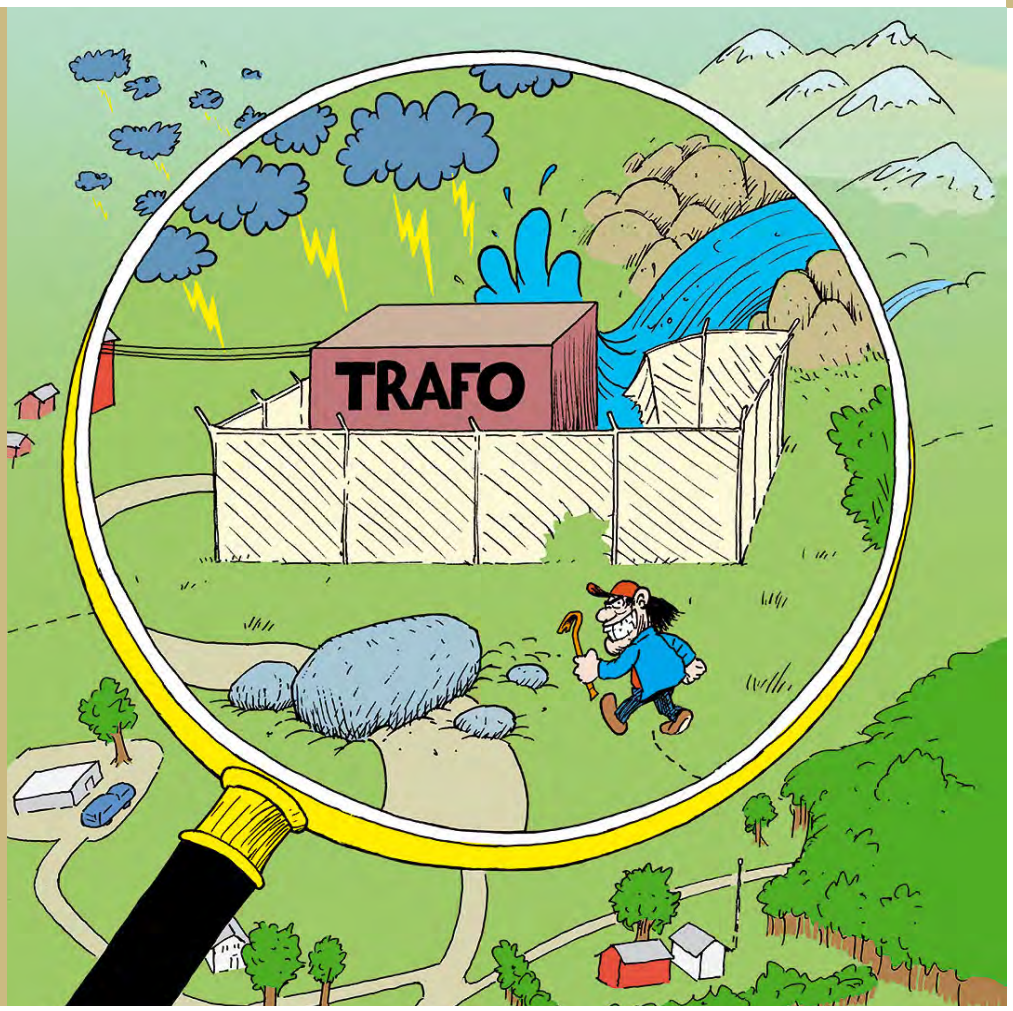
NVE

Rettleiing i risiko- og sårbarheitsanalysar for kraftforsyninga

4
2010



RETTLEIAR

Rettleiing i risiko- og sårbarheitsanalysar for kraftforsyninga

– Eit grunnlag for godt beredskapsarbeid –

Norges vassdrags- og energidirektorat
2010

Rettleiing nr. 4-2010

Rettleiing i risiko- og sårbarheitsanalysar for kraftforsyninga

Gitt ut av: Noregs vassdrags- og energidirektorat

Forfattar: *NVE & Proactima*
Denne rettleiinga er utarbeidd av Proactima på oppdrag av og i samarbeid med NVE 2010

Trykk: NVE sitt hustrykkeri
Opplag: 100
Framsidefoto: Illustrasjon: Ola H. Hegdal, NVE alle rettar
ISBN:
ISSN: 1501-0678

Samandrag: Ei innføring i korleis bruke risiko- og sårbarheitsanalysar for å tilfredsstille krava gitt av Forskrift om beredskap i kraftforsyningen.

Emneord: ROS, risikoanalysar, sårbarheitsanalysar, beredskapsforskrifta, energilova, forsyningstryggleik, kraftforsyninga, fjernvarme, nettselskap, kraftproduksjon, damtryggleik, vassdragsregulering, kraftforsyninga sin beredskapsorganisasjon (KBO), transportberedskap, driftskontroll, sensitiv informasjon, sambandsberedskap, tilgangskontroll, sikring

Språk Denne rettleiinga er tilgjengeleg på både nynorsk og bokmål. Sjå NVE sine nettsider www.nve.no for meir informasjon.

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

INNHALDSLISTE

Forord

Denne rettleiinga i bruk av risiko- og sårbarheitsanalysar har bakgrunn i krav nedfelt i Forskrift om beredskap i kraftforsyningen (beredskapsforskrifta). Ho er likevel såpass generell at ho med enkle tilpassingar også kan brukast til å analysere i samsvar med krav på andre kraftforsyningsrelevante område regulert av energilova, vassressurslova og forskrifter etter desse lovene. Fokuset og ikkje minst eksempel i denne rettleiinga er primært retta mot *korleis ein kan bruke risiko- og sårbarheitsanalysar som eit verktøy for å etterleve pliktene i beredskapsforskrifta.* Beredskapsforskrifta legg klare føringar på at norsk kraftforsyning (straum- og fjernvarmeforsyning og vassdragsregulering) skal kartleggje og vere førebudde til å handtere ekstraordinære hendingar. I denne samanhengen handlar det om å førebyggje og handtere hendingar som truar forsyningstryggleiken. Dette er gjerne hendingar som kan få alvorlege konsekvensar, ofte med lågt sannsyn. Det er viktig å presisere at eitt av krava i forskrifta er at ROS-analysane skal vere oppdaterte og dokumenterte.

Det å utarbeide slike analysar vil gi verksemda ei oversikt over risiko- og sårbarheitsforhold som kan redusere eller true verksemda si evne til å fungere. Føremålet med kravet til risiko- og sårbarheitsanalysar inkluderer for enkelte selskap det å identifisere risiko og sårbarheit ved ekstraordinære hendingar knytt til teknisk svikt, naturgitt skade og bevisst skadeverk. Vidare ligg det òg ei plikt i forskrifta til at analysen skal famne om alle beredskapstiltak som er nemnde i forskrifta. Dette inneber at ein i tillegg til å kartleggje moglege hendingar som kan true kraftforsyninga, òg har plikt til å kartleggje sårbarheit, for eksempel om pålagde beredskapstiltak vil kunne fungere under press, og kor vidt det vil vere nødvendig med fleire tiltak utover den pålagde grunnsikringa.

Den enkelte verksemda står sjølv ansvarleg for å oppfylle krav til å kartleggje risiko- og sårbarheit samt å ha tilstrekkeleg kompetanse til å utøve dette arbeidet. Dette omfattar òg det å velje metodisk verktøy. Denne rettleiinga er meint som eit hjelpemiddel for norsk kraftforsyning i arbeidet med å etterleve beredskapsforskrifta. Vi gjer merksam på at andre forskriftskrav i mindre grad er nemnde i denne rettleiinga.

Målgruppa for denne rettleiinga er verksemder som er pliktige til å følgje krava i beredskapsforskrifta, nærmare bestemt dei personane som skal leie og delta i arbeidet med å utarbeide risiko- og sårbarheitsanalysar for å oppfylle krava i forskrifta. Denne rettleiinga er noko detaljert i forklaringane, ettersom føremålet òg har vore å hjelpe dei som ikkje tidlegare har arbeidd med risiko- og sårbarheitsanalysar i større utstrekning. Dei som er svært rutinerte i arbeidet med ROS-analysar i samsvar med krava i beredskapsforskrifta, vil i mindre grad ha behov for å lese dei innleiande kapitla og kan gå direkte til kapittel 3. Er ein mindre rutinert, eller noko meir usikker på kva forskrifta krev når det gjeld arbeidet med risiko- og sårbarheitsanalysane, vil dei innleiande kapitla gi nyttige råd på vegen.

Rettleiinga er utarbeidd i perioden 2008–2010 i samarbeid med ei rekkje verksemder i kraftforsyninga, bransjeforeiningar og NVE. Konsulentselskapet Proactima

(www.proactima.no) vann anbodskonkurransen knytt til å utarbeide denne rettleiinga og har hatt hovudansvaret for å føre henne i pennen, i samarbeid med og under leiing av NVE. Rettleiinga har i tillegg blitt sendt ut på ei open høyring og blitt justert på ei rekkje område etter merknader som har kome inn.

NVE håpar at denne rettleiinga vil hjelpe den enkelte verksemda i arbeidet med å kartleggje eigen risiko og sårbarheit.

Oslo, juli 2010

Agnar Aas
vassdrags- og
energidirektør

1. Innleiing

Kraftforsyninga representerer ein grunnleggjande infrastruktur i eit moderne samfunn. Sjølv kortvarige avbrot kan få store konsekvensar for andre viktige samfunnsfunksjonar og dei enkelte innbyggjarane. Det er lang tradisjon for å stille strenge tryggleikskrav til kraftforsyninga, og all avbrotsstatistikk tilseier at kraftforsyninga har lykkast med å byggje ein robust infrastruktur med få avbrot i gjennomsnitt per sluttbrukar. Likevel har enkelthendingar bidrege til at nokre få har opplevd avbrot som har vart i fleire døgn.

I Forskrift om beredskap i kraftforsyningen (beredskapsforskrifta - BfK) blir det stilt krav til risiko- og sårbarheitsanalysar (ROS-analysar) for alle kraftforsyningsselskapa, det vil seie verksemder som utfører produksjon med tilhøyrande vassdragsregulering, overføring og distribusjon av elektrisk energi og fjernvarme etter energilova. Krava er formulerte i § 1–3 Risiko- og sårbarhetsanalyse og i § 5–4 Analyse i BfK. Ei klar tilråding er at ein set seg svært godt inn i forskriftskrava før ein startar med ROS-analysen for å sikre at analysen fangar opp dei forholda som må vere på plass. NVE har òg utarbeidd ei eiga rettleiing til beredskapsforskrifta, og denne kan lastast ned frå www.nve.no som ei hjelp til å tolke forskriftskravet.

Føremålet med beredskapsforskrifta er å førebyggje og handtere hendingar med omsyn til teknisk svikt, naturgitt skade og bevisst skadeverk. Dette skal bidra til god forsyningstryggleik. Føremålet med kravet til risiko- og sårbarheitsanalysar i beredskapsforskrifta følgjer av forskrifta: Det enkelte selskapet skal identifisere risiko og sårbarheit ved ekstraordinære hendingar knytte til teknisk svikt, naturgitt skade og bevisst skadeverk. Vidare skal analysen også famne om dei tiltaka forskrifta krev skal kunne setjast i verk av ulike beredskapstiltak.

1.1 Kva skal vi med risiko- og sårbarheitsanalysar i kraftbransjen?

Nokre viktige bruksmåtar og gevinstar ved rett bruk av ROS-analysar i kraftbransjen vil vere:

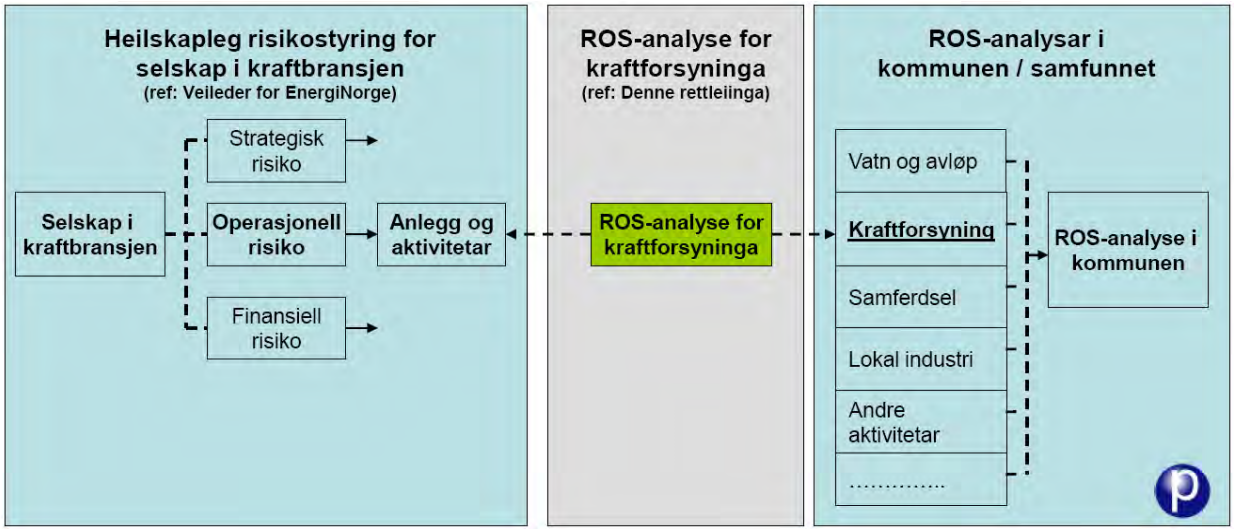
- betre evne til å førebyggje og handtere ekstraordinære hendingar
- meir stabil straumforsyning og færre avbrot
- meir fokusert ressursbruk til førebyggjande og skadereduserande tiltak
- synleggjere kva for konsekvensar ekstraordinære hendingar kan få for verksemda og samfunnet, slik at leiinga i verksemda kan bruke dette som ein viktig planføresetnad
- systematisere og dokumentere risiko og sårbarheit i samband med hendingar som verksemda kan komme til å stå overfor
- eit leiingsverktøy for betre å oppnå mål i verksemda[1]

Dei viktigaste ROS-krava i beredskapsforskrifta blir gjennomgått i Vedlegg 4.

ROS-analysar i kraftforsyninga spilar ein rolle både for å tilfredsstille behovet i samfunnet samt verksemdene sine eigne ønske og behov. Vi kan seie at ROS-analysane blir ein del av "risikostyringa" til

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

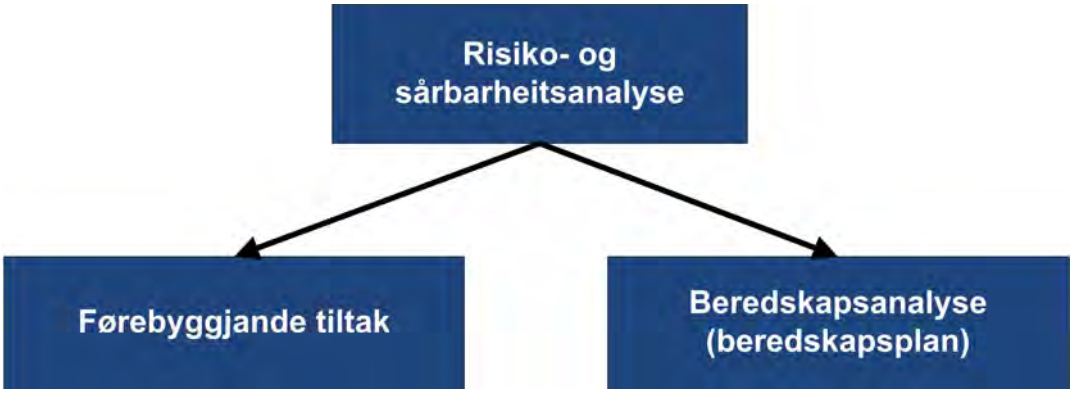
samfunnet på den eine sida og den heilskaplege risikostyringa til verksemdene på den andre sida. Dette er vist i Figur 1.



Figur 1: Samanheng mellom risikostyring på selskapsnivå, ROS-analyse av eit kraftforsyningsanlegg og samfunnstryggleik.

1.2 ROS-analysar og beredskap

ROS-analysar blir brukt til å identifisere og prioritere risikoreduserande tiltak. Nokre tiltak er årsaksreduserande (førebyggjande), det vil seie at dei forhindrar uønskte hendingar i å inntreffe. Andre tiltak er skadereduserande, det vil seie at dei avgrensar skadeverknadene dersom ei uønskt hending inntreff. Beredskapsanalysar og beredskapsplanar har som oppgåve å sikre at funksjonar raskt blir gjenoppretta når ei uønskt hending har skjedd. ROS-analysen dannar derfor eit utgangspunkt for å dimensjonere beredskapen. Vi kan dermed slå fast at ein god og robust beredskap er tufta på ein føregåande ROS-analyse.



