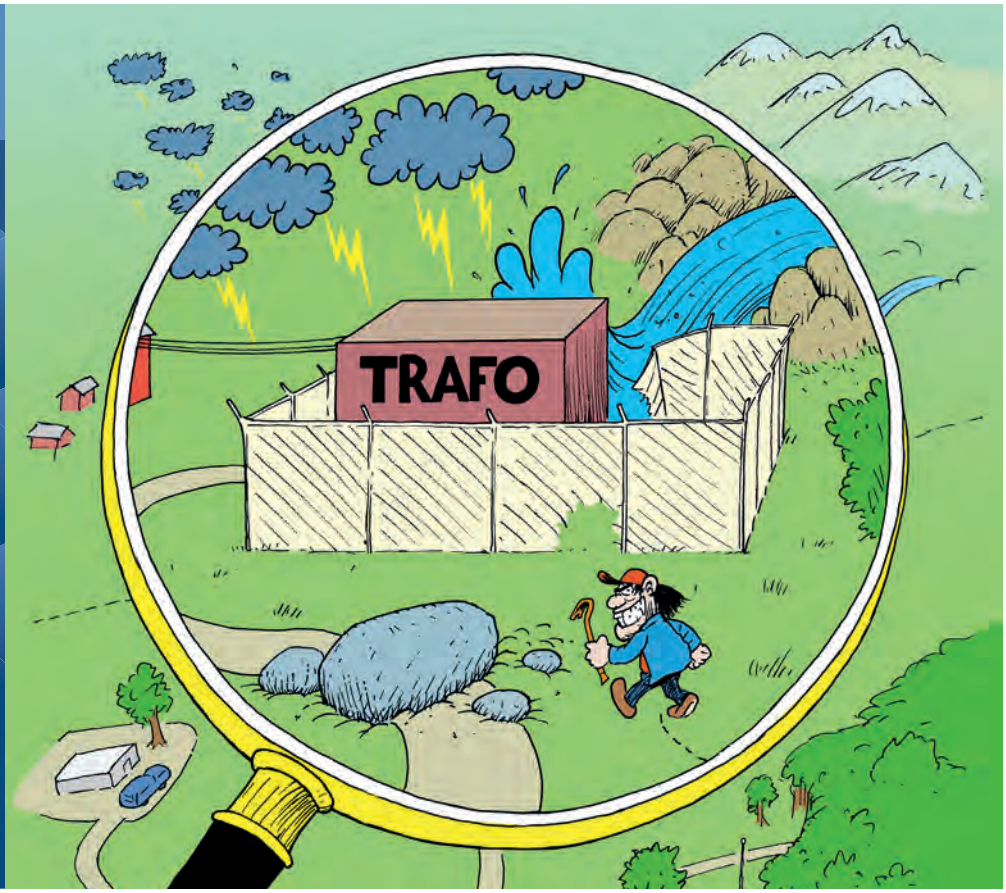
Eksempelsamling
Risiko- og sårbarhetsanalyser for kraftforsyningen

18
2012

RAPPORT



Eksempelsamling

Risiko- og sårbarhetsanalyser for kraftforsyningen

Norges vassdrags- og energidirektorat

2012

ISBN: 978-82-410-0802-3

ISSN: 1501-2832

Eksempelsamling - Risiko- og sårbarhetsanalyser for kraftforsyningen

Utgitt av:	Norges vassdrags- og energidirektorat
Redaktør:	Roger Steen, NVE
Forfattere:	Proactima.no og Roger Steen (NVE)

Trykk:	NVEs hustrykkeri
Opplag:	300
Forsidefoto:	Illustrasjon av Ola Hegdal, NVE alle rettigheter
ISBN	978-82-410-0802-3
ISSN	1501-2832

Sammendrag: Eksempelsamlingen er utviklet som et bidrag til å utarbeide ROS-analyser i tråd med de krav som beredskapsforskriften setter. Det gis eksempler til både prosess og case som forhåpentlig vil være til inspirasjon.

Emneord: Risikoanalyser, sårbarhetsanalyser, forebygging, beredskap, Forskrift om beredskap i kraftforsyningen (beredskapsforskriften)

Norges vassdrags- og energidirektorat (NVE)
Middelthunsgate 29
Postboks 5091 Majorstua
0301 OSLO

Telefon: 09575
Internett: www.nve.no

Juni 2012

FORORD

Denne eksempelsamlingen må ses i sammenheng med ”Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen” NVE publikasjon 2:2010.

Målgruppen for denne eksempelsamlingen er virksomheter som er pliktig til å følge krav om utarbeidelse av ROS-analyser slik det er nedfelt i Forskrift om beredskap i kraftforsyningen (beredskapsforskriften).

NVE håper at eksempelsamlingen vil hjelpe den enkelte virksomhet i arbeidet med å kartlegge egen risiko og sårbarhet.

Hoveddelen av denne eksempelsamlingen er utarbeidet av Proactima AS i samarbeid med og under ledelse av NVE. En rekke virksomheter og ressurspersoner har i tillegg bidratt underveis i dette arbeidet med erfaringer og råd.

Arthur Gjengstø
Seksjonssjef beredskapsseksjonen
Energiavdelingen

Roger Steen
Teamleder beredskap og øvelser
Beredskapsseksjonen, Energiavdelingen

Oslo, Juni 2012

Innholdsfortegnelse

FORORD **3**

1 Introduksjon **5**

1.1 Avgrensninger 5

2 Hvordan strukturere ROS-arbeidet i bedriften **6**

3 Prosesslederen **8**

4 Eksempel på ROS-analyser – fra nivå 1 til nivå 3 ..... **9**

4.1 Eksempel på ROS-analyse nivå 1 – prioritering av anlegg 9

4.2 Eksempel på ROS-analyse nivå 2 – analyse av spesifikk transformatorstasjon 17

4.3 Eksempel på ROS-analyse nivå 3 – analyse av uønsket hendelse i transformatorstasjon 25

4.3.1 Årsaksanalyse – manglende utkobling av vern 26

4.3.2 Konsekvensanalyse – eksplosjon i transformator 27

5 Eksempel på ROS-analyser av felles systemer **28**

5.1 Eksempel på ROS-analyse av transportberedskap (nivå 1) 28

5.1.1 ROS-analyser og transportberedskap 28

5.1.2 ROS-analyse av transportberedskap 30

5.2 Eksempel på ROS-analyse av fysisk sikring (nivå 1) 34

5.2.1 Krav til sikkerhetsnivå og sikkerhetstiltak 34

5.2.2 ROS-analyse av fysisk sikring 34

6 Eksempel på fremstilling og håndtering av risiko **39**

7 Referanser **41**

Vedlegg 1 – Sjekklister **42**

Vedlegg 2 – Prosessleder tips **43**

1 Introduksjon

Formålet med denne eksempelsamlingen er å hjelpe bedriftene med å komme i gang og strukturere arbeidet med risiko- og sårbarhetsanalyser (ROS-analyser) i egen organisasjon. Eksempelsamlingen skal gi utdypende råd til de som skal lede ROS-arbeidet i den enkelte virksomhet, og er et supplement til veiledningen i risiko- og sårbarhetsanalyser for kraftforsyningen (NVE og Proactima AS 2010). Både eksempelsamlingen og veiledning er utarbeidet med bakgrunn i krav nedfelt i Forskrift om beredskap i kraftforsyningen (beredskapsforskriften). Eksempelsamlingen er primært rettet mot bruk av risiko- og sårbarhetsanalysemetodikk som et verktøy for å etterleve kravene i beredskapsforskriften.

1.1 Avgrensninger

Eksempelsamlingen gir ikke en detaljert beskrivelse av alle mulige metoder som kan bli benyttet i forbindelse med ROS-analyser i kraftforsyningen. Eksempelsamlingen presenterer bruddstykker av tenkte analyser, og ikke hele eksempler. Det er tatt utgangspunkt i eksemplene som er benyttet i ROS-veiledningen, og en del av disse eksemplene er blitt utdypet i denne eksempelsamlingen. I tillegg gis det noen eksempler på hvordan ROS-analyser på ulike nivåer i virksomheten henger sammen og bør brukes som underlag for ROS-analyser på andre nivåer.
Hvert eksempel inneholder de tre hoveddelene 1) Planlegging, 2) Risiko- og sårbarhetsvurdering og 3) Risikohåndtering. Innenfor hvert eksempel er det fokusert på hva som er spesielt.

2 Struktur på ROS-arbeidet i virksomheten

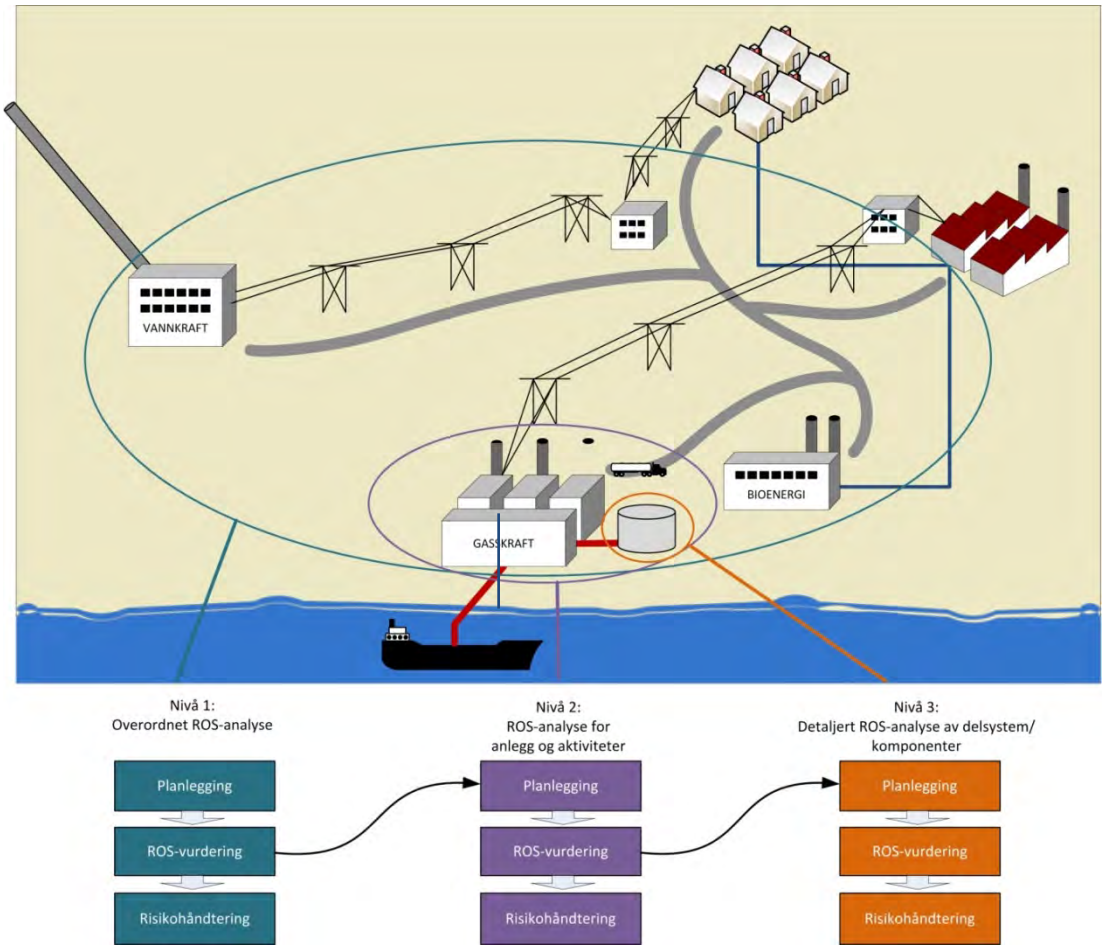
Beredskapsforskriften legger tydelige føringer på at norsk kraftforsyning skal kartlegge, forebygge og håndtere ekstraordinære hendelser. Kravet til ROS-analyser innbefatter at det enkelte selskap skal identifisere risiko og sårbarhet ved ekstraordinære hendelser knyttet til teknisk svikt, naturgitt skade og bevisst skadeverk som truer forsyningssikkerheten. Videre skal analysen også favne de tiltak forskriften krever skal kunne iverksettes av ulike beredskapstiltak.

Beredskapsforskriften stiller krav om å kartlegge virksomhetens risikopotensial. Erfaringsmessig vil arbeidet med etablering av et helhetlig risikobilde for virksomheten gjøres mest ressurseffektivt ved å tilpasse detaljeringsnivået i ROS-analysen ut fra analysens tiltenkte formål. Følgende inndeling kan anvendes:

Figur 1 nedenfor viser de ulike analystilnærmingene

- Nivå 1: Overordnet ROS-analyse.
- Nivå 2: ROS-analyse av anlegg og aktiviteter.
- Nivå 3: Detaljert ROS-analyse av delsystem eller komponenter.

For en nærmere beskrivelse av de ulike nivåene av ROS-analyser vises det til "Veileder i ROS-analyser i kraftforsyningen" (NVE og Proactima 2010).



Figur 1 Ulike nivåer av ROS-analyser.

Hva hvis?

Tenk igjennom hva som kunne vært konsekvensene for ditt selskap dersom:

- ✓ …det oppstår brann i / ved driftssentralen slik at den må evakueres.
- ✓ ...det bryter ut en pandemisk influensa slik at ca. 40 % av de ansatte til enhver tid er borte fra jobb i lengre perioder.
- ✓ …underleverandøren av tjenester ifm. transportberedskap går konkurs.

3 Prosesslederen

Det er viktig at den enkelte virksomhet har kompetanse til å lede og delta i ROS-analyseprosesser. I denne sammenheng har prosessleder en viktig rolle da det er hun / han som har ansvaret for å planlegge og gjennomføre ROS-analysen.

I forbindelse med planleggingen må formål og omfang av analysen defineres og analysen må forankres hos ledelsen. Hva skal resultatene fra analysen brukes til? Hva er det som skal analyseres? Hvilke beslutninger skal fattes er noen relevante spørsmål som bør trekkes frem?

Det er avgjørende å forstå hva som skal analyseres for å ivareta krav til kartlegging av risiko- og sårbarhet stilt gjennom relevante lover, forskrifter og konsesjonsvilkår.
Det er viktig å være klar over at man blir ikke en god prosessleder ”over natten”, men at dette krever øvelse og trening i rollen. En god forutsetning er å ha en god forståelse av det som skal analyseres og regelverket som regulerer kraftforsyningen. Videre god kunnskap om ROS som metode, og evnen til å hente inn og bruke god fagkunnskap

I vedlegg 2 gis det tips til hva som er viktig å huske på for en prosessleder i forbindelse med planlegging og gjennomføring av en ROS-analyse. Det vises også til ”Veileder i ROS-analyser i kraftforsyningen” (NVE og Proactima 2010).

4 Eksempel på ROS-analyser – fra nivå 1 til nivå 3

Nedenfor gis det noen eksempler på hvordan ROS-analyser på de ulike nivåene kan gjennomføres og hvordan resultatene fra de ulike analysene påvirker hverandre, samtidig som sammenhengen mellom de ulike analysene illustreres. Hvert eksempel inneholder de tre hoveddelene 1) Planlegging, 2) Risiko- og sårbarhetsvurdering og 3) Risikohåndtering, følger stegene som er foreslått i veilederen for ROS-analyser (NVE og Proactima 2010). Innenfor hvert eksempel er det fokusert på hva som er spesielt.

4.1 Eksempel på ROS-analyse nivå 1 – prioritering av anlegg

Et kraftforsyningsselskap har ulike anlegg med forskjellig strategisk betydning og sårbarhet i sin virksomhet (kraftverk, transformatorstasjoner, ledningsnett osv). En ROS-analyse på nivå 1 er en overordnet ROS-analyse som dekker alle de viktigste anleggene/linjene i selskapets virksomhet.

