

HØYPÅLITELIG KRAFTLEVERING OG DRIFT AV NETT FRA KONTROLLROM

MSAM60 Masteroppgave i samfunnssikkerhet



Universitetet i Stavanger

Det samfunnsvitenskapelige fakultet

Institutt for medie-, kultur- og samfunnsfag

Yvonne Hope Soltveit

UNIVERSITETET I STAVANGER

MASTERGRADSSTUDIUM I

SAMFUNNSSIKKERHET

MASTEROPPGAVE

SEMESTER:

Høst 2016 – Vår 2017

FORFATTER:

Yvonne Hope Soltveit

VEILEDER:

Kenneth Arne Pettersen

TITTEL PÅ MASTEROPPGAVE:

Høypålitelig kraftlevering og drift av nett fra kontrollrom

EMNEORD/STIKKORD:

Kraftlevering, pålitelighet, kraftnett, kontrollrom, High Reliability Organizations, Normal Accidents, kritisk infrastruktur, High Reliability Management, reliability professionals

SIDETALL:

84 (inkludert vedlegg)

STAVANGER 15.06.2017

SAMMENDRAG

Kraftforsyning anses som en kritisk infrastruktur og er fundamentalt i vårt samfunn. Andre infrastrukturer og samfunnsfunksjoner er avhengig av strøm, og bortfall av strøm kan medføre alvorlige samfunnsmessige følger. Per i dag er det en stabil forsyningssikkerhet, med en leveringspålitelighet på 99.987 % (Hansen et al., 2017). Nettselskaper har ansvaret for levering av elektrisitet til sluttbrukere innenfor sitt konsesjonsområde. Den teknologiske utviklingen medfører at kraftforsyningen blir tettere koblet og mer kompleks, blant annet ved at kraftanlegg fjernstyres fra nettselskapers kontrollrom. Ut i fra dette er problemstillingen for oppgaven: Hvordan kan nettselskaper opprettholde en høypålitelig strømlevering og hvilke forutsetninger må være til stede ved drift fra kontrollrom?

For å besvare problemstillingen blir det tatt utgangspunkt i ulike tilnærminger til sikkerhetsstyring av høyteknologiske organisasjoner; Normal Accidents, High Reliability Organization og High Reliability Management. I tillegg knyttes beredskap opp mot kraftforsyning. For å undersøke hvilke forutsetninger som ligger til grunn for drift av kontrollrom har dette studiet en kvalitativ tilnærming. Det har blitt innhentet data gjennom relevante dokumenter og ved å gjennomføre intervju og samtaler med åtte ansatte i et nettselskap.

Studiet viser at nettselskapers høypålitelige strømlevering og drift av nettet fra kontrollrommet forutsetter visse menneskelige og organisatoriske faktorer. Nettselskaper opplever som regel flere feilsituasjoner ved daglig drift. Når det oppstår hendelser utover daglige feilsituasjoner kan de betraktes som ekstraordinære hendelser. Ut i fra Beredskapsforskriften er det krav til at nettselskaper skal etablere et helhetlig beredskapskonsept og implementere det i virksomheten. Dette innebærer blant annet at det utarbeides en beredskapsplan. En slik plan er sentral for håndtering av hendelser, men operatørene på kontrollrommet må også evne å håndtere hendelser utover forventninger og beredskapsplanen. Det stiller krav til operatørens kognitive ferdigheter og erfaring ved improvisering og håndtering i sanntid. Faglige diskusjoner, scenariobygging, øvelser, evaluering og læring av hendelser er sentralt for å oppnå økt bevissthet og fleksibilitet, og dermed en mer pålitelig drift.

FORORD

Denne masteroppgaven marker slutten på to spennende og kjekke år på master i samfunnsikkerhet ved Universitet i Stavanger. Denne oppgaven tilsvarer 60 studiepoeng og har blitt skrevet over to semester. Det har vært en utfordrende, men også svært lærerik prosess.

Først og fremst vil jeg gi en stor takk til nettselskapet som har tatt meg godt i mot, samt alle informantene som har latt seg intervjuet og vist interesse for oppgaven. Uten deres bidrag ville det ikke vært mulig å skrive denne oppgaven.

Videre vil jeg takke veilederen min, Kenneth Arne Pettersen, for god hjelp under hele prosessen. Og tusen takk til nære og kjære som har lest korrektur.

Yvonne Hope Soltveit

Stavanger, 15. juni 2017

INNHALDSFORTEGNELSE

1	INNLEDNING	1
1.1	PROBLEMSTILLING	2
1.2	AVGRENSNING	2
1.3	TIDLIGERE FORSKNING	3
1.4	OPPGAVENS OPPBYGNING	3
2	BAKGRUNN OG KONTEKST	4
2.1	KRITISK INFRASTRUKTUR	4
2.2	DET NORSKE KRAFTSYSTEMET	5
2.3	KRAFTLEVERING	8
2.4	RELEVANTE FORSKRIFTER	9
2.4.1	BEREDSKAPSFORSKRIFTEN	9
2.4.2	LEVERINGSKVALITETFORSKRIFTEN	11
2.5	CASESTUDIE AV CALIFORNIA INDEPENDENT SYSTEM OPERATOR	12
2.5.1	HANDLINGSMODUS	14
2.5.2	FUNN I STUDIEN	16
3	TEORI	17
3.1	BEREDSKAP	17
3.1.1	PRINSIPPER FOR SAMFUNNSSIKKERHET OG BEREDSKAP	17
3.1.2	BEREDSKAP SARBEID	18
3.2	NORMAL ACCIDENTS	20
3.2.1	SYSTEMERS KOBLINGER OG INTERAKSJONER	22
3.3	HIGH RELIABILITY ORGANIZATIONS	24
3.4	MINDFULNESS	27
3.4.1	UTFORDRINGER KNYTTET TIL FORVENTNINGER OG PLANLEGGING	28
3.4.2	PRINSIPPER OM FORVENTNINGER OG BEGRENSNINGER	28
3.4.3	KOGNITIVE PROSESSER	32
3.5	HIGH RELIABILITY MANAGEMENT	33
3.6	OPPSUMMERING AV TEORI	37
4	METODE	39
4.1	FORSKNINGSDESIGN	39
4.2	FORSKNINGSSTRATEGI	39

4.3	FORSKNINGSMETODE	40
4.4	DATAINNSAMLING	40
4.4.1	INTERVJU	40
4.4.1.1	Valg av informanter	41
4.4.1.2	Gjennomføring av intervjuer	43
4.4.2	OBSERVASJON	43
4.4.3	DOKUMENTANALYSE	44
4.5	DATAREDUKSJON OG ANALYSE	45
4.6	VALIDITET OG RELIABILITET	45
4.7	ETISKE BETRAKTNINGER	47
5	EMPIRI	49
5.1	DAGLIG DRIFT	49
5.1.1	ARBEIDSOPPGAVER I LØPET AV EN ORDINÆR DAG	49
5.1.2	HÅNDTERING AV FEIL	51
5.2	BEVEGELSE MELLOM ULIKE BEREDSKAPSNIVÅER – SKJERPET DRIFT OG BEREDSKAP	53
5.2.1	BEREDSKAPSPLANENS ROLLE	53
5.2.2	HVEM TAR BESLUTNINGER?	54
5.2.3	SKJERPET DRIFT	55
5.2.4	PROSEDYRER VED BEREDSKAP	55
5.3	LÆRING KNYTTET TIL UØNSKEDE, UVENTEDE OG UKJENTE HENDELSER	57
5.4	RESULTAT FRA OBSERVASJON	59
6	DRØFTING	60
6.1	BEREDSKAP SARBEID I KRAFTFORSYNINGEN	60
6.2	STYRING AV HØYTEKNOLOGISK SYSTEM	61
6.3	MINDFULNESS SOM VERKTØY	63
6.4	KOGNITIVE FERDIGHETER	65
7	KONKLUSJON	68
7.1	VIDERE FORSKNING	69
8	REFERANSER	70
9	VEDLEGG	76

FIGURER

FIGUR 1: KRITISK INFRASTRUKTUR OG KRITISKE SAMFUNNSFUNKSJONER	5
FIGUR 2: HELHETLIG BEREDSKAPSKONSEPT	10
FIGUR 3: HANDLINGSMODUSER	14
FIGUR 4: BEREDSKAPSARBEID	19
FIGUR 5: INTERAKSJONER OG KOBLINGER	23
FIGUR 6: KOGNITIV PROSESS	32
FIGUR 7: HRO VS. HRM	34
FIGUR 8: KOGNITIVE DIMENSJONER	36
FIGUR 9: OVERSIKT OVER INFORMANTER	42

BEGREPSAVKLARING

CAISO	California Independent System Operator
DSB	Direktoratet for samfunnssikkerhet og beredskap
HRM	High Reliability Management
HRO	High Reliability Organizations
KBO	Kraftforsyningens beredskapsorganisasjon
KILE	Kvalitetsjusterte inntektsrammer ved ikke levert energi
NAT	Normal Accidents Theory
Nettsentral	Kontrollrom
NVE	Norges vassdrags- og energidirektorat

1 INNLEDNING

I dagens samfunn er det høy avhengighet til kraftforsyningen og ved bortfall kan det påvirke andre infrastrukturer og samfunnsfunksjoner. Per i dag kan forsyningssikkerheten for elektrisitet i Norge sies å være god og stabil (Meld. St. 25 (2015-2016), 2016, NOU 2006:6, 2006). I 2016 var leveringspåliteligheten 99.987 % (Hansen et al., 2017). På bakgrunn av avbruddsstatistikk kan man si at kraftforsyningen har etablert en robust infrastruktur hvor det er gjennomsnittlig få avbrudd per sluttbruker (NVE & Proactima, 2010). Det antas at investeringer i infrastrukturen sikrer en høypålitelig strømlevering, det er da snakk om blant annet vedlikehold, reparasjoner, utbedring av design og ny teknologi som for eksempel smarte målinger og ”smart-grids”. Utvikling av infrastruktur medfører at teknologien blir mer kompleks og det oppstår nye utfordringer som må håndteres på en tilfredsstillende måte (Roe & Schulman, 2016).

I dag finner man flere høyrisikoteknologier som er grunnleggende og nødvendig for å opprettholde samfunnet (Perrow, 1999). Organisatorisk pålitelighet handler om organisasjoners evne til å sikre en trygg og kontinuerlig håndtering av farlige tekniske systemer når risikoen for feil er høy. Interessen for dette feltet har økt de seneste årene. En årsak til dette er økende sosial avhengighet til teknologier som kan være farlige og krever høy ytelse, som for eksempel kjernekraft, el-nett og telekommunikasjon. Storulykker som Three Mile Island og Chernobyl har også vært med på å øke interessen for organisatorisk pålitelighet, da dette er eksempler på at teknisk design ikke garanterer kontinuerlig og trygg ytelse (Roe & Schulman, 2008). I følge Perrow (1999) sin teori om Normal Accidents er det ikke til å unngå at kompleks og tett koblet teknologi opplever ulykker, mens teorien om High Reliability Organizations ønsker å vise at hvis de rette strukturelle, kulturelle og ledelsesfaktorene er tilstede så kan høyrisikoteknologier unngå dette. Man må ta i betraktning at organisatoriske og menneskelige faktorer, i tillegg til det tekniske aspektet, medvirker til å opprettholde pålitelig kraftlevering.

Nettselskaper er sentrale aktører innenfor kraftforsyningen da de driver nettvirksomhet på distribusjons-, regional- eller sentralnivå og dermed har ansvaret for at deres kunder mottar strøm. I følge Roe og Schulman (2016, s. 37) er kontrollrom en viktig del av høypålitelig drift av infrastruktur, men til tross for det hevder de at; ”Yet infrastructure control rooms are under-researched in the organizational literature, and this is doubly true for the control room-to-control room relationships discussed in this book”. Tidligere studier har fokusert på fysisk

design, teknologi og analyser av menneskelige faktorer, mens det er få analyser med utgangspunkt i det organisatoriske knyttet til kontrollrom (Roe & Schulman, 2016).

1.1 Problemstilling

Med utgangspunkt i Roe og Schulman sin påstand om at kontrollrom er en viktig del av høypålitelig drift av infrastruktur er formålet med denne oppgaven å finne ut hva som danner grunnlaget for nettselskapers pålitelige strømlevering og betydning av deres kontrollrom. I henhold til nettselskapets robusthet vil det være hensiktsmessig å undersøke deres arbeid med forebygging av uønskede hendelse, beredskapsarbeid og hvilke praksiser de har for å opprettholde en stabil og tilfredsstillende produksjon, samt hvordan de håndterer uønskede hendelser. Problemstilling for denne oppgaven er følgende:

Hvordan kan nettselskaper opprettholde en høypålitelig strømlevering og hvilke forutsetninger må være til stede ved drift fra kontrollrom?

For å besvare problemstillingen på en systematisk måte vil følgende forskningsspørsmål være til god hjelp:

- Hva inngår i nettselskapet sin beredskapsstruktur og er det operasjonelt?
- Hvem tar beslutninger i beredskapssituasjoner?
- Hvordan tilegner nettselskapet seg ny kunnskap om risiko og farer, og hvordan anvendes dette?
- Hvilken kompetanse kreves det av de ansatte i nettselskapet?

1.2 Avgrensning

Som det fremkommer av problemstillingen vil fokuset ligge på kontrollrom sine forutsetninger for en høypålitelig strømlevering. Nettselskapers viktigste oppgave er å distribuere strøm til sluttbrukere, men for at det skal være mulig er de blant annet avhengig av at noen produserer og omsetter kraft (Meld. St. 25 (2015-2016), 2016). Dette avhengighetsforholdet vil ikke bli diskutert videre i oppgaven.

Oppgaven har en organisatorisk tilnærming, men det vil være behov for å inkludere noen tekniske aspekter for å danne en bedre forståelse av kraftlevering. Det vil ikke bli diskutert rundt teknologisk utvikling og utbedring av eksempelvis IKT-systemer eller kraftnettet og hvordan det kan påvirke nettselskapers leveringspålitelighet.

1.3 Tidligere forskning

Når det gjelder pålitelighet knyttet opp mot drift fra kontrollrom innen kraftforsyning er Roe og Schulman (2008; 2016) sine studier av høypålitelig styring innen kritisk infrastruktur svært relevant, men foruten om dette er det et tilsynelatende begrenset forskningsområde. Det er imidlertid gjort studier av sikkerhet og sårbarhet ved kraftforsyning (NOU 2006:6, 2006; Fridheim, Hagen, Henriksen, 2001).

1.4 Oppgavens oppbygning

I følgende kapittel vil bakgrunn og kontekst for oppgaven bli presentert. Det blir først sett nærmere på kritisk infrastruktur og hvor viktig det er for dagens samfunn. Deretter spisses det inn mot kraftlevering; hvordan det norske kraftsystemet er bygd opp, hvorfor en stabil kraftforsyning er nødvendig i dagens samfunn og relevante forskrifter som aktører innenfor kraftsektoren må forholde seg.

Kapittel tre tar for seg det teoretisk rammeverk. Først blir det gjort rede for begrepet beredskap og hvorfor det er sentralt for kraftlevering. Videre blir det gått gjennom to tradisjonelle tilnærminger av høyteknologiske organisasjoner, samt en alternativ tilnærming.

Kapittel fire går nærmere inn på hvordan datainnsamlingen har foregått, og resultatene fra datainnsamlingen blir presentert i kapittel fem. Det empiriske og teoretiske grunnlaget blir så analysert og drøftet i kapittel seks. I kapittel syv blir det presentert en konklusjon og avslutning for oppgaven.

2 BAKGRUNN OG KONTEKST

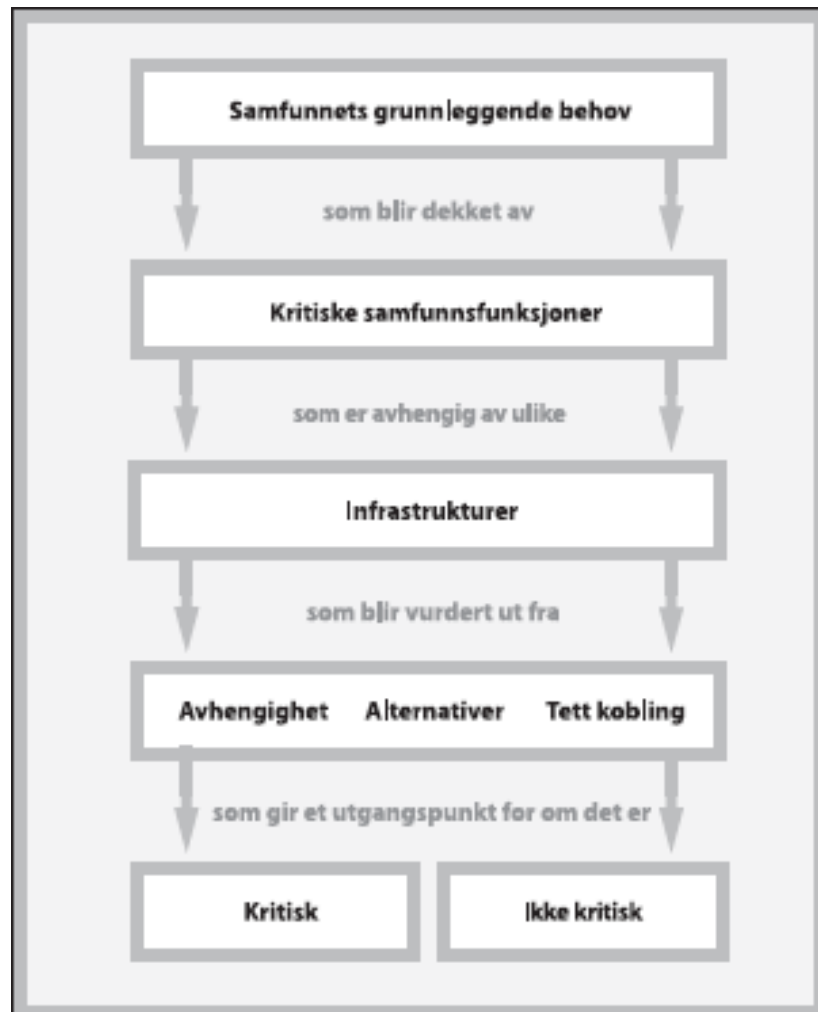
Dette kapittelet begynner med å kartlegge og identifisere kritiske infrastrukturer og kritiske samfunnsfunksjoner, og ser på hvordan disse er gjensidig avhengige. Deretter blir det norske kraftsystemet gjort rede for ved å se på struktur, organisering og funksjon. Det blir også knyttet opp relevante forskrifter som aktører innenfor kraftforsyning må forholde seg til. Til slutt blir det presentert en casestudie som danner et viktig grunnlag for oppgaven.

2.1 Kritisk infrastruktur

I NOU 2006:6 Når sikkerheten er viktigst (2006, s. 32) blir kritisk infrastruktur definert som ”... de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse”. Videre blir følgende infrastrukturer listet opp; elektrisk kraft, elektronisk kommunikasjon, vann og avløp, transport, olje og gass og satellittbasert infrastruktur – hvor samtlige betraktes som kritiske. Disse har blitt identifisert ut i fra tre kriterier; hvor stor avhengighet det er til infrastrukturen, om det er alternativer til infrastrukturen og hvor tett koblet infrastrukturen er (NOU 2006:6, 2006).

Ved å identifisere både kritisk infrastruktur og kritiske samfunnsfunksjoner vil man få en mer presis tilnærming til hva kritisk infrastruktur er. De samfunnsfunksjoner som er nødvendig for å dekke menneskers grunnleggende behov, som for eksempel vann og varme, betraktes som kritiske. Disse samfunnsfunksjonene vil også gi en pekepinn på hvilke infrastrukturer som er nødvendig ut i fra hva samfunnsfunksjonene er avhengighet av for å fungere. Eksempler på kritiske samfunnsfunksjoner er bank og finans, politi og matforsyning (NOU 2006:6, 2006). En annen tilnærming til hva som utgjør kritisk samfunnsfunksjoner finner man i Direktoratet for samfunnssikkerhet og beredskap sin KIKS-rapport hvor det vises til to forutsetninger for at en samfunnsfunksjon kan betraktes som kritisk; avgrensning i tid og kontekstuelle forutsetninger. Dersom samfunnet ikke klarer seg uten en samfunnsfunksjon i syv døgn og det utgjør en trussel mot grunnleggende behov, samt bortfallet av denne funksjonen skjer på et ubeleilig tidspunkt, kan funksjonen defineres som kritisk (DSB, 2012).

Identifisering og kartlegging av hvilke infrastrukturer og samfunnsfunksjoner som er kritiske vises i figur 1.



Figur 1: Kritisk infrastruktur og kritiske samfunnsfunksjoner (NOU 2006:6, 2006, s. 33)

Sikkerhet og beredskap innen kritisk infrastruktur er et aktuelt og interessant tema, og i denne oppgaven vil fokuset være på kraftlevering da elektrisk kraft er blant de infrastrukturene som blir identifisert som kritisk (NOU 2006:6, 2006).

2.2 Det norske kraftsystemet

Kraftforsyning utgjør den største delen av energiforsyning i Norge (Meld. St. 25 (2015-2016), 2016). Innen kraftforsyningen er det tre grunnleggende funksjoner: produksjon, overføring og omsetning. Et velfungerende kraftnett er helt nødvendig for at sluttbrukere skal få strøm. Kraftnettet er bygd opp av tre ulike nett; sentralnettet, regionalnettet og distribusjonsnettet.

Sentralnettet er hovednettet, regionalnettet fungerer som bindeledd mellom sentralnettet og distribusjonsnettet, og distribusjonsnettet er det lokale nett (NVE (2016, 02.08))

For å sikre en stabil og effektiv drift av kraftinfrastrukturen brukes det drifts- og styringssystemer for å styre de fysiske kraftinfrastrukturene som står for produksjonen, distribusjonen og omsetningen av elektrisk kraft. En stabil infrastruktur og en tett kobling til drifts- og styringssystemet er nødvendig når det gjelder handel av kraft. Produksjon av elektrisitet er just-in-time system og derfor krever det tilfredsstillende informasjonsflyt og koordinering mellom handels-, drifts- og styringssystemer. At ulike aktører innenfor kraftsektoren kan kommunisere raskt og utveksle informasjon er helt nødvendig for at elektrisitetsproduksjonen treffer forbrukernes behov.

Forbrukere utfordrer system ved å bruke lys, varmeovner, motorer og annet elektrisk utstyr. Den øyeblikkelige tilkoblingen av elektrisk utstyr krever en umiddelbar reaksjon fra aggregater og brytere i nettet for å opprettholde frekvensen, spenningsnivået og stabiliteten i leveransen (NOU 2006:6, 2006, s. 114).

Før IKT vokste frem var det ansatte som styrte de fysiske kraftinfrastrukturene manuelt, mens det i dag fjernstyres fra kontrollrom (NOU 2006:6, 2006). Nettselskaper har ansvar for å levere strøm til alle kundene i deres områdekonsesjon NVE (2016, 02.08)

I Norge er det Statnett som er ansvarlig for å opprettholde et balansert kraftsystem. Det vil si at de har overordnet fysisk styring og kontroll av kraftsystemet, noe som innebærer at de skal balansere produksjon og forbruk av strøm (Statnett, 2016, 04.08). Statnett er underlagt Forskrift om systemansvaret i kraftsystemet (Fos), som er en forskrift under energiloven, hvis formål er:

Denne forskriften skal legge til rette for et effektivt kraftmarked og en tilfredsstillende leveringskvalitet i kraftsystemet. Forskriften skal sikre at systemansvaret utøves på en samfunnsmessig rasjonell måte, herunder skal det tas hensyn til allmenne og private interesser som blir berørt (Forskrift om systemansvaret i kraftsystemet, 2002)

Norges vassdrags- og energidirektorat (NVE) er en sentral aktør innenfor det norske kraftsystemet. Tilsyn, veiledning og øvelser er viktige arbeidsoppgaver de har (NVE, 2016, 24.02). Blant annet ble Kraftforsyningens beredskapsorganisasjon (KBO) etablert med formål

om å organisere beredskap innen det norske kraftsystemet. KBO består av NVE og de virksomheter som står for kraftforsyninger, hvor det er NVE som har det overordnede ansvaret. Dette innebærer at de skal samordne beredskapsplanleggingen, og i beredskapssituasjoner og krig er det de som er ansvarlig for å lede landets kraftforsyning. Det er imidlertid opp til en hver virksomhet å sørge for tilstrekkelig forebygging, beredskap og krisehåndtering. Ved å etablere rammebetingelser, føre tilsyn, veilede og tilrettelegge for øvelser kan NVE legge føringer for at disse punktene oppfylles av virksomhetene. Når en ekstraordinær hendelse inntreffer er det ønskelig at situasjonen skal håndteres på lavest mulig nivå av de som har det daglige ansvaret, samt at organisering virksomheten er tilnærmet lik som i normaltilstand. Ved behov må det være åpent for både vertikalt og horisontalt samarbeid (NVE, 2016, 15.04). En slik tilnærming til krisehåndtering kan knyttes opp mot de fire beredskapsprinsippene: ansvarsprinsippet, likhetsprinsippet, nærhetsprinsippet og samvirkeprinsippet. Disse gjennomsyrrer hele den norske beredskapstankegangen (Meld. St. 29 (2011-2011), 2012).

