NTNU FFI Forsvarets forskningsinstitutt SINTEF

DECRIS ARBEIDSNOTAT 6

TITTEL

DECRIS Risikoanalyse av kritisk infrastruktur:
Komplett risikoanalyse og gjennomføring av detaljanalyse

FORFATTERE

Per Hokstad, Jørn Vatn, Ingrid B. Utne

SAMMENDRAG

Notatet gir oversikt over trinnene i en DECRIS risikoanalyse. Den komplette analysen inndeles i fem trinn og består av både en *grovanalyse* og *detaljanalyse(r)*.

Grovanalysen refereres her ganske kort og er nærmere beskrevet i Notatene 2-5.

Det gis overordnet beskrivelse av hvordan *detaljanalyser* utføres. Slike analyser er nøyere illustrert og beskrevet i Notatene 7-10.

ISBN	DATO
	2009-06-15
GRADERING	ANTALL SIDER
Åpen	18

KONTAKT DETTE NOTAT	ADRESSE
Per Hokstad	Per.Hokstad@sintef.no, SINTEF, Avdeling for Sikkerhet

NØKKELORD NORSK	NØKKELORD ENGELSK
Risikoanalyse, kritisk infrastruktur	Risk analysis, critical infrastructure

Innhold

1 Innledning

Konseptet for risiko- og sårbarhetsanalyser (ROS) ble utviklet tidlig på nittitallet i Norge. En målsetning med den opprinnelige ROS-metoden var å tilby en forholdsvis enkel metode for å identifisere og fastsette risiko for uønskede hendelser for virksomheter som har begrensede ressurser og/eller kompetanse slik at en fullstendig kvantitativ risikoanalyse ikke er gjennomførbar (eng: QRA = Quantitative Risk Assesment). I praksis har ROS-analysene i hovedsak vært gjennomført i form av en såkalt "grovanalyse" (eng: PHA = Preliminary Hazard Analysis). Styrken ved grovanalyseteknikken er at man med svært begrensede ressurser kan få et grovt bilde av risikoen ved en virksomhet. Resultatet fra analysen kan brukes til for eksempel beredskapsdimensjonering og identifisering av risikoreduserende resultat opp mot de største risikobidragene.

DECRIS-prosjektet har utviklet en risikoanalysemetodikk for sektorovergripende analyser, spesielt på tvers av kritiske infrastrukturer, der gjennomføringen av en komplett analyse beskrives ved følgende fem trinn:

Fase 1:
I. Oppstart / mål for analysen
II. Grovanalyse (dvs. utvidet "standard ROS-analyse")

Fase 2:
III. Utvelging av hendelser for detaljanalyse ("scenarier")
IV. Detaljanalyse av utvalgte hendelser / scenarier
V. Oppsummering / tiltak

Dette notatet vil gi en overordnet diskusjon av disse trinnene, med vekt på trinn IV. Grovanalysen (trinn II) er beskrevet i flere notat (se [3, 4, 5]), og vi går ikke i detalj inn på denne her.

I trinn I må en spesifisere formålet med analysene. Hva er beslutningssituasjonene? Videre bør det etableres et forum for de berørte aktører, og det må avgrensinger for analysen(e).

Aktørene (beslutningstakerne) må bl.a. også fastsette akseptkriterier, og videre bestemme kriterier for valg av detaljanalyse(r), (trinn III). Her kan ulike aktører ha forskjellige interesser.

For de hendelser som analyseres i mer detalj, kan ulike analyser benyttes. En grundigere vurdering av årsaker (frekvenser) kan gis, og mer detaljerte konsekvensvurderinger, inkl. analyse av avhengigheter kan utføres.

Når analyser er utført må de evalueres, og tiltak/aksjoner må prioriteres. Videre må en fastsette de ulike aktørers ansvarsområde for hvert enkelt tiltak.

2 Oppstart og mål for analysen

Vi ser først på det innledende (og viktige) trinn i sektorovergripende analyser, som bl.a. består i å definere målsetting(er) for analysen, identifisere og samle aktuelle aktører, og spesifisere begrensninger i analysen(e).

2.1 Målsettinger for en risikoanalyse

I enhver risikoanalyseprosess er det viktig at en først angir ***målsettingen for analysen***. Det kan være f.eks.:

- Rangere de "viktigste" hendelser eller de mest sårbare "elementer" for infrastrukturen.
- Identifisere konkrete risikoreduserende tiltak og bidra til evaluering /prioritering av ulike risikoreduserende tiltak.
- Bidra til dimensjonering av beredskapen.

Når det gjelder beskrivelse av infrastrukturer og aktuelle problemstillinger, viser vi til Notat [1].

Klare målsettinger er også viktig når en skal velge ut hendelser for detaljanalyse og gjennomføre disse. Ikke minst detaljanalysen kan ha ulike utforminger, avhengig av *hvem* som er oppdragsgiver, og vi kan for eksempel referere til en:

1. "*Totalanalyse*"; kan utføres for eksempel av kommune, fylke for å få en (relativt grov) oversikt over risiko knyttet til viktige og sårbare infrastruktur-"elementer". En ønsker å si noe overordnet (og rangere/prioritere) med hensyn til den totale risikoen for generelle system, som f.eks. transformatorstasjoner, sentrale jernbanestasjoner (trafikknutepunkt), felles framføringslinjer for strøm/IKT og IKT knutepunkt. Slike analyser står svært sentrale i utkastet til Lov om kommunal beredskapsplikt (juli 2008), [14], som i praksis pålegger kommunene å gjennomføre sektorovergripende risikoanalyser.