Figur 2: Gjennom ROS-analysen blir førebyggjande og skadereduserande tiltak identifiserte. Beredskapen blir etablert basert på føregåande ROS-analyse.

1.3 Omfang og avgrensingar

Kraftforsyninga er underlagd ei rekkje lover og forskrifter som stiller krav til tryggleik, beredskap og mellom anna ROS-analysar. Desse ROS-analysane kan mellom anna vere fokusert på tryggleik for tilsette, miljøforureining og liknande. I tillegg ser vi ein aukande tendens til at selskapet sjølv stiller eigne krav som ROS-analysen skal dekkje for å ta vare på interessene til verksemda for ei heilskapleg risikostyring. Temaet for *denne* rettleiinga er ROS-analysar for å oppfylle krav i beredskapsforskrifta. Metoden vil likevel kunne brukast for å tilfredsstille krav til ROS-analysar i andre lover og forskrifter samt i verksemda si risikostyring.

Denne rettleiinga vil prøve å gi svar på desse spørsmåla:

- Kva slags krav stiller beredskapsforskrifta til risiko- og sårbarheitsvurderingar?
- Kva slags metode børe ein bruke?
- Korleis planleggje ein ROS-analyse og korleis komme i gang?
- Korleis blir dei ulike stega i ROS-analysen gjennomførte?
- Korleis følgjer ein opp resultata frå ROS-analysen?
- Korleis kan resultata visualiserast og formidlast?

For nye anlegg er det ofte hensiktsmessig å gjennomføre ROS-analysar tidleg i designfasen. I denne fasen er det som regel mykje lettare å gjere endringar enn når anlegget er ferdig bygd. ROS-analysar er dessutan eit nyttig hjelpemiddel for mellom anna å planleggje sikringstiltak som tek omsyn til lokale naturgitte forhold mv. Metoden og prosessen for ROS-analysar som blir presentert her, er så generell at han òg kan brukast i designfasen. Vi fokuserer likevel hovudsakleg på ROS-analysar av eksisterande anlegg i den vidare teksten.

Beredskapsforskrifta stiller òg krav til informasjonstryggleik og har mellom anna spesielle krav til tryggleik for driftskontrollsystem. Metoden som blir presentert i denne rettleiinga, kan langt på veg også brukast til dette føremålet, men IKT-tryggleik er eit stort tema som det vil krevje for mykje å gjennomgå grundig i ei rettleiing av dette formatet. Ein del nyttige referansar om emnet finn ein likevel i kapittel □.

Denne rettleiinga er òg tilpassa å analysere anlegg med tanke på å plassere det i ein klasse (jf. krav til analyse i BfK § 5–4). På bakgrunn av kva for klasse anlegget får av NVE, skal det gjennomførast ein eigen risiko- og sårbarheitsanalyse, og anlegga og systema skal planleggjast og utførast slik det er gitt i forskrifta.

I kapittel 2 blir det presentert ein del nyttige omgrep og teori som inngår i ein risiko- og sårbarheitsanalyse. Det blir teke utgangspunkt i ein grovanalysemetode, i og med at denne er relevant for mange av analysane som blir gjennomførde for kraftforsyninga. Kapittel 3 gir ein gjennomgang av dei viktigaste stega i ein grovanalyse, skreddarsydd for eit kraftforsyningsanlegg. I kapittel 4 blir det gitt ei oppsummering av de viktigaste punkta. Vedlegga inneheld sjekklister og analyseskjema som kan vere nyttige for å komme i gang. Der finn ein òg ei ordliste samt ei framstilling av dei viktigaste krava i beredskapsforskrifta med omsyn til risiko- og sårbarheitsanalysar.

Vi har prøvd å halde metodeskildringa på eit kortfatta og lettlest nivå. Målet er at metodeskildringa, saman med tips og råd, skal gi lesaren eit godt grunnlag for å kunne gjennomføre og bruke ROS-analysar i si eiga verksemd.

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

Hovudintensjonen med krava i beredskapsforskrifta er å unngå at kraftforsyninga stoppar opp, og/eller at det tek lang tid å gjenopprette forsyninga. Nokre av hensiktene med beredskapsforskrifta er å førebyggje og vere i stand til å handtere ekstraordinære hendingar knytt til teknisk svikt, naturgitt skade og tilsikta skade. I dei neste avsnitta er dei ovannemnde omgrepa nærmare introduserte.

For det første skal ein *førebyggje og handtere*. Målet er å *førebyggje* hendingar, slik at dei ikkje skjer. Å *handtere* tyder i denne samanhengen å ha førebudd seg slik at ein best mogleg kan unngå at hendingane får alvorlege konsekvensar dersom dei skjer.

For det andre er det *ekstraordinære hendingar* som skal førebyggjast og handterast. Det er vanskeleg å gi ein heilt presis definisjon av kva som er ei ekstraordinær hending, og i mange tilfelle vil det vere nødvendig at selskapet sjølv langt på veg definerer kva dei legg i dette omgrepet. I grove trekk kan ein seie at ei ekstraordinær hending er ei uønskt hending som går ut over det som selskapet handterer i det daglege. Eksempel på slike ekstraordinære hendingar er store klimapåkjenningar, bevisst skadeverk, total svikt i driftskontrollsystemet, mastebrot over store område pga. uvêr, massivt røyrbrot i eit fjernvarmeanlegg, handtering av ein psykisk ustabil person i ein driftssentral og innbrot og hærverk/sabotasje i ein transformatorstasjon.

Éin strategi for å redusere risikoen for ekstraordinære hendingar kan vere å konstruere system med redundans, for eksempel at det er doble linjer inn til forbrukaren. Sjølv om systemet blir bygd med redundans, er det ikkje umogleg at det kan oppstå fellesfeil, det vil seie farar, truslar og uønskte hendingar som, dersom dei inntreff, kan føre til at redundante delar av systemet feilar. I ROS-analysesamanheng er det då viktig å prøve å identifisere slike moglege fellesfeil og deretter identifisere risikoreduserande tiltak.

Eit anna aspekt ved ekstraordinære hendingar er kaskadeeffektar. Dette er fleire uønskte hendingar som skjer etter kvarandre der "det eine fører til det andre". Med andre ord: Det at ei uønskt hending inntreff, kan vere ein medverkande faktor (årsak) til at nye uønskte hendingar inntreff. Ein viktig del av ROS-analysen er å prøve å identifisere moglegheita for slike kaskadeeffektar og deretter identifisere risikoreduserande tiltak, det vil seie tiltak som reduserer sannsynet for kaskadeeffektar eller reduserer konsekvensane dersom kaskadeeffektane likevel skulle komme.

Ekstraordinære hendingar kan vere relaterte til både utilsikta og tilsikta hendingar. I avsnitta over er det vist eksempel på begge desse kategoriane.

2. ROS-analysar – kva inneber det?

2.1 Sentrale omgrep

Nokre sentrale omgrep er skildra nedanfor. I Vedlegg 3 er det gitt ei oppsummering av dei viktigaste omgrepa.

2.1.1 Risiko, sannsyn og usikkerheit

Risiko handlar om framtida. Vil vi få ein alvorleg eksplosjon i transformatorstasjonen? Vil eit tre falle over linja? Vil nokon prøve å bryte seg inn i anlegget vårt? Vil nokon kunne angripe datasystema våre, og kva vil i så fall kunne skje? Det er dette som er risiko: at hendingar med ulike konsekvensar kan komme til å skje. Risikoen har på denne måten to hovudkomponentar: i) hendingane og dei tilhøyrande konsekvensane og ii) usikkerheit om desse – vil hendingane inntreffe, og kva vil konsekvensane bli? Desse to komponentane til saman er risiko.

Vi brukar sannsyn for å uttrykkje usikkerheita om framtidige uønskte hendingar og konsekvensane av dei. Eit sannsyn er ein måte å uttrykkje usikkerheita på, eller sagt på ein annan måte, kor truleg det er at ei bestemd hending vil inntreffe. Dersom du seier at sannsynet for ei enkelt ulykkeshending er 1 %, meiner du at det er same usikkerheit for (like truleg) at hendinga inntreff, som at du ved ei tilfeldig trekking skal trekkje ei bestemd kule ut av ein boks som inneheld 100 kuler. For å skildre risikoen – slik ein gjer i risiko- og sårbarheitsanalysen – bruker ein sannsyn. Då kan vi få uttrykt om risikoen er stor eller liten.

2.1.2 Føresetnader og hypotesar

Dessverre er det ikkje berre å sjå på sannsynstala når ein skal vurdere om risikoen er høg eller låg. Hugs at tala berre er eit verktøy for å uttrykkje risikoen, og dette verktøyet er ikkje perfekt. Ein må òg ta omsyn til kva desse sannsynstala byggjer på. Når ein vurderer sannsyn, legg ein til grunn ein viss kunnskap, og ein har ofte mange føresetnader og hypotesar. Men denne kunnskapen kan vere svært avgrensa, og nokre av føresetnadene kan komme til å vise seg å vere feil. Audmjukskap er med andre ord nødvendig når vi uttalar oss om risiko. Ingen har fasitsvaret når det gjeld risiko. Likevel kan risikoskildringar vere nyttige, fordi dei får fram kunnskapane og usikkerheitene. Dette kan hjelpe oss til å ta betre avgjersler om korleis vi skal handtere risikoen, for eksempel kor omfattande beredskap vi skal ha.

2.1.3 Sårbarheit

Omgrepet sårbarheit kan karakterisere evna eit system har til å oppretthalde sin funksjon når det blir utsett for påkjenningar. I norsk samanheng er definisjonen frå NOU 2000:24 mest brukt. *Sårbarheit er eit uttrykk for eit system si evne til å fungere når det blir utsett for ei uønskt hending, samt dei problema systemet får med å ta opp att verksemda si etter at hendinga har skjedd.* Systema som blir vurderte, kan vere både overordna (store) system og underordna (mindre) system.

Det motsette av sårbarheit er robustheit. Gjennom å kartleggje sårbarheita til verksemder vil ei slik opplisting raskt kunne karakteriserast som sensitiv, og må handterast deretter.

Noko som står sentralt i omgrepet sårbarheit, er evna eit system har til å oppretthalde (og vinne att) funksjonen sin når det blir utsett for ei uønskt hending.

Eit eksempel på sårbarheitsvurdering av eit overordna system:
Tenk deg eit kraftforsyningssystem som består av fleire produksjonsanlegg, fleire trafostasjonar samt overføringsnett og fordelingsnett til sluttbrukarar. Kor sårbart er dette systemet? For å kunne svare på det må vi tenkje gjennom dette: Sårbart for kva? Vi må med andre ord starte med dei uønskte hendingane og sjå på sårbarheita i forhold til kvar av desse. Lat oss ta utgangspunkt i den uønskte hendinga linjebrot (på ein spesifikk stad i nettverket). Å vurdere sårbarheit handlar då om å vurdere i kva grad systemet er i stand til å oppretthalde sin funksjon (levere kraft) dersom eit linjebrot skjer. Det vil då vere sentralt å sjå på i kva grad vi har fleire linjer inn til sluttbrukarane som kvar kan levere etter behovet.

Eit eksempel på sårbarheitsvurdering av eit tryggleikssystem:
Ta utgangspunkt i den uønskte hendinga med at ein generator får for høgt turtal og rusar. Som eit konsekvensreduserande tiltak er det installert eit vern som skal registrere for høgt turtal, slik at ytterlegare tiltak kan setjast i verk. Kva er sårbarheita til dette vernet i forhold til den uønskte hendinga med at generatoren får for høgt turtal? Slike tankar om sårbarheit handlar om å vurdere i kva grad vernet er i stand til å gjennomføre den tiltenkte funksjonen dersom generatoren får for høgt turtal. Dette kan vere pålitelegheitsanalysar av vernet, å vurdere om det finst fellesfeil osv. For eksempel kan det tenkast at vernet kan bli skadd av vibrasjonar i generatoren og på den måten ikkje fungerer i den situasjonen det er tiltenkt.

?

Refleksjon

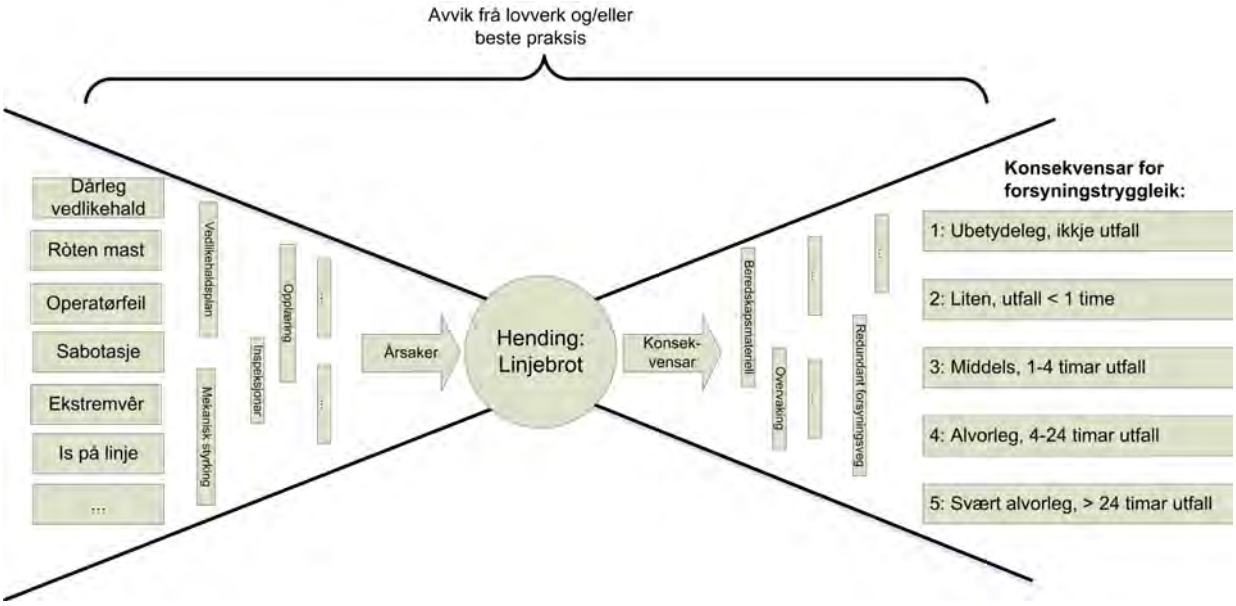
- Kva skjer dersom verksemda di mistar det viktigaste anlegget?
- Korleis blir dette handtert?
- Kva skjer dersom den viktigaste (under)leverandøren i samband med transportberedskap ikkje kan hjelpe til?
- Korleis blir dette handtert?
- Korleis får du mobilisert personell i verksemda dersom det offentlege telesystemet ikkje fungerer?

Slike og mange andre spørsmål bør stillast for å kartleggje sårbarheitane til verksemda.

2.1.4 Risiko- og sårbarheitsanalyse

Ein risiko- og sårbarheitsanalyse handlar om å identifisere hendingar som kan skje, og å vurdere risiko og sårbarheit knytt til desse hendingane. ROS-analysar kan fokusere både på positive hendingar (moglegheiter) og negative hendingar (farar/truslar). I og med at denne rettleiinga fokuserer på hendingar som skal leggjast til grunn for dimensjonering av beredskap, fokuserer vi berre på negative hendingar, eller med andre ord farar, truslar og uønskte hendingar. Vidare vil vi derfor bruke nemninga uønskte hendingar.

Feil! Ugyldig selvreferanse for bokmerke. Figur 3 viser eit såkalla bow-tie-diagram (sløyfediagram). Denne typen diagram er hensiktsmessig å bruke for å vise kva som inngår i ein ROS-analyse. I midten av diagrammet er den uønskte hendinga. I ein risiko- og sårbarheitsanalyse kartlegg vi ofte mange uønskte hendingar og framstiller desse i separate bow-tie-diagram. Til venstre i diagrammet er årsakene som kan føre til at dei uønskte hendingane kan inntreffe. Til høgre er konsekvensane dei uønskte hendingane kan få.



Figur 3: Bow-tie-diagram for uønskt hending

På venstre side kan vi ha barrierar som skal forhindre den uønskte hendinga i å inntreffe. Slike barrierar kallar vi for sannsynsreduserande (førebyggjande) barrierar eller tiltak. På høgre side har vi konsekvensreduserande (skadereduserande) barrierar og tiltak som har til hensikt å forhindre at den uønskte hendinga får alvorlege konsekvensar.

