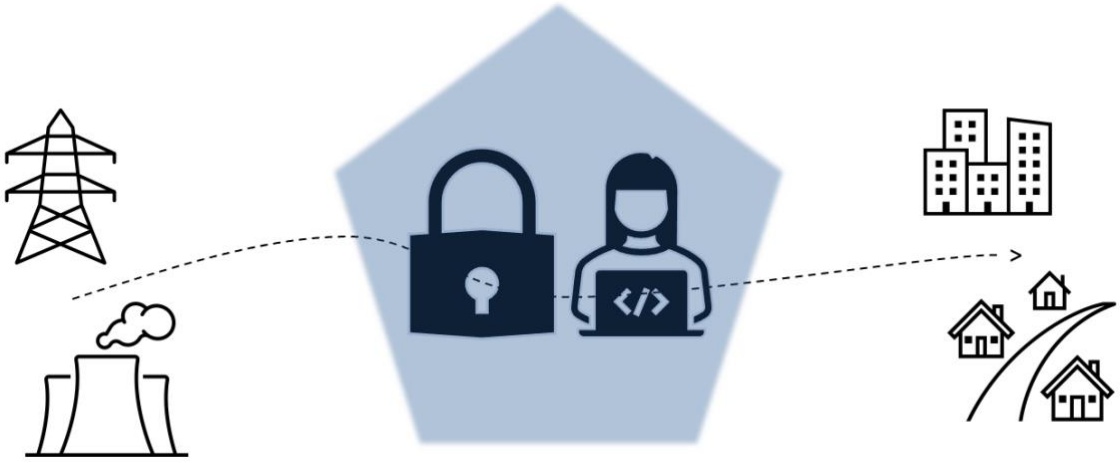
Resiliens i driftskontinuitet - med fokus på cyberangrep i kraftforsyningen

Carina Karlsen og Kristine Pettersen Kofoed

Hvordan kan prinsippene for «Resilience Engineering» og opprettholdelsen av driftskontinuitet benyttes til å forbedre forsyningssikkerheten hos aktører i kraftforsyningen på et systemnivå?



Masteroppgave i samfunnssikkerhet
vår 2023

DET TEKNISK-NATURVITENSKAPELIGE FAKULTETET

MASTEROPPGAVE

Studieprogram: Master i samfunnssikkerhet	Vår semesteret, 2023 Åpen / ~~Konfidensiell~~
Forfatter: Carina Karlsen og Kristine Pettersen Kofoed	
Veileder: Riana Steen **Fagansvarlig ved UiS**: Ole Andreas Engen	
Tittel på oppgaven: Resiliens i driftskontinuitet **Engelsk tittel:** Business continuity resilience	
Studiepoeng: 30	
Emneord: Resilience Engineering, Business continuity/Driftskontinuitet, Viable system model, Kraftforsyning, Cyberangrep, Beredskap, Kontinuitetsplaner	**Sidetall**: 110 Stavanger, 15.06.2023

Sammendrag

Kraftforsyningen i Norge er en kritisk samfunnsfunksjon som opplever en økende grad av digitalisering i sin kritiske infrastruktur. Dagens trusselbilde tilsier at kraftforsyningen, i likhet med andre kritiske samfunnsfunksjoner og infrastrukturer, er spesielt sårbare i møte med cybertrusler. Slike trusler er noe som virksomheter i kraftsektoren burde ha tatt en vurdering på både i henhold til lovkrav og dagens beredskapssituasjon i sektoren. Målet med oppgaven har vært å se hvordan virksomheter, henholdsvis to nettselskaper og to produksjonsselskaper, arbeider med prinsippene i Resilience Engineering (RE) og opprettholde driftskontinuitet gjennom et eventuelt cyberangrep på sektorens digitale systemer (SCADA). Oppgaven har dermed, gjennom et spesifikt scenario om cyberangrep, svart på problemstillingen «hvordan kan prinsippene for Resilience Engineering og opprettholdelsen av driftskontinuitet benyttes til å forbedre forsyningssikkerheten hos aktører i kraftforsyningen på et systemnivå?». Problemstillingen har blitt sett nærmere på gjennom RE-prinsippene: overvåke, forutse, respondere og lære, samt en forståelse av driftskontinuitet.

Vi har gjennomført en «Mixed Methods Approach» (MMA) hvor vi har benyttet oss av dokumentanalyse, gruppeintervjuer og en spørreundersøkelse. Vi har brukt Viable System Model (VSM) som et metodisk rammeverk for oppgaven for å kartlegge kraftforsyningen som helhetlig levedyktig system. Spørreundersøkelsen har vært en kartlegging av virksomhetenes generelle resiliens og er utformet ved hjelp av Resilience Analysis Grid (RAG). Gjennom gruppeintervjuene har vi undersøkt hvor resiliente virksomhetene er i møte med scenarioet vi har beskrevet og sett på dette opp mot resultatene fra spørreundersøkelsen.

Oppgavens hovedfunn har blitt presentert som tre diagnostiske problem utarbeidet ved hjelp av VSM. Det blir presentert løsninger på problemene gjennom oppgavens teoretiske grunnlag. Det første diagnostiske problemet omhandler mangelfull koordinering og samarbeid mellom nett- og produksjonsselskaper. Det andre diagnostiske problemet viser til en manglende kunnskap og erfaring rundt cyberangrep. Det tredje diagnostiske problemet baserer seg på nett- og produksjonsselskapenes prioriteringer av produksjonsmål vs. sikkerhetsmål. Forslagene viser til at virksomhetene burde ta i bruk prinsippene i RE og driftskontinuitet for å bli mer resiliente i møte med cybertrusler. I praksis ser vi at RE prinsippene kan anvendes i en praktisk tilnærming for å gjøre virksomhetene mer resiliente. Det vil nærmere bety at virksomhetene klarer å justere sine funksjoner både før, under og etter forstyrrelser og på den måten klarer å opprettholde nødvendige funksjoner i koordineringer med nødvendige aktører.

Abstract

The Norwegian power supply is a crucial component of a society where digitalization is becoming more pervasive in critical infrastructure. The threat image for today indicates how vulnerable the power supply is to cyber threats, along with other critical functions of society and infrastructures. Actors in the power sector should have evaluated these dangers considering the sector's existing state of emergency situation as well as statutory obligations. The thesis's objective was to determine how the actors, two network companies and two production companies, utilize the principles of Resilience Engineering (RE), and maintain business continuity trough a potential cyberattack on the sector’s digital system (SCADA). Therefore, the purpose of this thesis was to address the following problem statement, "How can the principles of Resilience Engineering and business continuity of operations be used to strengthen the continuity of the (power) supply at a systemic level?", utilizing the description of a cyberattack scenario. The principles of RE: monitor, anticipate, respond, and learn, have been used to examine the problem in greater detail along with knowledge of business continuity.

Using a "Mixed Methods Approach" (MMA), we conducted a survey, group interviews, and a document analysis. As a methodological framework for the purpose of mapping the power supply as a viable system, we utilized the Viable system model (VSM). The survey was created with the guidance of Resilience analysis grid (RAG) and served as a mapping of the actors' overall resilience. We have looked at the actors' resilience considering the scenario we have outlined through group interviews, taking the survey results into consideration.

Three diagnostic problems have been described applying the VSM to represent the findings. The theoretical underpinning of the thesis provides solutions to the issues. The first diagnostic problem relates to an inadequate coordination and cooperation within the network and production companies. Lack of information and experience about cyber threats is the subject of the second diagnostic problem. The third diagnostic problem entails the companies’ prioritization of production measures above safety measures. Recommendations suggest that for companies to be more resilient when faced with cyber threats, they should implement the RE and business continuity principles. The application of the RE principles in practice can be linked to an increase of corporate resilience. This indicates that the actors have the flexibility to modify their functions before, during, and after disturbances and thus carry out the required tasks in collaboration with the required parties.

Forord

Med dette avslutter vi to fantastiske år som studenter på master i samfunnssikkerhet ved Universitetet i Stavanger. Det å skrive masteroppgave sammen med hverandre har vært svært spennende, lærerikt og ikke minst betryggende. Vi har fått en enorm faglig mulighet til å lære om noe vi ikke hadde noe spesiell kunnskap om fra tidligere fag, samtidig som vi har fått knyttet det til fagkunnskaper vi har tilegnet oss underveis i studiet. Vi vil starte med å takke hverandre for x-antall timer vi har lagt ned i denne masteroppgaven og et bra samarbeid. Vi har i denne prosessen utnyttet hverandres styrker og spilt hverandre gode, og det er vi takknemlig for.

En stor takk til de fire involverte virksomhetene og deres tilhørende informanter som har gitt oss muligheten til å samle inn empiri. Uten dere hadde ikke denne oppgaven blitt til. Vi vil rette en stor takk til Safetec Nordic AS for støtte og tips til oppgaven, spesielt i henhold til utformingen av spørreundersøkelsen og faglig sparring sommeren 2022 angående tema. Det har vært til stor hjelp. Vi vil også takke Geir Ingvaldsen som vi, gjennom vår veileder, har tatt stor inspirasjon fra i utformingen av vår masteroppgave. Vi vil også takke våre flotte studievenner som har stått i den samme prosessen, men som også har vært svært gode støttespiller på flere plan. Uten dere hadde ikke disse to årene blitt det samme. Dere vet hvem dere er. En stor takk må også rettes til familiene våre som har støttet oss på alle plan gjennom skolegangen.

Sist, men ikke minst, en stor takk til vår fantastiske veileder, Riana Steen, for hennes engasjement, enorme kunnskap og tro på vår oppgave. Din konstruktive kritikk, gode tilbakemeldinger og faglige engasjement har vært helt avgjørende for oss.

Stavanger 2023

Carina Karlsen, Kristine Pettersen Kofoed

Forkortelser

DSB	Direktoratet for samfunnssikkerhet og beredskap
KBO	Kraftforsyningens beredskapsorganisasjon
KDS	Kraftforsyningens distriktssjefer
NFD	Nærings- og fiskeridepartementet
NSM	Nasjonal sikkerhetsmyndighet
NVE	Norges vassdrag og energidirektorat
OED	Olje- og energidirektoratet
PST	Politiets sikkerhetstjeneste
RAG	Resilience Analysis Grid
RE	Resilience Engineering
SC	Scenario
SCADA	Supervisory Control and Data Acquisition
SOC	Security Operations Center
VSM	Viable System Model

Definisjoner og begrep

Beredskap	Planlegging og forberedelse av tiltak for å håndtere uønskede hendelser på best mulig måte (NOU 2006:6, s. 38).
Driftskontinuitet	Brukes synonymt med «Business continuity». Kan forståes som evnen en virksomhet har til å opprettholde leveranser av produkter og tjenester innenfor akseptable tidsrammer ved forhåndsdefinert kapasitet under forstyrrelser (Standard Norge, 2019, s.2).
Cyberangrep	Forstås her som et angrep som har til hensikt å skade eller skape forstyrrelser i et datasystem eller en digital infrastruktur.
Forsyningssikkerhet	Kraftsystemets evne til å kontinuerlig levere elektrisk kraft av en gitt kvalitet til sluttbrukere. Sees på som et samlebegrep som omfatter driftssikkerhet, energisikkerhet og effektsikkerhet (NOU, 2022:6, s. 85).
Kontinuitetsplan	Plan som del av kontinuitetsplanlegging blir brukt som metode for å planlegge bortfall i innsatsfaktorer (varer, tjenester og arbeidskraft) DSB (2020).
Kraftforsyning	Alle aktører i Norge som driver med produksjon og distribusjon av kraft og deres tilhørende underkomponenter.
Kritisk infrastruktur	De systemer og anlegg som er nødvendig for å kunne ivareta samfunnets behov for elektrisk energi til husholdning, produksjon, oppvarmning, transport m.m., og fjernvarme der anlegg er utbygd (DSB, 2016; Meld.St.5 (2020-2021)).
Kritisk samfunnsfunksjon	De funksjoner som er nødvendige for å ivareta befolkningens og samfunnets grunnleggende behov og befolkningens trygghetsfølelse. Grunnleggende behov er definert som mat, vann, varme, trygghet og lignende (Meld.St.5 (2020-2021), s. 11).
Resiliens	Den iboende evnen i et system til å justere sine funksjoner i forkant av, under, eller etter endringer og forstyrrelser, slik at det kan opprettholde nødvendige funksjoner under både forventede og uforventede forhold (Hollnagel 2011, s. 275).
Risiko	En kombinasjon av trussel, sårbarhet og verdi (trefaktormodellen).

Sabotasje	Sabotasje forståes her som forståelse av *cybersabotasje* som åpenbare forstyrrelser i digitale systemer med en bakenforliggende ondsinnet hensikt om å påvirke verdiene til trusselmålet (Martin, 2019).
Sårbarhet	Manglende evne hos et analyseobjekt til å motstå virkninger av en uønsket hendelse og til å gjenopprette sin tilstand eller funksjon etter hendelsen. Manglende evne relateres til vår usikkerhet om fremtiden (Njå et al., 2020, s. 52).
Trefaktormodellen	Modell som kan benyttes til risikovurderinger for ondsinnede/tilsiktede handlinger (Njå et al., 2020).
Trussel	Vurdering av relevante trusselaktører og deres kapasitet (gjennomføringsevne) og intensjon (konkrete planer om å gjennomføre angrep) (Martin, 2019, s. 69).
Trusselbilde	Uttrykk som brukes i oppgaven for å henvise til de faktorer og situasjoner som er med på å beskrive i hvilken grad kraftsektoren er utsatt for trusler i nå- og framtid.
Usikkerhet	Et uttrykk for tvil, eller manglende kunnskap om kjente og ukjente forhold. Må sees i sammenheng med tidsperspektivene nåtid, fortid og fremtid (Njå et al., 2020).
Verdi	Subjektivt uttrykk som vil variere fra virksomhet til virksomhet. Virksomheter må kartlegge og definere sine verdier for å identifisere konsekvenser av uønskede handlinger. Sikkerhet må baseres på de verdiene som virksomheter verdsetter (Busmundrud et al., 2015; Jore, 2015).

Oversikt over tabeller og figurer

Figurer

Tabeller

Innholdsfortegnelse

1. Innledning

Formålet med oppgaven er å se hvordan Resilience Engineering (RE) og opprettholdelsen av driftskontinuitet kan benyttes for å styrke forsyningssikkerheten hos aktører i kraftforsyningen. Her skal det sees nærmere på forsyning av elektrisk energi, altså strøm, fra produsenten til sluttbrukere. Nærmere bestemt kraftforsyningskjeden. Innenfor denne kjeden er hovedfokuset på produsenter og distribuenter av elektrisk energi, nemlig aktører innen nett- og produksjonsselskaper. Det skal utforskes hvordan koordineringen og samarbeidet mellom disse er i praksis, sett i sammenheng med prinsippene i RE og driftskontinuitet. Bakgrunnen for valget på kraftsektoren er at det er en kritisk samfunnsfunksjon, som omhandler det å ivareta befolkningens grunnleggende behov. I Melding til Stortinget nr. 5 (2020-2021) er kritisk samfunnsfunksjon definert som «de funksjoner som er nødvendige for å ivareta befolkningens og samfunnets grunnleggende behov og befolkningens trygghetsfølelse. Grunnleggende behov er definert som mat, vann, varme, trygghet og lignende» (s. 11). Sett i sammenheng med kraftsektoren består den av kritisk infrastruktur som kan forstås som de systemer og anlegg som er nødvendig for å kunne ivareta samfunnets behov for elektrisk energi til husholdning, produksjon, oppvarmning, transport m.m., og fjernvarme der anlegg er utbygd (DSB, 2016; Meld.St.5 (2020-2021)). Ved å inkludere aktører fra den kritiske samfunnsfunksjonen og dens tilhørende kritiske infrastruktur, vil vi se hvordan et fokus på oppgavens teoretiske grunnlag kan lede til en forbedret forsyningssikkerhet. I forhold til dette er det relevant å etablere en forståelse på hva vi mener med forsyningssikkerhet. I henhold til denne oppgaven kan forsyningssikkerhet forstås som kraftsystemets evne til å kontinuerlig levere elektrisk kraft av en gitt kvalitet til sluttbrukere, og det sees på som et samlebegrep som omfatter driftssikkerhet, energisikkerhet og effektsikkerhet (NOU, 2022:6, s. 85).

I sammenheng med denne oppgaven er det to begreper som er svært relevante. Det første er resiliens som kan forstås ifølge Hollnagel (2011) som “den iboende evnen i et system til å justere sine funksjoner i forkant av, under, eller etter endringer og forstyrrelser, slik at det kan opprettholde nødvendige funksjoner under både forventede og uforventede forhold" (s. 275). i forhold til dette skal sees nærmere på prinsippene i RE, som er overvåke, forutse, respondere og lære. Det andre begrepet er driftskontinuitet, og kan forstås som “capability of an organization to continue the delivery of product and services within acceptable time frames at predefined capacity during a disruption” (Norsk Standard, 2019, s. 2). Begge disse konseptene kan sies å være beslektet med tanke på innhold. Dette kan sees i sammenheng med at i resiliens er fokuset både på systemets evne til å motstå forstyrrelser og opprettholde og justere sine

funksjoner i forkant av, under og etter endringer og forstyrrelser. Sett i sammenheng med driftskontinuitet som hovedsakelig fokuserer på det samme, med fokus på under selve forstyrrelsen og endringen. Ved å inkludere begge konseptene i utviklingen av problemsstilling er disse i hovedfokus når vi skal se nærmere på kraftforsyningskjeden og dens aktører.

1.1 Bakgrunn for valg av tema

Bakgrunnen for valget på kraftsektoren er dagens situasjon i Norge og Europa. Kraftforsyning er en kritisk samfunnsfunksjon og en viktig energikilde for alle som bor i Norge og Europa. Norge hadde en økning på 30% i eksporten av kraft i 2021, som gjør Norge til et viktig land når det kommer til eksport av kraft til andre europeiske land (Aanensen, 2022). Videre er viktige samfunnsfunksjoner og kritiske samfunnsoppgaver avhengige av fungerende system med pålitelig energiforsyning. I Norge er elektrisitetens andel av energiforbruket større enn hos andre land, som gjør oss sårbare på grunn av avhengigheten (DSB, 2016). På bakgrunn av dette stilles det store krav til forsyningssikkerheten. På denne måten er flere krav nedfelt i relevant lovverk som skal sikre beredskap og sikkerhet i kraftforsyningen (Energiloven, 1990; Kraftberedskapsforskriften, 2012). Med tanke på dagens endrede trusselbilde, hvor digitale trusler har blitt en større andel av maktmidlene som brukes i blant annet krig og konflikt, er beskyttelse av digitale verdier viktigere enn før (Meld. St. 25 (2015-2016)). NSMs sikkerhetsfaglige råd (2023b) kritiserer den norske trusselforståelsen, hvorav kraftsektorens infrastruktur regnes som utsatt for fremmed staters etterretning. Her påpeker NSM (2023b) at denne typen infrastruktur med særlig sikkerhetspolitisk betydning ikke har blitt nok prioritert i nasjonal verdikartlegging og ikke er godt nok sikret i forhold til dagens trusler. Videre påpeker NOU (2023:3) at endringer i trusselbildet for energiinfrastruktur fører med seg utfordringer for driftssikkerheten. Desto viktigere er det å beskytte disse digitale verdiene fra trusselaktører for en forbedret forsyningssikkerhet.

Planlegging er nødvendig i forhold til driften for å sikre forsyningssikkerheten når uønskede hendelser inntreffer. Hvis tilførselen av strøm ikke kommer frem til hvor den er ment, kan det i ett «worst case»-scenario føre til skader på verdier, som liv og helse og infrastruktur. En uønsket hendelse kan ifølge Engen et al. (2021) forstås som «en hendelse som har forårsaket eller kunne ha forårsaket ulike typer skader på sentrale verdier» (s. 302). I sammenheng med verdiene i kraftforsyningen kan sentrale verdier blant annet være: liv og helse, infrastruktur og økonomi. Kraftforsyningen består av et komplekst systemdrift- og aktørbilde, videre har det også blitt en økt digitalisering i kraftforsyningen. Denne integreringen av teknologi i fysisk infrastruktur kan kalles cyberfysiske systemer (Colabianchi et al., 2021; Rinaldi et al., 2001).