2. "*Detaljert totalanalyse*"; er basert på at en legger all infrastruktur "oppå hverandre" for å få det totale risikobilde (oversikt over trusler og sårbarheter) for de konkrete infrastrukturer i en gitt region. Slike analyser kan gjennomføres for beredskapsetater i kommune, fylke osv.
   Analysen kan være GIS[1]-basert; jfr. geomatikksamarbeid i Oslo (og etter hvert i Trondheim), der en skal skaffe seg oversikt over "alt som ligger i bakken".
   En kan bl.a. diskutere rundt ulike spørsmål med hensyn til å ha felles femføringslinjer for ulike typer infrastruktur: hva er fordeler/ulemper, hvilke kompenserende tiltak bør iverksettes for å ivareta sikkerhet, osv. Videre kan en for eksempel ønske å identifisere de aller mest kritiske/sårbare knutepunktene. I dag finnes det ikke utviklet en komplett metode for en slik analyse.

3. "*Leveranseanalyse*"; utført av/for en infrastruktureier (f.eks. vannverk, Telenor) for å analysere dennes leveransesikkerhet mot ulike "viktige" brukere; spesielt identifisere hvilke konsekvenser det vil få for leveransen til disse brukerne, dersom uønskede hendelser inntreffer i "hans" infrastruktur. Herav finner infrastruktureieren hvilken leveringssikkerhet han kan tilby de aktuelle brukerne.

[1] Geografiske informasjonssystemer

4. ”*Brukeranalyse*”; utført av/for en bruker av spesifisert infrastruktur. En konkret ”bruker” (f.eks. JBV eller et større sykehus) får oppgitt leveransesikkerhet til en spesiell infrastrukturleverandør (f.eks. av vann, elektrisk strøm eller IT); se pkt. over. Infrastrukturbrukeren vil så analysere hvilke konsekvenser det får for hans virksomhet når leveranseutfall inntreffer. På basis av en slik analyse tar brukeren stilling til om han har behov for redundans, (f.eks. nødkapasitet eller en ekstra leverandør).

Merk at den detaljanalysen som beskrives i Avsnitt 4 nærmest faller inn under den første av disse fire kategoriene. I Notatene 7-9 vil en imidlertid også finne eksempler på analyser med andre perspektiv. Men det er altså et viktig poeng at det aktuelle perspektivet må klargjøres innledningsvis; dvs., formålet med analysen(e) må presiseres: *Hvorfor utføres de og for hvem*?

Merk også at jo mer detaljert en risikoanalyse blir, jo større er muligheten for at resultatene blir sensitive og ikke bør komme offentligheten til gode. Dels blir det da et spørsmål om virksomhetene må begrense spredning av risikoanalyseresultatene av kommersielle hensyn, dels kan resultatene berøre problemstillinger i forhold til nasjonal sikkerhet og måtte graderes i henhold til sikkerhetsloven.

2.2 Ulike aktører og organisering av arbeidet

Da sektorovergripende risikoanalyser omfatter flere ulike infrastrukturer, vil det også være en rekke aktører involvert. Dette setter ekstra store utfordringer til organisering og gjennomføring av analysen(e). Mye må være på plass:

- Organisering. Det bør opprettes arbeidsgrupper med bred representasjon fra de involverte sektorene. Må spesifisere når aktørene skal trekkes inn og hvilke oppgaver de skal ha. Det kan bl.a. være og fremskaffe informasjon og kontaktpersoner, kvalitetssikre risikovurderinger, ha fokus på sensitivitet av resultater osv.

- Spesifisere hvilke typer informasjonsinnsamling en vil benytte,
  - møter,
  - intervju,
  - spørreskjema,
  - litteratursøk

- Arbeids/analyse-prosessen.
  - hvem benyttes for å skaffe informasjon og evaluere resultater
  - planlegg ulike type møter; type deltakere
  - gi framdriftsplan for avvikling av analyser; konkretiser ca møtetidspunkt og leveransetidspunkt.
  - Plan for interne beslutningsprosesser og av interaksjon mot ”eksterne interessenter” (media), osv.

Generelt er aktør/deltaker-perspektivet viktig. Det må etableres et forum for “aktørene”; noe som innebærer at:

- Dialog/fokus-grupper gis en rolle i DECRIS-metodikken.
- Det etableres en møteplass med kommunikasjon/kunnskapsutveksling mellom alle involverte aktører.

- En må få med dem som mener noe om ulike typer risiko (ulike trusler og konsekvenser); enten på vegne av seg selv eller en gruppe.
- Forumet må gi et "kreativt idégrunnlag"; reis spørsmålet: Hva betyr disse trusler og konsekvenser for meg?
- Ansvarsforhold for aktørene må klarlegges; dette er spesielt relevant når det er sterk interaksjon mellom flere infrastrukturer. Det må fastlegges hvem som har ansvaret for ulike oppgaver ved forskjellige hendelser, og hvem har ansvar for å implementere risikoreduserende tiltak; (gjelder både tiltak for å unngå hendelser og for å redusere konsekvenser av hendelser).
- Formulering av risiko-akseptkriterier og relasjon til kost/nytte-betraktninger må diskuteres. Dette har også sammenheng med overordnede prioriteringer, og bevilgende myndigheter må trekkes inn, men også de aktører som utsettes for risiko må høres.

