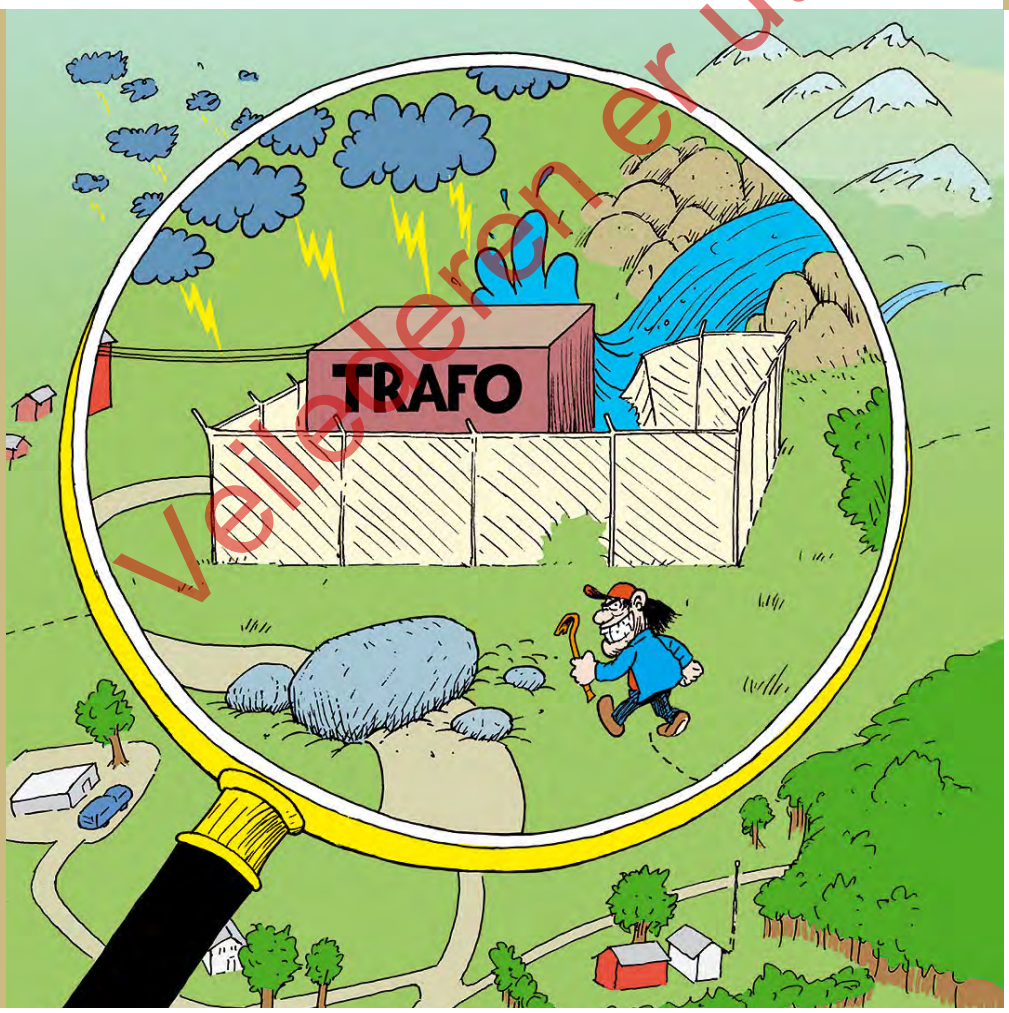
NVE

Veiledning i risiko- og sårbarhets-analyser for kraftforsyningen

Veilederen er utgått

2
2010

VEILEDER



Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen

- Et grunnlag for godt beredskapsarbeid -

Veilederen er utgått

Norges vassdrags- og energidirektorat
2010

Veileder nr: 2-2010

Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen

Utgitt av: Norges vassdrags- og energidirektorat

Forfatter: *NVE & Proactima*
Denne veiledningen er utarbeidet av Proactima på oppdrag av og i samarbeid med NVE 2010

Trykk: NVEs hustrykkeri
Opplag: 1000
Forsidefoto: Illustrasjon: Ola H. Hegdal, NVE alle rettigheter
ISBN:
ISSN: 1501-0678

Sammendrag: En innføring i hvordan bruke risiko- og sårbarhetsanalyser for å tilfredsstille kravene gitt av Forskrift om beredskap i kraftforsyningen.

Emneord: ROS, risikoanalyser, sårbarhetsanalyser, beredskapsforskriften, energiloven, forsyningssikkerhet, kraftforsyningen, fjernvarme, nettselskap, kraftproduksjon, damsikkerhet, vassdragsregulering, kraftforsyningens beredskapsorganisasjon (KBO), transportberedskap, driftskontroll, sensitiv informasjon, sambandsberedskap, adgangskontroll, sikring,

Språk Denne veiledningen er tilgjengelig på både nynorsk og bokmål, se NVEs nettsider www.nve.no for mer informasjon

Veilederen er utgått

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

Telefon: 22 95 95 95
Telefaks: 22 95 90 00
Internett: www.nve.no

Juli 2010

INNHOLDSFORTEGNELSE

Forord 5

1. Innledning 7

1.1 Hva skal vi med risiko- og sårbarhetsanalyser i kraftbransjen? 7
1.2 ROS-analyser og beredskap 8
1.3 Omfang og avgrensninger 9
1.3.1 Ekstraordinære hendelser: teknisk svikt, naturgitt skade og bevisst skadeverk 10

2 ROS-analyser – hva innebærer det? 11

2.1 Sentrale begreper 11
2.1.1 Risiko, sannsynlighet og usikkerhet 11
2.1.2 Forutsetninger og antagelser 11
2.1.3 Sårbarhet 11
2.1.4 Risiko- og sårbarhetsanalyse 12
2.1.5 Konsekvens 13
2.2 ROS-analyseprosessen 14
2.3 Kartlegge virksomhetens risikopotensiale - nivåinndeling 14
2.3.1 Nivå 1: Overordnet ROS-analyse 15
2.3.2 Nivå 2: ROS-analyse av anlegg og aktiviteter 16
2.3.3 Nivå 3: Detaljert ROS-analyse av delsystem eller komponenter 16

3 ROS-analyser i praksis – strukturert grovanalyse 17

3.1 Planlegging 17
3.1.1 Definere formål og omfang av analysen 18
3.1.2 Valg av konsekvens- og sannsynlighetsdimensjon 18
3.1.3 Informasjonsinnhenting 19
3.1.4 Organisering 20
3.1.5 Klargjøring av sjekklister og analyseskjema 21
3.2 Risiko- og sårbarhetsvurdering 23
3.2.1 Identifisere farer, trusler og uønskede hendelser 23
3.2.2 Risikoanalyse 25
3.2.3 Sårbarhetsvurderinger 28
3.2.4 Identifisere mulige risikoreduserende tiltak 28
3.2.5 Presentasjon av risikobildet 29
3.3 Risikohåndtering 31
3.3.1 Tiltaksanalyse 31
3.3.2 Beslutning og tiltaksplan 32
3.3.3 Beredskapsanalyse og beredskapsplan 33
3.3.4 Oppfølging 33
3.3.5 Sensitiv informasjon 33

Veilederen er utgått

4. Oppsummering: ROS-analyse steg for steg 34

5. Referanser.....35

Vedlegg 1 – Forslag til sjekklister..... 36
Vedlegg 2 – Forslag til analyseskjema og tiltaksplan 42
Vedlegg 3 – Ord og uttrykk 49
Vedlegg 4 – Relevante lover og forskrifter, de viktigste ROS-kravene i beredskapsforskriften 51

Veilederen er utgått

Forord

Denne veiledningen i bruk av risiko- og sårbarhetsanalyser (ROS) har sin bakgrunn i krav nedfelt i Forskrift om beredskap i kraftforsyningen (beredskapsforskriften), men er såpass generell at den med enkle tilpasninger også kan benyttes til å analysere i henhold til krav på andre kraftforsyningsrelevante områder regulert av energiloven, vannressursloven og forskrifter etter disse lovene. Fokuset og ikke minst eksempler i denne veiledningen er imidlertid primært rettet mot *hvordan bruke risiko- og sårbarhetsanalyser som et verktøy for etterlevelse av beredskapsforskriftens plikter.* Beredskapsforskriften legger tydelige føringer på at norsk kraftforsyning (strøm- og fjernvarmeforsyning, og vassdragsregulering) skal kartlegge og være beredt til å håndtere ekstraordinære hendelser. I denne sammenhengen handler det om å forebygge og håndtere hendelser som truer forsyningssikkerheten. Dette er gjerne hendelser som kan medføre alvorlige konsekvenser, ofte med lav sannsynlighet. Det er viktig å presisere at det er et forskriftskrav at ROS-analysene skal være oppdatert og dokumentert.

Utarbeidelse av slike analyser vil gi virksomheten en oversikt over risiko- og sårbarhetsforhold som kan redusere eller true virksomhetens evne til å fungere. Formålet med kravet til risiko- og sårbarhetsanalyser innbefatter at det enkelte selskap skal identifisere risiko og sårbarhet ved ekstraordinære hendelser knyttet til teknisk svikt, naturgitt skade og bevisst skadeverk. Videre ligger det også en plikt i forskriften til at analysen skal favne alle beredskapstiltak nevnt i forskriften. Dette betyr at man i tillegg til å kartlegge mulige hendelser som kan true kraftforsyningen, også har plikt til å kartlegge sårbarhet, for eksempel om pålagte beredskapstiltak vil kunne fungere under press og hvorvidt det vil være nødvendig med flere tiltak utover den pålagte grunnsikringen.

Den enkelte virksomhet står selv ansvarlig for å oppfylle krav til å kartlegge risiko- og sårbarhet, samt ha tilstrekkelig kompetanse til å utøve dette arbeidet. Dette innbefatter også valg av metodisk verktøy. Denne veiledningen er imidlertid ment som et hjelpemiddel for norsk kraftforsyning i arbeidet med etterlevelse av beredskapsforskriften. Det gjøres oppmerksom på at andre forskriftskrav i mindre grad er nevnt i denne veiledningen.

Målgruppen for denne veiledningen er virksomheter som er pliktig til å følge beredskapsforskriftens krav, og nærmere bestemt de personer som skal lede og delta i arbeidet med å utarbeide risiko- og sårbarhetsanalyser for å oppfylle forskriftens krav. Denne veiledningen er noe detaljert i sine forklaringer da hensikten også har vært å være til hjelp for de som ikke har jobbet med risiko- og sårbarhetsanalyser i større utstrekning tidligere. For de som er meget rutinerte i arbeidet med ROS-analyser iht beredskapsforskriftens krav vil i mindre grad ha behov for å lese de innledende kapitler og kan gå direkte til kapittel 3. Er man mindre rutinert, eller noe mer usikker på forskriftens forventinger til risiko- og sårbarhetsanalysearbeidet så vil de innledende kapitler gi nyttige råd på veien.

Denne veiledningen er utarbeidet i perioden 2008-2010 i samarbeid mellom en rekke virksomheter i kraftforsyningen, bransjeforeninger og NVE. Konsulentselskapet

Veilederen er utgått

Proactima (www.proactima.no) vant anbudskonkurransen knyttet til utarbeidelsen av denne veiledningen og har hatt hovedansvaret for å føre denne veiledningen i pennen i samarbeid med og under ledelse av NVE. Veiledningen har i tillegg vært sendt ut på en åpen høring og justert på en rekke områder i henhold til innkomne merknader.

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

Oslo, juli 2010

Agnar Aas
vassdrags- og
energidirektør

Veilederen er utgått

1. Innledning

Kraftforsyningen representerer en grunnleggende infrastruktur i et moderne samfunn. Selv kortvarige avbrudd kan medføre store konsekvenser for andre viktige samfunnsfunksjoner og den enkelte innbygger. Det er lang tradisjon for å stille strenge sikkerhetskrav til kraftforsyningen, og all avbruddsstatistikk tilsier at kraftforsyningen har lyktes med å bygge en robust infrastruktur med gjennomsnittlig få avbrudd per sluttbruker. Likevel har enkelthendelser bidratt til at noen har opplevd avbrudd som har vart over flere døgn.

I Forskrift om beredskap i kraftforsyningen (beredskapsforskriften - BfK) stilles det krav til risiko- og sårbarhetsanalyser (ROS-analyser) for alle kraftforsyningsselskaper, det vil si virksomheter som utfører produksjon med tilhørende vassdragsregulering, overføring og distribusjon av elektrisk energi og fjernvarme etter energiloven. Kravene er formulert i § 1-3 Risiko- og sårbarhetsanalyse og i § 5-4 Analyse i BfK. Det er en klar anbefaling at man setter seg meget godt inn i forskriftskravene før man starter med ROS-analysen for å sikre at analysen fanger opp de forhold som må være på plass. NVE har også utarbeidet en egen veiledning til beredskapsforskriften som kan lastes ned fra www.nve.no som bistand i fortolkningen av forskriftskravet.

Formålet med beredskapsforskriften er å forebygge og håndtere hendelser med hensyn til teknisk svikt, naturgitt skade og bevisst skadeverk. Dette skal bidra til god forsyningssikkerhet. Formålet med kravet til risiko- og sårbarhetsanalyser i beredskapsforskriften følger av forskriften: Det enkelte selskap skal identifisere risiko og sårbarhet ved ekstraordinære hendelser knyttet til teknisk svikt, naturgitt skade og bevisst skadeverk. Videre skal analysen også favne de tiltak forskriften krever skal kunne iverksettes av ulike beredskapstiltak.

Veilederen er utgått

1.1 Hva skal vi med risiko- og sårbarhetsanalyser i kraftbransjen?

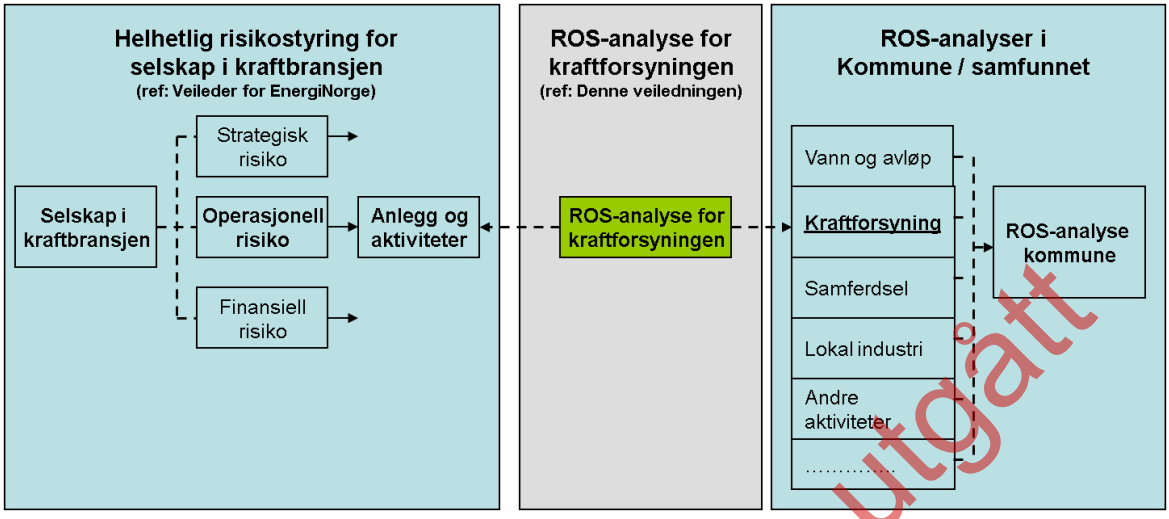
Noen viktige anvendelser og gevinster ved riktig bruk av ROS-analyser i kraftbransjen vil være:

- Økt evne til å forebygge og håndtere ekstraordinære hendelser
- Mer stabil strømforsyning og færre avbrudd
- Mer fokusert ressursbruk til forebyggende og skadereduserende tiltak
- Synliggjøre hvilke konsekvenser ekstraordinære hendelser kan medføre for virksomheten og samfunnet, slik at ledelsen i virksomheten kan bruke dette som en viktig planforutsetning
- Systematisere og dokumentere risiko og sårbarhet i forbindelse med hendelser som virksomheten kan stå ovenfor
- Et ledelsesverktøy for bedre måloppnåelse i virksomheten[1]

De viktigste ROS-kravene i beredskapsforskriften blir gjennomgått i Vedlegg 4.

[1] Dette er utførlig beskrevet i "Veileder i helhetlig risikostyring" utgitt av Energi Norge i 2010.

ROS-analyser i kraftforsyningen spiller en rolle både for å tilfredsstille samfunnets behov og bedriftens egne ønsker og behov. Vi kan si at ROS-analysene blir en del av samfunnets "risikostyring" på den ene siden og virksomhetens helhetlige risikostyring på den andre siden. Dette er vist i Figur 1
.

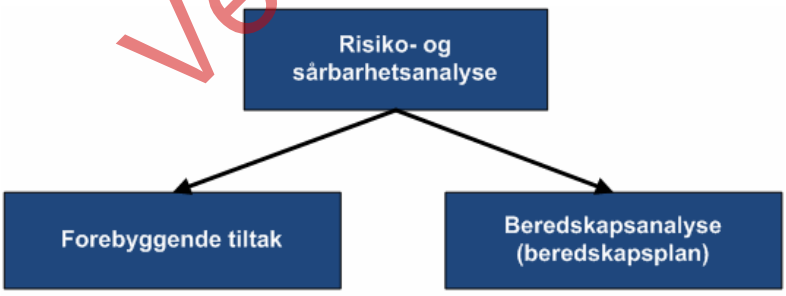


Figur 1 Sammenheng mellom risikostyring på selskapsnivå, ROS-analyse av et kraftforsyningsanlegg og samfunnssikkerhet.