Norges mange fjell, lange kystlinje og mengde nedbør, i tillegg til lokasjon i en kjølig klimasone, er faktorer som bidrar til at Norge har et særegent kraftsystem og skiller seg fra andre land. I motsetning til mange andre land produseres store deler av elektrisiteten av vannkraft fremfor andre energikilder som for eksempel olje og gass. Omtrent 98 prosent av kraften produseres av fornybar energi, i så måte har det resultert i lavest utslipp i Europa og høyest andel fornybar kraft (Meld. St. 25 (2015-2016), 2016, s. 29).

”Forsyningssikkerhet defineres som kraftsystemets evne til kontinuerlig å levere strøm av en gitt kvalitet til sluttbrukere, og omfatter både energisikkerhet, effektsikkerhet og driftssikkerhet” (Meld. St. 25 (2015-2016), 2016, s. 42). Dette omhandler evnen til å dekke energibruken og å dekke momentan belastning, samt evnen til å motstå driftsforstyrrelser. Mangel på energi, eksempelvis vann, kan medføre redusert produksjon av elektrisk energi og gi energiknapphet eller svikt i energisikkerheten. Energiknapphet kan strekke seg over en lengre periode, i motsetning til effektknapphet som vil si tilgjengelig kapasiteten i kraftproduksjon eller kraftnett, i enkelttimer hvor det er høyt forbruk (Meld. St. 25 (2015-2016), 2016).

Det er leveringspåliteligheten, spenningskvaliteten og kontakten mellom kundene og nettselskapet som utgjør leveringskvaliteten i et kraftsystem. Hvor ofte det oppstår avbrudd og avbruddets varighet kan brukes som et mål på leveringspåliteligheten, og kundene danner seg en mening om det er høy eller lav leveringspålitelighet basert på hvor mange avbrudd de

opplever. Per i dag er det ikke etablert et tallfestet krav som norske kraftselskaper må forholde seg til når det gjelder leveringspåliteligheten, det er imidlertid regulert gjennom forskrift om leveringskvalitet i kraftsystemet (leveringskvalitetsforskriften) (NVE, 23.02.17 b). Leveringspåliteligheten ligger på nærmere 99.99 %, men med det sagt vil det aldri bli 100 % da det krever urimelig store investeringer i infrastruktur. Dette krever at aktører som er avhengig av uavbrutt strømforsyning er ansvarlig for å ha alternativ forsyning tilgjengelig, eksempelvis nødstrømsaggregat (Meld. St. 25 (2015-2016), 2016, s. 44).

2.3 Kraftlevering

I det norske samfunnet i dag er det høyt elektrisitetsforbruk, noe som fører til at samfunnet er avhengig av en stabil kraftlevering (Fridheim, Hagen & Henriksen, 2001). Dette kan man også se ut i fra NVEs fjerde kvartalsrapport fra 2016 hvor det vises at den årlige kraftproduksjonen og -forbruket har økt betraktelig fra året før, samt at Norge er et av de nordiske landene med høyest produksjon og forbruk. I 2016 ble det produsert 148,8 TWh og brukt 132,3 TWh mot 143,4 TWh og 128,6 TWh i 2015. 2016 ble rekordår for produksjon av kraft i Norge, og det ble produsert 0,9 TWh mer enn sist rekord fra 2012. Hovedårsaken til den økte produksjonen og forbruket kan relateres til vær og klima, da året startet med påfølgende kalde uker (NVE, 2017, 19.01). Et fungerende og tilstrekkelig strømnnett er i dagens samfunn essensielt. Avhengigheten til kraftverk øker i takt med moderniseringen av samfunnet, hvor blant annet den teknologiske utviklingen har gjort samfunnet mer sårbart ovenfor strømstans (NOU 2006:6, s. 113).

Da elektrisitet er en fundamental infrastruktur for samfunnet vil det være interessant å undersøke hvor sårbart et samfunn kan bli ved brudd i strømforsyning over lengre tid – da med tanke på hvor lang tid er det snakk om før det kan oppstå skader av betydning, hvem som blir påvirket og i hvilken grad. Dette kan man oppnå mer kunnskap om ved å se tilbake på tidligere hendelser som har medført alvorlige konsekvenser. Et eksempel er isstormen som rammet Quebec, Canada i januar 1998, hvor 1.4 millioner forbrukere mistet strømmen. Kraftleveringen ble gjenopprettet innen en uke for de fleste av brukerne, men det var også noen som var uten strøm i opptil én måned. Kraftselskapene klarte å stabilisere strømleveringen i de utsatte områdene ved å mobilisere både nasjonale og internasjonale ressurser. Det viste seg at omtrent ti prosent av befolkningen hadde behov for assistanse, dette var hovedsakelig eldre og uføre. Selv om isstormen ikke medførte langsiktige nasjonaløkonomiske skadevirkninger var det fremdeles kostbart og det oppstod en momentan kollaps i samfunnet. Det normale

samfunnslivet og økonomien stoppet opp for en kort periode. Det oppstod utfordringer knyttet til hygiene og tilgang til mat og kontanter. Det oppstod også forstyrrelser i arbeidsmarkedet da folk ikke hadde mulighet til å komme seg på jobb. Erfaringene man kan ta fra denne hendelsen er at bortfall av kraftlevering i en ukes tid ikke nødvendigvis trenger å medføre langvarige konsekvenser så lenge situasjonen håndteres på en god måte (Fridheim, Hagen & Henriksen, 2001).

For at forbrukerne skal motta strøm fra produsentene krever det et fungerende overføringsnett (Meld. St. 25 (2015-2016), 2016). Eventuell strømstans i et område vil ha individuell påvirkning. Det kan være alt i fra mindre betydelige og hverdagslige handlinger som at man ikke får ladet mobilen eller at man ikke har internettilgang – til å berøre en på et mer alvorlig plan hvor det kan medføre uønskede konsekvenser, som for eksempel langvarig strømbrudd eller stans av kritiske samfunnsfunksjoner. Da strømbrudd kan oppfattes som alvorlige, kan kunders tillit til kraftleverandører være et insentiv for å holde en pålitelighet kraftlevering.

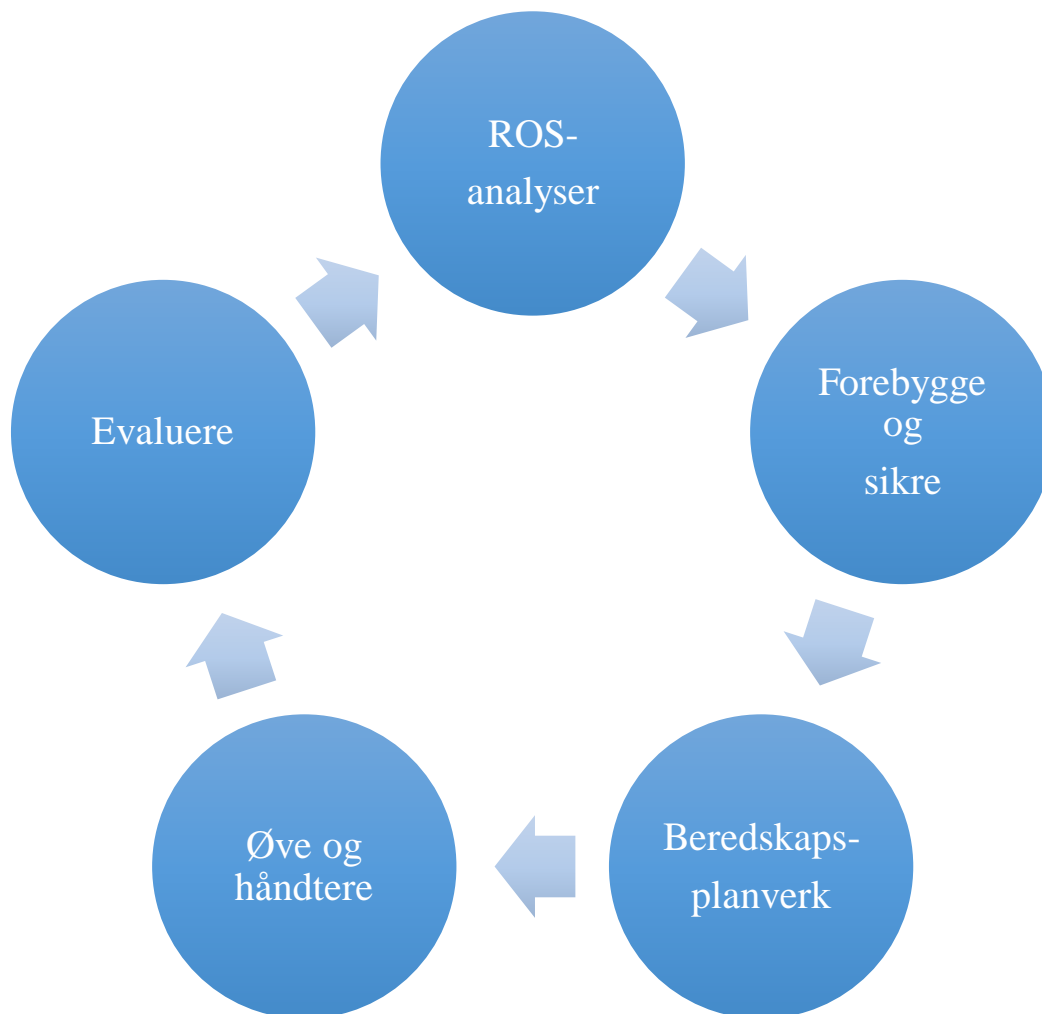
Som nevnt ovenfor har modernisering og teknologisk fremgang hatt stor betydning for samfunnsutviklingen, det er imidlertid en bakside ved dette; truslene blir flere og større. Det er en faktor som kraftselskaper må ta i betraktning og som bør prege deres arbeid med beredskap. I følge Losnegård (2013) innebærer et utvidet trusselbilde at samfunnet er sårbart ovenfor både menneskeskapte og naturlige hendelser; global oppvarming påvirker miljø, vær og vind, et stadig mer globalisert verdenssamfunn øker sjansen for at mennesker utfører vilde hendelser som kan være til skade for samfunnet, og svikt i teknologien kan medføre omfattende følger. Dette er faktorer som også blir tatt opp som trussel mot kraftforsyningen i Forsvarets forskningsinstitutt (FFI) sin BAS-rapport (beskyttelse av samfunnet) hvor de har undersøkt sårbarhet i henhold til kraftforsyning og samfunnet (Fridheim, Hagen & Henriksen, 2001).

2.4 Relevante forskrifter

2.4.1 Beredskapsforskriften

Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen, også referert til som Beredskapsforskriften, har som formål å ”sikre at energiforsyningen opprettholdes og at normal forsyning gjenopprettes på en effektiv og sikker måte i og etter ekstraordinære situasjoner for å redusere de samfunnsmessige konsekvensene” (§ 1-1, Beredskapsforskriften, 2012). Hva som utgjør en ekstraordinær hendelse vil være situasjonsbetinget, men det omfatter som regel

uønskede hendelser som avviker fra dagligdagse feilsituasjoner. En ekstraordinær hendelse kan eskalere til å bli en ekstraordinær situasjon – som det også er krav om at selskaper skal håndtere. For at selskaper skal være i stand til å håndtere ekstraordinære hendelser eller situasjoner må de ha etablert et helhetlig beredskapskonsept, som vist i figur 2.



Figur 2: Helhetlig beredskapskonsept (NVE, 2013, s. 13)

For å utvikle gode beredskapsplaner vil det være hensiktsmessig å gjennomføre ROS-analyser for å kartlegge og identifisere sårbarheter som kan true eller redusere virksomhetens drift. Det er viktig at man skiller mellom uønsket hendelse og årsak når man skal kartlegge og identifisere uønskede hendelser – uvær kan være en årsak til at en uønsket hendelse inntreffer, som for eksempel at en mast blir skadet (NVE, 2013, s. 9). ROS-analyser gir en mulighet til å sortere de hendelsene som kan forebygges og de som må håndteres ved hjelp av beredskapsplaner. Det er ikke alle hendelser som kan forebygges og det er hensiktsmessig å identifisere og kartlegge

disse slik at de blir mer håndterbare, og man får mulighet til å øve på håndtering av slike hendelser (NVE, 2013, s. 13). Ut i fra ROS-analyse utarbeides det risikoreducerende tiltak. Årsaksreducerende tiltak, eller forebyggende tiltak, skal forhindre at uønskede hendelser inntreffer, mens skadereducerende tiltak skal bidra til å begrense skadeomfanget hvis en uønsket hendelse inntreffer (NVE & Proactima, 2010). Det er krav til at ROS-analysene skal være oppdatert og dokumentert. I §2-4 fremkommer det at analysen skal gjennomgås minimum en gang i året og at den må oppdateres ved behov (NVE & Proactima, 2010; Beredskapsforskriften, 2012). Et slikt behov kan for blant annet oppstå etter evaluering av ekstraordinære hendelser eller øvelser (NVE, 2013, s. 13).

Det stilles krav til virksomheter om at de har beredskapsleder og beredskapskoordinator som er ansvarlig for at virksomheten retter seg etter Beredskapsforskriften. Ved å opprette disse funksjonene kan virksomhetene utvikle nødvendig kompetanse og bli bedre egnet til å håndtere hendelser som truer energiforsyningen.

2.4.2 Leveringskvalitetsforskriften

De som eier, driver eller bruker elektrisk anlegg eller elektrisk utstyr som er tilkoblet i det norske kraftsystemet må underlegge seg leveringskvalitetsforskriften. Formålet med leveringskvalitetsforskriften er følgende; ”Forskriften skal bidra til å sikre en tilfredsstillende leveringskvalitet i det norske kraftsystemet, og en samfunnsmessig rasjonell drift, utbygging og utvikling av kraftsystemet. Herunder skal det tas hensyn til allmenne og private interesser som blir berørt” (§ 1-1, Leveringskvalitetsforskriften, 2004). Hva som utgjør tilfredsstillende leveringskvalitet vil forandres i takt med samfunnsutviklingen. Dagens behov for elektrisitet er stort og dermed gir det høyere forventninger til hva som er tilfredsstillende leveringskvaliteten (NVE, 2016).

Avbrudd kan defineres som utelatt levering til en eller flere sluttbrukere hvor forsyningsspenningen er under 5 % av avtalt spenningsnivå. Et avbrudd anses som kortvarig ved varighet på inntil tre minutter og som langvarig dersom det overstiger tre minutter (NVE, 2016; NVE, 23.02.17 a). I 2016 opplevde sluttbrukerne i gjennomsnitt 0.3 varslet langvarig avbrudd, 1.6 uvarslet langvarige brudd og 1.7 kortvarige avbrudd. Dette utgjorde i gjennomsnitt en opplevelse av langvarig avbrudd på 2 timer og 9 minutter og 1 minutt og 12 sekunder med kortvarige avbrudd. Gjennomsnittlig gjenopprettingstiden for langvarige avbrudd var 1 time og 9 minutter og for kortvarige avbrudd tok det 42 sekunder (Hansen et al., 2017).

2.5 Casestudie av California Independent System Operator

I 2001 startet Roe og Schulman en casestudie av California Independent System Operator (CAISO). De begrunner deres studie av kritisk infrastruktur med at kritisk infrastruktur og de virksomheter som tilbyr det, er viktig for sosiale goder, tjenester og aktivitet (Roe & Schulman, 2008).

CAISO var ansvarlig for de fleste høyspentanlegg i California og kundetallet deres var estimert til å være rundt 65 millioner. CAISO ble etablert med mandat om å sikre høypålitelig kraftlevering under forutsetninger om feilstruktur og regulatorisk usikkerhet som følge av omstrukturering av kraftsektoren i California. Når Roe og Schulman startet casestudiet i 2001 var California midt i en kraftkrise, og formålet deres var å kartlegge de nødvendige ferdigheter for å vedlikeholde og ha en kontinuerlig levering av kritiske tjenester. Hovedmålet var å kunne beholde lyset på, selv i situasjoner hvor kapasiteten og ressursene var knapp (Roe & Schulman, 2008).

Under casestudiet fikk Roe og Schulman tilgang til CAISO sitt kontrollrom, og de opplevde energikrisen på nært hold og fra et nokså uventet perspektiv. Roe og Schulman beskriver kontrollrommet som en halvsirkel med god takhøyde hvor en oversikt over hele det høyspente kraftnettet i California var fremstilt på en hel vegg. Ved siden av kartet var det en stor multifunksjonell videomonitor som viste jevnlig oppdatert status på de viktigste indikatorene og parameterne til kraftnettet. Roe og Schulman understreker at operatørene på kontrollrommet sitt arbeid har endret seg fra de startet studiet i 2001 frem til 2007, når de skrev boken. Flere av disse endringene var en følge av kraftkrisen i California.

I perioden for studiet var det to viktige standarder for drift, fastsatt av North American Electric Reliability Corporation (NERC), som var relevant for å kunne vurdere påliteligheten til CAISOs drift. Den første ytelsesstandarden (CPS1) sammenligner forholdet mellom frekvenser på kraftnettet mot Area Control Error (ACE). CPS1 er et verktøy for å vedlikeholde stabilitet på kraftnettet, det er imidlertid vanskelig å håndtere (vurdere og følge med på) denne standarden. Den andre ytelsesstandarden, CPS2, er mer synlig ettersom det sier at ACE skal brukes for å overvåke og begrense overdreven kraftbruk da det kan medføre ustabilitet i kraftnettet. Dersom CAISO ikke overholder kravene som blir stilt i standarden, blir de tildelt en økonomisk sanksjon av WECC. I tillegg til ytelsesstandardene er CAISO sin drift av

kraftnettet også styrt etter standarder for kontroll av forstyrrelser (DCSs – disturbance control standards) (Roe & Schulman, 2008).

Roe og Schulman fikk som sagt tilgang til kontrollrommet i 2001, i perioden april til desember. I løpet av denne tiden ble det utført intervjuer og observasjon av arbeiderne i kontrollrommet, samt andre sentrale aktører og interessenter innenfor kraftsektoren. Imidlertid var CAISO hovedfokuset for datainnsamlingen. Ut i fra disse intervjuene og da særlig med tanke på CAISO, oppdaget Roe og Schulman et sterkt samvirke mellom de ulike aktørene i kraftsektoren i California. De oppdaget blant annet at hver av operatørene i kontrollrommet hos CAISO var knyttet til eksterne aktører via kommunikasjon- og tilbakemeldingssystemer. På grunn av omstruktureringer var kraftsektoren fragmentert, men fremdeles tett koblet sammen. En slik oppdeling gjorde at det var sterk avhengighet blant de ulike aktørene (Roe & Schulman, 2008).

Operatørene i CAISO sitt kontrollrom måtte evne å respondere raskt på uventende og ukontrollerte hendelser. Kraftkrisen medvirket til at arbeidstempoet og arbeidsoppgavene til operatørene sjeldent var på et ”normalt” nivå, ved deres første besøk i 2001. Under de travleste og hektiske periodene, observerte Roe og Schulman at det ikke var et system for å skille den viktigste informasjonen fra den mindre viktige, noe som medførte et økt behov for god informasjonsflyt både innad i CAISO og blant eksterne aktører. Ved overgang fra stadiet 1 til 2 ble arbeidsgruppen på kontrollrommet utvidet. Jo flere personer for å tolke informasjon, desto mindre sjans for å feil i driften. Imidlertid var noen dager verre enn andre, hvor for eksempel utførelse av en aktivitet kunne påvirke en annen aktivitet negativt – typisk raske løsninger. Dersom situasjonene da ble forverret kunne det gå fra stadiet 2 til 3 (Roe & Schulman, 2008).

Roe og Schulman sitt hovedfokus i studiet var forenligheten mellom CAISO sine alternativer og strategier for å oppnå krav om pålitelighet, som for øvrig handler om å balansere last og produksjon og overholde standarder, mens den andre delen handler om uforutsigbare og ukontrollerbare trusler mot målet om å oppnå pålitelighetskravene. En slik forenlighet oppstår dersom det er minst ett tilstrekkelig alternativ for å oppfylle kravene om pålitelighet i en hver situasjon. Det er til enhver tid mulighet for at det oppstår konflikt mellom systemvariablene som må opprettholdes for å oppnå pålitelighetskravene og de alternativer og strategier som er tilgjengelige for å håndtere disse variablene. Forenligheten mellom alternativer og systemkrav kan forklares følgende: i den omstrukturerte kraftsektoren er operatørene i kontrollrommet hos CAISO ansvarlig for kjerneoppgavene som er med på å opprettholde påliteligheten. Dette er

den eneste enheten som til en hver tid har to mandater å følge – opprettholde flyten og beskytte kraftnettet (Roe & Schulman, 2008).

2.5.1 Handlingsmodus

Høypålitelig styring i CASIO kan kategoriseres ut i fra de ulike nettverksalternativene som er tilgjengelig for operatørene (høy eller lav), volatiliteten i California sitt kraftsystem (høy eller lav), samt de resulterende handlingsmodusene som blir vedtatt i kontrollrommet. I den grad CAISO opplever uhåndterbare endringer eller uventede forhold som truer nettsystemet og påliteligheten til strømlevering (forstyrrelse av balansen mellom last og produksjon) kan omtales som volatilitet. Utvalg av nettverksalternativer innebærer ressurser som er tilgjengelig for CAISO når de skal respondere på en hendelse som forekommer i systemet slik at de kan vedlikeholde balansen mellom last og produksjon. De to dimensjonene illustreres i figur 3.

		SYSTEM VOLATILITY	
		High	Low
NETWORK OPTION VARIETY	High	Just-in-time performance	Just-in-case performance
	Low	Just-for-now performance	Just-this-way performance

Figur 3: Handlingsmoduser (Roe & Schulman, 2008, s. 42)

Denne figuren utgjør fire handlingsmoduser. Kort sagt kan man si at det handler om å vedlikeholde balansen mellom last og produksjon i samtlige tilstander, tilpasse seg eksterne endringer i systemvariablene for å kunne balansere last og produksjon, og bruke minst mulig tid i ”just-for-now”-modus. Roe og Schulman estimerte at CAISO i perioden juni 2001 til mai 2002 tilbrakte 20 % av tiden i ”just-for-now”, 70 % i ”just-in-time”, 10 % i ”just-in-case” og <1 % i ”just-this-way”. I april 2003 opplyste CAISO Roe og Schulman om at de i ca. 60 % av tiden var i ”just-in-time” og ”just-for-now” modusene. Selv om ett år med stabiliseringstiltak var gått, var forbedringene små (Roe & Schulman, 2008).

”Just-in-case performance”: Det er flere måter for å oppnå høy reliabilitet dersom nødvendig. I dette moduset er det lite informasjonsdeling da det er ikke behov for det, og operatørene tar i bruk individuell spesialisering og kompetanse for å følge prosedyrer og regler. Det er imidlertid viktig at operatørene er årvåken for forandringer som kan medføre feil selv om man er i en stabil tilstand.

”Just-in-time performance”: I en slik tilstand krever det at operatørene kan sette sammen de alternativer og strategier som er nødvendig for å vedlikeholde balansen mellom last og produksjon, dette er beslutninger som må tas raskt. Det krever god informasjonsflyt blant de involverte, og det blir gjerne satt inn ekstra arbeidskraft for en mer effektiv vurdering og kontinuerlig oppdateringer. Førsteprioriteten er å møte pålitelighetskravet og i noen situasjoner vil de operasjoner som utføres være akkurat nok til å opprettholde balansen. Man må være fleksibel kunne utvikle alternativer for å oppfylle kravene om pålitelighet. I dette handlingsmoduset krever det at operatørene kan handle raskt når uventede og ukontrollerbare hendelser oppstår, i tillegg forventes det at responsene deres da ikke er med på å forverre situasjonen. På grunn av høy volatilitet er det gjerne behov for ekstra arbeidskraft – det er mye informasjon som skal tolkes, og en av tankene bak at teamet utvides er at det skal redusere sjansen for feilhandlinger. I følge Boin, ‘t Hart, Stern og Sundelius (sitert i Roe & Schulman, 2008, s. 45) er det i dette handlingsmoduset at krisehåndteringen begynner å fremtre.

”Just-for-now performance”: Dette handlingsmoduset er det mest ustabile av de fire tilstandene og derfor ikke ønskelig å befinne seg i – dersom det er tilfellet vil operatørene arbeide for å bevege seg over i et av de andre modusene snarest mulig. Denne tilstanden er preget av raske løsninger. Det er færre og mindre tilstrekkelige alternativer tilgjengelig, og ved bruk av noen alternativer vil andre utelukkes. Dette kan medføre at forutsigbarhet og kontroll svekkes, og videre beslutninger kan lede til økning i volatilitet. I en slik tilstand kan marginale endringer være av betydelig trussel for leveringspålitelighet – dette er operatørene klar over.