Et slikt forum for aktører er derfor viktig for flere av elementene i risikoanalysen, og det er viktig å presisere de enkelte aktørenes rolle i beslutningsprosessen.

2.3 Avgrensinger

Ved oppstart av analysen må det angis en klar systemdefinisjon, og videre gis det ulike typer avgrensinger for analysene, bl.a.:

- Hvilke infrastruktur dekkes av analysen; merk at i beskrivelsen av DECRIS dekkes følgende:
  - Vannforsyning
  - Strømforsyning
  - Banebasert transport
  - Vegtransport
  - IKT (primært som støtte for øvrige infrastrukturer).

- Hvem er de relevante "aktører", f.eks.:
  - Kommune, (bl.a. representert ved beredskapsetat)
  - Kommunale etater, f.eks. Vann og Avløp
  - Infrastruktureiere
  - Publikum og viktige brukere.

- Angi evt. avgrensinger med hensyn til type uønskede hendelser; f.eks. utelate viljeshandlinger eller naturkatastrofer som årsak til hendelser.

- Avgrensinger mht type konsekvens, f.eks. kun se på
  - Tap av liv og helse
  - Tilgjengelighet av infrastruktur
  - Økonomiske tap.

- Avklar detaljeringsgraden i analysen(e).

3 Prinsipper for gjennomføring av risikoanalysen

I dette kapittelet ser vi på de overordnede prinsippene for gjennomføring av en DECRIS risikoanalyse.

3.1 En to-trinnsprosess

Som beskrevet i innledningen av notatet, kan DECRIS-analysen totalt beskrives ved fem trinn, (der trinn I ble beskrevet i forrige kapittel). Videre gjennomføres både en *grovanalyse* og *detaljanalyse*.

Metodeprinsipp 1. Analyse på to nivå

Grovanalyseteknikken er ikke egnet til å analysere risikoen knyttet til uønskede hendelser i detalj. I DECRIS-metoden utvikles derfor analysen på to nivå:

1. En *grovanalyse* for å identifisere flest mulig uønskede hendelser og fastsette risikoen for disse ved grove vurderinger.
2. De uønskede hendelser som representerer størst risiko (eller på annen måte finnes interessante) analyseres i *detaljanalysen(e)*. Da kan en studere årsaker, barrierer, avhengigheter mellom ulike infrastrukturer, osv.

Merk at formatet for hvordan vi beskriver risiko vil være forskjellig for grovanalysen og den detaljerte analysen. Dette diskuteres i Avsnitt 3.2.

3.2 Uønskede hendelser, konsekvenser og beskrivelse av risiko

Risiko beskrives ofte som en funksjon av sannsynligheten for, og konsekvensen av uønskede hendelser. En slik definisjon blir ofte for enkel når vi skal synliggjøre dynamikken i en uønsket hendelse eller ulykkeshendelse. En mer fyldig definisjon av risiko gjør bruk av scenario-begrepet, hvor risiko angis ved en opplisting av alle mulige relevante scenarier. Hvert scenario beskrives først med spørsmålet hva som kan gå galt, deretter hvor sannsynlig det er, og hvis det skulle skje hvor galt går det. Et slikt scenario, eller et ulykkesforløp, inkluderer bl.a.

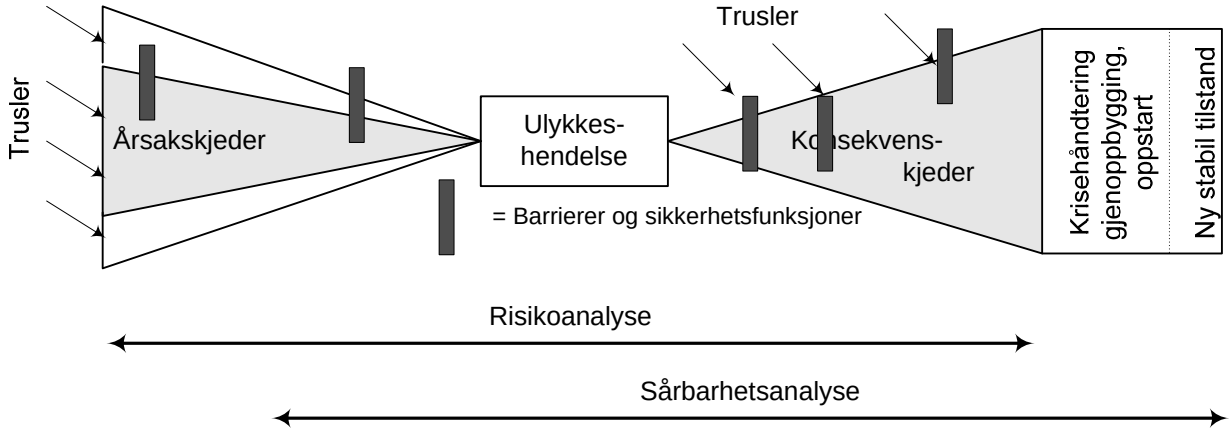
1. Initierende hendelse
2. Uønsket hendelse
3. Konsekvenser

Den *initierende* hendelsen defineres ofte ved første signifikante avvik fra normal driftssituasjon. Hva som er signifikant avgjøres ut fra en vurdering av hva som er hensiktsmessig i analysen. Et typisk eksempel kan være en sprekkdannelse i en hjulaksling på et tog, evt. feil på en kraftledning eller kabel, (jfr. kabelbrannen på Oslo S i nov. 2007, se Notat 10), osv.