På høgre side er det vist éin konsekvensdimensjon, nemleg forsyningstryggleik. Valet av konsekvensdimensjon avgjer kva vi ønskjer å vurdere risiko for. Konsekvensdimensjonane blir ofte valt ut frå det overordna målet til verksemda. I tillegg er lover og forskrifter med på å setje fokus for analysen.

Det er viktig å merkje seg at alle risiko- og sårbarheitsanalysar har til hensikt å kartleggje heile eller delar av bow-tie-diagrammet. Kva analysemetode som blir valt, vil variere avhengig av kva som skal vere fokuset i analysen. Nokre analysemetodar eignar seg til å identifisere farar, truslar og uønskte hendingar. På same måte vil det vere metodar som er betre eigna til å vurdere årsaker, konsekvensar, kor gode barrierane er, kor sårbare barrierane er, eller å vurdere systemet i heilskap. Felles for alle desse ulike risiko- og sårbarheitsmetodane er derimot at dei kan følgje den same risikoanalyseprosessen, og at alle kartlegg anten heile eller delar av eitt eller fleire bow-tie-diagram.

2.1.5 Konsekvens

Stabil kraftforsyning er viktig for heile samfunnet. Det er særleg viktig å ha merksemd på verste falls tilfelle. At ei hending ikkje har skjedd ved anlegget (eller tilsvarande anlegg) tidlegare, tyder ikkje at ho ikkje kan komme til å skje i framtida. Alle delar av systemet som har ein kritisk funksjon i produksjons-/distribusjonskjeda, må kartleggjast, og ein må ha klart for seg kva som kan skje dersom desse blir skadde, uavhengig av kor lite sannsynleg dette blir vurdert å vere. Føremålet med beredskapsforskrifta er å forplikte dei enkelte selskapa innan kraftforsyning til å førebyggje og handtere ekstraordinære hendingar. Dette gjeld særleg i forhold til naturgitte og tilsikta hendingar, men òg i forhold til teknisk svikt.
Beredskapsforskrifta gir ein del plikter som skal bidra til å forhindre at uønskte hendingar får svært alvorlege konsekvensar. Når ein gjennomfører ROS-analysar i kraftforsyninga, er det derfor nødvendig å

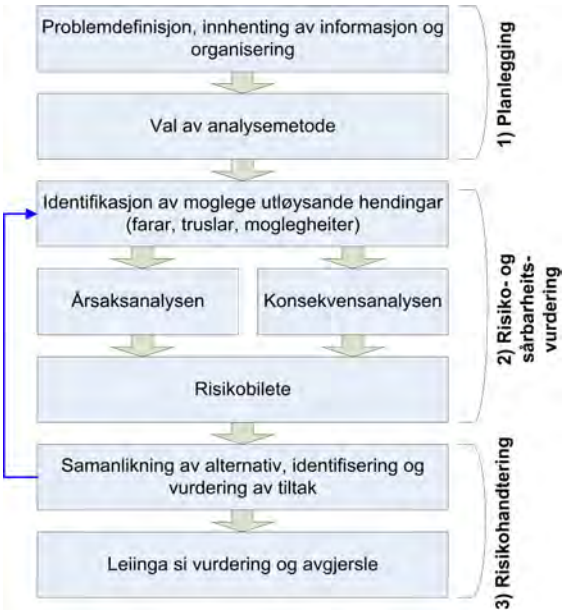
vere bevisst på å identifisere sårbarheitar og setje i verk tiltak med omsyn til viktige komponentar og anlegg dersom eit utfall vil kunne få massive konsekvensar. Dette gjeld også hendingar som er vurderte til å ha lågt sannsyn.

2.2 ROS-analyseprosessen

Det finst ei rekkje ulike eksempel på prosessar for korleis ein risiko- og sårbarheitsanalyse kan gjennomførast. Det er likevel slik at hovudinnhaldet i prosessane i stor grad er det same, sjølv om talet på boksar i framstillinga varierer. Risikoanalyseprosessen består i hovudsak av tre delar. Dette er:

1. Planlegging.
2. Risiko- og sårbarheitsvurdering.
3. Risikohandtering.

I denne rettleiinga har vi teke utgangspunkt i risikoanalyseprosessen som er skildra i boka Risikoanalyser – prinsipper og metoder, med anvendelser (Aven, Røed, Wiencke (2008)). Denne prosessen er basert på ISO 31000 (sjå Figur 4).



Figur 4: Dei ulike trinna i prosessen for risiko- og sårbarheitsanalyse (ref. Aven et al. 2008)

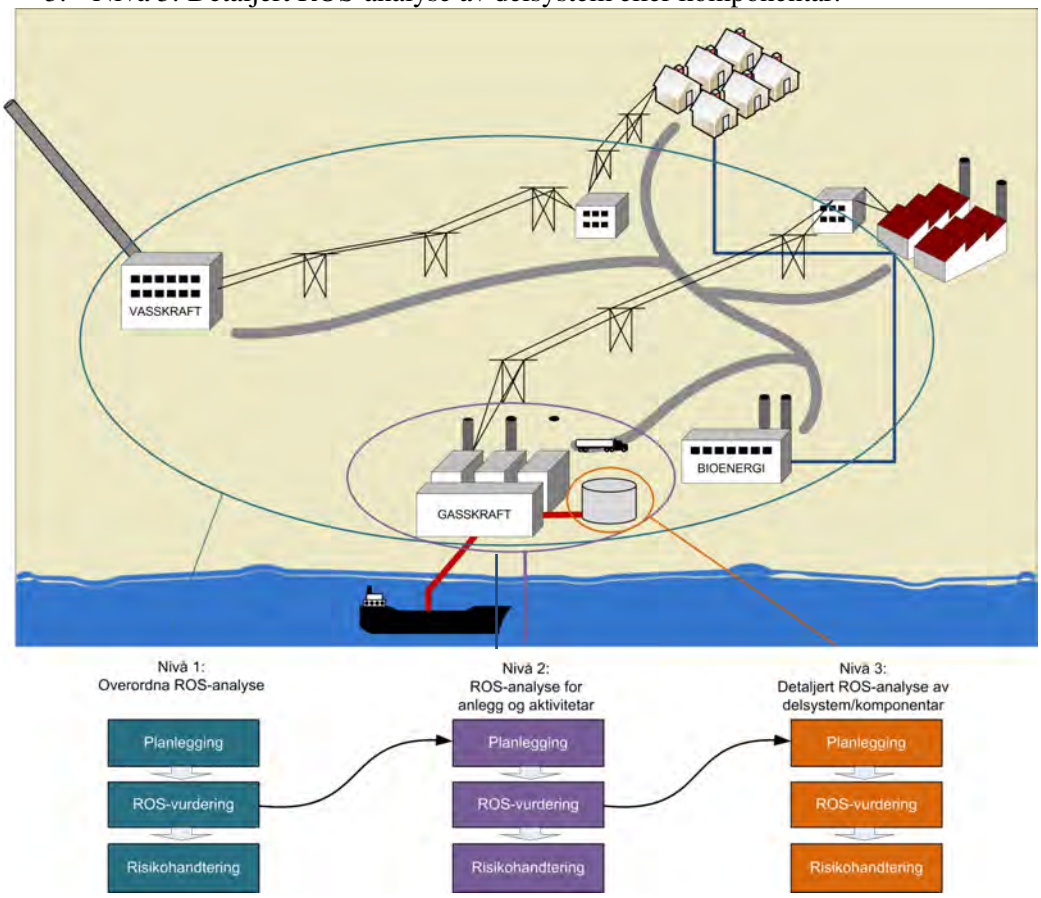
Denne generelle prosessen kan leggjast til grunn for alle ROS-analysar. Men kva slags risikoanalysemetode som blir valt, korleis risikobiletet best bør framstillast, og korleis risikoreduserande tiltak bør identifiserast og vurderast vil variere frå den eine analysen til den andre, avhengig av kva som er føremålet med analysen, kva slags objekt det er som skal analyserast, osv.

2.3 Kartleggje risikopotensialet til verksemda – nivåinndeling

Beredskapsforskrifta stiller krav om å kartleggje risikopotensialet til verksemdene. Erfaringsmessig vil arbeidet med å etablere eit heilskapleg risikobilete for verksemda gjerast på ein mest ressurseffektiv måte ved å tilpasse detaljeringsnivået i ROS-analysen ut frå det tiltenkte føremålet med analysen.

Denne nivåinndelinga er føreslege og vist i Figur 5: Ulike nivå av ROS-analysar

1. Nivå 1: Overordna ROS-analyse.
2. Nivå 2: ROS-analyse av anlegg og aktivitetar.
3. Nivå 3: Detaljert ROS-analyse av delsystem eller komponentar.



Figur 5: Ulike nivå av ROS-analysar

Refleksjon: *Kvifor bør vi ikkje gå rett i gang med detaljerte ROS-analysar?*

? ***Svar:*** *Dersom du startar med å kartleggje risikopotensialet til verksemda ved bruk av detaljerte ROS-analysar, vil du sannsynlegvis ende opp med omfattande analysar med svært avgrensa nytteverdi. Start kartlegginga på eit overordna nivå ved å gjere deg kjent med kva for anlegg som er kritiske/sårbare og kvifor. Deretter fokuserer du arbeidet på dei kritiske/sårbare anlegga og aukar detaljeringsnivået.*

2.3.1 Nivå 1: Overordna ROS-analyse

Ein ROS-analyse på overordna nivå er nyttig for å danne ei fullstendig oversikt over alle anlegga og kritiske prosessane som verksemda eig eller driv, og for kva desse har å seie for totalsystemet i ein ekstraordinær situasjon. På denne måten kan ein identifisere kva for anlegg som har mest å seie i verdikjeda. Område i systemet som vil bli slegne ut med ein gong (N-0) og føre til store konsekvensar, vil raskt rangere høgt på prioriteringslista for vidare analysar.

I den overordna analysen bør ein vurdere ulike farar og truslar og gjere seg tankar rundt uønskte hendingar som kan setje anlegga heilt eller delvis ut av drift. Vidare bør kvart anlegg og kvar kritiske prosess rangerast ut frå viktigheit for å oppretthalde produksjonen og forsyningstryggleiken. På denne måten dannar ein seg ei oversikt over sårbarheita i kraftforsyningssystemet.

Grovanalyse er ein veleigna metode for ROS-analysar på dette nivået. Nettverksanalysar (analysar av leveringspålitelegheit) og ekspertvurderingar vil kunne gi grunnlag for ein slik analyse.

Resultata frå analysen gir leiinga eit nyansert bilete av risiko og sårbarheit knytt til heile verksemda. Samtidig gir resultata grunnlag for å prioritere vidare ROS-analysar basert på kritikalitet i kraftforsyninga. Når den overordna analysen er gjennomført, kan ein gjennomføre ROS-analysar for dei enkelte anlegga og aktivitetane i prioritert rekkjefølgje (Nivå 2).

! *Prioriteringa av vidare ROS-analysar av anlegg og aktivitetar bør også sjåast i samanheng med klassifisering av anlegga, som definert av NVE, i tillegg til eiga vurdering av viktigheit.*

2.3.2 Nivå 2: ROS-analyse av anlegg og aktivitetar

I ein ROS-analyse av anlegg og aktivitetar bruker ein gjerne ein strukturert grovanalyse for å gjere ei omfattande kartlegging av moglege farar, truslar og uønskte hendingar og tilhøyrande risiko. Ein fordel med ein strukturert grovanalyse er at han kan gjennomførast med relativt avgrensa ressursar. Samtidig som metoden gjer det mogleg å etablere eit nyansert risikobilete, vil han òg avdekkje når det er behov for meir detaljerte ROS-analysar (Nivå 3).

Kapittel 3 gir ei nærmare skildring av korleis ein ROS-analyse med grovanalyse på Nivå 2 kan gjennomførast. Metoden er òg relevant for overordna analyse på Nivå 1.

Analysane som blir gjennomførte for anlegg og aktivitetar, vil i enkelte tilfelle avdekkje eit behov for meir detaljerte ROS-analysar av spesifikke delsystem, komponentar eller aktivitetar. Det vil spesielt vere hensiktsmessig å gjennomføre meir detaljerte analysar i tilfelle der det er høg usikkerheit knytt til konsekvensane av ei uønskt hending, for uønskte hendingar med høg risiko eller sårbarheit, eller i situasjonar der bakgrunnskunnskapen er mangelfull.

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

Sjølve gjennomføringa av detaljerte ROS-analysar på Nivå 3 er ikkje teke med i denne rettleiinga.

Dersom du vil gjere meir detaljerte analysar, kan du bruke kjende metodar for risiko- og sårbarheitsanalysar, for eksempel feiltre- eller hendingstreanalyse. Slike metodar er godt skildra i litteraturen, og det finst ei rekkje lærebøker på fagområdet. Det er utarbeidd fleire norske standardar (mellom anna NS 5814:2008) og ei rekkje lærebøker som kan vere til hjelp i samband med slike analysar.

Det er likevel viktig å trekkje ut funn i slike analysar, slik at desse òg kan vere viktige innspel i analysar på Nivå 1 og Nivå 2.

3. ROS-analysar i praksis – strukturert grovanalyse

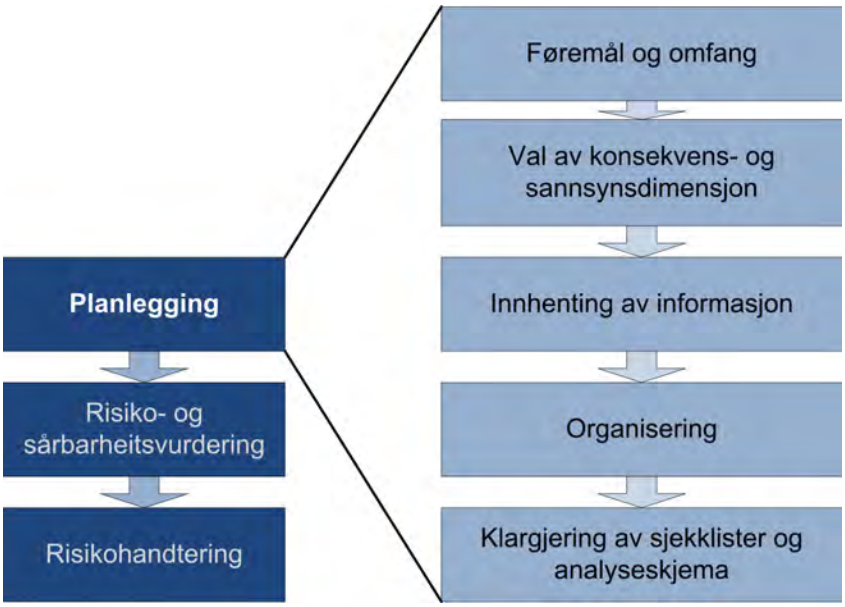
I dette kapitlet har vi fokusert på praktisk ROS-analyse på Nivå 2: ROS-analyse av anlegg og aktivitetar. Den tilrådde analysemetoden er strukturert grovanalyse med tilhøyrande analyseskjema og sjekklister. Metoden er også veleigna til ROS-analysar på Nivå 1: Overordna ROS-analyse. Metoden inneber bruk av analysemøte for å effektivisere analyseprosessen.

!	*Ofte blir det fokusert mykje på sjølve risikovurderinga (gjennomføringa), noko som gjer at ein får avgrensa tid til planlegging og oppfølging. Som ein tommelfingerregel bør 1/3 av tida setjast av til planlegging, 1/3 til risiko- og sårbarheitsvurdering og 1/3 til risikohandtering og oppfølging av resultat, av dette risikoreduserande tiltak.*

3.1 Planlegging

Det at arbeidsgruppa, som skal arbeide med ROS-analysen, har tilstrekkeleg med kunnskap om og erfaring med bruk av denne typen metode, vil ha svært mykje å seie for resultatet. Det er også viktig med god planlegging for å få eit godt resultat. Det er viktig å vere tydeleg på *kvifor* og *korleis* analysen skal gjennomførast, og ikkje minst kva for forskriftskrav som skal tilfredsstillast. Moment som bør inngå i planlegginga av ROS-analysen, er viste i Figur 6.

1. Definere føremål for og omfang av analysen.
2. Velje konsekvens- og sannsynsdimensjon.
3. Innhente informasjon.
4. Organisere arbeidet.
5. Klargjere analyseskjema og sjekklister.



Figur 6: Dei ulike stega i planlegginga av ROS-analysen

3.1.1 Definere føremål for og omfang av analysen

Å ha klare mål for analysen er ein føresetnad for å få eit godt resultat. Kvifor skal analysen gjennomførast? Kva skal resultata brukast til? Kva er det som skal analyserast? Kvar går systemgrensene? Utan å ha eit klart formulert føremål og omfang blir analysen ofte lite fokusert og gir ikkje dei svara ein treng for å gjere seg nødvendige tankar rundt tryggleiken og sårbarheita ved anlegget eller aktiviteten.