Veilederen er utgått

1.2 ROS-analyser og beredskap

ROS-analyser benyttes til å identifisere og prioritere risikoreduserende tiltak. Noen tiltak er årsaksreduserende (forebyggende), dvs. de hindrer uønskede hendelser i å inntreffe. Andre tiltak er skadereduserende, dvs. de begrenser skadevirkningene hvis en uønsket hendelse inntreffer. Beredskapsanalyser og beredskapsplaner har som oppgave å sikre rask gjenoppretting av funksjon når en uønsket hendelse har skjedd. ROS-analysen danner derfor et utgangspunkt for å dimensjonere beredskapen. Vi kan dermed slå fast at en god og robust beredskap er tuftet på en forutgående ROS-analyse.



Figur 2 Gjennom ROS-analysen identifiseres forebyggende og skadereduserende tiltak. Beredskapen etableres basert på forutgående ROS-analyse.

1.3 Omfang og avgrensninger

Kraftforsyningen er underlagt en rekke lover og forskrifter som stiller krav til sikkerhet, beredskap og blant annet ROS-analyser. Disse ROS-analysene kan blant annet være fokusert på sikkerhet for ansatte, miljøforurensing, og lignende. I tillegg er det en økende trend at selskapet selv stiller egne krav som ROS-analysen skal dekke for å ivareta virksomhetens interesser for helhetlig risikostyring. Temaet for *denne* veiledningen er ROS-analyser for oppfyllelse av beredskapsforskriftens krav. Metoden vil likevel kunne benyttes for å tilfredsstille krav til ROS-analyser i øvrige lover og forskrifter, samt i bedriftens risikostyring.

Denne veiledningen søker å gi svar på følgende spørsmål:

- Hvilke krav stiller beredskapsforskriften til risiko- og sårbarhetsvurderinger?
- Hvilken metode bør benyttes?
- Hvordan planlegger man en ROS-analyse og hvordan kommer man i gang?
- Hvordan gjennomføres de ulike stegene i ROS-analysen?
- Hvordan følger man opp resultatene fra ROS-analysen?
- Hvordan kan resultatene visualiseres og kommuniseres?

For nye anlegg er det ofte hensiktsmessig å foreta ROS-analyser 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. Metoden og prosessen for ROS-analyser som presenteres her er så generell at den også kan benyttes i designfasen. Vi fokuserer imidlertid hovedsaklig på ROS-analyser av eksisterende anlegg i den videre teksten.

Beredskapsforskriften stiller også krav til informasjonssikkerhet og har bl.a. spesielle krav til sikkerhet for driftskontrollsystemer. Metoden som presenteres i denne veiledningen kan langt på vei benyttes også til dette formålet, men IKT-sikkerhet er et stort tema som det vil kreve for mye å gjennomgå grundig i en veiledning av dette formatet. En del nyttige referanser om emnet er imidlertid gjengitt i kapittel 0.

Denne veiledningen er også tilpasset å analysere anlegg med tanke på innplassering i klasse (jf. krav til analyse i BfK § 5-4). På bakgrunn av hvilken klasse anlegget får av NVE skal det foretas en egen risiko- og sårbarhetsanalyse, samt at anleggene og systemene skal planlegges og utføres som angitt i forskriften.

I kapittel 2 presenteres en del nyttige begreper og teori som inngår i en risiko- og sårbarhetsanalyse. Det tas utgangspunkt i en grovanalysemetode, i og med at denne er relevant for mange av analysene som gjøres for kraftforsyningen. Kapittel 3 gir en gjenomgang av de viktigste stegene i en grovanalyse, skreddersydd for et kraftforsyningsanlegg. I kapittel 4 gis en oppsummering av de viktigste punktene. Vedleggene inneholder sjekklister og analyseskjemaer som kan være nyttige for å komme i gang. Der finnes også en ordliste, samt en gjengivelse av de viktigste kravene i beredskapsforskriften med hensyn på risiko- og sårbarhetsanalyser.

Vi har forsøkt å holde metodebeskrivelsen på et kortfattet og lettlest nivå. Målet er at metodebeskrivelsen, sammen med tips og råd, skal gi leseren et godt grunnlag for å gjennomføre og bruke ROS-analyser i sin egen virksomhet.

Veilederen er utgått

1.3.1 Ekstraordinære hendelser: teknisk svikt, naturgitt skade og bevisst skadeverk

Hovedintensjonen med beredskapsforskriftens krav er å unngå at kraftforsyningen stopper opp og/eller unngå at gjenopprettingen av forsyningen tar lang tid. Noen av hensiktene med beredskapsforskriften er å forebygge og være i stand til å håndtere ekstraordinære hendelser knyttet til teknisk svikt, naturgitt skade og tilsiktet skade. I de følgende avsnittene er de ovennevnte begrepene nærmere introdusert.

For det første; *forebygge og håndtere*. Målet er å *forebygge* hendelser slik at de ikke skjer. Å *håndtere* betyr i denne sammenhengen å ha forberedt seg slik at man best mulig kan unngå at hendelsene medfører alvorlige konsekvenser dersom de skjer.

For det andre, det som skal forebygges og håndteres er *ekstraordinære hendelser*. Det er vanskelig å gi en helt presis definisjon av hva som er en ekstraordinær hendelse, og i mange tilfeller vil det være nødvendig at det er selskapet selv som langt på vei definerer hva de legger i dette begrepet. I grove trekk kan man si at en ekstraordinær hendelse er en uønsket hendelse som går ut over det som selskapet håndterer i det daglige. Eksempler på slike ekstraordinære hendelser er store klimapåkjenninger, bevisst skadeverk, total svikt i driftskontrollsystemet, mastebrudd over store områder pga. uvær, massivt rørbrudd i et fjernvarmeanlegg, håndtering av en psykisk ustabil person i en driftssentral, og innbrudd og hærverk/sabotasje i en transformatorstasjon, m.v..

Èn strategi for å redusere risikoen for ekstraordinære hendelser kan være å konstruere systemer med redundans, for eksempel at det er doble linjer inn til forbruker. Selv om systemet bygges med redundans, kan det tenkes å oppstå fellesfeil, det vil si farer, trusler og uønskede hendelser som, dersom de inntrer, kan medføre at redundante deler av systemet feiler. I ROS-analysesammenheng er det da viktig å prøve å identifisere slike mulige fellesfeil, og deretter identifisere risikoreduserende tiltak.

Et annet aspekt ved ekstraordinære hendelser er kaskadeeffekter. Dette er flere uønskede hendelser som skjer etter hverandre der "det ene fører til det andre". Med andre ord: Det at en uønsket hendelse inntrer kan være en medvirkende faktor (årsak) til at nye uønskede hendelser inntrer. En viktig del av ROS-analysen er å prøve å identifisere muligheten for slike kaskadeeffekter, og deretter identifisere risikoreduserende tiltak, det vil si tiltak som reduserer sannsynligheten for kaskadeeffekter eller reduserer konsekvensene dersom kaskadeeffektene likevel skulle skje.

Ekstraordinære hendelser kan være relatert både til utilsiktede og tilsiktede hendelser. I avsnittene over er det vist eksempler på begge disse kategoriene.

Veilederen er utgått

2. ROS-analyser – hva innebærer det?

2.1 Sentrale begreper

Noen sentrale begreper er beskrevet under. I Vedlegg 3 er det gitt en oppsummering av de viktigste begrepene.

2.1.1 Risiko, sannsynlighet og usikkerhet

Risiko handler om fremtiden. Vil vi få en alvorlig eksplosjon i transformatorstasjonen? Vil et tre falle over linjen? Vil noen prøve å bryte seg inn i anlegget vårt? Vil noen kunne angripe datasystemene våre, og hva vil i så fall kunne skje? Det er dette som er risiko: at hendelser med ulike konsekvenser kan komme til å skje. Risikoen har således to hovedkomponenter: i) hendelsene og de tilhørende konsekvensene og ii) usikkerhet om disse – vil hendelsene inntreffe og hva vil konsekvensene bli? Disse to komponentene til sammen er risiko.

For å uttrykke usikkerheten om fremtidige uønskede hendelser og deres konsekvenser benyttes sannsynligheter. En sannsynlighet er en måte å uttrykke usikkerheten på, eller sagt på en annen måte, hvor trolig det er at en bestemt hendelse vil inntreffe. Dersom du sier at sannsynligheten for en enkelt ulykkeshendelse er 1 %, mener du at det er samme usikkerhet – det er like trolig at – hendelsen inntreffer som at du ved en tilfeldig trekning skal trekke en bestemt kule ut av en boks som inneholder 100 kuler. For å beskrive risikoen – slik det gjøres i risiko- og sårbarhetsanalysen – brukes sannsynligheter. Da kan vi få uttrykt om risikoen er stor eller liten.

2.1.2 Forutsetninger og antagelser

Dessverre er det ikke bare å se på sannsynlighetstallene når en skal vurdere om risikoen er høy eller lav. Husk at tallene er bare et redskap for å uttrykke risikoen, og dette redskapet er ikke perfekt. En må også ta hensyn til hva disse sannsynlighetstallene bygger på. Når en vurderer sannsynlighet, legger en til grunn en viss kunnskap og det gjøres ofte mange forutsetninger og antagelser. Denne kunnskapen kan imidlertid være svært begrenset, og noen av forutsetningene kan komme til å vise seg å være feil. Ydmykhet er med andre ord nødvendig når vi uttaler oss om risiko. Ingen har fasitsvaret når det gjelder risiko. Likevel kan risikobeskrivelser være nyttige fordi de får frem kunnskapene og usikkerhetene, og dette kan hjelpe oss til å ta bedre beslutninger om hvordan vi skal håndtere risikoen, for eksempel hvor omfattende beredskap vi skal ha.

2.1.3 Sårbarhet

Begrepet sårbarhet kan betegne et systems evne til å opprettholde sin funksjon når det utsettes for påkjenninger. I norsk sammenheng er definisjonen fra NOU 2000:24 mest brukt. *Sårbarhet er et uttrykk for et systems evne til å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet.* Systemene som vurderes kan være både et overordnet (stort) system, og et underordnet (mindre) system.

Det motsatte av sårbarhet er robusthet. Gjennom å kartlegge virksomhetens sårbarheter vil en slik opplisting raskt kunne karakteriseres som sensitiv og må håndteres deretter.

Sentralt i begrepet sårbarhet er evnen et system har til å opprettholde (og gjenvinne) sin funksjon når det utsettes for en uønsket hendelse.

Veilederen er utgått

Et eksempel på sårbarhetsvurdering av et overordnet system:
Tenk deg et kraftforsyningssystem som består av flere produksjonsanlegg, flere trafostasjoner samt overføringsnett og fordelingsnett til sluttbrukere. Hvor sårbart er dette systemet? For å kunne svare på det må vi tenke gjennom: Sårbarhet for hva? Vi må med andre ord starte med de uønskede hendelsene og se på sårbarheten i forhold til hver av disse. La oss ta utgangspunkt i den uønskede hendelsen linjebrudd (på et spesifikt sted i nettverket). Å vurdere sårbarhet handler da om å vurdere i hvilken grad systemet er i stand til opprettholde sin funksjon (levere kraft) dersom linjebrudd inntrer. Det vil da være sentralt å se på i hvilken grad vi har flere linjer inn til sluttbrukerne som hver kan levere iht. behov.

Et eksempel på sårbarhetsvurdering av et sikkerhetssystem:
Ta utgangspunkt i den uønskede hendelsen at en generator får for høyt turtall og ruser. Som konsekvensreduserende tiltak er det installert vern som skal detektere for høyt turtall, slik at ytterligere tiltak kan iverksettes. Hva er sårbarheten til dette vernet i forhold til den uønskede hendelsen at generatoren får for høyt turtall? Slike sårbarhetsbetraktninger handler om å vurdere i hvilken grad vernet er i stand til å gjennomføre sin tiltenkte funksjon dersom generatoren får for høyt turtall. Dette kan være pålitelighetsanalyser av vernet, vurdering av om det finnes fellesfeil etc. For eksempel kan det tenkes at vernet kan bli skadet av vibrasjoner i generatoren og således ikke fungerer i den situasjonen det er tiltenkt.

?

Refleksjon

- Hva skjer om din virksomhet mister det viktigste anlegget?
- Hvordan håndteres dette?
- Hva skjer hvis den viktigste (under)leverandøren ifm transportberedskap ikke kan bistå?
- Hvordan håndteres dette?
- Hvordan får du mobilisert personell i din virksomhet hvis det offentlige telesystemet ikke fungerer?

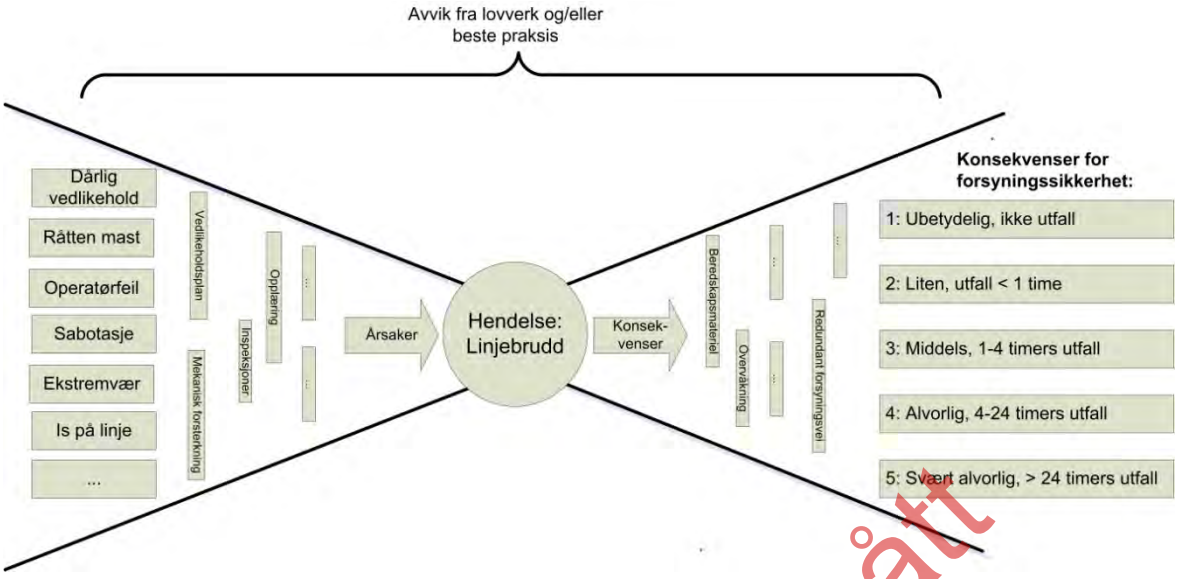
Slike og mange andre spørsmål bør stilles for å kartlegge virksomhetens sårbarheter.

Veilederen er utgått

2.1.4 Risiko- og sårbarhetsanalyse

En risiko- og sårbarhetsanalyse handler om å identifisere hendelser som kan skje, og å vurdere risiko og sårbarhet forbundet med disse hendelsene. ROS-analyser kan fokusere på både positive hendelser (muligheter) og negative hendelser (farer / trusler). I og med at denne veiledningen fokuserer på hendelser som skal legges til grunn for dimensjonering av beredskap, er fokuset kun på negative hendelser eller med andre ord farer, trusler og uønskede hendelser. Videre vil derfor betegnelsen uønskede hendelser benyttes.

Figur 3 viser et såkalt bow-tie (sløyfe) diagram. Et bow-tie diagram er en hensiktsmessig måte å vise hva som inngår i en ROS-analyse. I midten av diagrammet er den uønskede hendelsen. I en risiko- og sårbarhetsanalyse kartlegger vi ofte mange uønskede hendelser og fremstiller i separate bow-tie diagrammer. Til venstre i diagrammet er årsakene som kan føre til at de uønskede hendelsene kan inntre. Til høyre er konsekvensene de uønskede hendelsene kan medføre.



Figur 3 Bow-tie for uønsket hendelse

På venstre side kan vi ha barrierer som skal hindre den uønskede hendelsen i å oppstå. Slike barrierer kalles sannsynlighetsreduserende (forebyggende) barrierer eller tiltak. På høyre side har vi konsekvensreduserende (skadereduserende) barrierer og tiltak som har til hensikt å hindre at den uønskede hendelsen medfører alvorlige konsekvenser.

På høyre side er det vist én konsekvensdimensjon, nemlig forsyningssikkerhet. Valget av konsekvensdimensjon bestemmer hva vi ønsker å vurdere risiko for. Konsekvensdimensjonene velges ofte ut fra virksomhetens overordnede mål. I tillegg er lover og forskrifter med på å sette fokus for analysen.