”Just-this-way performance”: Dette handlingsmoduset er ment å være som en kortsiktig løsning når kriser inntreffer. I stedet for å være fleksibel når det gjelder alternativer og strategier er det ønskelig å ha full kontroll over systemvariabelen last.

2.5.2 Funn i studien

Roe og Schulman fant i studiene sine at CAISO sin praksis unnviker fra både teorien om høypålitelige organisasjoner (HRO) og Normal Accidents (NAT). Selv om de ulike teoriene ville resonneret seg frem til en konklusjon på ulik måte, sier de begge likevel at omstruktureringen i Californias kraftsektor skulle hatt en betydelig innvirkning på leveringspåliteligheten av strøm. Ut i fra NAT ville de tette koblingene og komplekse interaksjonene øke sannsynlighetene for kaskaderende feil, mens HRO antar av organisasjonens evne til å forutse hendelser svekkes. Derimot viste det seg at nettverket av deregulerte generatorer, verktøy og overføringsledere var preget av høy pålitelighet – selv under kraftkrisen. De fant det nødvendig å videreutvikle allerede etablerte teorier da de ikke støtter under det nivået av ”high reliability management” som de observerte under sitt studie av CAISO (Roe og Schulman (2008, s. 50)

Roe og Schulman (2008, s. 51) hevder at det har blitt viet lite oppmerksomhet mot ideen om at pålitelighet krever mer enn forventninger og planlagt beredskap, og i denne sammenhengen introduserer de begrepene ”high reliability management” og ”reliability professionals”. Disse vil det bli sett nærmere på i teorikapittelet.

3 TEORI

I dette kapittelet vil det teoretiske grunnlaget for oppgaven bli presentert. Først vil jeg se nærmere på hva beredskap innebærer og knytte det opp mot kraftsektoren. Deretter går jeg gjennom to sentrale teorier for risiko- og sikkerhetsstyring (Aven et al., 2004), ”Normal Accidents” og ”High Reliability Organizations”, som fokuserer på høyteknologiske organisatorer sin håndtering av uønskede hendelser og ulykker. I forbindelse med HRO-teorien er ”mindfulness” sentralt og det blir en gjennomgang av dette begrepet. Til slutt vil jeg se nærmere på en alternativ tilnærming, High Reliability Management, og hva det handler om.

3.1 Beredskap

Man ønsker å være beredt dersom uønskede hendelser inntreffer – uavhengig om det er forventet eller ei. Situasjonen vil bli mer håndterbar dersom man er forberedt, samt det kan være med på å minimere følger av hendelsen. Å forebygge og planlegge er sentralt for god og hensiktsmessig krisehåndtering (Engen et al., 2016).

3.1.1 Prinsipper for samfunnssikkerhet og beredskap

I Norge er det fire samfunnssikkerhets- og beredskapsprinsipper som danner grunnlaget for håndtering av uønskede hendelser. I utgangspunktet ble det utarbeidet tre prinsipper; ansvarsprinsippet, likhetsprinsippet og nærhetsprinsippet. Disse ble introdusert i St.meld. nr. 17 (2001-2002) Samfunnssikkerhet – veien til et mindre sårbart samfunn. Prinsippene viste seg hensiktsmessig, men det ble sett på som nødvendig å utarbeide et fjerde prinsipp slik at sammenhengen mellom samfunnets totale ressurser og samvirke mellom aktører ble inkludert. Prinsippene kan forklares følgende (Engen et al., 2016, s. 282-283; Meld. St. 29 (2011-2012), 2012, s. 39.):

1. Ansvarsprinsippet

Den myndighet, etat eller virksomhet som til daglig har ansvaret for et område, også har ansvaret for å utføre nødvendige beredskapsforberedelser og for den utøvende tjenesten ved kriser og katastrofer. Dersom det inntreffer en ekstraordinær hendelse har de også ansvar for å planlegge hvordan funksjoner innenfor eget ansvarsområde skal opprettholdes og videreføres.

2. Likhetsprinsippet

Under en krise skal organisasjonen som det opereres med være tilnærmet lik den organisasjonen man har til daglig, så langt det lar seg gjøre. Dette prinsippet understreker viktigheten av at ansvarsforhold ikke skal endres ved krisehåndtering.

3. Nærhetsprinsippet

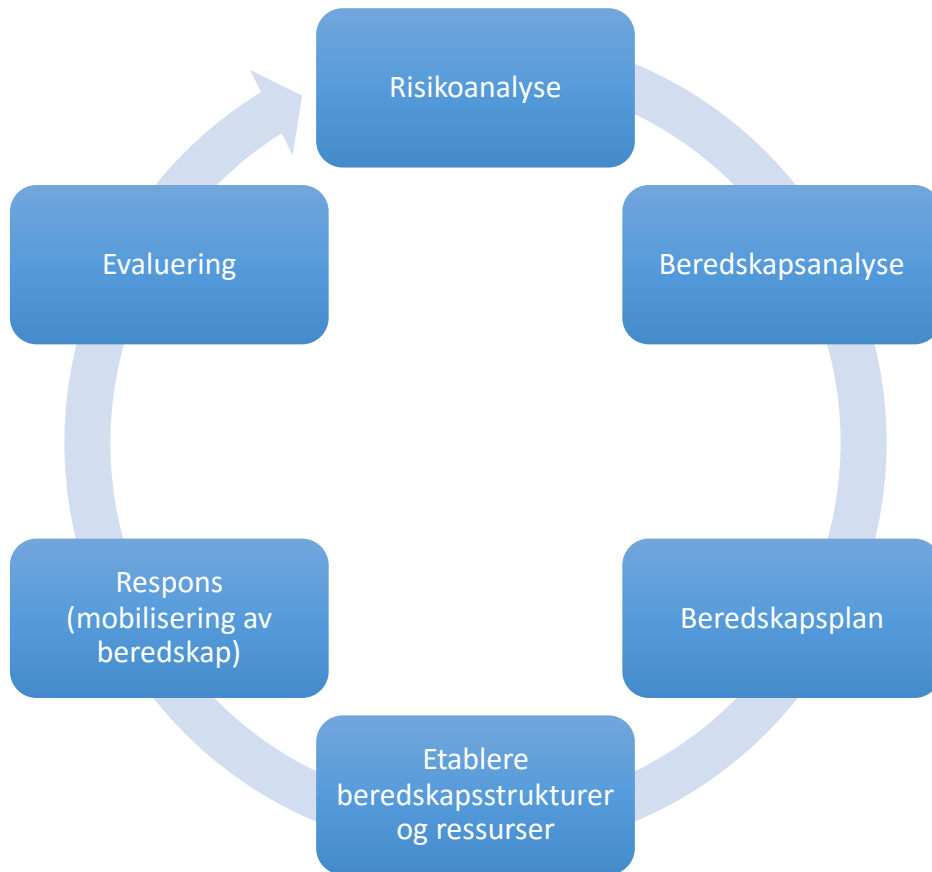
Kriser skal organisatorisk håndteres på lavest mulig nivå da de som har størst nærhet til krisen har best forutsetning for å forstå og håndtere situasjonen. Også dette prinsippet kan ses i sammenheng med ansvarsprinsippet da det er ønskelig at krisen skal håndteres innenfor det området som den inntreffer, med unntak ved sikkerhetspolitiske kriser.

4. Samvirkeprinsippet

Myndighet, etat eller virksomhet har et selvstendig ansvar for å sikre et best mulig samarbeid med relevante aktører i arbeidet med forebygging, beredskap og krisehåndtering. Formålet med prinsippet er å sikre at ressurser blir utnyttet på best mulig måte, noe som krever samvirke på tvers av ansvarsområder.

3.1.2 Beredskapsarbeid

Å identifisere, vurdere og håndtere risiko, samt følge dette opp, kan bidra til at risikoen ligger på et akseptabelt risikonivå. Det er også viktig at man forstår risikoen og eventuelle konsekvenser. Slik risikostyring er viktig for de fleste organisasjoner, og sentralt her er beredskapsplanlegging (Engen et al., 2016). Beredskapsarbeid innebærer at man planlegger og forbereder tiltak som kan iverksettes når en uønsket hendelse inntreffer (NOU, 2006). Engen et al. (2016) deler beredskapsarbeid inn i seks faser, som vist i figur 4.



Figur 4: Beredskapsarbeid (Engen et al, 2016, s. 284)

Det første steget er å utføre en risikoanalyse. En slik analyse har som formål å kunne beskrive risiko. Dette er en systematisk prosess hvor man tar utgangspunkt i identifiserte farer og trusler for å gjennomføre årsaks- og konsekvensanalyser av disse slik at man får etablert et risikobilde. Det vil foreligge usikkerhet til begge analysene og det er dermed viktig å inkludere usikkerhetsvurderinger i beslutningsgrunnlaget. De farer og trusler som identifiseres i forbindelse med risikoanalysen danner et viktig grunnlag for den neste fasen som er beredskapsanalyse. Man har nå et register over utvalgt uønskede hendelser som krever at man etablerer beredskap slik at de kan håndteres hvis de skulle inntreffe. En beredskapsanalyse har som formål å kartlegge virksomhetens mål knyttet til beredskap og tilgjengelige beredskapsressurser. Man bør se på både interne og eksterne ressurser for å få overblikk over hvilke ressurser man har og hvilke man mangler. Resultatet av beredskapsanalysen danner grunnlag for beredskapsplanen som skal utvikles. En slik plan inneholder ansvarsfordeling og beskrivelse av hvor, når og hvordan beslutninger skal tas. Det fremkommer også av planen hvilken beredskap som kreves for å håndtere gitte trusler og farer, hvordan ressurser skal

fordeles og hva slags beredskapsstruktur som skal etableres. Beredskapsorganisasjonen kan implementeres i virksomheten i forbindelse med virkelige hendelser eller som øvelse og trening. Det er viktig at virksomheten anser implementeringen som en gylden mulighet til å lære. Man er da kommet til den siste fasen i beredskapsarbeidet som innebærer at man evaluerer, og tar i bruk eventuell ny kunnskapen ved å oppdatere analysene og beredskapsplanen.

Å iverksette tiltak som kan bidra til å redusere sannsynligheten for at en hendelse skjer, samt bidra til å redusere følgene av uønskede hendelser, er forebyggende aktivitet. Det er imidlertid erkjent at det vil oppstå uønskede hendelser uavhengig av hvor god de forebyggende tiltakene er, og det er ikke alle hendelser som kan forebygges (NOU, 2006; Engen et al., 2016)

Det fremkommer av Beredskapsforskriften at KBO-enheter skal ha helhetlig, funksjonelt og kontinuerlig beredskapsarbeid:

Som det går fram av formålet §1-1, skal forskriften sikre at energiforsyningen opprettholdes og at normal forsyning gjenopprettes på en effektiv og sikker måte i og etter ekstraordinære situasjoner. Hensikten er å redusere de samfunnsmessige konsekvensene av manglende energiforsyning. En forutsetning for at selskapene skal være i stand til å håndtere ekstraordinære situasjoner, er at de har et helhetlig beredskapskonsept (NVE, 2013, s. 13).

3.2 Normal Accidents

Charles Perrow sin teori om "Normal Accidents" (NAT) handler om at systemulykker i høyrisikoteknologier ikke er til unngå; "Much can be done to make these systems somewhat safer, but accidents cannot be entirely avoided" (Perrow, 1999, s. 330). Sikkerhetstiltak, eksempelvis kvalitetskontroll og øvelser, som iverksettes for å unngå uønsket hendelse hjelper i den forstand at ulykkesfrekvensen reduseres. Til tross for effektiv sikkerhetsstyring tilsier karakteristikken ved høyrisikoteknologier at ulykker ikke kan unngås og de må betraktes som "normale" – derav "Normal Accidents".

NAT fokuserer på systemer fremfor individer og menneskelig feil da det er systemet i seg selv som frembringer skade, og av denne grunn så Perrow det nødvendig å etablere ulykkesdefinisjoner som fokuserer på karakteristikker ved systemet. Perrow skiller mellom

”accidents” og ”incidents”. Førstenevnte, ulykker, forklares som utilsiktede hendelser som involverer menneskelige og materielle skader i den grad at det forstyrrer nåværende eller fremtidig drift, samt har et betydelig skadeomfang. Hvis en utilsiktet og uønsket hendelse inntreffer uten å gi betydelige skader, betraktes det som en mindre hendelse (Perrow, 1984).

An accident is a failure in a subsystem, or the system as a whole, that damages more than one unit and in doing so disrupts the ongoing or future output of the system. An incident involves damage that is limited to parts or a unit, whether the failure disrupts the system or not. By disrupt we mean the output ceases or decreases to the extent that prompt repairs will be required (Perrow, 1999, s. 66).

Det skilles også mellom to former for ulykker; en systemulykke oppstår som følge av uventede interaksjoner mellom flere feil, mens en komponentfeil-ulykke innebærer at en eller flere komponentfeil – del, enhet eller delsystem – opptrer sammen, men da på en forventet måte. Ulykker kan altså skilles fra hverandre på grunnlag av om de er forutsett, forventet og forståelig for de som har utformet systemet og de som drifter det. Alle ulykker begynner med komponentfeil, men dersom det oppstår uventet samhandling mellom flere feil kan det medvirke til at komponentfeilen utvikler seg (Perrow, 1999, s. 71).

Ved å dele et system opp i fire nivåer blir det enklere å skille hendelsers betydning. Forstyrrelser på de to første nivåene anses som mindre hendelser, mens forstyrrelser på de to øverste nivåene er ulykker. De ulike nivåene er følgende (Perrow, 1999, s. 65):

1. Del

På det første nivået er det snakk om en del, eksempelvis en ventil, som er den minste komponenten i systemet.

2. Enhet

Flere deler utgjør til sammen en enhet, og dette er det andre nivået.

3. Delsystem

Det tredje nivået er delsystem bestående av flere enheter.

4. System

Til sammen utgjør delsystemene det helhetlige systemet, som er det fjerde og øverste nivået.

3.2.1 Systemers koblinger og interaksjoner

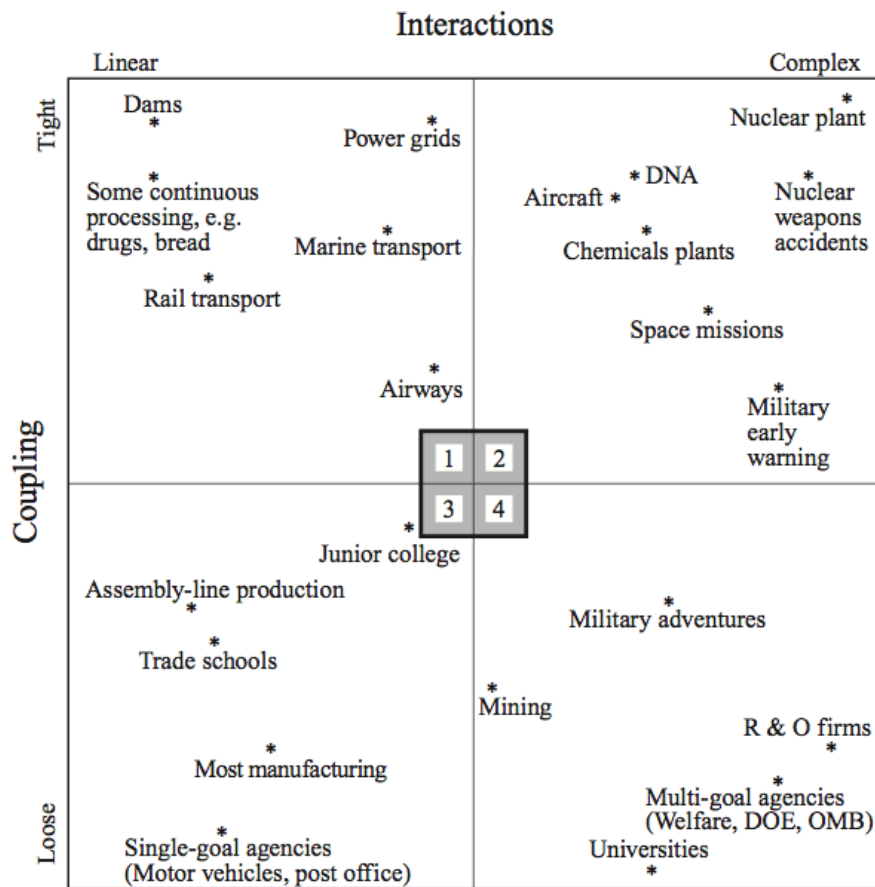
”Normale” ulykker kan knyttes til hvordan feil samhandler og hvordan systemet er oppbygd. Interaksjoner kan være lineære eller komplekse. Perrow definerer lineære interaksjoner som ”(...) those in expected and familiar production or maintenance sequence, and those that are quite visible even if unplanned”, mens komplekse interaksjoner er ”(...) unfamiliar sequences, or unplanned and unexpected sequences, and either not visible or not immediately comprehensive” (Perrow, 1999, s. 78). Det handler altså om interaksjonene er forventet eller ei.

At det er tette koblinger betyr at systemkomponentene er gjensidig avhengige. Endringer i en komponent kan påvirke en annen komponent og det er ikke rom for slakk mellom dem (Perrow, 1999). Skjer det en feil på nettet så må det i noen tilfeller fikses med en gang slik at det ikke får mulighet til å eskalere slik at den daglige driften forstyrres. I et løst koblet system vil det derimot være mulighet for å vente med å rette opp feil i en komponent uten at det påvirker daglig drift og det er ikke fare for at det sprer seg til en annen komponent eller utvikler seg til å bli kritisk. Overføringsnett kan oppleve kaskaderende hendelser, det vil si at en feil setter i gang kjedereaksjoner slik at flere kraftledninger detter ut (Almklov, Antonse, Fenstad, 2011). Et sentralt skille mellom tette og løse kobling er hvordan de gjenoppretter feil;

In tightly coupled systems the buffers and redundancies and substitutions must be designed in; they must be thought of in advance. In loosely coupled systems there is a better chance that expedient, spur-of-the-moment buffers and redundancies and substitutions can be found, even though they were not planned ahead of time.” (Perrow, 1999, s. 94-95).

Det er nødvendig å dimensjonere organisasjoners grad av interaksjoner ettersom så å si alle systemer er bygd opp av lineære interaksjoner, i tillegg opplever de fleste lineære systemer også komplekse interaksjoner. En kilde til kompleks interaksjon som alle systemer må forholde seg til er miljøet (Perrow, 1999, s. 75). Uvær medfører ofte uønskede hendelser for nettselskaper,

eksempelvis at lyn slår ned i en transformator eller at vinden river ned en mast. I figur 5 illustreres ulike sammensetningen av koblinger og interaksjoner med konkrete eksempler.



Figur 5: Interaksjoner og koblinger (Perrow, 1984, s. 97)

Som man kan se ut i fra kartet kan organisasjoner plasseres langs to dimensjoner; koblinger (tette eller løse) og interaksjoner (lineære eller komplekse). "Power grids", eller strømmnett, består av tette koblinger og lineære interaksjoner. I systemer som er tett koblede og lineære vil sentralisert ledelse være det beste styringsmåten (Engen et.al., 2016; Perrow, 1984). Et system med tette koblinger krever sentralisert styring og operasjoner, mens et system med komplekse interaksjoner krever desentralisert styring slik at uventede interaksjoner kan håndteres av de operatører som er nærmest og har best kjennskap til systemet.

En faktor som påvirker kraftforsynings kompleksitet er den stadige utviklingen av teknologien. Dette åpner opp muligheter for nettselskaper til å effektivisere drift, planlegging og vedlikehold av kraftnettet (NVE, 2015). Tidligere var større kraftforsyningsanlegg bemannet og de ble overvåket og manuelt betjent der i fra, mens i dag fjernstyres de fleste anleggene fra

driftssentraler. Denne utviklingen kommer imidlertid ikke uten en bakside; kompleksiteten og risikoen øker, og nye utfordringer oppstår (Fridheim, Hagen & Henriksen, 2001; NOU 2006:6, 2006; NVE, 2015). Ved at IKT-systemer er koblet sammen på en mer uoversiktlig måte enn tidligere, utgjør trolig enda tettere koblinger (Almklov, Antonsen & Fenstad, 2011). Kraftbransjen er avhengig av IKT, og kan sies å ha blitt en kritisk infrastruktur for andre infrastrukturer (Almklov, Fenstad & Røstum, 2011). Avhengighet til andre systemer bidrar også til at systemer opplever flere ukjente og uventede interaksjoner, og dermed blir mer sårbar for systemulykker (Perrow, 1999, s. 72).

3.3 High Reliability Organizations

Teorien om ”High Reliability Organizations” (HRO), eller høypålitelige organisasjoner, erkjenner at verken mennesker eller teknologi er feilfri – idealet om en feilfri organisasjon er dermed uopnåelig – og det er noen organisasjoner som har mer å tape enn andre dersom det forekommer alvorlige feil (LaPorte & Consolini, 1991). Deriblant er kraftlevering ansett som en høyrisikoteknologi hvor det er nødvendig med tilfredsstillende risikostyring, og derfor er det hensiktsmessig å ta med denne teorien for å danne et grunnlag for nettselskaper sitt utgangspunkt for å oppnå pålitelig kraftlevering.

Forskning viser at høypålitelige organisasjoners karakteristikk viser seg tydelig i kontrollrom; ”... a wide range of behaviour, namely technical competence, complex activities, high performance at peak levels, search for improvements, teamwork, pressures for safety, multiple (redundant) sources of information and cross-checks, and a culture of reliability, all working through tightly coupled, sophisticated technologies and systems” (Van Eeten & Roe, sitert i Schulman et al., 2004, s. 16).

Gjennomgående kjennetegn for høyteknologiske organisasjoner er at de er komplekse og tett koblede, har høy avhengighet, og de står ovenfor dynamiske omgivelser. Dersom en uønsket hendelse skulle oppstå kan det medføre alvorlige følger for både organisasjonen og samfunnet. At uønskede hendelser kan føre til at organisasjonen tar lærdom er ikke ukjent, men for høypålitelige organisasjoner vil konsekvensene og kostnadene overstige lærdommen som følge av visse hendelser. Slike organisasjoner må kunne håndtere komplekse teknologi slik at hendelser med alvorlige følger ikke inntreffer – samtidig som de må opprettholde produksjon av varer og tjenester for å møte de behov som er (LaPorte & Consolini, 1991).

Aven et al. (2004, s. 59) viser til fire kriterier som må oppfylles for at en organisasjon kan betraktes som høypålitelig:

1. Sikkerhet og pålitelighet har høyeste prioritet

Ledelsen skal ha sikkerhet og pålitelighet som høyeste prioritet, og det er deres oppgave å fremme dette i hele organisasjonen.

Høypålitelige organisasjoner kan karakteriseres ved at de på samme tid søker etter motstridende eller paradoksale egenskaper ved pålitelighet. Forsvarsregimer som skal beskytte mot en type feil kan trolig bidra til å øke sannsynligheten for at en annen type feil inntreffer og av denne grunn må organisasjoner ha klare og tydelige driftsprosedyrer og standarder, samt de kan ikke tillate seg å være ufølsom eller uoppmerksom mot uventede hendelser. For å unngå en slik utvikling er det nødvendig å utvikle strategier som er knyttet til forventninger og resiliens (Roe & Schulman, 2008, s. 51).

2. Redundans øker sikkerheten

Upålitelige komponenter kan til sammen utgjøre et pålitelig system, men det krever at organisasjonen har reservesystemer, overlapp og duplikasjoner. Teknisk redundans kan bygges inn i systemet, eksempelvis ekstra komponent. Dersom det oppstår feil i en komponent vil den tekniske redundansen ta noe av belastningen og det gir rom feil uten at det medfører katastrofale følger (Rosness et al., 2002).

Ved å bygge inn duplisering i systemet kan det gi bedre toleranse for feil. Med utgangspunkt i at mennesker kan begå feil vil for eksempel overlapping av hverandres arbeidsoppgaver og kompetanse være hensiktsmessig da det øker sannsynligheten for at feil oppdages og korrigeres. Dette betraktes som organisatorisk redundans, altså "(...) samhandlingsmønstre som tillater organisasjonen som et hele å opptre mer pålitelig enn operatørene hver for seg" (Rosness et al., 2002, s. 24). Organisatorisk redundans krever at strukturelle og kulturelle forhold er til stede i organisasjonen. I følge Aven et al. (2004) oppnås organisatorisk redundans ved at organisasjonsmedlemmene har ulik bakgrunn og erfaring, i så måte har organisasjonen større mulighet for å identifisere feil og farer. Det må også være åpent for organisasjonsmedlemmer å kunne korrigere hverandre og ikke minst rådføre seg med hverandre.