Kraftforsyningen kan dermed sees på som et cyberfysisk system i sin helhet og dens tilhørende infrastruktur. Den gjensidige avhengigheten mellom kraftforsyningen og dens aktører gjør oss sårbare i situasjoner ved lengre avbrudd av strøm. På bakgrunn av dette er det i oppgaven valgt å fokusere på ett scenario, nemlig cyberangrep mot Supervisory Control and Data Acquisition - systemet (SCADA-systemet) (nærmere beskrivelse i 1.2). Kort fortalt er dette systemet det digitale systemet som brukes i kraftforsyningen, også kalt driftskontrollsystem. Sentrale trusselvurderinger fra 2023 påpeker usikkerheten rundt og hyppigheten av cyberangrep mot kritisk infrastruktur fra ulike trusselaktører (Kripos, 2023; NSM, 2023a; PST, 2023). Dette er et område som må prioriteres i fremtidige beredskapsøvelser og gjennom oppdatering av planverk, og kraftsektoren er ikke et unntak. Dagens trusselbilde påvirker kraftsektoren på forskjellige måter, og det å holde seg oppdaterte på dagens trusler er essensielt i arbeidet med forsyningssikkerhet. Med dagens trusselbilde i denne oppgaven viser vi til den pågående trusselen fra russisk etterretning og andre trusselaktører som er ute etter å skade kritisk infrastruktur, i kjølvannet av krigen i Ukraina (PST, 2023). Spesielt i sammenheng med digitale trusler og sabotasje av digitale verdier i den kritiske infrastrukturen. Denne forståelsen av trusselbilde henger sammen med definisjonen av risikobegrepet, sett i sammenheng med trefaktormodellen (se delkapittel 3.1.).

Risiko knyttet til driftskontinuitet har følge Eriksen et al. (2021) ikke vært vanlig praksis å bruke som en del av risikoanalysene som virksomheter utfører. Dette til tross for at beredskapssituasjoner kan påvirke virksomhetenes drift ved å begrense tjenesteyting og produksjon. Eriksen et al. (2021) skriver videre at det ikke er vanlig praksis at driftskontinuitet i form av kontinuitetsplaner o.l. blir inkludert som en del av beredskapsplanverket. På bakgrunn av denne påstanden har det vært et ønske om å se nærmere på hvorvidt driftskontinuitet er noe virksomheter i kraftsektoren arbeider med. I sammenheng med dette kan det sees på som svært viktig å arbeide med driftskontinuitet, ettersom det kan medføre store konsekvenser for virksomhetene å neglisjere dette arbeidet. Problematisk blir det spesielt ved lengre beredskapshendelser hvor man må sikre driften gjennom produksjon og opprettholdelse av nødvendige leveranser. Arbeidet med dette kan også påvirke forsyningssikkerheten i en positiv retning, som vil bli vist i denne oppgaven.

1.2 Problemsstilling og forskningsspørsmål

Denne oppgaven har følgende problemsstilling:

Hvordan kan prinsippene for «Resilience Engineering» og opprettholdelsen av driftskontinuitet benyttes til å forbedre forsyningssikkerheten hos aktører i kraftforsyningen på et systemnivå?

For å kunne besvare problemsstillingen vil vi fokusere på ett scenario (SC):

Hendelseskategori: Sabotasje

SC: Cyberangrep på SCADA-systemet (gjelder både nett- og produksjonsselskap)

Beskrivelse av scenarioet: Dette er et «worst-case»-scenario. Inntrenger har klart å komme seg inn på SCADA-systemet gjennom ulike barrierer, og på den måten klart å plassere skadevare på systemet. Dette har inntrengeren gjort med hensikt om å ta over kontrollen og lammet systemet. På den måten har inntrengeren klart å ta over systemet for å styre det. Dette anses å være en langvarig beredskapshendelse (ca. 24t).

Overnevnte problemsstilling vil utredes ved å se på følgende forskningsspørsmål:

FS1: På hvilken måte er nett- og produksjonsselskapene avhengige av hverandre og eksterne aktører i arbeidet med cybersikkerhet?

FS2: Hvordan arbeider nett- og produksjonsselskapene med prinsippene i RE, sett opp mot SC?

FS3: Hvordan kan et fokus på driftskontinuitet og RE hos nett- og produksjonsselskapene være med på å forbedre forsyningssikkerheten i kraftsektoren?

Logikken bak å dele problemstillingen i tre forskningsspørsmål er å kunne dekke både realiteten, det vil si hvordan situasjonen er, samt utforske aktørenes tilpasningskapasitet i å imøtekomme utfordringer skissert i scenarioet. FS1 baserer seg på hvordan det virkelig bilde av hvordan den gjensidige avhengigheten er, det såkalte «sånn det er» (AS-IS). På den måten kan man enklere se hvor sårbare punkter befinner seg og på den måten gjøre hele systemet mer resilient. FS2 ser nærmere på hvordan de aktørene arbeider med prinsippene i RE, knyttet opp mot SC. Det er interessant å se hvordan nett- og produksjonsselskaper stiller seg til håndteringen av samme scenario, samt hvordan virksomhetene arbeider med prinsippene i RE. Videre vil FS3 knytte sammen de to forutgående forskningsspørsmålene og gir et svar på

problemsstillingen. Her vil tre diagnostiske problemer kartlegges og det vil bli foreslått løsninger på hvordan virksomhetene på et systemnivå kan bli mer resiliente i møte med cyber-relaterte trusler. Bakgrunnen for valget på ett scenario er tatt på bakgrunn av dagens trusselbilde og oppgavens tidsbegrensning. Valget har falt på en svært dagsrelevant trussel, som kan kategoriseres som sabotasje mot kritisk infrastruktur jf. kraftberedskapsforskriften §5-1 fjerde ledd. Sabotasje i sammenheng med denne oppgaven er basert på bakgrunn i beskrivelsen til Martin (2019) der cybersabotasje forstås som åpenbare forstyrrelser i digitale systemer med en bakenforliggende ondsinnet hensikt om å påvirke verdiene til trusselmålet. Vi får et klarere bilde på hvordan RE-prinsippene og opprettholdelsen av driftskontinuitet kan arbeides med ved å se på ett scenario, enn hvis vi skulle inkludert flere scenarioer. På den måten kan vi grundigere se hvordan det teoretiske rammeverket kan brukes i forhold til SC. Ved å gjøre dette kan vi få et overblikk over hvordan nett- og produksjonsselskapene arbeider med dette på et systemnivå.

1.3 Avgrensning

RE er et sikkerhetsperspektiv og representerer et større fagfelt. I denne oppgaven avgrenses RE til dens prinsipper ved å se nærmere på organisatorisk resiliens. På denne måten vil vi finne ut hvorvidt RE-prinsippene og opprettholdelsen av driftskontinuitet kan benyttes for å forbedre forsyningssikkerheten hos nett- og produksjonsselskaper i kraftforsyningen på et systemnivå. Vi vil undersøke hvorvidt det foregår en koordinering mellom de ulike aktørene i forsyningskjeden. Det valgte scenarioet er en tilsiktet uønsket hendelse som utgjør en security-risiko, mens RE ofte diskuteres i sammenheng med safety-risikoer. I denne oppgaven er ikke formålet å drøfte safety vs. security risikoer. Det skal redegjøres kort for forskjellen på safety og security i teorikapittelet, men ikke drøftes ytterliggere. Bakgrunnen for valget på en security-risiko er basert på dagens trusselbilde, som diskutert ovenfor. Fokuset i oppgaven er avgrenset på et overordnet systemnivå i lys av Viable system model (VSM) fra Beer (1984,1985). VSM er en modell som brukes for å se på hvordan systemer er levedyktige, altså hvordan systemer opprettholdes og vedlikeholdes over tid ved hjelp av systemer og sub-systemer. Denne modellen vil vi gå nærmere inn på i teorikapittelet 3.4 og satt i en kontekst i metodekapittel 4.2. Systemnivå i henhold til VSM kan sees i sammenheng med at det er basert på en systemisk diagnose av levedyktigheten til et system, som i denne oppgaven er kraftforsyningen, som og kan trekkes til å utforske systemets resiliente kapasitet (Pollock & Steen, 2021). De fire ulike virksomhetene som er inkludert i denne oppgaven er av ulik størrelse, men til felles består alle av ulike KBO-enheter som befinner seg under

kraftforsyningens beredskapsorganisasjon (KBO). KBO-enhetene har ansvar for å utføre oppgaver og plikter som følge av relevante regelverk (NVE, 2022a). Dette betyr at de har plikt til å sørge for et oppdatert planverk, sikringstiltak, iverksetter tiltak for å forebygge, håndtere og begrense virkningene av uønskede hendelser.

Empirien vil bestå av strukturerte gruppeintervjuer, spørreundersøkelse og dokumentanalyse. For å systematisere kraftforsyningskjeden, vil vi bruke VSM fra Beer (1984,1985). Når det kommer til gruppeintervjuene og spørreundersøkelsen vil vi få informanter fra to nettselskaper og to produksjonsselskaper. Alle virksomhetene får samme spørreundersøkelse, der hensikten er å kartlegge resiliens gjennom Resilience Analysis Grid (RAG) som er knyttet til RE. Spørsmålene i intervjuguiden er utviklet på bakgrunn RE- prinsippene og driftskontinuitet. Oppgaven har begrenset seg til et tidsintervall på dagens situasjon hos aktørene i kraftforsyningen, og hvordan deres arbeid med RE og driftskontinuitet kan forbedre forsyningssikkerhet i fremtiden.

1.4 Oppgavens utforming

Oppgaven er bygget opp av syv hovedkapitler: innledning, presentasjon av kraftforsyningskjeden, metode, empiri, drøfting og konklusjon. Innhold og formålet med de ulike kapitlene er beskrevet i tabell 1.

Tabell 1 Oppgavens oppbygging

Kapittel 1 Innledning:	Her presenteres tema og bakgrunn oppgavens fokus, i tillegg til problemsstilling og tilhørende forskningsspørsmål. Oppgavens avgrensninger og beskrivelse av oppgavens utforming blir presentert.
Kapittel 2 Systembeskrivelse av kraftforsyningskjeden:	Beskrivelse av organiseringen av den norske kraftforsyningskjeden. Utfordringer med dagens IKT-systemer i kraftforsyningen.
Kapittel 3 Teori:	Begrepsavklaring av sentrale begreper: safety/security, trefaktormodellen (risiko), usikkerhet, kompleksitet, krise, resiliens og driftskontinuitet. Presentasjon av Resilience Engineering-perspektivet og dens prinsipper: overvåke, forutse, respondere og lære. Forklaring av RAG og VSM.
Kapittel 4: Metode:	Beskrivelse av forskningsmetode og teoretisk grunnlag ift. metodevalgene. Kartlegging av aktivitet i kraftforsyningen gjennom VSM. Kvantitativ analyse: spørreundersøkelse. Kvalitativ analyse: dokumentanalyse og gruppeintervju. Validitet og reliabilitet. Fordeler og ulemper ved gjennomført metode.

Kapittel 5 Empiri:	I dette kapittelet presenteres det funn først fra spørreundersøkelsen, gjennom RAG-tilnærmingen. Målingene visualiseres gjennom radardiagram. Videre presenteres det funn fra gruppeintervjuene, der vi ser nærmere på driftskontinuitet og de fire RE-prinsippene, med utdrag av sitat fra gruppeintervjuene.
Kapittel 6 Drøfting:	Empiri blir knyttet sammen med teori. Her skal de tre forskningsspørsmålene besvares for å svare på oppgavens problemsstilling.
Kapittel 7 Konklusjon:	I dette kapittelet blir konkluderende funn fra drøftingen utredet og presisert som skal belyse problemsstillingen. Det henvises også til videre forskning på området.

2. Oppgavens kontekst: Kraftforsyningskjeden i Norge

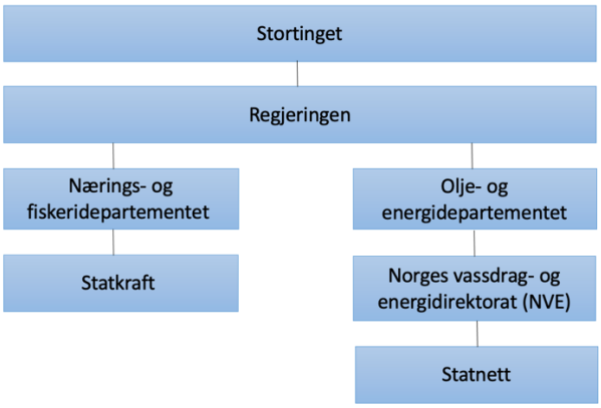
Formålet med oppgaven er å se nærmere på hvordan prinsippene i RE og opprettholdelsen av driftskontinuitet kan bidra til å forbedre forsyningssikkerheten hos aktører i kraftforsyningen. Systembeskrivelsen redegjør for nødvendig bakgrunnsinformasjon og utdyper oppgavens kontekst. Dette danner en forståelse av kraftsektoren og forsyningskjeden som en kritisk samfunnsfunksjon og dens oppbygning. Konteksten brukes som utgangspunkt for anvendelsen av Viable System Model (VSM) på kraftforsyningskjeden (kapittel 4.2).

2.1 Organisering av den norske kraftforsyningen: systembeskrivelse

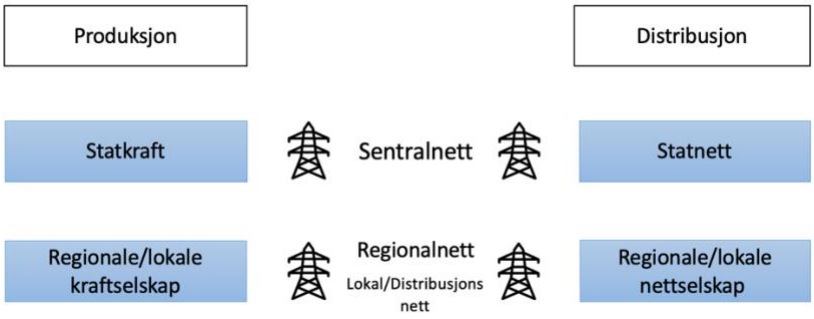
Kraftsektoren er en stor sektor som består av mange forskjellige aktører. For å illustrere dette er det laget en forenklet illustrasjon over aktørbildet på myndighetsnivå (figur 1). Figuren beskriver bare de mest overordnede forholdene på dette nivået. Dette er for å gi en enkel fremstilling av organiseringen til den norske kraftforsyningens myndighetsnivå. Øverste nivå er Storting med regjeringen. Under disse befinner Nærings-og fiskeridepartementet (NFD) og Olje- og energidepartementet (OED) seg. NFD har eieransvaret for Statkraft SF. OED er underlagt regjeringen, og har som hovedoppgave å forvalte en helhetlig og samordnet energipolitikk. Videre er Norges vassdrag- og energidirektorat (NVE) underlagt OED. NVE har ansvar for å forvalte energi- og vannressursene i Norge. NVE er også sentrale i beredskapsarbeidet i kraftsektoren. De har blant annet utarbeidet egen veileder til kraftberedskapsforskriften som er utarbeidet for kraftsektoren. NVE arbeider for en robust kraftforsyning med stabil kraftleveranse (NVE, 2022b). Det operative ansvaret for kraftforsyningsberedskapen er dermed gitt til NVE via OED. Dette vil si at NVE skal gjennomføre tilsyn, øvelser og veiledninger. Videre er Norges kraftforsyningsberedskap

organisert gjennom KBO som befinner seg under ansvaret til NVE og andre virksomheter som står for kraftforsyningen (NVE, 2022a). De andre virksomhetene som står for kraftforsyningen er alle de som driver eller eier kraftproduksjon med tilhørende vassdragsregulering, fjernvarme og overføring og distribusjon av elektrisk energi, altså strøm.

Myndighetsnivået er det som skal regulere kraftsektoren, spesielt gjennom lovverk og forskrifter. Videre gir NVE som nevnt, ut veiledninger for å bistå med beredskapsarbeidet hos kraftforsyningsaktørene. DSB (2016) oppsummerer relevante lovverk fra kraftsektoren: energiloven, el-tilsynsloven, sivilbeskyttelsesloven, energilovforskriften, forskrift om systemansvaret i kraftsystemet, kraftrasjoneringsforskriften, kraftberedskapsforskriften og forskrift om elektriske forsyningsanlegg. Alle lovene og forskriftene er med på å regulere kraftsektoren og deres beredskapsarbeid.



Figur 1 Illustrasjon over organiseringen av den norske kraftforsyningens myndighetsaktører.



Figur 2 Illustrasjon over produksjon- og nettselskap i Norge.

Under myndighetsnivået befinner kraftprodusenter og kraftnettdistributører. Norge består av et titalls ulike aktører innen både produksjon og distribusjon av kraftforsyning. Derfor er det delt mellom produksjon og distribusjon i figur 2. Som vist i begge figurene ovenfor, er det to heleide statlige selskap, nemlig Statkraft SF og Statnett SF. Statkraft SF drifter og utvikler anlegg for fornybar kraft, blant annet gjennom vind-, sol- og vannkraft (Statkraft, 2023). Statnett SF har

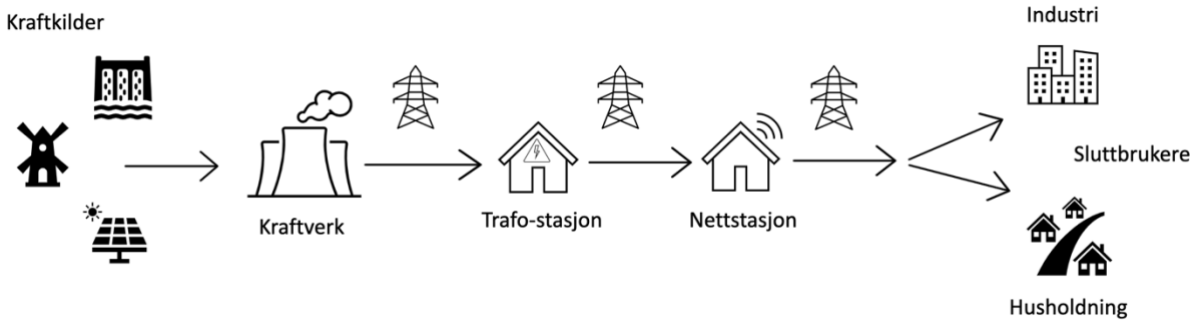
ansvaret for å koordinere produksjon og forbruk (Statnett, 2018). Statnett SF er operatør for transmisjonsnettet, også kalt sentralnettet i Norge, som forbinder produsenter og sluttbrukere i ulike deler av Norge med hverandre. Her befinner det seg også overføringsledninger til utlandet for eksport av energi. Videre når det gjelder distribusjon har man regionalnettet og distribusjonsnettet (Olje- og energidepartementet, 2014). Regionalnettet er nettnivået under sentralnettet, som er et bindeledd mellom sentralnettet og distribusjonsnettet. Distribusjonsnettet er det siste leddet i overføringen til sluttbrukere (husholdninger, tjenesteyting og industri). Her har man både høyspent distribusjonsnett og lavspent distribusjonsnett (se Glitre Energi illustrasjon 2023, figur 4). Skillet mellom monopolvirksomhet (nett) og markedsvirksomhet (produksjon, salg) fører med seg at driften er selvstendig fra kraftprodusentene til leverandørene. Ofte er nettselskapet og leverandør organisert under samme konsernledelse, hvor nettselskapene eksisterer som selvstendige rettssubjekt (Olje- og energidepartementet, 2014). Det eksisterer også konsern som både har produksjon og distribusjon av strøm til sluttbrukere. Det viktigste her er at man tar i betraktning at produksjon- og nettselskapene kan driftes separat med ulik ledelse, selv under samme konsern.

Dagens kraftsektor er organisert som et deregulert marked hvor både private og offentlige aktører kan produsere tjenester for forbrukere. Selv om det er et deregulert marked, er hovedandelen statlig-, fylkes- og kommunale eiere (Olje- og energidepartementet, 2019). Dette gjelder både produksjon-og nettselskaper. I figur 2, er disse fylkes- og kommunale eierne plassert under Statkraft SF og Statnett SF. Dette er for å få en enklere oversikt over hvordan organiseringen av den norske kraftforsyningen er. Selv om Statkraft SF er likestilt med andre kraftprodusenter, er de likevel plassert ovenfor på grunnlag av at de er et heleid statlig selskap. I denne oppgaven skal vi se nærmere på nivået som er under Statkraft SF og Statnett SF, nemlig regionale/lokale produksjon- og nettselskap. Dette har vi gjort for å avgrense oppgaven, og vi har inkludert to produksjonsselskap og to nettselskap på dette nivået.

2.1.2 Nærmere om kraftforsyningskjeden

Det skal gis en nærmere beskrivelse av kraftforsyningskjeden som oppgaven skal se nærmere på. Vi tar utgangspunkt i produksjonen av de fornybare energikildene vann-, vind- og solkraft. Dette er fordi disse er naturlige energikilder og er hovedandelen av den fornybare energien i Norge. I Norge er det ca. 98% av kraftproduksjonen fornybar, hvor den største andelen av dette kommer fra vannkraftproduksjon (Meld. St. 25 (2015-2016)).