Det er viktig å merke seg at alle risiko- og sårbarhetsanalyser har til hensikt å kartlegge hele, eller deler av, bow-tie diagrammet. Valg av analysemetode vil imidlertid variere avhengig av hva som skal være fokuset i analysen. Noen analysemetoder egner seg til å identifisere farer, trusler og uønskede hendelser. På samme måte vil det være metoder som er velegnet til å vurdere årsaker, konsekvenser, godheten til barrierene, sårbarheten til barrierene eller hele systemet som helhet etc. Felles for alle disse ulike risiko- og sårbarhetsmetodene er imidlertid at de kan følge den samme risikoanalyseprosessen, og at alle kartlegger enten hele eller deler av ett eller flere bow-tie diagrammer.

2.1.5 Konsekvens

Stabil kraftforsyning er viktig for hele samfunnet. Det er særlig viktig å ha oppmerksomhet på verste falls tilfeller. At en hendelse ikke har forekommet ved anlegget (eller tilsvarende anlegg) tidligere betyr ikke at den ikke kan oppstå i fremtiden. Alle deler av systemet som har en kritisk funksjon i produksjons- / distribusjonskjeden må kartlegges, og man må ha klart for seg hva som kan skje hvis disse blir skadet uavhengig av hvor lite sannsynlig dette vurderes å være. Beredskapsforskriftens formål er å gi de enkelte selskap i kraftforsyninger plikter til å forebygge og håndtere ekstraordinære hendelser. Dette gjelder særlig i forhold til naturgitte og tilsiktede hendelser, men også i forhold til teknisk svikt.

Beredskapsforskriften gir en del plikter som skal bidra til å hindre at uønskede hendelser medfører svært alvorlige konsekvenser. Ved gjennomføringen av ROS-analyser i kraftforsyningen er det derfor

Veilederen er utgått

nødvendig å være bevisst på å identifisere sårbarheter og gjennomføre tiltak overfor viktige komponenter og anlegg hvis utfall vil kunne gi massive konsekvenser. Dette gjelder også hendelser som er vurdert å ha lav sannsynlighet.

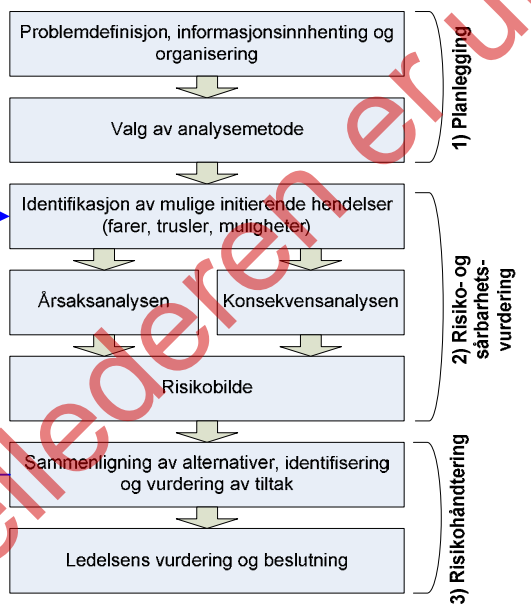
2.2 ROS-analyseprosessen

Det finnes en rekke ulike eksempler på prosesser for hvordan en risiko- og sårbarhetsanalyse kan gjennomføres. Det er imidlertid slik at hovedinnholdet i prosessene i stor grad er det samme selv om antall bokser i fremstillingen varierer. Risikoanalyseprosessen består i hovedsak av tre deler. Dette er:

1. Planlegging.
2. Risiko- og sårbarhetsvurdering.
3. Risikohåndtering.

I denne veiledningen har vi tatt utgangspunkt i risikoanalyseprosessen som er beskrevet i boken "Risikoanalyser – prinsipper og metoder, med anvendelser" (Aven, Røed, Wiencke (2008)). Denne prosessen er basert på ISO 31000, se Figur 4

Veilederen er utgått



Figur 4 Risiko- og sårbarhetsanalyseprosessens ulike trinn (ref. Aven et al. 2008)

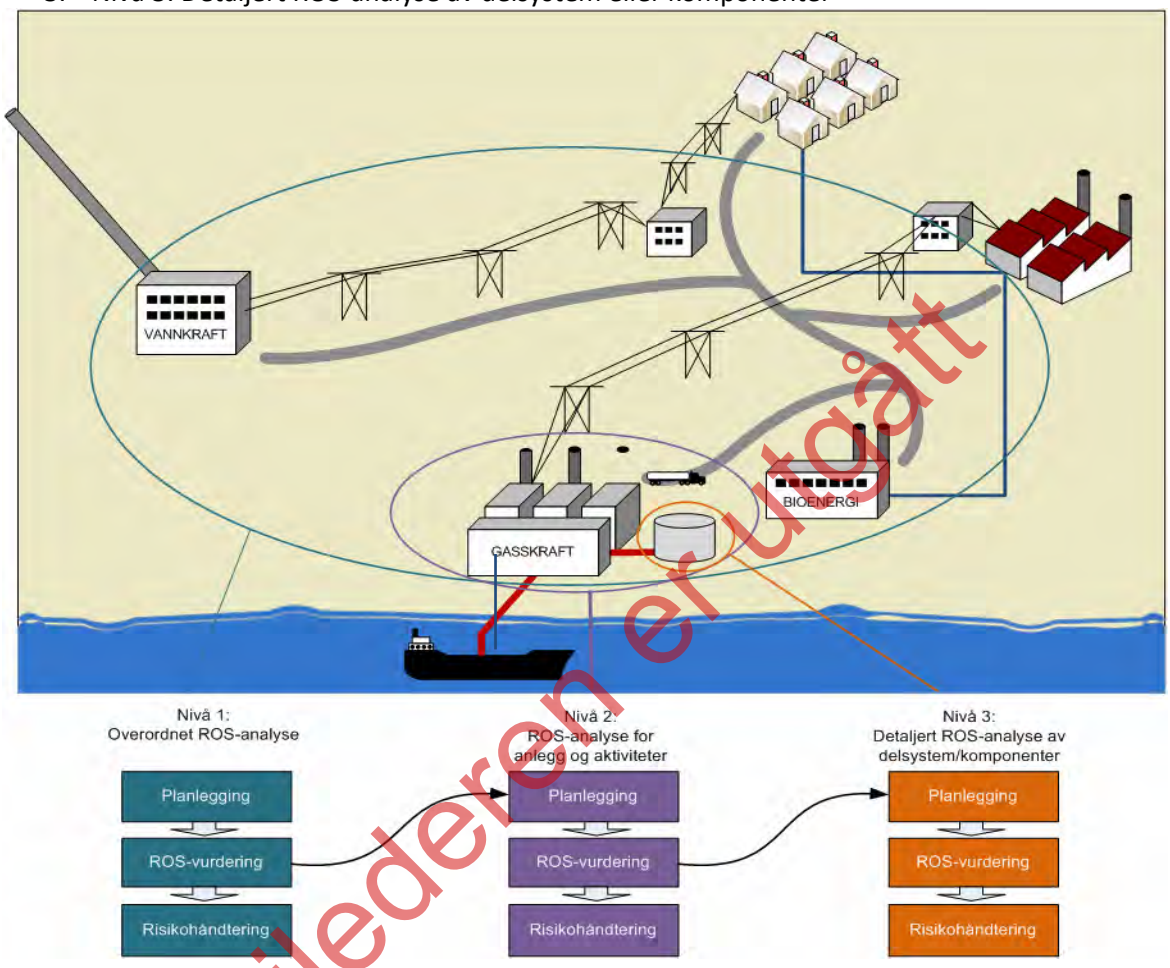
Denne generelle prosessen kan legges til grunn for alle ROS-analyser. Hvilken risikoanalysemetode som velges, hvordan risikobildet best bør fremstilles og hvordan risikoreduserende tiltak bør identifiseres og vurderes vil imidlertid variere fra den ene analysen til den andre, avhengig av hva som er hensikten med analysen, hva slags objekt det er som skal analyseres osv.

2.3 Kartlegge virksomhetens risikopotensiale - nivåinndeling

Beredskapsforskriften stiller krav om å kartlegge virksomhetens risikopotensiale. 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 nivåinndeling er foreslått og vist i Figur 5:

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



Figur 5 Ulike nivåer av ROS-analyser

Veilederen er utgått

Refleksjon: *Hvorfor bør vi ikke gå rett i gang med detaljerte ROS-analyser?*

? ***Svar:*** *Dersom du starter kartleggingen av virksomhetens risikopotensiale ved bruk av detaljerte ROS-analyser, vil du sannsynligvis ende opp med omfattende analyser med svært begrenset nytteverdi. Start kartleggingen på et overordnet nivå med å gjøre deg kjent med hvilke anlegg som er kritiske / sårbare og hvorfor. Deretter fokuseres arbeidet mot de kritiske / sårbare anleggene og detaljeringsnivået økes.*

2.3.1 Nivå 1: Overordnet ROS-analyse

En ROS-analyse på overordnet nivå er nyttig for å danne en fullstendig oversikt over alle de anlegg og kritiske prosesser som virksomheten eier eller driver, og for hvilken betydning disse har for totalsystemet i en ekstraordinær situasjon. På denne måten kan man identifisere hvilke anlegg som har størst betydning i verdikjeden. Områder i systemet som vil bli slått ut umiddelbart (N-0) og medføre store konsekvenser, vil raskt rangere høyt på prioritetslisten for videre analyser.

Den overordnede analysen bør vurdere ulike farer og trusler og gjøre betraktninger rundt uønskede hendelser som kan sette anleggene helt eller delvis ut av drift. Videre bør hvert anlegg og hver kritiske prosess rangeres utfra viktighet for å opprettholde produksjon og forsyningssikkerhet. På denne måten danner man seg en oversikt over sårbarheten i kraftforsyningssystemet.

Grovanalyse er en velegnet metode for ROS-analyser på dette nivået. Nettverksanalyser (leveringspålitelighetsanalyser) og ekspertvurderinger vil kunne danne underlag for en slik analyse.

Resultatene fra analysen gir ledelsen et nyansert bilde av risiko og sårbarhet tilknyttet hele virksomheten. Samtidig gir resultatene underlag for prioritering av videre ROS-analyser basert på kritikalitet i kraftforsyningen. Etter at den overordnete analysen er gjennomført kan man gjennomføre ROS-analyser for de enkelte anlegg og aktiviteter i prioritert rekkefølge (Nivå 2).

> ! *Prioriteringen av videre ROS-analyser av anlegg og aktiviteter bør også ses opp i mot klassifisering av anleggene som definert av NVE, i tillegg til egen vurdering av viktighet.*

Veilederen er utgått

2.3.2 Nivå 2: ROS-analyse av anlegg og aktiviteter

I en ROS-analyse av anlegg og aktiviteter benyttes gjerne en strukturert grovanalyse for å gjøre en omfattende kartlegging av mulige farer, trusler og uønskede hendelser og tilhørende risiko. En fordel med strukturert grovanalyse er at den kan gjennomføres med relativt begrensede ressurser. Samtidig som metoden gir mulighet for å etablere et nyansert risikobilde, vil den også avdekke når det er behov for mer detaljerte ROS-analyser (Nivå 3).

Kapittel 3 gir en nærmere beskrivelse av hvordan en ROS-analyse med grovanalyse på Nivå 2 kan gjennomføres. Metoden er også relevant for overordnet analyse på Nivå 1.

Analysene som gjennomføres for anlegg og aktiviteter vil i enkelte tilfeller avdekke behov for mer detaljerte ROS-analyser av spesifikke delsystem, komponenter eller aktiviteter. I særlig grad vil det være hensiktsmessig å gjennomføre mer detaljerte analyser 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.

2.3.3 Nivå 3: Detaljert ROS-analyse av delsystem eller komponenter

Selve gjennomføringen av detaljerte ROS-analyser på Nivå 3 er ikke dekket av denne veiledningen.

For å gjøre mer detaljerte analyser henvises det til bruk av kjente risiko- og sårbarhetsanalysemetoder som for eksempel feiltre- eller hendelsestreanalyse. 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 som kan fungere som hjelp ifm. slike analyser.

Det er imidlertid viktig å trekke ut funn i slike analyser slik at disse også kan være viktige innspill i analyser på Nivå 1 og Nivå 2-analyser.

3. ROS-analyser i praksis – strukturert grovanalyse

Fokus i dette kapitlet er praktisk ROS-analyse på nivå 2: ROS-analyse av anlegg og aktiviteter. Den anbefalte analysemetoden er strukturert grovanalyse med tilhørende analyseskjema og sjekklister. Metoden er også velegnet til ROS-analyser på nivå 1: Overordnet ROS-analyse. Metoden benytter bruk av analysemøte for å effektivisere analyseprosessen.

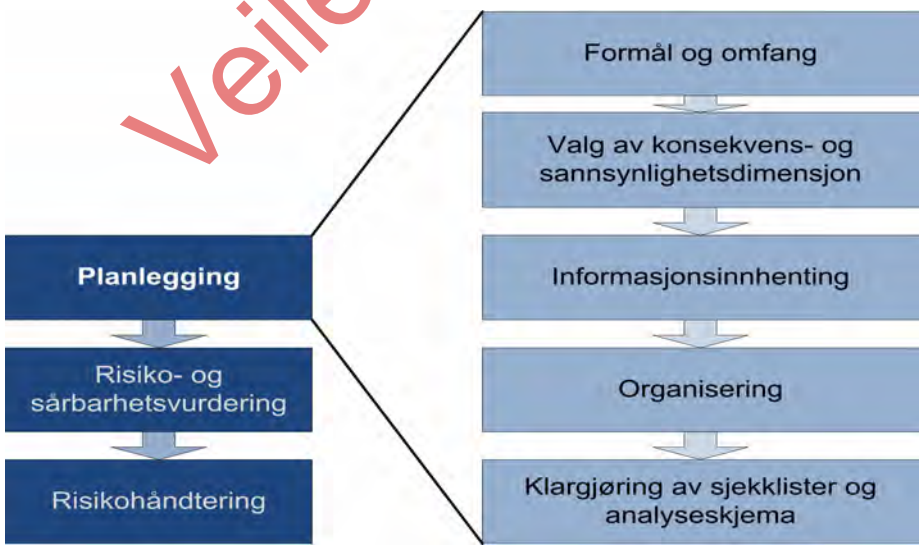
> ! *Ofte fokuseres det mye på selve risikovurderingen (gjennomføringen), noe som begrenser tilgjengelig tid til planlegging og oppfølging. Som en tommelfingerregel bør 1/3 av tiden settes av til planlegging, 1/3 til risiko- og sårbarhetsvurdering og 1/3 til risikohåndtering og oppfølging av resultater,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

Veilederen er utgått

3.1 Planlegging

Det at arbeidsgruppen, som skal jobbe med ROS-analysen, har tilstrekkelig kunnskap og erfaring med bruk av denne typen metode, vil ha stor betydning på resultatet. For å få et godt resultat er også god planlegging viktig. Det er viktig å være tydelig på *hvorfor* og *hvordan* analysen skal gjennomføres og ikke minst hvilke forskriftskrav som skal tilfredsstilles. Momenter som bør inngå i planlegging av ROS-analysen, er vist i Figur 6.

1. Definere formål og omfang av analysen.
2. Valg av konsekvens- og sannsynlighetsdimensjon.
3. Informasjonsinnhenting.
4. Organisering av arbeidet.
5. Klargjøring av analyseskjema og sjekklister.



Figur 6 De ulike stegene i planlegging av ROS-analysen

3.1.1 Definere formål og omfang av analysen

Klare mål for analysen er en forutsetning for et godt resultat. Hvorfor skal analysen gjennomføres? Hva skal resultatene brukes til? Hva er det som skal analyseres? Hvor går systemgrensene? Uten et klart formulert formål og omfang blir analysen ofte lite fokusert og gir ikke de svarene en trenger for å gjøre nødvendige betraktninger rundt sikkerheten og sårbarheten ved anlegget eller aktiviteten.

I tillegg til klar formålsdefinisjon er det viktig å sikre forankring hos beslutningstakerne i virksomheten. Dette gjelder både administrativ ledelse og styret. God forankring sikrer handlingsrom til å implementere risikoreduserende tiltak og etablere robust beredskap som en del av oppfølgingen av analysen.

Formålet med ROS-analysen knyttes gjerne opp mot krav i gjeldende lover og forskrifter, men bør også sees som en del av virksomhetens helhetlige risikostyring og således knyttes opp mot virksomhetens mål innen for eksempel forsyningssikkerhet, HMS og/eller økonomi.

I beredskapsforskriften er formålet med ROS-analyser angitt som *"forebygging og håndtering av alle ekstraordinære situasjoner som kan skade eller hindre produksjon, overføring og fordeling av elektrisk kraft"*. Analysen skal også inkludere en oversikt og vurdering over alle de tiltak beredskapsforskriften lister opp som en forutsetning for tilfredsstillende beredskap.

Eksempel

Formål og omfang
ROS-analysen har som formål å kartlegge forhold ved Energiselskapet AS sin transformatorstasjon som kan utgjøre en trussel mot forsyningssikkerhet, personellsikkerhet og ytre miljø. Videre skal det identifiseres risikoreduserende tiltak for å sikre en robust beredskap.

Veilederen er utgått

3.1.2 Valg av konsekvens- og sannsynlighetsdimensjon

Når formålet med analysen er definert, kan vi bestemme konsekvensdimensjoner. I beredskapsforskriften er det slått fast at ROS-analysen må fokusere på evnen til å opprettholde funksjon. Det vil si at forsyningssikkerhet som hovedregel alltid skal inngå som konsekvensdimensjon.