3. Desentralisert styring, sterk organisasjonskultur og kontinuerlig læring

Under kriser krever det at organisasjonen er fleksibel. Det innebærer at man ser bort i fra de roller og ansvarsforhold som man finner ved normal drift (Roberts, sitert i Roe & Schulman, 2008, s. 55). Det blir mindre formelt og mer fleksibelt når det kommer til koordinering og kommunikasjon mellom ansatte. LaPorte og Consolini (1991) sine studier viser at styringsstrukturen i høypålitelige organisasjoner beveger seg mellom tre ulike tilstander som var preget av rutiner og byråkrati, høytempo eller krisemodus. Rutinemessig og byråkratisk styringsstruktur finner man i situasjoner hvor det utføres standard prosedyrer og der hvor de som utfører arbeidet har høy kompetanse. Ved økt arbeidsmengde går styringsstrukturen over til å være høytempo. Det er de samme personene som jobber ved normalt tilstand, men det krever mer koordinering og samarbeid for optimal levering av tjenester. Det er økt fare for feilhandling og at en uønsket hendelse skal inntreffe og det er nødvendig med en rask respons. Beslutninger tas som regel av de på gulvet, og byråkratiet svekkes. Dersom organisasjonen går over i krisemodus når hendelser som inntreffer oppfattes som truende for liv og organisasjon. Det er da snakk om konkrete hendelser hvor planlagte og innøvde handlingssett iverksettes (La Porte & Consolini, 1991).

Organisasjonen må være i stand til å ta desentralisert beslutninger når uønskede hendelser oppstår og det er derfor viktig at organisasjonsmedlemmene på lavere nivå oppmuntres til å reagere på unormale situasjoner, gjennom kontinuerlig øvelse, trening og simulering. Dette antyder en sterk organisasjonskultur hvor pålitelighet er sentralt (Aven et al., 2004).

4. Organisatorisk læring

Organisasjonen kan ta erfaring og læring fra tidligere hendelser (Aven et al., 2004). Høypålitelige organisasjoner må kartlegge og identifisere uønskede hendelser. Ved å gjennomføre årsaksanalyser og gransking av forhold eller tidligere hendelser som impliserer risiko vil det legge føringer på hvordan organisasjonen skal oppnå pålitelighet. Det utvikles prosedyrer som begrenser atferd samtidig som alle i organisasjonen er bevisst på forhold som kan utløse feil (Roe & Schulman, 2008, s. 55).

3.4 Mindfulness

For å kunne håndtere det uventede må man forstå hvordan de organisatoriske forventningene fungerer, samt være bevisst på dette. Forventningene som er knyttet til de ulike rollene, rutinene og strategiene innad i en organisasjon danner grunnlaget for struktur og forutsigbarhet. Det er imidlertid en bakside ved slike forventninger da det danner en blindsoner hvor fokuset er på å bekrefte at forventningene faktisk stemmer, fremfor å avdekke uønskede hendelser. I denne blindsonen får mindre uønskede hendelser ofte mulighet til å utvikle seg til å bli større og de blir vanskeligere å håndtere. For å motvirke en slik virkning av satte forventningene krever det økt bevissthet – altså det som kan refereres til som ”mindfulness” (Weick & Sutcliffe, 2007).

”Mindfulness” kan kjennetegnes ved fem prinsipper og ved å følge disse prinsippene gjør det det mulig for å høypålitelige organisasjoner å vedlikeholde en pålitelig drift selv når de treffer på uventede hendelser. De tre første prinsippene handler om forventninger, mens de to siste handler om begrensninger (se seksjon 3.4.2). Å forberede seg på det uventede handler om mer enn bare å forvente det, og det er nettopp det de tre første prinsippene handler om. Forventninger innebærer at man forutser eller forestiller seg et eventuelt ukontrollert utfall som følge av små endringer. Man kan lage scenarioer hvor en liten endring fører til en større og alvorligere hendelse. Ved å forutse og lage scenarioer kan det fungere som en stopper for utvikling av uønskede hendelser. Man kan forhindre at små avvik eskaleres og sprer seg ved handlinger som operasjonaliserer de tre første prinsippene, men når et avvik først har fått mulighet til å eskalere seg er det ønskelig å forhindre konsekvenser som kan oppstå må det utføres handlinger som samsvarer med de to siste prinsippene stopper det (Weick & Sutcliffe, 2007).

Det er eksperter som hevder det er to sentrale årsaker som gjør det umulig å forvente det uventede; for det første så er man omringet av et uendelig antall svake signaler og for det andre så evner ikke de fleste organisasjoner å fange opp disse signalene da det går utenfor deres teknologiske evne. Imidlertid har det vist seg at organisasjoner som har mindre ulykker enn hva som er forventet ut i fra den virksomhet de driver, har bedre evne til å sanse uventede hendelser av betydning, enn de organisasjonene som har flere ulykker. Det betyr ikke nødvendigvis at høypålitelige organisasjoner oppdager avvik raskere, men når de først er avdekket så har de større forståelse og kan dermed håndtere hendelsen mer effektivt (Weick & Sutcliffe, 2007)

3.4.1 utfordringer knyttet til forventninger og planlegging

En beredskapsplan kan være et nyttig verktøy, men hvis man ikke erkjenner at det kan inntreffe hendelser som ikke er identifisert og kartlagt i planen vil den virke mot sin hensikt. Slike planer er laget ut i fra visse antagelser og belyser forventninger. Forventninger kan legge føringer på menneskers atferd og oppfatninger, og ofte danner man seg et bilde som kun bekrefter ens forventninger. Det er først når en ulykke har inntruffet at man oppdager et farefylt mønster av signaler som tidligere har blitt oversett. Man må passe på at beredskapsplaner ikke begrenser ens forventninger og ens oppfatning av egne evner. Beredskapsplanlegging utelukker ofte kombinasjoner av ens handlingsrepertoar for å håndtere uventede hendelser, i så måte kan beredskapsplaner utelukke improvisasjon. En siste utfordring er at beredskapsplaner fremmer gjentakelse av aktivitet som har vist seg vellykket tidligere og ved å fortsette slik oppnår man gode resultater, derimot vil ikke en slik tankegang ta i betraktning at rutiner ikke klarer å håndtere nye hendelser. Det er umulig å utvikle prosedyrer som passer til en hver situasjon, noe som krever at man er fleksibel; ”(...) reliable outcomes require the capabilities to sense the unexpected in a stable manner and yet deal with the unexpected in a variable manner” (Weick & Sutcliffe, 2007, s. 67). Det gjenspeiles i ens handlinger om man er “mindfulness” og fleksibel på samme tid ved at uventede hendelser håndteres på en tilfredsstillende måte.

3.4.2 Prinsipper om forventninger og begrensninger

De fem prinsippene er som følger:

1. Opptatt av feil

Høypålitelige organisasjoner har fokus på å avdekke eventuelle feil som kan eller har oppstått (Weick, Sutcliffe & Obstfeld, 1999). Ved å erkjenne og omfavne feil kan man også forhindre det. Dette innebærer at man må være oppmerksom på svake signaler om svikt da det kan være tegn på at det er større feil/problemer i systemet. I flere av strategiene som blir brukt av høypålitelige organisasjoner kommer det tydelig frem hvilke feil man ønsker. Organisasjoner som aktivt ser etter symptomer på funksjonsfeil, særlig symptomer som kan knyttes til strategisk feil, er bedre anlagt/i bedre stand til å skape praksiser som utelukker disse feilene.

Høypålitelige organisasjoner er opptatt av feil, i den forstand at de responderer på svake signaler om feil. Et eksempel her kan hentes fra et kraftselskap på østkysten i USA, hvor en av lederne hadde oppdaget en noe ukonvensjonell indikator på større problem i

systemet – økt forekomst av biestikk blant montører ble tolket som at de ikke så seg for når de skulle gripe etter ting, noe som vil si at de muligens slurver ved håndtering av kraftlinjene. Å oppdage feil er lettere sagt enn gjort. I noen tilfeller har man gjerne på følelsen at noe er galt, men vet ikke helt hva, mens andre ganger er det mer åpenbart og konkret. Når feil oppdages er det viktig at det rapporteres. Forskning viser at dersom virksomheter har god rapporteringskultur er det større sjanse for at de ansatte tør å rapportere. Ved å oppmuntre til og belønne rapportering vil høypålitelige organisasjoner kunne tilegne seg ny kunnskap (Weick & Sutcliffe, 2007).

2. Motvillig til å forenkle tolkninger

Forventninger forenkler verden og styrer observatører vekk fra det ubekreftede beviset som skygger for uventende problemer. For å hindre en slik forenkling foreslås det at man forsøker mindfulness da det retter fokus mot kontekst, kategorier og forventninger. Ved å se nærmere på kontekst vil man få et mer differensiert verdenssyn og tankegang, noe som igjen gjør det mulig å oppdage et bredere og mer variert bilde av konsekvenser, samt et bredere og mer variert sett av forholdsregler og tidlige varseltegn (Weick & Sutcliffe, 2007). Å unngå forenkling av tolkninger gjør at organisasjonsmedlemmene tar nødvendige forhåndsregler og det blir enklere for de å oppdage uønskede konsekvenser. Forenklinger er med på å øke sannsynligheten for uønskede hendelser fremtrer som overraskende (Weick, Sutcliffe & Obstfeld, 1999).

3. Operasjonell sensitivitet

Dette handler om individers situasjonsforståelse. Ved å være bevisst på ens omgivelser kan katastrofer avverges ved at små tiltak iverksettes for å hindre feil i å utvikle seg og forhindre at feil får rom til å samhandle (Weick, Sutcliffe & Obstfeld, 1999). Det kan knyttes til selve arbeidet som utføres og hvordan man faktisk handler uavhengig av hvilke intensjoner, system og planer som ligger til grunn. Et eksempel på slik operasjonell sensitivitet kan hentes fra helsesektoren; det ble oppdaget at et uvanlig høyt tall for stikkskader blant renholdspersonale, noe som kunne tenkes å være på grunn av at avfallsbeholderen var plassert rett under beholderen for sprøyteavfall. Avfallsbeholderen ble flyttet og stikkskadene ble redusert.

En god høypålitelig organisasjon må kunne gjennomføre prinsippet om operasjonell sensitivitet i praksis. Dette innebærer at deres handlinger erkjenner tvetydige

intensjoner og de jobber hardt for å gi oppmerksomhet mot små avvik og avbrudd i operasjonen deres (Weick & Sutcliffe, 2007).

Det er visse trusler som kan påvirke organisasjoners operasjonelle sensitivitet og som man må være bevisst på. Det er viktig at høypålitelige organisasjoner ikke skiller mellom kvalitativ kunnskap og kvantitativ kunnskap da det er nødvendig å ta begge typer kunnskap i betraktning for å kunne håndtere uventede hendelser. Man må sette pris på de avvik som man finner, differensiering av kategorier og årvåkenhet til endringer i tilstanden, samt ha kontinuerlige samtaler som er helt nødvendig for å håndtere risiko som ikke kan forventes ut i fra systemet. En annen trussel er når rutiner blir ”mindless”. Man må skille mellom handling som blir gjort av rutine og ”mindless” handling som blir gjort automatisk. ”If you assume that routine refers to an automatic activity, as in the phrase ”It’s a routine job”, you run the risk that people will forget to ask the question ”what if...?”” (Weick & Sutcliffe, 2007, s. 61). Ofte kan slike spørsmål anses som bortkastet tid. Ved å være mer ”mindful” tilpasses rutineene etter behov og oppdaterer rutineene etter hver som man oppnår ny kunnskap. En siste trussel mot operasjonell sensitivitet er knyttet til hvordan organisasjoner oppfatter nesten-ulykker. Høypålitelige organisasjoner bør betrakte nesten-ulykker som et tegn på potensiell fare, og ikke tenke at deres praksis er tilstrekkelig trygg. Selv om organisasjonen evnet å avverge en ulykke betyr ikke det at de klarer å avverge fremtidige hendelser (Weick & Sutcliffe, 2007).

4. Forpliktelse til resiliens

Verken mennesker eller systemer er feilfri og det er ikke til å unngå at det skjer uønskede hendelser. Dette krever at man i tillegg til å forebygge må fokusere på å håndtering. Resiliens handler om å være proaktiv fremfor reaktiv og at man evner å håndtere hendelser som har inntruffet før de får utfoldet seg. Organisasjoner er resiliente dersom de har kapasitet til å håndtere uventede hendelser og samtidig vedlikeholde driften. (Weick & Sutcliffe, 2007; Weick, Sutcliffe & Obstfeld, 1999; Woods & Hollnagel, 2012;). I følge Woods (2012) handler resiliens om mer enn kun å tilpasse seg, men også en organisasjons kapasitet til å håndtere uventede hendelser utover det som kommer frem i systembeskrivelsen og det som forventes av dem. Sentralt her er organisasjoners fleksibilitet, respons til uventede hendelser, samt god kommunikasjon og tilstrekkelig mobilitet av ressurser ved behov. Resiliens handler også om organisasjoners evne til å

avverge uønskede hendelser ved å forutse trusler. Dette kommer særlig til syne når det gjelder å balansere sikkerhet og produksjon (Hale & Heijer, 2012).

Weick & Sutcliffe (2007, s. 71) trekker frem tre sentrale evner som skal være tilstede i en resilient organisasjonen. For det første må de tåle belastninger og opprettholde organisasjonens funksjon i motgangstider, for det andre skal de gjenopprette seg etter uønskede hendelser og i stedet for å kollapse blir organisasjonens bedre rustet til å motstå uventede hendelser. Og for det tredje må de ta lærdom fra deres aktivitet.

Når en organisasjon skal gjenopprettes etter en hendelse kan de enten returnere til samme posisjon som før hendelsen, til en tilnærmet lik posisjon eller inntar en ny posisjon. Ved bytte av posisjon må organisasjonen finne ut om deres evne til å være fleksibel og resilient har økt, redusert eller er lik. Når en hendelse inntreffer vil organisasjonen sin respons ofte være preget av nye regler som er utviklet for å forhindre at den samme hendelsen skal skje igjen, og dette er et tegn på redusert fleksibilitet. Dette er imidlertid ikke til å unngå. Høypålitelige organisasjoner lærer underveis og bruker denne kunnskapen til å håndtere hendelser, noe som er med på å bevare fleksibiliteten. Som regel returnerer organisasjoner til en tilnærmet lik posisjon etter en hendelse. En resilient organisasjon vil forbedre responsevnen sin (Weick & Sutcliffe, 2007).

Høypålitelige organisasjoner som har kontinuerlig fokus på tilgjengelige ressurser for håndtering av hendelser fordi de antar at de kommer til å bli overrasket, kan sies å være resilient. Dette innebærer blant annet at de tilegner seg ny kunnskap, fokuserer på læring, har god kommunikasjon og kan improvisere ved behov. De er klar over at det kan dukke opp feil som de ikke har opplevd før og at de må være på vakt. For organisasjoner kan det være utfordrende å være resilient da man må ha kontinuerlig læring, men man vet ikke hva man skal lære og hvordan det skal tas i bruk. Man må forsøke å tilpasse seg uventede hendelser uten å redusere organisasjonens tilpasningsevne, noe resiliens skal forhindre (Weick & Sutcliffe, 2007).

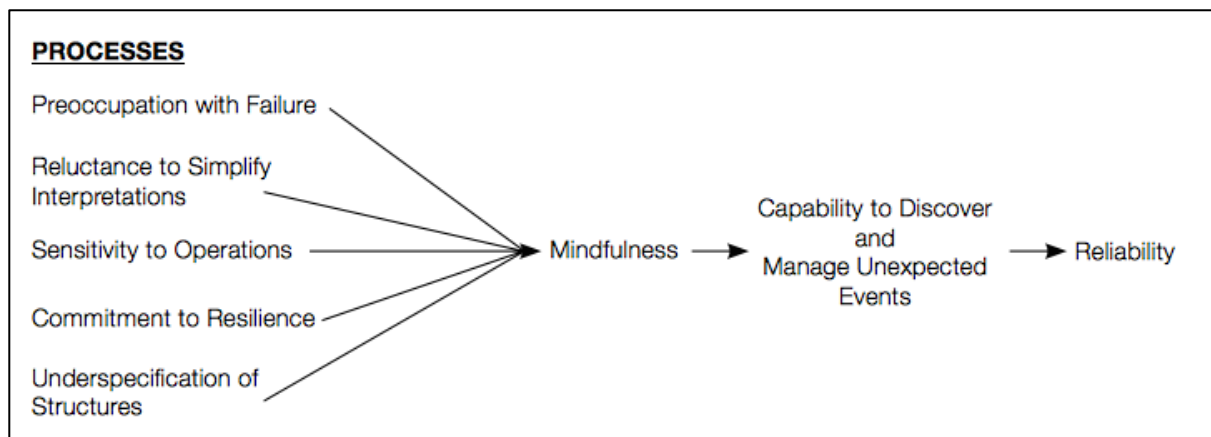
5. Underspesifisert struktur – respekt for kompetanse

Et kjennetegn ved høypålitelige organisasjoner er at de er desentralisert, gjerne til tross for at de har hierarkisk system. Typisk for organisasjoner med hierarki er at mye informasjon ikke når frem til det øverste sjiktet, ofte er det kun det positive som blir

mottatt og ledelsen er da i god tro om at alt er i orden og under kontroll. Et slikt informasjonsfilter kan være med på å motarbeide håndtering av uventede hendelser. Det er som regel noen som oppfatter signaler om fremvekst av en hendelse, men som regel er det da noen som er i den butte enden. Gjerne er de ikke klar over hva de har sett og ser ikke alvoret i det, eller kanskje de ikke tør å rapportere det. Dette er tendenser som høypålitelige organisasjoner klarer å unngå. Ens hierarkiske plassering trenger ikke nødvendigvis å samsvare med ens ekspertise og kompetanse. I beredskapssituasjoner blir organisasjonsmedlemmene anerkjent for sin kompetanse uavhengig av deres plassering i den hierarkiske strukturen (Weick & Sutcliffe, 2007; Weick, Sutcliffe & Obstfeld, 1999).

3.4.3 Kognitive prosesser

Knyttet til mindfulness og de fem prinsippene om forventninger og begrensninger er kognitive prosesser sentralt; ”What seems to happen in HROs is that there is variation in activity, but there is stability in the cognitive processes that make sense of this activity” (Weick, Sutcliffe & Obstfeld, 1999, s. 35). Dette illustreres i figur 6.



Figur 6: Kognitiv prosess (Weick, Sutcliffe & Obstfeld, 1999, s. 37)

Uventede hendelser forekomme i tre ulike former; når forventede hendelser ikke skjer, når en uventet hendelse skjer og når utilsiktede/utenkelige hendelser skjer. Felles for disse tre tilfellene er at de kan relateres til forventninger, i den forstand at man søker etter bekreftelse på forventningen fremfor å avkrefte dem (Weick & Sutcliffe, 2007, s. 29). En høypålitelig tilnærming oppmuntrer til å ha en kreativ fantasi da det vil kunne utvide kunnskapen deres om ukjente hendelser. Et sentralt mål innenfor høypålitelige organisasjoner er å øke forståelse for

den tredje formen av uventede hendelser. Dette oppnås ved å stadig undersøke de forventningene som er tilstede, kontinuerlig gjennomgang av forventninger sett opp mot nye erfaringer, være villig til å sette nye forventninger og kartlegging av nye dimensjoner. Å oppnå ny kunnskap er svært sentralt (Weick & Sutcliffe, 2007).

Kjente hendelser er hendelser som har inntruffet tidligere. Man har opparbeidet seg erfaringer og gjerne identifisert begreper og kategorier i henhold til hendelser, noe som gjør det enklere å forklare dersom det skulle inntreffe igjen. At slike begreper og kategorier er lett tilgjengelig ved rapportering av en hendelse kan ha en begrensende effekt på individer. Derimot kan man ved å øke bevisstheten, altså å være ”mindfulness”, ved å se forbi det kjente og heller avdekke det ukjente (Weick & Sutcliffe, 2007).

3.5 High Reliability Management

I studiet av CAISO fant Roe og Schulman (2008) at organisasjonen klarte å opprettholde en høypålitelig strømlevering til tross for at de opplevde en kraftkrise. Presidenten i North American Electric Reliability Council, Michael Gent, beskrev det nord-amerikanske kraftnettet som “a very complex system. It’s probably the most complex system ever invented by man, more complicated than a moon shot” (Perrow, 1999, S. 404). Komplekse systemer krever god forståelse av systemet, og i denne sammenhengen ble ”High Reliability Management” (HRM) introdusert som en alternativ tilnærming. HRM handler om hvordan man oppnår og vedlikeholder strategisk balanse mellom effektivitet og pålitelighet, mellom det å lære av prøving og feiling og å forebygge risikofylte feil, og mellom å maksimere ens forventninger til støt og å maksimere ens resiliens for å gjenopprette (Roe & Schulman, 2008, s. 5). Ut i fra denne tilnærmingen vil pålitelighet ha en annen betydning enn i den tradisjonelle HRO-tilnærming (Roe & Schulman, 2016, s. 12)

For å se et tydeligere skille mellom HRM og HRO kan Diablo Canyon, et kjernekraftverk som produserer strøm, brukes som moteksempel til CAISO. Begge virksomhetene har en høypålitelighet levering av sine tjenester, samt de er tett koblet og har kompleks interaksjoner. Et særtrekk ved HRM er graden av høypålitelig sanntidsstyring hvor det er høy systemvolatilitet, dette skiller seg fra tidligere HRO studier som har knyttet høypålitelig styring til forventninger og handlinger i ”just-in-case”- og ”just-this-way”-modusene. Handlinger som utføres i handlingsmodusene ”just-in-time” og ”just-for- now” er imidlertid sentralt for å opprettholde en pålitelig strømlevering. Høypålitelighet oppnås ved å manøvrere nettet på tvers

av handlingsmodusene. Når operatører skal utføre handlinger i sanntid trer ofte svakheter ved systemer og teknologier frem, en høypålitelig styring skal bidra til å redusere risiko og farer som oppstår av disse svakhetene (Roe & Schulman, 2016, s. 53). Høy pålitelighet i sanntid er viktig og CAISO kontrollrommet opplever en annen pålitelighetsstyring enn det tidligere HRO forskning har vist. Et annet sentralt skille er knyttet til læring av feil og redundans. Å handle i sanntid krever improvisasjon og eksperimentering, i motsetning til en HRO tilnærming hvor det blir unngått. Hos CAISO viste det seg at tett koblede og komplekse interaksjonene faktisk bidro til en høypålitelig drift, da det innebærer mange variabler som operatørene kunne bruke når de måtte improvisere løsninger i sanntid (Roe & Schulman, 2008, s. 63). I figur 7 blir særtrekk ved HRM og HRO beskrevet:

High Reliability Organizations Diablo Canyon	High Reliability Management CAISO
<ul style="list-style-type: none"> • High technical competence • Constant search for improvement • Hazard-driven adaptation to ensure safety • Often highly complex activities • Reliability is nonfungible • Limitations on trial-and-error learning • Operation within anticipatory analysis • Flexible authority patterns within HRO • Positive, design based redundancy to ensure stability of inputs and outputs • Low input, process, and output variance 	<ul style="list-style-type: none"> • High technical competence • Constant short-term search for improvement • Often hazard-driven adaptation to ensure safety • Often highly focused complex activities • Reliability is nonfungible in real time, except when service reliability jeopardizes grid reliability • Real-time operations necessitating improvisation and experimentation • Operations outside analysis • Flexible authority patterns within focal organization and across HRM • Maximum equifinality (positive redundancy), adaptive equifinality (not necessarily designed), and zero equifinality, all depending on network performance conditions • High input and low output variance requires high process variance

Figur 7: HRO vs. HRM (Roe & Schulman, 2008, s. 61)

”An engineer once told us that the control room operators he was meant to support were ”Neanderthals”, the prevailing view being that operators are the past, not the future” (Roe & Schulman, 2008, s. 33). Dette utsagnet viser til en oppfatning om at innovasjon, design og teknologi sikrer at kritiske infrastrukturer har en høypålitelig levering av tjenester. Roe og Schulman (2008; 2016) hevder derimot at operatører er en forutsetning for høypålitelig styring av kritisk infrastruktur. Dette er en noe forsømt, men viktig, gruppe av fagfolk som er forpliktet og dedikert til å utgjøre en forskjell mellom katastrofale feil av tjenester som vi er avhengig av og rutinemessige funksjoner som det forventes er til stede. Under studiet av CAISO kom det tydelig frem at operatørens ferdigheter og kapasitet knyttet til håndtering av hendelser i sanntid, utgjorde høy pålitelighet.