Hele kraftforsyningskjeden starter ved produksjon i kraftverkene. Dette kommer fra blant annet vann-, vind- og solkraft. Videre blir denne energien videreført gjennom regionalnettet til transformatorstasjoner. Her blir spenningsnivået redusert og videreført gjennom høyspent distribusjonsnett til en nettstasjon. Nettstasjonene befinner seg som regel i umiddelbar nærhet av bebyggelsen hvor den elektriske energien skal gjennom sitt siste ledd. For at alt dette skal kunne foregå er vi helt avhengige av kraftnettet. Kraftnettet fungerer som limet i hele denne kjeden og inkluderer alle tre nettene (sentral-, regional-, og distribusjonsnettet). Det siste leddet er lavspent distribusjonsnett hvor den elektriske energien kommer frem til sine sluttbrukere. Dette kan være husholdninger og mindre industri. Dette er enkelt fremstilt i figur 3.

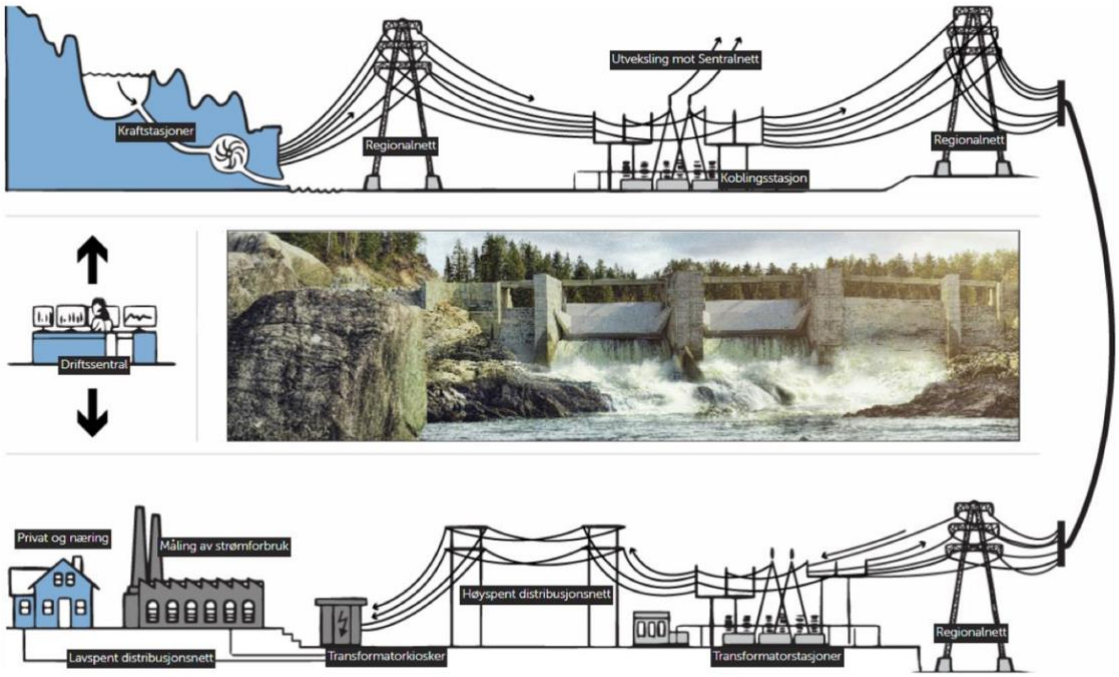


Figur 3 Forenklet illustrasjon over kraftforsyningskjeden fra produksjon til distribusjon.

Den regionale verdikjeden består av ulike deler. Dette fremstilles på en mer detaljert måte i figur 4. Denne har nærsammenheng med figur 3, men fremstiller mer visuelt hvordan den elektriske energien går fra å bli produsert, videre gjennom regionalnettet hvor energien overføres gjennom koblingsstasjoner mot sentralnettet. Deretter går det videre til transformatorstasjoner hvor spenningen blir nedbrutt og videreført til høyspent distribusjonsnett til transformatorkiosker, også kalt nettstasjoner. Her blir spenningen nedbrutt og sendt videre gjennom lavspent distribusjonsnett og til sluttbrukerne.

Basert på denne forståelsen er driftssentralen bindeleddet i verdikjedene. På driftssentralen kan produksjon, transmisjon og distribusjon overvåkes og styres (Meld. St. 25 (2015-2016). Gjennom driftssentralene gjennomfører man fjernstyring. Man kan i prinsippet styre alle funksjonene i den delen av kraftsystemet som er underlagt sentralen. På grunn av det lovpålagte skillet mellom markedsvirksomhet og monopolvirksomhet betyr dette at driftskontrollsystemene opererer selvstendig fra produksjon av kraft og til distribusjon av kraft. Dette vil si at nettselskapene har sitt eget driftskontrollsystem som overvåker deres strømnett og transformatorstasjoner. Videre har også kraftproduksjonselskapene sitt eget driftskontrollsystem som overvåker produksjon og videre distribusjon fra

produksjonsanleggene. I praksis er det ikke alltid nødvendigvis slik at driftskontrollsystemene er adskilt, men opererer med en sammenkobling fra produksjon- og nettselskapene.



Figur 2 Illustrasjon av regional verdikjede hentet fra (Glitre Energi, 2022)

Figur 4 Illustrasjon av regional verdikjede hentet fra Glitre Energi (2022).

2.3 Utfordringer med dagens IKT-systemer i kraftforsyningen

Basert på at oppgaven fokuserer på SC, skal det sees nærmere på informasjons- og kommunikasjonsteknologi systemet (IKT-system) som brukes i kraftforsyningen. «Smartnett» er brukt som en betegnelse som beskriver et kraftsystem som dekker et behov for tettere samspill i verdikjeden gjennom et «smart» bruk av IKT-systemer (Harrison et al., 2010). Dette viser til at det er en integrasjon mellom IKT og fysisk infrastruktur for å tilpasse produksjon og overvåke systemene. Denne integreringen av fysisk infrastruktur og IKT kan kobles opp mot begrepet cyberfysiske systemer (Rinaldi et al., 2001). Dette forstås av Lun et al. (2019) som integrasjonen av databehandling, nettverk og fysiske prosesser. Dermed blir det enklere å automatisere og effektivisere prosesser som tidligere krevde manuell behandling. På denne måten kan man plassere ut sensorer og målestasjoner i aktuelle områder i kraftforsyningskjeden, og fjernstyre disse via driftssentralene. Dette kalles ofte avanserte måle- og styringssystemer (AMS), og de blant annet overvåker og registrerer forbruk. For å nevne noe kan man på denne måten enkelt åpne- og lukke ventiler i produksjonsanleggene uten å fysisk være til stede og overvåke spenningsnivået i nettet. Selv om dette er svært viktig for å automatisere og effektivisere en viktig samfunnsfunksjon fører det med seg ulike utfordringer.

Digitaliseringen av kraftforsyningens informasjonssikkerhetssystem gjør forsyningskjeden sårbar overfor en rekke fysiske påkjenningen og angrep. SCADA-systemene, eller driftskontrollsystemer, som kraftforsyningsaktører benytter er industrielle databaserte prosess kontroll systemer for styring og overvåking (Nygård, 2004, s. ii; NVE, 2011). I oppgaven brukes begrepet SCADA-system fremfor driftskontrollsystemer, men de er synonymer. Dette systemet fungerer vanligvis med en fysisk forbindelse mellom SCADA-datanettet og det administrative datanettet i virksomheten. Det betyr at det gir mulighet for ekstern tilgang, fordi det administrative datanettet er koblet opp med Internettet. Dette kan gjøre at eksterne aktører kan få tilgang til viktige styringssystemer i driftssentralene. SC, som omhandler cyberangrep mot dette systemet, kan sette kraftforsyningen ute av spill og på den måten sette sentrale verdier i fare. Dermed er denne kritiske samfunnsfunksjonen svært sårbar ovenfor eksterne inntrengere i systemene. Hvis man ikke har tilstrekkelige sikkerhetstiltak og risikoforståelse rundt dette kan det gjøre systemet sårbart. Derfor er det utviklet særegne krav i kraftberedskapsforskriften som inkluderer informasjonssikkerhet (kap. 6) og beskyttelse av driftskontrollsystem (kap. 7). På denne måten er alle kraftprodusenter og nettselskap ment til å arbeide mot en sikker kraftforsyning.

Utfordringen ved IKT-sikkerheten har blitt belyst av Riksrevisjonen, der det har blitt gjennomført en undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen, her henviser Riksrevisjonen til flere kritikkverdige og alvorlige forhold (Riksrevisjonen, 2021). De viser til at ny teknologi, utenlandske leverandører, skyløsninger og integrering av ulike systemer som er koblet til Internett økter risikoen for uønskede hendelser innenfor IKT i kraftforsyningen. Riksrevisjonen (2021) viser til nasjonale trusselvurderinger hvor kraftsektoren som kritisk infrastruktur er spesielt utsatt for avanserte nettverksoperasjoner og etterretning. Det er NVE som har ansvaret for å samordne beredskapen i kraftforsyningen og forsikre seg om at den er i tråd med gjeldende krav. NVE har blitt utpekt som sektorvis responsmiljø for å koordinere og håndtere IKT-sikkerhetshendelser i kraftforsyningen (Riksrevisjonen, 2021, s. 4). Konklusjonene til Riksrevisjonen (2021) kan oppsummeres med det følgende: for det første har ikke NVE tilstrekkelig påsett at det er god nok beredskap for å håndtere IKT-angrep i kraftforsyningen. For det andre har ikke NVE gjennomført tilstrekkelig med tilsyn med IKT-sikkerhet, og de har ikke gjennomført tilstrekkelige beredskapsøvelser hvor IKT-angrep har vært sentralt. For det tredje er NVEs evne til å vurdere statusen og utviklingen av IKT-sikkerhetstilstanden mangelfull. Avslutningsvis ser vi at Riksrevisjonen

(2021) har påpekt en rekke svakheter i det nåværende arbeidet med IKT-sikkerhet i kraftforsyningen.

Arbeidet med en styrket IKT-sikkerhet i kraftforsyningen ble også påpekt i Melding til Stortinget nr. 38 (2016-2017). Dette er den første Stortingsmeldingen om IKT-sikkerhet, og Lysneutvalget (digitalt sårbarhetsutvalg) kommer med en rekke anbefalinger for å styrke arbeidet med IKT-sikkerhet innen en rekke sektorer, deriblant energiforsyning. Utvalget viser til at NVE har begrenset kapasitet til å følge opp med tilsyn innen IKT-sikkerhet og sårbarhet. Dermed burde NVE sikre større og mer ressurssterke fagmiljø i KBO-enhetene, fordi flere KBO-enheter er mindre og har få ansatte med begrenset IKT-kompetanse. Videre sikter utvalget til at det burde bygges et sterkt operativt fagmiljø for IKT-hendelseshåndtering. KraftCERT er utviklet i sammenheng med å optimalisere sikring av prosesskontrollsystemer for kraftbransjen, der de oppdaterer kundene sine om relevante trusler og sårbarheter (KraftCERT, 2023). De tilbyr tjenester innen sårbarhetsovervåking, trusseletterretning, deteksjon, hendelseshåndtering, øvelser og krusing innen IKT-sikkerhet. Denne tjenesten er noe utvalget anbefaler å videreutvikle for å bygge et sterkt fagmiljø innenfor operativ hendelseshåndtering. Selv om dette er noe produksjon- og nettselskaper kan ta i bruk, er det noe usikkerhet rundt hvor mye denne tjenesten blir brukt. Dette er noe Riksrevisjonen (2021) har nevnt som et kritikkverdig forhold i sin undersøkelse. Tiltakene til utvalget i Stortingsmeldingen ble tatt i betraktning når Riksrevisjonen (2021) foretok undersøkelser av NVEs IKT-sikkerhetsarbeid.

3. Teori

I dette kapittelet skal det redegjøres for terminologier og teoretiske perspektiver. Først skal det redegjøres for terminologiene safety versus security, risiko, usikkerhet, kompleksitet, krise, beredskap, resiliens og driftskontinuitet. Deretter redegjøres det for RE-perspektivet. Til slutt vil The Resilience Analysis Grid (RAG) bli presentert, som er en del av RE, og Viable System Model (VSM). Oppgaven har et hovedfokus på RE-perspektivet og driftskontinuitet.

3.1 Terminologi

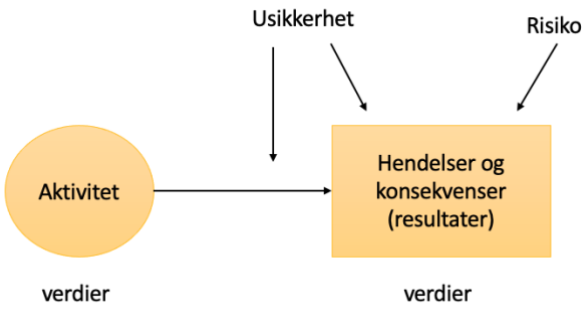
Safety versus security

Skillet mellom de engelske begrepene «safety» og «security» er svært omdiskutert. Det hersker også stor uenighet om begrepenes oversettelse til norsk (Engen et al., 2021; Jore, 2017). I risiko og samfunnssikkerhetsforskningen har forståelsen av disse begrepene utviklet seg til å skilles ved forskjeller i intensjonalitet. Det vil si at begrepene tilbyr en beskrivelse for å håndtere

forskjellige typer risikoer (Engen et al., 2021; Jore, 2017). For oppgaven vår er det hensiktsmessig å skille mellom begrepene og vi tar utgangspunkt i Jore (2017) sin forståelse. Her beskrives det hvordan begrepene baserer seg nettopp på intensjonalitet: «safety» handler om beskyttelse mot menneskelige og tekniske feil, skade på mennesker forårsaket av vilkårlige eller ikke-intensjonelle hendelser og naturkatastrofer, menneskelige feil, eller system og prosessfeil. «Security» handler om beskyttelse mot tilsiktede handlinger utført av mennesker, tap forårsaket av intensjonelle handlinger utført av mennesker og forsettlig menneskelig aktørfeil. For denne oppgavens formål vil det anvendes en security-risiko presentert gjennom SC.

Risiko

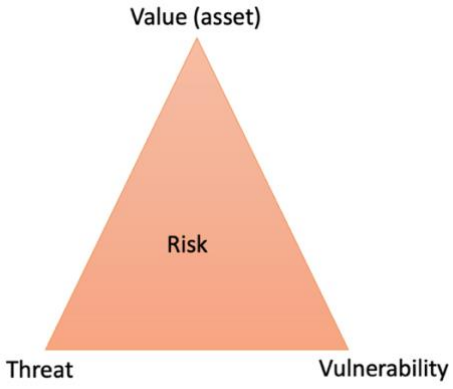
Aven og Renn (2010) har utviklet en felles deskriptiv definisjon av risiko basert på mange ulike definisjoner, som er: "usikkerheten om og alvorligheten av hendelser og konsekvenser (eller resultater) med hensyn til aktiviteter som mennesker verdsetter" (s. 2) (se figur 5 for illustrasjon). Denne definisjonen er utfyllende da den tar for seg både et «klassisk» syn på risiko (sannsynlighet x konsekvens) samtidig som den tar høyde for at mennesker har ulik persepsjon av risiko, altså hva mennesker verdsetter.



Figur 5 Illustrasjon av risikodefinisjon ifølge Aven og Renn (2010).

For denne oppgaven anses det som hensiktsmessig å også legge vekt på trefaktormodellen i forståelsen av risiko. Trefaktormodellen står også i stil med den norske standarden NS 5814:2021 og er ofte brukt i sammenheng med nasjonale trusselvurderinger (NSM, 2023a; PST, 2023). Trefaktormodellen kan benyttes til risikovurderinger for tilsiktede handlinger og består av tre kjernemomenter: trussel, sårbarhet og verdi (Njå et al., 2020). Her beskrives dermed risiko som en kombinasjon av disse tre kjernemomentene. Modellen anses som relevant for vårt formål ettersom oppgaven tar utgangspunkt i SC, som beskriver en tilsiktet handling.

Det første momentet omhandler trusselvurdering, som betyr å gjennomføre en analyse og vurdering av relevante trusselaktører og deres kapasitet (gjennomføringsevne) og intensjon (konkrete planer om å gjennomføre angrep) (Martin, 2019, s. 69). Et helhetlig mål med trusselvurdering er å forstå trusselnivået og de ulike metodene en trusselaktør benytter. På den måten kan man arbeide forebyggende mot eventuelle trusselmål. Det andre momentet, sårbarhet, er noe som det finnes mange forståelser og definisjoner av. En tilnærming til sårbarhet er at det er uttrykk for de problemene et system får med å fungere når det for eksempel utsettes for en uønsket hendelse, eller problemer med å gjenoppta sin virksomhet etter en hendelse (Njå et al., 2020). Njå et al. (2020) definerer sårbarhet som «manglende evne hos et analyseobjekt til å motstå virkninger av en uønsket hendelse og til å gjenopprette sin tilstand eller funksjon etter hendelsen. Manglende evne relateres til vår usikkerhet om fremtiden» (s. 52). Verdiene som verdsettes bestemmer hva de uønskede konsekvenser inneholder. Eksempler på sårbare mål er harde og myke mål, dette kan være fysiske sperringer av bygg (harde) eller cyberangrep av digitale rom (myke) (Martin, 2019). Det tredje momentet i modellen er verdi. Verdier kan sees i sammenheng med sårbarhet, og varierer fra aktør til aktør. Det er derfor viktig at virksomheter kartlegger sine verdier for å identifisere konsekvensene av uønskede handlinger (Busmundrud et al., 2015). Trusselaktører velger seg ofte mål basert på sårbarhetene rundt målet og hvilke verdier som vil bli påvirket. Når trusselaktører skal velge seg mål foretrekker de mål med stor politisk verdi, fremfor mål med størst materiell ødeleggelse (Hegghammer, 2012). Dette betyr at trusselaktørene foretrekker verdien menneskelig skade og frykt ovenfor økonomiske skader. Eksempelvis kan cyberangrep mot en kritisk samfunnsfunksjon spre frykt blant mennesker. Sikkerhet må dermed balanseres mellom verdiene som virksomheten verdsetter (Jore, 2015).



Figur 6 Trefaktormodellen (NSM, 2023a; PST, 2023).

Usikkerhet

Det finnes flere ulike forståelse på usikkerhet, og begrepet har ingen entydig definisjon (Njå et al., 2020). Usikkerhet er et viktig moment å ta høyde for når en skal ta beslutninger. Begrepet kan ha ulike betydninger i henhold til tidsperspektivet (fortid, nåtid og fremtid). I fortid handler usikkerhet om graden av korrekt forståelse av historien som har vært og er knyttet til metodene. Her gjelder det hva man har observert, fortolket, gjenkjent og gitt en underliggende forståelse. I nåtid handler usikkerhet om hva vi kan vite om våre samfunnsviktige funksjoner eller systemet vårt. Det handler altså om vår spesifikke kunnskap om systemet. Usikkerhet for framtiden handler om det som kan skje og er knyttet til risiko. Denne usikkerheten kan ikke måles eller reduseres, og på den måten kan en si at usikkerhet er en karakteristikk ved framtiden. Det knyttes til at vi har begrenset kunnskap om framtiden, noe som er viktig å ta høyde for når en skal ta beslutninger.

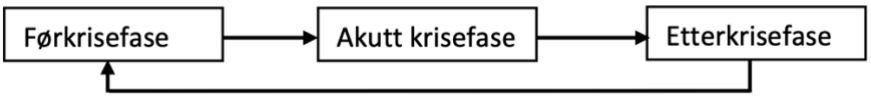
Kompleksitet

I henhold til oppgavens fokus på kraftforsyningen på et systemnivå er det hensiktsmessig å definere en forståelse rundt kompleksitet. Kraftforsyningen er en kritisk samfunnsfunksjon, og med dette følger det ofte en iboende kompleksitet. Slike systemer, som kritiske infrastrukturer og samfunnsfunksjoner, er komplekse fordi de krever styring og håndtering som skjer på tvers av forskjellige sektorer og ansvarlige myndigheter (DSB, 2016). Denne oppgavens forståelse av kompleksitet sees i lys av Perrow (2011). Han forklarer hvordan den raske teknologiske utviklingen gjør at systemene i dag har en kompleksitet som gjør at ulykker blir «normale», normal accidents teorien (NAT). Hovedelementene i denne forståelsen er at det er umulig å unngå at feilhandlinger eller svikt i enkeltkomponenter kan forplante seg videre i systemet og føre til større ulykker fordi systemene er tett koblet. Perrow omtaler dette som interaktiv kompleksitet. Interaktiv kompleksitet innebærer at ulike komponenter er koblet sammen på en måte som gjør det umulig å forutse hvordan en hendelse kan forplante seg videre i systemet. Motsetningen til dette er lineære koblinger, der man enklere kan se sammensetningen mellom de ulike delsystemene i systemet. Tette koblinger innebærer at hendelser som oppstår i systemet går fort over til andre delsystemer og dermed vanskelig å stoppe. Når disse koblingene er løsere, kan påvirkningen fra disse stoppes før de påvirker andre deler. Basert på dette vil da et system med høy interaktiv kompleksitet og tette koblinger være svært vanskelig – om ikke umulig ifølge Perrow – å styre. Perrow har fått kritikk for sin pessimistiske tankegang, noe man i dagens samfunn enklere lar seg håndtere ved ulike former for desentralisert og

sentralisert styring. Kraftforsyningen kan basert på dette sees på som et sosioteknisk system bestående av ulike former for tette koblinger og interaktiv kompleksitet. En framstilling av kraftforsyningen og dens tilhørende systemer kommer fram i figur 13.