Beredskapsforskriften stiller konkrete krav til bl.a.:

- Tilgang på nok, kompetent personell og evne til drift (§§ 3-1, 3-2, 3-4)
- Evne til gjenoppretting av funksjon (§ 3-5)
- Transportberedskap (§3-6)
- Informasjonsberedskap (§3-7)
- Sambandsberedskap (§3-8)
- Adgangskontroll (§ 4-5)
- Sikring av anlegg (§§ 5-1, 5-2, 5-4, 5-5, 5-6, 5-7)
- Informasjonssikkerhet (§§ 6-1, 6-2, 6-3, 6-5, 6-6)
- Driftskontrollsystemer (§ 6.4)

Det betyr at ROS-analysen blant annet må vurdere disse forholdene. Disse kan betraktes som forhold som påvirker forsyningssikkerheten, snarere enn å gi opphav til egne konsekvensdimensjoner. Vi har derfor valgt å ta disse med som egne punkter i sjekklisten som skal gjennomgås i hver ROS-analyse.

Andre konsekvensdimensjoner bør velges ut fra virksomhetens overordnede mål, samt øvrige lover og forskrifter som virksomheten er underlagt. Andre relevante konsekvensdimensjoner kan for eksempel være:

- Personellsikkerhet
- Ytre miljø
- Økonomi
- Omdømme

Vi anbefaler å benytte fem kategorier for konsekvenser og sannsynligheter. Hvis man synes dette gjør analyseprosessen unødig detaljert og komplisert kan fire eller tre kategorier benyttes.

Dersom kategoriene beskrives med ord som "ubetydelig", "liten", "middels" osv., er det viktig å si hva man mener med en "middels" konsekvens. Dvs. at vi bør tilstrebe å kvantifisere konsekvensdimensjonen. For forsyningssikkerhet kan dette se slik ut, men må tilpasses den enkelte virksomhet:

1. Ubetydelig. Ikke avbrudd i strøm- eller fjernvarmeforsyning.
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. Alvorlige konsekvenser i infrastruktur og lokalsamfunnet. Avbrudd ≥ 10 timer hos < 1000 sluttbrukere.
5. Kritisk. Samfunnsviktige funksjoner som liv og helse, samt viktig infrastruktur rammet / satt ut av funksjon. Avbrudd ≥ 10 timer hos ≥ 1000 sluttbrukere.

For sannsynlighetsdimensjonen kan kvantifiseringen gjøres ved hjelp av frekvenser. Med frekvens menes forventet antall hendelser i et bestemt tidsrom (for eksempel i løpet av 1 år). Følgende inndeling kan benyttes, men dette må tilpasses den enkelte virksomhet:

1. Sjeldnere enn hvert 1000. år (har aldri hørt om lignende hendelser). I denne gruppen legges også forhold som er svært sjeldne, tilnærmet "utenkelig".
2. Fra hvert 100. år til hvert 1000. år (har hørt om lignende hendelser i Norge eller utlandet).
3. Fra hvert 10. år til hvert 100. år (hendelser som har skjedd i selskapet eller hos andre).
4. Fra 1 gang pr. år til hvert 10. år (hendelser som har skjedd flere ganger i eget eller andres selskapet).
5. Oftere enn 1 gang pr. år (hendelser som skjer ofte / svært ofte i eget/andres selskap).

Veilederen er utgått

! *Det kan være hensiktsmessig å benytte samme kvantifisering av konsekvens- og sannsynlighetsdimensjon for alle ROS-analyser som gjennomføres i virksomheten. Da sikrer man at resultater fra ulike ROS-analyser er konsistente og at de kan fremstilles i samme risikobilde og utgjøre en del av virksomhetens helhetlige risikostyring.*

3.1.3 Informasjonsinnhenting

Forut for risikovurderingene er det viktig å skaffe til veie mest mulig informasjon om analyseobjektet. Ulike informasjonskilder som kan være nyttige både under planleggingen og i selve risiko- og sårbarhetsvurderingen er:

- Tegninger, flytskjema eller annen dokumentasjon som beskriver analyseobjektet
- Kart over anlegget og omgivelsene

- Tidligere utførte ROS-analyser
- Etablerte beredskapsanalyser og beredskapsplaner
- Relevant lovverk og/eller interne retningslinjer
- Data over historiske uønskede hendelser som har oppstått i tilknytning til analyseobjektet eller tilsvarende anlegg
- Lokalkunnskap, erfaringsdata, forskning, befaringer

> ! *Informasjon som er funnet relevant for analysen, vedlegges eller refereres til i ROS-analyserapporten. I rapporten er det også ofte hensiktsmessig å inkludere en systembeskrivelse / beskrivelse av analyseobjektet.*

For å få en god forståelse av analyseobjektet vil det, om mulig, også være hensiktsmessig at analysegruppen gjennomfører en befaring av anlegget/området. 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.

3.1.4 Organisering

> ! *Ved gjennomføring av ROS-analyser av anlegg og aktiviteter er det ofte hensiktsmessig å gjennomføre fareidentifikasjon og risikovurdering i ett eller flere analysemøter.*

Det er viktig å sikre at folk med kunnskap og kompetanse om analyseobjektet er tilgjengelige når ROS-analysen skal gjennomføres. I tillegg vil det være en fordel at en person med erfaring fra gjennomføring av ROS-analyser har rollen som prosessleder. I selve analysemøtet vil det være lurt å ha en dedikert person til å ta notater og føre analyselogg / fylle ut analyseskjemaet.

> ! *Ved gjennomføring av ROS-analyser av komplekse og sammensatte systemer er det både hensiktsmessig og nødvendig å bruke analysemøter bestående av en tverrfaglig analysegruppe. Deltakerne i denne gruppen bør ha forskjellig bakgrunn og kompetanse, som f.eks. drift, vedlikehold, driftssentralsystemer, montører osv. Behovet for å dekke alle fagområder må samtidig balanseres mot behovet for å holde antall deltakere på et håndterbart nivå. Erfaring viser at slike grupper ikke bør være over åtte personer for å være effektive. For at prosessen skal bli effektiv er det viktig at forarbeid og etterarbeid gjøres i en mindre prosjektgruppe.*
>
> *Det er viktig at alle i analysegruppen blir gjort oppmerksomme på deres rolle i ROS-analyseprosessen.*

Ulike ansvar og roller i analysemøtet

Prosesslederen har som hovedoppgave å:

- Planlegge analysen
- Styre diskusjonene
- Sikre fremdrift / passe tiden
- Aktivt bruke etablert metode

Veilederen er utgått

Analysegruppen har som hovedoppgave å:

- Bidra med egen kompetanse / erfaring / ekspertise
- Tenke utenfor sin egen erfaring og arbeidsområde
- Arbeide konstruktivt og målrettet
- Hjelpe til med å formulere anbefalinger
- Lytte til andres bidrag

Loggfører har som oppgave å:

- Sørge for at mest mulig av bakgrunnskunnskap, forutsetninger, antagelser og begrunnelse for risikovurderingen blir dokumentert
- Være en støtte for prosessleder
- Avdekke hull og mangler i det som har vært diskutert så langt i møtet

3.1.5 Klargjøring av sjekklister og analyseskjema

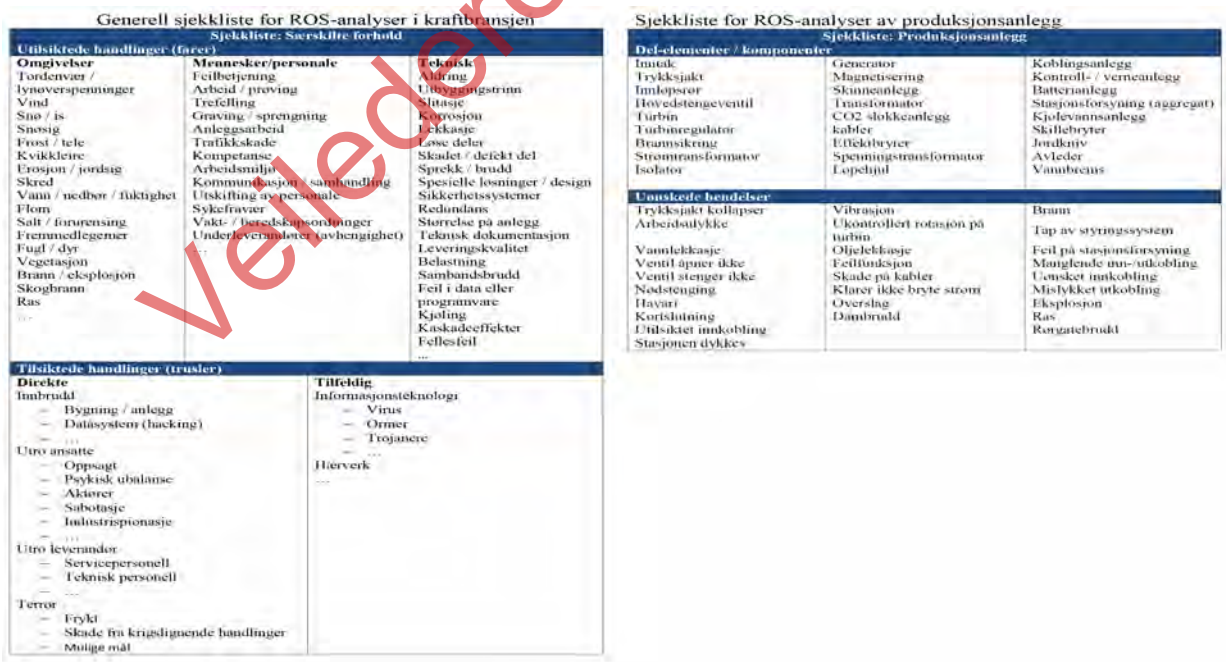
Analyseskjema og skreddersydde sjekklister er en sentral del av grovanalysemetoden. På bakgrunn av befaring, tilgjengelig informasjon og bakgrunnskunnskap om analyseobjektet kan man forberede sjekklister og analyseskjema til bruk i analysemøtet.

Veilederen er utgått

Sjekklister

Vi har presentert noen sjekklister i Vedlegg 1 som kan benyttes som utgangspunkt. Sjekklistene består av to deler – en generell del og en del som er spesifikk for det aktuelle analyseobjektet.

Figur 7 viser den sammensatte sjekklisten for et produksjonsanlegg.



Generell sjekkliste for ROS-analyser i kraftbransjen

Sjekkliste: Særskilte forhold

Utilsiktede handlinger (farer)

Omgivelser	Mennesker/personale	Teknisk
Tordenvær / lynoverspenninger	Feilbetjening	Aldring
Vind	Arbeid / prøving	Utbyggingstrinn
Snø / is	Trefelling	Slitasje
Snøsig	Graving / sprengning	Korrosjon
Frost / tele	Anleggsarbeid	Lekkasje
Kvikkleire	Trafikkskade	Løse deler
Erosjon / jordsig	Kompetanse	Skadet / defekt del
Skred	Arbeidsmiljø	Sprekk / brudd
Vann / nedbør / fuktighet	Kommunikasjon / samhandling	Spesielle løsninger / design
Flom	Utskifting av personale	Sikkerhetssystemer
Salt / forurensing	Sykefravær	Redundans
Fremmedlegemer	Vakt- / beredskapsordninger	Størrelse på anlegg
Fugl / dyr	Underleverandører (avhengighet)	Teknisk dokumentasjon
Vegetasjon	...	Leveringskvalitet
Brann / eksplosjon		Belastning
Skogbrann		Sambandsbrudd
Ras		Feil i data eller programvare
...		Kjøling
		Kaskadeeffekter
		Fellesfeil
		...

Tilsiktede handlinger (trusler)

Direkte	Tilfeldig
Innbrudd	Informasjonsteknologi
– Bygning / anlegg	– Virus
– Datasystem (hacking)	– Ormer
– ...	– Trojanere
Utro ansatte	– ...
– Oppsagt	Hjerverk
– Psykisk ubalanse	...
– Aktører	
– Sabotasje	
– Industrispionasje	
– ...	
Utro leverandør	
– Servicepersonell	
– Teknisk personell	
– ...	
Terror	
– Frykt	
– Skade fra krigsdignende handlinger	
– Mulige mål	

Sjekkliste for ROS-analyser av produksjonsanlegg

Sjekkliste: Produksjonsanlegg

Del-elementer / komponenter		
Inntak	Generator	Koblingsanlegg
Trykksjakt	Magnetisering	Kontroll- / verneanlegg
Innløpsrør	Skinneanlegg	Batterianlegg
Hovedstengeventil	Transformator	Stasjonsforsyning (aggregat)
Turbin	CO2 slokkeanlegg	Kjølevannsanlegg
Turbinregulator	kabler	Skillebryter
Brannsikring	Effektbryter	Jordkniv
Strømtransformator	Spenningstransformator	Avleder
Isolator	Løpehjul	Vannbrems

Uønskede hendelser		
Trykksjakt kollapser	Vibrasjon	Brann
Arbeidsulykke	Ukontrollert rotasjon på turbin	Tap av styringssystem
Vannlekkasje	Oljelekkasje	Feil på stasjonsforsyning
Ventil åpner ikke	Feilfunksjon	Manglende inn-/utkobling
Ventil stenger ikke	Skade på kabler	Uønsket innkobling
Nødstenging	Klarer ikke bryte strøm	Mislykket utkobling
Havari	Overslag	Eksplosjon
Kortslutning	Dambrudd	Ras
Utilsiktet innkobling		Rørgatebrudd
Stasjonen dykkes		

Figur 7 Sammensatt sjekkliste for et produksjonsanlegg – generell del til venstre og spesifikk del til høyre (en mer utskriftsvennlig versjon av sjekklistene for ulike typer anlegg ligger i Vedlegg 1).

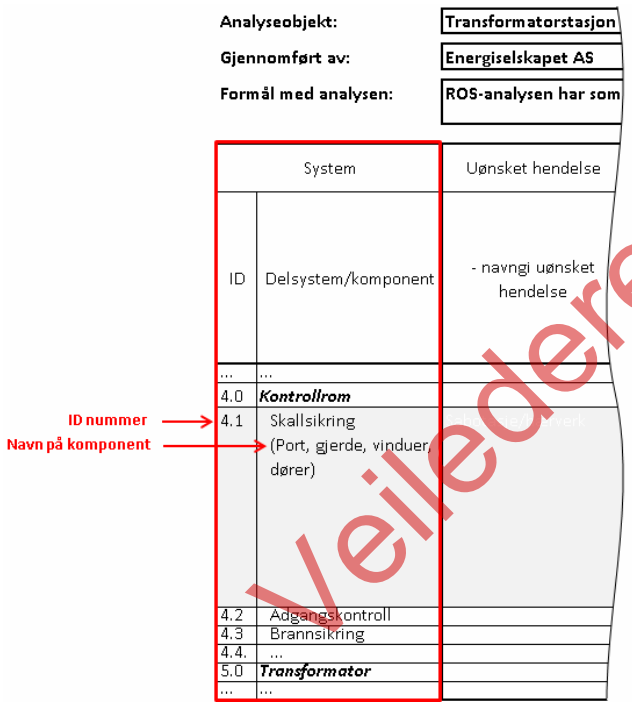
Sjekklistene bør utvides og justeres etter behov, tilpasset det aktuelle anlegget.

Analyseskjema

I Vedlegg 2 er det vist to typer analyseskjema. Det første gir mulighet til logging av én hendelse per ark og er gunstig til utskrift og manuell utfylling i en mindre arbeidsgruppe. Den andre typen legger opp til fortløpende logging av uønskede hendelser under hverandre i et regneark og passer for visning på storskjerm og direkte utfylling i et analysemøte. Selv om skjemaene har forskjellig format er innholdet, dvs. feltene som skal fylles ut, de samme.

> ! *Analyseskjemaet bør testes ut før man går i analysemøtet. Foreslå noen uønskede hendelser og fyll inn i skjemaet. Det er viktig at formatet på skjemaet fungerer for deg som prosessleder.*

En viktig del av planleggingsaktiviteten er å dele analyseobjektet inn i delsystemer og komponenter. Hvis du velger å benytte regnearket, kan du forhåndsutfylle de ulike delsystemene og komponentene før du går i analysemøtet. Et eksempel er vist i Figur 8.



Figur 8 Analyseskjema – utfylling (Delsystem/komponent)

Veilederen er utgått

3.2 Risiko- og sårbarhetsvurdering

I Figur 9 er de ulike stegene som inngår i risiko- og sårbarhetsvurderingen vist. Disse er:

1) Identifisere farer, trusler og uønskede hendelser
2) Risikoanalyse av uønsket hendelse
3) Sårbarhetsvurdering av uønsket hendelse
4) Identifisere mulige risikoreduserende tiltak
5) Presentasjon av risikobilde

På høyre side i figuren ser vi inndelingen i delsystem / komponenter, sjekklister og analyseskjemaet. Disse hjelpemidlene benyttes aktivt i denne fasen av ROS-analysen.

Figur 9 De ulike stegene i risiko- og sårbarhetsvurderingen

Veilederen er utgått

Kort oppsummert kan vi si at punkt 1) til punkt 4) handler om å fylle ut analyseskjemaet vi presenterte i forrige avsnitt. Punkt 5), risikobilde, handler om å presentere og kommunisere resultatene på en oversiktlig måte.