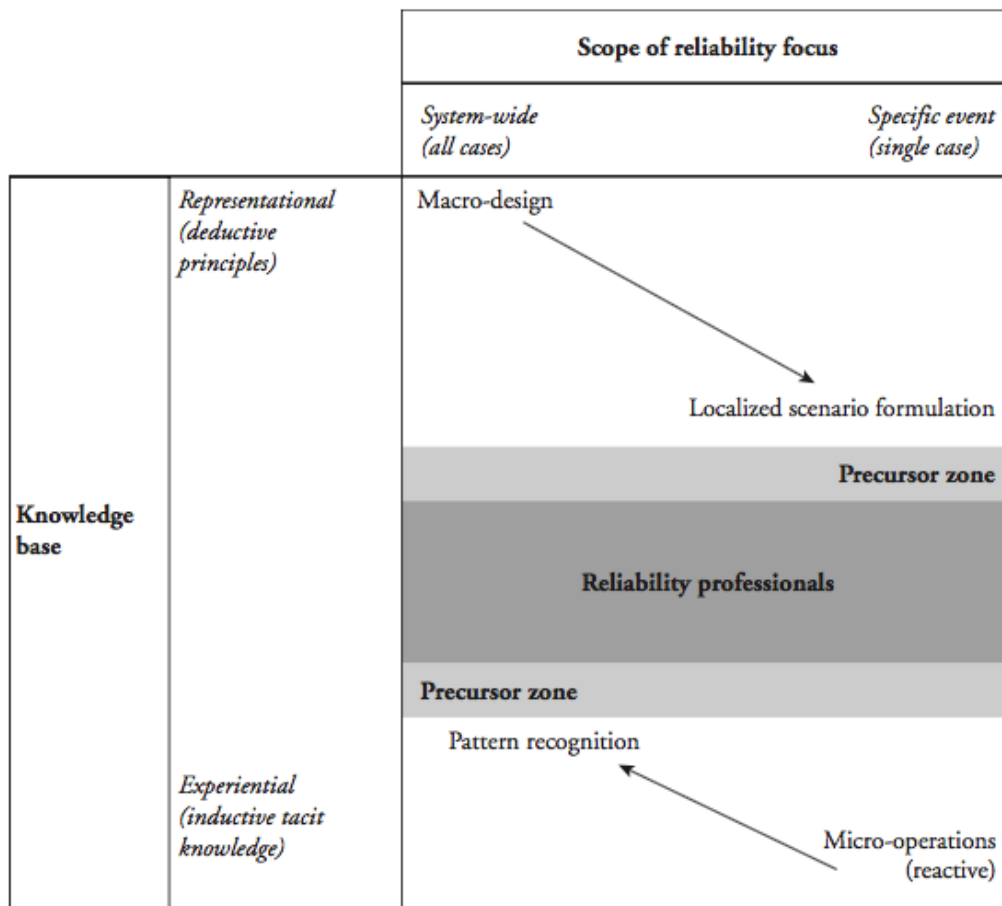
Krav om høy pålitelighet innen kraftsektoren reguleres av lovverk, offentlig og politisk etterspørsel og organisatoriske formål. Det er operatørene som sørger for at disse kravene etterleves. Man kan imidlertid ikke se bort i fra at operatører kan begå feil, men på en annen side så er det de som overvåker de tekniske systemene og oppdager eventuelle feil – feil som uansett ville utviklet seg hadde det ikke vært for at operatørene var der for å håndtere det. I tillegg til operatører av kontrollrom er ledere, teknikere og annet støttepersonell sentralt for en høypålitelig styring av kritisk infrastruktur – og det er denne gruppen fagfolk som utgjør ”Reliability Professionals”. Når Roe og Schulman bruker ordet ”professionals”, profesjonelle direkte oversatt til norsk, er det ikke akademisk kunnskap og høyere utdanning de sikter til, men heller kognitive ferdigheter og opparbeidet erfaringer; ”(...) recognition of their overriding commitment to the real-time reliability of their systems, and the unique set of skills they bring to their tasks (Schulman et al., 2004, s. 24). Operatører lærer stadig da de er omgitt av en dynamisk omgivelse, og etter som forholdene endrer seg må parametere som påvirker handlingene deres tilpasses nye betingelser.

A senior manager in the CAISO operations engineering unit, responsible for a large body of procedures, told us “part of the (control room) experience is to know when not to follow procedures... there are bad days when a procedure don’t cover it, and then you have to use your wits” (Roe & Schulman, 2008, s. 60).

Reliability professionals evne til å tilpasse seg omstendighetene og handle i sanntid er sentralt, men de skal også evne å tenke fremover. Det vil si at de må være klar over hvilke utfall beslutninger kan medføre. Når operatører må håndtere hendelser som ikke er kjent for dem kan

de oppdage og utvikle nye løsninger etter behov, innenfor de forutsetningene som er tilstede. En slik form for risikovurdering er også en sentral karakteristikk ved HRM (Roe & Schulman, 2008, s. 124).

Man finner alltid et nettverk av reliability professionals innen kritisk infrastruktur da en høypålitelig styring av infrastrukturer er komplekst. Et hvert individ har kognitive og rasjonelle begrensning, og det er derfor nødvendig at flere reliability professionals kan samvirke slik at disse begrensningene kan kompenseres for. Dette krever at disse personene har en god situasjonsforståelse. Søken etter pålitelighet innen kritisk infrastruktur kan ses ut i fra to kognitive dimensjoner; kunnskap som benyttes for å oppnå pålitelighet og fokus på oppmerksomhet eller omfang av innsats for å oppnå pålitelighet.



Figur 8: Kognitive dimensjoner (Roe & Schulman, 2016, s. 44)

Kunnskapsbasen strekker seg mellom formell kunnskap, hvor aktivitet forstås ut i fra abstrakte prinsipper og deduktive modeller basert på disse prinsippene, til eksperimentell kunnskap som er basert på mønstergjenkjenning eller erfaringskompetanse. Omfanget av oppmerksomhet varierer mellom å betrakte pålitelighet som en strøm av forutsigbare systemutganger som omfatter mange variabler og elementer, og å betrakte hver enkelt hendelse som distinktiv. Ut i fra de to dimensjonene dannes det to ytterpunkter for pålitelighet; makro-design og mikro-operasjoner. Den ene tilnærmingen forstår kritiske prosesser ut i fra formelle deduktive prinsipper. Det blir gjennomført analyser av systemet i helhet og det skal ikke utføres handlinger utover systemanalysen, og i så måte blir systemet brukt som et verktøy for å kontrollere atferd. I den andre tilnærmingen er det kontinuerlig reaktiv atferd, også i møte med overraskelser i sanntid på mikronivå. Her knyttes påliteligheten til operatørens reaksjonsevne, fremfor forventninger som fremkommer av systemdesign. Ingen av disse tilnærmingene vil alene gi høy pålitelighet, og reliability professionals innen kritisk infrastruktur må evne kombinere disse (Roe & Schulman, 2016, s. 46). Havner reliability profesisonals utenfor det kognitive området som er mellom de to dimensjonene, beveger de seg ut i ”precursor zone”, som indikerer kognitiv begrensning knyttet til ferdighet og kapasitet. Når denne grensen er nådd vil håndtering av hendelser være utenfor deres evne.

3.6 Oppsummering av teori

Alle KBO-enheter må forholde seg Beredskapsforskriften, hvor det fremkommer at de skal kunne håndtere ekstraordinære hendelser og situasjoner. Dette forutsetter at virksomheter har et kontinuerlig beredskapsarbeid. Beredskapsplanlegging og forebyggende aktiviteter gjør virksomheter bedre rustet i møte med uønskede hendelser.

Når det gjelder ulykker i høyrisikoteknologier har det blitt sett på to ulike tilnærminger. Teoriene om Normal Accidents og High Reliability Organizations kan ses som motpoler. Kraftforsyning blir stadig mer komplekst, dermed blir de også mer sårbar. Ut i fra NAT vil organisasjoner med tett koblede og komplekse interaksjoner oppleve systemulykke på et eller annet tidspunkt. Til tross for sikkerhetstiltak er det ikke til å unngå at systemulykker forekommer (Perrow, 1999). Denne pessimistiske tilnærmingen av styring av sikkerhetsstyring skiller seg fra HRO, som er en mer positiv tilnærming. Høypålitelige organisasjoner kjennetegnes ved at de har fokus på sikkerhet og pålitelighet, at teknisk og organisatorisk redundans er tilstede i organisasjonen, at de er fleksibel og at de kan lære fra tidligere hendelser.

Høypålitelige organisasjoner som er ”mindful” har en god forståelse for uønskede hendelser som oppstår (Weick & Sutcliffe, 2007).

I forbindelse med en studie gjennomført av Roe & Schulman ble ”High Reliability Management” og ”Reliability Professionals” introdusert. HRM kan ses som en alternativ tilnærming til NAT og HRO. Innenfor denne tilnærming er det særlig fokus på reliability professionals, som betraktes som et avgjørende nettverk av fagfolk for høypålitelig styring.

4 METODE

For at innsamlet data kan brukes til å svare på problemstillingen for oppgaven og gi gyldige og pålitelige resultater krever det en systematisk fremgangsmetode (Halvorsen, 2008; Jacobsen, 2015). I dette kapittelet vil jeg dermed gå nærmere inne på hvilke metoder som blir brukt for å samle inn data, samt begrunne valgene som har blitt tatt.

4.1 Forskningsdesign

I følge Blaikie (2010) er et forskningsdesign et teknisk dokument som utvikles av en eller flere forskere. Dette dokumentet blir brukt som en veiledning for hvordan forskningsprosjektet skal utføres og skal svare på tre fundamentale spørsmål; hva skal studeres, hvorfor skal det studeres og hvordan skal det bli studert (Blaikie, 2010). Et forskningsdesign skal altså gjøre rede for de beslutninger som skal tas i løpet av forskningsprosessen, samt begrunne, legitimere og evaluere valgene. Det må også forsikres at disse beslutningene samsvarer med hverandre. Et forskningsdesign er en syklisk sekvens av beslutninger, det vil si at beslutninger som tas vil påvirke andre beslutninger. Dersom man har mulighet bør man i den grad det er mulig, ta beslutninger knyttet til forskningsdesignet før man starter med forskningen. Imidlertid må det sies at dette ikke vil la seg gjøre i forskningsprosjekter, og det kan være en utfordring å forutse alle aspektene ved forskningen (Blaikie 2010). Det har blitt gjort flere endringer i perioden fra utviklingen av første prosjektskisse og frem til nå – slutten av forskningsprosessen. Blant annet har problemstillingen og forskningsspørsmålene blitt justert på underveis. I følge Jacobsen (2015) er det vanlig at problemstillingen utvikles og endres i takt med arbeidet. Til tross for endringer gjennom forskningsprosessen har forskningsdesignet vist seg å være svært nyttig da det har fungert som en god veileder.

Undersøkelsens formål er avgjørende for utformingen av forskningsdesignet. Ettersom formålet er å undersøke nettselskapers forutsetninger for høypålitelig kraftlevering, med fokus på ett nettselskap sin drift av kraftnett, har forskningsdesignet blitt utformet som casestudie. Casestudier kjennetegnes ved intensiv undersøkelse av en eller få enheter (Thagaard, 2013).

4.2 Forskningsstrategi

Når man starter forskningsprosessen vil man kunne velge mellom fire forskningsstrategier; induktiv, deduktiv, retroduktiv og abduktiv. I denne oppgaven er det valgt å ta i bruk en abduktiv forskningsstrategi, som har som formål å vise at noe ikke må være på en bestemt måte,

men heller at det kan være slik. Selv om et fenomen ses i lys av en teori, betyr det ikke nødvendigvis at denne teoretiske rammen er den eneste rette og man kan ikke utelukke at det er en av flere mulige tilnærminger. De slutningene som blir trukket er ikke definitive sannheter. Dette kan man se ut i fra det som refereres til som rekontekstualisering, som går ut på at forskeren observerer, beskriver, tolker og forklarer et fenomen sett i ny sammenheng – nye beskrivelser av et fenomen dyrkes da frem, og disse kan betraktes som rimelige (Danermark m.fl., 2002).

4.3 Forskningsmetode

Ut i fra hva slags type data man ønsker å samle inn tar man i bruk kvalitativ eller kvantitativ metode, eller en kombinasjon (Halvorsen, 2008). Da det ble gjennomført intensive undersøkelser av et begrenset antall enheter har oppgaven en kvalitativ tilnærming. En sentral karakteristikk ved kvalitativ forskning er fleksibilitet (Thagaard, 2013, s. 54). Dette har vært til fordel da det har tillatt meg å foreta endringer i forskningsdesignet under hele forskningsprosessen.

4.4 Datainnsamling

I denne oppgaven vil det bli hentet inn både primær- sekundær- og tertiærdata. Primærdata vil bli samlet ved hjelp av intervjuer. En form for dette er det som Blaikie (2010) refererer til som muntlige historier. Dette er særlig relevant med tanke på de ansatte i bedriften sine opplevelser og erfaringer knyttet til sikkerhet og beredskap. Sekundær- og tertiærdataen som blir benyttet i denne oppgaven er dokumenter. I tillegg til intervjuer og dokumentanalyse ble det gjort observasjoner. Formålet med å ta i bruk flere metoder er at det vil være komplementerende, i den forstand at de kan etablere en bedre forståelse i forhold til hverandre. Innenfor casestudier er det vanlig å kombinere datainnsamlingsmetoder (Thagaard, 2013).

4.4.1 Intervju

For å få et innblikk i menneskers tanker, holdninger og opplevelser blir intervjuet stadig brukt som kvalitativ tilnærming da det har vist seg å være en effektiv metode. Denne metoden er særlig fruktbar ved tilfeller hvor man ønsker å få mer kunnskap om individers erfaring innenfor en viss kontekst. Kvalitative intervjuer kan ha ulike grader av åpenhet, og beveger seg mellom å være strukturert eller relativt ustrukturert. Da et forskningsintervju gjennomføres på bakgrunn av et visst tema vil et intervju aldri være helt ustrukturert (Jacobsen 2015; Tanggard &

Brinkmann, 2010). Intervjuene som har blitt gjennomført i forbindelse med denne oppgaven har hatt en semistrukturert form.

Semistrukturert intervju krever systematisk planlegging og fremgang. Man bør klargjøre hva man ønsker å finne ut av før man finner ut av hvordan nødvendig kunnskap skal innhentes (Tanggaard & Brinkmann, 2012). Det ble i utgangspunktet utarbeidet flere intervjuguider, men på grunn av endringer knyttet til fokuset for studiet var det kun én av disse som var hensiktsmessig å bruke – denne er vedlagt i oppgaven. Spørsmålene i intervjuguiden er formulert slik at de fremstår som mer virkelighetsnære for informantene enn hva forskningsspørsmål ville vært, da de er abstrakte og søker forklaringer – intervju spørsmål har som formål å få konkrete beskrivelser (Tanggaard & Brinkmann, 2012). Fordelen ved å ta utgangspunkt i en intervjuguide er at man som intervjuer er fleksibel. Man kan omformulere spørsmål og endre på guiden etter hvert om man ser behov for det. En ulempe med akkurat det er at man gjerne ikke får stilt de samme spørsmålene til alle informantene, men på en annen side så kan det også være med på å belyse problemstillingen fra ulike synsvinkler (Halvorsen, 2008). Under intervjuene opplevde jeg at det var god flyt i samtalene, noe som medførte at det var unaturlig å gå gjennom spørsmålene i intervjuguiden punktlig. Til tross for at ikke alle informantene ble spurt nøyaktig samme spørsmål ble alle temaene i intervjuguiden dekket, og det var ikke noe problem å få tilstrekkelig med informasjon. Jeg opplevde også at informantene fikk snakke relativt fritt, noe som bidro til å berike datainnsamlingen ved at de tok opp nye emner som viste seg å være relevant.

4.4.1.1 Valg av informanter

Hvis utvalget som skal trekkes er lite og man samtidig ønsker høyest mulig kvalitativt innhold i informasjonen vil strategisk utvalg av informanter være hensiktsmessig. Jeg kontaktet et selskap som jeg anså som interessant og ikke minst relevant for det jeg ønsker å undersøke – dette går overens med hvordan Brandt mener utvelgning bør skje (Brandt, i Halvorsen, 2008, s. 164). Jeg ble satt i kontakt med virksomhetens beredskapskoordinator, og det ble videre avtalt og møtes for en samtale. Dette var i oktober 2016. Formålet med samtalen var å bli bedre kjent med bedriften og deres rutiner og prosedyrer i henhold til beredskap. Etter som jeg fikk kartlagt bedriften og videreutviklet problemstillingen for oppgaven, tok jeg på nytt kontakt med beredskapskoordinator og ble så henvist til en annen person i virksomheten som ble ansett å være relevant for gitt tema. Denne personen er seksjonssjef for nettsentralen og kunne bistå med å komme i kontakt med relevante personer, i tillegg til at vedkommende var en god kilde

i seg selv. Dette er det som Halvorsen (2008) kaller for snøballutvalgsmetode, som går ut på at en informant oppgir andre relevante personer som man kan snakke med, og slik fortsetter det. Ved bruk av en slik metode må man passe på at utvalget ikke blir for snevert sammensatt. Under noen av intervjuene hendte det informanten ikke kunne svare utfyllende på spørsmål og i den anledning anbefalte meg å snakke med gitte personer som hadde relevant kunnskap. Selv om informantene jobber i samme seksjon har de ulike stillinger og dermed ulik bakgrunn og kompetanse. Jeg opplevde at utvalget er variert og representerer forskjellige erfaringer og oppfatninger. Det er også noe variasjon i kjønn og alder, imidlertid skal det sies at jeg ikke oppfattet dette som særlige relevante faktorer. Det totale utvalget av informanter kan ses i tabellen nedenfor.

Stilling	Kjønn	Aldersgruppe
Beredskapskoordinator	Mann	50-60
El-maskinist	Mann	30-40
El-maskinist	Mann	40-50
Driftsingeniør	Mann	60-70
Seksjonssjef	Kvinne	40-50
Spesialrådgiver	Kvinne	40-50
Spesialrådgiver	Mann	40-50
Systemansvarlig	Mann	40-50

Figur 9: Oversikt over informanter

Det er ikke et fasitsvar på hvor mange informanter man bør intervju. Som Kvale og Brinkmann (2015, s. 148) sier: ”Intervju så mange personer som det trengs for å finne ut av det du trenger å vite”. Altså, det vil variere ut i fra forskningsprosjektets formål. Som forsker bør man være obs på at det ikke er for få informanter da det gjør det vanskelig å generalisere og det er ikke mulig å teste hypoteser om forskjellene mellom grupper. Og hvis det er for mange informanter vil man gjerne ikke ha tilstrekkelig med tid til dyptgående analyse av intervjuene (Kvale & Brinkmann, 2015).

Det ble gjennomført totalt syv intervjuer, i tillegg til en kartleggingssamtale med beredskapskoordinator. Felles for syv av informantene er at de jobber i samme seksjon, derimot

har de ulike stillinger og arbeidsoppgaver. Jeg anså det som hensiktsmessig å intervjuer både de operatørene på nettsentralen og de som jobber ute i nettseksjonen for å studere dynamikken og avhengighet mellom de ulike rollene.

Av de syv intervjuene var det ingen som var avtalt på forhånd, det var først når jeg møtte opp der at det ble avtalt nærmere. Det var noe vanskelig å lage faste avtaler da deres arbeidsdag kan være uforutsigbare med tanke på at det plutselig kan oppstå uønskede hendelser, i tillegg til at det var både ferieavvikling og sykdom i løpet av perioden jeg var der.

4.4.1.2 Gjennomføring av intervjuer

I forkant av intervjuene ble informantene informert om oppgavens formål, samt hvilke tema jeg ønsket å ta opp under intervjuene. Dette gir en pekepinn på at oppgaven fokuserer mer på det organisatoriske enn det tekniske knyttet til pålitelig kraftlevering. I forkant av intervjuene var det nødvendig å sette seg inn hvordan kraftsystemet fungerer samt gjøre seg kjent med tekniske begreper for å oppnå bedre forståelse under intervjuene. Det skal sies at informantene tok hensyn til at jeg ikke har teknisk bakgrunn og de var flink til å forklare underveis.

Alle intervjuene ble gjennomført ansikt til ansikt i lokalet til bedriften, og de var fordelt ut over flere dager. Varigheten på intervjuene varierte mellom 60 til 90 minutter. Før vi startet intervjuet ble informantene spurt om det var greit at det ble benyttet diktafon under intervjuene, noe alle utenom én samtykket til. Det ble forklart at lydopptakene kun ville bli hørt av meg og at de ville bli slettet så snart opptakene var transkribert. Da jeg skriver masteroppgave alene var diktafonen er svært nyttig verktøy da det lot meg fokusere på informanten og vår samtale, fremfor å bli distraheret ved ta notater i tillegg – og ikke minst ble sjansen for å gå glipp av viktig informasjon minimert.

4.4.2 Observasjon

I tillegg til å utføre intervjuer har noen av informantene, nærmere sagt de som sitter på nettsentralen, blitt observert. Det må imidlertid presiseres at dataen som samles inn via intervjuer og dokumentanalyse er det som utgjør hoveddelen av innsamlet data, hvor observasjonen er supplerende. I følge Thagaard (2013, s. 58) er denne metoden "(...) særlig godt egnet til å gi informasjon om praksis i dagliglivet, om hvordan personer forholder seg til hverandre og hvordan de presenterer seg i sine omgivelser". Under intervju har informantene

fått mulighet til å fortelle om deres arbeidssituasjon – gjøremål, aktiviteter, prosedyrer osv. – mens ved observasjon fikk jeg se deres faktiske handlinger i en naturlig sammenheng. Det er imidlertid ikke alltid slik at handlinger er selvforklarende og det krever at man danner seg en mening om hva man har sett. Det ble gjennomført en ikke-deltakende feltobservasjon med ustrukturert form. Det var en direkte observasjon da de observerte var klar over at jeg var på nettsentralen for å observere dem, og gjør det viktig å ta i betraktning om de observerte oppfører seg annerledes fordi de vet de blir fulgt med på (Halvorsen, 2008). Det ble gitt informasjon om at jeg ville oppholde meg inne på nettsentralen for å observere dem. Dette kan også knyttes til det etiske aspektet ved observasjoner da det er en utbredt oppfatning om at skjult observasjon er uetisk (Thagaard, 2013, s. 80). Det ble ikke planlagt i forkant når observasjonen skulle finne sted og det ble ikke registrert nøyaktig tidspunkt for når observasjonen startet og sluttet, noe som kan betraktes som en ulempe. Under og etter observasjoner kan feltnotater, lydopptak eller videoopptak være nyttig for å bearbeide erfaringer, samt et fungere som et godt verktøy videre i analysen av dataen (Thagaard, 2013). Det ble valgt å ta notater i etterkant av observasjonene. Av sikkerhetsmessige årsaker var det ikke lov til å filme eller å ta bilder inne på kontrollrommet.

4.4.3 Dokumentanalyse

Innenfor samfunnsvitenskapelig forskning er dokumentanalyse en av de mest brukte metodene for innsamling av data, og kan brukes innen ulike undersøkelsesområder (Lynggard, 2012, s. 153). Dokumentanalyse kan være studie av alt fra dagbøker til mer offentlige dokumenter som stortingsmeldinger. I følge Scott kan alle skriftlige kilder betegnes som dokumenter (sitert i Thagaard, 2013, s. 59). Man må imidlertid være oppmerksom på hvilken kontekst dataen har blitt utformet i og om det er et troverdig dokument. Temaet for denne undersøkelse er høypålitelig kraftlevering, og det vil være hensiktsmessig å benytte seg av dokumentanalyse for å orientere seg i faglitteraturen knyttet til dette temaet (Thagaard, 2013).

I dette studiet har offentlige dokumenter vært viktig for å danne et kunnskapsgrunnlag rundt norsk kraftforsyning. Dette har hjulpet meg å danne en bedre forståelse for blant annet hvordan det norske kraftsystemet er bygd opp – både fysisk og organisatorisk, hvorfor kraftinfrastrukturen er kritisk, samt hvilke ytre faktorer som påvirker dem. Særlig dokumenter fra sentrale aktører som DSB og NVE, eller offentlige dokumenter som Norges offentlige utredning (NOU), melding til Stortinget (meld. St.) og forskrifter har vært relevant. Flere av dokumentene som er brukt har i likhet med valg av informanter til intervju, blitt funnet frem til

ved hjelp av snøballmetode. Dette innebærer at man finner dokumenter ved å se gjennom dokumenters referanseliste (Lynggaard, 2012, s. 158).

En utfordring med dokumentanalyse kan blant annet knyttes opp mot dokumenters tilgjengelighet. Da kraftlevering går under kritisk infrastruktur medfører det sensitiv informasjon. Nettselskapets private dokumenter er derfor ikke inkludert i empirien.

4.5 Datareduksjon og analyse

Uavhengig om man har brukt en kvalitativ eller kvantitativ metode for datainnsamling, må dataen som er innhentet som regel reduseres og komprimeres før det kan analyseres. Dataanalyser har som formål å skape oversikt i datamaterialet som er samlet inn, og ved kvalitative metoder gjennomføres det systematisk sortering (Grennes, 2012). Ryen hevder at det ikke finnes standardiserte teknikker for analyse av kvalitative data, noe han begrunner med at informasjon er ustrukturert og av ulike former (Ryen, sitert i Halvorsen, 2008, s. 2010). Dette sier Grennes (2012) seg enig i, men argumenterer så for at det likevel ikke er fritt frem – kvalitativ analyse handler like mye om kvaliteten til forskeren som dataen som analyseres, og dette kan knyttes opp mot reliabilitet. Det kan være utfordrende å analysere kvalitative data, og det krever i mange tilfeller at man veksler mellom å se på helheten og delene av datamaterialet (Dalland, 2000). I etterkant av intervjuene ble lydopptakene transkribert, og deretter kategorisert ut i fra temaene i intervjuguiden. I tillegg ble relevante og gode utsagn markert. Dette fant jeg svært nyttig da jeg fikk en god oversikt over innsamlet data og gjorde det lettere å utforme empirikapittelet. All data har blitt hentet inn og analysert av meg, dette kan betraktes som en fordel da det gir et godt grunnlag for en helhetsbeskrivelse av det observerte (Halvorsen, 2008, s. 210).