Egne ROS-analyser på nivå 1 skal også gjennomføres for fellessystem som transportberedskap, sikring av anlegg, driftskontrollsystemer og kritiske arbeidsprosesser. Eksempler på analyser av fellessystem finnes i kap.5. **Planlegging**

Formål og omfang

Før vi begynner en ROS-analyse er det viktig å avklare hva analysen skal brukes til. Formålet med en ROS-analyse på nivå 1 vil være å identifisere hendelser som kan true forsyningssikkerheten i selskapets virksomhetsområde, og analysen skal gi en overordnet prioritering av anlegg/linjer for videre analyser og tiltak. Analysen må omhandle hendelser som har vesentlige konsekvenser for forsyningssikkerheten, men kan også inkludere konsekvenser ift. dimensjoner som økonomisk tap og tap av tillit/omdømme etter hva virksomheten har av særlige interesser. En del av formålet kan også være å gi systemkompetanse til beslutningstakere i virksomheten.

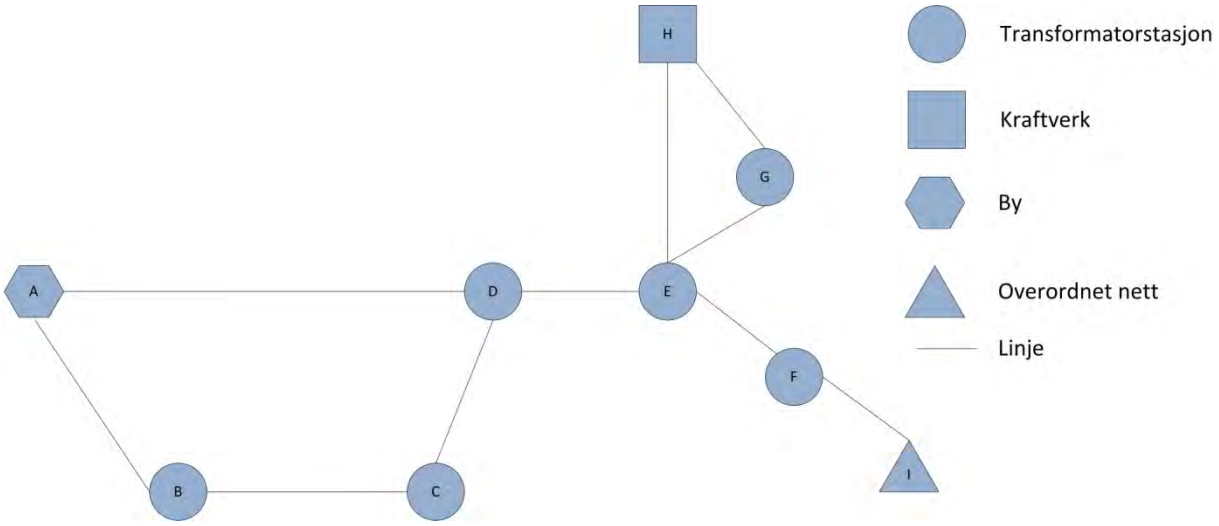
Valg av konsekvens- og sannsynlighetsdimensjon

> **Skal alt analyseres?**
> Ifm. planleggingen av ROS-analysen er det viktig å avklare hvilke konsekvensdimensjoner en skal vurdere risiko i forhold til. I en overordnet ROS-analyse der formålet er å etablere en prioritert oversikt over anleggene i virksomheten (nivå 1), kan det være tilstrekkelig å vurdere risiko og sårbarhet ift. forsyningssikkerhet iht. krav i beredskapsforskriften. I nivå 2 analyser av de enkelte anlegg er det da relevant å adressere også andre konsekvensdimensjoner.

I dette eksempelet velger vi å bruke de samme kategoriinndelingene for forsyningssikkerhet og sannsynlighet / frekvens som i veilederen (NVE og Proactima 2010). Det er imidlertid viktig at dette tilpasses den enkelte virksomhet.

Informasjonsinnhenting

Det er viktig å skaffe informasjon om og danne seg en oversikt over systemet / nettverket som skal analyseres. Her er det også viktig å ta med grensesnittet mot overordnet nett og distribusjonsnett. Figuren under viser et eksempel på et enkelt overføringsnettverk som kan være gjenstand for en slik ROS-analyse. Dette nettverket brukes også i de følgende eksemplene.



Figur 2 Eksempel på et enkelt overføringsnettverk.

Denne typen modell kan være nyttig underlag for ROS-analysen. Annen nyttig informasjonsunderlag til en slik analyse kan være allerede gjennomførte nettverks-, system- og pålitelighetsanalyser, i kombinasjon med ekspertvurderinger. Kraftsystemutredninger kan gi informasjon om allerede identifiserte sårbarheter i eksisterende nett. Felles for mange av de tilgjengelige analysene er at de håndterer ”normale” variasjoner og ikke uten videre ekstraordinære hendelser.

Annen informasjon som er viktig å innhente er informasjon om klimatiske forhold, og vurderinger i forhold til hvordan dette kan påvirke lokale forhold i fremtiden. Værpåkjenninger er en betydelig årsak til de feil og avbrudd som skjer i kraftforsyningen. Uten fysiske tilpasninger vil energiselskapene trolig få økte utfordringer i takt med endringer i klimaet. Disse klimatiske forandringene vil kunne gi endrede fysiske belastninger og kan påvirke grunnforholdene, skredområder, flomsoner, havnivåstigning etc.

Analysegruppe (ressurser)

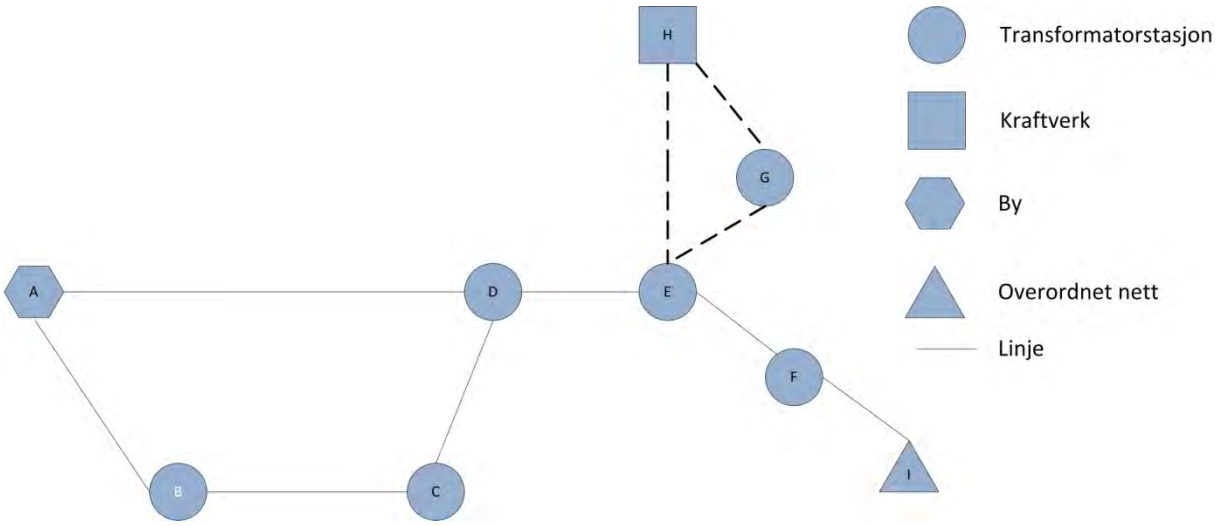
Det er viktig å sikre at personell med god nettverksforståelse og beredskapskompetanse deltar i gjennomføringen av en slik analyse. Dette kan for eksempel være personer som til daglig jobber i driftssentralen og personell innen nettutvikling. Eksperter på klima og grunnforhold kan være aktuelle å trekke inn. Likeså IKT-sikkerhet og andre profesjonsområder der det er relevant.

Klargjøring av analyseskjema og sjekklister

Det besluttes å gjennomføre en strukturert grovanalyse. Før analysemøtet må analyseskjema og sjekklister gjøres klar og testes ut. Analyseskjemaet og den generelle sjekklisten i ”Veiledning i ROS-analyser for kraftforsyningen” (NVE og Proactima 2010) kan her benyttes som et utgangspunkt, men sjekklisten bør alltid oppdateres etter hvert som ny kunnskap erverves. Systemet som er gjenstand for analyse deles inn i delsystemer (som for eksempel sentralnett, regionalnett, overføringsnett, transformatorstasjoner (300 kV, 132 kV og 50 kV) og produksjonsanlegg). Et stort kart som viser geografisk plassering av anleggene og topografien vil være nyttig å bruke i analysemøtet.

Risiko- og sårbarhetsvurdering
Risiko- og sårbarhetsvurderingen gjennomføres i et analysemøte. Nettverks-, system- og pålitelighetsanalysene gir underlag til hvilke anlegg / linjer som må feile, enten individuelt eller i kombinasjon, for å resultere i avbrudd i strømforsyningen. Det må også tas hensyn til fellesfeil og kaskadefeil i kraftsystemet. I vurderingene må det også ta hensyn til fleksibilitet, avhengighet og sårbarhet i nettverket Vurdering av sannsynlighet gjøres på et overordnet nivå basert på informasjon om nettverket, tilgjengelig avbruddsstatistikk og sårbarhetsvurderinger av nettverket. Momenter som er viktige å ta med i en slik overordnet ROS-analyse er bl.a. type, kapasitet og utnyttelsesgrad (normal og maks last) på anlegg og linjer, omfang av viktige forsyningsobjekter, hvor mange sluttbrukere som vil bli berørt av et eventuelt avbrudd i strømforsyning, tilgjengelighet/robusthet til de ulike anleggene i forhold til å gjenopprette en feil, vern, redundans osv.

Det kan være fordelaktig å illustrere kombinasjoner av feil som vurderes skjematisk, både i analysemøtet og i rapporten hvor ROS-analysen dokumenteres. Se figuren under for et eksempel på hvordan dette kan illustreres (Pedersen & Thorstad 2008). I figuren illustreres samtidig utfall av linje H-G, linje G-E og linje H-E.



Figur 3 Kombinasjon av feil som gir avbrudd i strømforsyning.

Hvordan navngi uønskede hendelser?
Siden fokuset i dette eksempelet er forsyningssikkerhet er det viktig at de uønskede hendelsene navngis slik at de faktisk kan medføre en konsekvens for forsyningssikkerhet. F.eks. kan "utfall av linje H-E som følge av snøskred" være en uønsket hendelse i denne sammenheng, mens "snøskred" i denne sammenheng ikke er en uønsket hendelse, men en årsak til en uønsket hendelse.

Nedenfor gis det et eksempel på et utdrag fra analyseskjemaet fra ROS-analysen av overføringsnettet (nivå 1).

Figur 4 Utdrag fra ROS-analyseskjema – ROS-analyse av overføringsnette

Analyseobjekt: Overføringsnettet til Energiselskapet AS

Gjennomført av: Energiselskapet AS **Dato:** 01.07.2010

Formål: ROS-analysen har som formål å etablere en oversikt over de viktigste anleggene til virksomheten ift. forsyningssikkerhet

System		Uønsket hendelse	Risiko- og sårbarhetsvurdering								Risikohåndtering		
			Beskrivelse / begrunnelse	Årsaker	Sannsynlighet / frekvens	Konsekvens; 5: svært alvorlig, 1: ubetydelig			Usikkerhet (sett kryss)	Sårbarhetsvurdering			
ID	Delsystem / komponent	Navngi uønsket hendelse	Nærmere beskrivelse av hendelsen. Kommentarer og diskusjon som ligger til grunn for valgt frekvens og konsekvens	- årsak til hendelse - særskilte forhold - avvik fra regelverk ...	5: > 1 gang pr år 4: 1 gang pr år - hvert 10. år 3: hvert 10. år - hvert 100. år 2: hvert 100. år - hvert 1000. år 1: < hvert 1000. år	K1: **Forsyningssikkerhet**: bortfall av strøm/ antall sluttbrukere berørt	K2: ...	K3: ...		Beskrivelse av sårbarhet - forventet nedetid - finnes reservedeler på lager? - hvor kritisk er komponenten?	Eksisterende barrierer **NB!** Forutsetninger for angitt risikonivå	Foreslåtte barrierer / tiltak	Styrbarhet: - høy - middels - lav
1.1	Transformator-stasjon D	Utfall av transformator-stasjon D	Transformatorstasjon D har to transformatorer i separate nisjer. Eksplosjon i transformator 1 kan medføre skade på koblingsanlegg. Transformator 2 må kobles ut inntil feil på koblingsanlegg er utbedret. Dette medfører utfall av transformatorstasjon D i lengre tid. Eksplosjon i transformatorer har skjedd tidligere hos andre kraftselskaper i Norge. Transformatorstasjon D er viktig for forsyningssikkerheten for by A (N-0).	Eksplosjon i transformator som følge av vedlikehold i anlegget	2. hvert 100. år - hvert 1000. år	5. Svært alvorlig. Samfunnsviktige funksjoner som liv og helse, samt viktig infrastruktur rammet / satt ut av funksjon. Avbrud ≥ 10 timer hos ≥ 1000 sluttbrukere.	-	-		Utfall av transformator-stasjon D gir avbrudd i strømforsyning for by A. Reservedeler til koblings-anlegg finnes på lager. Feil på koblingsanlegget vil kunne gjenopprettes innen 10-24 timer.	1. Redundans i de to transformatorene. 2. Reservedeler til koblingsanlegget.	1. Ny linje til overordnett nett X. 2. Gjennomføre ROS-analyse av transformator-stasjon D, samt av transport-beredskap.	Høy
2.1	Linje H-G Linje G-E Linje H-E	Samtidig utfall av linjer	Flere linjer går over høyfjellet og er eksponert for samme naturfenomen som dekker et større område, f.eks. storm, kraftig snøfall osv. Dette har tidligere skjedd i selskapet. Medfører ikke avbrudd i strømforsyning for by A pga. forsyning kan gå fra overordnet nett via linje I-F og linje F-E. I lavlastperioder vil dette ikke gi noen konsekvenser ift. forsyningssikkerhet. I høylastperioder kan dette medføre seksjonering og avbrudd i strømforsying for noen mindre områder.	Storm Ising Snø	3. hvert 10. år - hvert 100. år	3. Middels. Noen lokale konsekvenser for privatabonnementer. Avbrudd < 10 timer hos < 1000 sluttbrukere eller ≥ 10 timer hos < 10 sluttbrukere.	-	-		Ikke avbrudd i strømforsyning for by A dersom det er tilstrekkelig kapasitet fra overordnet nett. Mer utsatt i høylastperioder hvor det kan bli behov for seksjonering av enkelte områder. Det er sammenfall mellom høylastperiode og noen av årsakene. Dette medfører at selskapet er spesielt sårbar i enkelte perioder av året (vinter). Også sårbar ift. frem-kommelighet i samme periode.	1. Strømforsyning fra overordnet nett via linje I-F og linje F-F. 2. Dobbel linjetrasé på enkelte strekninger.	1. Ved oppgradering / utbedrelse av linjenett bør alternativ linjetrasé vurderes, f.eks. nede i dalen i steden for oppe på høyfjellet. 2. Gjennomføre ROS-analyse av transport-beredskap. Vurdere behov for spesielle kjøretøy / helikopter.	Middels
...	...	...	...	...	...	...	-	-	...	...	...	...	...