3.2.1 Identifisere farer, trusler og uønskede hendelser

> ! *Husk å kartlegge anleggets risiko og sårbarhet med tanke på naturgitte forhold, teknisk svikt og bevisst skadeverk. Ubevisste feilhandlinger må også tas med.*

Iht. beredskapsforskriften skal det identifiseres hendelser som truer kraftforsyningens evne til å fungere iht. intensjon, samt evne til å beskytte anlegg, ressurser og informasjon mot naturgitte forhold, teknisk svikt og bevisste skadeverk. Ubevisste feilhandlinger må også tas med. Det kan være aktuelt å vurdere også andre hendelser med relevans for bedriftens måloppnåelse. Dette vil til en viss grad være styrt av de konsekvensdimensjonene man har valgt å benytte, se avsnitt 3.1.2

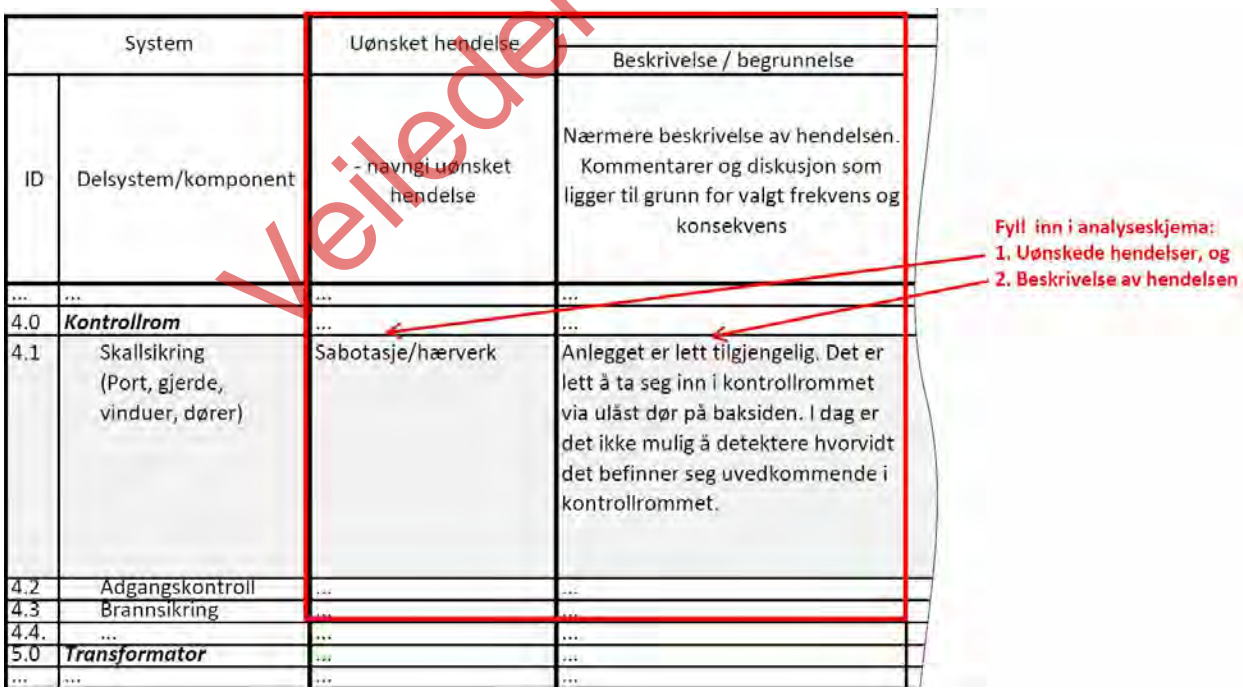
Ofte har møtedeltakerne tenkt igjennom før møtet ulike ting som "kan gå galt" ved anlegget eller aktiviteten. Det er viktig at denne informasjonen blir dokumentert nokså tidlig i møtet mens den ennå sitter friskt i minnet. Vi anbefaler derfor følgende fremgangsmåte for identifikasjon av farer, trusler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

! *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 …?".*
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.

Veilederen er utgått

I den strukturerte gjennomgangen tar man utgangspunkt i oppdelingen av anlegget i delsystemer og komponenter og identifiserer farer, trusler og uønskede hendelser for hvert element. Et eksempel er vist i Figur 10.



Figur 10 Analyseskjema – utfylling (uønsket hendelse + beskrivelse)

I forbindelse med identifisering av uønskede hendelser blir det ofte diskutert forhold rundt hendelsen – hva er hendelsesforløpet, årsaker, mulige konsekvenser, om dette har skjedd tidligere osv. Dette er viktig bakgrunnsinformasjon for risikoanalysen og bør logges i feltet merket "Beskrivelse / begrunnelse".

Til slutt går man igjennom sjekklistene (avsnitt 3.1.5 og Vedlegg 1) for å fange opp mulige forhold som ikke er fanget opp til nå.

! *Ofte vil identifiseringen av hendelser følge en 80-20-regel. Deltakerne bør ha tenkt igjennom ulike forhold ved anlegget på forhånd, og det er viktig at alle får mulighet til å "tømme hodene" i en form for idédugnad nokså tidlig i møtet. Dette kan ofte kartlegge ca. 80 % av de uønskede hendelsene og også identifisere en del viktige tiltak. De resterende 20 % av de uønskede hendelsene fanges så opp ved hjelp av en strukturert gjennomgang av delsystemer og komponenter med tilhørende sjekklister. Den initielle idédugnaden tar typisk mye kortere tid (20 %) enn den strukturerte gjennomgangen (80 %)*

! *Fokuser og prioriter tiden slik at nok tid blir satt av til de viktige, alvorlige hendelsene. Gå raskere igjennom hendelser med mindre alvorlig konsekvens.*

Veilederen er utgått

3.2.2 Risikoanalyse

For hver av de uønskede hendelsene gjør vi en nærmere betraktning av årsaker, sannsynligheter, konsekvenser, samt forutsetninger og antagelser. De viktigste feltene i analyseskjemaet er vist i Figur 11.

Uønsket hendelse	Beskrivelse / begrunnelse	Årsaker	Sannsynlighet / frekvens	Konsekvens
- navngi uønsket hendelse	Beskriv årsak, antatt frekvens og konsekvens for hver av de uønskede hendelsene.	- 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 kunder berørt
...	...	...	...	...
...	...	...	...	...
Sabotasje/hærverk	Anlegget er lett tilgjengelig. Det er lett å ta seg inn i kontrollrommet via ulåst dør på baksiden. I dag er det ikke mulig å detektere hvorvidt det befinner seg uvedkommende i kontrollrommet.	Alarm eller kameraovervåkning er ikke installert på anlegget	hvert 100. år - hvert 1000. år	Avbrutt levering i flere dager

Figur 11 Analyseskjema – utfylling (årsaker, sannsynligheter, konsekvenser)

En del av denne informasjonen kan allerede være fanget opp i feltet "Beskrivelse / begrunnelse".

Årsaker

Angi mulige årsaker til hendelsen. Tenk samtidig igjennom om det er særskilte forhold ved dette anlegget / denne komponenten som gjør at risikoen avviker fra andre tilsvarende anlegg / komponenter. Avvik fra regelverk eller beste praksis kan også være en indirekte årsak til uønskede hendelser, og bør kartlegges her.

Sannsynlighet / frekvens

Hvor stor sjanse er det for at hendelsen skal skje? For å vurdere dette kan vi for eksempel bruke frekvenskategoriene som ble definert i avsnitt 3.1.2 Her kan historiske data, feilstatistikk for kjente komponenter, ekspertvurderinger etc. legges til grunn.

> ! *Å basere seg kun på historiske data og feilstatistikker i vurderingen av sannsynligheter og frekvenser er uheldig og kan sammenlignes med å kjøre bil ved å se ut bakvinduet. En pragmatisk bruk av statistikk er fornuftig – benytt historiske data der datagrunnlaget er godt og komponenter og omgivelser er sammenlignbare. I andre tilfeller er man avhengig av en subjektiv vurdering. Det siste kan være uvant for noen.*

> ! *Beredskapsforskriften er særlig opptatt av hendelser med alvorlige konsekvenser. Slike hendelser har ofte lav sannsynlighet. Husk derfor å vurdere de hendelsene med lav sannsynlighet hvis konsekvensen kan være alvorlig / katastrofal.*

Konsekvens

Ved angivelsen av konsekvens forsøker man å beskrive hvilke konsekvenser den uønskede hendelsen kan føre til. Ofte er flere utfall mulige. En mast som blåser overende, kan gi alt fra intet avbrudd til avbrudd i flere timer avhengig av hvor i nettet hendelsen skjer, framkommeligheten på stedet, tilgang på montører og reservedeler osv. Det må fattes en beslutning om én konsekvenskategori er representativ for alle de mulige konsekvensene av hendelsen eller om det å bruke kun én kategori gir en for snever fremstilling av risikoen, jf. eksemplet under og diskusjonen om usikkerhet i neste avsnitt.

For forsyningssikkerhet er beredskapsforskriften tydelig på at de alvorlige hendelsene skal kartlegges. Det betyr at vi må vie spesiell oppmerksomhet til de hendelsene som kan gi skade på viktige anlegg og avbrudd i strømforsyningen og konsekvensene knyttet til dette.

> ! *Hvis en hendelse kan ha avbrudd i strømforsyning som konsekvens i "worst case", må dette fanges opp i ROS-analysen. En logging av "worst case" må imidlertid ses i sammenheng med sannsynlighetsvurderingen. For å få en bedre angivelse av hva som kan skje, og hvor stor sjanse det er for at det skal skje, kan man derfor velge å analysere og fremstille flere separate uønskede hendelser med ulik alvorlighet i konsekvens. For eksempel kan man kalle hendelsen "Mast kantrer og gir strømavbrudd". Da oppnår man en mer presis og relevant vurdering av risiko.*

Den samme fremgangsmåten benyttes for å kartlegge konsekvenser innen andre konsekvensdimensjoner (omdømme, HMS, økonomi etc.). Det kan også være hensiktsmessig å beskrive hendelsene ulikt, jf. eksempelet over, for å få frem forskjeller mellom ulike konsekvensdimensjoner.

Hvorvidt man velger å se på en "worst case" konsekvens, en representativ konsekvens eller å fremstille den uønskede hendelsen som flere separate uønskede hendelser, må vurderes i hvert enkelt tilfelle. Basis for denne vurderingen er spennet i mulige konsekvenser, og ikke minst hva som er formålet med analysen, se avsnitt 3.1.1.

Veilederen er utgått

Usikkerhet

Hvis det er stor forskjell i hvilke utfall som er mulige, sier vi at vi har **høy usikkerhet.** Dette kan logges i analyseskjemaet med for eksempel et kryss, se Figur 12. Du kan også benytte dette feltet hvis det er mangelfull bakgrunnskunnskap om hendelsen.

Angivelsen av usikkerhet er viktig når man skal gjøre utvelgelse og prioritering av tiltak og oppfølgingsaktiviteter. Dette er tatt opp i kapitlet om risikohåndtering.

> ! *Ved å logge at usikkerheten er høy forteller du at et stort spekter av konsekvenser er mulige – hendelsen kan gi opphav til "kryss i flere celler" i risikomatrisen. Dette bør tas med senere når risikobildet skal presenteres og vil gi nyttig informasjon når tiltak og beredskap skal vurderes og prioriteres.*

Risiko- og sårbarhetsvurdering			Risikohåndtering		
	Sårbarhetsvurdering				
Usikkerhet (sett kryss)		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
...	...	...	...	...	
X		Fra kontrollrommet har en adgang til å styre inn-/utkobling av stasjon. Feil styring kan i verste fall medføre omfattende skade på anlegget, med reperasjonstid på inntil flere dager selv om en har reservedeler på lager.	1: Port og gjerder er montert. 2. Lås på port og alle dører inn til kontrollrom.	1. Montering av overvåkingskamera i anlegg (klasse 3). Ved uautorisert adgang vil kamera (ITV) og sirene aktiveres. Samtidig vil driftsentral bli varslet.	Høy
...	...	...	...	...	...
...	...	...	...	...	

Figur 12. Du kan også benytte dette feltet hvis det er mangelfull bakgrunnskunnskap om hendelsen.

Veilederen er utgått

3.2.3 Sårbarhetsvurderinger

Sårbarhet er som tidligere nevnt et systems evne til å opprettholde sin funksjon når det utsettes for påkjenninger, det vil si når det inntrer uønskede hendelser. Sårbarhet kan dermed knyttes til barrierer / tiltak som har til hensikt å begrense konsekvensene når en hendelse har inntruffet.
Sårbarhetsvurderingene på dette nivået består i å gjøre betraktninger rundt kritikaliteten av komponenten i kraftforsyningen, en vurdering av hvor robuste vern og barrierer man har, samt vurderinger rundt hvor lenge man forventer at et eventuelt avbrudd vil vare.

Nyttige problemstillinger å drøfte i analysegruppen kan være:

- Kan denne hendelsen føre til at man mister strømforsyningen?
- Er komponenten kritisk for anlegget?
- Hvilke barrierer må svikte for at man skal miste strømforsyningen av en viss varighet?
- Hva er forventet nedetid?
- Hva er worst-case nedetid?
- Finnes reservedeler på lager?
- Er det tilstrekkelig personell med nødvendig kompetanse for reparasjon og beredskap?

Et eksempel på utfylling er vist i Figur 12

> ! *En forenklet måte å logge sårbarheten på kan være å logge to forventede nedetider gitt at hendelsen skjer. Nedetid 1: Hvis man har reservedeler på lager. Nedetid 2: Hvis man ikke har reservedeler på lager. Hvis forskjellen er stor, indikerer det at komponenten er kritisk. Sårbarheten kan således reduseres ved å ha reservedeler på lager.*

Gjennom sårbarhetsvurderingen blir det klarlagt om systemet har tilstrekkelig robusthet til å stå i mot påkjenningen som den uønskede hendelsen representerer.

Veilederen er utgått

3.2.4 Identifisere mulige risikoreduserende tiltak

Eksisterende barrierer er forutsetninger
Det er svært viktig å logge hvilke barrierer og vern som allerede er på plass. Disse barrierene er forutsetninger for vurderingene som er gjort i risiko- og sårbarhetsanalysen. Det kan også være nyttig for analysegruppen som helhet å få en felles forståelse av tilstanden på barrierer og vern.

Nye barrierer og tiltak
Vi legger ikke opp til en fullstendig tiltaksanalyse i selve risikoanalysemøtet, men ofte vil forslag til barrierer dukke opp som en del av diskusjonen. Vi har satt av plass i analyseskjemaet til å logge foreslåtte nye barrierer.

Husk at tiltak kan være både sannsynlighetsreduserende (forebyggende) og konsekvensreduserende (skadereduserende), ref. bow-tie i Figur 3.

! *Å sette av plass og tid til å foreslå nye barrierer og tiltak setter fokus på forebygging og stimulerer til proaktiv holdning. Som prosessleder kan du stille spørsmålene: Hva kan gjøres for å unngå at denne hendelsen skal inntreffe? Hva kan gjøres for å unngå at denne hendelsen utvikler seg til å true forsyningssikkerheten?*

En fullstendig gjennomgang av risikoreduserende tiltak er tema i neste kapittel, Risikohåndtering.

Styrbarhet
Styrbarheten sier noe om hvor lett det er å kontrollere risikoen for en gitt hendelse. Hvor lett er det å implementere tiltak som reduserer sannsynligheten for at hendelsen skal inntreffe? Hvor lett er det å sette i verk tiltak eller høyne beredskapen for å sikre at konsekvensene av hendelsen blir små?

! *Vi anbefaler å angi styrbarheten med en tre-deling: Lav, medium, høy. Man kan for eksempel relatere styrbarheten til følgende kategorier:*
- *Høy: Innenfor selskapets kontroll, kjente tiltak finnes og kan implementeres nokså enkelt.*
- *Medium: Selskapet kan påvirke.*
- *Lav: Selskapet kan ikke kontrollere / styre risikoen. Ingen kjente, tilgjengelige tiltak.*

Angivelsen av styrbarhet er viktig når man skal gjøre utvelgelse og prioritering av tiltak og oppfølgingsaktiviteter. Dette er tema i kapitlet om risikohåndtering.

3.2.5 Presentasjon av risikobildet

Vi har nå logget uønskede hendelser og angitt hvilke konsekvenser som kan inntre, tilhørende sannsynlighet / frekvens, usikkerhet og styrbarhet. Denne informasjonen benyttes så til å presentere risikobildet.

! *Ta med uønskede hendelser, konsekvenser med tilhørende sannsynlighet / frekvens, usikkerhet og styrbarhet når risikobildet skal presenteres.*

Veilederen er utgått

Poenget med å ta med usikkerhet er å få frem uønskede hendelser som kan ha et stort spekter av konsekvenser, samt hendelser der vurderingene er gjort på et begrenset grunnlag. Vurderingen av både sårbarhet og styrbarhet er nyttig når risikoreduserende tiltak prioriteres og iverksettes.