4.6 Validitet og reliabilitet

Det er viktig at det empiriske grunnlaget i en undersøkelse er valid og reliabel (Jacobsen, 2015). Validitet, altså gyldighet og relevans knyttet til innsamlet data, handler om å se sammenheng mellom virkeligheten som har blitt forsket på og de resultatene som har kommet frem. Man må da stille seg selv spørsmålet om dataene faktisk svarer på forskningsspørsmålene. Dette er særlig viktig når formålet med forskningen er mer enn å bare beskrive, men også forklare og vise forståelse. Analysen representerer fortolkninger av det fenomenet som har blitt studert

(Jacobsen, 2015; Thagaard, 2013). En perfekt forskningsprosess er umulig å oppnå, men evner man å se egne svakheter kan det styrke oppgavens pålitelighet og troverdighet (Jacobsen, 2015).

Det skilles mellom to typer gyldighet og relevans; intern validitet og ekstern validitet. Begge prinsippene handler om at man som forsker bør redegjøre og argumentere for de handlingene som har ledet til resultater, samt at ved å ha kritisk blick til egen analyse vil det kunne styrke validiteten (Thagaard, 2013). Intern validitet viser til årsakssammenhenger innen for en bestemt studie, om det er god nok dekning for å trekke konklusjoner. I denne oppgaven har det blitt tatt i bruk tre ulike metoder for datainnsamling; intervju, observasjon og dokumentstudier, noe som kan styrke den interne validiteten. En utfordring ved å gjennomføre forskningsprosessen på egen hånd er at oppgaven består av kun mine tolkninger. Dette er imidlertid noe jeg har vært bevisst på og tatt hensyn til under intervjuene. Blant annet for å unngå at informantens utsagn ville bli mistolket krevde det at jeg formulerte spørsmålene slik at de ble oppfattet riktig, samt at jeg kunne forklare hva jeg mente med spørsmålet dersom informanten var usikker. Hvis det var noe jeg oppfattet som uklart med informantens svar ble de bedt om å utdype. Under prosessen har jeg også hatt mulighet til å diskutere oppgavens innhold med fagfolk, samt veileder.

Når det gjelder ekstern validitet siktes det til om funnene i studiet kan generaliseres og kan være representative i andre sammenhenger (Jacobsen, 2015; Thagaard, 2013). Nettselskaper i Norge kan skilles fra hverandre ved blant annet konsesjonsområde, størrelse og eierskap, men man finner også likheter; de leverer de samme tjenestene, de er underlagt det samme lovverket og de har kontrollrom. På bakgrunn av disse fellesnevnerne antas det at funnene i studiene, som for øvrig er basert på ett nettselskap, er overførbare.

For å oppnå høy validitet forutsetter det også at undersøkelsen har høy reliabilitet (Halvorsen, 2008, s. 68). Reliabilitet handler om hvorvidt forskningen er pålitelig. I dette ligger spørsmålet om en annen forsker ville fått samme resultat som meg dersom vedkommende hadde tatt utgangspunkt i mitt forskningsdesign (Thagaard, 2013, s. 202). Dersom de som undersøkes er klar over at de blir undersøkt kan det påvirke deres oppførsel da de blir usatt for ulike stimuli og signaler (Jacobsen, 2015, s. 241). Under et intervju vil informanten bli påvirket av for eksempel språkbruket, kroppsspråket eller utseendet til intervjueren – dette kan refereres til som intervjuereffekt. En slik påvirkning vil også fremtre ved observasjoner, hvor den som undersøkes opplever observatøreffekt. En fordel med at jeg skriver alene er at

undersøkelsesobjektene kun trenger å forholde seg til én person. Utføres intervjuene og objektene av flere personer vil de gi ulike stimuli og dermed kan resultatene variere ut i fra hvem som undersøker (Jacobsen, 2015, s. 243). Som man ser, kan intervjuereffekt og observatøreffekt påvirke det endelige resultatet for undersøkelser. Jeg forsøkte å holde meg nøytral under intervjuene og observasjonene.

Reliabilitet oppnås også ved å vise til hvordan datainnsamlingen har foregått og hvordan dataen blir brukt (Jacobsen, 2015; Thagaard, 2013). Alle intervjuene og observasjonene ble gjennomført i lokalene til nettselskapet, henholdsvis på kontrollrommet og kontorene deres. I følge Jacobsen (2015) kan det ha en positiv effekt at undersøkelsene utføres i en naturlig sammenheng, men påpeker samtidig at det kan være utfordrende å få innpass i disse naturlige omgivelsene og det forutsetter blant annet at informantene tar seg tid til å bli intervjuet. Dette løste seg ved at jeg var fleksibel og tilpasset meg deres timeplan. Jeg fikk ikke inntrykk av at noen av informantene følte seg utilpass. Videre i datainnsamlingsprosessen må innhentet data registreres, det er viktig at dette utføres nøyaktig. Som nevnt tidligere ble det benyttet diktafon under intervjuene, og lydopptakene ble transkribert.

4.7 Etiske betraktninger

I løpet av forskningsperioden vil det gjerne dukke opp etiske eller moralske spørsmål i sammenheng med intervju. I følge Kvale og Brinkmann (2015) kan slike spørsmål knyttes opp mot alle fasene i en intervjuundersøkelse. I begynnelsen av intervjuundersøkelsen er det særlig tre etiske retningslinjer man som forsker bør ta i betraktning; informert samtykke, konfidensialitet og konsekvenser.

Informert samtykke handler om at forskningsdeltakerne blir informert om undersøkelsens overordnede formål (Kvale & Brinkmann, 2015). I begynnelsen av forskningsprosessen hadde jeg en kartleggingssamtale med beredskapskoordinator, hvor ønsket tema for oppgaven ble presentert og diskutert. Her ble det blant annet diskutert rundt sensitiv informasjon og jeg skrev under på en konfidensialitetsavtale. Senere i prosessen, i forkant av intervjuene, hadde jeg en telefonsamtale med seksjonssjefen for nettsentralen, hvor det ble snakket om motivet for forskningsprosjektets samt hva som var interessert i å undersøke nærmere. Seksjonssjefen fikk også tilsendt en grov oversikt over aktuelle temaer for intervju. Med hensyn til oppgaven ønsket jeg ikke å sende helhetlig intervjuguide da det kan påvirke undersøkelsens pålitelighet. Man

ønsker å unngå at informantene får anledning til å tilpasse svar eller handlinger ved at de vet alt om hva som skal undersøkes (Jacobsen, 2015).

Konfidensialitet innebærer at forskningsdeltakerne ikke skal kunne identifiseres, og hvis forskningen inneholder private data som gjør en person gjenkjennelig så må vedkommende gjøres oppmerksom på det og gi sitt samtykke til at informasjonen offentliggjøres (Kvale & Brinkmann, 2015). Dette anser jeg ikke som en aktuell problemstilling i forhold til min oppgave da både virksomheten og alle informantene er anonyme. Den eneste informasjonen som fremkommer knyttet til informantene er stillingstittel, kjønn og aldersgrupper. Dette ble diskutert med flere personer i virksomheten, og på grunn av sensitiv informasjon ble det tatt av en avgjørelse om at alle anonymiseres. Det er i liten grad personsensitiv informasjon, men heller sensitiv informasjon som knyttes opp mot virksomhetens systemer og drift.

Konsekvenser handler om at deltakelse i et forskningsprosjekt kan gi både fordeler og ulemper for informanten. Som forsker har man ansvar for å reflektere over mulige konsekvenser, både på et individuelt plan og for den gruppen deltakeren representerer (Kvale & Brinkmann, 2015). Det er ikke grunn til å tro at deres deltakelse vil påvirke dem i etterkant. Jeg har under hele prosessen uttrykt at min interesse er rettet mot seksjonen som en enhet og ikke ute etter å evaluere individuelt arbeid. I presentasjonen av empirien blir det i liten grad avslørt hvem av informantene som sier hva.

5 EMPIRI

I dette kapittelet vil jeg presentere resultatene fra datainnsamlingen, og dette er det empiriske grunnlaget for videre drøfting i oppgaven. Dataen fra intervjuene har blitt delt opp i ulike kategorier; daglig drift, skjerpet drift og beredskap, og læring. Hensikten er å få frem et skille med tanke på arbeidsoppgaver, arbeidsmengde og ansvarsfordeling. Etter som skjerpet drift og beredskap henger tett sammen har jeg valgt å ta de under ett og samme kapittel.

Da det er sensitiv informasjon som blir presentert i dette kapittelet har jeg sett det nødvendig å anonymisere informantene. De vil kun bli omtalt som informant.

5.1 Daglig drift

5.1.1 Arbeidsoppgaver i løpet av en ordinær dag

For å få en bedre forståelse av hvordan selskapet klarer å opprettholde og gjenoprette en stabil og pålitelig kraftlevering vil det være hensiktsmessig å undersøke hvordan de ansatte sine arbeidsdager ser ut. Som nevnt tidligere er det utført intervjuer av både de som sitter inne på nettsentralen og andre sentrale personer som jobber i nettseksjonen. Etter som informantene har ulike stillinger innebærer det ulike arbeidsdager. La oss først begynne med de som sitter inne på nettsentralen. Her er stillingene fordelt på nettnivå, det vil si at driftsingeniører jobber med transmisjonsnettet og el-maskinister med distribusjonsnettet. Alle jobber turnus og det rulleres på dag-, ettermiddag- og nattskift.

Daglig drift preges av grunnleggende beredskap samt rutiner og prosedyrer, og det er kontinuerlig overvåking av nettet. På spørsmålet om hvordan en ordinær arbeidsdag er, forklarer en av informantene at alle vaktene begynner med overlapp hvor man blir informert om hva som har skjedd på skiftet før. Dette er spesielt hensiktsmessig om det er noen spesifikke hendelser eller koblinger som man må være oppmerksom på, imidlertid blir alle hendelser registrert i systemet deres. Når man begynner på dagvakt er det som regel faste arbeidsoppgaver som skal utføres, da i form av koblingsordrer. Dette er koblinger som har blitt planlagt på forhånd, men det krever likevel at man får en oversikt slik at man finner ut om arbeidet kan utføres som planlagt.

”Det er vår jobb å ordne at koblingen av nettet blir riktig og at det ikke skjer feilkoblinger og at man blir minst mulig berørt av det”.

Hvis ikke arbeidet er avsluttet til dagskiftet er ferdig så er det de som begynner på kveldsskiftet som fullfører oppdraget. I tillegg til dette er kundehenvendelser en del av kveld- og nattskiftet etter som bedriftens kundeservice er stengt. Det hender også at de som jobber dagskift må bistå kunder dersom ikke kundeservice er tilstrekkelig. Noen kundehenvendelser er mer alvorlige enn andre, det kan være alt i fra spørsmål om elektriske biler til sikringsskap, og i noen tilfeller så har kundene mistet strømmen. Her forklarer den ene informanten at de ikke alltid får automatisk melding om at en husstand er strømløs, for eksempel på grunn av klemme på en ledning, og da er det opp til kunden å gi beskjed slik at feilen kan rettes opp i. Nettsentralen har overvåking og god kontroll på de store transformatorstasjonene og de viktigste strømledningene – de nettdelene som berører mange kunder når de feiler. Ut mot den enkelte kunden er overvåkingen begrenset. I følge en av informantene kan kundehenvendelser være et forstyrrende element i noen situasjoner, for eksempel ved et større strømbrudd, men sier videre at det også kan fungere som et lite avbrekk på en ellers hektisk dag. Videre forteller informanten at de som sitter på kundeservice sjelden har montørbakgrunn og ikke har samme kompetanse som de på nettsentralen, og det er av en grunnene til at kundehenvendelser blir sendt videre fra kundeservice til de som sitter på nettsentralen. Det er imidlertid ikke alltid at kunder ringer for å få hjelp, men heller for å informere om at de har hørt et smell fra for eksempel en trafo, og da kan de på nettsentralen sende noen for å sjekke det ut og eventuelt få det fikset – det er veldig greit at kunder kan bidra til at arbeidet går fortere.

I tillegg til kundehenvendelser skal nettsentralen også ha kontakt med montørene som er ute og gjør oppdrag. Noen av el-maskinistene har erfaring med å jobbe som montør, noe som i følge flere av informantene er en stor fordel. De har den tekniske forståelsen i tillegg til at de vet hvordan det er å jobbe ute i feltet og kan gjerne ta hensyn på en annen måte enn de som ikke har den erfaringen. De vet hvordan det er å klatre opp i stolper eller master i all slags vær, og hvordan det føles å stå ute i kulde mens man venter på informasjon fra nettsentralen. Montørene er ofte lokalkjent og har god oversikt over deres område, men de på nettsentralen kan hjelpe de med å finne frem til steder på enklest måte. En av informantene sier at montørene har med seg en iPad ut, men at de ikke vil ha like god tilgang til programmer som de som sitter på nettsentralen. Ved at nettsentralen kan hjelpe montørene sparer man tid, og ikke minst sitter montørene pris på få gode tips og anbefalinger. Det er imidlertid opp til montørene om de ønsker å følge rådene som nettsentralen kommer med. Nettsentralen gir også montørene ordre om hva som skal kobles inn og ut og når det skal gjøres, og disse ordrene skal følges så langt

det lar seg gjøre. Montørene har en leder for sikkerhet som tar endelige avgjørelser når det gjelder sikkerhet for de som skal arbeide på eller nær ved strømførende anlegg.

I likhet med de som jobber skift på nettsentralen har de andre på nettseksjonen også noen faste oppgaver i løpet av arbeidsdagen. Dette kan være i form av ulike prosjekter som er i gang. En av informantene kan fortelle at en viktig oppgave er å registrere alle avbrudd som har vært. Dette gjøres ved å hente registrerte avbrudd fra systemet som brukes på nettsentralen, og overfører de til et feil- og avbruddskjema. Når avbrudd blir registrert i systemet er det også mulighet for å inkludere årsak og om det er reparert. En annen informant forteller at de som er fagansvarlige fungerer som et støtteapparat for driftsingeniørene og el-maskinistene, hvis de for eksempel har spørsmål angående systemene som de bruker eller faglige spørsmål. Dette gjelder imidlertid ikke kun på dagtid, de kan også kontakte fagansvarlige utenom kontortiden om nødvendig. I tillegg er det noen av dem som nå holder på å få opplæring i systemene som brukes inne på nettsentralen.

5.1.2 Håndtering av feil

Når det oppdages feil på nettet som medfører strømbrudd, er det aller viktigst å få gjenopprettet strømleveringen så raskt som mulig.

”Hovedprosedyren er å få gjenopprettet strømmen raskest mulig. Det blir å varsle kunder, få ut vakter, legge om i nettet det vi kan gjøre fjernstyrt og manuell styring ute ved hjelp av montører”.

Når strømmen forsvinner er målet å få den tilbake snarest mulig. Det er i alles interesse, både nettsentralen, selve virksomheten og sluttbrukere. På en vanlig dag skjer det som regel ikke flere feil samtidig og det er ikke nødvendig å prioritere hvilken feil som skal repareres først. I situasjoner hvor flere feil inntreffer samtidig så må de forholde seg til en fastsatt prioriteringsliste, eller kundekategorier, over hvilke områder som skal gjenopprettes først. Liv og helse er førsteprioritet, eksempelvis sykehus, sykehjem eller gårdsbruk. Også infrastruktur som transport og vannforsyning er høyt på prioriteringslisten. En annen ting nettsentralen må forholde seg til er KILE-utgifter. Dette kan knyttes til avgjørelser rundt hvilket område som er lurest og kjappest å gjenopprette først. En av informantene forteller at ute i distriktene er montørene til stor hjelp da de er lokalkjent, de vet eksempelvis hvilket sted det er raskest å kjøre til. Montørene som jobber ute blir imidlertid ikke informert om disse utgiftene. Etter som de på

nettsentralen må håndtere henvendelser fra både montører, kunder og andre aktører som blir berørt, eksempelvis kommune, politi og sykehus, må det også gjøres prioriteringer for hvilke henvendelser som skal besvares først og sist. Ved hjelp av fargekoder på telefonskjermen kan de se hvem som ringer og hvilken prioritet de har.

Det er imidlertid ikke alltid at feil på nettet medfører strømbrudd og da gjelder det å finne feilårsaker og hindre at det får eskalert seg og at det vil påvirke sluttbrukerne.

”Det er jo det som er jobben, å sikre at alle avvik fra normalen blir håndtert. Så det er nok en del slike hendelser i løpet av et døgn som vi må jobbe med. Det er ikke kritiske ting, men det krever at man gjør noe”.

Noen feil er mer kritisk enn andre, og spørsmålet om det er en feil man kan leve med eller om det er en kritisk feil er det i utgangspunktet den som har rollen ”leder for kobling” som avgjør. Det er en leder for kobling på begge nettnivåene og det er faste oppgaver for håndtering. Hvis det for eksempel oppstår feil på distribusjonsnettet er det el-maskinistene som står for håndteringen. Mens de feilsøker og feilretter hjelper driftsingeniørene til med kommunikasjon med blant annet kunder – og omvendt når det er feil på transmisjonsnettet, forklarer en av informantene. Forskjellen på distribusjonsnettet og transmisjonsnettet er at det skjer oftere feil på distribusjon, men når det først inntreffer på transmisjon er det som regel snakk om feil av større omfang.

At det er godt samarbeid mellom driftsingeniørene og el-maskinistene er alle informantene enig om, samtlige påpeker at det er helt nødvendig. Det er en ganske klar arbeidsfordeling mellom driftsingeniørene og el-maskinistene i og med at det er delt opp etter nettnivå. De som jobber med distribusjonsnettet bruker et annet system enn de som jobber med transmisjonsnettet. Det ønskelig at driftsingeniørene kan hjelpe til på distribusjonsnettet i både normal tilstand og i feilsituasjoner. Å jobbe på transmisjonsnettet krever derimot at man er ingeniør eller sivilingeniør og man må ha myndighet til å jobbe på det nettnivået.

Noen signaler som de får inn i systemet sitt må tolkes, og da er det opp til de som er på vakt å ta avgjørelsen om hvordan de skal reagere på dette signalet. Da kan blant annet spørsmålene om skal de koble om, skal de vente for å se hva som skjer eller hva er mulig å gjøre, dukke opp. Flere av informantene mener at hvordan man handler videre i slike situasjoner påvirkes av ens

erfaring. I denne sammenheng påpeker en av informantene at signaler i systemet kun forteller at det og det har skjedd, men ut i fra disse signalene kan de som drifter systemene relatere det til tidligere hendelser – da ut i fra sin erfaring.

”Det viktigste vi gjør her hos oss er å fokusere på hvor det kan oppstå en feil i dag – hva er det mest kritiske punktet i dag? Og å være litt i forkant på om det kan skje noe”.

Til tross for dette så klarer de ikke å forutse hver hendelse som kommer. Feil kan oppstå som følge av svikt i tekniske komponenter, naturgitte forhold eller i form av hærverk. Derimot er etterpåklokskap lett for, påpeker en av informantene. Målet er at driften skal holdes inne på nettsentralen med minst mulig innblanding utenfra. Skjer det ekstraordinære hendelser må det selvsagt gis beskjed om til høyere hold, kan en annen informant fortelle.

5.2 Bevegelse mellom ulike beredskapsnivåer – skjerpet drift og beredskap

5.2.1 Beredskapsplanens rolle

En sentral del av de ansattes stilling er å håndtere uønskede hendelser. Det opereres med tre beredskapsnivåer; daglig drift, skjerpet drift og beredskap. Skjerpet drift er det andre og mellomste nivået, mens beredskap er det tredje og øverste beredskapsnivået i bedriften. Det er egne prosedyrer og rutiner for disse nivåene og hvordan overgangen mellom disse skal foregå, dette er beskrevet i beredskapsplanen.

Til tross for beredskapsplaner er det ikke alltid like enkelt å forberede seg på å gå i beredskap. I noen tilfeller kan det plutselig komme en alarm som krever rask respons, mens andre ganger kan man forberede seg ved at man går gjennom skiftplaner og sjekker hvor mye kapasitet man har. Eksempelvis kan feil som oppstår som følge av teknisk svikt komme brått på og medføre alvorlige konsekvenser, mens man kan forberede seg ved meldt orkan. Knyttet til dette presiserer en av informantene at selv om man kjenner innholdet i beredskapsplanen inn og ut, fungerer den kun som en sjekklister. Det er for eksempel ikke nødvendigvis slik at alle prosedyrene som er beskrevet gitt en hendelse er relevante, og det må derfor være rom for egne tanker og handlinger. Dette sier en av de andre informantene seg enig i og forteller at noen situasjoner krever andre fremgangsmetoder enn det som står beskrevet i planen – da må man bare forkaste planen og improvisere.

Alle skal ha kjennskap til planen, og man må skrive under på at planen er lest og forstått, kan en av informantene fortelle. Og hvis det skulle skje endringer i planen, blir det gitt beskjed om. En av informantene kan fortelle beredskapsplanen blir oppdatert minimum en gang i året, noe det også er krav til – og noen ganger foretar de endringer flere ganger i løpet av ett år. Som regel er det knyttet til vinterhalvåret at det fremtrer endringer, dette på grunn av at det er da det skjer flest uønskede hendelser. Det er en bestemmelse om at beredskapsplanen skal være oppdatert per 1. november hvert år.

Som nevnt tidligere er det fastsatte prioriteringer for hvilke områder og kundegrupper som skal gjenoprettes først ved strømbrudd. Dette er informasjon som man finner i beredskapsplanen. Deler av denne planen utarbeides i samarbeid med aktører, blant annet kommuner, og de får mulighet til å komme med innspill. Planen fungerer som en sjekklister for håndtering av hendelser, i tillegg til å informere om hvem som skal kontaktes angående hva. Når det gjelder rutiner og prosedyrer for overgangene mellom de ulike beredskapsnivåene, nevnes det at det har blitt opplevd som noe mer uryddig etter omorganiseringen i fjor, ved at blant annet kontaktinformasjon i planen var ukorrekt.

5.2.2 Hvem tar beslutninger?

Et sentralt skille mellom driftsingeniører og el-maskinister er ansvarsfordelingen. Store deler av døgnet er det kun de inne på nettsentralen som er på jobb da de andre på avdelingen jobber vanlig kontortid. På dagtid er beredskapsledelsen med på å ta avgjørelser knyttet til endring i beredskapsnivå. Foruten om kontortiden er det driftsingeniører som er tillagt ansvaret å sette skjerpet drift eller beredskap og tilkalle beredskapsledelsen. En av informantene forteller at dette ansvaret føles naturlig. På kveld- og nattskiftet er det én driftsingeniør og én el-maskinist på jobb, og selv om det er driftsingeniøren som har det formelle ansvaret å avgjøre om de skal gå i skjerpet drift eller beredskap så sier samtlige av informantene at det diskuteres mellom de to som er på vakt og at de blir enig seg i mellom. Flere av informantene sier at det er godt å ha noen å støtte seg til da det kan være snakk om store avgjørelser. God kommunikasjon og ydmykhet er sentralt. Er de veldig usikker så kontakter de den personen som er driftsleder, dersom det er tid. I noen tilfeller vil det være slik at man må ta en avgjørelse der og da, og hvis ikke driftslederen er enig må det gjerne gjøres endringer i ettertid.

5.2.3 Skjerpet drift

Det er ulike årsaker til at man beveger seg fra daglig drift til skjerpet drift. Det kan blant annet være på grunn av værvarsel, hvis det for eksempel er meldt lyn og torden, vind eller snø. Nettsentralen har gode verktøy tilgjengelig og kan bruke både selskapet sine interne meteorologiske ressurser, et værprogram som blant annet registrerer lynnedslag og meteorologisk institutt. I tillegg til værphenomener kan flere feil samtidig også være grunn til å gå opp i beredskapsnivå. Hvis de som er på vakt ser at de trenger hjelp til å håndtere kan de gå i skjerpet drift og kalle inn ekstra bemanning. Slike beslutninger tas da på bakgrunn av statusen der og da, hva som kan forventes utover og ikke minst tidligere erfaringer. Når de går i skjerpet drift kalles det gjerne inn en eller to ekstra personer.

I skjerpet drift er det hensiktsmessig å gå gjennom nettet og se etter kritiske punkter. Hvis det for eksempel er en kabel som koblet ut på grunn av planlagt arbeid kan det være nødvendig å utsette dette og koble inn kabelen igjen slik at den kan brukes ved behov. Det er ønskelig å få mest mulig tilbake til normalstatus i tilfelle situasjonen eskalerer til en å større feilhendelse.