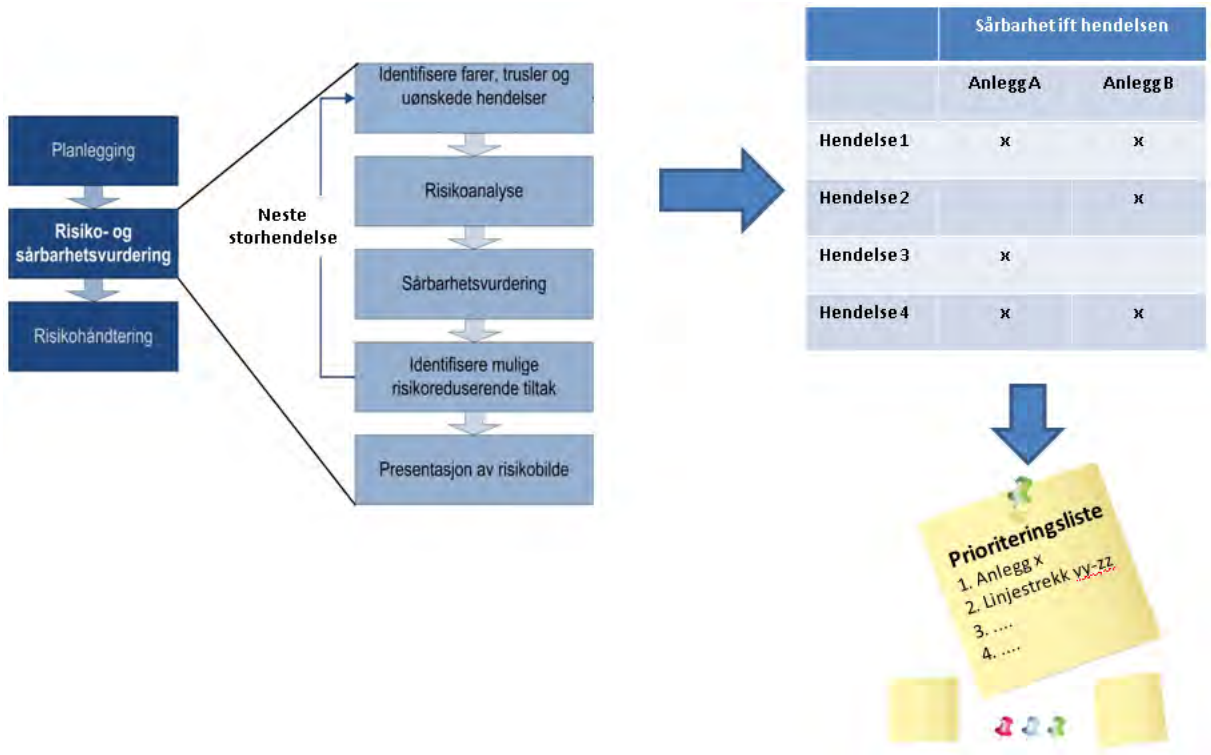
t (nivå 1).

Presentasjon av risikobilde

Resultatene fra en nivå 1 ROS-analyse vil være en kartlegging av hvilke anlegg som er vurdert som viktigst for systemet med hensyn til forsyningssikkerhet. Klassifisering av anleggene sier også noe om viktigheten av de ulike anleggene. Men ROS-analysen vil også naturlig omfatte de uklassifiserte anleggene.

De ulike anlegg/linjer vil ha ulik konsekvens i forhold til hvor mange kunder som blir rammet pga. manglende evne til levering av energi ved utfall. Disse anleggene/linjene er også ulikt eksponert ift. hendelsene/storulykkene som er identifisert. Kombinasjonen av konsekvensene ved utfall og sårbarheten i forhold til hendelsene gir rangeringen.

! **Hvordan prioritere anleggene/linjene?**
De identifiserte storhendelsene danner grunnlaget for rangeringen, som gjøres ved å vurdere konsekvensene ved utfall ift. forsyningssikkerheten for det enkelte anlegg/linje og sårbarheten i forhold til hendelsen.

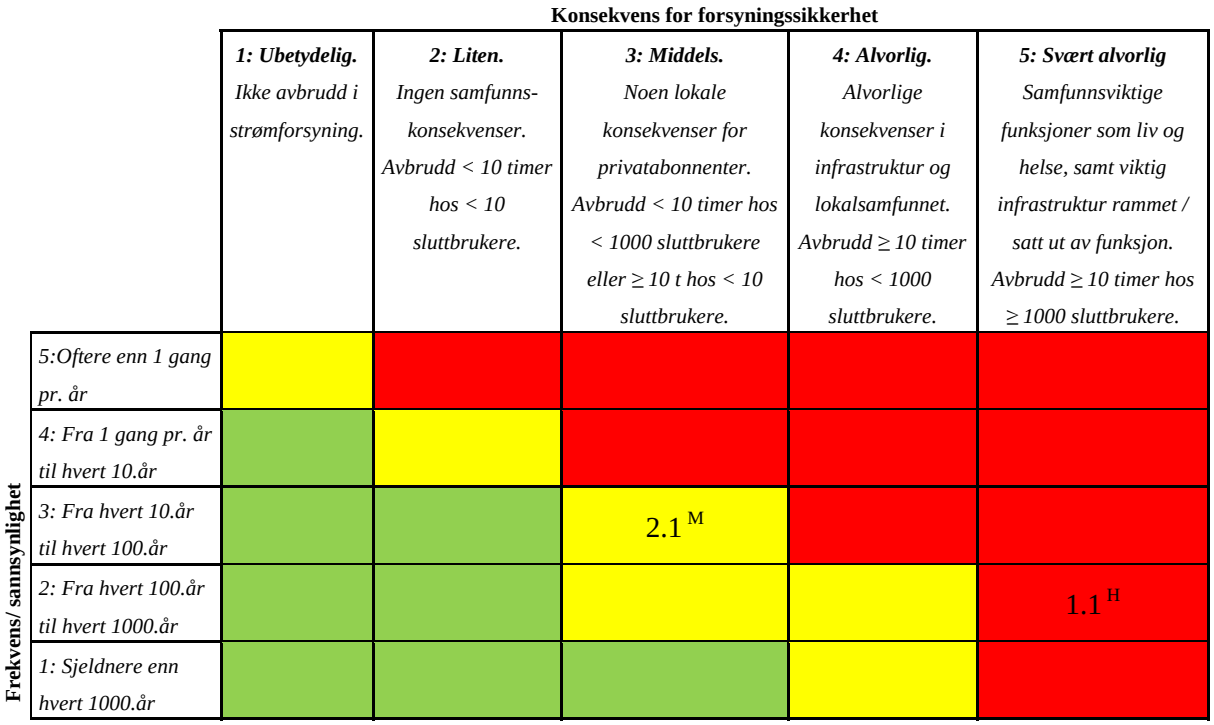


Figur 5 De ulike stegene i risiko- og sårbarhetsvurderingen

Presentasjon

Resultatene fra risiko- og sårbarhetsvurderingen kan presenteres på mange ulike måter. Ofte velger man en eller annen variant av en risikomatrise. Et eksempel på dette er vist i Figur 6 under. Her er hendelsene plottet med løpenummeret som benyttet i analyseloggen. Uthevet skrift indikerer usikkerhet, mens H, M, L indikerer grad av styrbarhet. Man kan også rangere risiko på andre måter. Hvilken fremstillingsmåte som velges bør avhenge av hva man ønsker å synliggjøre.

Tabell 1 nedenfor synliggjør hvilke anlegg som oppfattes å være viktigst ut fra et forsyningssikkerhetsperspektiv. Med andre ord hvilke anlegg som bør prioriteres for videre oppfølging.



Figur 6 Eksempel på hvordan resultatene fra en risiko- og sårbarhetsvurdering kan presenteres ved bruk av risikomatrise.

Hva er viktigst?

Rangeringen av anlegg, systemer og funksjoner kan være nyttig i forhold til å prioritere hvilke man skal analysere først. Viktigheten sett opp mot opprettholdelse av forsyningssikkerheten gjør det lettere for alle å få en totaloversikt over hvor man bør starte jobben.

Etter å ha vurdert rangeringen kan denne presenteres i tabellsform (se tabell 1)

Tabell 1Rangering av anlegg/linjer

Pri	Anlegg/linje
1	Trafostasjon A (300kV)
	Trafostasjon B (300kV)
	Trafostasjon C (300kV)
2	Linje A-B (300kV)
	Trafostasjon F (132kV)
3	Trafostasjon X (300kV)
	Produksjonsanlegg …
	….
	….

Risikohåndtering
Resultatene fra en slik overordnet ROS-analyse kan eksempelvis brukes til å gi beslutningsunderlag til hvilke anlegg som skal prioriteres for videre analyse eller hvilke anlegg som skal prioriteres ved iverksetting av tiltak. Det er viktig å ansvarliggjøre ledelsen når det kommer til å følge opp tiltakene fra ROS-analysen.

! Ekstraordinære hendelser kan inntreffe samtidig på ulike anlegg pga. felles årsak, f.eks. ekstremt vær. Dersom det er begrensning i tilgjengelighet på utstyr, materiell og/eller kompetanse til å få gjenopprettet strømforsyningen, kan resultatene fra en slik overordnet ROS-analyse brukes som grunnlag for prioritering av ressurser etter at hendelsen har skjedd.

Noen anlegg gir større bidrag til konsekvens i forhold til forsyningssikkerhet enn andre og det er disse det da bør fokuseres på. Fra dette eksempelet kan det være naturlig å rangere transformatorstasjon D (ID 1.1) høyere enn linjene H-G, G-E og H-E (ID 2.1) i forhold til forsyningssikkerhet (se Figur 6).

! **Ekstremvind, risiko og sårbarhet**
I NVEs rapport "Klimautfordringer i kraftsektoren frem mot 2100" pekes det på at klimarelaterte hendelser allerede i dag er en viktig årsak til feil og avbrudd innen kraftforsyningen. I rapporten konkluderes det med at endringer for kraftforsyningen i stor grad vil være av kvantitativ art, med økt frekvens av hendelser. En av hendelsestypene med mulighet for økt frekvens er ekstremvind, som har stort skadepotensial.

Et eksempel på dette er ekstremværet Dagmar, som traff Norge i romjulen 2011. Innrapporterte KILE-beløp (Kvalitetsjusterte inntektsrammer ved Ikke Levert Energi) og USLA-beløp (Utbetaling ved Svært Langvarige Avbrudd) fra nettselskapene i februar 2012 viste en samlet sum på over en halv milliard kroner, og i tillegg er reparasjonskostnader beregnet til i underkant av 150 millioner kroner. Rundt 570 000 strømkunder ble berørt, og over 35 000 kunder var uten strøm i mer enn 24 timer[1].

Beredskapsforskriften (BfK) stiller krav til hurtig gjenoppretting av funksjon ved ekstraordinære hendelser, herunder blant annet krav til personell (§ 3-1), kompetanse (§ 3-2), transportberedskap (§ 3-6) og sambandsberedskap (§ 3-8). Ekstremvind rammer ofte et større område, og påvirker ikke bare kraftnettet. Det er viktig at selskapene inkluderer risikomomenter relatert til tilgjengelige ressurser (kompetanse og reservedeler) i sine vurderinger, og at man også tar høyde for at samme værfenomen kan ramme flere selskaper enn deres eget. Her er gode avtaler med leverandører et nøkkeltiltak. Dagmar ga store utfordringer for kraftforsyningen på Vestlandet, Midt-Norge og Østlandet.

Selskapene må også inkludere sammenfallende hendelser, som kan medføre en eskalering av situasjonen, i sine ROS-analyser. Eksempler på dette er utfall av nett kombinert med svikt i samband, og/eller redusert framkommelighet. Redusert framkommelighet kan eksempelvis redusere selskapets evne til å reparere sine anlegg. Samband er ofte spunnet i fiber på ledningsmastene, noe som kan gi utfordringer når offentlig kommunikasjon også feiler. Det

[1] NVE: "Første inntrykk etter ekstremværet Dagmar, julen 2011" (2012)

er viktig at samband opprettholdes selv om de sambandsløsningene man normalt benytter har omfattende og langvarige utfall, hvilket også er et krav i Beredskapsforskriften (§ 3-8[2]). Følgefeil (eksempelvis skader på trafoer eller kabler) må også risikovurderes.

En av hovedutfordringene i håndteringen av klimapåkjenninger (både ut fra dagens og fremtidig klima) er at selskapene står ovenfor betydelig usikkerhet. Et sentralt spørsmål er: hvilke(t) scenario(er) skal man legge til grunn? Klimascenarioer indikerer at det kan bli en økning i antall dager med ekstremvind, samtidig som det også kan bli endringer i rådende vindretninger. Ekstremvind kan dermed medføre utfordringer i forhold til linjestrekk og bygninger som per i dag ikke har vært utsatt for denne problematikken. Det er viktig at man i ROS-analyser løsriver seg fra personlige erfaringer, og baserer seg på vurderinger og relevante framtidsscenarioer snarere enn statistikk. Usikkerhet i, og forutsetninger for, de vurderinger som gjøres må synliggjøres, slik at dette kan tas høyde for i beslutningsprosesser. Det er viktig å innhente informasjon om klimaendringer fra relevante kilder, og da spesielt gode metrologiske kilder (for eksempel www.met.no).

ROS-analyser må søke å avdekke nye risikoer og sårbarheter som følger av potensielle klimautfordringer, med spesielt fokus på ekstremvær og at anlegg er tilstrekkelig dimensjonert i forhold til påregnelige værpåkjenninger. Planlegging og utbygging i kraftbransjen har et langsiktig tidsperspektiv, og endringer i ettertid av utbygging er ofte forbundet med høye kostnader. Det er derfor viktig at værpåkjenninger tidlig er i fokus i ROS-analyser relatert til (re-)investeringer og oppgraderinger. Funn fra ROS-analyser må også implementeres ved planlegging av vedlikehold og inspeksjon av eksisterende anlegg. Erfaringene fra nyttårsorkanen i 1992 og Dagmar i 2011 viste tydelig behovet for strategiske vurderinger rundt rydding av skog, kabling og nettforsterkning. Videre vil det å ha tilstrekkelig kunnskap om skogstypers motstandsdyktighet i forhold til vind, tilveksthastighet, bruken av uisolerte luftlinjer versus isolerte luftlinjer når det gjelder avbrudd med videre være en forutsetning for å kunne vurdere risiko og sårbarhet på en god måte. Prioriterte linjer bør vurderes særskilt i ROS-analysene.

[2] Se også "Veiledning til forskrift om beredskap i kraftforsyningen" (NVE, 2011), kapittel 3.8.1

4.2 Eksempel på ROS-analyse nivå 2 – analyse av spesifikk transformatorstasjon

Basert på den overordnete ROS-analysen (nivå 1) skal det gjennomføres ROS-analyser av de anleggene som ble vurdert å være viktigst i forhold til forsyningssikkerhet. Det er også andre situasjoner der det skal gjennomføres ROS-analyser av spesifikke anlegg og aktiviteter som for eksempel ved større modifikasjoner av eksisterende anlegg og ved bygging av nye anlegg.
I dette eksempelet planlegger et kraftforsyningsselskap å bygge en ny transformatorstasjon og skal i den sammenheng gjennomføre en ROS-analyse av det planlagte anlegget.

Planlegging

Formål og omfang

Formålet med analysen kan være å kartlegge forhold ved den nye transformatorstasjonen som kan utgjøre en trussel mot forsyningssikkerhet og personellsikkerhet. Resultatene fra analysen skal brukes til å gi innspill til design av anlegget og som underlag for melding av klassifisering av anlegg til NVE.

> **!** **Planlegging**
> For å kunne gi innspill til design er det viktig at ROS-analysen foretas tidlig i designfasen. I denne fasen er det som regel mye lettere å foreta endringer enn når anlegget er ferdigbygd, og ROS-analyser er et nyttig hjelpemiddel for bl.a. å planlegge sikringstiltak som tar hensyn til lokale naturgitte forhold m.v.
>
> Etter hvert vil det være mer detaljer rundt anlegget som kan legges til grunn for ROS-analysen. Samtidig vil det være mindre mulighet til å gjøre endringer i design og utforming av anlegget. Dette er en balansegang der det er viktig å gjennomføre ROS-analysen på et tidspunkt der det fremdeles er mulighet til å påvirke beslutninger. Noen ganger må derfor ROS-analysen gjennomføres flere ganger etter hverandre.

Valg av konsekvens- og sannsynlighetsdimensjoner

> **!** **Skal alt analyseres?**
> Ifm. planleggingen av ROS-analysen er det viktig å avklare hvilke konsekvensdimensjoner en skal vurdere risiko i forhold til. Beredskapsforskriften stiller krav til at risiko og sårbarhet skal vurderes ift. forsyningssikkerhet. ROS-analysen er imidlertid en del av risikostyringen av selskapet (virksomhetsstyring) og i den forbindelse er det også relevant å vurdere risiko og sårbarhet ift. andre konsekvensdimensjoner. (Dette er også en forventning ift. krav stilt til kraftbransjen gjennom annet regelverk som kan være relevant)

I dette eksempelet velger vi å bruke de samme kategoriinndelingene for forsyningssikkerhet og sannsynlighet / frekvens som i veilederen (NVE og Proactima 2010).

Tabell 2 Eksempler på konsekvenskategorier (dette må tilpasses den enkelte virksomhet).