I tillegg til ein klar definisjon av føremål er det viktig å sikre forankring hos dei som tek avgjerslene i verksemda. Dette gjeld både administrativ leiing og styret. God forankring sikrar at ein har handlingsrom til å implementere risikoreduserande tiltak og etablere robust beredskap som ein del av oppfølginga av analysen.

Føremålet med ROS-analysen blir gjerne knytt opp mot krav i gjeldande lover og forskrifter, men bør også sjåast som en del av verksemda si heilskaplege risikostyring, og på den måten knytast opp mot verksemda sitt mål innan for eksempel forsyningstryggleik, HMS og/eller økonomi.

I beredskapsforskrifta er føremålet med ROS-analysar gitt som *"forebygging og håndtering av alle ekstraordinære situasjoner som kan skade eller hindre produksjon, overføring og fordeling av elektrisk kraft"*. Analysen skal også inkludere ei oversikt og vurdering over alle dei tiltaka beredskapsforskrifta listar opp som ein føresetnad for ein tilfredsstillande beredskap.

Eksempel

Føremål og omfang
ROS-analysen har som føremål å kartleggje forhold ved Energiselskapet AS sin transformatorstasjon som kan utgjere ein trussel mot forsyningstryggleiken, personaltryggleiken og det ytre miljøet. Vidare skal ein identifisere risikoreduserande tiltak for å sikre ein robust beredskap.

3.1.2 Velje konsekvens- og sannsynsdimensjon

Når føremålet med analysen er definert, kan vi avgjere konsekvensdimensjonar. I beredskapsforskrifta er det slege fast at ROS-analysen må fokusere på evna til å oppretthalde funksjonen. Det vil seie at forsyningstryggleik alltid skal inngå som konsekvensdimensjon.

Beredskapsforskrifta stiller konkrete krav til mellom anna dette:

- tilgang på nok kompetent personell og evne til drift (§ 3–1, 3–2, 3–4)
- evne til å gjenopprette funksjon (§ 3–5)
- transportberedskap (§ 3–6)
- informasjonsberedskap (§ 3–7)
- sambandsberedskap (§ 3–8)
- tilgangsberedskap (§ 4–5)
- sikring av anlegg (§ 5–1, 5–2, 5–4, 5–5, 5–6, 5–7)
- informasjonstryggleik (§ 6–1, 6–2, 6–3, 6–5, 6–6)
- driftskontrollsystem (§ 6–4)

Det tyder at ROS-analysen mellom anna må vurdere desse forholda. Vi kan sjå desse som forhold som verkar inn på forsyningstryggleiken, snarare enn å gi opphav til eigne konsekvensdimensjonar. Vi har derfor valt å ta desse med som eigne punkt i sjekklista som skal gjennomgåast i kvar ROS-analyse.

Andre konsekvensdimensjonar bør veljast ut frå det overordna målet til verksemda samt andre lover og forskrifter som verksemda er underlagd. Andre relevante konsekvensdimensjonar kan for eksempel vere:

- personaltryggleik
- ytre miljø
- økonomi
- omdømme

Vi tilrår å bruke fem kategoriar for konsekvensar og sannsyn. Dersom ein føler dette gjer analyseprosessen unødig detaljert og komplisert, kan ein bruke tre eller fire kategoriar.

Dersom kategoriane blir skildra med ord som "ubetydeleg", "liten", "middels" osv., er det viktig å seie kva ein meiner med ein "middels" konsekvens. Dvs. at vi bør prøve å kvantifisere konsekvensdimensjonen. For forsyningstryggleik kan dette sjå slik ut (men må tilpassast den enkelte verksemda):

1. Ubetydeleg. Ikkje avbrot i straum- eller fjernvarmeforsyning.
2. Liten. Ingen samfunnskonsekvensar. Avbrot < 10 timar hos < 10 sluttbrukarar.
3. Middels. Nokre lokale konsekvensar for privatabonnentar. Avbrot < 10 timar hos < 1000 sluttbrukarar eller ≥ 10 timar hos < 10 sluttbrukarar.
4. Alvorleg. Alvorlege konsekvensar i infrastruktur og i lokalsamfunnet. Avbrot ≥ 10 timar hos < 1000 sluttbrukarar.
5. Kritisk. Samfunnsviktige funksjonar som liv og helse samt viktig infrastruktur ramma / sett ut av funksjon. Avbrot ≥ 10 timar hos ≥ 1000 sluttbrukarar.

For sannsynsdimensjonen kan kvantifiseringa gjerast ved hjelp av frekvensar. Med frekvens meiner vi det forventa talet på hendingar i eit bestemt tidsrom (for eksempel i løpet av 1 år). Denne inndelinga kan brukast, men dette må tilpassast den enkelte verksemda:

1. Sjeldnare enn kvart 1000. år (har aldri høyrt om liknande hendingar). I denne gruppa kan ein også leggje forhold som er svært sjeldne, tilnærma "utenkeleg".
2. Frå kvart 100. år til kvart 1000. år (har høyrt om liknande hendingar i Noreg eller i utlandet).
3. Frå kvart 10. år til kvart 100. år (hendingar som har skjedd i selskapet eller hos andre).
4. Frå 1 gang pr. år til kvart 10. år (hendingar som har skjedd fleire gonger i eige eller andre selskap).
5. Oftare enn 1 gang pr. år (hendingar som skjer ofte / svært ofte i eige eller andre selskap).

!	*Det kan vere hensiktsmessig å nytte den same kvantifiseringa av konsekvens- og sannsynsdimensjon for alle ROS-analysar som blir gjennomførde i verksemda. Då sikrar ein at resultat frå ulike ROS-analysar blir konsistente, og at dei kan framstillast i det same risikobiletet og utgjere ein del av den heilskaplege risikostyringa i verksemda.*

3.1.3 Innhenting av informasjon

Før ein set i gang risikovurderingane, er det viktig å skaffe til vegar mest mogleg informasjon om analyseobjektet. Ulike informasjonskjelder som kan vere nyttige både under planlegginga og i sjølve risiko- og sårbarheitsvurderinga, er:

- teikningar, flytskjema eller annan dokumentasjon som skildrar analyseobjektet
- kart over anlegget og omgivnadene
- tidlegare utførde ROS-analysar
- etablerte beredskapsanalysar og beredskapsplanar

- relevant lovverk og/eller interne retningslinjer
- data over historiske uønskte hendingar som har oppstått i tilknyting til analyseobjektet eller tilsvarande anlegg
- lokalkunnskap, erfaringsdata, forsking, synfaringar

! *Informasjon som er funne å vere relevant for analysen, skal leggjast ved eller refererast til i ROS-analyserapporten. I rapporten er det også ofte hensiktsmessig å inkludere ei systemskildring/skildring av analyseobjektet.*

For å få ei god forståing av analyseobjektet vil det også vere hensiktsmessig at analysegruppa gjennomfører ei synfaring av anlegget/området, dersom dette let seg gjere. Ei synfaring kan hjelpe til med å avdekkje forhold som nyleg har endra seg eller er vanskelege å føresjå utan at ein har djupare kjennskap til anlegget. I tillegg kan synfaringa bidra til ein betre prosess ved at analysegruppa får ei felles forståing av problemstillinga.

3.1.4 Organisering

! *Når ein skal gjennomføre ROS-analysar av anlegg og aktivitetar, er det ofte hensiktsmessig å gjennomføre fareidentifikasjon og risikovurdering på eitt eller fleire analysemøte.*

Det er viktig å sikre at folk med kunnskap og kompetanse om analyseobjektet er tilgjengelege når ROS-analysen skal gjennomførast. I tillegg vil det vere ein fordel at ein person med erfaring med å gjennomføre ROS-analysar har rollen som prosessleiar. På sjølve analysemøtet vil det vere lurt å ha utpeikt ein person til å ta notat og føre analyselogg / fylle ut analyseskjemaet.

! *Når ein skal gjennomføre ROS-analysar av komplekse og samansette system, er det både hensiktsmessig og nødvendig å ta i bruk analysemøte som består av ei tverrfagleg analysegruppe. Deltakarane i denne gruppa bør ha ulik bakgrunn og kompetanse, som f.eks. drift, vedlikehald, driftssentralsystem, montørar osv. Behovet for å dekkje alle fagområde må samtidig balanserast mot behovet for å halde talet på deltakarar på eit handterbart nivå. Erfaringa viser at slike grupper ikkje bør vere på meir enn åtte personar dersom dei skal vere effektive. Det er viktig at forarbeid og etterarbeid blir gjort i ei mindre prosjektgruppe for at prosessen skal bli effektiv.*

I tillegg må alle i analysegruppa bli gjort merksame på kva for ein rolle dei har i ROS-analyseprosessen.

Ulike ansvar og rollar på analysemøtet

Dette er hovudoppgåvene til prosessleiaren:

- planleggje analysen
- styre diskusjonane
- sikre framdrift / passe tida
- bruke etablert metode aktivt

Dette er hovudoppgåvene til analysegruppa:

- bidra med eigen kompetanse/erfaring/ekspertise
- tenkje utanfor eigen erfaring og eige arbeidsområde
- arbeide konstruktivt og målretta
- hjelpe til med å formulere tilrådingar
- lytte til andre sine bidrag

Oppgåvene til loggføraren:

- sørgje for at mest mogleg av bakgrunnskunnskap, føresetnader, hypotesar og grunngiving for risikovurderinga blir dokumentert
- vere ei støtte for prosessleiaren
- avdekkje hol og manglar i det som har vore diskutert så langt på møtet

3.1.5 Gjere klar sjekklister og analyseskjema

Analyseskjema og skreddarsydde sjekklister er ein sentral del av grovanalysemetoden. På bakgrunn av synfaring, tilgjengeleg informasjon og bakgrunnskunnskap om analyseobjektet kan ein gjere klar sjekklister og analyseskjema til bruk på analysemøtet.

Sjekklister

Vi har presentert nokre sjekklister i Vedlegg 1 som kan brukast som utgangspunkt. Sjekklistene består av to delar, ein generell del og ein del som gjeld spesifikt for det aktuelle analyseobjektet.

Figur 7 viser den samansette sjekklista for eit produksjonsanlegg.

Generell sjekkliste for ROS-analysar i kraftbransjen

Sjekkliste: Særskilde forhold		
Utilsikta handlingar (feiar)		
Omgivnadar	**Menneske / personale**	**Teknisk**
Torevêr / lynoverspenningar	Feil bruk	Aldring
Vind	Arbeid / prøving	Utbyggingstrinn
Snø / is	Trefelling	Slitasje
Snøsig	Graving / sprenging	Korrosjon
Frost / tele	Anleggsarbeid	Lekkasje
Kvikkleire	Trafikkskade	Lause delar
Erosjon / jordsig	Kompetanse	Skadd / defekt del
Skred	Arbeidsmiljø	Sprekk / brot
Vatn / nedbør / fukt	Kommunikasjon / samhandling	Spesielle løysningar / design
Flaum	Utskifting av personale	Tryggleikssystem
Salt / forurening	Sjukefråvær	Redundans
Framandlekamar	Vakt- / beredskapsordningar	Storleik på anlegg
Fuglar / dyr	Underleverandørar (avhengigheit)	Teknisk dokumentasjon
Vegetasjon	...	Leveringskvalitet
Brann / eksplosjon		Belastning
Skogbrann		Sambandsbrot
Ras		Feil i data eller programvare
...		Kjøling
		Kaskadeeffekter
		Fellesfeil
		...
Tilsikta handlingar (truslar)		
Direkte	**Tilfeldig**	
Innbrot	Informasjonsteknologi	
– Bygning / anlegg	– Virus	
– Datasystem (hacking)	– Ormar	
– ...	– Trojanarar	
Utru tilsette	– ...	
– Oppsagd	Hærverk	
– Psykisk ubalanse	...	
– Aktorar		
– Sabotasje		
– Industrispionasje		
– ...		
Utru leverandørar		
– Servicepersonell		
– Teknisk personell		
– ...		
Terror		
– Frykt		
– Skade frå krigsliknande handlingar		
– Møglege mål		

Sjekkliste for ROS-analysar av produksjonsanlegg

Sjekkliste: Produksjonsanlegg		
Del-element / komponentar		
Inntak	Generator	Koplingsanlegg
Trykksjakt	Magnetisering	Kontroll- / vernanlegg
Innløpsrøyr	Skinneanlegg	Batterianlegg
Hovudstengjeventil	Transformator	Stasjonsforsyning (aggregat)
Turbin	CO2-slokkjeanlegg	Kjølevassanlegg
Turbinregulator	Kablar	Skillebrytar
Brannsikring	Effektbrytar	Jordknivar
Straumtransformator	Spenningstransformator	Avleiar
Isolator	Løpehjul	Vassbrems
Uønskte hendingar		
Trykksjakt kollapsar	Vibrasjon	Brann
Arbeidsulykke	Ukontrollert rotasjon på turbin	Tap av styringssystem
Vasslekkasje	Oljelekkasje	Feil på stasjonsforsyning
Ventil opnar ikkje	Feilfunksjon	Manglande inn-/utkopling
Ventil stenger ikkje	Skade på kablar	Uønskt inkopling
Nødstenging	Klarar ikkje bryte straum	Mislukka utkopling
Havari	Overslag	Eksplosjon
Kortslutning	Dambrot	Ras
Utilsikta inkopling		Røyrgatebrot
Stasjonen blir dykka		

Figur 7: Samansett sjekkliste for eit produksjonsanlegg – generell del til venstre og spesifikk del til høgre (ein meir utskriftsvenleg versjon av sjekklistene for ulike typar anlegg ligg i Vedlegg 1).

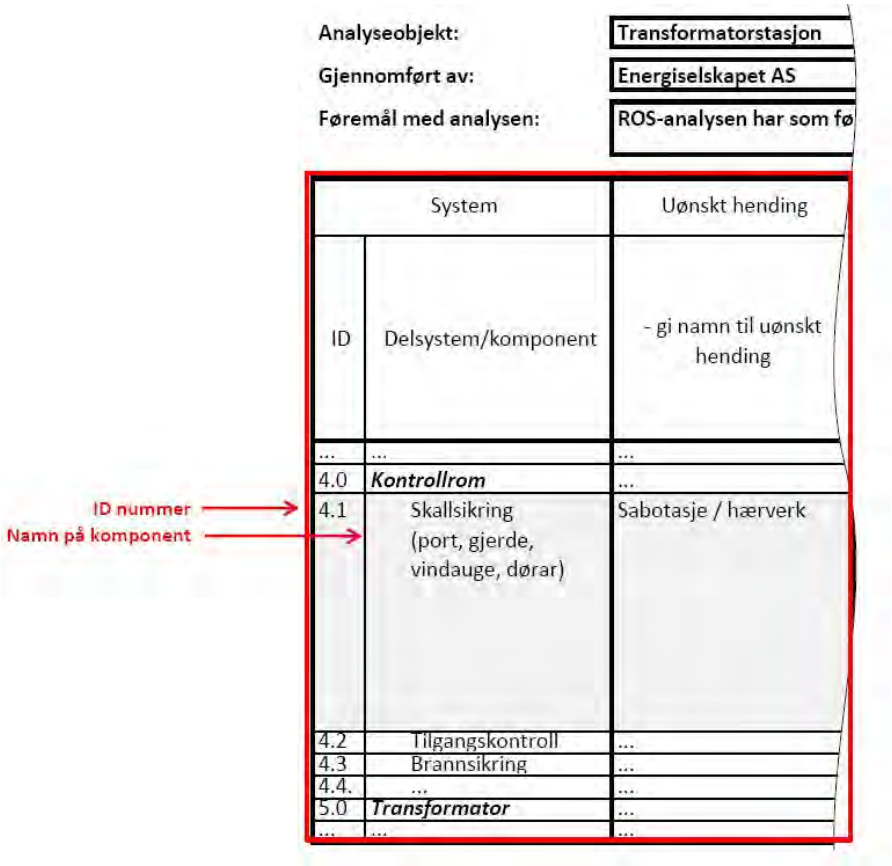
Sjekklistene bør utvidast og justerast etter behov, tilpassa det aktuelle anlegget.

Analyseskjema

I Vedlegg 2 er det vist to typar analyseskjema. Med det første kan ein logge éi hending per ark, og dette er gunstig til utskrift og manuell utfylling i ei mindre arbeidsgruppe. Den andre typen legg opp til at ein loggar uønskte hendingar fortløpande under kvarandre i eit rekneark, og passar for vising på storskjerm og direkte utfylling på eit analysemøte. Sjølv om skjemaa har ulikt format, er innhaldet, dvs. felta som skal fyllast ut, dei same.