Krise

Krisebegrepet er komplekst og vanskelig å definere (Gundel, 2005; Kruke, 2015). Spesielt verdifulle for oppgaven vår er Rosenthal et al. (1989), sin definisjon som kan oversette som: «en alvorlig trussel mot strukturer, verdier og normer i et sosialt system som under tidspress og usikkerhet gjør det nødvendig å foreta kritiske beslutninger» (s.10) , samt NOU 2000:24 sin definisjon: «en hendelse som har potensial til å true viktig verdier og svekke en organisasjons evne til å utføre viktige funksjoner» (s. 19). Kriser kan deles inn i ulike tidsperspektiver, og Kruke (2012) har definert tre krisefaser: førkrisefase, akuttkrisefase og etterkrisefase. Her er faseinndelingen en sirkulærprosess, der man alltid vil komme tilbake til en ny normaltilstand etter en krise og til en ny førkrisefase. Når man kommer tilbake på en ny førkrisefase er man forhåpentligvis mer resilient mot nye risikoer som kan oppstå. Dette vil si man aldri kommer tilbake til «status quo».



Figur 7 Illustrasjon av krisefaser (Kruke, 2012).

Dette kan kobles til tidsperspektivet på styringen av resiliens. Å dele inn kriser i tidsperspektiv er en forenklingsstrategi som kan sees i sammenheng med RE og RAG-tilnærmingen. Utformingen av spørsmålene i intervjuguiden vil dermed basere seg på før, under og etter krisen (SC) og det er viktig at spørsmålene stilles med en konsekvent struktur deretter. På den måten utelukkes alle generiske spørsmål som inkluderer flere tidsperspektiver.

Beredskap

Beredskap er et begrep som det er vanskelig å finne en felles, akseptert definisjon på. Eriksen et al. (2021) definerer beredskap som «forberedelse og utøvelse av konsekvenshåndtering ved uønskede situasjoner» (s. 30). Njå et al. (2020) beskriver beredskap som alle operasjonelle, organisatoriske og tekniske tiltak som hindrer at faresituasjoner kan utvikle seg til ulykkessituasjoner, eller skal forhindre skadevirkningene av mulige ulykkeshendelser (s. 262). I NOU 2006:6 blir det påpekt at «beredskap er planlegging og forberedelse av tiltak for å håndtere uønskede hendelser på best mulig måte» (s. 38). Dette er et lite utvalg av definisjoner,

men viser forskjeller og likheter som inngår i de ulike forståelsene. Fellestrekk ved definisjonene er at de sier noe om planlegging og tiltak. Planlegging og tiltak knyttes igjen til forebygging, begrensning og konsekvenshåndtering av eventuelle uønskede situasjoner.

I denne oppgaven er det hensiktsmessig det tatt utgangspunkt i NOU 2006:6 sin definisjon, som anvendes rundt vår forståelse om beredskap i kraftsektoren, som også står i stil med kraftberedskapsforskriftens formål jf. §1-1. Her pålegger kravene i forskriften virksomhetene plikter som må oppfylles, både når de er i en normal driftssituasjon og før det oppstår ekstraordinære beredskapssituasjoner. Disse pliktene kan på denne måten ivaretas ved å planlegge forebyggende sikringstiltak og forberede beredskapstiltak. På denne måten er det nødvendig med forberedelse og planlegging av tiltak for å forberede seg på uønskede hendelser (NOU 2006:6, s. 38). Forståelsen av beredskap sees også i sammenheng med forståelsen av driftskontinuitet.

Resiliens

Det er mange forskjellige forståelser og tolkninger av begrepet resiliens, og noen av disse skal redegjøres for før oppgaven tar standpunkt på en definisjon fra Hollnagel (2011). I følge Aven og Thekdi (2021) kan resiliens defineres som «the ability to quickly return to the normal state given an event (risk source) (s. 18). Dette gjelder både kjente og ukjente hendelser. I Melding til Stortinget nr. 5 (2020- 2021) blir begrepet motstandsdyktighet brukt i stedet for resiliens. Regjeringen vil videreutvikle samfunnets motstandsdyktighet gjennom økt vektlegging av det forebyggende arbeidet. Motstandsdyktigheten gir gode forutsetninger for å leve med risiko (Meld.St.5 (2020- 2021), s. 33). Gjennom å øke motstandsdyktigheten i kritiske samfunnsfunksjoner reduseres sannsynligheten for at større kriser vil ramme Norge, samtidig som det beregner mulige negative konsekvenser slike kriser kan ha. Forebygging bidrar til å skape robusthet og motstandsdyktighet i kritiske samfunnsfunksjoner og grunnleggende nasjonale funksjoner. Motstandsdyktighet brukes dermed i denne stortingsmeldingen hyppig fremfor å bruke begrepet resiliens. Motstandsdyktighetsbegrepet kan sies å være en del av begrepet resiliens, men erstatter det ikke (Stavland & Bruvoll, 2019). Videre er resiliens definert av Sellevåg et al. (2020) som «resiliens er brukt for å beskrive ønsket tilstand i et system. Det omhandler et systems evne til å opprettholde og gjenoppta sin funksjonalitet etter at det har blitt utsatt for en hendelse» (s. 13). Videre definerer Engen et al. (2021) resiliens som «den kapasiteten et sosialt system har til å motstå og tilpasse seg forventede og uventede forstyrrelser, og til å gjenopprette funksjonaliteten etter alvorlige påkjenninger fra slike

forstyrrelser» (s. 61). Det er viktig å belyse tvetydigheten rundt begrepsbruken, ettersom resiliens ikke har en entydig definisjon, for å få en bredere forståelse.

Det er hensiktsmessig for denne oppgaven å ta utgangspunkt i Hollnagel (2011) sin definisjon av resiliens, som videre sees i sammenheng med RE-perspektivet. Resiliens er definert av Hollnagel (2011b) som «[...] den iboende evnen i et system til å justere sine funksjoner i forkant av, under eller etter endringer og forstyrrelser, slik at det kan opprettholde nødvendige funksjoner under både forventede og uforventede forhold» (s. 275). Hollnagel et al. (2006, 2011) viser til fire kjennetegn for resiliente organisasjoner. For det første er evnen til effektiv og fleksibel respons på både regulære og irregulære trusler. For det andre er evnen til å overvåke situasjoner og ha kunnskap om hendelser som kan oppstå. Dette innebærer også evnen til å overvåke egne prestasjoner. For det tredje er evnen til å ta lærdom fra hendelser som oppstår, samt fra tidligere hendelser. For det fjerde er kunnskap om hva som kan forventes, eller hvordan situasjonen og trusler kan utvikle seg. Forenklet kan man si at de fire hovedtrekkene ved en resilient organisasjon baserer seg på evnen til å respondere, overvåke, lære og forutse hendelser. Hollnagel med kollegaer sitt sikkerhetsperspektiv RE skal videre redegjøres for i delkapittel 3.2.

Driftskontinuitet

Driftskontinuitet er et begrep som ikke er særlig etablert i norsk sammenheng. Den litteraturen som omhandler driftskontinuitet, bruker hovedsaklig eksplisitt begrepet business continuity. Det er mange forskjellige forståelser og tolkninger rundt begge disse begrepene. For denne oppgavens formål er tatt utgangspunkt i litteraturen omkring «business continuity»-begrepet på engelsk for å beskrive hva vi mener med driftskontinuitet. Vi er innebefattet med at det ikke er det samme som driftskontinuitet, men det kan tenkes at de har mange fellestrekk når det kommer til begrepsbruk og planleggingen av driftskontinuiteten i virksomheter. Dermed kan vi komme frem til en forståelse av hva driftskontinuitet handler om basert på business continuity. Videre i oppgaven vil driftskontinuitet og business continuity begrepene brukes synonymt. Det skal først sees på to norske bidrag som omhandler business continuity og kontinuitetsplanlegging, før det skal redegjøres for to vitenskapelige artikler.

NS-ISO 2230 om kontinuitetsledelse omtaler «business continuity» og kan knyttes til driftskontinuitet. Den bruker eksplisitt begrepet business continuity. Standarden definerer business continuity som «capability of an organization to continue the delivery of product and services within acceptable time frames at predefined capacity during a disruption» (Standard

Norge, 2019, s.2). Formålet med dette er dermed å være forberedt og vedlikeholde essensielle system, og på den måten kan organisasjonens evne styrkes i møte med forstyrrelser. Standarden spesifiserer strukturen og kravene for å implementere og opprettholde et Business Continuity Management System (BCMS). Ved å opprette en BCMS formes systemet av organisasjonens lovlige, regulatoriske, organisatoriske og industrielle krav. Videre inkluderer dette også produkter og tjenester som tilbys, størrelse og struktur av organisasjonen, og kravene til interessenter. Dermed vil et BCMS fremheve viktigheten av å forstå organisasjonens behov når det kommer til drift, vedlikeholdsprosesser og responsstrukturer for å sikre at virksomheten klarer å overleve forstyrrelser i driften. Denne formen for styringssystem vil inneholde en policy, definerte ansvarsområder, planlegging, vurdering av resultater, gjennomgang av ledelsen og kontinuerlig forberedelse. Interessenter kan stille krav til leveranse av produkter, tjenester, informasjon o.l. Dermed er det essensielt å arbeide kontinuerlig med å opprettholde driften og planverk for dette når forstyrrelser inntreffer.

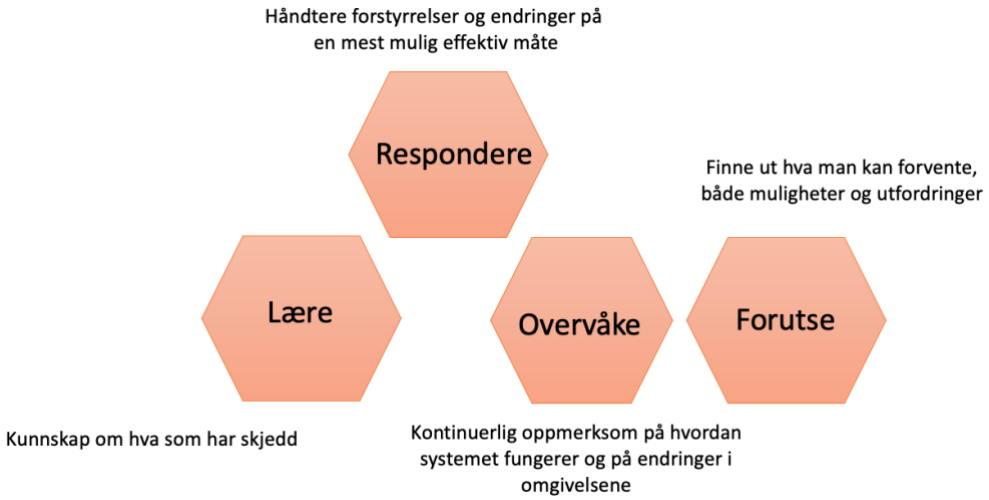
Dette er i likhet med det DSB (2020) skriver om i sin rapport om kontinuitetsplanlegging. Her kan kontinuitetsplanlegging som metode brukes for å planlegge bortfall i innsatsfaktorer (varer, tjenester og arbeidskraft). Nærmere kan man bruke kontinuitetsplanlegging for å redusere sannsynligheten for stopp i produksjon og på den måten finne løsninger på hvordan virksomheten kan opprettholde driften på et akseptabelt nivå, uansett hvilke uønskede hendelser som skulle inntreffe. Basert på dette ser man at BCMS og kontinuitetsplaner er like i sin utforming og kan refereres til som det samme. Dermed vil begrepet kontinuitetsplaner brukes videre i oppgaven. DSB (2020) mener at alle virksomheter som består av en kritisk samfunnsfunksjon bør planlegge opprettholdelse i sine leveranser, uansett hvilke uønskede hendelser som vil inntreffe. Her forstås kontinuitet som en evne til å sikre løpende produksjon og levering av varer og tjenester (DSB, 2020). Denne evnen er avhengig av tilgang til innsatsfaktorer, som er elementer som inngår i produksjonen av en tjeneste eller vare. Avhengigheten virksomheter har til innsatsfaktorer medfører sårbarheter ettersom bortfall av dem kan medføre hel eller delvis svikt i produksjonen. Her kan man skille mellom interne og eksterne innsatsfaktorer. Interne innsatsfaktorer kan være råvarer som virksomheten produserer selv, mens eksterne kjøpes fra andre virksomheter. Dette kan sies å være en sentral del av opprettholdelsen av driftskontinuitet og dens tilhørende kontinuitetsplaner. Basert på dette er den adaptive kapasiteten til en virksomhet sentral for å være mest mulig resiliente mot forstyrrelser i systemet. Den adaptive kapasiteten til en virksomhet kan forstås som hvor god virksomheten er til å justere og tilpasse seg når uønskede hendelser inntreffer.

I sammenheng med et bredere teoretisk grunnlag i henhold til driftskontinuitet skal to relevante artikler fra *Journal of business continuity and emergency planning* redegjøres for. Artikkelen til Hodges & Larraaga (2021) beskriver komplekse adaptive systemer i sammenheng med krisehåndtering, og hvordan denne håndteringen i disse systemene kan ved fokus på en adaptiv tilnærming øke effektiviteten til håndteringen i dynamiske og usikre miljøer. Dette kan sees i sammenheng med Perrow (2011) hvor komplekse systemer består av en interaktiv kompleksitet som kan kreve en bredere forståelse. Hodges & Larraaga (2021) mener basert på kompleksiteten i systemet at det kreves et skifte fra den nåværende lineære forståelsen til en konsekvensbasert systemtilnærming på å oppdage farer i systemet. På denne måten foreslår de at det burde utbygges en bredere forståelse av systemhelheten, prosessen og tilstanden av konvergering og påvirkningsfaktorer innenfor og utenfor det helhetlige systemet. Basert på dette foreslår de at systemeiere kartlegger deres avhengigheter innenfor og utenfor virksomheten og etablerer en forståelse i virksomheten om komplekse adaptive systemer. På denne måten kan systemeiere og deres virksomheter bygge seg resiliente i møte med komplekse utfordringer. Artikkelen til Gierczak & Blake Messmer (2022) påpeker at flere virksomheter anser sin nåværende plan til å være egnet for formålet, selv om fremtidig risiko vil skape ulike former for forstyrrelser og påvirkning på systemet. I en hverdag hvor styring av driftskontinuitet er viktigere enn noen gang, er det dermed et stort behov for å se på hvordan man skal implementere arbeidet med driftskontinuitet i sin virksomhet. De anser driftskontinuitet-begrepet som et paraplybegrep som dekker ulike konsepter som kontinuitetsplanlegging, Disaster Recovery (DR), risikostyring med mer. Tradisjonelle kontinuitetsplaner gir virksomheter en strategisk plan på hvordan man kan utvikle mekanismer i egen virksomhet for å støtte evnen til å fortsette driften under forstyrrelser. Disse artiklene sees i sammenheng med begrepsforståelsen av driftskontinuitet i NS-ISO 2230 og DSB (2016).

3.2 Resilience Engineering

RE-perspektivet er viktig fagfelt innen sikkerhetsforskningen. Perspektivet bygger hovedsakelig på boken «Resilience Engineering in Practice» (Hollnagel, 2011b). Målet til RE er å finne ut hvordan man kan oppnå resiliens i et system (Hollnagel, 2011b). Det som er viktig er systemets evne til å justere dens funksjoner. En viktig del av utviklingen i forskning knyttet til RE-perspektiver viser et skifte fra tankegangen som i stor grad fokuserer på det som kan gå galt eller feil, til å i større grad fokusere på normale daglige operasjoner eller funksjoner i et system (Woods & Hollnagel, 2006). Konseptet resiliens og verktøyene som tas i bruk gjennom RE-perspektivet er ment å løse svakheter i blant annet sikkerhetsstyringen i systemer

(Wreathall, 2006). Hensikten med RE-perspektivet og dens konsepter gjennom å respondere, overvåke, forutse og lære skal hjelpe virksomheter å oppnå disse prosessene. Resiliente virksomheter behandler sikkerhet som en kjerneverdi (Woods & Hollnagel, 2006). Idealet er at systemer bygger seg sterkere i møte med forstyrrelser og påkjenninger.



Figur 8 De fire kjerneegenskapene for resiliens (Hollnagel et al., 2011).

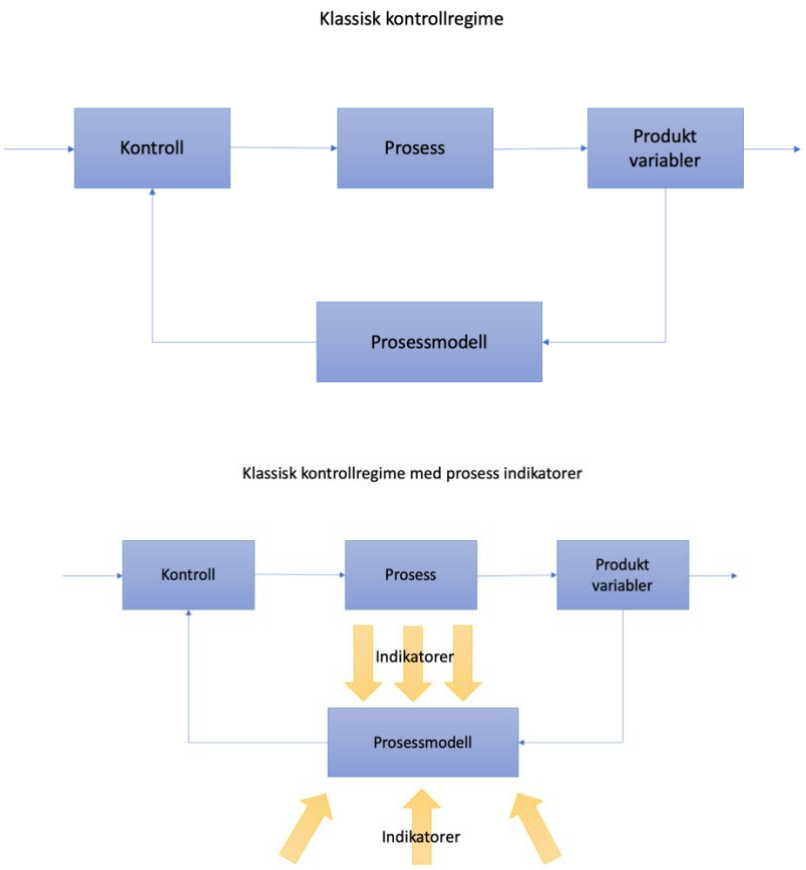
Forståelsen rundt resiliens gjøres mer detaljert ved å se nærmere på dens fire kjerneegenskaper (se figur 8) (Hollnagel, 2011b). Det å vite hva man skal gjøre når forutsette og utforutsette forstyrrelser i systemet oppstår, kan gjøres gjennom implementering av beredskap eller ved å justere den normale funksjonen. Dette er evnen til å adressere det faktiske og baserer seg på hvordan *responsen* er i systemet. Viktigheten av å vite hva man skal se etter, baserer seg på hvordan man kan *overvåke* det som kan bli en trussel for systemet. Kontinuerlig overvåking av systemets miljø og det faktiske systemet i seg selv er essensielt for å oppdage forstyrrelser. Dette baserer seg på evnen til å ta tak i det kritiske. Det å vite hva man kan forvente, som vil si hvordan man kan *forutse* utviklingen, trusler og muligheter i fremtiden baserer seg på å forutse mulige endringer, forstyrrelser, press og dets konsekvenser. Basert på dette handler det om evnen til å adressere potensialet. Å vite hva som har skjedd, baserer seg på å *lære* av erfaring, spesielt hvordan man lærer de riktige hendelsene fra de riktige erfaringene. Dette gjelder både å lære av det som er riktig og lære av feil. Videre er dette evnen til å ta opp det faktiske.