Konsekvenskategori	Forsyningssikkerhet
1) Ubetydelig	Ikke avbrudd i strømforsyning
2) Liten	Ingen samfunnskonsekvenser. Avbrudd < 10 timer hos < 10 sluttbrukere.
3) Middels	Noen lokale konsekvenser for privatabonnenter. Avbrudd < 10 timer hos < 1000 sluttbrukere eller ≥ 10 t hos < 10 sluttbrukere.
4) Alvorlig	Noen lokale konsekvenser for privatabonnenter. Avbrudd < 10 timer hos < 1000 sluttbrukere eller ≥ 10 t hos < 10 sluttbrukere.
5) Svært alvorlig	Alvorlige konsekvenser i infrastruktur og lokalsamfunnet. Avbrudd ≥ 10 timer hos < 1000 sluttbrukere.

Informasjonsinnhenting

Relevant bakgrunnsinformasjon for en slik analyse kan typisk være:

- Nivå 1 ROS-analyse for hele kraftsystemet.
- Tidligere gjennomførte ROS-analyser for dette og tilsvarende anlegg (nivå 2).
- Tegninger, flytskjema eller annen dokumentasjon som beskriver anlegget.
- Kart over anlegget og omgivelsene.
- Etablerte beredskapsanalyser og beredskapsplaner for anlegget.
- Relevant lovverk og/eller interne retningslinjer.
- Data over historiske uønskede hendelser som har oppstått i tilknytning til anlegget eller tilsvarende anlegget.
- Lokalkunnskap, erfaringsdata, forskning.
- …

> **!** For en ROS-analyse av et eksisterende anlegg kan det være hensiktsmessig at analysegruppen gjennomfører en befaring av anlegget for å få en god forståelse av anlegget. En befaring kan hjelpe til med å avdekke forhold som nylig har endret seg eller er vanskelig å forutse uten dypere kjennskap til anlegget. I tillegg kan befaringen bidra til en bedre prosess ved at analysegruppen får en felles forståelse av problemstillingen.

Analysegruppe

Det er besluttet å gjennomføre en strukturert grovanalyse. Som for andre ROS-analyser er det viktig å sikre at personell med kunnskap og kompetanse om anlegget er tilgjengelig. Blant annet kan følgende disipliner være relevante:

- Drift og vedlikehold (innenfor ulike fagområder som transformatorer, kontrollanlegg, vern, brytere, anlegg, grunn, elektro, IKT-sikkerhet osv.).
- Beredskap
- Driftssentral.
- Montører.
- …

Klargjøring av analyseskjema og sjekklister

Før analysemøtet må analyseskjema og sjekklister gjøres klar og testes ut. Analyseskjemaet og den generelle sjekklisten, sammen med sjekklisten for transformatorstasjoner, i "Veiledning i ROS-analyser for kraftforsyningen" (NVE og Proactima 2010) kan her benyttes som et utgangspunkt, men sjekklisten bør alltid oppdateres etter hvert som ny kunnskap erverves.. Transformatorstasjonen deles inn i delsystemer og komponenter som gitt i tabell 3.

Tabell 3 Oversikt over delsystemer og komponenter for transformatorstasjonen (tabellen gir ikke en komplett oversikt).

ID	Delsystem	ID	Komponent
1	Transformator	-	-
2	Effektbryter	-	-
3	Skillebryter	-	-
4	Jordbryter	-	-
5	Avganger	5.1	Innstrekkstativ
		5.2	Klemmer
		5.3	…
6	Samleskinne	6.1	Samleskinne
		6.2	Jordbryter
		6.3	Isolator
		6.4	…
7	Måling	7.1	Strømtransformator
		7.2	Spenningstransformator
		7.3	…
8	Bygninger / anlegg	-	-
9	Vern & kontrollanlegg	-	-
10	…	…	…

Risiko- og sårbarhetsvurdering

Risiko- og sårbarhetsvurderingen gjennomføres i et analysemøte.

I en slik analyse bør også inkludere eksempler på uønskede hendelser som kan knyttes til beredskapsforskriftens felles plikter som transportberedskap og fysisk sikring (for en analyse av disse forholdene på tvers av selskapet (nivå 1) vises det til eksempler i kapittel 5.

! Vi vurderer den uønskede hendelsen ”eksplosjon i transformator”. Transformatorstasjonen er normalt ubemannet og det er normalt personell til stede kun ca. 2 timer hver uke ifm. vaktrunde. Dersom den uønskede hendelsen også vurderes å kunne inntreffe når det ikke er personell til stede, er det ikke direkte sammenheng mellom konsekvens for forsyningssikkerhet og personellsikkerhet, gitt at hendelsen inntreffer. Det er ulike måter å ta hensyn til dette på i risiko- og sårbarhetsvurderingen. Eksempelvis kan vi dele den uønskede hendelsen inn i mer detaljerte hendelser og vurdere disse hendelsene vær for seg; eksempelvis ”eksplosjon i transformator ved vedlikehold i anlegget” og ”eksplosjon i transformator ubemannet stasjon”.

Alternativt kan vi vurdere hendelsen ”eksplosjon i transformator”, og angi at det er stor usikkerhet ift. konsekvens for personellsikkerhet da det er personell tiltede kun i perioder. Vi kan også vurdere sannsynlighet for hendelsen ”eksplosjon i transformator”, for så å vurdere betinget sannsynlighet for hhv. personellskade og avbrudd i strømforsyning.

Nedenfor gis det et eksempel på et utdrag fra analyseskjemaet fra ROS-analysen av den planlagte transformatorstasjonen (nivå 2).

Figur 7 Utdrag fra ROS-analyseskjema – ROS-analysen av ny transformatorstasjon (nivå 2) – del 1.

Analyseobjekt: Planlagt transformatorstasjon

Gjennomført av: Energiselskapet AS **Dato:** 10.07.2010

Formål: ROS-analysen har som formål å kartlegge forhold ved den nye transformatorstasjonen som kan utgjøre en trussel mot forsyningssikkerhet og personellsikkerhet.
Resultatene fra analysen skal brukes til å gi innspill til design og plassering av anlegget og som underlag for melding av klassifisering av anlegg til NVE.

System		Uønsket hendelse	Risiko- og sårbarhetsvurdering								Risikohåndtering		
			Beskrivelse / begrunnelse	Årsaker	Sannsynlighet / frekvens	Konsekvens; 5: svært alvorlig, 1: ubetydelig			Usikkerhet (sett kryss)	Sårbarhetsvurdering			
ID	Delsystem / komponent	Navngi uønsket hendelse	Nærmere beskrivelse av hendelsen. Kommentarer og diskusjon som ligger til grunn for valgt frekvens og konsekvens	- årsak til hendelse - særskilte forhold - avvik fra regelverk ...	5: > 1 gang pr år 4: 1 gang pr år - hvert 10. år 3: hvert 10. år - hvert 100. år 2: hvert 100. år - hvert 1000. år 1: < hvert 1000. år	K1: **Forsyningssikkerhet**: bortfall av strøm/ antall sluttbrukere berørt	K2: **Personellsikkerhet** skade / dødsfall	K3: ...		Beskrivelse av sårbarhet - forventet nedetid - finnes reservedeler på lager? - hvor kritisk er komponenten?	Eksisterende barrierer **NB!** Forutsetninger for angitt risikonivå	Foreslåtte barrierer / tiltak	Styrbarhet: - høy - middels - lav
1.0	Transformator	Eksplosjon i transformator	Transformatorstasjonen er planlagt med to transformatorer i separate nisjer. Eksplosjon i transformator 1 kan medføre skade på koblingsanlegg. Transformator 2 må kobles ut inntil feil på koblingsanlegg er utbedret. Dette medfører utfall av transformatorstasjonen i lenger tid. Transformatorstasjonen er normalt ubemannet. Normalt er det personell til stede to timer i uken i tillegg til ved vedlikehold. Eksplosjonen oppstår imidlertid som en direkte følge av vedlikehold i anlegget. Eksplosjon i transformatorer har skjedd tidligere hos andre kraftselskaper i Norge. Da som følge av vedlikehold i anlegget.	Vedlikehold i anlegget	2. hvert 100. år - hvert 1000. år	4. Alvorlig. Alvorlige konsekvenser i infrastruktur og lokalsamfunnet. Avbrudd ≥ 10 timer hos < 1000 sluttbrukere.	5. Svært alvorlig. To dødsfall.	-		Strømforsyning til sluttbrukere kan opprettholdes i lavlastperioder via annen transformatorstasjon. Mer utsatt i høylastperioder hvor det kan bli behov for seksjonering av enkelte områder. Reservedeler til koblingsanlegg finnes på lager. Feil på koblingsanlegget vil kunne gjenopprettes innen 10-24 timer.	1. Redundans i de to transformatorene. 2. Transformator-stasjon bygges med nyeste teknologi. 2. Reservedeler til koblingsanlegget.	1. Øke avstand mellom de to transformatorene. 2. Designe transformatornisjene med retningsspesifikk avlastningsflate.	Høy
2.0	Uteanlegg	Havari av uteanlegg	Uteanlegget er plassert inntil en fjellknaus. Dette gir enkel adkomst for uvedkommende til å kaste ting inn på eller skyte i stykker de strømførende komponentene i uteanlegget. Dette gjør også at uteanlegget er utsatt for steinsprang. Dette kan medføre kortslutning / overslag med påfølgende eksplosjon slik at uteanlegget faller ut. Steinsprang er et kjent fenomen på andre anlegg. Selskapet har også på en annen transformatorstasjon opplevd at ungdommer skyter på uteanlegget for å prøve å treffe komponentene i uteanlegget. Dette har enda ikke medført store skader, men potensialet er der. Det er lite trolig at det er personell til stede i anlegget ved en slik hendelse.	Hærverk / sabotasje Steinsprang	2. hvert 100. år - hvert 1000. år	4. Alvorlig. Alvorlige konsekvenser i infrastruktur og lokalsamfunnet. Avbrudd ≥ 10 timer hos < 1000 sluttbrukere.	1. Ubetydelig. Ikke personskade.	-		Feil på uteanlegget medfører utfall av transformatorstasjonen. Strømforsyning til sluttbrukere kan opprettholdes i lavlastperioder via annen transformatorstasjon. Mer utsatt i høylastperioder hvor det kan bli behov for seksjonering av enkelte områder. Selskapet har tilgjengelige reservedeler til komponentene i uteanlegget. Feil på uteanlegget vil kunne gjenopprettes innen 10-24 timer.	1. Sikringstiltak tilfredsstiller krav til klasse 3 anlegg i beredskaps-forskriftens § 5-5 om sikringsnivå. 2. Redundans i de to transformatorene.	1. Flytte uteanlegget vekk fra fjellknausen. 2. Gjerde inn et større område. 3. Installere et høyere gjerde. 4. Sikre fjellknausen mot ras.	Middels

Figur 8 Utdrag fra ROS-analyseskjema – ROS-analysen av ny transformatorstasjon (nivå 2) – del 2.

Analyseobjekt: Planlagt transformatorstasjon

Gjennomført av: Energiselskapet AS **Dato:** 10.07.2010

Formål: ROS-analysen har som formål å kartlegge forhold ved den nye transformatorstasjonen som kan utgjøre en trussel mot forsyningssikkerhet og personellsikkerhet.
Resultatene fra analysen skal brukes til å gi innspill til design og plassering av anlegget og som underlag for melding av klassifisering av anlegg til NVE.

System		Uønsket hendelse	Risiko- og sårbarhetsvurdering								Risikohåndtering		
			Beskrivelse / begrunnelse	Årsaker	Sannsynlighet / frekvens	Konsekvens; 5: svært alvorlig, 1: ubetydelig			Usikkerhet (sett kryss)	Sårbarhetsvurdering			
ID	Delsystem / komponent	Navngi uønsket hendelse	Nærmere beskrivelse av hendelsen. Kommentarer og diskusjon som ligger til grunn for valgt frekvens og konsekvens	- årsak til hendelse - særskilte forhold - avvik fra regelverk ...	5: > 1 gang pr år 4: 1 gang pr år - hvert 10. år 3: hvert 10. år - hvert 100. år 2: hvert 100. år - hvert 1000. år 1: < hvert 1000. år	K1: **Forsyningssikkerhet**: bortfall av strøm/ antall sluttbrukere berørt	K2: **Personellsikkerhet** skade / dødsfall	K3: ...		Beskrivelse av sårbarhet - forventet nedetid - finnes reservedeler på lager? - hvor kritisk er komponenten?	Eksisterende barrierer **NB!** Forutsetninger for angitt risikonivå	Foreslåtte barrierer / tiltak	Styrbarhet: - høy - middels - lav
3.0	Vern	Manglende utkobling	Manglende utkobling ved behov pga. feil på vern. Dette kan gi følgefeil som eksplosjon og utfall av hele transformatorstasjonen. Selskapet har jevnlig erfart feil på vern i andre anlegg (~1 gang pr. år). Dette har ikke gitt skade på anlegget, evt. begrensede skader. Det er lite trolig at det er personell til stede i anlegget ved en slik hendelse.	Feilfunksjon	1. < hvert 1000. år	4. Alvorlig. Alvorlige konsekvenser i infrastruktur og lokalsamfunnet. Avbrudd ≥ 10 timer hos < 1000 sluttbrukere.	1. Ubetydelig. Ikke personskade.	-	X	Strømforsyning til sluttbrukere kan opprettholdes i lavlastperioder via annen transformatorstasjon. Mer utsatt i høylastperioder hvor det kan bli behov for seksjonering av enkelte områder. Det er redundans i de fleste deler av vern- og kontrollanleggsystemet, men felles kabelføringer. Dette medfører at en hendelse kan medføre feil på hele vern- og kontrollanleggsystemet. Kontroll- og vernsystemets sammensetning er ofte veldig komplekst. Dette er spesielt utfordrende for personell som inngår i vaktordning da de kan ha begrenset kjennskap til systemene. Under ekstraordinære forhold kan dette medføre unødvendig lang tid til gjenoppretting av feil. Vernsystemet på det nye anlegget skal kommunisere og fungere sammen med vern på andre anlegg av eldre dato. Dette er en utfordring.	1. Redundans i de fleste deler av vern- og kontrollanlegg-systemet. 2. Dokumentasjon på vern og kontrollanlegget as-built.	1. Sikre redundans i alle deler av vern- og kontrollanleggsystemet. 2. Sikre kompetanse til gjenoppretting ved feil på komponenter i anlegget. 3. Sikre oppdatert dokumentasjon på vern- og kontrollanlegg ved både mindre og større endringer på anlegget. 4. Gjennomføre mer detaljert analyse av vernsystemet. 5. Sikre riktig innstilling av vern. 6. Sikre gode rutiner for innstilling og kontroll av vern.	Høy
...	...	...	...	...	...	...	...	-	...	...	...	...	...

Presentasjon av risikobilde

Resultatene fra en slik ROS-analyse vil være en kartlegging av forhold ved transformatorstasjonen som kan utgjøre en trussel mot forsyningssikkerhet og personellsikkerhet. ROS-analysen kan brukes til å gi innspill til design av transformatorstasjonen, samt som underlag for melding av klassifisering av anlegget til NVE.

Resultatene fra risiko- og sårbarhetsvurderingen kan presenteres ved bruk av risikomatriser. Det må brukes en matrise for hver konsekvensdimensjon, i dette eksempelet henholdsvis forsyningssikkerhet og personellsikkerhet. Et eksempel på dette er vist i Figur 9 og Figur 10 under. Her er hendelsene plottet med løpenummeret som ble benyttet i analyseloggen. Uthevet skrift indikerer usikkerhet, mens H, M, L indikerer grad av styrbarhet.

Konsekvens for forsyningssikkerhet

Frekvens/ sannsynlighet	***1: Ubetydelig.*** *Ikke avbrudd i strømforsyning.*	***2: Liten.*** *Ingen samfunns-konsekvenser. Avbrudd < 10 timer hos < 10 sluttbrukere.*	***3: Middels.*** *Noen lokale konsekvenser for privatabonnenter. Avbrudd < 10 timer hos < 1000 sluttbrukere eller ≥ 10 t hos < 10 sluttbrukere.*	***4: Alvorlig.*** *Alvorlige konsekvenser i infrastruktur og lokalsamfunnet. Avbrudd ≥ 10 timer hos < 1000 sluttbrukere.*	***5: Svært alvorlig*** *Samfunnsviktige funksjoner som liv og helse, samt viktig infrastruktur rammet / satt ut av funksjon. Avbrudd ≥ 10 timer hos ≥ 1000 sluttbrukere.*
5:Oftere enn 1 gang pr. år					
4: Fra 1 gang pr. år til hvert 10.år					
3: Fra hvert 10.år til hvert 100.år					
2: Fra hvert 100.år til hvert 1000.år				1.0 H, 2.0 M	
1: Sjeldnere enn hvert 1000.år				**3.0** H	

Figur 9 Eksempel på hvordan resultatene fra en risiko- og sårbarhetsvurdering kan presenteres ved bruk av risikomatrise.