Risikobildet kan presenteres i listeform eller ved hjelp av en risikomatrise. Har man logget risiko for flere konsekvensdimensjoner, fyller man ut en matrise for hver dimensjon. Et **eksempel** på risikomatrise for konsekvensdimensjonen forsyningssikkerhet er vist i Figur 13. Her er hendelsen ”Kantret mast” med løpenummer 4.1 plottet inn. Høy usikkerhet kan for eksempel synliggjøres ved bruk av en annen font, fete typer eller et eget symbol. Disse hendelsene tiltrekker seg da automatisk mer oppmerksomhet enn hendelser med lav usikkerhet.

Frekvens/ sannsynlighet	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. 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					4.1
1: Sjeldnere enn hvert 1000.år					

Konsekvens for forsyningssikkerhet

Figur 13 Eksempel på risikomatrise for konsekvensdimensjonen forsyningssikkerhet – det er viktig at virksomheten selv vurderer hva som skal ligge i de ulike kategoriene

Veilederen er utgått

Beredskapsforskriftens fokus retter seg i stor grad til de feltene som er merket med rødt og gult i risikomatrisen i fig 13. Dersom konsekvensen kan være alvorlig, skal forholdene analyseres selv om sannsynligheten er lav.

Ofte knyttes handlingsregler til de ulike fargene i risikomatrisen. For eksempel kan man si at for alle hendelser som havner i rødt område *må* man iverksette tiltak. For alle hendelser i gult område *bør* man iverksette tiltak, mens for hendelser i grønt område er ingen videre tiltak nødvendig. Vi vil advare mot en slik mekanisering av beslutningsprosessen. Mer om dette i neste kapittel.

! *Husk at risikomatrisen kun er et presentasjonsverktøy. Unngå å ta beslutninger utelukkende basert på hvilken fargesone en risiko havner i.*

Med hensyn på beredskapsforskriften og forsyningssikkerheten er det viktig å vurdere hendelser i nederste høyre hjørne, selv om de "bare" ligger i gult område. Dette er hendelser som kan ha svært alvorlig utfall, men der sannsynligheten for slike utfall er lav.

Andre måter å presentere risikobildet på kan for eksempel være i en matrise med risikonivå på den ene aksen og styrbarhet på den andre.

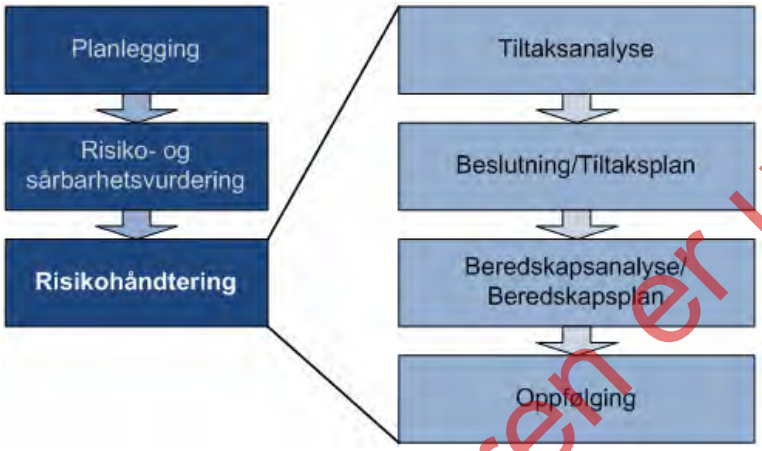
Målet med risikobildet er å enkelt kunne kommunisere "tilstanden" eller risikonivået ved anlegget / aktiviteten til omverdenen slik at nødvendige tiltak kan bli iverksatt.

! *Ledelsen i et kraftforsyningsselskap bør etterspørre eller bli forelagt oppdatert risikobilde for virksomheten på jevnlig basis. For å oppnå en helhetlig risikostyring bør oppdatert risikobilde og beredskapsspørsmål være fast punkt på ledermøter*

3.3 Risikohåndtering

Risikohåndtering består av å betrakte resultatet fra ROS-vurderingene og iverksette tiltak der hvor man finner det nødvendig. Iht. risiko- og sårbarhetsanalyseprosessen i Figur 4 inngår ledelsens vurdering og beslutning i denne aktiviteten.

Den videre strukturen på dette kapitlet er vist i Figur 14.



Veilederen er utgått

Figur 14 De ulike stegene i risikohåndteringen

Vi har valgt å dele risikohåndteringen inn i følgende steg:

1) Tiltaksanalyse
   a. Identifiser risikoreduserende tiltak
   b. Vurder og ranger tiltak utfra kost-effektivitetsbetraktninger
2) Beslutning og tiltaksplan
   a. Bestem hvilke tiltak som skal iverksettes
   b. Bestem hvem som er ansvarlig for gjennomføring
   c. Sett en frist for gjennomføring
3) Beredskapsanalyse og -plan
4) Oppfølging av tiltaksplan og beredskapsplan

3.3.1 Tiltaksanalyse

Identifisere risikoreduserende tiltak
Som tidligere nevnt kan risikoreduserende tiltak være enten sannsynlighetsreduserende (forebyggende), eller konsekvensreduserende (skadereduserende).

Det er verken nødvendig eller hensiktsmessig å foreslå risikoreduserende tiltak for samtlige av de uønskede hendelsene. Man bør hele tiden ha fokus på å sette inn innsatsen der hvor risikoen er størst og man oppnår størst risikoreduserende effekt av å sette inn tiltak.

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

Ta tak i risikobildet fra avsnitt 3.2.5. Gjennom risikomatriser og lister ser vi hvor det er viktig å redusere risikoen. Velg så ut hvilke uønskede hendelser du vil håndtere risikoen for og identifiser tiltak som kan redusere risikoen – enten for at hendelsen inntreffer, eller for at konsekvensene av hendelsen blir alvorlige.

> ! *Husk å identifisere både sannsynlighetsreduserende og konsekvensreduserende tiltak. De sannsynlighetsreduserende tiltakene er viktige for å forebygge at uønskede hendelser skjer. De konsekvensreduserende / skadereduserende tiltakene er en viktig del av beredskapen.*

Veilederen er utgått

Kost-effektivitetsvurdering av tiltak

For å prioritere ulike tiltak opp mot hverandre er det viktig å vurdere tiltakenes risikoreduserende effekt. Analysegruppen må vurdere hvert tiltak opp mot følgende spørsmål: Hvis vi innfører dette tiltaket,

- hvor mye vil sannsynligheten for den uønskede hendelsen reduseres?
- hvor mye kan konsekvensene eller skadeomfanget reduseres?
- hvor mye reduseres sårbarheten til systemet?

I tillegg angis kostnaden (ressurser / penger) ved hvert tiltak.

> ! Når risikoreduserende effekt og kostnad ved hvert tiltak er kjent, kan tiltakene rangeres ut fra kost-effektivitet.

I denne sammenhengen er det viktig å gjøre oppmerksom på at for enkelte hendelser har man ikke noe valg. Tiltak for å forebygge og eller begrense konsekvensene av mulige alvorlige hendelser som kan true kraftforsyningen, skal prioriteres foran mindre viktige forhold.

3.3.2 Beslutning og tiltaksplan

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

Som en del av beslutningen må man angi:

- Hvilke tiltak skal implementeres?
- Hvem er ansvarlig for gjennomføring?
- Hva er tidsfristen for gjennomføring?

Disse punktene utgjør til sammen en tiltaksplan.

3.3.3 Beredskapsanalyse og beredskapsplan

Dette er ikke en veiledning i beredskapsanalyse eller beredskapsplaner. ROS-analysene som er i fokus i denne veiledningen skal legge grunnlaget for en robust og hensiktsmessig beredskap. Gjennom hele gjennomgangen har vi hatt fokus på beredskapsforskriftens krav til ROS-analyser, og ved å følge anbefalingene her vil man komme et godt stykke på vei.

For å oppnå en robust beredskap må man ta resultatene fra ROS-analysen ett steg videre. Noen momenter er:

- Etablert register over uønskede hendelser kan benyttes som innspill til scenarioer man ønsker å dimensjonere beredskapen for.
- Identifiserte konsekvensreduserende tiltak og barrierer er nyttige innspill til beredskapstiltak og aktiviteter.
- Basert på kravene i beredskapsforskriften og kunnskapen fra ROS-analysene etableres en beredskapsplan.
- For å ha en fulltrent beredskapsorganisasjon må man gjennomføre beredskapsøvelser.

3.3.4 Oppfølging

Oppfølging av resultatene fra ROS-analysen og iverksetting av tiltak er en viktig del av ledelsens ansvarsområde. ROS-analysen vil på en rekke områder trolig peke på behovet for å implementere eller forsterke ulike tiltak for å sikre at beredskapsforskriftens krav blir oppfylt. Det å synliggjøre at enkelte oppfølgingsbehov er direkte knyttet til pliktene i forskriften er viktig å få synliggjort for ledelsen.

> ! 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 ledermøter.

3.3.5 Sensitiv informasjon

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 iht. beredskapsforskriften. Dette trenger ikke å angå hele ROS-analysen, men 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 tjenestelige behov og rettmessige krav, uten å gi fra seg kraftsensitiv informasjon.

Veilederen er utgått

4. Oppsummering: ROS-analyse steg for steg

Før analysemøtet: Planlegging

- Definer formålet og omfanget av analysen – sørg for forankring hos ledelsen
- Bestem hvilke konsekvensdimensjoner og konsekvenskategorier, samt hvilke kategorier som skal benyttes for sannsynlighetsdimensjonen
- Innhent informasjon om analyseobjektet
- Kall inn relevant kompetanse til analysemøte
- Etabler sjekkliste for analyseobjektet – del inn analyseobjektet i delelementer
- Gjør klar analyseskjema – test analyseskjemaet ved å prøvelogge noen hendelser

På analysemøtet: Fareidentifikasjon, risiko- og sårbarhetsvurdering

- Identifiser uønskede hendelser og fyll inn i analyseskjemaet
  - Gjennom idédugnad
  - Gjennom strukturert gjennomgang av anlegget
  - Ved bruk av sjekklister
- Gå igjennom hver identifiserte hendelse og:
  - Kartlegg bakenforliggende årsaker
  - Diskuter sannsynlighet / frekvens
  - Kartlegg hvilke konsekvenser hendelsen kan medføre, og vurder om "worst case" utfall av hendelsen kan true strøm-/fjernvarmeforsyningen og viktige anlegg. Kan én av de mulige konsekvensene representere hendelsen, eller bør hendelsen splittes? Vurder også samtidige hendelser
  - Angi om det er stor usikkerhet
  - Kartlegg eksisterende barrierer – dvs. forutsetninger for vurderingene som er gjort
  - Gjør en vurdering av sårbarheten
  - Foreslå risikoreduserende barrierer og tiltak
  - Angi styrbarheten
- Husk å dokumentere begrunnelsen for valg av kategorier for konsekvens og sannsynlighet / frekvens

Etter analysemøtet: Risikobilde og rapport. Risikohåndtering.

- Gå igjennom og kompletter analyseskjemaet. Innhent tilleggsinformasjon og tilleggsekspertise hvis nødvendig
- Avklar om det er nødvendig med mer detaljerte analyser
- Fyll inn uønskede hendelser i risikomatrise – en for hver konsekvensdimensjon
- Prioriter uønskede hendelser ut fra risikonivå og usikkerhet
- Foreslå risikoreduserende tiltak
- Skriv rapport
- Presenter risikobildet for ledelsen
- Beslutt hvor risikoreduserende tiltak skal iverksettes. Gjør en vurdering utfra:
  - Risikonivå og usikkerhet
  - Styrbarhet
  - Kost-effektivitet
- Lag tiltaksplan – sett ansvarlig for oppfølging av tiltak og tidsfrist
- Vurder om resultatene fra ROS-analysen bør føre til endringer i beredskapsplaner og beredskapsorganisasjonen
- Følg opp tiltaksplanen

Veilederen er utgått

5. Referanser

Aven, T., Røed, W., Wiencke, H.S. (2008). *Risikoanalyse*. Oslo: Universitetsforlaget.

Energi Norge (2010). *Veileder for helhetlig risikostyring for kraftbransjen.*

ISO (2009). ISO/FDIS 31000:2009. *Risk management – Principles and guidelines.*

Norges vassdrags- og energidirektorat (2009). *Forprosjekt ROS i kraftforsyningen.* 16.02.2009.

Norges vassdrags- og energidirektorat (2002). *Forskrift om beredskap i kraftforsyningen (Beredskapsforskriften).* FOR 2002-12-16 nr 1606.

Norges vassdrags- og energidirektorat (2008). *Veiledning til forskrift om beredskap i kraftforsyningen.* 29.10.2008. (under revisjon)

NOU (2000). *NOU 2000:24. Et sårbart samfunn. Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet.*

NS (2008). *NS 5814:2008. Krav til risikovurderinger.*

Proactima: www.proactima.no

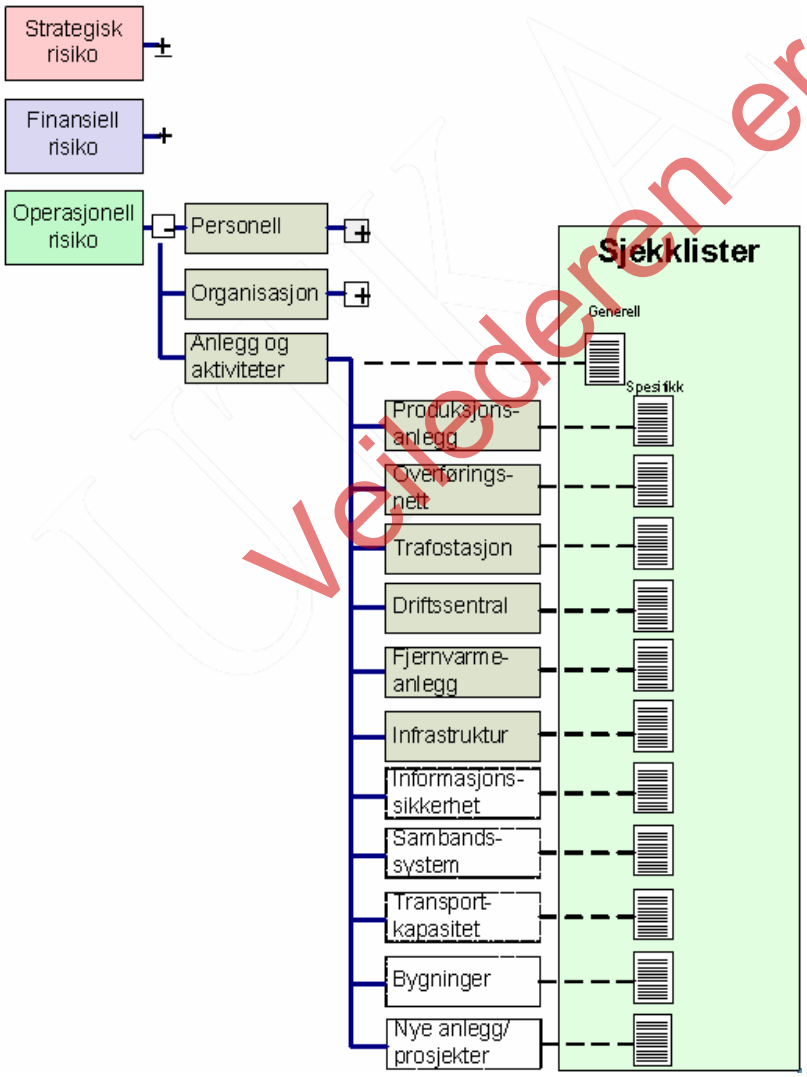
Veilederen er utgått

Vedlegg 1 – Forslag til sjekklister

Vedlegg 1 inneholder et sett med sjekklister som er ment for hjelp i en grovanalyse. Som figuren under viser, er sjekklistene bygget opp i to deler. Del 1, som vist i den første tabellen, beskriver en del hjelpeord for særskilte forhold. Denne listen er generell og kan knyttes opp mot alle de ulike anleggstypene. De særskilte forholdene er delt inn i utilsiktede handlinger (farer) og tilsiktede handlinger (trusler). Del 2, som vist i de påfølgende tabellene, danner et sett med anleggsspesifikke sjekklister. Disse spesifikke sjekklistene definerer en del typiske komponenter som inngår i anleggstypen, samt at de identifiserer en rekke uønskede hendelser som kan knyttes til denne typen anlegg.

Det er viktig å merke seg at sjekklistene ikke tar høyde for alle forhold som kan være relevante for et vilkårlig analyseobjekt. Sjekklistene skal i så måte ikke sees på som en uttømmende liste, og ytterligere kartlegging vil ofte være nødvendig for en fullstendig analyse.

Systematisk bruk av sjekklister gir mulighet for erfaringsoverføring gjennom videreutvikling av sjekklistene etter hvert som ny kunnskap tilkjennegjør seg.