En *uønsket hendelse* er en hendelse hvor vi i stor grad har mistet kontroll over situasjonen, og hvor videre forløp i liten eller begrenset grad er kontrollerbart. I togeksemplet vil et akselbrudd være en slik uønsket hendelse. Den uønskede hendelse trenger ikke representere direkte tap ut over begrensede materielle skader, og evt. produksjonstap.

Det er ikke alltid åpenbart hvor i hendelsesforløpet vi vil legge den ”uønskede hendelsen”. Bl.a. kan vi også snakke om en *ulykkeshendelse*, som er en uønskede hendelse som gir signifikant tap i forhold til helse, miljø og sikkerhet, evt. også materielle tap. For togeksemplet vil ”avsporing med drepte og/eller skadde” være en slik ulykke. Vi velger i DECRIS å se på uønskede hendelser som også er ulykkeshendelser, og innfører da ikke noe skille mellom disse begrepene.

Figur 1 viser et såkalt *bow-tie* diagram for risiko- og sårbarhetsanalyser, der en ut fra en uønsket hendelse (ulykkeshendelse) analyserer årsaker (til venstre) og konsekvenser til høyre. En kan legge inn barrierer både for å forhindre at initierende hendelser utvikler seg til ulykkeshendelser, og for å redusere konsekvenser av ulykkeshendelser. Ulike trusler kan både igangsette initierende hendelser og bidra til å svekke barrierer.



Figur 1 *Bow-tie* diagram i Risiko og sårbarhetsanalyse.

Ulike typer (dimensjoner”) av *konsekvenser* kan angis. Ofte fokuseres det på tap av liv og helse. I togeksemplet kan konsekvensen fastsettes til for eksempel 3 drepte, 15 hardt skadde, og 25 lettere skadde. Imidlertid kan også andre *dimensjoner* av risiko vurderes, f.eks. økonomiske/materielle tap og tap av regularitet (leveringsevne).

I ’grovanalysen’ (eng: PHA = Preliminary Hazard Analysis) benyttes den enkleste definisjonen av risiko, dvs. sannsynligheten for, og konsekvensen av de uønskede hendelser. Det vil si at vi ikke synliggjør hele hendelsesforløpet, men velger ut en ”uønsket hendelse” og fastsetter sannsynlighet for denne, og angir én konsekvens for hver av de dimensjoner som vurderes. Når vi skal angi konsekvensen, må vi ta stilling til hvilken av de mulige (slutt)konsekvensene vi skal angi (for hver dimensjon). Her må vi huske at dersom vi velger ”verst tenkelig konsekvens”, vil vi måtte justere sannsynlighet for hendelsen ned fordi kun et fåtall av disse gir verst tenkelig konsekvens.

Det vil også variere hvor langt ut i hendelsesforløpet en vil forfølge konsekvensene. I en grovanalyse nøyer en seg ofte med å se på ”direkte konsekvenser” (på relativt kort sikt), og kanskje uten å forfølge konsekvensene for samfunnet ellers.

Metodeprinsipp 2. Valg av uønsket hendelse, sannsynlighet og konsekvens

- I grovanalysen velges *uønsket hendelse* svært langt ut i hendelsesforløpet, dvs. som en ulykkeshendelse.
- Ved fastsettelse av *konsekvens* av uønsket hendelse velges (for hver dimensjon) en konsekvens som er mer alvorlig en forventet konsekvens, men ikke er helt urealistisk.
- Ved fastsettelse av *sannsynlighet* tar vi høyde for hvor ofte den uønskede hendelsen vil inntreffe *med den sluttkonsekvensen som er valgt*.

Når vi eksplisitt skal beskrive den uønskede hendelsen, kan vi velge hvor detaljert denne skal beskrives. Hendelsen kan f.eks. presiseres ved hjelpeordene:

1. Hva?
2. Hvor?
3. Når?

Det første spørsmålet angår hvor detaljert man skal spesifisere hendelsen, f eks kan man angi en ”Transportulykke” på et veldig overordnet nivå, eller man kan utdype mer f eks ”Jernbaneulykke”, eller bli enda mer detaljert ved å angi ”Togavsporing”. I BAS5-studien (Henriksen m.fl. 2007) ble det laget et klassifikasjonssystem (taksonomi) for å kategorisere uønskede hendelser. Denne studien indikerte at det er behov for å gjennomføre ROS analyser på et nasjonalt nivå. Med utgangspunkt i at dette kan bli realisert på sikt, benytter DECRIS samme kategorisering som BAS5, men i noe forenklet versjon da DECRIS kun dekker noen infrastrukturer. Denne klassifikasjonen ligger også inne i verktøyet InfraRisk (se Notatene 3, 4). I InfraRisk, [3] benyttes begrepet *Main Event,* og i DECRIS bruker vi altså dette synonymt med *uønsket hendelse*.