Nettsentralen er sårbar når det kommer til sykdom, og mangel på bemanning kan være en årsak til at man går i skjerpet drift.

5.2.4 Prosedyrer ved beredskap

Nettsentralen er oftere i skjerpet drift enn beredskap. Det hender også at de går i beredskap for kun noen timer, gjerne på grunn av ukjent omfang, mens andre ganger kan det være over flere dager. Det er ikke alltid at man kan forberede seg på å gå i skjerpet drift eller beredskap. Det er kun når det er meldt uvær, forteller en av informantene. Det kan også oppstå uventede hendelser som for eksempel brann eller kabelfeil som gjør at de må gå i beredskap. Når de har fått oversikt over situasjon og vet hvordan det skal håndteres så kan de gå ut av beredskap.

Når det er meldt uvær er det sjeldent at de går i beredskap med en gang, de ser heller situasjonen an og hvordan været utspiller seg. Det krever likevel planlegging i tilfelle de må gå i beredskap. I forkant av ekstremvær møtes beredskapsledelsen og gjennomgår prosedyren som beskriver alle forberedelser som skal gjøres. Her besluttet også alle tiltak som skal iverksettes før uværet inntreffer. Faktorer som spiller inn her er blant annet hvilken dag det er og tidspunkt. Er det en ukedag er det som regel tilstrekkelig med bemanning, men lander uværet på en helg eller helligdag krever det mer koordinering. I forkant av beredskap prøver man å beregne

ressursbruken slik at man har nok bemanning når det verste står på, dette gjelder både bemanning på nettsentralen og blant montørene. Folk må være klar over at det er beredskapstilstand og at de kan bli kalt inn. Ved uvær er det også noen områder som er mer utsatt enn andre, som regel ute i distriktene, og det er viktig at man legger opp ressursene deretter – målet er å ha montører tilgjengelig i disse områdene. En fordel ved å gå inn i beredskap er at det er lettere å beordre bemanning, samt sette jobbprioritet på det som er årsaken til beredskap. Når man er i beredskap er det viktig at man tenker på det er nok folk til å ta over skift. En back-up de har er at de fagansvarlige for både distribusjon og transmisjon får opplæring i å bruke datasystemene inne på nettsentralen. Dette krever kontinuerlig øving og er nødvendig for at de skal fungere optimalt inne på nettsentralen – dersom det er behov for det.

En av informantene kan ut i fra erfaring fra tidligere hendelser fortelle at når man er i beredskap så blir arbeidsoppgaver delegert og man har da full oversikt over sitt distrikt og det man selv jobber med. En slik oppdeling krever likevel god kommunikasjon da nettet strekker seg over flere soner. Når man skal rette opp i feil blir man veldig fokusert på akkurat den jobben og når det skjer mye rundt en er det lett for at man ikke får med seg alt som blir gjort og sagt. En av informantene hevder at en storskjerm som viste for eksempel alle sonene, ville gjort jobben lettere. Ved en av de siste større hendelsene var nettopp dette litt problematisk, men det var likevel ikke et kritisk punkt. Det handler ikke om effektivitet, men heller sikkerhet for de som jobber ute fysisk med nettet, for eksempel hvis man går over i en annen sin sone der man er mindre kjent og kobler i et nett er det pågår arbeid. Informanten forteller at det heldigvis ikke har skjedd noen uhell eller ulykker til nå og at de har veldig fokus på sikkerhet. Nettsentralen har tatt i bruk et system som er relativt nytt for dem og det er nå opp til de å lage et godt system for å ivareta sikkerheten. Når de er i beredskap skal de også rapportere til en koordinator som har full oversikt over hvor det er strømbrydd, hvor mange som er strømløse og lignende, men som ikke jobber direkte med feilene som har oppstått.

”Ja, det er ganske mye ansvar. Er ikke helt sikker på om alle er klar over hvor mye ansvar det faktisk er. Vi skal ha oversikt og kontroll over alt og vi skal kunne ordne opp i det hvis det skjer noe. Mye ansvar for protokollføring og sikkerhet. Skal passe på at det ikke kommer strøm på områdene som folk jobber på. Det er viktig at ting gjøres riktig og at vi har sikring på de riktige punktene. Det er ganske alvorlig om man svikter der”.

Sikkerhet er viktig, og alle informantene er samstemte om at sikkerhet går fremfor alt. En av informantene presiserer at det er bedre at noen kunder er strømløs en periode enn at de som reparerer nettet blir skadet.

Hvis de går i beredskap på grunn av en uønsket hendelse som har inntruffet og som har medført strømbrudd er det prosedyrer som skal følges. Det er blant annet viktig å få varslet og informert kunder som blir berørt. Det første varselet blir sendt ut i løpet av få minutter. Et slikt varsel inkluderer estimert tid for når strømmen kommer tilbake slik at kundene har noe å forholde seg til. Når en feil oppstår så vet de at et område er strømløst, de vet som regel ikke feilårsak eller feilsted, og noen vil gjerne få strømmen tilbake før estimert tid og andre senere enn det. Transmisjonsnettet er et maskenett og det er da flere forbindelser mellom forskjellige punkter i nettet, så ved normale feil tar det som regel ikke så lang tid før strømmen er tilbake. Ved større feilutfall, som for eksempel at et større område blir mørklagt, vil det derimot ta lengre tid å gjenopprette strømmen.

En av informantene kan fortelle at det er de samme personene som arbeider ved daglig drift, skjerpet drift og når de er i beredskap, men at det blir innkalt ekstra personell etter som situasjoner utvikler seg og det er behov for det.

5.3 Læring knyttet til uønskede, uventede og ukjente hendelser

Uønskede hendelser kan fungere som et godt verktøy for læring om det blir brukt riktig. I de tilfellene hvor feil fremstår som uventede og ukjente blir de gjerne diskutert, ofte med den som er fagansvarlig for det nettnivået det gjelder. I ettertid av mindre feil trenger det ikke nødvendigvis å gjennomføres en formell evaluering, men det kan være greit å diskutere hvordan det ble håndtert. En av informantene forteller at det som regel skjer alt i fra tre til tolv feilsituasjoner i uken så folk jobber med det hele tiden, og disse feilene kan regnes som daglig drift. I tillegg brukes det rapporteringssystem hvor for eksempel farlige forhold, uønskede hendelser eller forbedringer registreres. Ved å gå gjennom dette vil det gjerne gi en god evaluering. En av informantene erkjenner likevel at læring etter hendelser er et område som de kan bli bedre på.

Transmisjonsnettet har færre feil enn distribusjon, og her sier en av informantene at ved å ha mer informasjonsdeling med andre aktører så kan man bruke de feilene som oppstår, enten i eget eller andre sitt område, som en måte å tilegne seg ny kunnskap om risiko og farer.

”Feil på transmisjonsnettet? Nei, alt for sjeldent. Man skal jo ikke si det, men det er jo med tanke på egentrening”.

Til tross for at det ikke utveksles noe særlig med informasjon spesifikt for å tilegne seg ny kunnskap, deltar blant annet de fagansvarlige på temadager, kurs og lignende sammenkomster – og der vil man også få nye innspill og ny kunnskap.

Flere av informantene er enig om at det er få øvelser og at de gjerne kunne hatt flere, men at det er lette sagt enn gjort. For det første må det være tid til det og for det andre så må øvelsene være realistisk for at det skal ha hensikt. Nettselskapet har imidlertid opplevd flere større hendelser hvor de har gått i beredskap på grunn av uvær, med jevne mellomrom i løpet av de siste årene. Flere av informantene sier i denne sammenheng at det i seg selv er en god øvelse. I slike situasjoner blir de testet og de får mulighet til å avdekke eventuelle svakheter. I etterkant av noen av de større hendelsene har det vært innkalt til evalueringsmøter med ansatte i selskapet og sentrale aktører, eksempelvis kommuner. De som jobber på nettsentralen er invitert til å delta etter som de har vært en sentral del av problemhåndteringen, men på grunn av skiftordning er det ikke alle som har mulighet til å stille opp.

En av informantene forteller at foruten om de øvelsene de har hatt, samt reelle hendelser, så er det opp til de selv å gå gjennom tenkelige scenarioer. Særlig i forkant av koblinger diskuteres det rundt mulige scenarioer. De kan også simulere hendelser i et av systemene deres. I tillegg til at de synes det er interessant, kan man si at det er en del av stillingen deres da den tilsier at nettet skal driftes på så effektiv måte som det lar seg gjøre og med så få avbrudd som mulig.

”Det viktigste er å få strømmen opp igjen så fort som mulig, men vi må alltid se konsekvensene av det vi gjør. (...) og hele tiden kan man bli lurt. Det er det som er interessant, for det er stadig nye oppgaver. Eller så kunne man bare fått en maskin til å gjøre det”.

En dag på nettsentralen er uforutsigbar, og dette innebærer blant annet at de alltid må være bevisst på at noe kan skje.

Mange av de som jobber på nettsentralen har lang erfaring, men det er ikke til å unngå at noen slutter og at nye folk kommer inn – da er det nødvendig med tilstrekkelig og god opplæring.

”(...) han var faktisk heldig, for i sin opplæringsperiode hadde vi en del feil som han fikk være med på å håndtere. For hver feil så får man erfaring og man blir tryggere”.

Selv om de som har vært på nettsentralen over lengre tid har god erfaring å spille på, skal stillingene som driftsingeniør og el-maskinist i utgangspunktet være standardisert. Det vil si at flere personer har den samme stillingen og de samme arbeidsoppgavene. For utenforstående skal det ikke spille noen rolle om hvem man snakker med for å få informasjon, men alle vil selvsagt ha sin måte å jobbe på og ha ulike erfaringer som kan påvirke dem.

Det føres statistikk over når nettsentralen er i daglig drift, skjerpet drift og beredskap, men det blir ikke brukt som målestokk i den forstand at man jobber mot forårets tall. For må man være i beredskap så må man være i beredskap. Det er ønskelig å gjøre ting bedre for hver feilsituasjon, samtidig må man huske på at ingen feilsituasjon er lik. Det man eventuelt kan måle seg på da er for eksempel informasjonsflyt, effektivitet, struktur i arbeid, ansvarsfordeling, hvordan pressen har blitt håndtert osv.. Dette er punkter som kan evalueres og sammenlignes mot lignede hendelser som har skjedd tidligere, forteller en av informantene.

5.4 Resultat fra observasjon

Som nevnt i metodekapittelet fikk jeg tilgang til kontrollrommet og dermed mulighet til å observere driftsingeniørene og el-maskinistene. Observasjonene ble gjennomført under en relativt rolig periode, og jeg fikk et innblikk i hvordan deler av en ordinær dag kan se ut. Under observasjonene kom samhandlingene mellom operatørene tydelig frem. Operatørene hadde hver sin arbeidsstasjon med et sett dataskjermer. De jobbet med hver sine oppgaver knyttet til deres nettnivå, henholdsvis transmisjon og distribusjon. Til tross for dette var det god kommunikasjon og de diskuterte hverandres oppgaver.

6 DRØFTING

I dette kapittelet blir innhentet data presentert og drøftet i lys av det teoretiske grunnlaget for oppgaven.

6.1 Beredskapsarbeid i kraftforsyningen

Kritiske infrastrukturer og kritiske samfunnsfunksjoner må være velfungerende for at samfunnets grunnleggende behov skal tilfredsstilles. Når det kommer til infrastruktur har blant annet elektrisk kraft blitt identifisert som en kritisk infrastruktur ut i fra spørsmålene om hvor stor avhengighet det er, om det finnes alternativer og hvor tett kobling det er (NOU 2006:6, 2006). Det er flere grunner til at man ønsker å unngå ekstraordinære hendelser innenfor kritisk infrastruktur, blant annet så er dette tjenester som er gjensidig avhengig av hverandre – det er flere infrastrukturer og samfunnsfunksjoner som er helt avhengig av strøm. Man ser også en avhengighet innenfor kraftforsyningen da det forutsetter produksjon, distribusjon og omsetning av elektrisitet.

Nettselskapers hovedansvar er å drifte et fungerende overføringsnett slik at sluttbrukeren mottar strøm og opplever en tilfredsstillende forsyningssikkerhet. Etter som Norge har et høyt strømforbruk stilles det også høye krav til kraftlevering (Meld. St. 25 (2015-2016), 2016). For å etterleve kravene må nettselskaper blant annet forholde seg til Leveringskvalitetsforskriften som har som formål å sikre tilfredsstillende leveringskvalitet. Denne forskriften er relevant for nettselskapets daglige drift. Avbruddsstatistikk viser at den norske kraftinfrastrukturen er robust og har høy leveringspålitelighet, som henholdsvis lå på 99.987 % i 2016 (Hansen et al., 2017).

En stabil strømlevering er fundamentalt i dagens samfunn er det ønskelig å være beredt på at det kan inntreffe uønskede hendelser som kan medføre feil. Empirien viser at det ikke er alle feil som medfører bortfall av strømlevering, mens noen feil vil være mer kritisk enn andre. I Beredskapsforskriften fremkommer det blant annet at nettselskaper skal kunne håndtere ekstraordinære hendelse, dette innebærer som regel hendelser av større omfang enn feilsituasjoner som håndteres til daglig (NVE, 2013). Dette samsvarer også med ansvarsprinsippet, likhetsprinsippet og nærhetsprinsippet (Meld. St. 29 (2011-2012), 2012). Uavhengig av hvilken type feil det er snakk om er det hensiktsmessig å finne årsak til feil og reparere. Ved å ha fokus på beredskap kan man forberede seg til en viss grad, noe som igjen

bidrar til bedre håndtering og minimere eventuelle følger (Engen et al., 2016). Dette kan man se igjen i eksempelet som presenteres i delkapittel 2.3. Det er hentet fra Quebec i Canada hvor sluttbrukere mistet strømmen i opptil én måned som følge av en isstorm. Denne hendelsen viste at god håndtering av situasjonen gjorde at de unnslopp langvarige konsekvenser (Fridheim, Hagen & Henriksen). Etter som dette eksempelet er fra 1998, altså 19 år siden, kan det tenkes at følgene av langvarig strømbrudd ville vært annerledes i dag. Det må også tas høyde for at dette var i Canada og at de har andre forutsetninger enn Norge. Nettselskaper må være beredt på ekstraordinære hendelser. Alle KBO-enheter må rette seg etter Beredskapsforskriften, som inneholder funksjonskrav rettet mot etablering av et helhetlig beredskapskonsept.

6.2 Styring av høyteknologisk system

I følge Perrow vil høyrisikoteknologier oppleve systemulykker på et eller annet tidspunkt, det er ikke til å unngå og det må betraktes som normalt (Perrow, 1984). NAT har særlig fokus på det tekniske aspektet ved organisasjoner, og sett i lys av dette er kraftforsyningen tett koblet og blir stadig mer kompleks (Hagen, 2015; Perrow, 1999). Økt kompleksitet kan blant annet knyttes til at teknologi tar over arbeidsoppgaver som tidligere har blitt utført manuelt av mennesker. I stedet for manuell betjening fjernstyres kraftforsyningsanlegg fra driftssentraler (Fridheim, Hagen & Henriksen, 2001; NOU 2006:6, 2006). Operatørene på nettsentralen har oversikt over hele nettselskapets kraftnett. Det er altså store områder fordelt på noen få personer. Det krever at systemene fungerer som de skal, og ikke minst at det er forståelig for de som skal bruke systemet – hovedsakelig operatørene. Systemene er utviklet slik at de kan fange opp feil og avvik på nettet, men det er likevel noen som går ubemerket hen. Som en av informantene forteller så hender det at kunder ringer til nettselskapet for å informere om at strømmen er borte. Dette problemet viser til at selv om teknologien er godt utviklet er det fremdeles mangler og rom for utbedringer. Det vil si at det er nye sårbarheter som fremtrer.

Høyteknologiske organisasjoner må driftes på en sikker måte, men også sørge for tilfredsstillende levering av tjenester (LaPorte & Consolini, 1991). Med utgangspunkt i empirien kan det trekkes likhetstegn mellom nettselskapet og de kriteriene for høypålitelige organisasjoner som Aven et al. (2004) peker på. Redundans er viktig, både teknisk og organisatorisk. Et eksempel på organisatorisk redundans er at folk som ikke jobber til daglig inne på nettsentralen får opplæring i systemene som brukes på kontrollrommet. Selv om det i utgangspunktet er driftsingeniører og el-maskinister som drifter nettsentralen ser nettselskapet det nødvendig å ha en back-up. Det er flere årsaker til at det ikke er tilstrekkelig med operatører,

det kan for eksempel være på grunn av sykdom. Det er et begrenset antall driftsingeniører og el-maskinister og de er derfor sårbar overfor sykdom. Økt arbeidsmengde kan også medføre et større behov for operatører, for eksempel på grunn av uvær. De personene som midlertidig inntretr som operatører må være kvalifisert til å håndtere systemene. Det kan antas at de ikke har den samme erfaringen som de som jobber fast som operatør, men de må ha tilstrekkelig kunnskapsgrunnlag og forståelse for arbeidsoppgavene. Disse personene vil dermed ha en annen bakgrunn og erfaring enn de faste operatørene, det ikke nødvendigvis negativt da de kan bidra med nytt syn på ting og kan potensielt styrke den organisatoriske redundansen. En annen sentral faktor er at operatørene på nettselskapet har et bredt støtteapparat som de kan rådføre seg med, blant annet de som er fagansvarlig for transmisjons- og distribusjonsnettet. Som en av informantene påpeker er ydmykhet en viktig egenskap, dette viser at man er mottakelig for korrigerende og ikke minst at man ønsker å ta best mulig avgjørelse.

Nettselskapet veksler mellom daglig drift, skjerpet drift og beredskap. En slik kategorisering av tilstander og styringsstruktur finner man også i LaPorte og Consolini (1991) sine studier av høypålitelige organisasjoner, hvor det ble identifisert tre ulike tilstander som var preget av enten rutiner og byråkrati, høytempo eller krisemodus. Det var de samme personene som beveget seg mellom tre tilstander, noe som også er tilfellet hos nettseksjonen. Ut i fra hva informantene har fortalt kan man se likhetstrekk ved nettselskapets organisering og tidligere studier. De ansatte ved nettseksjonen har sine faste oppgaver ved normal drift. Ved skjerpet drift eller beredskap vil arbeidsoppgavene deres variere noe ut i fra hvilket nettnivå det har oppstått feil på. Sentralt her er skillet mellom sentralisert og desentralisert styring. Når beredskapslederen for nettseksjonen ikke er på jobb er det driftsingeniøren som har det formelle ansvaret å erklære at nettsentralen er i skjerpet drift eller beredskap, men det fremkommer av intervjuene at avgjørelsen tas i fellesskap av både driftsingeniør og el-maskinist – alt etter hvilket nettnivå det er snakk om. Dette viser til at de er fleksibel og i så måte er det desentralisert styring.

Når nettseksjonen er i beredskap delegeres arbeidsoppgavene ut i fra hvilket nettnivå det er feil på. Hver av operatørene får et område som de skal jobbe med og ha full oversikt over. Operatørene jobber selvstendig med sitt ansvarlige område, men det er likevel visse prosedyrer som må følges. Ved strømbrudd er det blant annet viktig at det sendes ut informasjon til de som blir berørt og dette skjer relativt fort, det er kun snakk om et par minutter. Når det gjelder gjenoppretting av strømlevering er det fastsatte prioriteringslister som de må forholde seg til, hvor liv og helse er førsteprioritet, i tillegg til KILE-kostnader. Selv om byråkratiet svekkes,

vil det likevel være til stede – bare i mindre grad. At de må forholde seg til ytre faktorer kan anses som positivt da det letter på ansvaret til operatørene. I stressende situasjoner er det gjerne ikke alltid like enkelt å ta de beste avgjørelsene, samt det reduserer sjansen for intern konflikt knyttet til viktige avgjørelser.

Når det gjelder reaksjoner på hendelser og reparasjoner opplever operatørene at de har frihet, men med dette kommer det også et stort ansvar for helse, miljø og sikkerhet. Dette gjelder særlig ut mot montørene da det er de som er ute og reparerer nettet fysisk. Samtlige av informantene påstår at man alltid må tenke HMS, og ingen på nettsentralen tar avgjørelser knyttet til montørens egen sikkerhet – dette er det montørene sin ”leder for sikkerhet” som styrer. Sier montørene at et oppdrag er uforsvarlig å gjennomføre så godtar nettsentralen det uten å stille spørsmål ved det. Det fremstår som at holdningen til at sikkerhet er viktigst gjennomsyrrer hele nettseksjonen, noe som også en sentral karakteristikk ved høypålitelige organisasjoner. Knyttet til sikkerhet ut mot montørene krever det at operatørene på kontrollrommet kommuniserer godt når de jobber med hver sine områder, slik at det for eksempel ikke kobler spenning på en kabel som det jobbes på. En slik feil kan medføre fatale konsekvenser, og for å unngå dette må man være oppmerksom på både seg og andre sitt arbeid.

6.3 Mindfulness som verktøy

Når det kommer inn signaler om feil eller avvik er det opp til operatørene å tolke disse ut i fra det som fremkommer i systemet. Dette kan knyttes opp mot det å være mindfulness, eller å ha økt bevissthet. Det beskrives fem prinsipper som kan bidra til en høypålitelig og kontinuerlig drift, i denne sammenheng nettselskapets forsøk på å opprettholde en stabil og høypålitelig strømlevering. De tre første prinsippene er knyttet til perioden før en feil oppstår, mens de to siste viser til hvordan feil skal håndteres for å minimere følgene. Mens noen hevder at man ikke kan forvente det uventede så vil andre argumentere for at organisasjoner som opplever færre ulykker enn forventet, har bedre evne til å oppdage uventede hendelser eller en bedre forståelse av hendelser som har inntruffet (Weick & Sutcliffe, 2007).

Ut i fra forventninger kan man lage skriftlige beredskapsplaner. Det oppfattes som at alle informantene er godt kjent med innholdet i beredskapsplanen. Informantene referer til beredskapsplanen som et godt verktøy for håndtering av hendelser, imidlertid er de bevisst på at dette kun fungerer som en veileder og at det kan oppstå hendelser som krever løsninger som ikke er beskrevet i denne planen. En slik holdning til beredskapsplanen er helt nødvendig for at

beredskapsplanen ikke skal motvirke sin hensikt. Selv om hendelser som inntreffer fremstår som svært lik og kjente er det viktig å ta betraktning at ingen hendelser vil være helt identisk og at den løsningen som fungerte bra på forrige hendelse ikke er like effektiv senere (Weick & Sutcliffe, 2007). Det kan tenkes at når det oppstår slike situasjoner er det ikke like enkelt å se bort i fra beredskapsplanen etter som de løsningene har gitt gode resultater tidligere, og at faktorer som erfaring og kompetanse vil påvirke ens bedømmelse av situasjonen og ens fleksibilitet. Jo lengre erfaring man har, desto enklere vil det være å orientere seg blant alternativer av løsninger.

Det første mindfulness-prinsippet handler om at høypålitelige organisasjoner har et ønske å avdekke feil som kan oppstå eller som allerede har inntruffet. Å erkjenne at feil forekommer kan gi en fordel ved at man er mer oppmerksom på signaler som kan antyde svikt eller avvik, og reagerer man på disse signalene i tide så kan man avdekke eller avverge større feil. For at alle feil og avvik skal bli registrert er det viktig med god rapporteringskultur (Weick & Sutcliffe, 2007). Flere av informantene nevner at alle hendelser som skjer i nettet blir registrert i systemene deres. Når operatørene på nettsentralen har vaktskifte er det satt av tid til overlapp og at de informerer hverandre blant annet om spesifikke hendelser. At alle på nettseksjonen bidrar i faglige diskusjoner rundt hendelser som skiller seg ut fra daglig drift kan tenkes å være nyttig i den forstand at de har ulik kompetanse og erfaring å tolke hendelser ut i fra.

Operasjonell sensitivitet er svært sentralt og handler om de ansatte i nettseksjonen sin situasjonsforståelse. Rutiner er positivt så lenge man ikke blir blendet av dem, og at man handler på automatikk (Weick & Sutcliffe, 2007). Nettselskapet har uforutsigbare arbeidsdager, noe de selv virker bevisst på. Er man bevisst på at det kan forekomme plutselige hendelser kan det tenkes at man også er mer oppmerksomhet for små avvik. Og hvis det oppstår en nesten-ulykke er det viktig at nettsentralen anser dette som ny kunnskap, fremfor å bruke det kun som en bekreftelse på god beredskap.