Veilederen er utgått

Generell sjekkliste for ROS-analyser i kraftbransjen

Sjekkliste: Særskilte forhold

Utilsiktede handlinger (farer)

Omgivelser	**Mennesker / personale**	**Teknisk**
Tordenvær / Lynoverspenninger	Feilbetjening	Aldring
Vind	Arbeid / prøving	Utbyggingstrinn
Snø / is	Trefelling	Slitasje
Snøsig	Graving / sprengning	Korrosjon
Frost / tele	Anleggsarbeid	Lekkasje
Kvikkleire	Trafikkskade	Løse deler
Erosjon / jordsig	Kompetansemangel	Skadet / defekt del
Skred/Ras	Arbeidsmiljø	Sprekk / brudd
Vann / nedbør / fuktighet	Kommunikasjon / samhandling	Spesielle løsninger / design
Flom	Utskifting av personale	Sikkerhetssystemer
Salt / forurensing	Sykefravær	Redundans
Fremmedlegemer	Streik	Størrelse på anlegg
Fugl / dyr	Vakt- / beredskapsordninger	Teknisk dokumentasjon
Vegetasjon	Underleverandører (avhengighet)	Belastning
Brann / eksplosjon	…	Sambandsbrudd
Skogbrann		Feil i data eller programvare
Adkomst ifm særskilte situasjoner		Kjøling
…		Kaskadeeffekter
		Fellesfeil
		Branntilløp

Tilsiktede handlinger (trusler)

Direkte

Innbrudd
- Bygning / anlegg
- Datasystem (hacking)
- …

Utro ansatte
- Oppsagt
- Psykisk ubalanse
- Aktører
- Sabotasje
- Industrispionasje
- …

Utro leverandør
- Servicepersonell
- Teknisk personell…

Terror
- Frykt
- Skade fra krigslignende handlinger
- Mulige mål

Tilfeldig

Informasjonsteknologi
- Virus
- Ormer
- Trojanere
- …

Hærverk

…

Evakuering av driftssentral
- Brann i bygning
- Trusler
- …

Veilederen er utgått

Sjekkliste for ROS-analyser av produksjonsanlegg

Sjekkliste: Produksjonsanlegg		
Del-elementer / komponenter		
Inntak	Generator	Koblingsanlegg
Trykksjakt	Magnetisering	Kontroll- / verneanlegg
Innløpsrør	Skinneanlegg	Batterianlegg
Hovedstengeventil	Transformator	Stasjonsforsyning (aggregat)
Turbin	CO2 slokkeanlegg	Kjølevannsanlegg
Turbinregulator	Kabler	Skillebryter
Brannsikring	Effektbryter	Jordkniv
Strømtransformator	Spenningstransformator	Avleder
Isolator	Løpehjul	
Uønskede hendelser		
Trykksjakt kollapser	Vibrasjon	Brann
Arbeidsulykke	Ukontrollert rotasjon på turbin	Tap av styringssystem
Vannlekkasje	Oljelekkasje	Feil på stasjonsforsyning
Ventil åpner ikke	Feilfunksjon	Manglende inn-/utkobling
Ventil stenger ikke	Skade på kabler	Uønsket innkobling
Nødstenging	Klarer ikke bryte strøm	Mislykket utkobling
Havari	Overslag	Eksplosjon
Kortslutning	Dambrudd	Skred/Ras
Utilsiktet innkobling		Rørgatebrudd
Stasjonen dykkes		

Sjekkliste for ROS-analyser av transformatorstasjon

Sjekkliste: Transformatorstasjon		
Del-elementer / komponenter		
Avledere	Jordbryter	Sikring
Bygninger	Kabler	Skillebryter
Effektbryter	Klemmer	Slukkespole
Endeavslutning	Kondensatorbatteri	Spenningstransformator
Gjennomføringer	Kontroll-/måleanlegg	Strømtransformator
Innstrekkstativ	Muffer	Transformator
Isolator	Samleskinne	
Uønskede hendelser		
Havari	Uønsket innkobling Fallende	Utilsiktet innkobling
Ubalanse i fasespenning	gjenstand	Over- / underspenning
Klarer ikke bryte strøm	Brudd	Kantret mast
Mislykket innkobling	Overslag	Varmgang
Eksplosjon	Utfall	Måler feil
Frakobling	Manglende utkobling	Måler ikke
Uønsket utkobling	Manglende innkobling	Redusert kompensering

Veilederen er utgått

Sjekkliste for ROS-analyser av overføringsanlegg

Sjekkliste: Overføringsanlegg		
Del-elementer / komponenter*		
Mast	Oppheng	Kabel
Linje	Klemmeanordning	Muffe
Isolator	Flymarkør	Trykkluftanlegg
Avledere	Lynavleder	
Jording	Fundamentering/barduner	
Uønskede hendelser		
Kantret mast	Havari av isolator	Kordell brudd
Fallende gjenstand	Overslag	Brudd
Varmgang	Brudd	Mast knekker
Mekaniske skader	Oljelekkasjer	Vibrasjoner
Overslag	Overslag	Galoppering
Kortslutning / jordslutning	Lekkasje	

**Sjekklisten er med hensikt gjort meget generell. Avhengig av omfanget for analysen kan en beskrive de ulike nettene (lavspent- / distribusjon / sentral- / regionalnett) og komponentene i nettet (eks. transformatorer) kan disse vurderes sammen eller hver for seg.*

Sjekkliste for ROS-analyser av fjernvarmeanlegg

Sjekkliste: Fjernvarmeanlegg		
Del-elementer / komponenter		
Kjelanlegg	Varmesentral	Rør (gass / vann)
Kontrollsystem	Ventil (gass / vann)	Avløpsrør
Pumpe	Vannrenseanlegg	Strømforsyning
Transformator nettstasjon	Brenselsilo	Avfallslager
Generator	Kundesentral	Temperaturregulator
Uønskede hendelser		
Frost på anlegg	Gassflaske faller	Fallskader
Antennelse av brennbart materiale (brannfare)	Feil på kontrollanlegg	Svikt i kjel
Svikt i kommunalt avløp	Vannlekkasje til følsomt utstyr	Kuttskader
Koking i varmesentral	Svikt i vanntilførsel	Svikt i strømtilførsel
Utslipp av luft fra gasskjel	Utilsiktet drenering av gasskjel	Rørbrudd (vann)
Gasslekkasje	Rørbrudd (gass)	Koking i nett
Brann i avfallslager	Lekkasje i fjernvarmenett	Svikt i temperaturregulering (kundesentral)
Sikkerhetsventil blåser på personell	Utslipp (miljøforurensing) (NOx / CO2 / gass / kjemikalier?)	Varme overflater (brannskader)
Brann i brenselsilo		Havari elektrokjele - knallgass
Damputslipp		

Veilederen er utgått

Sjekklister for ROS-analyser av fysisk sikring

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

Sjekkliste for ROS-analyse av kontrollrom / driftssentral

Sjekkliste: Kontrollrom / driftssentral		
Del-elementer / komponenter		
Bygning	Brannalarm / -detektorer	Kabler
Inngang	Slokkeanlegg (gass m.m.)	IT-systemer
Dører	Håndslokkeutstyr	Kontrollromsutstyr
Vinduer	Brannfarlige materialer	
…	Sluk / avløp	
Hendelser		
Se generell sjekkliste		

Veilederen er utgått

Sjekkliste for ROS-analyse av data / sambandsrom

Sjekkliste: Data / sambandsrom		
Del-elementer / komponenter		
Bygning	Brannalarm / -detektorer	Kabler
Inngang	Slokkeanlegg (gass m.m.)	IT-systemer
Dører	Håndslokkeutstyr	
Vinduer	Brannfarlige materialer	Sambandsutstyr
…	Sluk / avløp	
Hendelser		
Se generell sjekkliste		

Sjekkliste for ROS-analyse av batterirom / aggregat / nødstrøm

Sjekkliste: Batterirom / aggregat / nødstrøm		
Del-elementer / komponenter		
Bygning Inngang Dører Vinduer Drivstofftank (størrelse/driftstid) …	Brannalarm / -detektorer Slokkeanlegg (gass m.m.) Håndslokkeutstyr Brannfarlige materialer Sluk / avløp	Kabler (felles?) Gjennomføringer Batterier Aggregat og tilkoblinger for mobilt aggregat, kjøling, dieselfilter Fysisk skille Drivstoff
Hendelser		
Overbelastning Kobler seg ikke inn Tomt for drivstoff …	Eksplosjon Brann …	

Det er viktig å teste nødstrøm. Spørsmål som kan stilles er:

- Testes det regelmessig? Hvor ofte?
- Testes det med maksimalbelastning det kan bli utsatt for (inkl. hjelpesystemer som nødlys og kjøling) over lengre tid?
- Hvor ofte foregår testen ved at ordinær strømforsyning fysisk kobles fra og med prioritert last innkoplet?
- Hvor lenge?
- Hvor mye drivstoff er på tanken – driftstid – etterforsyningsmulighet?

Veilederen er utgått

Sjekkliste for ROS-analyse av …

Sjekkliste: …		
Del-elementer / komponenter		
…		
Hendelser		

NB: Disse forslagene til sjekklister er ikke uttømmende…

Sjekklister er noe den enkelte virksomhet må utarbeide og utvikle…..

Vedlegg 2 – Forslag til analyseskjema og tiltaksplan

Skjema for Registrering av Risiko og Sårbarhet for uønsket hendelse	ID:				
Analyseobjekt:		Delsystem / komponent:			
Uønsket hendelse					
Beskrivelse av uønsket hendelse					
Årsak(er) til uønsket hendelse					
Sannsynlighet / frekvens for hendelsen	☐ *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: Sjeldnere enn hvert 1000.år*
	5: Hendelser som skjer ofte / svært ofte i selskapet *4: Hendelser som har skjedd noen ganger i selskapet* *3: Hendelser som har skjedd i selskapet eller hos andre*		*2: Har hørt om lignende hendelser i Norge eller utlandet* *1: Har aldri hørt om lignende hendelser.*		
Begrunnelse					
Konsekvens for forsyningssikkerhet	☐ *1: Ubetydelig. Ikke avbrudd*	☐ *2: Liten. Avbrudd < 10 timer hos < 10 sluttbrukere.*	☐ *3: Middels. Avbrudd < 10 timer hos < 1000 sluttbrukere eller ≥ 10 t hos < 10 sluttbrukere.*	☐ *4: Alvorlig. Avbrudd ≥ 10 timer hos < 1000 sluttbrukere.*	☐ *5: Svært alvorlig. Avbrudd ≥ 10 timer hos ≥ 1000 sluttbrukere.*
Begrunnelse:					
Konsekvens for	☐ *1: Ubetydelig.*	☐ *2: Liten*	☐ *3: Middels*	☐ *4: Alvorlig*	☐ *5: Svært alvorlig*
Begrunnelse:					
Konsekvens for	☐ *1: Ubetydelig.*	☐ *2: Liten*	☐ *3: Middels*	☐ *4: Alvorlig*	☐ *5: Svært alvorlig*
Begrunnelse:					
Usikkerhet					
Sårbarhetsvurdering					
Eksisterende barrierer / tiltak					
Foreslåtte barrierer / tiltak					
Styrbarhet					
Kommentar					

Veilederen er utgått

Beskrivelse av de ulike feltene i analyseskjemaet.

ID:
Løpenummer for enkelt å kunne identifisere hendelsen. F.eks. kan første hendelse gis ID nr 1, andre hendelse nr 2 osv. Man kan også velge å gruppere hendelser etter delsystem/komponent. F.eks. hvis en produksjonstrafo har komponent nr. 8 kan hendelsen "eksplosjon i trafo" gis ID 8.1, "transformatorhavari" gis ID 8.2 osv.

Delsystem / komponent:
Angivelse av hvilket delsystem / hvilken komponent hendelsen angår. Eksempel: Bygning, transformator, effektbryter, strømtransformator, samleskinne, etc.

Uønsket hendelse:
Navn på uønsket hendelse. Bør være presist så misforståelser unngås. Evt. kan kommentarfeltet benyttes for å utdype hendelsen. Eks: "Eksplosjon i transformator", "Svikt i sirkulasjonspumpe".

Beskrivelse / begrunnelse:
Benytt dette feltet til å fange opp så mye som mulig av beskrivelsen av hendelsen og begrunnelsen for valgte kategorier for risiko.

Årsaker:
Angi mulige årsaker til hendelsen. Tenk samtidig igjennom om det er særskilte forhold ved dette anlegget / denne komponenten som gjør at risikoen avviker fra andre anlegg / komponenter. Avvik fra regelverk kan også være en indirekte årsak og bør kartlegges her.

Sannsynlighet / frekvens:
Angi hvor ofte den uønskede hendelsen er vurdert å inntreffe. Som hjelp til valg av frekvenskategorier kan følgende inndeling benyttes:
1*: Hendelser som skjer ofte / svært ofte i selskapet.*
2: Hendelser som har skjedd noen ganger i selskapet.
3: Hendelser som har skjedd i selskapet eller hos andre selskaper som ligner på oss.
4: Har hørt om lignende hendelser i Norge eller utlandet, har ikke skjedd hos oss.
5: Har aldri hørt om lignende hendelser.

Konsekvens:
Forsyningssikkerhet bør alltid være med som konsekvensdimensjon. De øvrige konsekvensdimensjonene velges etter behov, f.eks. personellsikkerhet, ytre miljø, økonomiske tap, omdømme etc.
Det er viktig å beskrive hva man mener med en "svært alvorlig" eller "middels alvorlig konsekvens". Eksempelvis for forsyningssikkerhet kan dette se slik ut:
5: Svært alvorlig. Samfunnsviktige funksjoner som liv og helse, samt viktig infrastruktur rammet/satt ut av funksjon. Avbrudd ≥ 10 timer hos ≥ 1000 sluttbrukere.
4: Alvorlig. Alvorlige konsekvenser i infrastruktur og lokalsamfunnet. Avbrudd ≥ 10 timer hos < 1000 sluttbrukere.
3: Middels. Noen lokale konsekvenser for privatabonnenter. Avbrudd < 10 timer hos < 1000 sluttbrukere eller ≥ 10 t hos < 10 sluttbrukere.
2: Liten. Ingen samfunnskonsekvenser. Avbrudd < 10 timer hos < 10 sluttbrukere.
1: Ubetydelig. Ikke avbrudd i strømforsyning.

Veilederen er utgått

Usikkerhet:
Sett kryss hvis mange ulike konsekvenser er mulige / det er stor spredning i utfallsrommet av hendelsen (eks. eksplosjon i trafo kan gi alt fra 0 skadde til flere drepte). Sett også kryss her hvis bakgrunnsinformasjonen er mangelfull slik at det er vanskelig å vurdere frekvens / konsekvens.

Sårbarhetsvurdering:
Beskriv sårbarheten. Hva er forventet nedetid? Finnes reservedeler på lager? Kan denne hendelsen føre til at man mister strømforsyningen? Hvor kritisk er denne komponenten?

Eksisterende barrierer / tiltak:
Angi hvilke barrierer og tiltak som allerede finnes. **NB: Disse barrierene / tiltakene er en forutsetning for risikovurderingen.**

Foreslåtte barrierer / tiltak:
Foreslå risikoreduserende tiltak.

Styrbarhet:
Angi styrbarheten, dvs. hvor lett det er å redusere risikoen med barrierer / tiltak. Angis med lav - medium - høy.

Veilederen er utgått

Eksempel på utfylt analyseskjema

Skjema for Registrering av Risiko og Sårbarhet for uønsket hendelse	ID:	*4.1*

Analyseobjekt: *Transformatorstasjon*	Delsystem/komponent: *Skallsikring (port, gjerder, vinduer, dører)*

Uønsket hendelse	*Sabotasje / hærverk*
Beskrivelse av uønsket hendelse	*Uvedkommende tar seg inn på anlegget og setter viktige komponenter ut av funksjon / feilstyrer anlegget.*
Årsak(er) til uønsket hendelse	*Alarm eller kameraovervåkning er ikke installert på anlegget*
Sannsynlighet/ frekvens for hendelsen	☐ *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: Sjeldnere enn hvert 1000.år* *5: hendelser som skjer ofte / svært ofte i selskapet* *4: Hendelser som har skjedd noen ganger i selskapet* *3: Hendelser som har skjedd i selskapet eller hos andre* *2: Har hørt om lignende hendelser i Norge eller utlandet* *1: Har aldri hørt om lignende hendelser.*
Begrunnelse	*Anlegget er lett tilgjengelig. Det er lett å ta seg inn i kontrollrommet via vindu på baksiden. I dag er det ikke mulig å detektere hvorvidt det befinner seg uvedkommende i kontrollrommet.*
Konsekvens for forsyningssikkerhet	☐ *1: Ubetydelig. Ikke avbrudd.* ☐ *2:Lliten. Avbrudd < 10 timer hos < 10 sluttbrukere.* ☐ *3: Middels. Avbrudd < 10 timer hos < 1000 sluttbrukere eller ≥ 10 t hos < 10 sluttbrukere.* ☐ *4: Alvorlig. Avbrudd ≥ 10 timer hos < 1000 sluttbrukere.* ☒ *5: Svært alvorlig. Avbrudd ≥ 10 timer hos ≥ 1000 sluttbrukere.*
Begrunnelse:	*Feil styring kan medføre omfattende skade på anlegget.*
Konsekvens for personellsikkerhet	☐ *1: Ubetydelig.* ☐ *2: Liten* ☐ *3: Middels* ☐ *4: Alvorlig* ☐ *5: Svært alvorlig*
Begrunnelse:	
Konsekvens for	☐ *1: Ubetydelig.* ☐ *2: Liten* ☐ *3: Middels* ☐ *4: Alvorlig* ☐ *5: Svært alvorlig*
Begrunnelse:	

Veilederen er utgått

Usikkerhet	*Høy.*
Sårbarhetsvurdering	*Fra kontrollrommet har en adgang til å styre inn-/utkobling av stasjon. Feilstyring kan gi alvorlig skade med reparasjonstid på inntil flere dager selv om en har reservedeler på lager.*
Eksisterende barrierer / tiltak	*1: Port og gjerder er montert.* *2. Lås på port og alle dører inn til kontrollrom.*
Foreslåtte barrierer / tiltak	*1. Montering av innbruddsalarm/kamera i anlegg (klasse 3). Ved uautorisert adgang vil kamera (ITV) og sirene aktiveres. Samtidig vil driftsentral bli varslet.*
Styrbarhet	*Høy*
Kommentar	*Beskrivelse av den uønskede hendelsen "sabotasje" er ment å illustrere bruken av analyseskjemaet i Veiledning i ROS-analyse for kraftforsyningen.*

Veilederen er utgått

Analyseskjema – til bruk på storskjerm etc.

