfidensialitet (når det gjelder informasjon) og tilgjengelighet (når det gjelder objekter). Og hvordan skal dette beskyttes?* Stein Henriksen, NSM.
- 1540 *Oppsummering.* Per Hokstad, SINTEF.
- 1600 **Slutt**

Deltakende virksomheter

Prosjektpartnerne i DECRIS

Oslo kommune og samarbeidspartnere:

- Vann- og avløpsetaten (VAV)
- Hafslund Nett AS
- Samferdselsetaten (SAM)
- Ruter AS (Oslo Sporveier)
- Brann- og redningsetaten (BRE)
- Utviklings- og kompetanseetaten (UKE)
- Oslo Forsikring AS
- Oslo Havn KF
- Beredskapsetaten (BER)

Andre:

- Ullevål universitetssykehus
- Telenor Norge
- Post- og teletilsynet (NPT)
- Fylkesmannens Beredskapsstab
- Vestforsk
- Direktoratet for samfunnsikkerhet og beredskap (DSB)
- Nasjonal sikkerhetsmyndighet (NSM)
- LUCRAM
- Ecole des Mines de Paris

12. februar 2009: Sårbarhet og avhengigheter i kritisk infrastruktur

Agenda

Lerkendal Stadion, Trondheim

- 0915 **Åpning**
- 0920 *DECRIIS-prosjektet og metodikk for ROS-analyser.*
Ulike elementer av DECRIIS-metodikken, bl.a. håndtering av avhengigheter.
Eksemplifisert ved case; Fellesføringer (kulvert Oslo S). SINTEF.
- 1000 *Gjennomgang av ulike case fra Oslo kommune (innlagt kaffepause)*
- Hendelser i kraftsystem
- Bortfall Oset (Ullevål Sykehus)
- Hendelse Sjursøya
SINTEF + partnere.
- 1200 **Lunsj**
- 1250 *Teknikker for bruk av GIS i beskrivelse av risiko/sårbarhetsbildet knyttet til samfunnssikkerhet*
Torstein Nielsen, Beredskapssjef Stavanger kommune.
- 1325 *Resultater fra det utførte arbeidet med risiko og sårbarhetsanalyse for Trøndelagsfylkene - ROS Trøndelag 2009*
Dag Otto Skar, Beredskapssjef Sør-Trøndelag Fylkeskommune.
- 1400 **Kaffe**
- 1430 *Brukernes avhengighet til ekom-tjenester i relasjon til gjennomføring av ROS-analyser.*
Egil A. Andersen, Fagansvarlig Samfunnssikkerhet i Telenor Norge.
- 1500 *Utfordringer knyttet til beredskap i Oslo Kommune*
Jan Egil Bäckmark, Beredskapsetaten, Oslo Kommune
- 1520 *Oppsummering. Utfordringer og veien videre.* Per Hokstad, SINTEF.
- 1600 **Slutt**

Deltakende virksomheter

Prosjektpartnerne i DECRIIS

Oslo kommune og samarbeidspartnere:

- Vann- og avløpsetaten (VAV)
- Hafslund Nett AS
- Beredskapsetaten (BER)

Andre:

- Direktoratet for samfunnssikkerhet og beredskap (DSB)
- Ullevål universitetssykehus
- Telenor Norge
- Norges vassdrags- og energidirektorat (NVE)
- Statoil

- Exxon Mobil
- Stavanger kommune
- Trondheim kommune
- Fylkesmannen i Oslo og Akershus (FMOA), Beredskapsstaben
- Fylkesmannen i Sør-Trøndelag
- Fylkesmannen i Hordaland, Mattilsynet
- Fylkesmannen i Rogaland
- Fylkesmannen i Aust-Agder
- St. Olavs hospital
- Statens vegvesen, region vest
- AdaptCRVA
- CISS