Metodeprinsipp 3. Klassifikasjon av uønskede hendelser

Vi legger forslaget fra BAS5-studien til grunn for en klassifikasjon av uønskede hendelser, (se [4]). Denne klassifikasjonen har fire nivå, og en kan velge hvor langt ned i hierarkiet en vil gå for å analysere enkelthendelser.

I en grovanalyse vil man ofte ikke bli veldig eksplisitt på spørsmålene ”hvor” og ”når”, og dette blir ikke angitt eksplisitt, med mindre dette vil lette vurderingene. I de detaljerte analysene vil sted og tidspunkt bli håndtert eksplisitt for de fleste scenariene.

3.3 Hendelser og tap av samfunnskritiske funksjoner

I grovanalysen er startpunktet de *uønskede hendelser,* og en kan referere til to typer:

1. En uønsket hendelse som *resulterer* i tap av en samfunnskritisk funksjon, (i DECRIS betyr det tap av en kritisk infrastruktur)[2].
2. Den uønskede hendelsen er ”svikt i en samfunnskritiske funksjon”.

[2] *Kritisk infrastruktur*: De anlegg og systemer som er helt nødvendige for å opprettholde samfunnets *kritiske funksjoner* som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse (NOU 2006:6). Elektrisk kraft, vann og avløp, transport, elektronisk kommunikasjon er definert som *kritisk infrastruktur*, mens bank og finans, matforsyning, helse- og sosial, politi mm er definert som *kritiske samfunnsfunksjoner*.

Eksempel på den første kan være ulike typer ekstremvær, en brann, eller en sabotasjehandling, som alle vil kunne true en kritisk infrastruktur, (og dermed evt. samfunnskritiske funksjoner, SKF). Et eksempel på den andre typen hendelser vil være teknisk svikt i renseanlegg for vannforsyning. I klassifikasjonen som er utviklet i BAS5-prosjektet er det definert hendelser av begge disse typene.

I InfraRisk, [3] kan man som en del av grovanalysen synliggjøre hvordan de samfunnskritiske funksjonene (SKF) inngår i hendelsesforløpet. Flere SKF kan kobles opp mot en uønsket hendelse. For å angi koblingen angis:

1. Om en SKF er involvert før, etter, eller både før og etter den uønskede hendelsen
2. Hvor sterk kobling til hendelsesforløpet en SKF har

Metodeprinsipp 4. Klassifikasjon av samfunnskritiske funksjoner (SKF)

Vi legger forslaget fra BAS5-studien til grunn for en klassifikasjon av SKF, se [3]. Denne klassifikasjonen har fire nivå, og en kan velge hvor langt ned i hierarkiet man vil gå for å spesifisere den samfunnskritiske funksjonen. Flere SKF kan angis for hver uønsket hendelse.

3.4 Fastsettelse av konsekvensdimensjoner

De aller fleste ROS-analyser vurderer risiko for helse miljø og sikkerhet. Andre dimensjoner som materielle skader, økonomiske tap, tap av viktige samfunnsfunksjoner osv tas også med i varierende grad. Basert på BAS5-studien inkluderes følgende konsekvensdimensjoner i en detaljanalyse:

1. Liv og helse
2. Miljø
3. Økonomisk tap, inklusive materielle skader
4. Omdømme / befolkningens generelle trygghetsfølelse
5. Styrbarhet[3]
6. Tilgjengelighet av kritisk infrastruktur (evt. SKF)

I DECRIS grovanalyse fokuserer en gjerne på dimensjonene *liv og helse* (spesielt hendelser med potensial for storulykker), og *utilgjengelighet av kritisk infrastruktur.*

3.5 Utvelgelse av hendelser for detaljanalyse(r)

Uønskede hendelser med høy risiko er kandidater for detaljerte analyser. Ved utvelgelse av hendelser for detaljanalyse (jfr. trinn III i Innledning) kan som et eksempel følgende kriterier legges til grunn; en inkluder:

1. Hendelser i risikokategoriene ”høy risiko” og ”veldig høy risiko”
2. Hendelser med konsekvenskategori ”kritisk” og ”katastrofal”, (dvs. storulykkespotensial)
3. Hendelser hvor det er sterke avhengigheter eller samspilleffekter mellom to eller flere kritiske infrastrukturer

[3] Rednings og krisehåndtering, nasjonal handlefrihet, myndighetsutøvelse, territorial kontroll

4. Hendelser med spesielle årsaker, (f.eks. teknisk/menneskelige feil; destruktive handlinger; osv.)
5. Hendelser hvor redningsarbeid vurderes svært vanskelig, eller hvor svært store ressurser er påkrevd.

4 Detaljanalyser

I oversikten over DECRIS-metodikken (se Innledning) er ”Detaljanalyse av utvalgte hendelser” angitt som et trinn IV. Detaljanalysene tar utgangspunkt i utvalgte hendelser fra grovanalysen. For disse gjennomføres ulike analyser (f.eks. årsaksanalyser, konsekvensanalyse). I detaljanalyse vil dessuten risikoen vurderes for opptil seks risikodimensjoner, (Avsnitt 3.5).