> ! *Analyseskjemaet bør testast ut før ein går på analysemøtet. Føreslå nokre uønskte hendingar, og fyll desse inn i skjemaet. Det er viktig at formatet på skjemaet fungerer for deg som prosessleiar.*

Ein viktig del av planleggingsaktiviteten går ut på å dele analyseobjektet inn i delsystem og komponentar. Dersom du vel å bruke reknearket, kan du førehandsutfylle dei ulike delsystema og komponentane før du går i analysemøtet. Eit eksempel er vist i Figur 8.



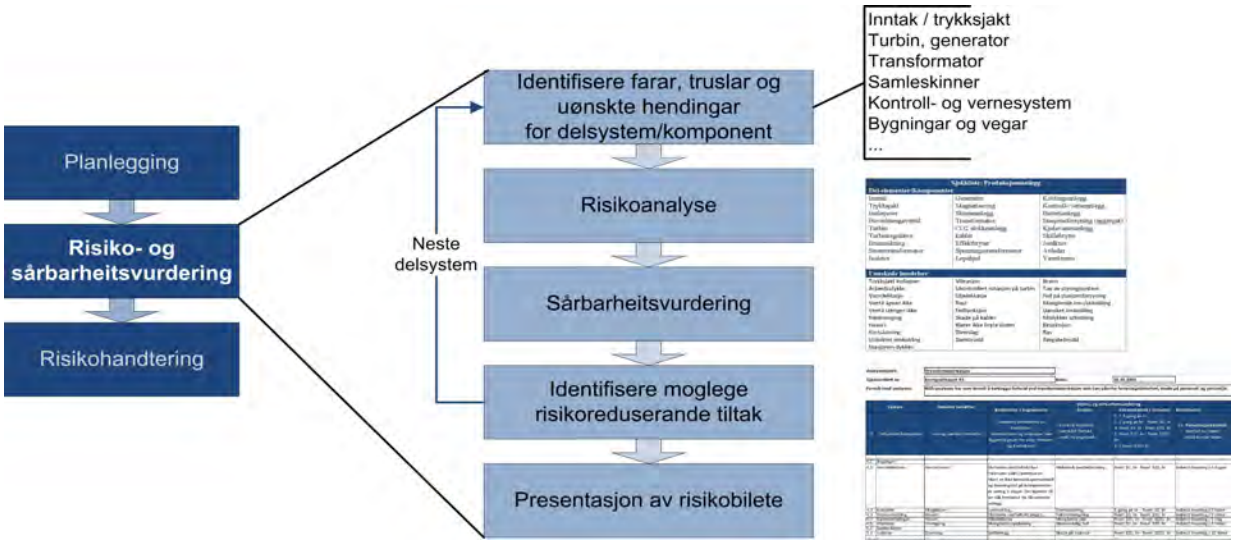
Figur 8: Dei ulike stega i risiko- og sårbarheitsvurderinga

3.2 Risiko- og sårbarheitsvurdering

I Figur 9 er dei ulike stega som inngår i risiko- og sårbarheitsvurderinga, vist. Desse er:

1) identifisere farar, truslar og uønskte hendingar
2) risikoanalyse av uønskt hending
3) sårbarheitsvurdering av uønskt hending
4) identifisere moglege risikoreduserande tiltak
5) presentere risikobilete

Til høgre i figuren ser vi inndelinga i delsystem/komponentar, sjekklister og analyseskjemaet. Desse hjelpemidla blir brukt aktivt i denne fasen av ROS-analysen.



Figur 9: Dei ulike stega i risiko- og sårbarheitsvurderinga

Kort oppsummert kan vi seie at punkt 1) til punkt 4) handlar om å fylle ut analyseskjemaet vi presenterte i førre avsnitt. Punkt 5), risikobilete, handlar om å presentere og formidle resultata på ein oversiktleg måte.

3.2.1 Identifisere farar, truslar og uønskte hendingar

> ! *Hugs å kartleggje risikoen og sårbarheita til anlegget med tanke på naturgitte forhold, teknisk svikt og bevisst skadeverk. Ubevisste feilhandlingar må òg takast med.*

Ifølgje beredskapsforskrifta skal det identifiserast hendingar som truar den evna kraftforsyninga har til å fungere slik ho skal, samt til å verne anlegg, ressursar og informasjon mot naturgitte forhold, teknisk svikt og bevisst skadeverk. Ubevisste feilhandlingar må òg takast med. Det kan òg vere aktuelt å vurdere andre hendingar som er relevante i forhold til bedrifta si måloppnåing. Dette vil til ein viss grad vere styrt av dei konsekvensdimensjonane ein har valt å bruke, sjå avsnitt 3.1.2.

Ofte har møtedeltakarane før møtet tenkt gjennom ulike ting som kan gå gale ved anlegget eller aktiviteten. Det er viktig at denne informasjonen blir dokumentert tidleg på møtet, mens han enno sit friskt i minnet. Vi tilrår derfor følgjande framgangsmåte for å identifisere farar, truslar og uønskte hendingar:

- Idédugnad. Møtedeltakarane får moglegheit til å "tømme hovudet".
- Strukturert gjennomgang av anlegget – farar, truslar og uønskte hendingar for delelement og komponentar blir identifisert.
- Gjennomgang av sjekklista.

! *Som prosessleiar er det di oppgåve å stimulere analysegruppa til å tenkje og skildre kva som kan gå gale ved anlegget/aktiviteten. Du bør vere bevisst på korleis du stiller spørsmåla til analysegruppa. "Kva kan gå gale med denne komponenten?", "Kan denne komponenten havarere?", "Kva skjer dersom …?".*
Ver nysgjerrig. Det er betre å stille for mange spørsmål enn for få. "Dumme" spørsmål kan ofte vere smarte på den måten at analysegruppa blir tvungen til å tenkje gjennom uvande problemstillingar.

I den strukturerte gjennomgangen tek ein utgangspunkt i å dele opp anlegget i delsystem og komponentar og identifiserer farar, truslar og uønskte hendingar for kvart element. Eit eksempel er vist i

System		Uønskt hending	Skildring / grunngiving
ID	Delsystem/komponent	- gi namn til uønskt hending	Nærmare skildring av hendinga. Kommentarar og diskusjon som ligg til grunn for valt frekvens og konsekvens.
…	…	…	…
4.0	***Kontrollrom***	…	…
4.1	Skallsikring (port, gjerde, vindauge, dørar)	Sabotasje / hærverk	Anlegget er lett tilgjengeleg. Det er lett å ta seg inn i kontrollrommet via ulåst dør på baksida. I dag er det ikkje mogleg å oppdage om det er uvedkomande i kontrollrommet.
4.2	Tilgangskontroll	…	…
4.3	Brannsikring	…	…
4.4.	…	…	…
5.0	***Transformator***	…	…
…	…	…	…

Fyll inn i analyseskjema:
1. Uønskte hendingar, og
2. Skildring av hendinga

Figur 10: Analyseskjema – utfylling (uønskt hending + skildring)

I samband med identifisering av uønskte hendingar diskuterer ein ofte forhold rundt hendinga – kva er hendingsgangen, årsaker, moglege konsekvensar, om dette har skjedd tidlegare osv. Dette er viktig bakgrunnsinformasjon for risikoanalysen og bør loggast i feltet merkt Skildring/grunngiving.

Til slutt går ein gjennom sjekklistene (avsnitt 3.1.5 og Vedlegg 1) for å fange opp moglege forhold som ikkje er fanga opp til no.

> **!** *Ofte vil identifiseringa av hendingar følgje ein 80-20-regel. Deltakarane bør ha tenkt gjennom ulike forhold ved anlegget på førehand, og det er viktig at alle får sjansen til å "tømme hovudet" i form av ein idédugnad nokså tidleg på møtet. Dette kan ofte kartleggje ca. 80 % av dei uønskte hendingane og dessutan identifisere ein del viktige tiltak. Dei resterande 20 % av dei uønskte hendingane blir deretter fanga opp ved hjelp av ein strukturert gjennomgang av delsystem og komponentar med tilhøyrande sjekklister. Den første idédugnaden tek vanlegvis mykje kortare tid (20 %) enn den strukturerte gjennomgangen (80 %).*

> **!** *Fokuser og prioriter tida slik at det blir sett av nok tid til dei viktige, alvorlege hendingane. Gå raskare gjennom hendingar med mindre alvorleg konsekvens.*

3.2.2 Risikoanalyse

For kvar av dei uønskte hendingane ser vi nærmare på årsaker, sannsyn, konsekvensar samt føresetnader og hypotesar. Dei viktigaste felta i analyseskjemaet er vist i Figur 11.

Uønskt hending	Skildring / grunngiving	Årsaker	Sannsyn / frekvens	Konsekvens
- gi namn til uønskt hending	Skildre årsak, frekvens og konsekvens for kvar av dei uønskte hendingane.	- årsak til hending - særskilde forhold - avvik frå regelverk ...	5: > 1 gang pr. år 4: 1 gang pr. år - kvart 10. år 3: kvart 10. år - kvart 100. år 2: kvart 100. år - kvart 1000. år 1: < kvart 1000. år	K1: Forsyningstryggleik: bortfall av straum / tal på kunder som er råka
...	...	...	...	...
...	...	...	...	
Sabotasje / hærverk	Anlegget er lett tilgjengeleg. Det er lett å ta seg inn i kontrollrommet via ulåst dør på baksida. I dag er det ikkje mogleg å oppdage om det er uvedkomande i kontrollrommet.	Alarm eller kameraovervaking er ikkje installert på anlegget	Kvart 100. år - kvart 1000. år	Avbroten levering i fleire dagar

Figur11: Analyseskjema – utfylling (årsaker, sannsyn, konsekvensar)

Ein del av denne informasjonen kan allereie vere fanga opp i feltet Skildring/grunngiving.

Årsaker

Nemn moglege årsaker til hendinga. Tenk samtidig gjennom om det finst særskilde forhold ved dette anlegget / denne komponenten som gjer at risikoen avvik frå andre tilsvarande anlegg/komponentar. Avvik frå regelverk eller beste praksis kan også vere ei indirekte årsak til uønskte hendingar, og bør kartleggjast her.

Sannsyn/frekvens
Kor stor sjanse er det for at hendinga skal skje? For å vurdere dette kan vi for eksempel bruke frekvenskategoriane som blei definerte i avsnitt 3.1.2. Her kan historiske data, feilstatistikk for kjende komponentar, ekspertvurderingar osv. leggjast til grunn.

! *Det å berre basere seg på historiske data og feilstatistikk når ein skal vurdere sannsyn og frekvens, er uheldig og kan samanliknast med å køyre bil ved å sjå ut bakvindauget. Ein pragmatisk bruk av statistikk er fornuftig – bruk historiske data der datagrunnlaget er godt og komponentar og omgivnader er samanliknbare. I andre tilfelle er ein avhengig av ei subjektiv vurdering. Det siste kan vere uvant for enkelte.*

! *Beredskapsforskrifta er særleg oppteken av hendingar med alvorlege konsekvensar. Slike hendingar har ofte lågt sannsyn. Hugs derfor å vurdere hendingar med lågt sannsyn dersom konsekvensen kan vere alvorleg/katastrofal.*

Konsekvens
Når ein oppgir konsekvens, prøver ein å skildre kva for konsekvensar den uønskte hendinga kan føre til. Det er ofte fleire moglege utfall. Ei mast som blæs over ende, kan gi alt frå null avbrot til avbrot i fleire timar, avhengig av kvar i nettet hendinga skjer, framkomet på staden, tilgang på montørar og reservedelar osv. Det må takast ei avgjersle med omsyn til om éin konsekvenskategori er representativ for alle dei moglege konsekvensane av hendinga, eller om det å bruke berre éin kategori gir ein for snever framstilling av risikoen, jf. eksemplet under og diskusjonen om usikkerheit i neste avsnitt.

For forsyningstryggleik er beredskapsforskrifta tydeleg på at dei alvorlege hendingane skal kartleggjast. Det tyder at vi må vie spesiell merksemd til dei hendingane som kan gi skade på viktige anlegg og avbrot i straumforsyninga samt konsekvensane som er knytte til dette.

! *Dersom ei hending kan ha avbrot i straumforsyning som konsekvens i "worst case", må dette fangast opp i ROS-analysen. Ei logging av "worst case" må derimot sjåast i samanheng med vurderinga av sannsyn. For å få ei betre forståing av kva som kan skje, og kor stor sjanse det er for at det skal skje, kan ein derfor velje å analysere og framstille fleire separate uønskte hendingar med ulike konsekvensar som ikkje alle er like alvorlege. Ein kan for eksempel kalle hendinga "Mast kantrar og gir straumbrot". Då oppnår ein ei meir presis og relevant vurdering av risiko.*

Den same framgangsmåten kan brukast for å kartleggje konsekvensar innan andre konsekvensdimensjonar (omdømme, HMS, økonomi osv.). Det kan også vere hensiktsmessig å skildre hendingane på ulik måte, jf. eksemplet over, for å få fram forskjellar mellom ulike konsekvensdimensjonar.

Kor vidt ein vel å sjå på ein "worst case"-konsekvens, ein representativ konsekvens eller å framstille den uønskte hendinga som fleire separate uønskte hendingar, må vurderast i kvart enkelt tilfelle. Grunnlaget for denne vurderinga er spennet i moglege konsekvensar, og ikkje minst kva som er føremålet med analysen, sjå avsnitt 3.1.1.

Usikkerheit

Dersom det er stor forskjell i kva for utfall som er moglege, seier vi at vi har **høg usikkerheit.** Dette kan loggast i analyseskjemaet med for eksempel eit kryss, sjå Figur 12. Du kan også bruke dette feltet dersom det er lite bakgrunnskunnskap om hendinga.

Det å oppgi usikkerheit er viktig når ein skal velje ut og prioritere tiltak og oppfølgingsaktivitetar. Dette er teke opp i kapitlet om risikohandtering.

! *Dersom du loggar at usikkerheita er høg, fortel du at eit stort spekter av konsekvensar er moglege. Hendinga kan gi opphav til å krysse av i fleire celler i risikomatrisa. Dette bør takast med seinare når risikobiletet skal presenterast, og vil gi nyttig informasjon når tiltak og beredskap skal vurderast og prioriterast.*

Risiko- og sårbarheitsvurdering		Risikohandtering		
Usikkerheit (sett kryss)	Sårbarheitsvurdering Skildre sårbarheita - forventa nedetid? - finst det reservedelar på lager? - kor kritisk er komponenten?	Eksisterande barrierer NB! Føresetnader for angitt risikonivå	Føreslegne barrierar / tiltak	Grad av styring: - høg - middels høg - låg
...	...	...	...	
X	Frå kontrollrommet har ein tilgang til å styre inn-/utkopling av stasjon. Feilstyring kan gi alvorleg skade med reparasjonstid på opptil fleire dagar, sjølv om ein har reservedelar på lager.	1: Port og gjerde er montert. 2. Lås på port og alle dører inn til kontrollrom.	1. Montering av innbrotsalarm / kamera i anlegg (klasse 3). Ved uautorisert tilgang vil kamera (ITV) og sirene bli aktivert. Samtidig vil driftssentralen bli varsla.	Høg
...	...	...	...	...
...	...	...	...	

Figur 12 Du også bruke dette feltet dersom det er lite bakgrunnskunnskap om hendinga.

3.2.3 Sårbarheitsvurderingar

Sårbarheit er som tidlegare nemnt den evna eit system har til å oppretthalde funksjonen når det blir utsett for påkjenningar, det vil seie når uønskte hendingar skjer. Sårbarheit kan dermed knytast til barrierar/tiltak som har som føremål å avgrense konsekvensane når ei hending har skjedd. Sårbarheitsvurderingane på dette nivået består i å gjere seg opp tankar om kor kritisk komponenten i kraftforsyninga er, vurdere kor robuste vern og barrierar ein har, samt vurdere kor lenge ein forventar at eit eventuelt avbrot vil vare.

Nyttige problemstillingar å drøfte i analysegruppa kan vere:

- Kan denne hendinga føre til at ein mistar straumforsyninga?
- Er komponenten kritisk for anlegget?
- Kva slags barrierar må svikte for at ein skal miste straumforsyninga over visst lang tid?
- Kva er forventa nedetid?
- Kva er worst-case-nedetid?
- Finst det reservedelar på lager?
- Har ein tilstrekkeleg med personell med nødvendig kompetanse for reparasjon og beredskap?

Eit eksempel på utfylling er vist i Figur 12.