Konsekvens knyttet til personellsikkerhet

Virksomheten må også selv vurdere hva som skal legges inn av vekting i den enkelte konsekvensklasse

Frekvens/ sannsynlighet	***1: Ubetydelig***	***2: Liten.***	***3: Middels.***	***4: Alvorlig.***	***5: Svært alvorlig***
5:Oftere enn 1 gang pr. år					
4: Fra 1 gang pr. år til hvert 10.år					
3: Fra hvert 10.år til hvert 100.år					
2: Fra hvert 100.år til hvert 1000.år	2.0 M				1.0 H
1: Sjeldnere enn hvert 1000.år	**3.0** H				

Figur 10 Eksempel på hvordan resultatene fra en risiko- og sårbarhetsvurdering kan presenteres ved bruk av risikomatrise.

Poenget med å vise det samme risikobildet i to ulike matriser henholdsvis forsyningssikkerhet (Figur 9) og personellsikkerhet (Figur 10) som presenterer to ulike aspekt av risiko. Når man setter ulike risikobilder opp foran en beslutningstaker vil ulike vurderinger også bli foretatt. Hvis Figur 10 personellsikkerhet hadde blitt presentert alene vil plottet 2.0 og 3.0 tilsynelatende virke ”uskyldige”. I personsikkerhetsperspektivet kan dette stemme, men for å opprettholde god forsyningssikkerhet vil situasjonen være en annen.

Risikohåndtering
Fra risikomatrisen for forsyningssikkerhet ser vi at alle de tre hendelsene er plassert i gult område, mens i matrisen for personellsikkerhet ser vi at hendelsen eksplosjon i transformator (ID 1.0) er plassert i rødt område, mens hendelsene havari av uteanlegg (ID 2.0) og feil ved vern (ID 3.0) er plassert i grønt område. Videre viser resultatene at det er høy usikkerhet knyttet til konsekvensene av feil ved vernsystemet (ID 3.0), samt at det er vurdert å være høy styrbarhet for hendelsene relatert til transformatorstasjonen (ID 1.0) og vernsystemet (ID 3.0), mens det er vurdert å være middels styrbarhet for hendelsen relatert til uteanlegget (ID 2.0). Fra anlayseloggen ser vi også at vernsystemet er vurdert å være et komplekst og sårbart system. Basert på dette bør god kontroll på og godt vedlikehold av systemet prioriteres.

> **!** Vurder å gjøre mer detaljerte ROS-analyser av spesifikke delsystem, komponenter eller aktiviteter der hvor det er knyttet høy usikkerhet rundt konsekvensene av en uønsket hendelse, for uønskede hendelser med høy risiko eller sårbarhet, eller i situasjoner der bakgrunnskunnskapen er mangelfull.

I dette eksempelet kunne det derfor vært naturlig å gjennomføre mer detaljerte vurderinger av vernsystemet.

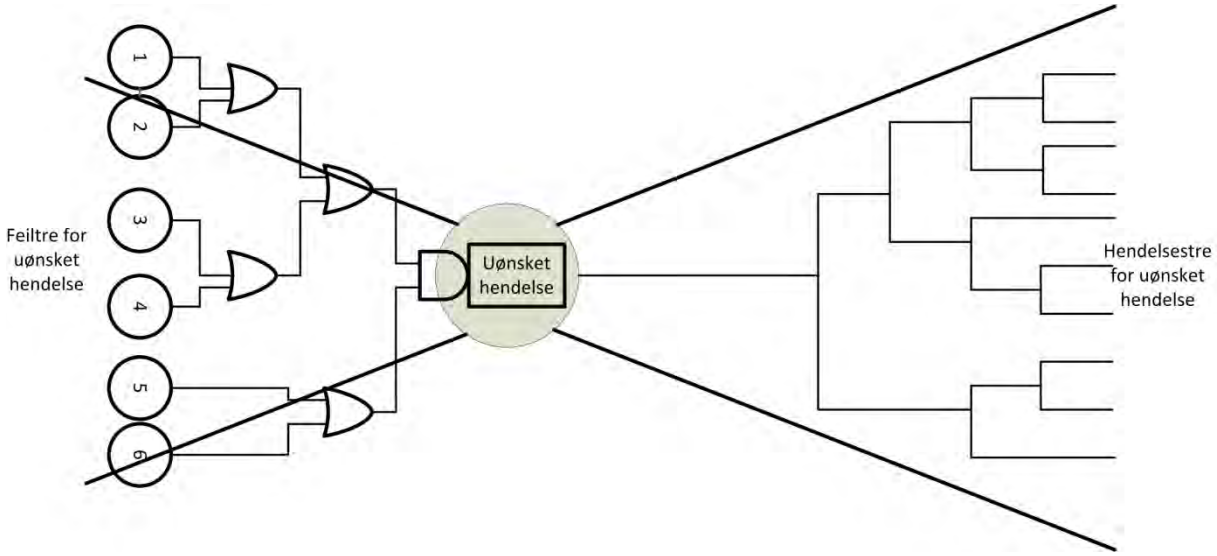
Nivå 2 analysen er en ROS-analyse av spesifikke anlegg og aktiviteter som brukes til å kartlegge forhold ved anleggene som kan true forsyningssikkerheten, mens nivå 1 analysen er en overordent ROS-analyse av alle selskapets anlegg som brukes til å prioritere videre analyser av og tiltak på anlegg. Etter å ha gjennomført ROS-analyser av spesifikke anlegg og aktiviteter (nivå 2) bør ROS-analysen for det overordnete systemet til selskapet (nivå 1) oppdateres for å reflektere resultatene fra disse analysene.

ROS-analyser av spesifikke anlegg og aktiviteter danner bakgrunn for beredskapsplaner som selskapet må etablere. ROS-analysen gir bl.a. innspill til hvilke scenarioer beredskapen skal dimensjoneres for og som skal øves, samt hvor ofte og under hvilke forhold det skal øves.

4.3 Eksempel på ROS-analyse nivå 3 – analyse av uønsket hendelse i transformatorstasjon

Et resultat av ROS-analysen som ble gjennomført på nivå 2, kan være at det er behov for å gjøre mer detaljerte vurderinger for spesifikke delsystemer, komponenter eller aktiviteter. For å gjøre mer detaljerte analyser henvises det til bruk av kjente risiko- og sårbarhetsanalysemetoder, eksempelvis årsaksanalyser som feiltreanalyse og feilmodi- og feileffektanalyse (Failure Modes and Effect Analysis – FMEA), samt konsekvensanalyser som hendelsestreanalyse og brann- / eksplosjonsberegninger. Slike metoder er godt beskrevet i litteraturen og det finnes en rekke lærebøker på fagområdet. Det er utarbeidet ulike norske standarder (bl.a. NS 5814:2008) og en rekke lærebøker (bl.a. Aven, Røed, Wiencke 2008) som kan fungere som hjelp i forbindelse med slike analyser.

Figuren under viser sammenhengen mellom en uønsket hendelse og årsaks- og konsekvensanalyser der et feiltre er lagt på til venstre for en uønsket hendelse i et bow-tie diagram, og et hendelsestre er lagt på til høyre for den uønskede hendelsen i diagrammet.

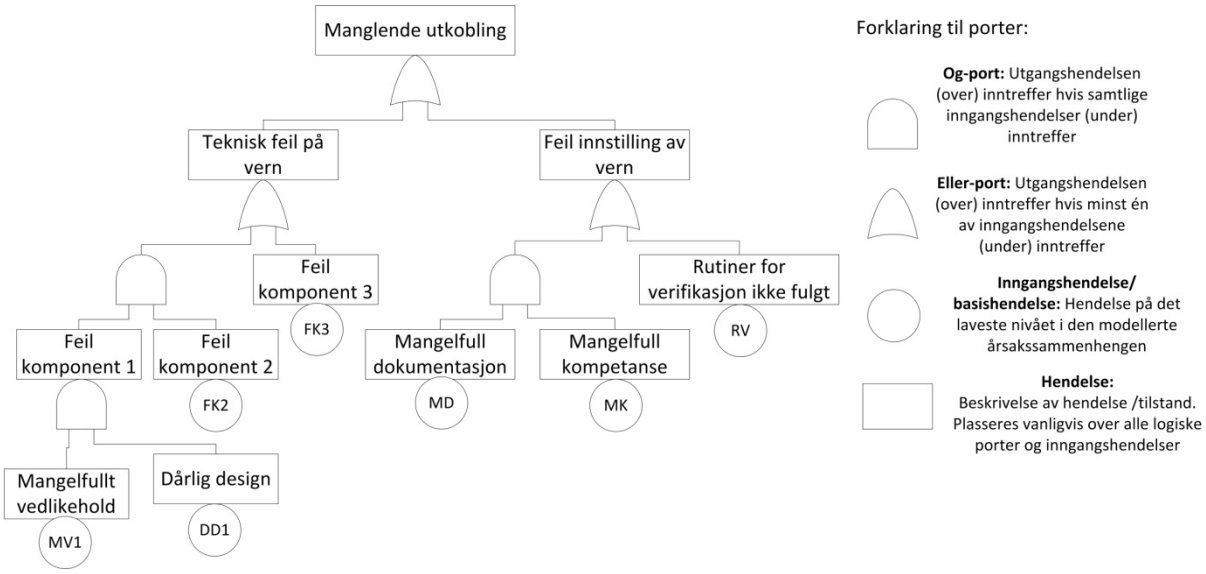


Figur 11 Feiltre- og hendelsestreanalyse satt i sammenheng.

Nedenfor vises to eksempler på hvordan henholdsvis feiltre- og hendelsestreanalyse kan brukes på nivå 3. Formålet med en slik analyse kan være å få en bedre forståelse av uønskede hendelser relatert til spesifikke delsystemer og komponenter i anlegget, og kan brukes som underlag for ROS-analysen av det spesifikke anlegget (nivå 2) når tiltak skal vurderes og prioriteres, samt beredskap dimensjoneres og beredskapsplaner etableres.

4.3.1 Årsaksanalyse – manglende utkobling av vern
La oss se nærmere på den uønskede hendelsen manglende utkobling av vern.

Figur 12 illustrerer hvordan et feiltre kan brukes til å analysere årsakene til en slik hendelse. Feiltreanalyser er ofte nyttige å bruke for system med redundans.

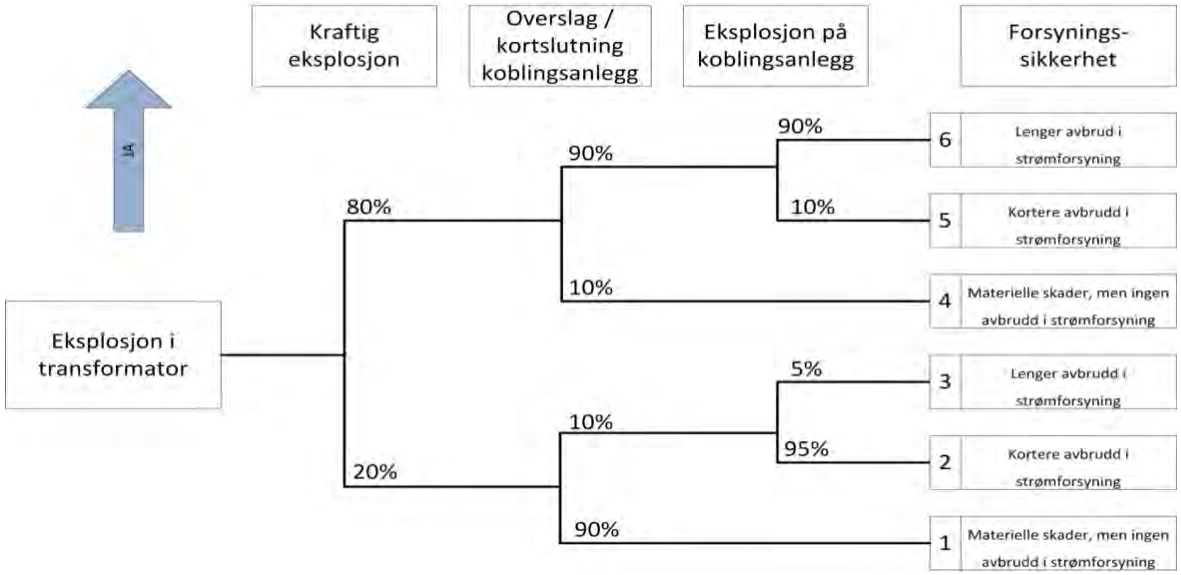


Figur 12 Eksempel på bruk av feiltre – manglende utkobling av vern.

Av figuren ser vi at manglende utkobling er vurdert å kunne skyldes komponentfeil, systemfeil eller menneskelig feil, der menneskelig feil enten kan skyldes manglende dokumentasjon eller manglende kompetanse på vernsystemet.

4.3.2 Konsekvensanalyse – eksplosjon i transformator
La oss se nærmere på den uønskede hendelsen eksplosjon i transformator under vedlikeholdsarbeid

Figur 13 illustrerer hvordan et hendelsestre kan brukes til å analysere hvordan en eksplosjon i en transformator vil kunne utvikle seg.



Figur 13 Eksempel på bruk av hendelsestre – eksplosjon i transformator.

Av figuren ser vi at en eksplosjon i en transformator er vurdert å kunne gi alt fra kun lokale skader, til store skader på uteanlegg, med påfølgende muligheter for avbrudd i strømforsyning. Denne kartleggingen ser isolert på konsekvensen opp mot forsyningssikkerhet.
Som en del av den detaljerte analysen, kan det også være nyttig å gjennomføre detaljerte brann- og eksplosjonssimuleringer. Det henvises til anerkjent programvare for slike simuleringer.
Andre aspekter av hendelsen kan også være gjenstand for analyse, slik som HMS, økonomi, omdømme osv. Men dette bør gjøres i adskilte prosesser slik at den de ulike konsekvensklassene ikke overskygger hverandre. Beredskapsforskriftens fokus ligger på å analysere ulike risiko og sårbarhet sett opp mot forsyningssikkerhet. Virksomhetene må derfor sikre seg at dette er godt ivaretatt i analysene.

5 Eksempel på ROS-analyser av felles systemer

Beredskapsforskriften stiller konkrete krav til blant annet:

- Tilgang på nok, kompetent personell og evne til drift
- Evne til gjenoppretting av funksjon .
- Transportberedskap
- Informasjonsberedskap
- Sambandsberedskap
- Adgangskontroll
- Sikring av anlegg
- Informasjonssikkerhet
- Driftskontrollsystemer

Dette er forhold som må dekkes i selskapets ROS-analyser, både overordnet analyse (nivå 1) og analyser av spesifikke anlegg og aktiviteter (nivå 2).

Beredskapsforskriften setter krav til gjennomføring av ROS-analyser av fellessystem, der en må se på de totale utfordringene for nettvirksomheten for disse fellesløsningene. Også for disse systemene kan man tenke seg analyser på ulike nivå.

! **Hvordan gjennomføre en ROS-analyse av driftskontrollsystem på ulike nivå?**
Nivå 1: Overordnet ROS-analyse – Driftskontrollsystemer, samband, informasjons-sikkerhet og beredskap.
Nivå 2: ROS analyse av kritiske systemer
Nivå 3: Spesifikke analyser (penetrasjonstester, ...)

Videre i dette kapittelet presenteres to eksempler på ROS-analyser av beredskapsforskriftens plikter, henholdsvis transportberedskap og fysisk sikring på overordnet nivå (nivå 1). Hvert eksempel inneholder de tre hoveddelene 1) Planlegging, 2) Risiko- og sårbarhetsvurdering og 3) Risikohåndtering, følger stegene som er foreslått i veilederen for ROS-analyser (NVE og Proactima 2010) . Innenfor hvert eksempel er det fokusert på hva som er spesielt.