Vi gir i dette kapitlet noen overordnede kommentarer til slike detaljanalyser, og viser ellers til Notat 7, [6] og Notat 10, [9] som gir eksempler.

4.1 Oppstart og gangen i en detaljanalyse

Som beskrevet i Avsnitt 2, må også en detaljanalyse starte med å presisere formålet med analysen, angi detaljeringsgrad/omfang og aktuelle aktører som skal trekkes inn.

Gangen i selve detaljanalysen er skissert i Figur 2; (alle trinn trenger ikke inngå i enhver analyse).

Scenariobeskrivelse
Det forutsettes at forutgående grovanalyse har identifisert uønskede hendelser. Disse vil normalt omfatte utfall av eller hendelser i en kritisk infrastruktur, og er relatert til kritiske (sårbare) enheter/delsystem i infrastrukturen. Det kan gjelde f.eks.

- Inføringstransformatorer
- Vannkilde
- Drivstofflager
- Fellesføringer for strøm/IKT, evt. vann.

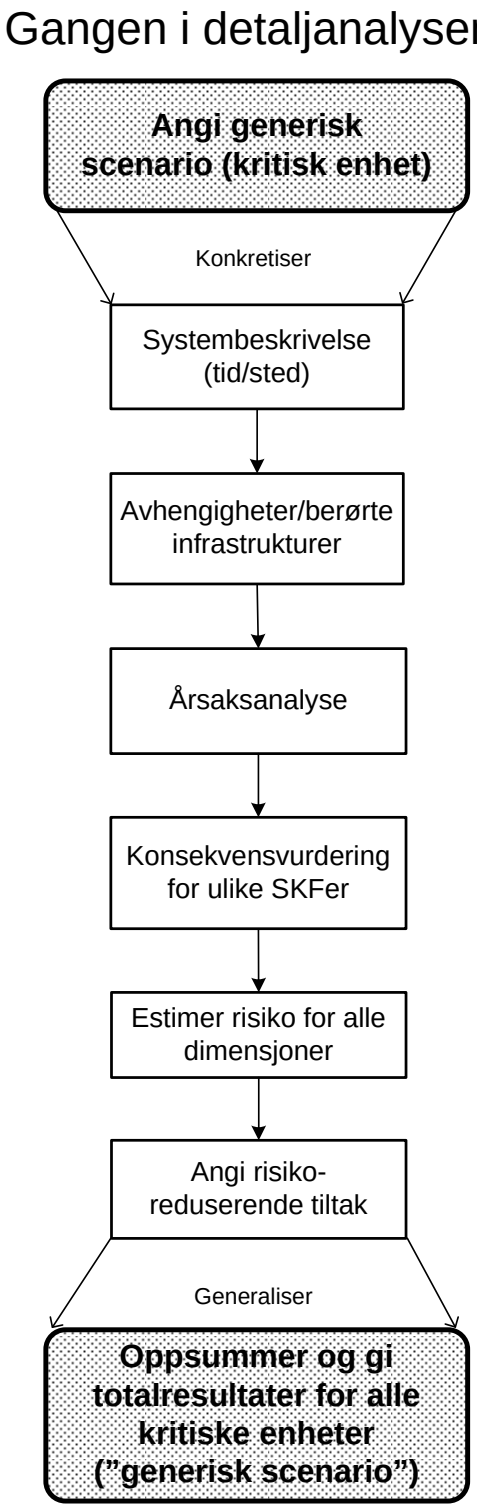
Disse kan (evt. i generalisert form) gi opphav til å definere generiske scenarier (se topp av Figur 2). Med utgangspunkt i eksemplet ”Fellesføringer for strøm/IKT” kunne det *generiske scenariet* f.eks. være:

”Ødeleggelse i felles framføringslinje for kraft, IKT-samband, evt. vann/avløp i sentralt byområde.” Dette kan spesifiseres til å gjelde fysiske fremføringslinjer, plassert enten under bakkenivå (kulvert eller lignende) eller på bro. Alle mulige årsaker til hendelsen, og alle mulige konsekvenser kan vurderes. Det er total risiko knyttet til et slikt generisk scenario en ønsker å si noe om ved hjelp av detaljanalyser. Svært ofte vil det generiske scenariet være knyttet til (skade på) en *kritisk enhet*, (for eksempel kulvert eller transformator). Men hvis f.eks. hendelsen er en naturkatastrofe, vil den som regel ikke knyttes til ett system.

Ut fra et slikt generisk scenario, spesifiseres så et konkret system, knyttet til en spesifikk lokasjon, jfr. boks 2 i Figur 2, og for dette konkrete system utføres ulike detaljanalyser. Ut fra det generiske senariet ”fellesføringer”, kunne man spesifisere en spesiell kulvert, (f.eks. plassert i Oslo sentrum). Deretter gis en grunnleggende beskrivelse av det konkrete scenariet, inkl. relevante deler av infrastrukturene.