3.2.1. Overvåke – det kritiske

Et kjerneelement i RE er overvåke. Enhver organisasjon som er opptatt av sikkerhet burde gjennomføre analyser for risikoakseptkriterier for å måle virksomheters nivå av sikkerhet for å avgjøre hvilke risikoer de ser på som akseptable eller ikke. Risikoakseptkriterier er ulike

kriterier som er satt for å vurdere risikoen, og på den måten avgjøre om den gitte risikoen er akseptabel, tolererbar eller ikke-tolererbar (Aven & Thekdi, 2021; Njå et al., 2020). Hvis risikoen anses som tolererbar av virksomheten burde den overvåkes og man kan eventuelt utvikle risikoreduserende tiltak som kan iverksettes når det oppstår et behov for det. Risikoakseptkriterier kan eksempelvis illustreres ved hjelp av risikomatriser. En risikomatrise er et diagram for å oppsummere og beskrive risiko, og består av to dimensjoner: konsekvenskategori for en gitt hendelse og tilhørende sannsynlighet (Aven & Thekdi, 2021; Njå et al., 2020). Her plasserer man risikoer som virksomheten står ovenfor basert på disse dimensjonene, og ofte etter fargekoden grønn, gul og rødt. Virksomheter kan også ta i bruk prinsippet ALARP (as low as reasonably practicable), her skal risikoen reduseres så langt som praktisk mulig (Njå et al., 2020). Det er hensiktsmessig å ha indikatorer på hvilke risikoer som tolereres i virksomheten i henhold til hvordan virksomheten skal overvåke de gitte risikoene. Disse måtene å måle risiko på kommer til kort når man skal håndtere sikkerhet i fremtiden (Wreathall, 2011). Tanken rundt dette er at det ofte blir et større fokus på de «verste» utfallene, som ofte preges av større tilfeldigheter enn andre risikoer. Videre gir ofte ikke slike hendelser informasjon om årsaker eller hvordan det kan ordnes i fremtiden. Risikoreduserende tiltak som iverksettes gir liten nytte for å forberede seg på uforutsette og forutsatte hendelser, eller for å håndtere de proaktive prosessene som sikrer sikker og effektiv ytelse i systemet (Wreathall, 2011). Wreathall (2011) hevder at i miljøet rundt systemet og dens interne prosesser er dynamiske, og dermed er fjorårets eller gårsdagens sikkerhetsytelse (safety performance) svake i møte med morgendagens risikoer.

Indikatorer i målinger er en essensiell del av enhver organisasjon. Wreathall (2011) understreker et gammelt uttrykk som er like aktuelt i dagens lys: «You can’t manage what you don’t measure» (s. 62). Der en indikator har som hensikt å angi noe. I sammenheng med utviklingen av RE-perspektivet og hvordan resiliens anvendes i organisasjonsledelse presenterer Wreathall en klassisk kontrollteorimodell som både er med og uten proaktive indikatorer.



Figur 9 Kontrollteorimodell basert på Wreathall (2011).

Prosessen som befinner seg i den midterste boksen er alle hovedaktivitetene i organisasjonen. Fra produksjon, koordinering, økonomi o.l., her oppnås en rekke resultater som inkluderer sikkerhet, produksjon og økonomisk ytelse. Som vist i modellen blir produktet evaluert gjennom en prosessmodell som via en kontrollfunksjon justerer eller regulerer tilbake inn i prosessene (se figur 9). Kravene kan settes i det interne miljøet, men også av eksterne aktører. Typisk krav satt av eksterne aktører er gjennom lovverk, retningslinjer, skatt o.l. som en virksomhet må følge. For det interne miljøet kan det være interne retningslinjer, som rutiner. Wreathall (2011) viser til risikostyring tradisjonelt har fulgt klassisk kontrollteori. På den måten skjer endringer i sikkerhetsprosedyrer etter det har skjedd et avvik i sikkerheten. Dette kan føre til eksempelvis tap av liv og helse og økonomi. Dette kan sies å være en form for reaktiv styring.

I motsetning til den reaktive styringsformen foreslår RE å være proaktiv i arbeidet med risikostyring. For å kunne være mer proaktiv i styringen, kreves det mer informasjon som vist i figur 9. Her vil de pilene fungere som indikatorer, som skal gi fortløpende informasjon om hva som skjer i forskjellige stadier av prosessen før vesentlige forstyrrelser og endringer inntreffer. På denne måten er det mulig å gripe inn for å forhindre større skade av systemet. I

forhold til denne oppgaven, så kan slike indikatorer være endringer i trafikk i SCADA-systemene eller endringer i det dynamiske trusselbilde for kraftsektoren. Å forutse slike endringer gjør det mulig å møte endringer i systemet, og forhindre at det totalkollapser. Dette er en viktig del av å kunne opprettholde stabilitet over tid i systemene (Wreathall, 2011). I forhold til dette påpeker også Westrum (1999) hvor man anvender «faint signals» som indikatorer er en særdeles essensiell egenskap for å opprettholde resiliens i en virksomhet. Dette kan vises gjennom indikatorer på utfordringer som oppstår i systemer gjennom hint i prosessen.

3.2.2 Forutse – potensiale

Evnen til å forutse og tilpasse seg når det oppstår forstyrrelser i systemet er en viktig del av et systems resiliens (Woods, 2011). Det er viktig at alle nivåer i et system kan håndtere forstyrrelser på måter som vil bidra til å opprettholde kontrollen til tross for hindringer. Essensielt i resiliens er dens adaptive kapasitet, og gjennom dens evne til å tilpasse seg systemet slik at den svarer på kravene som den vil møte i fremtiden. For å gjøre dette må systemet være i stand til å gjenkjenne endringer som krever justeringer og respons (Woods, 2011). Hvis systemet overser eller avskriver indikatorer (signaler) gjør det at systemets adaptive kapasitet er nedgående som videre gjør systemet sårbart for tap eller sammenbrudd (Woods, 2011). I RE beskrives det seks ulike mønstre for hvordan resiliente systemer kan forutse at den adaptive kapasiteten feiler. Noen av mønstrene inneholder for eksempel være at buffere eller reserver tømmes eller at målsetningen for systemet endres. Det første mønstret omhandler at resiliente systemer har evnen til å oppdage at den adaptive kapasiteten er i ferd med å feile eller er uregelmessig. Denne evnen er grunnleggende hevder Woods (2011) for at man kan unngå å bli fanget i dekompensasjon. Dette betyr at man ikke naturlig greier å kompensere for en svekket funksjon. På denne måten påpekes det i RE at om et system reduserer hastigheten for å hente seg inn etter forstyrrelser og avbrudd, kan det sees på som en indikator på at systemet er på vippepunktet og på vei mot dekompensasjon. I henhold til dette er det svært viktig å se etter tegn hvor potensialet kan føre til kaskadeeffekt i systemet. Her vil da endringer føre til å skape nye sammenhenger og gjensidige avhengigheter som påvirker hverandre.

Det andre mønstret som beskrives under prinsippet om forutse baserer seg på at resiliente systemer burde være i stand til å gjenkjenne om det trues av at ressursene utmattes ut over det man har av reserver og buffer (Woods, 2011). RE understreker viktigheten av evnen å arbeide med håndteringen av større forstyrrelser og stress i systemet (Lay, 2011). Ikke bare ved å respondere og handle på hva som skjer, men ved å tilpasse hvordan dette gjøres. Ved å

gjenkjenne hva som kan true systemet, og hva som kan forårsake at ressursene uttømmes bygger systemet resiliens. Woods (2011) nevner ulik forskning fra casestudier hvor det problematiseres at buffere kan over tid oppløses gjennom en rekke mindre beslutninger som kan føre til større svikt i systemet. I sammenheng med dette kan profesjonalitet kobles til å være en spesiell og viktig ressurs i møte erosjon i systemet, eksempelvis mot produksjonspress. Dette kan sees i sammenheng med handlingsrommet til å respondere, hvor eksempelvis arbeidere i profesjonelle stillinger er i stand til å vurdere handlingsrommet i en situasjon og se potensialet. Dermed kan evnen til å respondere i tide knyttes til evnen for å forutse.

Det tredje mønsteret for forutsigelser i RE er at resiliente systemer er i stand til å gjenkjenne når det burde skiftes prioritet på bekostninger av, eller fordeler for noe annet (Woods, 2011). Studier om adaptiv kapasitet i komplekse systemer viser at avveininger er grunnleggende og fundamentale for resiliente systemer. En viktig indikator for resiliens er hvordan et system håndterer situasjoner hvor målkonflikter oppstår, og som gjenkjennes og dermed gir avkall på produksjonsmål til fordel for å prioritere sikkerhetsmål. I RE kan det dermed tenkes at hvis systemet ikke er i stand til å understøtte menneskene i dette ved å endre målsetningen for å investere i sikkerhet, vil de fleste systemer i praksis drifte mot høyere risiko enn de innser eller nødvendigvis ønsker.

Det fjerde mønstret for forutsigelser er at resiliente systemer klarer å endre perspektiver og anvende det som kan være en utpreget motsetning fra det som representerer den daglige normen (Woods, 2011). Enklere forstås det som evnen til å endre perspektiver. Dette kan vise seg gjennom å skape et rammeverk som kan identifisere interne prosesser som har en stor grad av funksjonsavhengighet av hverandre. På denne måten kan man utvikle en metode for en proaktiv identifikasjon av risiko i utfallet eller produktet av prosessen. Opp- og nedgående resiliens mellom ulike nivåer i et system kan forstås som at det må forutsettes evne til å kunne endre perspektiver for å anvende det som kan være en motsetning fra det som representerer den daglige normen. På bakgrunn av dette kan da systemet endre perspektiv og gi evnen til identifikasjon av ulike særegenskaper i en prosess.

Det femte mønstret for forutsigelser er at resiliente systemer i stand til å navigere gjennom funksjonsavhengigheter på tvers av roller, aktiviteter og nivåer (Woods, 2011). Dette betyr at for at systemet skal kunne utøve evnen å være forutseende, må ulike nivåer i systemet tilpasses hverandre. Eksempelvis må prosedyrene på strategisk, taktisk og operativt nivå samstemme med hverandre. Her må da funksjonene på strategisk nivå tilpasses funksjonene på taktisk nivå,

og videre ned mot operativt nivå. Uten en evne til å kommunisere endringer av funksjoner til det underordnede eller overordnede nivået står responser fra de ulike nivåene igjen i fare for å bli utilstrekkelig. I verste fall kan det føre til større skadelige konsekvenser. Det påpekes både i det fjerde og femte mønsteret for forutseende resiliens at det er i retning av at denne evnen må forsterkes i kontrollstrategier for ledelse i beredskap og kriser.

Det sjette og siste mønstret for forutseende resiliens er at systemet er i stand til å gjenkjenne behovet for å lære nye måter å tilpasse seg (Woods, 2011). Dette viser seg i at resiliens i hovedsak handler om hvordan systemet lærer. Woods viser til at det er vanskelig for systemet å reflektere over hvordan det er i stadig endring av gjensidige avhengigheter og ulike sammenkoplete aspekter, for og deretter identifisere svakheter og utvikle nye metoder eller prosesser. Hollnagel (2011) nevnte innledningsvis i boken at for å effektiserte resiliens må systemet lære å justere sin tilpasningsevne for å kontinuerlig oppdatere denne evnen til å svare på endrede forutsetninger som kan komme igjennom muligheter eller økt press.

Avslutningsvis kan det oppsummeres at RE vektlegger disse seks mønstrene som kjennetegner resiliente systemers evne til å forutse (Woods, 2011):

- De evner å gjenkjenne når tilpasningsevnen avtar.
- Gjenkjenner når buffere eller reserver utmattes.
- De evner å gjenkjenne når de må gjøre kompromisser på tvers av målsetning.
- De evner å endre perspektiver og anvende det som står i kontrakt til det daglige normen.
- De evner å styre endringer mellom avhengigheter på tvers av roller, aktiviteter, nivå og målsetninger.
- De gjenkjenner når de må lære nye måter å tilpasse seg på.

3.2.3 Respondere – på det aktuelle

Respondere er en av de fire kjennetegnene i RE-perspektivet. Pariés (2011) beskriver dette som evnen til en organisasjon eller system til å «håndtere det aktuelle». Dette vil si at man svarer på kravene til den nåværende situasjonen, hvor det har oppstått en forstyrrelse. Her er det viktig at man klarer å håndtere det mest aktuelle og reagere på det en situasjon krever, som følge av en eventuell forstyrrelse. Evnen til systemet i denne sammenheng må ifølge Pariés (2011) klare å handle på riktig tidspunkt for å optimalisere eller redusere virkningene av forstyrrelsen. Dette vil si at systemet må kunne forstå når eksempelvis en barriere eller ressurs er mangelfull, som senere kan forårsake at systemet feiler. Videre kan man forstå dette som «resiliens i sanntid». Som vil si at systemet har en evne til å prioritere mellom ulike mål for å gi størst grad av

sikkerhet, eksempelvis gjennom et kost/nytte-perspektiv (Pariés, 2011). Det er viktig at man vet hva man skal respondere på og bestemme hva man skal gjøre og ikke når man håndterer forstyrrelser i et system.

Beredskapen til å respondere baserer seg i hovedsak på to strategier (Pariés, 2011). Den første er den proaktive tilnærmingen, som vil si at man bør forutse mulige forstyrrelser i systemet. Her burde man ha klart definert planverk eller retningslinjer slik at man vet hvordan man skal håndtere situasjonen, dette kan for eksempel være beredskapsplaner, krisehåndteringsplaner o.l. Den andre strategien er den reaktive tilnærmingen, som baserer seg på ad-hoc løsninger. Dette betyr at det må skapes og utvikles umiddelbare handlinger i behov for øyeblikks bestemte løsninger. Her er man ikke forberedt på situasjonen, og dermed må reagere ad-hoc som gir rom for improvisasjon (Engen et al., 2021). Denne formen for «resiliens i øyeblikket», kan forstås nærmere gjennom synkrone og diakrone perspektiver, der synkrone kan forstås som at det ikke tar hensyn til tidsperspektivet i forskning, mens diakron forskning tar hensyn til tidsperspektivet til et fenomen (Pariés, 2011). Den «butte enden» av systemet består av blant annet ledelse og instruktører. Når man snakker om «resiliens i øyeblikket» i denne delen av systemet omhandler det hvordan man sikrer at de nødvendige ressursene som personell, utstyr og kompetanse er til stede eller kan etableres i tide. Videre er det gunstigere å ta utgangpunkt i spørsmålet rundt hvordan man etablerer (nå) og opprettholder (i morgen) en beredskapsevne som kan etableres når som helst i fremtiden. Avslutningsvis er det viktig å få frem at den primære egenskapen til å respondere, er å faktisk respondere.

3.2.4 Lære – av det faktiske

Den siste av de fire hovedegenskapene til resiliens er lære. Å lære hva som har gått galt, og hva som går bra er essensielt for RE. I praksis er evnen til å lære, like viktig som de tre forutgående, selv om den forfattes sist. For at læring skal finne sted, må tre betingelser være oppfylt (Hollnagel, 2011c). Den første betingelsen er at det eksisterer rimelige muligheter for å lære. Det vil si at situasjonene der noe kan læres oppstår i tilstrekkelig høy grad. Dette betyr at situasjoner må oppstå relativt ofte slik at man kan trekke lærdommer fra de gitte situasjonene. På den måten unngår man at læringen fra en gitt situasjon blir delvis glemt. Den andre betingelsen er at situasjonene er tilstrekkelig like til å la seg generalisere. Dette vil si at de må ha noe til felles og være sammenlignbare. Hollnagel (2011b) påpeker her at mennesker og virksomheter må kunne gjenkjenne at noe i situasjon A kan identifiseres i situasjon B, ikke bare basert på resultatene, men også i årsakene. Den tredje betingelsen er at det skal være tilstrekkelig mulighet til å verifisere at de riktige lærdommene er trukket ut av situasjonen.

Hollnagel (2011b) viser til at denne betingelsen kan sees på som en sammenkobling mellom de to forutgående betingelsene. Dette viser seg at en sammenlignbar hendelse må skje før lærdommen er glemt, og forhåpentligvis i god tid før lærdommen må anvendes i en faktisk hendelse.

Betingelsene som må ta plass i forhold til læring kan illustreres gjennom noen eksempler. Ulykker og kriser illustreres viktigheten av å finne ut hvorfor hendelsen oppstod. Heldigvis skjer ikke større ulykker og kriser ofte, og på den måten er det vanskelig å lære av slike hendelser på bakgrunn av den lave hyppigheten. Ofte er ulykker forskjellig i sin natur som også gjør det vanskelig å trekke lærdommer fra slike hendelser, og på den måten er det vanskelig å verifisere om riktige lærdommer er trukket ut fra hendelsen. På bakgrunn av illustrasjonen kan det sies at læring er mer effektiv basert på hendelser som oppstår hyppig. Dermed påpeker Hollnagel (2011b) at det er mer effektivt å lære av hva som går riktig enn å lære av det som går galt. Dette er fordi det som går riktig skjer hyppigere enn situasjoner som går galt. Ifølge Hollnagel et al. (2006) står dette i samsvar med det grunnleggende prinsippet i RE om at feil er baksiden av suksess og at begge har sitt opphav i ytelsesvariabilitet på det systemiske og individuelle nivået.

Effekten av læringen er også viktig i henhold til å tilegne seg ny kunnskap. De fire prinsippene i resiliens er alle gjensidig avhengighet av hverandre. Hvis man tar læring som utgangspunkt, kan det være enkelt å argumentere for at evnen til å respondere vil være av liten verdi uten evnen til å lære. Et system kan alltids benytte seg av forhåndsdefinerte eller stereotypiske responser (Hollnagel, 2011c). Så lenge karakteristikkene for dette miljøet ikke endrer seg, og omgivelsene er stabile kan responsen være tilstrekkelig. Hvis systemet har et skiftende miljø og omgivelser, vil de forhåndsdefinerte responsene bli utdaterte. Dermed er det nødvendig å lære nye måter å respondere på, og dette kan gjøres gjennom å evaluere og observere effektiviteten på responsen. På denne måten kan systemet lære nye og effektive måter å respondere på uønskede hendelser. Et lignende argument kan vises gjennom relasjonen mellom læring og overvåke (Hollnagel, 2011c). Gjennom overvåking må man velge indikatorer som skal prioriteres i henhold til systemets forhold, dette skjer først og fremst gjennom praktisk læring som gir en evne til å tolke disse indikatorene og prioritere hvilke indikatorer som er viktige for det systemet. Det kan sies at effektiviteten av å overvåke er avhengig av utvelgelsen av rett type erfaringer for læring. Videre kan vi se læring i sammenheng når det gjelder å forutse (Hollnagel, 2011c). Basert på dette må systemet kunne gjenkjenne når det er nødvendig å lære på nye måter og tilpasse seg endringer i forutsetningene. I relasjon til å forutse, er læring

essensielt for å produsere realistiske måter å forstå hva på som kan oppstå i systemet i et fremtidig perspektiv. Dette fremhever viktigheten av å lære de riktige leksjonene, som baserer seg på å forstå hva som kan skje på en måte som er brukbar for de fremtidige funksjonene i systemet.

På hva som burde læres bidrar alle fire prinsippene i RE på ulike måter. Hollnagel (2011c) påpeker at i søken etter forklaringen om uønskede hendelser kan det være sterkt påvirket av antagelser på hvordan forskjellige faktorer samhandler. I sammenheng med dette finner man ofte det man leter etter i systemet, som kan føre til skjevheter i hva man ser etter og lærer av. Ved å søke etter hva man forventer i systemet, er det umulig å lære av det som ikke har skjedd. På bakgrunn av dette kan man overse vesentlige faktorer som kan ha påvirket systemet på ulike nivået. Gjennom bruken av RE kan det være lurt å søke etter underliggende faktorer som kan påvirke og forårsaket en uønsket hendelse. Dette er kanskje spesielt viktig i henhold til koordinasjon og kommunikasjon i sosiotekniske systemer som kraftforsyningen er.

3.2.5 Kartlegging av resiliens - The Resilience Analysis Grid (RAG)

Et verktøy som brukes for å kartlegge resiliens hos virksomheter er RAG (Resilience Analysis Grid). Her beskrives det hvordan dette verktøyet som metode kan brukes for å se nærmere på å respondere, overvåke, forutse og lære, og hvordan dette kan vurderes gjennom å besvare relevante spørsmål og hvordan funnene av disse kan presenteres (Hollnagel, 2011a). RE er opptatt av hva som gjør et system resilient, og hvordan kan opprettholde og administrerere resiliens i systemet. Resiliens referer ofte til noe et system gjør, og på den måten kan man si at styringen av dette er en type prosesskontroll (Hollnagel, 2011a). Hollnagel (2011a) påpeker at det må besvares tre grunnleggende spørsmål når man skal styre en prosess, likegyldig med å styre resiliens: Hva er nåværende posisjon? Hvor skal vi? Hvordan kommer man seg dit? I sammenheng med resiliens i en virksomhet kan dette kobles til å kartlegge den nåværende posisjonen til virksomheten, hva målsetningen er og hvilke midler som kan anvendes for å innfri dette. Ved utviklingen av RAG er formålet og måle, den nåværende situasjon eller status for å bygge videre på dette (Hollnagel, 2011a).