5.1 Eksempel på ROS-analyse av transportberedskap (nivå 1)

5.1.1 ROS-analyser og transportberedskap

Å etablere rutiner for transport som gjør det mulig å håndtere ekstraordinære hendelser og gir evne til rask gjenoppretting, er en plikt for det enkelte kraftselskap (ref. beredskapsforskriftens krav). For å imøtekomme dette kravet er det naturlig å etablere en plan for transportberedskap.

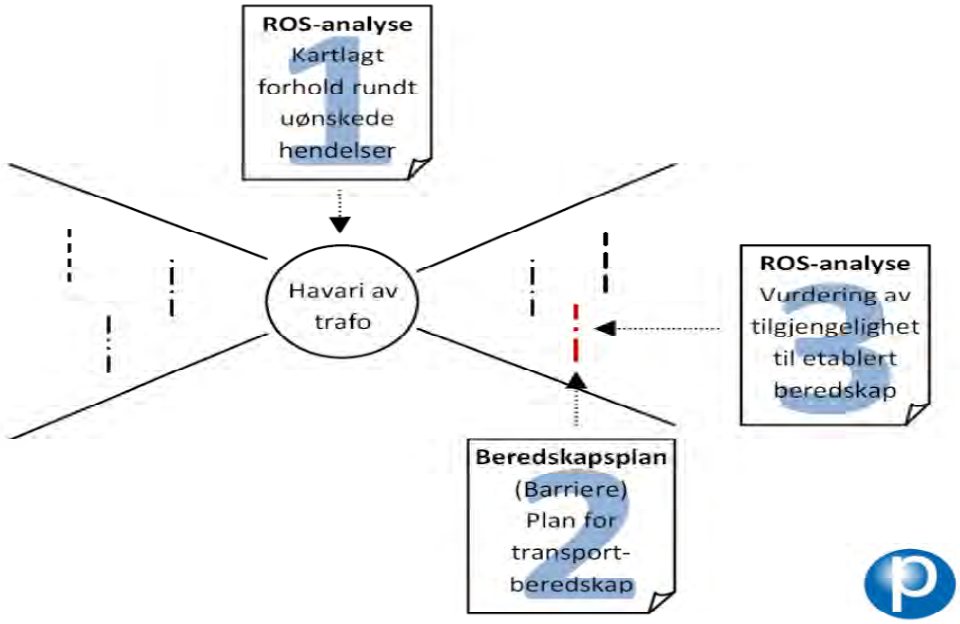
Selskapet bør etablere en felles plan for hvordan transportberedskapen skal arrangeres, hvilke ressurser som skal stilles til rådighet og eventuelt hvor disse resursene skal hentes fra. Planen må i tillegg ta hensyn til særegenheter ved de enkelte anleggene, alternativt grupperinger av anlegg som har mange fellesetrekk. Hvilke elementer som bør inngå i en plan for transportberedskap er nærmere beskrevet i Veiledning til forskrift om beredskap i kraftforsyningen (NVE 2011).

Plan for transportberedskap bør etableres ut fra de uønskede hendelsene som har fremkommet i ROS-analysene for kraftsystemet (nivå 1), og de spesifikke anleggene (nivå 2). Det er de identifiserte hendelsene som forteller oss hvilke feilsituasjoner som kan forventes, og hvordan nødvendig beredskap skal / bør etableres. Deretter dimensjoneres transportberedskapen for å sikre en snarlig gjenoppretting.

I tillegg til eventuelle konsekvensreduserende tiltak vil resultatene fra ROS-analysen gi viktige innspill til både planlegging og gjennomføring av beredskapsøvelser som kan være med å verifisere at tilstrekkelig transportberedskap er etablert.

! **Selskapet har allerede etablert en plan for transportberedskap. Hva gjør vi med den?**
Mange kraftselskap har allerede en etablert plan for transportberedskap uten at denne nødvendigvis er basert på resultater fra ROS-analyser. Etter hvert som ROS-analysene for de ulike anleggene gjennomføres eller oppdateres, bør planen revideres for å ta hensyn til resultatene fra ROS-analysene.

Figur 14 under viser sammenhengen mellom de ulike ROS-analysene som gjennomføres og etablering av plan for transportberedskap. I kapittel 6 vises et eksempel på gjennomføring av en ROS-analyse av transportberedskap.



Figur 14 Sammenhengen mellom ROS-analyser og plan for transportberedskap.

5.1.2 ROS-analyse av transportberedskap

Planlegging

Formål og omfang

For å sikre at etablert transportberedskap er robust kartlegger vi forhold som kan påvirke tilgjengeligheten til de ressursene som inngår i planen. Dette gir oss følgende omfang og formål for ROS-analysen:

ROS-analysen av energiselskapets transportberedskap har som formål å vurdere tilgjengeligheten av etablert transportberedskap.

Forutsetninger og antagelser

Det forutsettes at ROS-analyser for kraftsystemet (nivå 1) og anlegg (nivå 2) er gjennomført.
Gitt at vi skal vurdere hvilke hendelser som kan påvirke tilgjengeligheten på ressurser som inngår i beredskapen, forutsettes det også at selskapet har etablert en plan for hvilken transportberedskap som er nødvendig i henhold til beredskapsforskriftens krav.

Valg av konsekvens- og sannsynlighetsdimensjon

Selskapet tilstreber å tilby en pålitelig leveranse av strøm til enhver tid til alle forbrukere, også når anleggene blir utsatt for uønskede hendelser. Dette reflekteres i valg av konsekvensdimensjon, og fokus for denne ROS-analysen primært rette mot forsyningssikkerhet.

Informasjonsinnhenting

I forbindelse med informasjonsinnhenting bør en typisk skaffe til veie:

- Nivå 1 ROS-analyser for hele kraftsystemet.
- Nivå 2 ROS-analyser for anlegget som betraktes.
- Etablert policy og plan for transportberedskap og evt. beredskapsmateriell.
- Relevante opplysninger om anlegget, og hva som evt. kan være aktuelt å transportere.
- Kart over området med veier og evt. restriksjoner i vekt, lengde osv.
- Evt. forhåndsdispensasjon fra Statens vegvesen.
- Historiske data på vær, etc.
- …

Analysegruppe

Som for andre ROS-analyser er det viktig å sikre at personell med kunnskap og kompetanse på analyseobjektet er tilgjengelig. Blant annet kan følgende dimensjoner være relevante:

- Beredskapsstab (beredskapsleder, beredskapskoordinator, operativ leder, innsatsleder og utførende personell).
- Drift og vedlikehold.
- Transport og logistikk.
- Eksterne leverandører
- …

Klargjøring av analyseskjema og sjekklister

Det besluttes å gjennomføre en strukturert grovanalyse for ROS-analysen av transportberedskapen. Før analysemøtet har vi utarbeidet analyseskjema og sjekklister. I tillegg til analyseskjemaet og den generelle sjekklisten etablert i ”Veiledning i ROS-analyser for kraftforsyningen” (NVE og Proactima 2010) har selskapet etablert en egen sjekkliste for transportberedskap. Se nærmere i vedlegg 1.

Den vedlagte sjekklisten beskriver ulike komponenter / del-elementer i transportberedskapen vår, samtidig som den lister opp kjente uønskede hendelser.

Risiko- og sårbarhetsvurdering

Risiko- og sårbarhetsvurderingen gjennomføres i et analysemøte hvor relevant kompetanse fra selskapet, evt. også eksterne aktøre, er til stede.

Figur 15 på neste side gir eksempel på et utfylt analyseskjema hvor noen typiske hendelser relevant i forhold til transportberedskap er vurdert.

> ! **Selskapet har etablert avtaler med eksterne leverandører. Må slike avtaler også vurderes?**
> Det er også viktig å ta hensyn til eksterne forhold ifm. ROS-analyse av transportberedskap. Dette kan være forhold som begrensninger i felles beredskapsressurser eller kapasitet hos underleverandører / driftsselskap.

Analyseobjekt: Transportberedskap

Gjennomført av: Energiselskapet AS **Dato:** 12.07.2010

Formål: ROS-analysen av transportberedskap har som formål å vurdere tilgjengeligheten av etablert transportberedskap.

System		Uønsket hendelse	Risiko- og sårbarhetsvurdering								Risikohåndtering		
			Beskrivelse / begrunnelse	Årsaker	Sannsynlighet / frekvens	Konsekvens; 5: svært alvorlig, 1: ubetydelig			Usikkerhet (sett kryss)	Sårbarhetsvurdering			
ID	Delsystem / komponent	Navngi uønsket hendelse	Nærmere beskrivelse av hendelsen. Kommentarer og diskusjon som ligger til grunn for valgt frekvens og konsekvens	- årsak til hendelse - særskilte forhold - avvik fra regelverk ...	5: > 1 gang pr. år 4: 1 gang pr. år - hvert 10. år 3: hvert 10. år - hvert 100. år 2: hvert 100. år - hvert 1000. år 1: < hvert 1000. år	K1: **Forsyningssikkerhet:** bortfall av strøm/ antall sluttbrukere berørt	K2:	K3:		Beskrivelse av sårbarhet - forventet nedetid - finnes reservedeler på lager? - hvor kritisk er komponenten?	Eksisterende barrierer **NB!** Forutsetninger for angitt risikonivå	Foreslåtte barrierer / tiltak	Styrbarhet: - høy - medium - lav
...	...	...	...	...	...	...	...	...	...	...	...	...	...
2.0	Sjåfør	Eget transportpersonell er ikke tilgjengelig ved behov.	Transport av "lettere" beredskapsmateriell skjer ved benyttelse av egne kjøretøy. Kun to personer i selskapet har sertifikat for denne typen kjøretøy.	Ferieavvikling, sykdom (pandemi), streik	3: hvert 10. år - hvert 100. år	3. Middels. Noen lokale konsekvenser for privatabonnementer. Avbrudd < 10 timer hos < 1000 sluttbrukere eller ≥ 10 timer hos < 10 sluttbrukere.	-	-		Selskapet vil være avhengig av å skaffe til veie eksternt personell dersom hendelsen skulle inntreffe, noe som vil forlenget utkoblingstid på inntil 24 timer.	1. Etablert kapasitet i kraftselskapet. 2. Personell som inngår i vaktordning har sertifikat på tyngre kjøretøy.	1. Kjøretøyopplæring (tyngre kjøretøy) av flere egne ansatte. 2. Etablere egne avtaler med transportselskap(er).	Høy
3.0	Tyngre kjøretøy (ekstern)	Kontraktør (transport) har ikke tilgjengelig tyngre kjøretøy ved behov	Energiselskapet har etablert avtale med Norske Transportselskap. I følge avtalen skal selskapet stille til rådighet kjøretøy for transport av særskilt lange/tunge gjenstander (inntil 10 meter). Selskapet selger denne kapasiteten til flere kraftselskap i regionen, samtidig som kjøretøyet også benyttes til andre oppdrag. Typiske fraktoppdrag: mast/ samleskinner.	Fellesfeil, ekstremvær som fører til at uønskede hendelser ved flere kraftanlegg i regionen (ulike kraftselskap). Avtalebrudd, kontraktør kan ikke stille til rådighet kjøretøy i henhold til avtale.	3: hvert 10. år - hvert 100. år	5. Svært alvorlig. Samfunnsviktige funksjoner som liv og helse, samt viktig infrastruktur rammet / satt ut av funksjon. Avbrud ≥ 10 timer hos ≥ 1000 sluttbrukere.	-	-	X	Selskapet er avhengig at denne typen tyngre kjøretøy er tilgjengelig for transport av større komponenter til transformatorstasjoner. I en akutt situasjon vil det være vanskelig å andre egnede kjøretøy. Dette kan i verste fall gi utkoblingstid på inntil 48 timer i påvente av alternative transportmidler.	1. Etablert kontrakt med Norske Transportselskap, ref. beredskapsplan.	1. Sikre prioritet hos Norske Transportselskap i situasjoner med konkurrerende "kunder". 2. Vurdere alternative tilbydere av denne typen transporttjenester. 3. Inngå kontrakt med ytterligere ett transportselskap (redundans).	Middels
4.0	Ferje (transport over sjø)	Ferje/kai er ikke dimensjonert til transporter av større komponenter (f.eks. transformator).	Ferjesamband som benyttes fra beredskapslager til Kraftverk H har fått redusert kapasitet. Nyåpning av bro lenger inne i fjorden har medført at en mindre ferje er satt inn i dette sambandet.	Innsatt ferje har redusert lastekapasitet. Mangelfullt vedlikehold av kaianlegg har ført til restriksjoner på maks tillatt aksellast på kaianlegg.	5. > 1 gang pr. år	3. Middels. Noen lokale konsekvenser for privatabonnementer. Avbrudd < 10 timer hos < 1000 sluttbrukere eller ≥ 10 timer hos < 10 sluttbrukere.	-	-		Ikke avbrudd i strømforsyning for by A dersom det er tilstrekkelig kapasitet fra overordnet nett. Mer utsatt i høylastperioder hvor det kan bli behov for seksjonering av enkelte områder.	1. En del beredskapsmateriell er lagret ved kraftverket.	1. Etablere avtale med alternativ transportør av større komponenter (eks. Statnett Transport). 2. Ha en del større komponenter som del av beredskapsmateriell ved anlegget.	Lav
...	...	...	...	...	...	...	...	...	...	...	...	...	...

Figur 15 Eksempel på analyseskjema for transportberedskap.

Risikopresentasjon

Resultatene fra risiko- og sårbarhetsvurderingen kan også her presenteres ved bruk av risikomatriser. Risikomatrisen for forsyningssikkerhet som presentert i Figur 16 angir plassering av de tre hendelsene som ble kartlagt i eksempelet over.

		Konsekvens for forsyningssikkerhet				
		1: Ubetydelig. *Ikke avbrudd i strømforsyning.*	***2: Liten.*** *Ingen samfunns-konsekvenser. Avbrudd < 10 timer hos < 10 sluttbrukere.*	***3: Middels.*** *Noen lokale konsekvenser for privatabonnenter. Avbrudd < 10 timer hos < 1000 sluttbrukere eller ≥ 10 t hos < 10 sluttbrukere.*	***4: Alvorlig.*** *Alvorlige konsekvenser i infrastruktur og lokalsamfunnet. Avbrudd ≥ 10 timer hos < 1000 sluttbrukere.*	***5: Svært alvorlig*** *Samfunnsviktige funksjoner som liv og helse, samt viktig infrastruktur rammet / satt ut av funksjon. Avbrudd ≥ 10 timer hos ≥ 1000 sluttbrukere.*
Frekvens/ sannsynlighet	*5:Oftere enn 1 gang pr. år*			4.0^{L}		
	4: Fra 1 gang pr. år til hvert 10.år					
	3: Fra hvert 10.år til hvert 100.år			2.0^{H}		**3.0^{M}**
	2: Fra hvert 100.år til hvert 1000.år					
	1: Sjeldnere enn hvert 1000.år					

Figur 16 Eksempel på risikomatrise for transportberedskap.

Vi ser at to av de tre hendelsene er vurdert så kritiske at de er plassert i rødt område, samtidig som den tredje hendelsen er plassert i gult område.

Risikohåndtering

Plasseringen av de ulike hendelsene er ofte med på å gi noen føringer på hvilke hendelser som risikoreduserende tiltak bør vurderes. I tillegg til plassering bør en også ta hensyn til usikkerhet og styrbarhet når tiltak vurderes.

Hendelser med høy usikkerhet er angitt i matrisen over med uthevet skrift (eks. ID 3.0). For å kunne fortelle noe om påvirkningskraften som selskapet har på de ulike hendelsene har vi indikert styrbarhet ved å markere hendelsen med H (høy), M (middels), L (lav).

Sårbarhet

Gjennom ROS-analysen ble det også kartlagt sårbarheter i forhold til transportberedskapen. Slike sårbarheter kan enten presenteres i form av den fulle beskrivelsen fra analyseskjemaet, eller i stikkordsform. Oversikt over identifiserte sårbarheter i forhold til transportberedskap:

- Begrenset tilgang til eget personell (tyngre kjøretøy).
- Etablert kontrakt med bare en transportleverandør (tyngre kjøretøy).