Analyseobjekt:

Gjennomført av: **Dato:**

Formål med analysen:

System		Uønsket hendelse	Risiko- og sårbarhetsvurdering								Risikohåndtering		
			Beskrivelse / begrunnelse	Årsaker	Sannsynlighet / frekvens	Konsekvens, 5: katastrofalt, 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: **Leveringssikkerhet:** bortfall av strøm/ antall kunder 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

Veilederen er utgått

Skjema for tiltakshåndtering

Funksjon / aktivitet:			
Risiko:			**Ref:**
Sammendrag: Anbefalt risikoreduserende tiltak			
Aksjonsplan **1. Foreslå tiltak**			
2. Hvilke ressurser trengs			
3. Ansvarlig			
4. Tidsplan			
5. Rapportering og oppfølging			
Ferdigstilt av:	**Dato:**	**Godkjent av:**	**Dato:**

Veilederen er utgått

Vedlegg 3 – Ord og uttrykk

ALARP prinsippet	Risikoen skal reduseres så langt som praktisk mulig (ALARP: As Low As Reasonably Practicable). ”Omvendt bevisbyrde”
Akseptkriterier for risiko	Se risikoakseptkriterium.
Analyseobjekt	Kraftsystemet bestående av tekniske, organisatoriske, miljømessige og menneskelige systemer/forhold som omfattes av risikoanalysen.
Barrierer	Tiltak og funksjoner som er planlagt for å bryte et spesifisert uønsket hendelsesforløp.
Beredskap	Omfatter alle tekniske, operasjonelle og organisatoriske tiltak som hindrer at en inntrådt fare / trussel utvikler seg til en ulykkessituasjon / tapssituasjon eller som hindrer eller reduserer virkningene av inntrådte ulykkessituasjoner / tapssituasjoner.
Beslutningskriterier	Kriterier som har innvirking på beslutninger som må tas, for eksempel akseptkriterier for risiko, økonomiske kriterier, tilgjengelig tid og hva som er politisk akseptabelt.
Forsyningssikkerhet	Begrepet forsyningssikkerhet går igjen i ulike sammenhenger når man snakker om sikkerhet og beredskap i kraftforsyningen. Forsyningssikkerhet kan forstås å inkludere energisikkerhet, effektsikkerhet og systemets evne til å håndtere ekstraordinære hendelser i kraftsystemet.
Frekvens	Forventet antall hendelser i et gitt tidsrom.
HAZID-samling	HAZard IDentification – fareidentifikasjon som foregår gjennom en tverrfaglig gruppeprosess.
Konsekvens	Følge av en uønsket hendelse. Konsekvenser kan uttrykkes kvalitativt som skadegrad eller kvantitativt som antall ulykker eller skader på anlegg, utstyr eller ressurser.
Konsekvensanalyse	Systematisk fremgangsmåte for å beskrive og/eller beregne konsekvenser for anlegg, utstyr eller ressurser som følge av initierende hendelser.
Risiko	Kombinasjon av mulige fremtidige konsekvenser / utfall og tilhørende usikkerhet. Sannsynligheter kan benyttes til å angi usikkerhet. Dersom dette gjøres, kan vi si at risiko er en funksjon av sannsynlighet og konsekvens.
Risikoakseptkriterium	Uttrykker hva som er vurdert til å være et akseptabelt (tolererbart) risikonivå, og angir en øvre grense for risiko.
Risikoanalyse	En risikoanalyse er en analyse av risiko. Analysen innbefatter identifikasjon av uønskede hendelser, årsaksanalyse, konsekvensanalysen og kartlegging av risiko.
Risikobilde	Samlet presentasjon av risikoresultater.
Risikostyring	Alle tiltak og aktiviteter som gjøres for å styre risiko.
Risikostyringspolicy	Føringer for gjennomføring av risikostyring og spesifiserer risikostyringsprosessen.
Risikoreduserende tiltak	Tiltak med sikte på å redusere sannsynlighet for og/eller konsekvens av uønskede hendelser.
Sannsynlighet	Grad av tro på at en hendelse vil inntreffe.
Styrbarhet	Styrbarhet angir i hvilken grad det er mulig å kontrollere og redusere usikkerhetene og dermed oppnå ønskede utfall.

Veilederen er utgått

Sårbarhet	Et uttrykk for et systems evne til å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet.
Usikkerhet	Mangel på kunnskap om hva som er eller vil bli verdien av en ukjent observerbar størrelse.
Uønsket (initierende) hendelse	Hendelse eller tilstand som kan medføre konsekvenser for f.eks. anlegg, utstyr eller ressurser.

Veilederen er utgått

Vedlegg 4 – Relevante lover og forskrifter, de viktigste ROS-kravene i beredskapsforskriften

Kraftforsyningsselskap har en rekke lover og forskrifter å forholde seg til. Noen av de viktigste er:

- Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven, 1990)
- Forskrift om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energilovforskriften, 1990)
- Forskrift om beredskap i kraftforsyningen (beredskapsforskriften, 2002)
- Forskrift om sikkerhet ved vassdragsanlegg (damsikkerhetsforskriften, 2010)

De viktigste paragrafene i beredskapsforskriften med hensyn på ROS er gjengitt nedenfor. Særskilte krav som må vurderes i ROS-analysene er skrevet med **fete typer**.

§ 1-3 – Risiko- og sårbarhetsanalyse
Alle enheter i KBO skal ha **oppdaterte risiko- og sårbarhetsanalyser for å identifisere virksomhetens risikopotensiale** og **de tiltak som effektivt oppfyller kravene** i denne forskriften.

Beredskapsforskriften stiller krav til at virksomheten gjennom systematisk bruk av risiko- og sårbarhetsanalyser skal kartlegge risiko og sårbarhet i forhold til *naturgitte forhold, teknisk svikt eller bevisst skadeverk* på de systemer, anlegg m.v virksomheten eier og driver.

Analysen skal også inkludere en oversikt og vurdering over alle de tiltak beredskapsforskriften lister opp som en forutsetning for tilfredsstillende beredskap. Her listes det i kortform de viktigste plikter en ROS-analyse skal favne over, utover den generelle analysen hjemlet i §1-3. Det anbefales at den til enhver tid gjeldende veiledning til beredskapsforskriften legges til grunn for analysen slik at alle plikter fremkommer i fulltekst.

§ 3-1 – Personell
Alle enheter i KBO skal kunne **dekke personellbehovet som kreves for å holde driften gående i ekstraordinære situasjoner**. For dette skal det foreligge en plan som omfatter eget personell, innleid personell og eventuelt behov for å få tilført personell fra arbeidsetaten.

§ 3-2 – Kompetanse
Alle enheter i KBO **skal ha personell med den kompetanse som kreves** i ulike funksjoner for å kunne gjennomføre oppgaver i forbindelser med ulykker, skader og andre ekstraordinære situasjoner på en sikker og effektiv måte.

§ 3-4 – Drift
Alle enheter i KBO skal i ekstraordinære situasjoner **effektivt kunne drive de kraftforsyningsanlegg og den del av kraftsystemet** enheten har ansvaret for. Enheten skal planlegge og etablere en organisasjon med kompetanse, utholdenhet og ressurser til å gjennomføre de oppgaver dette krever på en sikker og effektiv måte.

Veilederen er utgått

Kraftforsyningsanlegg, utstyr og øvrige ressurser **av betydning for drift og sikkerhet skal holdes i forsvarlig stand**. Dette utstyret og ressursene skal være tilgjengelig for enheten.

§ 3-5 – Gjenoppretting av funksjon
Alle enheter i KBO skal på **kort varsel kunne fremskaffe nødvendig antall egnede og kompetente personer til å gjenopprette nødvendige funksjoner** ved de kraftforsyningsanlegg og den del av kraftsystemet enheten har ansvaret for.

Enheten skal ha den **nødvendige oversikt over og tilgang til reservedeler, reparasjonsutstyr og øvrige ressurser** som trengs for å gjennomføre dette på en sikker og effektiv måte. Reservemateriell og andre nødvendige ressurser for gjenoppretting av funksjon skal holdes i forsvarlig stand og klar til bruk.

Enheten skal kunne dokumentere de **kraftforsyningsanlegg og den delen av kraftsystemet den har ansvaret for, herunder blant annet prioriterte kunder, utkoblbar last, koblingsbilder og flaskehalser**.

§ 3-6 – Transport
Alle enheter i KBO skal ha en **tilstrekkelig transportberedskap til å kunne håndtere ekstraordinære situasjoner, og evne til rask gjenoppretting** av funksjon.

Dette omfatter **transportmidler med nødvendig utstyr og personer** som kan håndtere disse…

§ 3-7 – Informasjon
Alle enheter i KBO skal ha **en informasjonsplan og en effektiv informasjonsberedskap** i ekstraordinære situasjoner. Dette skal blant annet omfatte informasjon internt i enheten, til berørte myndigheter, publikum og media, samt råd og anvisninger til kundene.

§ 3-8 – Samband
Alle enheter i KBO **skal ha intern og ekstern sambandsberedskap** for daglig drift, håndtering av ekstraordinære situasjoner og evne til rask gjenoppretting av nødvendige funksjoner for ledelse, drift og sikkerhet.

§ 4-5 - Adgangskontroll
Alle kraftforsyningsanlegg **skal være sikret mot adgang for uvedkommende**. Dette gjelder også øvrige bygg av betydning for kraftforsyningens ledelse og drift. Driftssentraler med tilhørende utrustning skal i tillegg defineres som egen adgangskontrollert sikkerhetssone.

§ 5-1 - Sikringsplikt
Alle anlegg som omfattes av energilovforskriften § 6-3 skal være **sikret mot uønskede hendelser og handlinger**.

Veilederen er utgått

§ 5-2 – Meldeplikt
Eiere av eksisterende og planlagte kraftforsyningsanlegg som omfattes av energilovforskriften § 6-3 – jf. energiloven § 6-6, skal **melde fra til NVE god tid før arbeidet settes i gang**.

Slike meldinger om bygging, utvidelser ombygging med videre av anlegg, skal være bilagt de dokumenter som er nødvendig for at vedtak om sikringsnivå kan treffes.

§ 5-4 – Analyse (iht. klasse)
Eier skal på bakgrunn av NVEs **vedtak om klasse foreta egen risiko- og sårbarhetsanalyse** (ROS), samt planlegge og utføre anleggene og systemene som angitt i denne forskriften. NVE skal informeres om de tiltak som planlegges utført, og når anlegget er ferdigstilt.

§ 5-5 – Sikringsnivå (iht. klasse)
Kraftforsyningsanlegg **skal etter sin klasse oppfylle følgende krav til sikring**. Beredskapsforkriften lister opp en rekke krav som skal etterleves.

§ 5-6 – Vakthold
Eier av kraftforsyningsanlegg som er prioritert for **vakthold i ekstraordinære situasjoner**, skal bidra til planlegging og gjennomføring av vaktholdet i samarbeid med politi og forsvar.

§ 5-7 - Kontroll og vedlikehold
Eier av anlegg skal **føre kontroll med at pålagt og gjennomførte sikringstiltak så som utstyr, materiell, fysiske og elektroniske anordninger er tilstede, fungerer etter hensikten og at nødvendig vedlikehold utføres**.

§ 6-1 – Generelt (informasjonssikkerhet)
Alle enheter i KBO skal foreta en **løpende helhetlig vurdering av informasjonssikkerheten**. Nødvendige tiltak og rutiner skal etableres og vedlikeholdes.

Informasjonssikkerheten i kraftforsyningen skal omfatte konfidensialitet, integritet og tilgjengelighet av informasjon og ressurs. Forskriften lister opp en rekke eksplisitte krav knyttet til denne plikten

§ 6-2 – Beskyttelse av informasjon
Sensitiv informasjon om kraftforsyningen skal ikke offentliggjøres.
Det skal identifiseres hvor sensitiv informasjon befinner seg og hvem som er rettmessige brukere av denne informasjonen.

§ 6-3 - Sikkerhetskopier
Det skal til **enhver tid foreligge oppdaterte sikkerhetskopier av informasjon og programvare som er av betydning for kraftforsyningens drift og sikkerhet**. Herunder skal all nødvendig informasjon og programvare sikres med fjernlagring av sikkerhetskopier.

Veilederen er utgått

Nødvendig dokumentasjon om kraftsystem og anlegg som lagres på datamedia skal også foreligge som utskrifter. Disse skal oppdateres årlig og oppbevares på et sikkert sted.

§ 6-4 - Særlige krav til driftskontrollsystemer
Driftskontrollsystemer omfatter driftssentraler, sambandsanlegg og øvrige anlegg og komponenter som ivaretar driftskontrollfunksjoner.

a) Planer og dokumentasjon
Alle enheter i KBO skal til en hver tid ha **oppdatert dokumentasjon** over de eksisterende og planlagte driftskontrollsystemer.

b) Tilgangskontroll
Alle driftskontrollsystemer **skal ha kontrollordninger som effektivt beskytter mot intern og ekstern uautorisert fysisk og elektronisk tilgang** og spredning av ondsinnet programvare og lignende.

c) Systemsikkerhet
Driftskontrollsystem i klasse 2 skal utføres med **redundans** frem til det enkelte kraftforsyningsanlegg i klasse 2 og 3 slik at ikke viktige funksjoner tapes på grunn av feil eller enkelt hendelse.

Driftskontrollsystem i klasse 3 **skal utføres med full redundans i hele systemet** frem til det enkelte kraftforsyningsanlegg i klasse 2 og 3, og til andre relevante driftskontrollsystemer i klasse 2 og 3, slik at en feil eller enkelt hendelse ikke kan sette viktige funksjoner ut av drift. Redundansen skal utføres med fysisk og elektronisk separering. Driftskontrollsystemet skal utføres så robust at funksjon også opprettholdes under store og langvarige påkjenninger.

Driftskontrollsystemer i klasse 3 skal kunne **fungere uavhengig av offentlige nett og teletjenester**.

Driftskontrollsystemer i klasse 2 og 3 og annet samband av betydning for kraftforsyningens drift og sikkerhet **skal minimum ha to fysisk adskilte og uavhengige sambandsveier** til kraftforsyningsanlegg i klasse 2 og 3.

d) EMP og EMI beskyttelse
Driftssentraler, annen kontrollutrustning og sambandsinstallasjoner i klasse 2 og 3 **skal beskyttes mot** elektromagnetisk puls (EMP) og elektromagnetisk interferens (EMI).

e) Brannsikkerhet
Automatisk brannalarm skal installeres i alle rom i den delen av bygget hvor driftssentralen med tilbehør er installert. Denne skal også varsle eventuell hjemmevakt.

Veilederen er utgått

f) Beredskapsrom

Alle driftssentraler i kontrollsystem klasse 3 skal **ha beredskapsrom for ledelse og driftspersonell.**

Norges vassdrags- og energidirektorat kan vedta om driftssentraler i kontrollsystem klasse 1 og 2 skal ha beredskapsrom. Beredskapsrom skal tjene som nøddriftssentral og understøtte andre ledelses- funksjoner i ekstraordinære situasjoner, samt gi personell beskyttelse.

§ 6-5 Mobile radionett - driftsradio

Alle enheter i KBO som er avhengig av pålitelig mobilkommunikasjon for drift, sikkerhet eller gjenoppretting av funksjon **skal ha tilgang til et mobilt sambandssystem**. Beredskapsforskriften gir eksplisitte krav til dette sambandssystemet.

§ 6-6 Relésamband – vern av kraftsystem

Kommunikasjonsbaserte vernsystemer i sentral- og regionalnett **skal ha pålitelige og sikre samband som fungerer upåvirket av feiltilstander i kraftsystemet**, og sørger for overføring av nødvendige signaler og meldinger mot relevante driftssentraler.

Vernsystemer skal sørge for rask og selektiv frakopling av enhet med funksjonsfeil for å begrense konsekvensen av feil i kraftforsyningssystemet.

Veilederen er utgått

Veilederen er utgått

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

Utgitt i Veilederserien i 2010

Nr. 1 Veileder i planlegging, bygging og drift av små kraftverk. Ny utgave (37 s)

Nr. 2 Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen (52 s.)

Veilederen er utgått

Norges
vassdrags- og
energidirektorat

NVE

Veilederen er utgått

Norges vassdrags- og energidirektorat

Middelthunsgate 29
Postboks 5091 Majorstuen,
0301 Oslo

Telefon: 22 95 95 95
Internett: www.nve.no