Et system anses som sikkert når antallet av uønskede hendelser holdes nede på et akseptabelt nivå (Hollnagel, 2011a). Fordelen med å forstå sikkerhet på denne måten er at man kan måle sikkerheten ved antall ulike hendelser. På denne måten kan sikkerheten forstår som fravær av uønskede hendelser. I sammenheng med RAG kan sikkerhet forstås som *evne til å lykkes under varierte forhold* (Hollnagel, 2011a). Ifølge RE er det mer til sikkerhet enn å bare redusere antallet uønskede hendelser, og fokuserer på både hva som går riktig og galt. Dermed oppstår

feil fra justeringer som må gjøres for å kompensere for underspesifikasjoner av den virkelige verden, fremfor sammenbrudd eller funksjonsfeil av normale systemfunksjoner. Dermed er forståelsen av sikkerhet i RAG i samsvar med RE-perspektivet. Forståelsen tar sikte på å forstå systemets evne til å fungere under varierte forhold med konsekvenser for hvordan resiliens måles, og hvordan det kan styres (Hollnagel, 2011a, s. 276).

Det er tre nøkkelegenskaper for et resilient systems evne til å justere sin ytelse etter behov (Hollnagel, 2011a). Disse justeringene kan i praksis være proaktive, synkrone eller reaktive. Den første nøkkelegenskapen er *proaktive justeringer* (fremtid), og innebærer at et system kan endre seg fra en tilstand for normal drift til tilstand med forhøyet beredskap. Dette gjør det mulig at en handling kan skje før hendelsen inntreffer. På denne måten kan ressurser tildeles der det trengs for nødvendig respons til en forventet hendelse og at funksjoner kan aktiveres og gi økt beskyttelse i barrierer. Hollnagel (2011a) påpeker at en åpenbar fordel for proaktiv respons er at det er mindre ressurskrevende å håndtere en hendelse før den inntreffer og blir kritisk. Den andre nøkkelegenskapen er *synkrone justeringer* (nåtid). Dette innebærer en rask justering som inntreffer og pågår samtidig som hendelsen utvikler seg. Dette er basisfunksjonen for klassisk kontrollregime. Den tredje nøkkelegenskapen er *reaktive justeringer* (fortid). Dette går ut på at justeringene inntreffer i etterkant av hendelsen, og som også kan trekkes til lærdommer og anbefalinger fra hendelsen. Å respondere når noe har hendt, kan ikke garantere systemets sikkerhet, selv om responsen er rask. Dette er fordi systemet kan bare forberede seg på å respondere på et begrenset sett med hendelser. Hendelser som faller utenfor dette, vil ta lengre tid og er mindre sannsynlig til å lykkes. Dette kan sees i sammenheng med de tre ulike krisefasene til Kruke (2012) (se kapittel 3.1).

3.3 Modell for levedyktige systemer (Viable system model)

Viable system model (VSM), eller modell for levedyktige systemer på norsk, er en styringsmodell utviklet av Stafford Beer (1985) som tilbyr en måte å se hvordan interaksjoner mellom fem nivåer (sub-systemer) samarbeider for å skape en effektiv organisasjon (Pollock & Steen, 2021). Utgangspunktet for utviklingen av denne modellen var å finne ut hvordan systemer er levedyktige, og modellen har blant annet blitt brukt for å forsterke organisatorisk resiliens (Pollock & Steen, 2021). I sammenheng med at modellen ofte brukes i forhold til organisasjoner, vil det dermed bli referert til «organisasjonen» gjennom forklaringen av modellen. Kompleksiteten, den organisatoriske resiliensen og systemforståelsen er flere av grunnene for at vi har valgt å bruke modellen som utgangspunkt for oppgaven vår. I selve modellen står rekursjonsprinsippet sentralt, som vil si at det totale systemet i modellen er

avhengig av å inneholde selvorganiserende og autonome (selvstyrende) systemer (sub-systemer). På den måten vil disse sub-systemene organisere og styre seg selv uavhengig av de andre systemene i modellen. Likevel er det totale systemets levedyktighet avhengig av samhandling og koordinering med de andre selvorganiserende og autonome systemene. Dette er et kriterium for VSM. Forholdet mellom disse systemene og deres strukturer, nøkkelprosesser, kommunikasjon, informasjonsflyt og hvordan systemet tar hånd om kompleksitet og et miljø i endring utgjør sentrale aspekter av VSM.

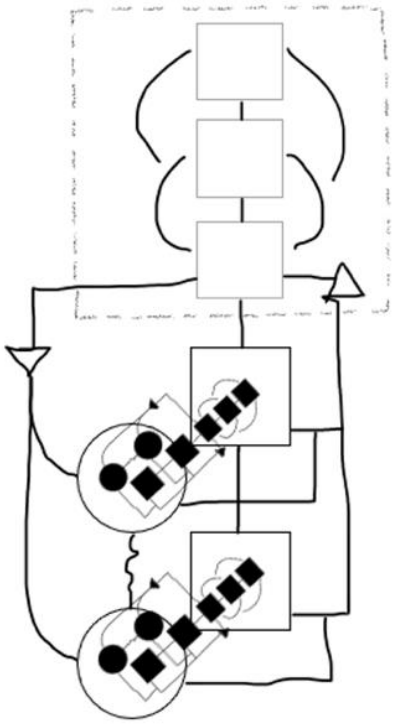
Fernandes og Tribolet (2019) beskriver fire prinsipper for å forstå og anvende VSM i en praktisk sammenheng:

1. Rekursjonsprinsippet: beskriver en organisasjon som et levedyktig system som inneholder et sett av levedyktige systemer (sub-systemer).
2. Det essensielle i at det totale systemet inneholder et sett med funksjonelt sammenhengende sub-systemer, og at disse samarbeider med hverandre. På denne måten skapes det tilstrekkelige forhold for at det totale systemet skal være levedyktig.
3. Hvilken som helst form for avvik eller svikt i et hvert styringssystem, vil true levedyktigheten til det totale systemet.
4. Levedyktigheten, koordineringen, og selv-organiseringen av et system avhenger av at disse funksjonene arbeider sammen på alle nivåer.

Denne logikken kan visualiseres gjennom en russisk tredukke (Pollock & Steen, 2021). En russisk tredukke kan åpnes, og inni vil du finne en mindre versjon av den samme dukken, og inni der igjen en mindre versjon av de to foregående dukkene, helt til man til slutt kommer til den minste dukken. For at man skal kunne sette sammen disse dukkene er det helt essensielt at formen, størrelsen og andre aspekter ved dukken gjør at de passer perfekt inni hverandre. Vi kan se dette analogt med et system på den måten at et systems sub-systemer er gitt primære oppgaver, og systemet som en helhet er avhengig av at alle sub-systemene gjør sine gitte oppgaver. Dersom sub-systemene ikke som en helhet utfører sine oppgaver i seg selv, vil ikke systemet være levedyktig; altså dukkene vil ikke passe sammen.

VSM´s bruksområder innebærer eksempelvis å identifisere diagnostiske problemer (diagnostic problems). Slike diagnostiske problemer kan identifiseres ved hjelp av VSM for å oppdage svakheter i sub-systemene som kan føre til svikt i organisasjonen eller hele systemet. Modellen tilbyr dermed en identifikasjon av disse problemene og løsninger på dem slik at organisasjonen kan fungere mer effektivt og skape en bedre tilpasning til endringer i omgivelsene. Det er

nettopp ved identifiseringen (og løsningen) av disse problemene som gjør at organisasjoner kan optimalisere funksjonene sine og dermed være levedyktig over tid (Beer, 1985). Beer (1985) presiserer at når en skal ta i bruk VSM er det svært viktig å bestemme presist hvilke system som skal modelleres, og spesifisere systemets grenser, selv om disse kan endres ettersom systemet tilpasser seg. Deretter må man definere dens levedyktige sub-systemer, og det større levedyktige systemet. Hvis vi ser på modellen under, så ser vi at det totale systemet inneholder to systemer som er identisk med det totale systemet. Disse systemene er altså levedyktige systemer i seg selv, som utgjør deler av det totale systemet.



Figur 10 VSM basert på Beer (1985).

Firkantene i figuren representerer ledelsesdelen av systemet det som eksempelvis består av koordinering og kontroll, overvåkning og andre styringselementer, samtidig som sirklene representerer det operasjonelle der hvor eventuell produksjon av produkt og lignende foregår. I metodekapittel 4.2 skal det sees nærmere på denne modellen i henhold til den norske kraftforsyningen.

3.4 Oppsummering av teoretisk grunnlag

I denne delen har vi gjennomgått de viktigste teoretiske bidragene og terminologien i oppgaven som skal diskuteres ytterliggere i senere kapitler og knyttes til den innsamlede empirien. Vi har definert viktig terminologi som inkluderer safety og security, risiko, usikkerhet, kompleksitet,

krise, resiliens og en spesielt viktig del av oppgaven, nemlig driftskontinuitet. Videre er det nøye gjennomgått RE i dybden og hvordan de ulike prinsippene innenfor det teoretiske grunnlaget er. Der vi har sett nærmere prinsippene, forutse, overvåke, respondere og lære. Det teoretiske grunnlaget bak fremstillingen av spørreundersøkelsen gjennom RAG har blitt presentert. På samme måte er det teoretiske grunnlaget bak fremstillingen av det totale systemet som skal gjennomgås nærmere i metoden, presentert gjennom VSM.

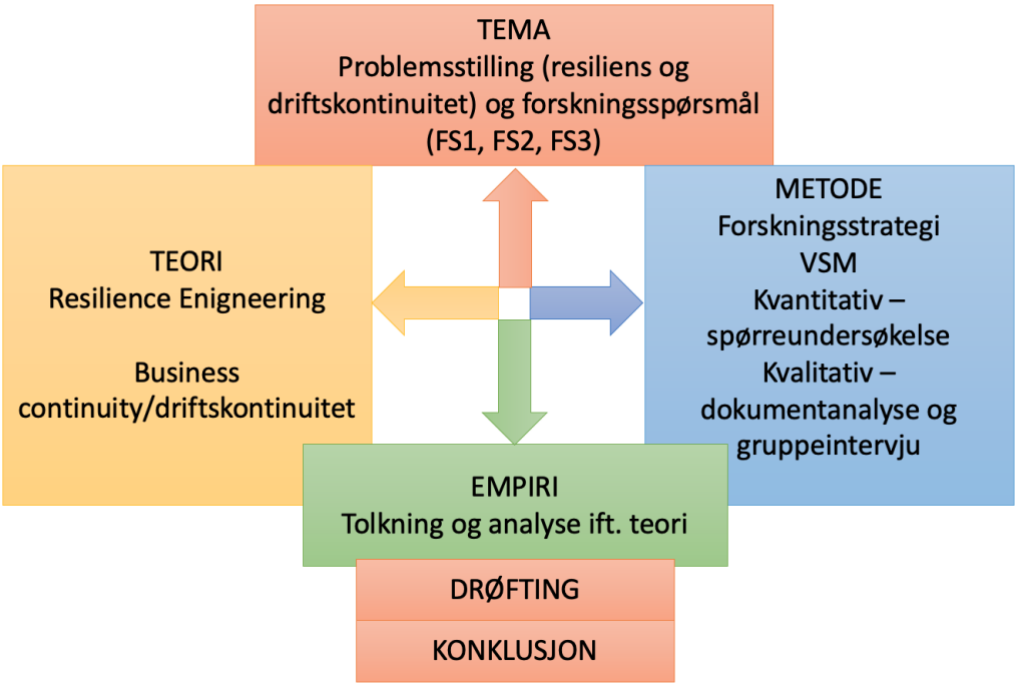
4. Metode

I dette kapittelet presenteres oppgavens forskningsdesign og hvilken måte datainnsamlingen er gjennomført for å kunne besvare problemsstillingen og de tilhørende forskningsspørsmålene. Kapittelet viser til at forskningsprosessen strekker seg etter krav til relevante teoriperspektiver, representativt utvalg av informanter og tilstrekkelig analyse på bakgrunn av relevant data. Oppgavens reliabilitet og validitet skal også sees nærmere på. Avslutningsvis skal det diskuteres fordeler og ulemper ved de metodologiske valgene.

4.1 Forskningsdesign

For å besvare oppgavens problemstilling og tilhørende forskningsspørsmål har vi valgt å inkludere dokumentanalyse, strukturerte gruppeintervjuer og en spørreundersøkelse. Metodevalget vårt inkluderer både kvalitativ og kvantitativ tilnærming, som også omtales som Mixed Methods Approach (MMA) (Blaikie & Priest, 2019). Denne studien bygger på Danermark et al. (2002) sin forståelse av abduktiv forskningsstrategi. Her finner man tre hovedtrekk: rekontekstualisering, tolkning og formell logikk. Dette innebærer å tolke, observere, forklare og beskrive et fenomen innenfor rammene av en ny kontekst. Abduksjon innebærer et tolkningselement, der vi skal gi mening til det vi observerer under forskningsprosessen og tolke dette på en bestemt måte med et forhåndsutvalgt teoretisk rammeverk. Dermed gir det en plausibel tolkning ut fra et konseptuelt rammeverk (Danermark et al., 2002). Basert på dette vil det si at vi har hatt som mål å tolke kraftforsyningen gjennom VSM og koble dette til utvalgt teori gjennom RE. På denne måten kan vi rekonstruere en forståelse av kraftforsyningskjeden gjennom et rammeverk basert på RE-prinsippene og driftskontinuitet. Danermark et al. (2002) trekker frem gjennom den abduktive tilnærmingen at formålet er å utvikle en forståelse for de dataene som samles inn med utgangspunkt i det valgte konseptuelle rammeverket. Dette kan trekkes til vårt formål med studien, der vi ser kraftforsyningen i lys av VSM for å skape en forståelse av systemet (kraftforsyningen). Videre ser vi på hvordan systemet er levedyktig, kompleksiteten den utgjør og hvordan systemene er

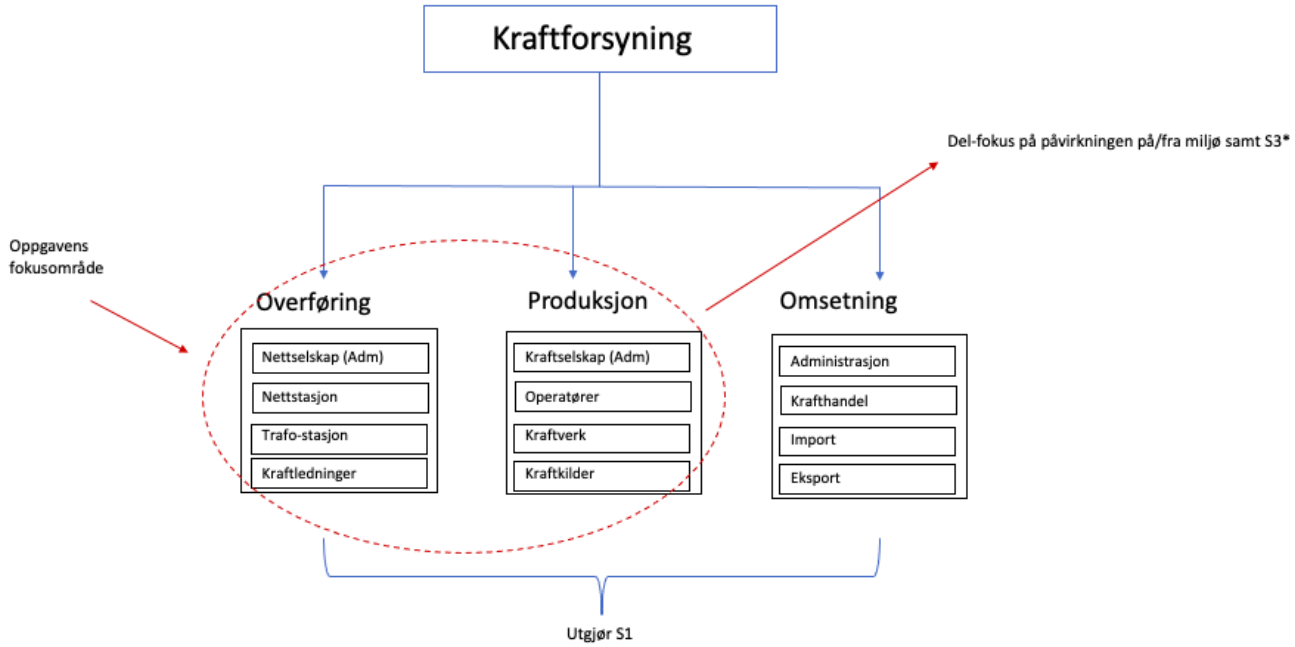
avhengige av hverandre. De valgte teoretiske rammeverkene vil kunne bringe frem en ny tolkning av kraftforsyningskjeden og hvordan aktørene er koordinert. Gjennom denne oppgaven har vi følgende forskningsdesign i en forenklet visuell fremstilling:



Figur 11 Forskningsdesign.

4.2 Anvendelse av VSM på den norske kraftforsyningen

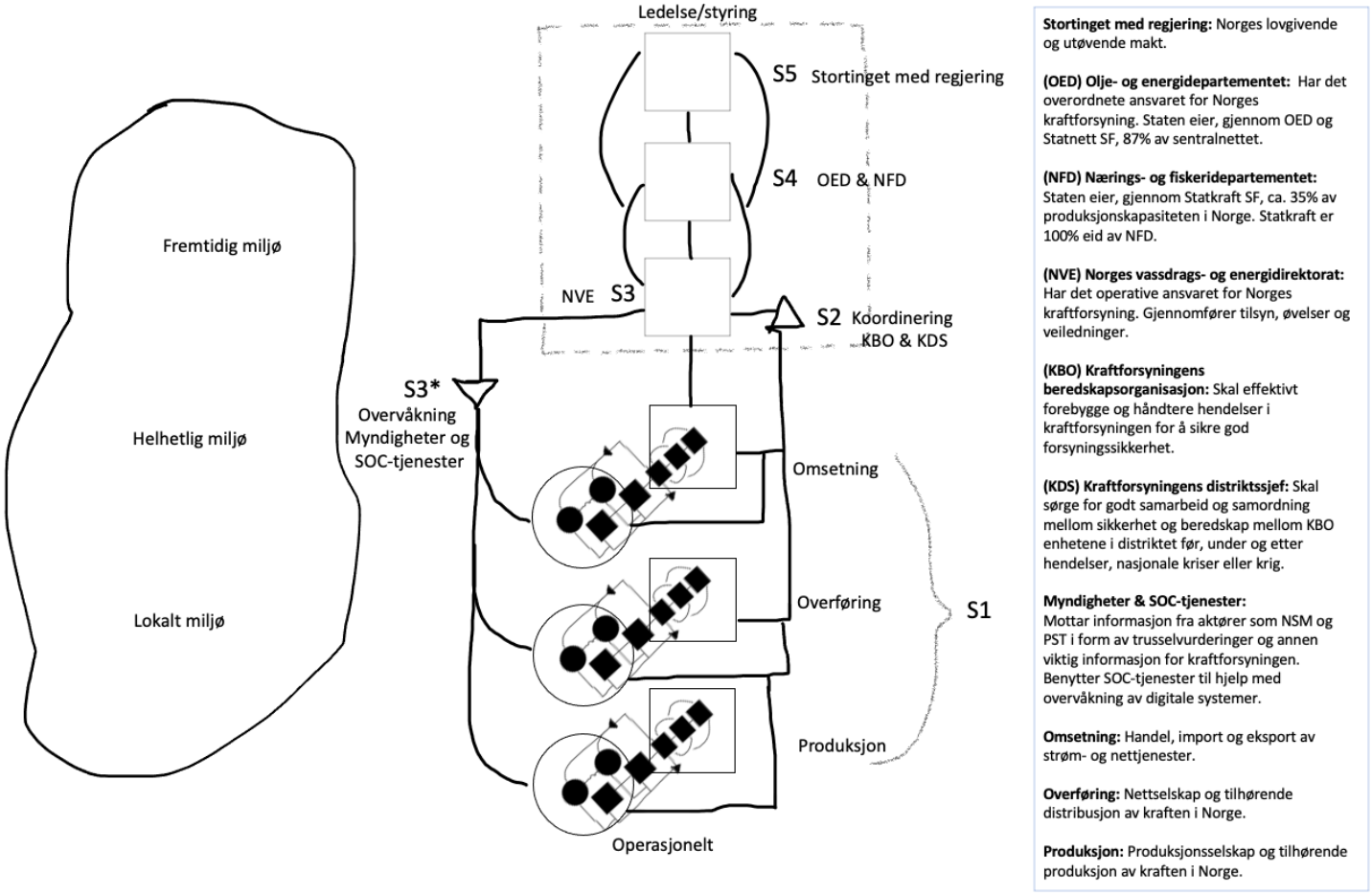
VSM sier at levedyktige systemer er organisert basert på rekursjonsprinsippet. Dette vil si at de har levedyktige systemer innen seg selv. For å anvende VSM på den norske kraftforsyningen har vi identifisert tre primære funksjoner i S1: produksjon, overføring og omsetning. Dette er kraftforsyningens grunnleggende funksjoner, og disse funksjonene er levedyktige systemer i seg selv. Det vil si at funksjonene er forenelig med det som Beer (1984) vektlegger med viktigheten av rekursjonsprinsippet, hvor systemene inneholder flere sub-systemer. Sub-systemene utgjør de primære funksjonene som systemene er avhengige av for å kunne eksistere og fungere på egenhånd. Det kan illustreres på denne måten:



Figur 12 Systemene i S1 og sine sub-systemer, samt oppgavens fokusområde.