!	*Ein forenkla måte å logge sårbarheita på kan vere å logge to forventa nedetider, gitt at hendinga skjer. Nedetid 1: Dersom ein har reservedelar på lager. Nedetid 2: Dersom ein ikkje har reservedelar på lager. Dersom forskjellen er stor, indikerer det at komponenten er kritisk. Sårbarheita kan på den måten reduserast ved å ha reservedelar på lager.*

Gjennom vurderinga av sårbarheit blir det klarlagt om systemet er robust nok til å stå imot påkjenninga som den uønskte hendinga representerer.

3.2.4 Identifisere moglege risikoreduserande tiltak

Eksisterande barrierar er føresetnader

Det er svært viktig å logge kva slags barrierar og vern som allereie er på plass. Desse barrierane er føresetnader for dei vurderingane som er gjort i risiko- og sårbarheitsanalysen. Det kan òg vere nyttig for analysegruppa som heilskap å få ei felles forståing av tilstanden til barrierar og vern.

Nye barrierar og tiltak

Vi legg ikkje opp til ein fullstendig tiltaksanalyse på sjølve risikoanalysemøtet, men ofte vil forslag til barrierar dukke opp som ein del av diskusjonen. Vi har sett av plass i analyseskjemaet til å logge nye barrierar som blir føreslegne.

Hugs at tiltak kan vere både sannsynsreduserande (førebyggjande) og konsekvensreduserande (skadereduserande), jf. bow-tie-diagram i Figur 3.

!	*Å setje av plass og tid til å føreslå nye barrierar og tiltak set fokus på førebygging og stimulerer til ei proaktiv haldning. Som prosessleiar kan du stille desse spørsmåla: Kva kan gjerast for å unngå at denne hendinga skal skje? Kva kan gjerast for å unngå at denne hendinga utviklar seg til å true forsyningstryggleiken?*

Ein fullstendig gjennomgang av risikoreduserande tiltak er temaet i neste kapittel, Risikohandtering.

Grad av styring

Graden av styring seier noko om kor lett det er å kontrollere risikoen for ei gitt hending. Kor lett er det å implementere tiltak som reduserer sannsynet for at hendinga skal skje? Kor lett er det å setje i verk tiltak eller auke beredskapen for å sikre at konsekvensane av hendinga blir små?

!	*Vi tilrår å oppgi tre ulike gradar av styring: Låg, middels høg og høg. Ein kan for eksempel relatere styringa til desse kategoriane:* • *Høg: Innanfor selskapet sin kontroll, kjende tiltak finst og kan implementerast nokså enkelt.* • *Middels høg: Selskapet kan påverke.* • *Låg: Selskapet kan ikkje kontrollere/styre risikoen. Ingen kjende, tilgjengelege tiltak.*

Det å oppgi grad av styring er viktig når ein skal velje ut og prioritere tiltak og oppfølgingsaktivitetar. Dette er teke opp i kapitlet om risikohandtering.

3.2.5 Presentasjon av risikobiletet

Vi har no logga uønskte hendingar og oppgitt kva slags konsekvensar som kan oppstå, tilhøyrande sannsyn/frekvens, usikkerheit og grad av styring. Denne informasjonen kan deretter brukast til å presentere risikobiletet.

!	*Ta med uønskte hendingar, konsekvensar med tilhøyrande sannsyn/frekvens, usikkerheit og grad av styring når risikobiletet skal presenterast.*

Poenget med å ta med usikkerheit er å få fram uønskte hendingar som kan ha eit stort spekter av konsekvensar, samt hendingar der vurderingane er gjort på eit avgrensa grunnlag. Vurderinga av både sårbarheit og grad av styring er nyttig når ein skal prioritere og setje i verk risikoreduserande tiltak.

Risikobiletet kan presenterast i listeform eller ved hjelp av ei risikomatrise. Dersom ein har logga risiko for fleire konsekvensdimensjonar, fyller ein ut ei matrise for kvar dimensjon. Eit eksempel på risikomatrise for konsekvensdimensjonen forsyningstryggleik er vist i Figur 13. Her er hendinga "Kantra mast" med løpenummer 4.1 plotta inn. Høg usikkerheit kan for eksempel gjerast meir synleg ved å bruke ein annan skrifttype, feit skrift eller eit eige symbol. Desse hendingane tiltrekk seg dermed automatisk meir merksemd enn hendingar med låg usikkerheit.

Frekvens/sannsyn \ Konsekvens for forsyningstryggleik	***1: Ubetydeleg.*** *Ikkje avbrot i straumforsyninga.*	*2: Liten. Ingen samfunnskonsekvensar. Avbrot < 10 timar hos < 10 sluttbrukarar.*	*3: Middels. Nokre lokale konsekvensar for privatabonnentar. Avbrot < 10 timar hos < 1000 sluttbrukarar eller ≥ 10 timar hos < 10 sluttbrukarar.*	*4: Alvorleg. Alvorlege konsekvensar i infrastruktur og i lokalsamfunnet. Avbrot ≥ 10 timar hos < 1000 sluttbrukarar.*	*5: Svært alvorleg. Samfunnsviktige funksjonar som liv og helse samt viktig infrastruktur ramma / sett ut av funksjon. Avbrot ≥ 10 timar hos ≥ 1000 sluttbrukarar.*
5: Oftare enn 1 gang pr. år.					
4: Frå 1 gang pr. år til kvart 10. år.					
3: Frå kvart 10. år til kvart 100. år.					
2: Frå kvart 100. år til kvart 1000. år.					**4.1**
1: Sjeldnare enn kvart 1000. år.					

Figur 13: Eksempel på risikomatrise for konsekvensdimensjonen forsyningstryggleik – det er viktig at verksemda sjølv vurderer kva som skal liggje i dei ulike kategoriane

Fokuset i beredskapsforskrifta rettar seg i stor grad mot dei felta som er merkte med raudt og gult i risikomatrisa i Figur 13. Dersom konsekvensen kan vere alvorleg, skal forholda analyserast sjølv om sannsynet er lågt.

Ofte blir det knytt handlingsreglar til dei ulike fargane i risikomatrisa. For eksempel kan ein seie at ein *må* setje i verk tiltak for alle hendingar som hamnar i det raude området. For alle hendingar i det gule området *bør* ein setje i verk tiltak, mens for hendingar i det grøne området er det ikkje nødvendig med vidare tiltak. Vi åtvarar mot å mekanisere avgjersleprosessen på denne måten. Meir om dette i neste kapittel.

> **!** *Hugs at risikomatrisa berre er eit presentasjonsverktøy. Unngå å ta avgjersler utelukkande basert på kva for ei fargesone ein risiko hamnar i.*
>
> *Med omsyn til beredskapsforskrifta og forsyningstryggleiken er det viktig å vurdere hendingar i nedste høgre hjørne, sjølv om dei "berre" ligg i det gule området. Dette er hendingar som kan ha svært alvorleg utfall, men der sannsynet for slike utfall er lågt.*

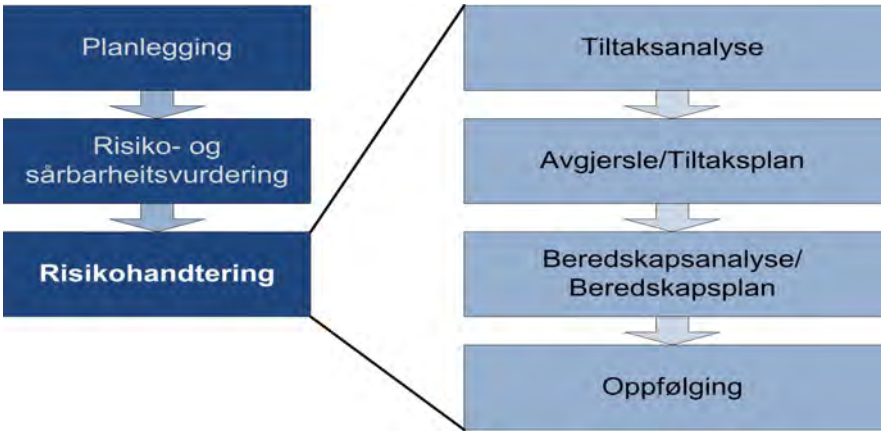
Andre måtar å presentere risikobiletet på kan for eksempel vere i ei matrise, med risikonivå på den eine aksen og grad av styring på den andre.
Målet med risikobiletet er å enkelt kunne formidle "tilstanden" eller risikonivået ved anlegget/aktiviteten til omverda, slik at nødvendige tiltak kan bli sett i verk.

!	*Leiinga i eit kraftforsyningsselskap bør etterspørje eller få lagt fram eit oppdatert risikobilete for verksemda med jamne mellomrom. Oppdatert risikobilete og beredskapsspørsmål bør vere fast eit punkt på leiarmøte for å oppnå ei heilskapleg risikostyring.*

3.3 Risikohandtering

Risikohandtering består i å gjennomgå resultatet frå ROS-vurderingane og setje i verk tiltak der ein finn det nødvendig. I samsvar med risiko- og sårbarheitsanalyseprosessen i Figur 4, er leiinga si vurdering og avgjersle ein del av denne aktiviteten.

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



Figur 14: Dei ulike stega i risikohandteringa

Vi har valt å dele risikohandteringa inn i desse stega:

1) Tiltaksanalyse
   a. Identifiser risikoreduserande tiltak.
   b. Vurder og ranger tiltak i forhold til kostnader og effektivitet.
2) Avgjersle og tiltaksplan
   a. Avgjer kva slags tiltak som skal setjast i verk.
   b. Avgjer kven som er ansvarleg for å gjennomføre dei.
   c. Set ein frist for å gjennomføre dei.
3) Beredskapsanalyse og -plan
4) Oppfølging av tiltaksplan og beredskapsplan

3.3.1 Tiltaksanalyse

Identifisere risikoreduserande tiltak
Som tidlegare nemnt kan risikoreduserande tiltak vere anten sannsynsreduserande (førebyggjande) eller konsekvensreduserande (skadereduserande).

Det er verken nødvendig eller hensiktsmessig å føreslå risikoreduserande tiltak for alle dei uønskte hendingane. Ein bør heile tida fokusere på å setje i verk tiltak der risikoen er størst, og der ein oppnår størst risikoreduserande effekt av å setje inn tiltak.

> ! *Ta usikkerheit og grad av styring med i vurderinga når du avgjer kva slags hendingar du vil redusere risikoen for.*

Ta tak i risikobiletet frå avsnitt 3.2.5. Gjennom risikomatriser og lister ser vi kvar det er viktig å redusere risikoen. Vel deretter ut kva for uønskte hendingar du vil handtere risikoen for, og identifiser tiltak som kan redusere risikoen – anten for at hendinga skjer, eller for at konsekvensane av hendinga blir alvorlege.

> ! *Hugs å identifisere både sannsynsreduserande og konsekvensreduserande tiltak. Dei sannsynsreduserande tiltaka er viktige for å førebyggje at uønskte hendingar skjer. Dei konsekvensreduserande/skadereduserande tiltaka er ein viktig del av beredskapen.*

Kost-effektivitetsvurdering av tiltak

Det er viktig å vurdere den risikoreduserande effekten av tiltaka for å kunne prioritere ulike tiltak opp mot kvarandre. Analysegruppa må vurdere kvart tiltak opp mot desse spørsmåla: Dersom vi innfører dette tiltaket,

- kor mykje vil sannsynet for den uønskte hendinga bli redusert?
- kor mykje kan konsekvensane eller skadeomfanget bli redusert?
- kor mykje blir sårbarheita til systemet redusert?

I tillegg må ein oppgi kostnaden (ressursar/pengar) ved kvart tiltak.

> ! Når risikoreduserande effekt og kostnad ved kvart tiltak er kjent, kan tiltaka rangerast ut frå kost-effektivitet.

I denne samanhengen er det viktig å gjere merksam på at ein for enkelte hendingar ikkje har noko val. Tiltak for å førebyggje og/eller avgrense konsekvensane av moglege alvorlege hendingar som kan true kraftforsyninga, skal prioriterast framfor mindre viktige forhold.

3.3.2 Avgjersle og tiltaksplan

> ! Det å avgjere kva for tiltak som skal implementerast, er ei avgjersle leiinga skal ta.

Som ein del av avgjersla må ein opplyse om dette:

- Kva for tiltak skal implementerast?
- Kven er ansvarleg for å gjennomføre dei?
- Kva er tidsfristen for å gjennomføre dei?

Desse punkta utgjer til saman ein tiltaksplan.

3.3.3 Beredskapsanalyse og beredskapsplan

Dette er ikkje ei rettleiing i beredskapsanalyse eller beredskapsplanar. ROS-analysene som er i fokus i denne rettleiinga, skal leggje grunnlaget for ein robust og hensiktsmessig beredskap. Gjennom heile rettleiinga har vi fokusert på beredskapsforskrifta sitt krav til ROS-analysar, og ved å følgje tilrådingane her vil ein komme eit godt stykkje på veg.

Men dersom ein skal oppnå ein robust beredskap, må ein ta resultata frå ROS-analysen eitt steg vidare. Nokre moment er:

- Etablert register over uønskte hendingar kan brukast som innspel til scenario ein ønskjer å dimensjonere beredskapen for.
- Identifiserte konsekvensreduserande tiltak og barrierar er nyttige innspel til beredskapstiltak og aktivitetar.
- Basert på krava i beredskapsforskrifta og kunnskapen frå ROS-analysane, kan ein opprette ein beredskapsplan.
- Dersom ein skal ha ein godt nok trena beredskapsorganisasjon, må ein gjennomføre beredskapsøvingar.

3.3.4 Oppfølging

Ein viktig del av ansvarsområdet til leiinga går ut på å følgje opp resultata frå ROS-analysen og setje i verk tiltak. ROS-analysen vil på ei rekkje område truleg peike på behovet for å implementere eller styrkje ulike tiltak for å sikre at krava i beredskapsforskrifta blir oppfylte. Det er viktig å få leiinga til å forstå at enkelte oppfølgingsbehov er direkte knytte til pliktene i forskrifta.

> **!** Vi tilrår at oppdatert risikobilete, endring i risikobilete og status på aksjonar og tiltak inngår som eit fast punkt på leiarmøte for å sikre eit kontinuerleg fokus.

3.3.5 Sensitiv informasjon

Det er viktig å vere klar over at spesielt sårbarheitsvurderingar som måtte komme fram av ein ROS-analyse, raskt kan definerast som sensitiv informasjon om kraftforsyninga, og vil av den grunn ikkje kunne offentleggjerast, jf. § 6–2 "Beskyttelse av informasjon" i beredskapsforskrifta. Dette treng ikkje å gjelde for heile ROS-analysen, men delar av han. Samtidig er det viktig å vere bevisst på at mange samarbeidande verksemder og styresmakter vil etterspørje relevant informasjon om kraftforsyninga til eigne ROS-analysar. Her blir det viktig å tilby relevant informasjon, basert på tenestebehovet til dei enkelte og rettmessige krav, utan at ein gir frå seg kraftsensitiv informasjon.

4. Oppsummering: ROS-analyse steg for steg

Før analysemøtet: Planlegging

- Definer føremålet med og omfanget av analysen – sørg for forankring hos leiinga.
- Avgjer kva for konsekvensdimensjonar og konsekvenskategoriar samt kva for kategoriar som skal brukast for sannsynsdimensjonen.
- Innhent informasjon om analyseobjektet.
- Kall inn relevant kompetanse til analysemøtet.
- Opprett ei sjekkliste for analyseobjektet – del analyseobjektet inn i delelement.
- Gjer klar analyseskjema – test analyseskjemaet ved å prøvelogge hendingar.

På analysemøtet: Identifikasjon av farar, risiko- og sårbarheitsvurdering

- Identifiser uønskte hendingar, og fyll inn i analyseskjemaet.
    - Ved hjelp av idédugnad.
    - Ved hjelp av ein strukturert gjennomgang av anlegget.
    - Ved bruk av sjekklister.
- Gå gjennom kvar hending som blir identifisert, og gjer dette:
    - Kartlegg kva årsaker som ligg bak.
    - Diskuter sannsyn/frekvens.
    - Kartlegg kva for konsekvensar hendinga kan få, og vurder om "worst case"-utfall av hendinga kan true straum-/fjernvarmeforsyninga og viktige anlegg. Kan éin av de moglege konsekvensane representere hendinga, eller bør hendinga splittast? Vurder også samtidige hendingar.
    - Oppgi om det er stor usikkerheit.
    - Kartlegg eksisterande barrierar – dvs. føresetnader for vurderingane som er gjort.
    - Gjer ei vurdering av sårbarheita.
    - Føreslå risikoreduserande barrierar og tiltak.
    - Oppgi graden av styring.
- Hugs å dokumentere grunngivinga for kva kategoriar som er valt for konsekvens og sannsyn/frekvens.

Etter analysemøtet: Risikobilete og rapport. Risikohandtering.