Oppsummering

Med utgangspunkt i selskapets nivå 1 og nivå 2 ROS-analyser for selskapets anlegg hadde Energiselskapet allerede utarbeidet en plan for transportberedskap. Eksempelet over viser hvordan en videre kan benytte ROS-analyse til å kartlegge uønskede hendelser som kan påvirke tilgjengeligheten

på de ressursene som inngår i transportberedskapen. Resultatene benyttes til å øke robustheten i den etablerte beredskapsplanen.

Fra eksempelet ser vi at vi kan gjøre selskapets transportberedskap mer robust ved å øke tilgangen på interne ressurser som kan håndtere selskapets egne tyngre kjøretøy, eller etablere kontrakt med ytterligere en transportleverandør.

5.2 Eksempel på ROS-analyse av fysisk sikring (nivå 1)

5.2.1 Krav til sikkerhetsnivå og sikkerhetstiltak

Eierne av anlegg som omfattes av energilovforskriften § 6-3 skal være sikret mot uønskede hendelser og handlinger. Selv for anlegg som ikke er klassifisert er det en forventning om at eier av anlegget kan fremvise en dokumentert vurdering (ROS-analyse) vedrørende nødvendige sikkerhetstiltak.

ROS-analysen har som formål å kartlegge forhold som kan true den etablerte sikringen av anleggene, og som har konsekvens for forsyningssikkerhet. Felles systemer som vurderes kan eksempelvis være overvåknings- og varslingssystemer, inspeksjonsrutiner eller adgangskontrollrutiner.

For klassifiserte anlegg er det definert egne krav til fysisk sikring, deteksjon og reaksjon. Her henvises det også til Veiledning til forskrift om beredskap i kraftforsyningen (NVE, 2011).

5.2.2 ROS-analyse av fysisk sikring

Planlegging

Formål og omfang

Formålet med ROS-analysen er å danne grunnlag for helhetlig sikkerhetstenkning i virksomheten samtidig som en sikrer at kravene til sikringstiltak er ivaretatt (ref. beredskapsforskriften § 5.5). Denne ROS-analysen tar for seg transformatorstasjoner som er klassifiserte som anlegg i klasse 3.

Forutsetninger og antagelser

Det forutsettes at anleggenes klassifisering er vurdert og kjent. Det forutsettes også at anleggene tilfredsstiller minimumskravene til sikring som definert i beredskapsforskriften.

Valg av konsekvens- og sannsynlighetsdimensjon

Fokuset for denne ROS-analysen er å kartlegge forhold som er vesentlige for sikring av anleggene. Sikring av anlegget skal hindre at uvedkommende får anledning til å ta seg inn på anlegget, eller kan volde anlegget skade som kan resultere avbrutt levering av strøm. Av den grunn vil ROS-analysen først og fremst ha fokus på konsekvensdimensjonen forsyningssikkerhet.

Informasjonsinnhenting

I forbindelse med informasjonsinnhenting bør en typisk skaffe til veie:

- Overordnet ROS-analyse for selskapets anlegg (nivå 1).
- Informasjon vedrørende klassifisering av anlegg.
- Tidligere ROS-analyser for anleggene.
- Andre relevante opplysninger om anleggene (skisser, tegninger etc.).
- Kart over områdene.
- "Nabolagsprofiler" (informasjon om bebyggelse i området eller infrastruktur i området).
- Trusselvurdering fra lokalt politi
- …

Analysegruppe

Som for andre ROS-analyser er det viktig å sikre at personell med kunnskap og kompetanse på analyseobjektene er tilgjengelig. Blant annet kan følgende disipliner være relevante:

- Bygg og anlegg.
- Drift og vedlikehold.
- IT og radio- /telekommunikasjon.
- Sikkerhet og beredskap.
- …

Klargjøring av analyseskjema og sjekklister

Det tas her utgangspunkt i generell sjekkliste etablert i "Veiledning i ROS-analyser for kraftforsyningen" (NVE og Proactima 2010), samt egen sjekkliste for perimetersikring, ref. vedlegg 1.

Den vedlagte sjekklisten beskriver typiske komponenter / del-elementer som utgjør sikring av anlegg. Komponentene som er identifisert i sjekklisten danner også grunnlag for den strukturerte gjennomgangen. For en oversikt over kjente farer og uønskede hendelser henvises det til den generelle sjekklisten.

Risiko- og sårbarhetsvurdering

Risiko- og sårbarhetsvurdering gjennomføres i et analysemøte hvor relevant kompetanse er til stede.

Det finnes en rekke forhold som skal vurderes rundt sikring av anleggene. Blant annet; beliggenhet, klassifisering, teknisk løsning (fjellanlegg, uteanlegg), alder på anlegg, omgivelsene rundt anlegget osv.

Figur 17 gir eksempel på et utfylt analyseskjema hvor noen typiske hendelser relevant i forhold til fysisk sikring er vurdert.

Analyseobjekt: Skallsikring, Klasse 3 anlegg

Gjennomført av: Energiselskapet AS **Dato:** 12.07.2010

Formål: Formålet med ROS-analysen er å danne grunnlag for helhetlig sikkerhetstenkning og sikre at kravene til sikringstiltak er ivaretatt.

System		Uønsket hendelse	Risiko- og sårbarhetsvurdering								Risikohåndtering		
			Beskrivelse / begrunnelse	Årsaker	Sannsynlighet / frekvens	Konsekvens; 5: svært alvorlig, 1: ubetydelig			Usikkerhet (sett kryss)	Sårbarhetsvurdering			
ID	Delsystem / komponent	Navngi uønsket hendelse	Nærmere beskrivelse av hendelsen. Kommentarer og diskusjon som ligger til grunn for valgt frekvens og konsekvens	- årsak til hendelse - særskilte forhold - avvik fra regelverk ...	5: > 1 gang pr. år 4: 1 gang pr. år - hvert 10. år 3: hvert 10. år - hvert 100. år 2: hvert 100. år - hvert 1000. år 1: < hvert 1000. år	K1: **Forsyningssikkerhet**: bortfall av strøm/ antall sluttbrukere berørt	K2:	K3:		Beskrivelse av sårbarhet - forventet nedetid - finnes reservedeler på lager? - hvor kritisk er komponenten?	Eksisterende barrierer **NB!** Forutsetninger for angitt risikonivå	Foreslåtte barrierer / tiltak	Styrbarhet: - høy - medium - lav
...	...	...	...	...	...	...	...	...	...	...	...	...	...
3.0	Trafostasjon/ bygg og anlegg	Sabotasje	Selskapet har kontroll over en rekke transformatorstasjoner i klasse 3, og er er viktig for kraftforsyningen i regionen. Tilgang til informasjon om anlegget og forsyningslinjer synes lett tilgjengelig på internett (google maps etc.)	Terrorlignende handlinger/ krigssituasjon	1: < hvert 1000. år	5: Svært alvorlig Samfunnsviktige funksjoner som liv og helse, samt viktig infrastruktur rammet / satt ut av funksjon. Avbrudd ≥ 10 timer hos ≥ 1000 sluttbrukere.				Transformatorstasjoner i klasse 3 vil normalt kunne medføre lengre utkoblingstid for et høyt antall kunder dersom skader på anlegget er omfattende. Gjerne utkoblingstid på inntil 48 timer.	1. Passiv sikring installert, gjerder, lås, sikkerhetsglass i vinduer	1. Installere veibom, betongblokker, samt annen kraftigere fysisk sikring 2. Etablere	Lav
3.1	Trafostasjon/ bygg og anlegg	Uvedkommende på anlegget oppdages ikke straks	Det er ikke installert overvåkningsutstyr på selskapet transformatorstasjoner som muliggjør deteksjon av uvedkommende på anlegget. Etablert sikring synes ikke å tilfredsstille kravene til sikringsnivå i forskriften. Selskapet har opplevd at uvedkommende har vært inne på denne typen anlegg. Tyveri av utstyr har forekommet, men ikke sabotasje eller hærverk.	Overvåkningsutstyr ikke installert, Avbrutt tele-/ datakommunikasjon mot driftssentral	3: hvert 10. år - hvert 100. år	4: Alvorlig. Alvorlige konsekvenser i infrastruktur og lokalsamfunnet. Avbrudd ≥ 10 timer hos < 1000 sluttbrukere.				Mangelfull overvåkning av anleggene gir anledning for uvedkommende å gjøre større skader på anlegget før dette oppdages.	1. Passiv sikring installert, gjerder, lås, sikkerhetsglass i vinduer	1. Installasjon av alarm og overvåkningsutstyr som tilfredsstiller FG-normen.	Høy
3.2	Trafostasjon/ bygg og anlegg	Havari av transformator, koblingsanlegg eller vern	Energiselskapet har etablert gode rutiner for tildeling og kontroll av nøkler til selskapets anlegg. Enkelte kontraktører tildeles egne nøkler mot formell godkjennelse, men Energiselskapet har i praksis liten kontroll på hvem som oppbevarer disse.	Mangelfull adgangskontroll, Kopiering av utdelte nøkler	2: hvert 100. år - hvert 1000. år	4: Alvorlig. Alvorlige konsekvenser i infrastruktur og lokalsamfunnet. Avbrudd ≥ 10 timer hos < 1000 sluttbrukere.			X	Uvedkommende med nøkler til anlegget kan volde stor skade på anlegget før dette detekteres av driftssentral da det ikke er installert overvåkningskamera eller alarmsystemer på anleggene. I verste fall kan dette gi utkoblingstid på opp til 24 timer. (Se forøvrig også punkt 3.1)	1. Dagens etablerte adgangskontroll-rutiner	1. Etablere tidsbegrenset elektronisk adgangskontroll for kontraktører 2. Kun gi adgang til anlegg sammen med selskapets ansatte. 3.	Høy
...	...			...	...		...	...	...	...	...	...	...

Figur 17 Eksempel på analyseskjema for fysisk sikring.

Risikopresentasjon

Risikobildet kan presenteres ved bruk av en risikomatrise. De tre hendelsene fra analyseskjemaet er her presentert i risikomatrisen i Figur 18. Det er vurdert å være høy usikkerhet knyttet til konsekvensene av den uønskede hendelsen havari av transformator, koblingsanlegg eller vern (ID 3.2). Dette skyldes at hendelsen også kan få mindre eller mer alvorlige konsekvenser avhengig av tiden som uvedkommende har til rådighet for å volde skade på anlegget før de blir oppdaget.

		Konsekvens for forsyningssikkerhet				
		1: Ubetydelig. *Ikke avbrudd i strømforsyning.*	***2: Liten.*** *Ingen samfunns-konsekvenser. Avbrudd < 10 timer hos < 10 sluttbrukere.*	***3: Middels.*** *Noen lokale konsekvenser for privatabonnenter. Avbrudd < 10 timer hos < 1000 sluttbrukere eller ≥ 10 t hos < 10 sluttbrukere.*	***4: Alvorlig.*** *Alvorlige konsekvenser i infrastruktur og lokalsamfunnet. Avbrudd ≥ 10 timer hos < 1000 sluttbrukere.*	***5: Svært alvorlig*** *Samfunnsviktige funksjoner som liv og helse, samt viktig infrastruktur rammet / satt ut av funksjon. Avbrudd ≥ 10 timer hos ≥ 1000 sluttbrukere.*
Frekvens/ sannsynlighet	*5:Oftere enn 1 gang pr. år*					
	4: Fra 1 gang pr. år til hvert 10.år					
	3: Fra hvert 10.år til hvert 100.år				3.1^{H}	
	2: Fra hvert 100.år til hvert 1000.år				**3.2^{H}**	
	1: Sjeldnere enn hvert 1000.år					3.0^{L}

Figur 18 Eksempel risikomatrise fysisk sikring.

Risikohåndtering

Formålet med ROS-analysen var å danne grunnlag for en helhetlig sikkerhetstenkning i virksomheten, samt å verifisere at kravene til sikkerhetstiltak er ivaretatt. I forhold til sikkerhetstenkning og krav til sikkerhetstiltak ser Energiselskapet at ROS-analysen har identifisert at kravene til sikring for deres klasse 3 anlegg ikke tilfredsstiller kravene i gjeldende regelverk (ref. ID 3.1).

Begrenset mulighet for deteksjon av inntrengere gir også utslag på flere av de identifiserte risikoene, og er åpenbart et forhold hvor tiltak må vurderes. Særlig med tanke på at hendelsen synes å ha høy styrbarhet ved at alarm- / overvåkningsutstyr relativt enkelt kan anskaffes.

Sårbarhet

Gjennom ROS-analysen ble det også kartlagt en rekke sårbarheter. Vi har listet noen av disse under. For en fullstendig beskrivelse av sårbarhet refereres det til analyseskjemaet.

- Transformatorstasjonen er ett av to kritiske anlegg med tanke på kraftforsyning til by A og en større region rundt.
- Uvedkommende kan ha anledning til å volde stor skade på anlegget før dette detekteres av driftssentral da det ikke er installert overvåkningskamera eller alarmsystemer på anleggene.

Oppsummering

ROS-analysen ble brukt for å vurdere selskapets felles systemer for sikring av anlegg. Felles systemer som ble vurdert i eksempelet var overvåknings- og varslingssystemer, informasjonstilgang og adgangskontrollrutiner. ROS-analysen viser at en del felles systemer og gode interne rutiner er etablert av selskapet, men avdekket samtidig flere uønskede hendelser samt avvik fra regelverket som selskapet må håndtere.

6 Eksempel på fremstilling og håndtering av risiko

Risiko- og sårbarhetsvurdering

Presentere risikobilde

Resultatene fra risiko- og sårbarhetsvurderingen kan som tidligere beskrevet presenteres ved bruk av risikomatriser. Et eksempel på dette er vist i Figur 19. Hendelsene plottes med løpenummeret som ble benyttet i analyseloggen. Uthevet skrift indikerer usikkerhet, mens H, M, L indikerer grad av styrbarhet.

Det finnes også andre måter å plotte denne informasjonen i en risikomatrise. Eksempelvis kan det brukes andre tegn for usikkerhet, og grad av styrbarhet kan illustreres med f.eks. liten, middels eller stor boble rundt løpenummeret, eller med en sirkel (liten styrbarhet), trekant (middels styrbarhet) eller firkant (stor styrbarhet).

		Konsekvens for forsyningssikkerhet				
		1: Ubetydelig. *Ikke avbrudd i strømforsyning.*	***2: Liten.*** *Ingen samfunns-konsekvenser. Avbrudd < 10 timer hos < 10 sluttbrukere.*	***3: Middels.*** *Noen lokale konsekvenser for privatabonnenter. Avbrudd < 10 timer hos < 1000 sluttbrukere eller ≥ 10 t hos < 10 sluttbrukere.*	***4: Alvorlig.*** *Alvorlige konsekvenser i infrastruktur og lokalsamfunnet. Avbrudd ≥ 10 timer hos < 1000 sluttbrukere.*	***5: Svært alvorlig*** *Samfunnsviktige funksjoner som liv og helse, samt viktig infrastruktur rammet / satt ut av funksjon. Avbrudd ≥ 10 timer hos ≥ 1000 sluttbrukere.*
Frekvens/ sannsynlighet	*5:Oftere enn 1 gang pr. år*					
	4: Fra 1 gang pr. år til hvert 10.år					
	3: Fra hvert 10.år til hvert 100.år					1.0 L
	2: Fra hvert 100.år til hvert 1000.år		4.0 M			
	1: Sjeldnere enn hvert 1000.år				**3.0** H	2.0 H

Figur 19 Eksempel på hvordan resultatene fra en risiko- og sårbarhetsvurdering kan presenteres ved bruk av risikomatrise.

Det finnes også andre måter å presentere risikobildet på. Eksempelvis kan risikobildet illustreres i et risiko- og styrbarhetsdiagram, der risiko vises på den ene aksen og styrbarhet på den andre. På denne måten kommer styrbarheten godt frem. En ulempe med en slik fremvisning kan være at hendelser med alvorlige konsekvenser, men som er vurdert å være sjeldne, ikke kommer tydelig nok frem.

Risikohåndtering

Tiltaksanalyse, beslutnings- og tiltaksplan

I henhold til beredskapsforskriften skal man fokusere på hendelser med store konsekvenser, selv om disse er vurdert å være sjeldne hendelser. Dvs. man skal ikke kun fokusere på hendelser forbundet med høy risiko, dvs. hendelsene som ligger i øverste høyre hjørne i risikomatrisen, men også de hendelsene som ligger i nederste høyre hjørne i risikomatrisen. Når tiltak skal prioriteres, er det ofte hensiktsmessig å begynne med de hendelsene som er vurdert å kunne medføre store konsekvenser.