Oppgavens fokusområde er illustrert i den røde stiplete linjen, og fokuset ligger her ettersom vi ønsker å se på hvordan systemene for overføring (distribusjon) og produksjon arbeider med RE og driftskontinuitet direkte innen seg selv. Samtidig har vi lagt inn et del-fokus på systemenes påvirkning på/fra miljøet samt S3* på bakgrunn av oppgavens problemstilling og tilhørende forskningsspørsmål. Ved å inkludere «*» bak S3* vises det til at den tilhører S3, men likevel er en separat del av systemet.

Ved anvendelsen av VSM på den norske kraftforsyningen har vi utarbeidet denne modellen:



Figur 13 VSM anvendt på den norske kraftforsyningen.

Nedenfor vil vi presentere en beskrivelse av systemene. Beskrivelsene er basert på Beer (1984 Pollock & Steen (2021), samt Buckl et al. (2009), og vi vil samtidig presentere vår anvendelse av modellen på den norske kraftforsyningen.

(S1) System 1 (Primære funksjoner): Hovedaktiviteten(e) som organisasjonen eksisterer for å gi. Den delen av det levedyktige systemet som produserer dette. Denne delen av systemet evner å produsere og vedlikeholde seg selv, uavhengig av de andre systemene, og inneholder i seg selv flere levedyktige system. I modellen vår inkluderer dette produksjon, overføring (distribusjon) og omsetning av kraft. Disse systemene er levedyktige i seg selv og er basert på rekursjon (se figur 12.). Systemene i S1 har direkte interaksjon med miljøet.

(S2) System 2 (Koordinering): Inkluderer de informasjonskanalene som sikrer at hovedaktivitetene ikke kommer i konflikt med hverandre og demper svingninger. Norges kraftforsyningsberedskap er organisert gjennom KBO, som befinner seg under NVE sitt ansvar. KBO-enhetene skal kunne forebygge og håndtere hendelser i kraftforsyningen. KBO

består av NVE og andre virksomheter som står for kraftforsyningen. Dette vil eksempelvis være alle som de driver eller eier kraftproduksjon med tilhørende vassdragsregulering, fjernvarme og overføring og distribusjon av elektrisk energi, som vi finner i S1. KDS er NVE sin representant i fylkesberedskapsrådet. KDS har som oppgave å opprettholde et godt samarbeid og samordning om sikkerhet og beredskap mellom de forskjellige KBO-enhetene i distriktet under ekstraordinære hendelser, nasjonale kriser eller krig (NVE, 2022b).

(S3) System 3 (Kontroll og sammenheng): Gjør de primære hovedaktivitetene til en større helhet ved å koble sub-systemene med systemene som de tilhører. I vår kontekst er det her vi finner NVE. Direktoratet har ansvaret for å forvalte energi- og vannressursene i Norge og er sentrale i kraftsektorens beredskapsarbeid. NVE har ansvaret for å samordne beredskapsplanleggingen og gjør dette blant annet gjennom KBO og KDS.

(S3*) System 3* (Overvåking): Omgår enhetsledelsen og engasjerer seg i virkeligheten til enhetenes aktiviteter. Her finner vi andre ansvarlige myndigheter i samråd med NVE, som for eksempel NSM og PST, i samsvar med ledelsen i virksomhetene som vi finner i S1. Dette er alle organisasjoner og myndigheter som aktørene i kraftforsyningen bruker i sitt arbeid med overvåkning av sektoren (eksempelvis ved oppdatering på dagens trusselbilde). For å overvåke sine digitale systemer bruker kraftforsyningsaktørene SOC-tjenester. Her befinner det seg cybersikkerhetsanalytikere som arbeider kontinuerlig for å overvåke og oppdage cyberrelaterte trusler (Shah et al., 2018). Disse er eksternt kjøpte tjenester som blant annet jobber med å overvåke digitale systemer, eksempelvis Telenor Security Operations Center. Ofte befinner disse SOC-tjenestene seg utenfor egen virksomhet, blant annet på bakgrunn av mangel på kompetanse innad i virksomheten og virksomhetens størrelse.

(S4) System 4 (Planlegging): S4 ser utenfor organisasjonen og inn i framtiden. Det tilbyr selvbevissthet for systemet-i-fokus (her kraftforsyningen). Her finner vi OED og NFD som er eiere av Statkraft SF og Statnett SF.

(S5) System 5 (Politikk, framtid og identitet): Den organisatoriske etos og distinktive identitet. Her finner vi de som er ansvarlig for å styre de overordnede politiske beslutningene. Strategisk beslutningstaking er en prosess av å tilpasse nåværende virkelighet til fremtidige behov. I vår kontekst er det regjeringen med stortinget som har som hovedoppgave å regulere kraftforsyningen gjennom lovverk og forskrifter, og tilpasse dette med hensyn til framtidige behov og endringer.

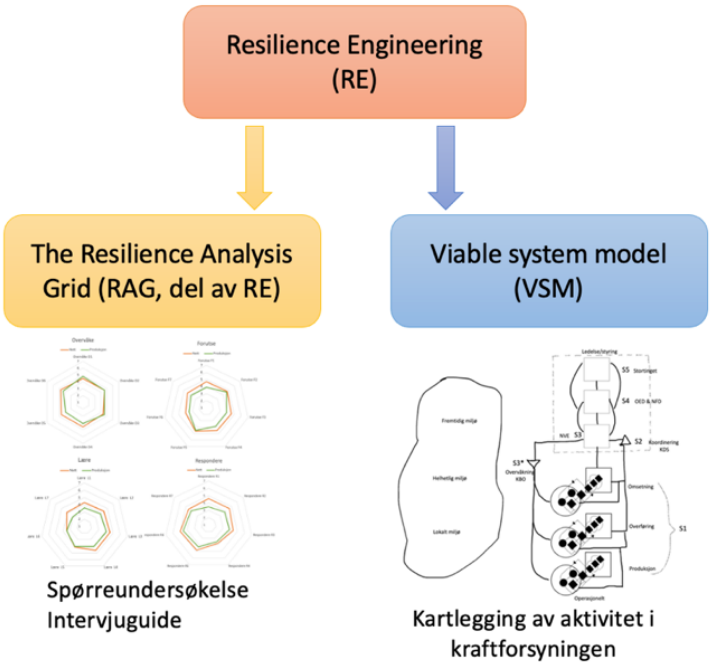
Miljø: Å beskrive og ta hensyn til miljøet er viktig for å vite hvordan systemet skal tilpasse seg og forberede seg på eventuelle endringer i miljøet. Miljø-delen av modellen viser både til «lokalt miljø» og «framtidig miljø». Lokalt miljø knytter seg direkte til S3 og S3* og handler om å tilpasse seg de lover og regler som er satt for sektoren, samt lokale omgivelser, dvs. dagens trusselbilde, dagens samfunn i henhold til teknologisk utvikling og klima og generelt de faktorer som kan påvirke systemet her og nå. Framtidig miljø knytter seg direkte til S5 og handler om tilpasningen til framtidige trusler, og eventuell forebygging av disse slik at systemet vil være levedyktig over tid. I oppgaven vår står det lokale miljøet i størst fokus ettersom vi ønsker å se på dagens trusler og dagens arbeid med RE og driftskontinuitet, og også hvordan dette står i stil med blant annet dagens lovverk.

Oppsummerende kan man si at S1-S3 kan sees på som styringen av «innsiden og nåtiden» av kraftforsyningen, mens S4-S5 styrer «utsiden og framtiden» (Buckl et al., 2009). I kraftforsyningen vil dette si at S1-3 konsentrerer seg om den daglige driften og hvordan driften skal tilpasses nåtiden, hvor S4-5 konsentrer seg om strategier og eventuelle endringer i systemet som alt er rettet mot framtiden. I forhold til dette ligger vårt fokus på S1 med delfokus på miljø og S3*, ettersom oppgavens problemstilling fokuserer på sektorens arbeid med å kunne opprettholde driften til tross for nåtidens trusler og utfordringer. Ved hjelp av Beers (1984, 1985) «diagnostic problems» har vi brukt VSM for å identifisere systemet (kraftforsyningen), og problemene som kan oppstå i kraftforsyningen ved å neglisjere arbeidet med RE og driftskontinuitet i kraftforsyningens individuelle systemer, og som dermed kan true sektorens/hele systemets levedyktighet over tid. Dette kommer vi tilbake til i oppgavens drøfting (kapittel 6).

4.3 Datainnsamling: Kvalitativ og kvantitativ tilnærming

Det har lenge vært et dominerende skille mellom kvalitativ og kvantitativ metode i samfunnsvitenskapen (Marx et al., 2014). Kvalitativ metode uttrykkes ofte i form av tekst, utvalget er som regel mindre og forskeren er i kontakt med aktørene som skal studeres. Her er det viktig å utforske den sosiale aktørens meninger og man er ute etter diskursive beskrivelser (Blaikie & Priest, 2019). Typiske metoder er ulike former for intervju, dokumentanalyse og deltakende observasjon. Intervju er en av de mest brukte metodene i kvalitativ forskning (Qu & Dumay, 2011). Kvantitativ metode er mer fleksibel i sin natur og kan sies å være mer uforutsigbar. I den forstand at man er ute etter å måle og tallfeste aspekter ved det sosiale livet (Blaikie & Priest, 2019). Metoder som kan anvendes her er eksempelvis spørreskjema, regresjonsanalyser og todimensjonal analyse. Det prinsipielle skillet baserer seg hovedsakelig

på hvordan data registreres og analyseres (Johannessen et al., 2021). I de senere årene har det oppstått et behov for å både inkludere kvalitativ og kvantitativ metode for å dekke omfanget av forskningen i studier i samfunnsvitenskapelig metoder. Dette er på bakgrunn av at flere av de samfunnsvitenskapelige studiene er store og komplekse, og dermed trenger mer data å forholde seg til. Dette har skapt sammenslåingen av disse metodene og har fått navnet MMA. På bakgrunn av dette er det valgt å gjennomføre en dokumentanalyse, strukturerte gruppeintervjuer og en spørreundersøkelse. Dermed kan problemsstillingen og forskningsspørsmålene besvares på en triangulert måte. Nedenfor vises en oversikt over hvilket teoretisk grunnlag som er brukt i utførelsen av metodevalgene og visualiseringen av kraftforsyningen og hvilke virksomheter som er inkludert gjennom spørreundersøkelse og gruppeintervju.



Figur 14 14 Teoretisk grunnlag brukt i utførelsen av metode.

Tabell 2 Tabelloversikt over sendte spørreundersøkelser og gruppeintervjuer fordelt på hver virksomhet.

	Produksjonsselskap		Nettselskap	
	P1	P2	N1	N2
Gruppeintervju med relevante ansatte	x	x	x	x
Spørreundersøkelse	x	x	x	x

4.5 Kvantitativ analyse

4.5.1 Valg av informanter til spørreundersøkelse

Da vi skulle kontakte relevante aktører i kraftforsyningen, måtte vi velge ut ansatte som er relevante for problemsstillingen. Det kan dermed sies at det ble foretatt et såkalt «purposeful sampling» (Johannessen et al., 2021), der valget på informanter baserer seg på hvilke arbeidsoppgaver de har i produksjon- og nettselskapet. Vi fikk kontakt med informanter til oppgaven ved å gjennomføre telefonsamtaler med relevante aktører høyt oppe i virksomhetene. Disse sendte oss videre til våre kontaktpersoner, som var enhetsledere i de aktuelle nett- og produksjonsselskapene. Deretter sendte vi ut informasjon i en e-post til våre kontaktpersoner i virksomhetene (se vedlegg 2). På denne måten fikk vi direkte kontakt med ledere og kunne da bli henvist videre til riktige personer for vårt formål. Det kan dermed sies at vi tok i bruk snøballmetoden (Johannessen et al., 2021), hvor vi da rekrutterte informanter ved at vi avhørte oss om hvilke personer som er relevante til å gjennomføre denne spørreundersøkelsen, som hovedsakelig arbeider med drift, vedlikehold, informasjonssikkerhet og beredskap i virksomheten. Kontaktpersonene våre i de ulike virksomhetene hadde kontroll på hvem som arbeider under dem og enklere kunne videresende lenken til spørreundersøkelsen til sine ansatte.

I henhold til spørreundersøkelsen ville vi inkludere så mange som mulig i de ulike virksomhetene for å kartlegge resiliensen gjennom RAG. Vi valgte å inkludere både informanter fra administrative stillinger som ledelse og administrasjon, og stillinger som driftsoperatører, ingeniører og konsulenter. Informantene hadde også muligheten til å legge inn sin stillingstittel. Fokuset i denne oppgaven er ikke å skille de ulike stillingstitlene fra hverandre, men å se et helhetlig bilde av arbeidet med resiliens gjennom RAG som supplement for gruppeintervjuene. Valget på disse informantene ble gjort for å øke kausaliteten med dataene som produseres. I tillegg, var det også viktig at antallet av valgte informanter skulle være stort nok til å kunne besvare problemsstillingen og de tilhørende forskningsspørsmålene. Dette for å kunne skape en bedre forståelse av konteksten til oppgaven, og på den måten fange opp ulike perspektiver for å kunne danne et bredere bilde av hele kraftforsyningen. På denne måten kunne vi unngå bias og for ensidige data gjennom spørreundersøkelsen. I henhold til kraftforsyningen som vi har kartlagt gjennom VSM ble også valget av informanter valgt på bakgrunn av oppgavens hovedfokus på virksomheter i S1 (se figur 12 og 13).

4.5.2 Utforming av spørreundersøkelse

For denne oppgavens formål ble det gjort et valg om å gjennomføre spørreundersøkelse. Spørreundersøkelser er en svært vanlig kvantitativ datainnsamlingsmetode. En kvantitativ spørreundersøkelse skal være utformet på en så enkel og forståelig måte at den som skal besvare den ikke trenger noen annen hjelp enn forhåndsbestemte, nedskrevne instruksjoner (Blaikie & Priest, 2019). Bakgrunnen for gjennomføring av spørreundersøkelse er basert på at vi på den måten kan inkludere flere enheter som enkelt kan systematiseres og standardiseres (Jacobsen, 2005). Spørreundersøkelsen ble utformet på bakgrunn av det teoretiske grunnlaget i RAG (se tabell 4) og spørsmålene ble dermed formulert deretter. Dette er gjennomført på en forenklet måte for å kartlegge resiliens hos både nett- og produksjonsselskapene. Ved å inkludere RE prinsippene: overvåke, forutse, respondere og lære. Programmet som ble valgt for gjennomføring av spørreundersøkelsen var SurveyXact som vi fikk tilgang til gjennom Universitetet i Stavanger. Programmet er laget for å gjennomføre spørreundersøkelser og legger til rette for behandling av sensitiv informasjon som personvern. Dette programmet har hjulpet oss med å fremstille svarene i enkle analyser før vi senere tok svarene og analyserte dem i henhold til RAG.

Vi startet med å gjennomgå de standardiserte spørsmålene til RAG. Ut ifra disse spørsmålene oversatte vi fra engelsk til norsk på en enkel og forståelig formulert måte, med påstander hvor informantene måtte ta stilling til i hvilken grad de var enig i påstanden. Påstandene ble i stor grad omformulert på en forståelig og presis måte, for å prøve å unngå dobbeltbetydning. Formuleringen av påstandene ble dobbeltsjekket av våre kontaktpersoner i Safetec Nordic AS. *Påstandene blir presentert i tabellene i empirikapittel 5.1.3.* På bakgrunn av dette mener vi at påstandene kan trekkes til RAG-tilnærmingen og på den måten fortsatt kartlegge resiliens i virksomhetene. Vi valgte å ikke inkludere alle påvirkningsfaktorene som er presentert gjennom RAG, fordi vi ikke anså det som nødvendig i henhold til oppgavens problemstilling. Dermed er noen av påstandene formulert gjennom samme påvirkningsfaktor som henvist i tabell 4.

Påstandene ble besvart med en gradering fra «*helt uenig*» til «*helt enig*». Vi valgte også å inkludere svaralternativene «*vet ikke*» og «*ikke relevant*». Til sammen er det syv ulike svaralternativer: *helt uenig, delvis uenig, verken enig eller uenig, delvis enig, vet ikke* og *ikke relevant* (Nivå 1-7). Bakgrunnen for valget på «*vet ikke*» og «*ikke relevant*» baserer seg på at vi valgte å inkludere flere ansatte som arbeider i nett- og produksjonsselskaper med mange forskjellige oppgaver, som eksempelvis drift/vedlikehold, ledelse og administrasjon. På den måten kunne eksempelvis en ansatt med stillingen *«driftsoperatør»* anse flere av påstandene

som ikke relevant for sin stilling, og fikk dermed muligheten til å krysse av for alternativet «*ikke relevant*». På samme måte kunne en i ledelsen se på den samme påstanden og oppleve den som relevant for sin stilling, og krysse av for svaralternativet som passer den personens holdninger. Hvis informantene ikke var kjent med en påstand, hadde de mulighet til å krysse av for «*vet ikke*». Dersom de ansatte stilte seg nøytral til en påstand kunne de krysse av for «*verken uenig eller enig*». I introduksjonen til spørreundersøkelsen ble det gitt med beskrivelser for når de kunne benytte svaralternativene *«ikke relevant», «vet ikke» og «verken uenig eller enig»*. Gjennom rangeringen av svaralternativer kunne vi måle intensiteten i holdninger gjennom påstandene (Jacobsen, 2005). Påstandene ble formulert på en enkel måte og uten vanskelige fremmedord, og de begrepene som kunne virke spesielt fremmed ble definert i introduksjonen til spørreundersøkelsen. Dette ble et viktig steg i prosessen for å unngå upålitelige svar. Det ble også gjort et forsøk på å gjøre undersøkelsen så kort som mulig for å oppnå en høy svarprosent. Spørreundersøkelsen tok mellom 3-5 minutter å gjennomføre, noe som ikke var for lang tid slik at de ansatte skulle ha mulighet til å gjennomføre den i arbeidstiden. Undersøkelsen var anonym å svare på og valgfri å ta for de som mottok den.

Tabell 3 Visuell fremstilling av svaralternativene

Nivå 1	Nivå 2	Nivå 3	Nivå 4	Nivå 5	Nivå 6	Nivå 7
Helt uenig	Delvis uenig	Verken enig eller uenig	Delvis enig	Helt enig	Vet ikke	Ikke relevant

Tabell 4 Liste over påvirkningsfaktorer av resiliens brukt i henhold til utforming av spørreundersøkelse (se Hollnagel, 2011. s. 284-288) (inspirasjon fra Steen et al., 2021)

Overvåke	Forutse	Respondere	Lære
O1: Indikator	F1: Kommunikasjon	R1: Hendelseslite	L1/L2: Seleksjonskriterier
O2: Indikator type	F2: Frekvens	R2: Grunnlag	L3: Datainnsamling/ Klassifisering
O3: Validitet	F3/F4: Antakelser	R3: Terskel for respons	L4: Frekvens
O4: Målfrekvens	F5: Tidsaspekt/ forutsigelser	R4: Respons liste	L5: Læringsmål
O5: Stabilitet	F6: Risikoaksept	R5: Hurtighet	L6: Verifikasjon
O6: Verifikasjon/revisjon	F7: Årsakssammenheng	R6: Varighet/ Ressurser	L7: Læringsmål
		R7: Normalisering	

4.5.3 Gjennomføring av spørreundersøkelse og anonymitet

Det ble gjennomført en spørreundersøkelse fordelt på fire virksomheter, to produksjonsselskap (P1, P2) og to nettselskap (N1, N2). Avhengig av tidsperspektivet til de ulike virksomhetene ble undersøkelsen delt ut til de forskjellige virksomhetene på ulike tidspunkt. P1 og P2 fikk undersøkelsen utdelt først, og deretter N1 og N2 med egne interne gjennomføringsfrister på én

uke. Undersøkelsen ble likevel liggende åpen til de to siste virksomhetene hadde gjennomført den, og vi stengte undersøkelsen helt etter den interne fristen hadde gått ut hos de to siste virksomhetene (N1 og N2). På den måten hadde spørreundersøkelsen vært ute i 30 dager til sammen. Vi fulgte med på om det kom inn flere informanter fra første utdeling hos P1 og P2, hvorav bare en person tok den etter deres interne frist hadde gått ut. Dermed så ikke vi det som utslagsgivende for funnene at spørreundersøkelsen var åpen lenger for de to første enn for de to siste virksomhetene. Hvis man hadde gjennomført spørreundersøkelsen kunne man heller ikke ta den igjen. På startsiden til spørreundersøkelsen ble det som nevnt inkludert noen definisjoner/forståelser av begreper som brukes i spørreundersøkelsen, for å redusere misforståelser eller feiltolkninger av påstandene. Begrepene vi inkluderte var: system, beredskap, beredskapsplan, beredskapshendelse, kontinuitetsplaner, risiko, risikoforhold, hendelser/uønskede hendelser og trusselbilde.