- Gå gjennom og fullfør analyseskjemaet. Innhent tilleggsinformasjon og tilleggsekspertise dersom det er nødvendig.
- Avklar om det er nødvendig med meir detaljerte analysar.
- Fyll inn uønskte hendingar i risikomatrise – éi for kvar konsekvensdimensjon.
- Prioriter uønskte hendingar ut frå risikonivå og usikkerheit.
- Føreslå risikoreduserande tiltak.
- Skriv rapport.
- Presenter risikobiletet for leiinga.
- Avgjer kvar risikoreduserande tiltak skal setjast i verk. Gjer ei vurdering ut frå:
    - Risikonivå og usikkerheit.
    - Grad av styring.
    - Kost-effektivitet.
- Lag ein tiltaksplan – set opp kven som er ansvarleg for å følgje opp tiltak, og for at tidsfristar blir helde.
- Vurder om resultata frå ROS-analysen bør føre til endringar i beredskapsplanar og beredskapsorganisasjonen.
- Følg opp tiltaksplanen.

5. Referansar

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.*

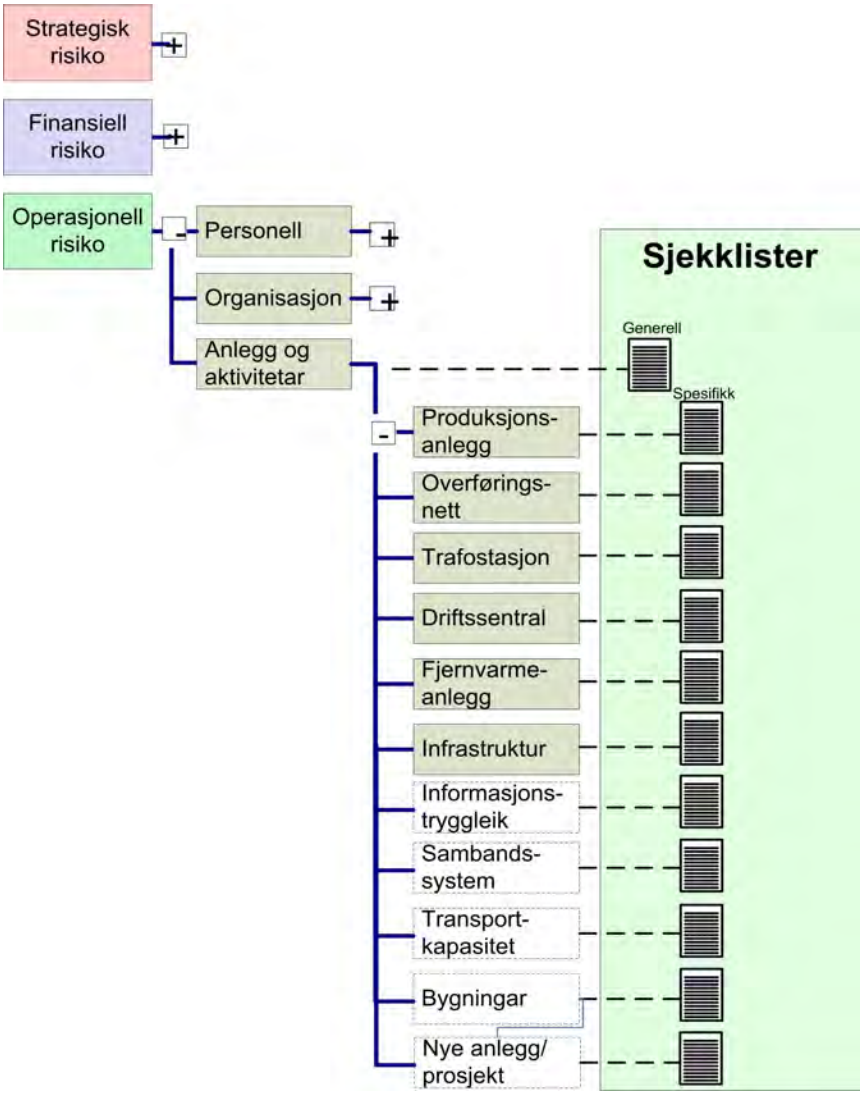
Proactima: www.proactima.no

Vedlegg 1 – Forslag til sjekklister

Vedlegg 1 inneheld eit sett med sjekklister som er meint å vere til hjelp i ein grovanalyse. Som figuren under viser, er sjekklistene inndelte i to delar. Del 1, som vist i den første tabellen, skildrar ein del hjelpeord for særskilde forhold. Denne lista er generell og kan knytast opp mot alle dei ulike anleggstypane. Dei særskilde forholda er inndelte i utilsikta handlingar (farar) og tilsikta handlingar (truslar). Del 2, som vist i dei neste tabellane, dannar eit sett med anleggsspesifikke sjekklister. Desse spesifikke sjekklistene definerer ein del typiske komponentar som inngår i anleggstypen, og ei rekkje uønskte hendingar som kan knytast til denne typen anlegg.

Det er viktig å merkje seg at sjekklistene ikkje tek høgd for alle forhold som kan vere relevante for eit vilkårleg analyseobjekt. Sjekklistene skal i så måte ikkje reknast som ei uttømmande liste, og det vil ofte vere nødvendig med ytterlegare kartlegging for å få ein fullstendig analyse.

Dersom ein systematisk bruker sjekklister, gjer dette det mogleg å overføre erfaring gjennom å vidareutvikle sjekklistene etter kvart som ny kunnskap gjer seg til kjenne.



Generell sjekkliste for ROS-analysar i kraftbransjen

Sjekkliste: Særskilde forhold		
Utilsikta handlingar (farar)		
Omgivnader	**Menneske/personale**	**Teknisk**
Torevêr/lynoverspenningar	Feil bruk	Aldring
Vind	Arbeid/prøving	Utbyggingstrinn
Snø/is	Trefelling	Slitasje
Snøsig	Graving/sprenging	Korrosjon
Frost/tele	Anleggsarbeid	Lekkasje
Kvikkleire	Trafikkskade	Lause delar
Erosjon/jordsig	Kompetansemangel	Skadd/defekt del
Skred	Arbeidsmiljø	Sprekk/brot
Vatn/nedbør/fukt	Kommunikasjon/samhandling	Spesielle løysingar / design
Flaum	Utskifting av personale	Tryggleikssystem
Salt/forureining	Sjukefråvær	Redundans
Framandlekamar	Streik	Storleik på anlegg
Fugl/dyr	Vakt-/beredskapsordningar	Teknisk dokumentasjon
Vegetasjon	Underleverandørar (avhengigheit)	Belastning
Brann/eksplosjon	…	Sambandsbrot
Skogbrann		Feil i data eller programvare
Ras		Kjøling
Tilkomst i særskilde situasjonar		Kaskadeeffektar
…		Fellesfeil
		Branntilløp
Tilsikta handlingar (truslar)		
Direkte		**Tilfeldig**
Innbrot – Bygning/anlegg – Datasystem (hacking) – … Utru tilsette – Oppsagd – Psykisk ubalanse – Aktørar – Sabotasje – Industrispionasje – … Utru leverandør – Servicepersonell – Teknisk personell… Terror – Frykt – Skade frå krigsliknande handlingar – Moglege mål		Informasjonsteknologi –Virus –Ormar –Trojanarar –… Hærverk … Evakuering av driftssentral - Brann i bygning - Truslar - …

Sjekkliste for ROS-analysar av produksjonsanlegg

Sjekkliste: Produksjonsanlegg		
Delelement/komponentar		
Inntak	Generator	Koplingsanlegg
Trykksjakt	Magnetisering	Kontroll-/verneanlegg
Innløpsrøyr	Skinneanlegg	Batterianlegg
Hovudstengjeventil	Transformator	Stasjonsforsyning (aggregat)
Turbin	CO2-sløkkjeanlegg	Kjølevassanlegg
Turbinregulator	Kablar	Skiljebrytar
Brannsikring	Effektbrytar	Jordkniv
Straumtransformator	Spenningstransformator	Avleiar
Isolator	Løpehjul	
Uønskte hendingar		
Trykksjakt kollapsar	Vibrasjon	Brann
Arbeidsulykke	Ukontrollert rotasjon på turbin	Tap av styringssystem
Vasslekkasje	Oljelekkasje	Feil på stasjonsforsyning
Ventil opnar ikkje	Feilfunksjon	Manglande inn-/utkopling
Ventil stengjer ikkje	Skade på kablar	Uønskt innkopling
Nødstenging	Klarar ikkje bryte straum	Mislukka utkopling
Havari	Overslag	Eksplosjon
Kortslutning	Dambrot	Ras
Utilsikta innkopling		Røyrgatebrot
Stasjonen blir dykka		

Sjekkliste for ROS-analysar av transformatorstasjon

Sjekkliste: Transformatorstasjon		
Delelement/komponentar		
Avleiarar	Jordbrytar	Sikring
Bygningar	Kablar	Skiljebrytar
Effektbrytar	Klemmer	Sløkkjespole
Endeavslutning	Kondensatorbatteri	Spenningstransformator
Gjennomføringar	Kontroll-/verneanlegg	Straumtransformator
Innstrekkstativ	Muffer	Transformator
Isolator	Samleskinne	
Uønskte hendingar		
Havari	Uønskt innkopling	Utilsikta innkopling
Ubalanse i fasespenning	Fallande gjenstand	Over-/underspenning
Klarar ikkje bryte straum	Brot	Kantra mast
Mislukka innkopling	Overslag	Varmgang
Eksplosjon	Utfall	Måler feil
Fråkopling	Manglande utkopling	Måler ikkje
Uønskt utkopling	Manglande innkopling	Redusert kompensering

Sjekkliste for ROS-analysar av overføringsanlegg

Sjekkliste: Overføringsanlegg		
Delelement/komponentar*		
Mast	Oppheng	Kabel
Linje	Klemmemekanisme	Muffe
Isolator	Flymarkør	Trykkluftanlegg
Avleiarar	Lynavleiar	
Jording	Fundamentering/bardunar	
Uønskte hendingar		
Kantra mast	Havari av isolator	Kordellbrot
Fallande gjenstand	Overslag	Brot
Varmgang	Brot	Mast knekk
Mekaniske skadar	Oljelekkasjar	Vibrasjonar
Overslag	Overslag	Galoppering
Kortslutning/jordslutning	Lekkasje	

**Sjekklista er med hensikt gjort svært generell. Avhengig av omfanget av analysen, kan ein skildre dei ulike netta (lågspent-/distribusjons-/sentral-/regionalnett) og komponentane i nettet (eks. transformatorar), og desse kan vurderast saman eller kvar for seg.*

Sjekkliste for ROS-analysar av fjernvarmeanlegg

Sjekkliste: Fjernvarmeanlegg		
Delelement/komponentar		
Kjelanlegg	Varmesentral	Røyr (gass/vatn)
Kontrollsystem	Ventil (gass/vatn)	Avløpsrøyr
Pumpe	Vassrenseanlegg	Straumforsyning
Transformator nettstasjon	Brenselsilo	Avfallslager
Generator	Kundesentral	Temperaturregulator
Uønskte hendingar		
Frost på anlegg	Gassflaske fell	Fallskadar
Tenning av brennbart materiale (brannfare)	Feil på kontrollanlegg	Svikt i kjel
Svikt i kommunalt avløp	Vasslekkasje til følsamt utstyr	Kuttskadar
Koking i varmesentral	Svikt i vasstilførsel	Svikt i straumtilførsel
Utslepp av luft frå gasskjel	Utilsikta drenering av gasskjel	Røyrbrot (vatn)
Gasslekkasje	Røyrbrot (gass)	Koking i nett
Brann i avfallslager	Lekkasje i fjernvarmenett	Svikt i temperaturregulering (kundesentral)
Sikringsventil blæs på personell	Utslepp (miljøforureining) (NOx/CO2/gass/kjemikaliar?)	Varme overflater (brannskadar)
Brann i brenselsilo		Havari elektrokjele – knallgass
Damputslepp		

Sjekklister for ROS-analysar av fysisk sikring

Sjekkliste: Perimetersikring		
Delelement/komponentar		
Port	Gjerde	Overvakings- og alarmsystem
Portstolpar inkl. feste i grunn	Gjerdeduk	Belysning av uteområde
Lås	Strekkstål	Høgtalaranlegg
Mellomrom mellom port med to fløyer	Gitter	Porttelefon
Vegbom	Gjerdestolpar	Observasjonsstillingar
Kantstein	Piggtråd	
Betongblokkar	Topptråd	
…	Botntråd	
Hendingar		
Sjå generell sjekkliste		

Sjekkliste for ROS-analyse av kontrollrom/driftssentral

Sjekkliste: Kontrollrom/driftssentral		
Delelement/komponentar		
Bygning Inngang Dører Vindauge …	Brannalarm/-detektorar Sløkkjeanlegg (for eksempel gass) Handsløkkjeutstyr Brannfarlege materialar Sluk/avløp	Kablar IT-system Kontrollromsutstyr
Hendingar		
Sjå generell sjekkliste		

Sjekkliste for ROS-analyse av data/sambandsrom

Sjekkliste: Data/sambandsrom		
Delelement/komponentar		
Bygning Inngang Dører Vindauge …	Brannalarm/-detektorar Sløkkjeanlegg (for eksempel gass) Handsløkkjeutstyr Brannfarlege materialar Sluk/avløp	Kablar IT-system Sambandsutstyr
Hendingar		
Sjå generell sjekkliste		

Sjekkliste for ROS-analyse av batterirom/aggregat/nødstraum

Sjekkliste: Batterirom/aggregat/nødstraum		
Delelement/komponentar		
Bygning Inngang Dører Vindauge Drivstofftank (storleik/driftstid) …	Brannalarm/-detektorar Sløkkjeanlegg (for eksempel gass) Handsløkkjeutstyr Brannfarlege materialar Sluk/avløp	Kablar (felles?) Gjennomføringar Batteri Aggregat og tilkoplingar for mobilt aggregat, kjøling, dieselfilter Fysisk skilje Drivstoff
Hendingar		
Overbelasting Koplar seg ikkje inn Tomt for drivstoff …	Eksplosjon Brann …	

Det er viktig å teste nødstraum. Spørsmål som kan stillast, er:

- Blir det testa regelmessig? Kor ofte?
- Blir det testa med den maksimale belastinga det kan bli utsett for (inkl. hjelpesystem som nødlys og kjøling) over lengre tid?
- Kor ofte skjer testen ved at ein koplar frå den ordinære straumforsyninga fysisk og lèt prioritert last vere innkopla?
- Kor lenge?
- Kor mykje drivstoff er på tanken – driftstid – etterforsyningsmoglegheit?

Sjekkliste for ROS-analyse av …

Sjekkliste: …		
Delelement/komponentar		
…		
Hendingar		

NB: Desse forslaga til sjekklister er ikkje uttømmande …

Sjekklister er noko den enkelte verksemda må utarbeide og utvikle.

Vedlegg 2 – Forslag til analyseskjema og tiltaksplan

Skjema for registrering av risiko og sårbarheit for uønskt hending	ID:				
Analyseobjekt:		Delsystem/komponent:			
Uønskt hending					
Skildring av uønskt hending					
Årsak(er) til uønskt hending					
Sannsyn/frekvens for hendinga	☐ *5: Oftare enn 1 gang pr. år.*	☐ *4: Frå 1 gang pr. år til kvart 10. år.*	☐ *3: Frå kvart 10. år til kvart 100. år.*	☐ *2: Frå kvart 100. år til kvart 1000. år.*	☐ *1: Sjeldnare enn kvart 1000. år.*
	5: Hendingar som skjer ofte / svært ofte i selskapet *4: Hendingar som har skjedd nokre gonger i selskapet* *3: Hendingar som har skjedd i selskapet eller hos andre*		*2: Har høyrt om liknande hendingar i Noreg eller utlandet* *1: Har aldri høyrt om liknande hendingar*		
Grunngiving					
Konsekvens for forsyningstryggleik	☐ *1: Ubetydeleg. Ikkje avbrot.*	☐ *2: Liten. Avbrot < 10 timar hos < 10 sluttbrukarar.*	☐ *3: Middels. Avbrot < 10 timar hos < 1000 sluttbrukarar eller ≥ 10 timar hos < 10 sluttbrukarar.*	☐ *4: Alvorleg. Avbrot ≥ 10 timar hos < 1000 sluttbrukarar.*	☐ *5: Svært alvorleg. Avbrot ≥ 10 timar hos ≥ 1000 sluttbrukarar.*
Grunngiving:					
Konsekvens for	☐ *1: Ubetydeleg.*	☐ *2: Liten.*	☐ *3: Middels.*	☐ *4: Alvorleg.*	☐ *5: Svært alvorleg.*
Grunngiving:					
Konsekvens for	☐ *1: Ubetydeleg.*	☐ *2: Liten.*	☐ *3: Middels.*	☐ *4: Alvorleg.*	☐ *5: Svært alvorleg.*
Grunngiving:					
Usikkerheit					
Sårbarheitsvurdering					
Eksisterande barrierar/tiltak					
Barrierar/tiltak som er føreslegne					
Grad av styring					
Kommentar					

Skildring av dei ulike felta i analyseskjemaet.