Systembeskrivelse og avhengigheter til andre infrastrukturer
En må både skaffe seg oversikt over de infrastrukturer som blir direkte berørt av den aktuelle uønskede hendelse, og videre skaffe seg en (evt. grov) oversikt av hvilke andre infrastrukturer som kan bli berørt (pga av avhengigheter mellom infrastrukturer, se [9]). En vil m.a.o. se på

1. Kritisk infrastruktur (”primær SKF) som blir direkte berørt. I eksempel med kabelkulvert er dette strømforsyning og signalkabler (IKT) i selve kulverten. (I et annet eksempel kan det være en transformator, og da vil en også inkludere underliggende strømforsyninger som berøres).
2. Øvrige SKF (”sekundær SKF”) som kan berøres som følge av den uønskede hendelsen; dvs. de funksjoner som er avhengig av primære SKF. (e.g. strøm/IKT), og som faller ut som en direkte følge av at ”primær SKF” skades).



Figur 2 Gangen i detaljanalysen (”totalanalyse”)

Detaljanalyser og konklusjoner
På det konkrete scenariet vil en så utføre detaljanalyser; se diskusjon i neste avsnitt. Resultatene fra disse analysene blir så vurdert, og dette blir så generalisert slik at en kan komme med utsagn om risikoen knyttet til det *generiske* scenariet, se "generalisering", nederst i Figur 2. Hvis vi igjen bruker eksempel med fellesføring, kan analyser av konkret kulvert benyttes til å gi vurderinger av risiko knyttet til "fellesføringer" generelt (innen for eksempel Oslo). En slik generalisering må basere seg på opplysninger om totalt antall av den aktuelle enheten (e.g. kulverter) innenfor det aktuelle området (e.g. Oslo), og om den analyserte enhet har en "typisk" risiko, eller om den vurderes å ha høyere/lavere risiko enn tilsvarende "typiske" enheter innen dette området.

4.2 Ulike detaljanalyser

Valg av detaljanalyse(r) vil avhenge av formål med analysen, og hvem den utføres for, (jfr. Avsnitt 2). Disse er oftest kvantitative analyser der det lages detaljerte probabilistiske modeller bl.a. for hendelsesforløpet, og dermed fås bedre innsikt og estimat for risikoen. Noen analyser er:

- Årsaksanalyser
- Barriereanalyse
- Avhengighetsanalyse
- Konsekvensanalyse
- Analyse av krise og redningsledelse

Enkelte eksempler finnes i Notatene 7-10, dvs. refs. [6-9].

4.2.1 Årsaker til uønsket hendelse og barrierer

Når det er behov for å identifisere de ulike (mulige) årsaker til en uønsket hendelse benyttes ofte feiltreanalyse (FTA = Fault Tree Analysis), se [8] for et eksempel. Ved en slik analyse oppnås en strukturert nedbryting av årsaker, og det også mulighet til å beregne frekvens eller sannsynlighet for den uønskede hendelsen.

Som innledende øvelse vil en gå igjennom en generell trussel/årsaks-liste, som vil omfatte bl.a. :

- Brann
- Sabotasje
- Oversvømmelse (mer generelt naturhendelse)
- Menneskelig feil (trafikkulykke; tap av kontroll av teknisk utstyr)
- Teknisk svikt

En detaljert risikoanalyse vil også synliggjøre *barrierer* og sikkerhetsfunksjoner som påvirker hendelsesforløpet, jfr. Figur 1. I togeksemplet nevnt i Avsnitt 3.2 over vil ultralydinspeksjon av hjulakslinger være en barriere som avdekker initierende sprekker før de utvikler seg til brudd, mens ledeskinner er barrierer som begrenser skadene etter et eventuelt akselbrudd. En vil identifisere eksisterende barrierer og status for disse; generelle eksempel er:

- Fysisk beskyttelse/separasjon av system
- Adgangskontroll
- Redundans/reserveenhet

Barrierer mot at uønskede hendelser skal inntreffe bør kategoriseres etter hvilke årsaker de skal forhindre.

4.2.2 Analyse av konsekvenser og avhengigheter

Ved analyse av konsekvensene for berørte SKFer, benyttes ofte hendelsestreanalyse (ETA = Event Tree Analysis), se [8] for et eksempel. Ved en slik analyse kan en beregne *sannsynlighetsfordelingen* over de ulike mulige konsekvenser, (og ikke bare én typisk konsekvens). Hvis vi f.eks. skal analysere en avsporingsulykke, kan vi ikke angi konsekvensen nøyaktig (f.eks. målt i antall omkomne), men ved hjelp av en ETA kan anslå *sannsynlighetsfordelingen* over antall omkomne i angitt ulykkestype.

I tillegg til drepte og skadde vil en i detaljanalysen normalt også vurdere andre dimensjoner, f eks miljøkonsekvenser (hvis det f.eks. er avsporing av et tog med farlig gods), materielle skader, omdømmetap, osv.

En viktig oppgave i detaljanalysen er normalt å gi en mer omfattende vurdering av konsekvenser for tilgjengeligheten av ulike infrastrukturer. En vil ta utgangspunkt i hvilke brukere/kundegrupper som blir berørt av utfall av tjeneste (f.eks. strøm, IKT, transport). I den sammenheng identifiseres

- Antall berørte abonnenter (for ulike kraftforsynings- og IKT- tjenester); tilsvarende for jernbane osv.
- *Varigheter* av utfall / redusert ytelse (for ulike årsaker til hendelsen)
- Viktige kritiske/sårbare kundegrupper

Et viktig spørsmål er også om det kan være langsiktige konsekvenser for aktuelle aktører/interessenter. Dette kan også analyseres ved hjelp av hendelsestre, og dreier seg primært om å identifisere konsekvenser som viser seg etter lang tid, f.eks. omdømmetap; se også ytterste høyre del av Figur 1.