Læring av hendelser kan knyttes opp mot det fjerde mindfulness-prinsippet som handler om evnen til å lære av tidligere hendelser, dette er sentralt for resiliens og høy pålitelighet (Weick & Sutcliffe, 2007; Aven et al., 2014). Empirien tyder på at det er lite formell evaluering som alle får deltatt på. Derimot forteller flere informanter at de likevel er opptatt av å diskutere hendelser. Som en av informantene påpeker er mange av feilsituasjonene ”dagligdagse” og betraktes som en del av den daglige driften, da til tross for at det er uønsket og gjerne uventet

eller ukjent. I så måte kan alle hendelser betraktes som øving, både store og små. Foruten om reelle hendelser som inntreffer mener flere av informantene at det kunne vært flere planlagte øvelser, men de er imidlertid tydelig på at det da må arrangeres realistiske hendelser for at det skal være hensiktsmessig. Nettselskapet har opplevd flere store hendelser knyttet til uvær i løpet av de siste årene, hvor det da var nødvendig å gå i beredskap. Her sier flere av informantene at dette var god trening for nettseksjonen og at de da fikk testet seg. Her får man mulighet til å avdekke både svakheter og styrker. Et sentralt spørsmål knyttet opp mot læring er om selskapet ville hatt flere planlagte øvelser dersom ikke reelle hendelser oppstod.

Det hender også at operatørene lager sine egne scenarioer – både fordi det er relevant for stillingen og arbeidsoppgavene deres, men også fordi de finner det interessant. Som en av informantene sier så kan man alltid bli lurt av hendelser og at man derfor alltid må være bevisst på at noe uventet kan skje, og i følge Weick og Sutcliffe (2007) er dette et tegn på en organisasjon er resilient. Videre påpeker Weick og Sutcliffe (2007) at læring kan frembringe spørsmålene; hva skal man lære og hvordan skal dette eventuelt brukes på en hensiktsmessig måte? Dette er utfordringer som alle organisasjoner støter på, og det kan løses ved å være fleksibel og å ha god tilpasningsevne. Har man for eksempel oversikt over tilgjengelige ressurser vil man kunne håndtere uventede hendelser bedre. Læring, evaluering og etablering av ressurser inngår som viktige faser i beredskapsarbeidet (Engen et al., 2017). Til tross for at nettseksjonen har potensial knyttet til læring av hendelser, kan det likevel tyde på at de er opptatt av å tilegne seg ny kunnskap og at de plukker med seg nyttig informasjon og kunnskap underveis. Det betraktes også som positivt at nettseksjonen er bevisst på at det er et læringspotensial til stede.

6.4 Kognitive ferdigheter

I forbindelse med en studie av amerikanske California Independent System Operator (CAISO) presenterer Roe og Schulman (2008) de to begrepene ”high reliability management” og ”reliability professionals”. I forhold til dette studiet av et norsk nettselskap er det kontekstuelle og strukturelle ulikheter, men til tross for dette finner man også sentrale likheter. En vesentlig forskjell mellom det norske nettselskapet og CAISO er at sistnevnte forholdt seg til en pågående kraftkrise i California. Det er også eksterne og interne forutsetninger som skiller selskapene fra hverandre, men det er likevel en svært sentral fellesnevner; begge selskapene har som mål å opprettholde en høypålitelig strømlevering og kontrollrommene er sentrale for å styre et tett koblet og komplekst system.

Roe og Schulman har kartlagt, identifisert og kategorisert handlingsmønstrene til operatørene på kontrollrommet til CAISO; ”just-in-case”, ”just-in-time”, ”just-for-now” og ”just-this-way” (Roe & Schulman, 2008). Sett opp mot de tre beredskapsnivåene, daglig drift, skjerpet drift og beredskap, som nettsentralen har etablert, kan man se en viss likhet. Daglig drift består av grunnleggende beredskap og prosedyrer og rutiner, akkurat som i CAISO sin ”just-in-case”. Når nettsentralen beveger seg over til skjerpet drift, kan det sammenlignes med ”just-in-time”. CAISO sine to siste handlingsmoduser ”just-for-now” og ”Just-this-way” samsvarer med nettselskapets siste beredskapsnivå, altså når de er i beredskap. I så måte kan det også trekkes likheter til de tre tilstandene som LaPorte og Consolini (1991) fant i høypålitelige organisasjoner.

HRM inkluderer mange av de samme elementene som HRO og mindfulness, men et sentralt skille er blant annet den høypålitelige styringen i sanntid. HRM viser til at fleksibel styring er nødvendig i tillegg til forventninger og planlagt beredskapsarbeid. Dette kommer særlig frem ved ”just-in-time”, som innebærer at man improviserer i sanntid, og det er ofte snakk om avgjørelser som må tas raskt (Roe & Schulman, 2008; 2016). Et slikt handlingsmønster kan man også se hos nettseksjonen. Flere av operatørene forteller at de tolker signaler som oppstår i systemet ut i fra erfaringer. Her kan det tenkes at evaluering av tidligere hendelser kan bidra til å øke bevisstheten deres, ved at de har et bredere grunnlag å tolke ut fra.

Dersom det oppstår for eksempel to-tre feil på samme tid, vil det bli det bli delegert oppgaver blant de som jobber på kontrollrommet. I tilfeller hvor arbeidet foregår kjapt og man har begrenset tid på seg kan det tenkes at både organisatoriske og menneskelige faktorer påvirker håndteringen. Når det gjelder faktorer som erfaring og kompetanse, kan det antas at de som ikke jobber fast inne på nettsentralen jobber noe annerledes enn de som jobber der fast. Det kan også tenkes at man ser forskjell mellom de som jobber fast på kontrollrommet, ut i fra blant annet hvor lenge de har jobbet der og hvor mange lignende hendelser de har vært med på tidligere. Igjen vil kommunikasjon være en sentral faktor for en høypålitelig drift, i den forstand at de kan rådføre seg med andre.

Andre faktorer som påvirker ”just-in-time” handlinger, og for øvrig atferd generelt, er selskapets organisasjonsstruktur, deres evne til å planlegge beredskapsarbeid og i hvilken grad de er ”mindful”. I situasjoner hvor beredskapsplanen ikke er hensiktsmessig og det er

nødvendig å improvisere, må man være i stand til å tenke konsekvenser slik at man unngå å utføre handlinger som kan forverre tilstanden. Det kan tenkes at dette er en evne som utvikler seg over årene etter som man får erfaring. Individens kognitive begrensninger er et faktum, og det er derfor man finner et nettverk av reliability professionals (Roe & Schulman, 2016).

Et nettverk av reliability professionals består av operatører, støttepersonell og ledere – og disse personene er helt nødvendig for HRM. I tillegg til å drifte nettet i sanntid er det andre sentrale karakteristikk ved dem. Store deler av arbeidsdagen til operatørene på kontrollrommet tilbringes bak dataskjermen hvor de overvåker nettet via IKT-systemer og reagerer på feil og avvik som oppstår. I tillegg til å utføre tekniske oppgaver har de også en annen viktig oppgave; de skal ha kontakt med montører, kunder og andre aktører. Montører og kunder har de daglig kontakt med, mens andre aktører som for eksempel kommuner eller politi, har de som regel kun kontakt med hvis det har inntruffet feil. Dette er også oppgaver som et system ikke kunne tatt seg av og det viser at det er nødvendig med fysisk personell, til tross for en oppfatning om at operatører hører fortiden til og at innovasjon og teknologi er fremtiden (Roe & Schulman, 2016). Ut i fra samtalene med informantene i nettselskapet fremkommer det anerkjennelse til de som sitter inne på nettsentralen. Det er ikke et spørsmål om deres funksjon er nødvendig eller ei. Uansett hvor gode systemer som utvikles vil mennesker alltid ha egenskaper som ikke vil være mulig å bygge inn i et system.

Når det gjelder montører er dette en viktig gruppe med fagfolk og helt nødvendig for at nettet skal fungere – det er tross alt de som utfører de fysiske reparasjonene på nettet. Flere av informantene kan fortelle at det er viktig med god kommunikasjon dem i mellom. Her kommer menneskelige egenskaper til syne. El-maskinistene har selv jobbet som montører og har dermed en annen forståelse for arbeidet til montørene enn det andre har. Det kan tenkes at dette kan styrke og effektivisere arbeidet ute, som igjen kan påvirke strømleveringen.

7 KONKLUSJON

Dette studiet har forsøkt å besvare følgende problemstilling:

Hvordan kan nettselskaper opprettholde en høypålitelig strømlevering og hvilke forutsetninger må være til stede ved drift fra kontrollrommet?

Den norske kraftforsyningen har en robust infrastruktur og ut i fra avbruddsstatistikker ser man at det er en høy leveringspålitelighet. Dette forutsetter at produksjon, overføring og omsetning av strøm er tilfredsstillende. I denne oppgaven har fokuset vært på distribusjon av elektrisitet. Kraftnettet består av sentralnettet, regionalnettet og distribusjonsnettet. Det er nettselskaper som har ansvaret for å drifte disse nettene og sørge for at sluttbrukere mottar strøm. Den teknologiske utviklingen har påvirket kraftleveringen på flere måter. For det første så er andre infrastrukturer og samfunnsfunksjoner avhengig av stabil strømforsyning og denne avhengigheten påvirker samfunnsmessige konsekvenser ved bortfall av strøm. For det andre så har behovet for elektrisitet økt og dermed også forbrukere sin forventning til kraftforsyning, og for det tredje så har drift av kraftforsyning blitt mer kompleks. Dette er utfordringer som alle nettselskaper står ovenfor. Per i dag er det ikke et tallfestet krav til leveringskvalitet, men i Leveringskvalitetsforskriften fremkommer det at behovet for elektrisitet indikerer hva som er tilfredsstillende leveringskvalitet.

Ut i fra dette studiet har NAT og HRO vist seg å være interessante teorier for å undersøke hvordan nettselskaper kan opprettholde en pålitelig strømlevering. Mens NAT ser på hvordan systemegenskaper utgjør sårbarheter, har HRO som formål å bygge en robust organisasjon. Imidlertid har HRM også vist seg hensiktsmessig da det gir en alternativ tilnærming til pålitelighet. High reliability management og reliability professionals betraktes som relevante begreper overført til en norsk kontekst. Etersom nettselskapet skal sørge for at alle brukerne i konsesjonsområdet mottar strøm, er det nødvendig med en høypålitelig drift av kraftnettet og at det er fokus på de personene som drifter nettet. Her finner man et viktig sammenheng mellom mennesker og teknologi.

En følge av at kraftinfrastrukturen har blitt tettere koblet og mer kompleks er blant annet at kraftforsyningsanlegg blir fjernstyrt fra nettselskapers kontrollrom. Her kommer reliability professionals inn i bildet. Dette begrepet vil være hensiktsmessig å bruke ved omtale av

operatørene på nettsentralen, ledere og annet personell i nettseksjonen da det har vist seg at de utgjør en sentral rolle for høypålitelig styring og drift av nettet. Det er operatørene på kontrollrommet som har ansvar for kontinuerlig overvåking og drift av transmisjons- og distribusjonsnettet. Ved daglig drift innebærer dette prosedyrer og rutiner, men når det skjer uønskede hendelser er nettselskapets evne til å håndtere hendelser viktig. Ut i fra forventninger har det blitt utarbeidet en beredskapsplan og dette er et sentralt verktøy for håndtering av hendelser. Det kan imidlertid oppstå situasjoner hvor man må handle utover beredskapsplanen, i slike tilfeller vil operatørens kognitive ferdigheter og erfaringer bidra til en tilfredsstillende håndtering i sanntid. Sett i lys av NAT kan kraftforsyningen betraktes som høyrisikoteknologi da det er tett koblete og komplekse system, og i så måte blir de mer sårbar. Derimot kan en slik kompleksitet ha en positiv funksjon, forutsatt at operatørene har en god forståelse og at de evner å se kraftnettet i helhet. Det innebærer blant annet at de kan håndtere hendelser i sanntid ved å improvisere, men samtidig er bevisst på hvilke følger det kan medføre. For at nettselskaper skal få ny kunnskap om farer og feil bør alle hendelser som oppstår i nettet registreres, slik at de har mulighet til å diskutere hendelsene i ettertid, samt det danner et kunnskapsgrunnlag for tolkning av fremtidige hendelser.

Studiet har belyst organisatoriske og menneskelige faktorer som må være tilstede ved drift av kraftnett fra kontrollrom. Ved å ha fokus på karakteristikker ved høypålitelige organisasjoner og bruke mindfulness som et verktøy kan man oppnå en høypålitelig strømlevering. Samhandling og god kommunikasjon mellom operatørene på kontrollrommet og mellom kontrollrommet og andre ansatte på nettseksjonen har vist seg å være sentralt, eksempelvis ved at de kan rådføre seg med hverandre. De ansatte ved nettseksjonen sine kognitive ferdigheter og erfaring, kontinuerlig stimuleres gjennom øvelser, evaluering, scenariobygging og faglige diskusjoner.

7.1 Videre forskning

En slik studie vil få mer dybde ved å inkludere et teknisk aspekt, eksempelvis ved å undersøke sårbarhet knyttet til kraftnettet og IKT-systemer. Det vil også være hensiktsmessig å ta med flere ytre faktorer, som for eksempel endringer i kraftmarkedet og etterspørsel og behov for strøm. Etersom dette studiet kun har tatt utgangspunkt i ett nettselskap, kan det være hensiktsmessig å undersøke andre nettselskapers forutsetninger for høypålitelig strømlevering og drift fra kontroll. Dette kan bidra til en bredere forståelse av kontrollrommet sin rolle knyttet opp mot høypålitelig kraftlevering.

8 REFERANSER

Almklov, P.G., Antonsen, S, Fenstad, J. (2011). *NPM, kritiske infrastrukturer og samfunnssikkerhet*. Hentet fra

<https://samforsk.no/SiteAssets/Sider/publikasjoner/NPM%20kritisk%20infrastruktur%202%20UTGAVE%20TRYKKERIET%20180211.pdf>

Almklov, P.G., Fenstad, J.S. & Røstum, J. (2011). *Offentlige etaters rolle i å sikre robusthet i komplekst organiserte og tett koblede infrastrukturekter. Notat om gjennomføring med funn og ideer for videre forskning*. Hentet fra <http://samforsk2.no/oer/docs/SluttrapportOER.pdf>

Aven, T., Boyesen, M., Njå, O., Olsen, K.H. & Sandve, K. (2004). *Samfunnssikkerhet*. Oslo: Universitetsforlaget

Beredskapsforskriften (2012). Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (*beredskapsforskriften*). Hentet fra

<https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157?q=Beredskapsforskriften>

Blaikie, N. (2010). *Designing Social Research*. Malden: Polity Press

Dalland, O. (2000). *Metode og oppgaveskriving for studenter* (3. utg.). Oslo: Gyldendal akademisk

Danermark, B., Ekström, M., Jakobson, L. & Karlsen, J.C. (2002). *Explaining Society: An Introduction to Critical Realism in the Social Sciences*. New York: Routledge

Direktoratet for samfunnssikkerhet og beredskap (DSB) (2012). *Sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner – modell for overordnet risikostyring (KIKS-prosjektet – 1. delrapport)*. Hentet 01.10.16 fra

<https://www.dsb.no/rapporter-og-evalueringer/sikkerhet-i-kritisk-infrastruktur---delrapport-1/>

Direktoratet for samfunnssikkerhet og beredskap (DSB) (2016). *Samfunnets kritiske funksjoner. Hvilken funksjonsevne må samfunnet opprettholde til enhver tid? Versjon 1.0.*

Hentet 15.05.17 fra https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-2_januar.pdf

Engen, O.A.H., Kruke, B.I, Lindøe, P.H., Olsen, K.H., Olsen, O.E. & Pettersen, K.A. (2016). *Perspektiver på samfunnsikkerhet*. Oslo: Cappelen Damm

Forskrift om systemansvaret i kraftsystemet (2002). *Forskrift om systemansvaret i kraftsystemet*. Hentet fra <https://lovdata.no/dokument/SF/forskrift/2002-05-07-448>

Fridheim, H., Hagen, J. & Henriksen, S. (2001). *En sårbar kraftforsyning - Sluttrapport etter BAS3 (FFI/Rapport-2001/02381)*. Kjeller: FFI

Grennes, T. (2012). *Hvordan kan du vite om noe er sant?*. Latvia: Cappelen Damm akademisk

Hale, A. & Heijer, T. (2012). *Defining Resilience*. I E. Hollnagel, D.D. Woods & N.G. Leveson (red.), *Resilience Engineering: Concepts and Precepts*. Ashgate

Halvorsen, K. (2008). *Å forske på samfunnet. En innføring i samfunnsvitenskapelig metode*. Oslo: Cappelen akademisk forlag

Hansen, H., Eggum, E., Ånestad, A. & Aabakken, C. (2017). *Avbrottsstatistikk 2016 (NVE Rapport nr. 43-2017)*. Hentet fra http://publikasjoner.nve.no/rapport/2017/rapport2017_43.pdf

Jacobsen, D.I. (2015). *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode (3. utgave)*. Oslo: Cappelen Damm AS

Kvale, S. & Brinkmann, S. (2015). *Det kvalitative forskningsintervju (3. utgave)*. Oslo: Gyldendal Norsk Forlag AS

LaPorte, T. & Consolini, P.M. (1991). *Working in Practice but Not in Theory: Theroretical Challenges of "High-Reliability Organizations"*. *Journal of Public Administration Research and Theory: J-PART*, Vol. 1, No. 1. (Jan., 1991), s. 19-48

Leveringskvalitetsforskriften (2014). *Forskrift om leveringskvalitet i kraftsystemet*. Hentet fra <https://lovdata.no/dokument/SF/forskrift/2004-11-30-1557>

Losnegård, G. (2013). *Norske ulykker og katastrofar*. Skald

Lynggaard, K. (2012). *Dokumentanalyse*. I S. Brinkmann & L. Tanggard (red.), *Kvalitative metoder. Empiri og teoriutvikling* (s. 153-170). Oslo: Gyldendal Akademisk

Meld. St. 25 (2015-2016). (2016). *Kraft til endring. Energipolitikken mot 2030*. Hentet 20.12.2016 fra <https://www.regjeringen.no/no/dokumenter/meld.-st.-25-20152016/id2482952/sec1>

Meld. St. 29 (2011-2012). (2012). *Samfunnssikkerhet*. Hentet 08.05.2017 fra <https://www.regjeringen.no/contentassets/bc5cbb3720b14709a6bda1a175dc0f12/no/pdfs/stm201120120029000dddpdfs.pdf>

Norconsult (2014). *Langvarig strømbrudd i Lofoten. Sårbarhets- og konsekvensvurdering*. Hentet fra https://www.fylkesmannen.no/Images/Bilder%20FMNO/Samfunnssikkerhet/Rapport_langvarig%20strømbrudd%20Lofoten_11FEB14_endelig.pdf

NOU 2006:6 (2006). *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner*. Oslo: Departementenes servicesenter, Informasjonsforvaltning

NVE (2013). *Veiledning til forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (Veileder nr. 1-2013)*. Hentet fra http://publikasjoner.nve.no/veileder/2013/veileder2013_01.pdf

NVE (2015). *Teknologiskifte i energiforsyningen. Studie om muligheter og sårbarhet. Rapport nr. 118-2015*. Hentet fra http://publikasjoner.nve.no/rapport/2015/rapport2015_118.pdf

NVE (2016). *Veileder til leveringskvalitetsforskriften (Veileder nr. 4-2016)*. Hentet fra http://publikasjoner.nve.no/veileder/2016/veileder2016_04.pdf

NVE (2016, 02.08). *Nett*. Hentet 30.05.2017, fra <https://www.nve.no/energiforsyning-og-konsesjon/nett/>

NVE (2016, 24.02). *Energiforsyningsberedskap*. Hentet 02.02.19 fra <https://www.nve.no/damsikkerhet-og-energiforsyningsberedskap/energiforsyningsberedskap/>

NVE (2016, 15.04). *Kraftforsyningens beredskapsorganisasjon (KBO)*. Hentet 07.02.17 fra <https://www.nve.no/damsikkerhet-og-energiforsyningsberedskap/energiforsyningsberedskap/organisering-av-energiforsyningsberedskap/kraftforsyningens-beredskapsorganisasjon-kbo/>

NVE (2017, 19.01). *Kraftsituasjonen, 4. kvartal og året 2016*. Hentet 13.02.17 fra <https://www.nve.no/Media/5248/q42016.pdf>

NVE (2017, 23.02 a). *Avbruddsstatistikk*. Hentet 03.03.17, fra <https://www.nve.no/elmarkedstilsynet-marked-og-monopol/nettjenester/leveringskvalitet/leveringspalitelighet/avbruddsstatistikk/>

NVE (2017, 23.02 b). *Leveringspalitelighet*. Hentet 03.03.17, fra <https://www.nve.no/elmarkedstilsynet-marked-og-monopol/nettjenester/leveringskvalitet/leveringspalitelighet/>

NVE & Proactima (2010). *Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen. Veileder nr: 2-2010*. Hentet fra http://publikasjoner.nve.no/veileder/2010/veileder2010_02.pdf

Perrow, C. (1999). *Normal Accidents: Living with High Risk Technologies*. Princeton University Press

Perrow, C. (2004). *The Next Catastrophe. Reducing Our Vulnerabilities to Natural, Industrial and Terrorist Disasters*. Princeton University Press

Roe, E. & Schulman, R. (2008). *High Reliability Management. Operating on the Edge*. California: Stanford University Press

Roe, E. & Schulman, P.R. (2016). *Reliability and Risk: The Challenge of Managing Interconnected Infrastructures*. California: Stanford University Press

Rosness, R., Skjerve, A.B.M., Alteren, B., Berg, Ø., Bye, A., Hauge, S., Seim, L.Å., Sklet, S., Tveiten, C.K. & Aase, K. (2002). *Feiltoleranse, barriere og sårbarhet (SINTEF rapport STF38 A03404)*. Hentet fra http://www.forskningsradet.no/csstorage/vedlegg/153537_tema2.pdf

Schulman, P., Roe, E., van Eten, M. & de Bruijne, M. (2004). *Journal of Contingencies and Crisis Management*, 12(1): 14-28 (March 2004). *High Reliability and the Management of Critical Infrastructures*. Hentet fra http://onlinelibrary.wiley.com/doi/10.1111/j.0966-0879.2004.01201003.x/epdf?r3_referer=wol&tracking_action=preview_click&show_checkout=1&purchase_referrer=www.google.no&purchase_site_license=LICENSE_DENIED

Statnett (2016, 04.08). *Nettdrift er en balansekunst*. Hentet 02.02.17 fra <http://www.statnett.no/Samfunnsoppdrag/vart-samfunnsoppdrag/Nettdrift-er-en-balansekunst/>

Tanggaard, L. & Brinkmann, S. (2012). *Intervjuet*. I S. Brinkmann & L. Tanggaard (red.), *Kvalitative metoder. Empiri og teoriutvikling* (s. 17-45). Oslo: Gyldendal Akademisk

Thagaard, T. (2013). *Systematikk og innlevelse (4. utgave)*. Bergen: Fagbokforlaget

Weick, K.E. & Sutcliffe, K.M. (2007). *Managing the Unexpected. Resilient Performance in an Age of Uncertainty (2. edt.)*. San Fransisco: Jossey-Bass

Weick, K.E., Sutcliffe, K. & Obstfeld, D. (1999). *Organizing for High Reliability: Process of Collective Mindfulness*. R.S. Sutton and B.M. Staw (red.), *Research in Organizational Behavior*, Volume 1 (Stanford: Jai Press, 1999), s. 81–123. Hentet 02.11.16 fra <http://www.archwoodside.com/wp-content/uploads/2015/09/Weick-Organizing-for-High-Reliability.pdf>

Woods, D.D. (2012). *Essential Characteristics of Resilience*. I E. Hollnagel, D.D. Woods & N.G. Leveson (red.), *Resilience Engineering: Concepts and Precepts* (s. ??). Ashgate

Woods, D.D. & Hollnagel, E. (2012). *Prologue: Resilience Engineering Concepts*. I E. Hollnagel, D.D. Woods & N.G. Leveson (red.), *Resilience Engineering: Concepts and Precepts* (s. 1-6). Ashgate

9 VEDLEGG

Vedlegg 1 Intervjuguide

Kjønn:

Alder:

Utdanning:

Erfaring:

Samtykker til lydopptak: Ja / Nei

Daglig drift

- Hvordan ser en normal arbeidsdag ut?
- Kan du nevne typiske hendelser som kan være forstyrrende, men ikke nødvendigvis kritisk, for normaldrift?
- Hvor ofte skjer disse hendelsene i gjennomsnitt av en måned?
- Hva innebærer standard prosedyrer i normal tilstand?

Beredskap

- Hvordan er prosedyrene dersom det oppdages feil og avvik?
- Kan handlingene etter uønskede hendelser kategoriseres?
- Hvordan forbereder dere dere dersom det er forventet å gå inn i full beredskap i løpet av få dager?
- Kan du nevne typiske hendelser som anses som kritiske og som medfører endring i beredskapsnivå?
- Hvordan oppleves overgangene mellom de ulike beredskapsnivåene?
- Når blir relevante aktører kontaktet?
- Hvordan koordineres relevante aktører ved beredskap?
- Mottas det tilbakemelding etter endt beredskap?

Beslutninger

- Hvordan er ansvarsfordelingen blant dere som jobber på kontrollrommet?
- Hvem tar avgjørelser i normaltilstand?
- Hvem tar avgjørelser i beredskapstilstand?