ID:
Løpenummer for enkelt å kunne identifisere hendinga. F.eks. kan første hending få ID nr. 1, andre hending nr. 2 osv. Ein kan også velje å gruppere hendingar etter delsystem/komponent. Dersom for eksempel ein produksjonstrafo har komponentnummeret 8, kan hendinga "eksplosjon i trafo" få ID 8.1 og "transformatorhavari" få ID 8.2 osv.

Delsystem/komponent:
Nemning av kva slags delsystem / kva slags komponent hendinga gjeld. Eksempel: Bygning, transformator, effektbrytar, straumtransformator, samleskinne osv.

Uønskt hending:
Namn på uønskt hending. Bør vere presist, slik at ein unngår misforståingar. Ev. kan kommentarfeltet brukast for å utdjupe hendinga. Eks: "Eksplosjon i transformator", "Svikt i sirkulasjonspumpe".

Skildring/grunngiving:
Bruk dette feltet til å fange opp så mykje som mogleg av skildringa av hendinga og grunngivinga for kva kategoriar som er valt for risiko.

Årsaker:
Nemn moglege årsaker til hendinga. Tenk samtidig gjennom om det finst særskilde forhold ved dette anlegget / denne komponenten som gjer at risikoen avvik frå andre anlegg/komponentar. Avvik frå regelverk kan òg vere ei indirekte årsak, og dette bør kartleggjast her.

Sannsyn/frekvens:
Nemn kor ofte den uønskte hendinga er vurdert til å skje. Som hjelp til å velje frekvenskategoriar kan denne inndelinga brukast:
1*: Hendingar som skjer ofte / svært ofte i selskapet.*
2: Hendingar som har skjedd nokre gonger i selskapet.
3: Hendingar som har skjedd i selskapet eller hos andre selskap som liknar på oss.
4: Har høyrt om liknande hendingar i Noreg eller utlandet, men har ikkje skjedd hos oss.
5: Har aldri høyrt om liknande hendingar.

Konsekvens:
Forsyningstryggleik bør alltid vere med som konsekvensdimensjon. Dei andre konsekvensdimensjonane blir valde etter behov, f.eks. personelltryggleik, ytre miljø, økonomiske tap, omdømme osv.
Det er viktig å skildre kva ein meiner med ein "svært alvorleg" eller "middels alvorleg konsekvens".
Eksempelvis for forsyningstryggleik kan dette sjå slik ut:
5: Svært alvorleg. Samfunnsviktige funksjonar som liv og helse samt viktig infrastruktur ramma / sett ut av funksjon. Avbrot ≥ 10 timar hos ≥ 1000 sluttbrukarar.
4: Alvorleg. Alvorlege konsekvensar i infrastruktur og i lokalsamfunnet. Avbrot ≥ 10 timar hos < 1000 sluttbrukarar.
3: Middels. Nokre lokale konsekvensar for privatabonnentar. Avbrot < 10 timar hos < 1000 sluttbrukarar eller ≥ 10 timar hos < 10 sluttbrukarar.
2: Liten. Ingen samfunnskonsekvensar. Avbrot < 10 timar hos < 10 sluttbrukarar.
1: Ubetydeleg. Ikkje avbrot i straumforsyninga.

Usikkerheit:
Set kryss dersom mange ulike konsekvensar er moglege, eller dersom det er stor spreiing i utfallsrommet av hendinga (eks. eksplosjon i trafo kan gi alt frå 0 skadde til fleire drepne). Set òg kryss her dersom bakgrunnsinformasjonen er mangelfull, slik at det er vanskeleg å vurdere frekvens/konsekvens.

Sårbarheitsvurdering:
Skildre sårbarheita. Kva er forventa nedetid? Finst det reservedelar på lager? Kan denne hendinga føre til at ein mistar straumforsyninga? Kor kritisk er denne komponenten?

Eksisterande barrierar/tiltak:
Nemne kva for barrierar og tiltak som allereie finst. **NB: Desse barrierane/tiltaka er ein føresetnad for risikovurderinga.**

Barrierar/tiltak som er føreslegne:
Føreslå risikoreduserande tiltak.

Grad av styring:
Nemn graden av styring, dvs. kor lett det er å redusere risikoen med barrierar/tiltak. Før dette opp med låg – middels høg – høg.

Eksempel på utfylt analyseskjema

Skjema for registrering av risiko og sårbarheit for uønskt hending	ID:	*4.1*

Analyseobjekt: *Transformatorstasjon*	Delsystem/komponent: *Skalsikring (port, gjerder, vindauge, dører)*

Uønskt hending	*Sabotasje/hærverk*
Skildring av uønskt hending	*Uvedkomande tek seg inn på anlegget og set viktige komponentar ut av funksjon / feilstyrer anlegget.*
Årsak(er) til uønskt hending	*Alarm eller kameraovervaking er ikkje installert på anlegget.*
Sannsyn/frekvens for hendinga	☐ *5: Oftare enn 1 gang pr. år.* ☐ *4: Frå 1 gang pr. år til kvart 10. år.* ☒ *3: Frå kvart 10. år til kvart 100. år.* ☐ *2: Frå kvart 100. år til kvart 1000. år.* ☐ *1: Sjeldnare enn kvart 1000. år.* *5: Hendingar som skjer ofte / svært ofte i selskapet.* *4: Hendingar som har skjedd nokre gonger i selskapet.* *3: Hendingar som har skjedd i selskapet eller hos andre.* *2: Har høyrt om liknande hendingar i Noreg eller utlandet.* *1: Har aldri høyrt om liknande hendingar.*
Grunngiving	*Anlegget er lett tilgjengeleg. Det er lett å ta seg inn i kontrollrommet via vindauge på baksida. I dag er det ikkje mogleg å oppdage om det er uvedkomande i kontrollrommet.*
Konsekvens for forsyningstryggleik	☐ *1: Ubetydeleg. Ikkje avbrot.* ☐ *2:Lliten. Avbrot < 10 timar hos < 10 sluttbrukarar .* ☐ *3: Middels. Avbrot < 10 timar hos < 1000 sluttbrukarar eller ≥ 10 timar hos < 10 sluttbrukarar.* ☐ *4: Alvorleg. Avbrot ≥ 10 timar hos < 1000 sluttbrukarar.* ☒ *5: Svært alvorleg. Avbrot ≥ 10 timar hos ≥ 1000 sluttbrukarar.*
Grunngiving:	*Feil styring kan føre til omfattande skade på anlegget.*
Konsekvens for personelltryggleik	☐ *1: Ubetydeleg.* ☐ *2: Liten.* ☐ *3: Middels.* ☐ *4: Alvorleg.* ☐ *5: Svært alvorleg.*
Grunngiving:	
Konsekvens for	☐ *1: Ubetydeleg.* ☐ *2: Liten.* ☐ *3: Middels.* ☐ *4: Alvorleg.* ☐ *5: Svært alvorleg.*
Grunngiving:	

Usikkerheit	*Høg.*
Sårbarheitsvurdering	*Frå kontrollrommet har ein tilgang til å styre inn-/utkopling av stasjon. Feilstyring kan gi alvorleg skade med reparasjonstid på opptil fleire dagar, sjølv om ein har reservedelar på lager.*
Eksisterande barrierar/tiltak	*1: Port og gjerde er montert.* *2. Lås på port og alle dører inn til kontrollrom.*
Barrierar/tiltak som er føreslegne	*1. Montering av innbrotsalarm/kamera i anlegg (klasse 3). Ved uautorisert tilgang vil kamera (ITV) og alarmsirene bli aktivert. Samtidig vil driftssentralen bli varsla.*
Grad av styring	*Høg*
Kommentar	*Skildring av den uønskte hendinga "sabotasje" er meint å illustrere bruken av analyseskjemaet i Rettleiing i risiko- og sårbarheitsanalysar for kraftforsyninga.*

Norges vassdrags- og energidirektorat

proactima
PRO-ACTIVE MANAGEMENT

Analyseskjema – for eksempel til bruk på storskjerm.

Analyseobjekt:

Gjennomført av: **Dato:**

Føremål med analysen:

System		Uønskt hending	Risiko- og sårbarheitsvurdering								Risikohandtering		
			Skildring / grunngiving	Årsaker	Sannsyn / frekvens	Konsekvens, 5: katastrofalt, 1: ubetydeleg			Usikkerheit (sett kryss)	Sårbarheitsvurdering			
ID	Delsystem/komponent	- gi namn til uønskt hending	Nærmare skildring av hendinga. Kommentarar og diskusjon som ligg til grunn for valt frekvens og konsekvens.	- årsak til hending - særskilde forhold - avvik frå regelverk ...	5: > 1 gang pr. år 4: 1 gang pr. år - kvart 10. år 3: kvart 10. år - kvart 100. år 2: kvart 100. år - kvart 1000. år 1: < kvart 1000. år	K1: Forsyningstryggleik: bortfall av straum / tal på kunder som er råka	K2:	K3:		Skildre sårbarhelta - forventa nedetid? - finst det reservedelar på lager? - kor kritisk er komponenten?	Eksisterande barrierer NB! Føresetnader for angitt risikonivå	Føreslegne barrierar / tiltak	Grad av styring: - høg - middels høg - låg

Skjema for tiltakshandtering

Funksjon/aktivitet:			
Risiko:			**Ref.:**
Samandrag: Risikoreduserande tiltak som er tilrådd			
Handlingsplan **1. Føreslå tiltak**			
2. Kva slags ressursar er nødvendig?			
3. Ansvarleg			
4. Tidsplan			
5. Rapportering og oppfølging			
Ferdigstilt av:	**Dato:**	**Godkjent av:**	**Dato:**

Vedlegg 3 – Ord og uttrykk

ALARP-prinsippet	Risikoen skal reduserast så langt som praktisk mogleg (ALARP: As Low As Reasonably Practicable). "Omvendt bevisbyrde".
Akseptkriterium for risiko	Sjå risikoakseptkriterium.
Analyseobjekt	Kraftsystemet med dei tekniske, organisatoriske, miljømessige og menneskelege systema/forholda som er omfatta av risikoanalysen.
Barrierar	Tiltak og funksjonar som er planlagde for å bryte eit spesifisert uønskt hendingsforløp.
Beredskap	Omfattar alle tekniske, operasjonelle og organisatoriske tiltak som hindrar at ein fare/trussel som har oppstått, utviklar seg til ein ulykkessituasjon/tapssituasjon, eller som hindrar eller reduserer verknadene av ulykkessituasjonar/tapssituasjonar som har oppstått.
Avgjerslekriterium	Kriterium som har innverknad på avgjersler som må takast, for eksempel akseptkriterium for risiko, økonomiske kriterium, tilgjengeleg tid og kva som er politisk akseptabelt.
Forsyningstryggleik	Omgrepet forsyningstryggleik går att i ulike samanhengar når ein snakkar om tryggleik og beredskap i kraftforsyninga. Forsyningstryggleik kan forståast slik at det inkluderer energitryggleik, effekttryggleik og systemet si evne til å handtere ekstraordinære hendingar i kraftsystemet.
Frekvens	Forventa tal på hendingar i eit gitt tidsrom.
HAZID-samling	HAZard IDentification – fareidentifikasjon som skjer gjennom ein tverrfagleg gruppeprosess.
Konsekvens	Følgje av ei uønskt hending. Konsekvensar kan uttrykkjast kvalitativt som skadegrad eller kvantitativt som tal på ulykker eller skadar på anlegg, utstyr eller ressursar.
Konsekvensanalyse	Systematisk framgangsmåte for å skildre og/eller rekne ut konsekvensar for anlegg, utstyr eller ressursar som eit resultat av utløysande hendingar.
Risiko	Kombinasjon av moglege framtidige konsekvensar/utfall og tilhøyrande usikkerheit. Sannsyn kan brukast til å vise usikkerheit. Dersom dette blir gjort, kan vi seie at risiko er ein funksjon av sannsyn og konsekvens.
Risikoakseptkriterium	Uttrykkjer kva som er vurdert til å vere eit akseptabelt (tolererbart) risikonivå, og er den øvre grensa for risiko.
Risikoanalyse	Ein risikoanalyse er ein analyse av risikoen. Analysen inkluderer identifikasjon av uønskte hendingar, årsaksanalyse, konsekvensanalyse og kartlegging av risiko.
Risikobilete	Samla presentasjon av risikoresultat.
Risikostyring	Alle tiltak og aktivitetar som blir gjort for å styre risikoen.
Risikostyringspolicy	Føringar for å gjennomføre risikostyring og spesifisere risikostyringsprosessen.
Risikoreduserande tiltak	Tiltak med sikte på å redusere sannsyn for og/eller konsekvensane av uønskte hendingar.
Sannsyn	Grad av tru på at ei hending vil inntreffe.
Grad av styring	Grad av styring seier noko om i kva grad det er mogleg å kontrollere og redusere usikkerheitene og dermed oppnå ønskte utfall.

Sårbarheit	Eit uttrykk for eit system si evne til å fungere når det blir utsett for ei uønskt hending, samt dei problema systemet får med å ta opp att verksemda si etter at hendinga har skjedd.
Usikkerheit	Mangel på kunnskap om kva som er eller vil bli verdien av ein ukjend storleik som kan observerast.
Uønskt (utløysande) hending	Hending eller tilstand som kan få konsekvensar for f.eks. anlegg, utstyr eller ressursar.

Vedlegg 4 – Relevante lover og forskrifter, dei viktigaste ROS-krava i beredskapsforskrifta

Kraftforsyningsselskap har ei rekkje lover og forskrifter dei må halde seg til. Nokre av dei viktigaste er:

- Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energilova, 1990)
- Forskrift om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energilovforskrifta, 1990)
- Forskrift om beredskap i kraftforsyningen (beredskapsforskrifta, 2002)
- Forskrift om sikkerhet ved vassdragsanlegg (damtryggleiksforskrifta, 2010)

Dei viktigaste paragrafane i beredskapsforskrifta med omsyn til ROS er gitt nedanfor. Særskilde krav som må vurderast i ROS-analysane, er skrivne med **feit skrift**.

§ 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.

Beredskapsforskrifta stiller krav til at verksemda gjennom å ta i bruk risiko- og sårbarheitsanalysar på ein systematisk måte, skal kartleggje risiko og sårbarheit i forhold til *naturgitte forhold, teknisk svikt eller bevisst skadeverk* på dei systema, anlegga osv. som verksemda eig og driv.

Analysen skal også inkludere ei oversikt og vurdering over alle dei tiltaka beredskapsforskrifta listar opp som ein føresetnad for ein tilfredsstillande beredskap. Her finn ein ei kort liste over dei viktigaste pliktene ein ROS-analyse skal famne over, utover den generelle analysen med heimel i § 1–3: Det er tilrådd at den til ei kvar tid gjeldande rettleiinga til beredskapsforskrifta blir lagt til grunn for analysen, slik at alle pliktene kjem fram 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.

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**.

§ 5–2 – Meldeplikt
Eiere av eksisterende og planlagte kraftforsyningsanlegg som omfattes av energilovforskriften § 6–3 – jf. energiloven § 6–6, skal **melde fra til Norges vassdrags- og energidirektorat i 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 Norges vassdrags- og energidirektorats **vedtak om klasse foreta egen risiko- og sårbarhetsanalyse** (ROS), samt planlegge og utføre anleggene og systemene som angitt i denne forskriften. Norges vassdrags- og energidirektorat 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**. Beredskapsforkrifta listar opp ei rekkje krav som skal etterlevast.

§ 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. Forskrifta listar opp ei rekkje eksplisitte krav knytte til denne plikta.

§ 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.

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.

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 ledelsesfunksjoner 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**. Beredskapsforskrifta 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.

Denne serien blir publisert av Noregs vassdrags- og energidirektorat (NVE)

Publisert i Rettleiarserien/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 (56 s.)

Nr. 3 Konsesjonshandsaming av vasskraftsaker: Rettleiar for utarbeiding av meldingar, konsekvensutgreiingar og søknader (92 s.)

Nr. 4 Rettleiing i risiko- og sårbarheitsanalysar for kraftforsyninga (56 s.)

Noregs
vassdrags- og
energidirektorat

Noregs vassdrags- og energidirektorat

Middelthunsgate 29
Postboks 5091 Majorstuen,
0301 Oslo

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