Infrastruktur dreier seg i stor grad om nettverk. Derfor kan en form for *nettverksanalyse* være meget viktig i en detaljert analyse av konsekvenser av uønskede hendelser; se [6]. Dette - og spesielt kopling mellom nettverk for ulike infrastrukturer - er imidlertid et område en ikke er kommet langt med i DECRIS.

Analyse av følgekonsekvenser for øvrige infrastrukturer er imidlertid et sentralt element av DECRIS-metoden. Dette er nært knyttet til analyse av *avhengigheter*, og analyser tilsvarende hendelsetre benyttes, se eksempel i [9]. Avhengigheter kan også medføre mulig forsterkende konsekvenser (samspillseffekter) ved at flere ulike SKFer berøres; (det er ikke nødvendigvis bare additivt effekt av ulike konsekvenser).

Notat 10 ([9]) beskriver analyse av ulike typer *avhengigheter*, som skyldes

- Funksjonelle koplinger; (For at System B skal virke forutsetter det at System A virker)
- Fysisk nærhet
- Felles komponenter
- Manglende skiller/barrierer mellom system/enheter: Hvis én barriere brytes, vil mange enheter ”blottlegges” (jfr. ”villede handlinger”).

4.2.3 Krise og redningsledelse

Beredskapstiltak/krisehåndtering kan også være tema for detaljanalyse. Spesielt kan det være avhengigheter i krisehåndtering for ulike SKFer. Analyse av krise og redningsledelse vil ta utgangspunkt utvalgte uønskede hendelser (”dimensjonerende hendelser”). I verktøyet InfraRisk kan en som utgangspunkt legge inn informasjon om slike dimensjonerende ulykkeshendelser. Videre er det viktig å studere mer eksplisitt samhandling i krisesituasjonen, og kommunikasjon

både internt og ut til media/berørte parter. Hendelsesforløpet etter den uønskede hendelsen har inntruffet kan beskrives ved hjelp av et STEP diagram, [13] . Studien for Stavanger-regionen har utviklet en metode for å analysere beredskapssituasjonen. Ellers er dette et område som ikke er ferdig utviklet, og der en ikke har fått utrettet mye i DECRIS.

5 Risikoreduserende tiltak og oppsummering

Avslutning på detaljanalysen innebærer en generalisering av de analyser som er utført av konkrete *kritiske enheter*, som ender opp med å gi vurderinger om risikoen knyttet til denne type system i det aktuelle område (for eksempel Oslo). En slik generalisering må basere seg på opplysninger om hvor mange slike enheter som finnes i det aktuelle området, og om den analyserte enheten vurderes å ha høyere, evt. lavere risiko enn en tilsvarende "typisk" enhet.

Videre omfatter det avsluttende trinn i en komplett analyse en oppsummering og vurdering av risikoreduserende tiltak (jfr. "Trinn V", se Innledning). Både på årsakssiden og konsekvenssiden må en vurdere effekt for risiko av ulike tiltak og tiltakspakker som er identifisert i løpet av analysen.
Det er bl.a. snakk om å innføre nye barrierer og forsterke eksisterende, og bedring av beredskap/krisehåndtering.

Meget sentralt er her å ha diskusjoner i dialog/fokusgruppen med de ulike aktører. Ansvar for oppfølging av tiltak må klargjøres; jfr. generell oversikt over aktøransvar gitt i Notat 9 ([8]).

Mulig videre arbeid er å lage ett generelt hendelsestre per infrastruktur vi ser på; (f.eks. ett ifm. kraftbortfall, ett ifm. bortfall av vann osv) Disse kan så være grunnlag for noe modifikasjon når vi skal analysere spesifikke hendelser innenfor infrastrukturene. Det kan bli svært arbeidskrevende men antas å være fruktbar angrepsmåte.

Referanser

[1] Notat 1, DECRIS – Promstillinger rundt tversektorielle risikoanalyser. Kritisk infrastruktur

[2] Notat 2, Sammendrag Ros analyser

[3] Notat 3, Method for identification and ranking of societal critical functions (beskrivelse av verktøyet InfraRisk).

[4] Notat 4, Beskrivelse av grovanalyse-metodikk

[5] Notat 5, Oppsummering av grovanalyse, Oslo

[6] Notat 7, Kritiske hendelser i strømforsyning

[7] Notat 8, Bortfall av vannforsyning

[8] Notat 9, Leveringssikkerhet

[9] Notat 10, Avhengighetsanalyse

[10] Henriksen, S., K. Sørli og L. Bogen (2007) Metode for identifisering og rangering av kritiske Samfunnsfunksjoner. FFI-rapport 2007/00874. ISBN 978-82-464-1192-7. (BAS 5 – metoden).

[11] NOU 2006:6. Når sikkerheten er viktigst.

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

[13] Hendrick, K., Benner, L. (1987), Investigating Accidents with STEP Marcel Dekker, Inc., New York.

[14] Lov om kommunal beredskapsplikt (juli 2008),