! Ta med usikkerhet og styrbarhet i vurderingen når du bestemmer hvilke hendelser du vil redusere risikoen for.

Høy usikkerhet viser at den uønskede hendelsen kan gi andre konsekvenser, mens grad av styrbarhet viser hva vi faktisk kan gjøre noe med.
Fra eksempelet som er presentert i risikomatrisen i Figur 19 kan dette for eksempel gi følgende prioritering av uønskede hendelser for iverksetting av tiltak:

1. ID 2.0
2. ID 3.0
3. ID 1.0
4. ID 4.0
5. …
6. …

Denne prioriteringen er basert på plassering i risikomatrisen, sammen med en vurdering av usikkerhet og styrbarhet. I tillegg kan det være relevant å gjennomføre effektivitetsvurderinger og/eller kost-effektivitetsvurderinger av potensielle tiltak. Basert på dette bør det etableres en beslutnings- og tiltaksplan.

! Å avgjøre hvilke tiltak som skal implementeres, er en ledelsesbeslutning.

Beredskapsanalyse og beredskapsplan
ROS-analysene bør også danne bakgrunn for beredskapsplaner som selskapet må etablere. ROS-analysen gir bl.a. innspill til hvilke scenarioer beredskapen skal dimensjoneres for og som skal øves, samt hvor ofte og under hvilke forhold det skal øves.

Oppfølging
Oppfølging av resultatene fra ROS-analysene og iverksetting av tiltak er en viktig del av ledelsens ansvarsområde. Det er viktig å synliggjøre for ledelsen at enkelte oppfølgingsbehov er direkte knyttet til pliktene i beredskapsforskriften.

! For å sikre et kontinuerlig fokus anbefaler vi at oppdatert risikobilde, endring i risikobilde og status på aksjoner og tiltak inngår som et fast punkt på hvert ledermøte.

7 Referanser

- ✓ Aven, T., Røed, W., Wiencke, H.S. (2008). *Risikoanalyse*. Oslo: Universitetsforlaget.
- ✓ Energi Norge & Proactima (2010). *Veileder i helhetlig risikostyring for kraftbransjen.* Publikasjonsnummer 307-2010.
- ✓ Norges vassdrags- og energidirektorat & Proactima (2010). *Veiledning i risiko- og sårbarhetsanalyse i kraftforsyningen.* Juli 2010.
- ✓ Norges vassdrags- og energidirektorat (2002). *Forskrift om beredskap i kraftforsyningen (beredskapsforskriften).* FOR 2002-12-16 nr 1606.
- ✓ Norges vassdrags- og energidirektorat (2011). *Veiledning til forskrift om beredskap i kraftforsyningen.* Veileder nr 1-2011.
- ✓ NS (2008). *NS 5814:2008. Krav til risikovurderinger.*
- ✓ Pedersen, L.M. og Thorstad, H.H. (2008). *Risk analysis of the electric power transmission grid.* European Safety and Reliability Conference (ESREL). Valencia, Spania 2008.
- ✓ NVE rapport 3:2012 “Første inntrykk etter ekstremværet Dagmar, julen 2011”
- ✓ NVE rapport 6:2010 ”Klimautfordringer i kraftsektoren frem mot 2100, R. Steen, mfl.

Vedlegg 1 – Sjekklister

Sjekkliste: Transportberedskap*		
Del-elementer / komponenter		
Eksterne ressurser Personell	Personbil Lastebil Helikopter Ferje Snøscooter Mobilkran Leggefartøy Sjåfør Drivstoffanlegg Drivstoff …	Opp- og avlastningssted Transportrute Vei Jernbanenett Kai Kjørelem Reservedeler
Uønskede hendelser		
Kjøretøy ikke tilgjengelig Kjøretøy ikke riktig dimensjon Sjåfør ikke tilgjengelig Drivstoff ikke tilgjengelig …	Transportrute ikke tilgjengelig Reservedeler ikke tilgjengelig	

Sjekkliste: Perimetersikring*		
Del-elementer / komponenter		
Port Portstolper Lås Mellomrom mellom tofløyd port Veibom Kantstein Betongblokker …	Gjerde Gjerdeduk Gjerdestolper Piggtråd Topptråd Bunntråd	Overvåkings- og alarmsystemer Belysning av uteområde Høyttaleranlegg Porttelefon Observasjonsstillinger
Hendelser		
Se generell sjekkliste		

*Det er viktig å merke seg at sjekklistene som er presentert over ikke er utfyllende. Etter hvert som det gjennomføres ROS-analyser vil det bli gjort kjent en rekke nye komponenter av betydning eller uønskede hendelser. Det er da viktig at sjekklistene oppdateres for å sikre erfaringsoverføring.

Vedlegg 2 – Prosessleder tips

Nedenfor gis enkelte tips i forbindelse med gjennomføring av en ROS-analyse. Tipsene gir momenter som det er viktig for prosessleder å huske på, og er ikke en komplett gjennomgang av ROS-analyseprosessen. Det vises også til "Veiledning i ROS-analyser for kraftforsyningen" (NVE og Proactima 2010).

Planlegging

Det er prosessleders ansvar å planlegge ROS-analysen. Før gjennomføring av en ROS-analyse er det viktig å definere formål og omfang av analysen og forankre analysen hos ledelsen. Hva skal resultatene fra analysen brukes til? Hva er det som skal analyseres? Hvilke beslutninger skal fattes? Konsekvens- og sannsynlighetsdimensjoner og kategorier må også avklares. Informasjonsunderlag må hentes inn og det må vurderes hvem som bør delta i arbeidsgruppen som skal jobbe med ROS-analysen, for å sikre riktig kompetanse.

Ofte er det hensiktsmessig å gjennomføre et analysemøte som en del av ROS-analysen. Som en del av forberedelsene til samlingen, bør mulige hendelser identifiseres, objekter, systemer osv kartlegges, videre bør analyseobjektet deles inn i delelementer / aktiviteter, sjekklister må utarbeides og analyseskjemaet bør testes ut på forhånd. I analysemøtet er det ofte nyttig å ha tegninger / skjema av analyseobjektet vist på skjerm eller hengende på veggen. Dette må også forberedes før analysemøtet.

! Ofte fokuseres det mye på selve risikovurderingen (gjennomføringen), noe som begrenser tilgjengelig tid til planlegging og oppfølging. Som en tommelfingerregel bør 1/3 av tiden settes av til planlegging, 1/3 til risiko- og sårbarhetsvurdering og 1/3 til risikohåndtering og oppfølging av resultater, herunder risikoreduserende tiltak.

Deltagelse

De som deltar bør ha bred fagkunnskap og erfaring tilknyttet de områder som inngår i analysen for å sikre god kvalitet. Det kan i tillegg til egne ressurser bli aktuelt å hente kompetanse utenfra der det kommer opp tema man selv har lite kunnskap om eller erfaring med. Klassiske enmannsutredninger er ofte lite hensiktsmessig innen denne type analyser.
Ekstern deltakelse kan også gjøres ved for eksempel referansegrupper tilpasset lokale forhold, tema for analysen og arbeidets omfang. Referansegruppen(e)s oppgave er å bidra til å gi en bredere kompetanse og sikre en tverrfaglig plattform til de vurderinger og analyser som foretas.

Kompetanse og informasjon kan hentes fra:

- Egne ansattes kunnskap om virksomheten
- Dokumentasjon av anlegg
- Informasjon fra andre kraftlag
- Rapporterte hendelser i egne eller andres anlegg
- Tilsynsrapporter
- Uhells- og skadestatistikk
- Eksisterende avvikshåndterings- og beredskapsplaner
- Driftsdata
- KDS
- Forsknings- og evalueringsrapporter
- Informasjon og veiledning fra NVE
- Andre kilder
  - Kommunen
  - Brannvesen
  - IT- og teleleverandører
  - Fylkesmannen
  - …

Medvirkning

Redusert sårbarhet og risiko er ikke alltid noe virksomheten kan løse alene. Medvirkningsprosesser er en fin anledning til å få kundene (innbyggere og næringsliv) til å bli mer bevisste og oppmerksomme på hva de selv kan bidra med for å redusere egen sårbarhet. Medvirkning må tilpasses og organiseres i forhold til hvilke tema og omfang analysen er ment å dekke.

Forankring

Forankring av arbeidet med risiko og sårbarhet i den administrative ledelse er en selvfølge for å oppnå prioritering og gjennomføring av tiltak. På tilsvarende måte bør den administrative ledelsen søke forankring og involvering av eierne (styret) av virksomheten da det essensielle spørsmålet rundt dette arbeidet handler om tjenesteproduksjonen og inntektsgrunnlaget for virksomheten, og forsyningssikkerheten for samfunnet.

Risiko- og sårbarhetsvurdering

Hvordan komme i gang?
Det er ofte hensiktsmessig å begynne analysemøtet med en kort presentasjon av analyseobjektet, samt en kort presentasjon av deltakerne i møtet dersom ikke alle er godt kjent. Det er viktig at alle i analysegruppen blir gjort oppmerksomme på deres rolle i ROS-analyseprosessen. Videre er det prosessleders ansvar å sikre en felles forståelse av hva som er formålet med ROS-analysen, hva som skal analyseres og hvordan dette skal gjøres, tidlig i analysemøtet.

Ofte har møtedeltakerne før møtet tenkt igjennom ulike ting som ”kan gå galt” ved anlegget eller aktiviteten som skal analyseres. Det er viktig at denne informasjonen blir dokumentert nokså tidlig i møtet mens den ennå sitter friskt i minnet. Vi anbefaler derfor følgende fremgangsmåte for identifikasjon av farer, trusler og uønskede hendelser:

- Idédugnad. Møtedeltakerne gis mulighet til å ”tømme hodene”.
- Strukturert gjennomgang av anlegget – farer, trusler og uønskede hendelser for delelementer og komponenter identifiseres.
- Gjennomgang av sjekklisten.

Hvordan sikre fremdrift?
Som prosessleder er det din oppgave å sikre fremdrift / passe tiden. Fokuser og prioriter tiden slik at nok tid blir satt av til de viktige, alvorlige hendelsene. Gå raskere igjennom hendelser med mindre alvorlig konsekvens.
Det finnes ulike måter å legge opp den strukturerte gjennomgangen på. En løsning er å først gå igjennom og sjekke at alle delelementer, samt farer, trusler og uønskede hendelser relatert til disse er identifisert før risiko- og sårbarhetsvurderingen av de ulike uønskede hendelsene gjøres. En annen løsning er å gjennomføre risiko- og sårbarhetsvurderingen av de ulike uønskede hendelsene samtidig med at disse identifiseres. Hvis formålet med analysen er å sammenligne to alternative løsninger, kan enten de to ulike løsningene vurderes hver for seg, eller de uønskede hendelsene som identifiseres for hver av de to ulike løsningene kan vurderes parallelt.

Hvordan involvere?
Som prosessleder er det din oppgave å stimulere analysegruppen til å tenke og beskrive hva som kan gå galt ved anlegget / aktiviteten. Du bør være bevisst på hvordan du stiller spørsmålene til analysegruppen. ”Hva kan gå galt med denne komponenten?”, ”Kan denne komponenten havarere?”, ”Hva skjer hvis …?”.
En god prosessleder snakker lite selv, men klarer likevel å oppnå at alle relevante deler av risiko- og sårbarhetsvurderingen blir diskutert. Dette oppnås ved målrettet valg av spørsmål. Vær nysgjerrig. Det er bedre å stille for mange spørsmål enn for få. ”Dumme” spørsmål kan ofte være smarte på den måten at analysegruppen tvinges til å tenke igjennom uvante problemstillinger.

Risikohåndtering

Beredskapsforskriften stiller krav til at ROS-analysene som gjennomføres skal dokumenteres på en systematisk måte, og raskt skal kunne hentes frem ved behov (jf. § 1-2 om krav til kvalitetssystem). Det er hensiktsmessig å dokumentere resultatene fra ROS-analysen i en rapport. I rapporten er det viktig at formålet og omfanget av analysen klart fremgår. Det er også viktig å tydeliggjøre forutsetninger, antakelser og avgrensninger for analysen. Vurderingene som er gjort, inklusive analyseskjemaet, må også dokumenteres i rapporten. Det er ofte hensiktsmessig å inkludere en systembeskrivelse / beskrivelse av analyseobjektet i rapporten. Informasjon som er funnet relevant for analysen, vedlegges eller refereres til i rapporten.

Eksempel på oppbygging av en ROS-analyserapport:

1. Oppsummering og konklusjon
2. Introduksjon m/ bakgrunn, formål, forutsetninger, avgresninger
3. Systembeskrivelse
4. Metodikk
5. Identifikasjon av farer, trusler og uønskede hendelser
6. Risikoanalyse og sårbarhetsvurdering
7. Identifikasjon av risikoreduserende tiltak
8. Presentasjon av risikobilde
9. Risikohåndtering – tiltaksanalyse, videre arbeid m.m.
10. Eventuelle vedlegg

Det er viktig å være klar over at spesielt sårbarhetsvurderinger som måtte fremgå av en ROS-analyse, raskt kan defineres som sensitiv informasjon om kraftforsyningen og av den grunn ikke kan offentliggjøres, jf. § 6.2 Beskyttelse av informasjon i henhold til beredskapsforskriften. Dette trenger ikke å angå hele ROS-analysen, men er ofte relevant for deler av den. Samtidig er det viktig å være bevisst på at mange samarbeidende virksomheter og myndigheter vil etterspørre relevant informasjon om kraftforsyningen for egne ROS-analyser. Her blir det viktig å tilby relevant informasjon, basert på den enkeltes behov, uten å gi fra seg sensitiv informasjon.

Denne serien utgis av Norges vassdrags- og energidirektorat (NVE)

Utgitt i Rapportserien i 2012

Nr. 1 Kvikkleireskred ved Esp, Byneset i Trondheim. Kari Øvrelid (20 s.)

Nr. 2 Årsrapport for tilsyn 2011 (40 s.)

Nr. 3 Første inntrykk etter ekstremværet Dagmar, julen 2011 (28 s.)

Nr. 4 Energy consumption. Energy consumption in mainland Norway (59 s.)

Nr. 5 Climate change impacts and uncertainties in flood risk management:
Examples from the North Sea Region (62 s.)

Nr. 6 Kvartalsrapport for kraftmarknaden. 4. kvartal 2011. Finn Erik Ljåstad Pettersen (red.) (86 s.)

Nr. 7 Statistikk over nettleie i regional- og distribusjonsnettet 2012. Inger Sætrang (53 s.)

Nr. 8 Flomrisikoplan for Gaula ved Melhus. Et eksempel på en flomrisikoplan etter EUs flomdirektiv (78 s.)

Nr. 9 Inntak Viddal – FoU-prosjekt på tilbakespyling. Sluttrapport. Jan Slapgård (31 s.)

Nr. 10 Oversikt over vedtak og utvalgte saker. Tariffer og vilkår for overføring av kraft 2011 (15 s.)

Nr. 11 Flomsonekart: Delprosjekt Ålen: Kjartan Orvedal, Julio Pereira

Nr. 12 NVEs årsmelding 2011

Nr. 13 Vannet vårt. Hydrologi i Norge 2011

Nr. 14 Capacity building in Hydrological Services Course in Water Level recording and Data Processing at Ministry of Water and Energy 13th – 16th February 2012. Documentation (23 s.)

Nr. 15 Landsomfattende mark- og grunnvannsnett. Drift og formidling 2011.
Jonatan Haga og Per Alve Glad (40 s.)

Nr. 16 Challenges in Flood Risk Management Planning. An example of a Flood Risk Management Plan for the Finnish-Norwegian River Tana. Eirin Annamo (59 s.)

Nr. 17 Kvartalsrapport for kraftmarknaden. 1. kvartal 2012. Finn Erik Ljåstad Pettersen (red.) (s.)

Nr. 18 Eksempelsamling. Risiko- og sårbarhetsanalyser

Norges
vassdrags- og
energidirektorat

Norges vassdrags- og energidirektorat

Middelthunsgate 29
Postboks 5091 Majorstuen
0301 Oslo

Telefon: 09575
Internett: www.nve.no