Det er viktig at personvernet blir godt ivaretatt når man sender ut en spørreundersøkelse. Det ble inkludert i introduksjonen til spørreundersøkelsen at den var frivillig å ta, og at de, ved å gjennomføre den, samtykket til at svarene ville bli brukt for tolkning i vår oppgave. Prosjektet og intervjuguiden har blitt godkjent gjennom *Sikt* (se vedlegg 4), og godkjenningen viser til at vi må tilrettelegge for at personvernet blir ivaretatt. Det var viktig for oss at ingen ville bli gjenkjent av oss gjennom spørreundersøkelsen, og dermed valgte vi å sende ut en felles spørreundersøkelse for alle fire virksomhetene og ikke skille mellom dem. På den måten kunne ingen av de ansatte «spores» tilbake på hva de hadde svart. Formålet med denne oppgaven er å se på overordet nivå den generelle oppfatningen av prinsippene i RE hos de fire virksomhetene. Våre kontaktpersoner i de ulike virksomhetene sendte lenken med spørreundersøkelsen videre til de aktuelle kandidatene, og på den måten hadde vi ingen måte å kunne spore informantene tilbake på og dermed sikret deres anonymitet.

Tabell 5 Oversikt over utsendt spørreundersøkelse med tilhørende utdelinger i virksomhetene.

	Produksjonsselskap		Nettselskap	
	P1	P2	N1	N2
Spørreundersøkelse	Sendt 28.02.2023 Svarfrist 03.03.2023	Sendt 28.02.20203 Svarfrist 03.03.2023	Sendt 07.03.2023 Svarfrist: 10.03.2023	Sendt 14.03.2023 Svarfrist: 17.03.2023
Antall som har mottatt undersøkelsen	8	6	10	19

Tabell 6 Prosentandel som har svart på spørreundersøkelsen.

	Produksjonsselskap (P1 og P2)	Nettselskap (N1 og N2)
Sendt til	14	29
Gjennomført	10	19
Total prosentandel gjennomført	**71,4%**	**65,5%**
Overordnet svarprosent	**67,4%**	

4.6 Kvalitativ analyse

I den kvalitative delen av analysen benyttet vi dokumentanalyse og strukturerte gruppeintervjuer. Først og fremst gjorde vi en grundig dokumentanalyse for å skape et godt grunnlag som senere skal supplere funnene vi gjorde fra gruppeintervjuene. Deretter hadde vi et ønske om å kartlegge virksomhetenes syn på driftskontinuitet og prinsippene i RE, sett opp mot SC, og få fram deres synspunkter på dette via strukturerte gruppeintervjuer. Målet med dette har vært å finne ut hvordan og hvor mye virksomhetene arbeider med prinsippene i RE og driftskontinuitet både direkte og indirekte i henhold til SC, og til slutt analyserte vi dette i relasjon til kartleggingen vi gjorde gjennom RAG og spørreundersøkelsen.

4.6.1 Dokumentanalyse

Som utgangspunkt for oppgaven og et nødvendig steg for å forstå helheten i den norske kraftforsyningen, har det vært essensielt og helt nødvendig å gjennomføre en dokumentanalyse. En dokumentanalyse kan også kalles for en kvalitativ innholdsanalyse, og brukes av forskeren for å samle inn data som analyseres for å få frem informasjon og sammenhenger som er spesifikt knyttet til det som forskeren ønsker å studere (Grønmo, 2004). I dokumentanalysen har vi tatt for oss en rapport, en stortingsmelding, Norges offentlige utredninger, energiloven og kraftberedskapsforskriften. Å bruke dokumentanalyse som en del av en kvalitativ metode vil si at man identifiserer tema og fenomen og knytter det opp mot det man ønsker å studere (Blaikie & Priest, 2019). I denne prosessen var problemstillingen helt avgjørende for hvilken informasjon vi skulle velge å hente ut fra de forskjellige dokumentene. Dokumentene vi har brukt er stort sett sekundær- og tertiærdata. Dette betyr at dokumentene anvender allerede eksisterende data som er offentlig og noe er tolket gjennom de ulike dokumentene (Grønmo, 2004). På denne måten er det hensiktsmessig å nevne at dokumentene kan være skrevet på bakgrunn av et annet grunnlag enn denne oppgavens hensikt. I søket etter dokumenter har vi brukt søkeord som «kraftforsyning», «kraft» og «kraftproduksjon», «forsyningssikkerhet» og «strømnett». Det har videre blitt brukt Nvivo for kryss-analysere ulike kategorier for å systematisere dataene samt effektivisere prosessen, som vi fikk tilgang til gjennom universitetet i Stavanger. Her valgte vi å kode materialet gjennom overordnede kategorier. Kategoriene var: forsyningssikkerhet, beredskap og driftskontinuitet, risiko, koordinering,

drift, trusselbilde og IKT-sikkerhet. Dokumentene presenteres i tabellen under, der fokusområde og dokumentenes relevans i forhold til oppgaven presiseres. Dokumentene vil bli brukt supplerende i henhold til funnene våre i oppgavens drøfting i kapittel 6.

Tabell 7 Oversikt over dokument og lovverk.

Dokumenter	Fokusområde	Dokumentets relevans til oppgaven
Olje- og energidepartementet (2014). Et bedre organisert strømnett.	Organisering av det norske strømnettet. Hovedfokuset ligger på de tre ulike nettene (sentral-, regional-, og lokalnettet). Inkluderer også produksjonsselskaper i forhold til avhengigheten til strømnettet.	Dokumentet stryker bakgrunnskunnskapene og gir en bedre kontekst for virksomhetsområdet generelt. Synliggjør verdikjeden til kraftsektoren.
Meld. St. 25 (2015-2016). (2016). Kraft til endring— Energipolitikken mot 2030. Olje- og energidepartementet.	Handler om kraftforsyningens hovedområde for utviklingstrekk, status og perspektiver. Inkluderer også Europas betydning for den norske kraftforsyningen og det globale energimarkedet.	Dokumentet styrker bakgrunnskunnskapen og konteksten og synliggjør verdikjedene til kraftforsyningen. Viser også til en forbedret forsyningssikkerhet.
Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften)	Forskrift om sikkerhet og beredskap i kraftforsyningen, inkluderer alle KBO-enheter.	Egne kapitler om informasjonssikkerhet og beskyttelse av driftskontrollrom (kap. 6 og 7). Relevant for SC.
Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven)	Fokusområder på de overordnede områdene i energiforsyningen: produksjon, omforming, overføring, omsetning, fordeling og bruk av energi.	Kap. 9. omhandler beredskap i kraftforsyningen (KBO-enheter)
NOU 2023:3 (2023). Mer av alt – raskere – Energikommisjonens rapport.	Kartlegge energibehovene og foreslå økt energiproduksjon med mål om at Norge skal ha overskudds produksjon av kraft og at rikelig tilgang på fornybar energi skal være en konkurranse fortrinn for norsk industri.	Nyere rapport som viser til den norske kraftproduksjonen og forsyningssikkerhet i forhold til dagens situasjon. Energikommisjonen kommer med tiltak og anbefalinger når det kommer til styrket forsyningssikkerhet i Norge. Dette viser også hvordan verdikjedene i kraftforsyningen er avhengige av hverandre.

4.6.2 Valg av informanter til gruppeintervju

Når det kom til valg av informanter til gruppeintervjuer kontaktet vi de relevante aktørene på samme måte som ved spørreundersøkelsen (se kapittel 4.5.1). En forskjell fra informantene til spørreundersøkelsen, er at det her ble inkludert mindre grupper fra hver virksomhet. Gruppene var sammensatte av informanter i forskjellige stillinger, som ledelse og administrasjon, driftsoperatører og ingeniører. Noen beredskapsansvarlige var også med. Alle hadde relevante arbeidsoppgaver i henhold til vår problemsstilling og tilhørende forskningsspørsmål. Dermed

ble valget på informanter til gruppeintervjuene inkludert på bakgrunn av deres rolle i sin virksomhet. På bakgrunn av spørsmålene i intervjuguiden, så vi på det som nødvendig å ha gruppeintervju der de ulike ansatte hadde ulike arbeidsoppgaver. På den måten kunne de spille hverandre gode, og svare utfyllende på de spørsmålene vi hadde. Virksomhetenes størrelse varierte og på den måten kunne én person i en virksomhet ha flere roller og ansvarsområder enn en person i de større virksomhetene. Oppsummerende vil det si at det var kunnskapen personene satt på som var viktigst for oss i henhold til oppgavens formål som utgjorde utvalget til intervju. Vi stilte ingen krav til at informantene som ble intervjuet måtte ha gjennomført spørreundersøkelsen. Vi nevnte likevel at de kunne være en fordel ettersom vi tok opp noen av funnene våre fra spørreundersøkelsen i gruppeintervjuene.

4.6.3 Utforming av intervjuguide og strukturert gruppeintervju

Før vi startet med gjennomføringen av gruppeintervjuene utformet vi intervjuguiden vår. Den ble holdt kort og presis, og ble lagt opp på en slik måte at informantene kunne fortelle mest mulig rundt spørsmålene. Vi måtte likevel utforme spørsmål i henhold til oppgavens problemsstilling, og på den måten kunne vi få svar på det vi trengte. Intervjuguiden ble utformet ved hjelp av det teoretiske grunnlaget om prinsippene i RE og driftskontinuitet. I tillegg til dette fikk vi hjelp av vår veileder, samt kontaktpersoner i Safetec Nordic AS, til utformingen av spørsmål og ferdigstillingen av intervjuguiden. Intervjuguidens kjernespørsmål tok for seg SC, og gikk i dybden inn på det teoretiske grunnlaget bak. Dermed gjennomførte vi strukturerte gruppeintervju, som vil si at vi tok utgangspunkt i en overordnet intervjuguide for alle gruppeintervjuene hvor alle spørsmålene skulle bli besvart systematisk (Johannessen et al., 2021) (se vedlegg 1 for intervjuguide). Det ble stilt oppfølgingsspørsmål som ikke var inkludert i intervjuguiden der det ble ansett som relevant, og på den måten kunne vi utdype spørsmålene nærmere og mer utfyllende. Alle virksomhetene fikk de samme forhåndsbestemte spørsmålene. Dette gjorde vi fordi vi ønsket å se hvordan de arbeider med prinsippene i RE og driftskontinuitet, og eventuelt oppdage nyanser i svarene deres. Vi hadde et overordnet mål om at intervjuene ikke skulle oppleves for formelle, men likevel være preget av en viss strukturert standard. Under gruppeintervjuene fikk informantene muligheten til å rekonstruere hendelser ved hjelp av egne ord og språk (Johannessen et al., 2021). På denne måten kunne de svare fritt på spørsmålene.

Gruppeintervju er også en form for kvalitativt intervju der en gjerne har en moderator som organiserer og styrer en diskusjon mellom et utvalg av deltakere rundt et tema (Johannessen et al., 2021). På bakgrunn av oppgavens omfang og valget vårt om å gjennomføre et strukturert

intervju, valgte vi å gjennomføre gruppeintervjuer med 2-5 deltakere, også en såkalt «minigruppe» (Johannessen et al., 2021). Dette gjorde vi fordi vi ønsket å se hvordan personene på intervjuene diskuterte med hverandre, samtidig som vi ikke ønsket for mange deltakere slik at alle fikk komme til med sine svar og meninger. Det vil også være flere fordeler med å gjennomføre gruppeintervju i minigrupper, blant annet at det kan være lettere å diskutere sensitive tema, det kan være lettere å ta ordet, og man kan få fram flere detaljer. Oppgavens hensikt er heller ikke å gjøre rede for individuelle synspunkter, men heller gruppesynspunkter (Johannessen et al., 2021), på virksomhetsnivå.

4.6.4 Gjennomføringen av gruppeintervju

Det ble gjennomført gruppeintervju hos alle fire selskapene som mottok spørreundersøkelsen. Dermed landet vi på en total gjennomføring av fire gruppeintervjuer, med totalt 13 informanter. Gruppeintervjuene ble gjennomført med en blanding av ledere og ansatte som ingeniører, informasjonssikkerhetsansvarlige, beredskapsansvarlige og driftsoperatører. Basert på gruppesammensetningen var vi ute etter kunnskapen de sitter på, og ikke hvilken stillingstittel de har.

Intervjuene ble gjennomført på Microsoft Teams. På den måten ble det enklere og mer fleksibelt i måten vi har gjennomført intervju på, siden flere av virksomhetene er lokalisert på forskjellige steder rundt i Norge. Dermed fikk vi samlet inn data på en fleksibel og miljøvennlig måte. I forkant av intervjuene fikk hver virksomhet tilsendt informasjon gjennom Teams-innkallelsen med det forhåndsskrevne scenarioet og en samtykkeerklæring som måtte signeres før intervjustart. SC ble brukt som utgangspunkt for kjernespørsmålene i gruppeintervjuet. Vi startet intervjuene med å presentere oss selv og kort om prosjektet vårt før vi startet med introduksjonsspørsmålene. Vi ønsket at informantene skulle se at vi er to masterstudenter som tar dette på alvor. Weiss (1994) påpeker at samarbeidet mellom forskeren og informantene er viktig for å produsere gode data. Dermed var det viktig for oss å gi et hyggelig, inkluderende og profesjonelt inntrykk, og fortelle informantene at de kunne fortelle oss alt de tenkte på uten at dette kommer til å få noen konsekvenser for dem og deres arbeidsplass.

Gjennomføringen av intervjuene på Teams gikk ryddig for seg. Vi hadde opprettholdt kontakten med våre kontaktpersoner i hver virksomhet slik at vi kjente til de på forhånd, som gjorde gjennomføringen av gruppeintervjuet naturlig. De kunne når som helst stille spørsmål til oss hvis det var noe de lurte på. Dynamikken mellom oss og de ulike gruppene i hver virksomhet var bra og informantene i gruppene spilte hverandre gode, samtidig som de

utfordret hverandre i henhold til enkelte svar på våre spørsmål. Vi utfordret også informantene på ulike måter gjennom spørsmålene, noe de tok veldig bra. Selv om undertonen i intervjuet var alvorlig, kunne vi ha humor rundt enkelte temaer. På denne måten fløt samtalen mellom informantene gjennom hvert spørsmål på en god måte og vi fikk svar på spørsmålene vi hadde i intervjuguiden vår. Vi fikk et overordnet inntrykk av at hver virksomhet var ærlige i svarene de hadde på spørsmålene våre. Selskapene varierte likevel i måten de mottok spørsmålene på. Det framstod som om N1 ikke skjønte helt hvorfor vi hadde et fokus på produksjonsselskaper under deres intervju, selv om vi forklare at vi skulle se på hele forsyningskjeden og koordineringen mellom nett- og produksjonsselskapene. Cyberangrep, som SC, var kjent for de fleste selskapene (N1, N2 og P2), men omfanget av SC som vi presenterte var derimot de fleste ikke veldig godt kjent med. P1 forklarte at de ikke var særlig kjent med et slikt scenario, blant annet på bakgrunn av at de deler driftssentral med et nettselskap hvor bare ansatte fra nettselskapet sitter. Dette betyr at nettselskapet som de er koordinert med sitter på kontrollen over driftssentralen og ulike former for beredskapssituasjoner som oppstår der. Dette redegjøres ytterligere for kapittel 5.

Tabell 8 Oversikt over antall deltakere per virksomhet.

	Produksjonsselskap		Nettselskap	
	P1	P2	N1	N2
Gjennomført gruppeintervju	10.03.2023	16.03.2023	17.03.2023	24.03.2023
Antall deltakere	3	2	5	3

Alle informantene fikk tilsendt samtykkeerklæringen på forhånd av gruppeintervjuene (se vedlegg 3). På denne måten kunne hver informant lese hva deltagelse i gruppeintervju betydde for dem. Informantene kan når som helst trekke samtykke fram til innlevering og på denne måten blir personvernet i varetatt. Samtykkeerklæringen er utformet på bakgrunn av malen til *Sikt*. Alle informantene som deltok i gruppeintervjuet vil gjøres anonyme, og på den måten vil ingen kunne kjenne de igjen, utenom de andre som deltok på samme gruppeintervju.

Etter at alt fra gruppeintervjuene ble transkribert begynte utvalget av datamateriale som skulle brukes i analysen. Alt av datamateriale ble tatt opp ved hjelp av diktafon-appen fra Universitetet i Oslo, og det som ble nevnt utenfor forskningsspørsmålene ble ekskludert. Hovedelementene fra intervjuguiden blir brukt i analysen. Koding kan hjelpe å organisere

datamaterialet (Blaikie & Priest, 2019). Ved hjelp av koding av gruppeintervjuene kunne vi organisere materialet på en systematisk måte. Dette ble gjennomført ved hjelp av Nvivo, som kan brukes til å kategorisere ulike temaer som er relevante for vår masteroppgave. De overordnede kategoriene som ble brukt er: prinsippene i RE og driftskontinuitet. Videre hadde vi underkategorier for de ulike overordnede kategoriene som er basert på det teoretiske grunnlaget.

4.7 Validitet, reliabilitet og etiske betraktninger

Når det kommer til datagrunnlagets psykometri er validitet og reliabilitet brukt til å kvalitetssikre resultatene gjennom datainnsamlingen som er gjennomført. Validitet handler om at vi måler det vi har til hensikt å måle, mens reliabilitet tar for seg om undersøkelsen er til å stole på (Ringdal, 2018247). Forenklet betyr validitet hvor godt spørsmålene måler det vi vil måle, og reliabilitet hvor pålitelige svar informantene gir. Avslutningsvis skal det redegjøres for noen etiske betraktninger.

Validitet og reliabilitet i spørreundersøkelsen

I forhold til spørreundersøkelsen er validiteten påvirket av ulike faktorer. RAG-tilnærmingen er oversatt fra engelsk til norsk. Påstandene under RAG er formet ut ifra generelle påstander under de fire hovedtemaene med tilhørende undertema, eksempelvis «overvåke» som hovedtema og «kommunikasjon» som undertema (se tabell 4). Vi valgte å ikke inkludere alle undertemaene fordi det ble for mange spørsmål for en spørreundersøkelse med vårt formål. Grunnen til at vi ikke inkluderte alle undertemaene var fordi vi ville ha en overordnet kartlegging av resiliens i virksomhetene og denne spørreundersøkelsen skulle supplere gruppeintervjuene som gikk dypere inn på problemsstillingen. Etter vi hadde forenklet spørsmålene, satte vi det inn i konteksten til kraftforsyningen, for at det skulle gi mening for informantene. Vi var veldig påpasselige med at spørsmålsformuleringene skulle være enkle, fordi forskjellige informanter med ulik kunnskap skulle ta denne undersøkelsen. På den måten blir validiteten styrket ved at vi har klart formulerte spørsmål som er enkle å forstå basert på det teoretiske grunnlaget. Videre kan oversettelsen fra engelsk til norsk påvirke validiteten. Dermed gjennomgikk vi hvert spørsmål som vi har inkludert og påså at kjerneelementene i RAG var til stede. Basert på dette kan vi gjennom spørreundersøkelsen kartlegge det vi faktisk var ment å kartlegge - nemlig resiliens.

For å styrke validiteten til spørreundersøkelsen ble det gjennomført en «pilot-test» (Saunders et al., 2019). Spørreundersøkelsen ble revidert en del ganger basert på tilbakemeldinger vi fikk

fra test-gruppene. Vi gjennomførte to pilottester med ulike grupper. Den første gruppen var gjennom våre kontaktpersoner i Safetec Nordic AS. Den andre gruppen var våre medstudenter på universitetet. På denne måten fikk vi tilbakemeldinger på om spørsmålene i spørreundersøkelsen ga mening. Dette kalles også *face validity* og blir ofte brukt gjennom en pilottest for å undersøke hvorvidt spørsmålene gir mening eller ikke. Gjennom dette fikk vi også undersøkt hvor lang tid spørreundersøkelsen tok, og dermed forsikret oss at den ikke var for lang. Tilbakemeldingene gikk også ut på hvilke begreper som var uklare og trengte en definisjon i starten av spørreundersøkelsen.

Når det kommer til reliabilitet, kan det påvirke spørreundersøkelsen på ulike måter. Den første er representativitet. Vi har valgt å inkludere to produksjonsselskaper og to nettselskaper for spørreundersøkelsen, som til sammen utgjør fire ulike virksomheter. På denne måten hadde vi inkludert like mange produksjonsselskaper og nettselskaper. Fordelingen av informanter i virksomhetene varierer noe, som kan skape usikkerhet i resultatene. Selv om dette er tilfellet, er skillet ikke stort på antall informanter fra de ulike virksomhetene. Dette er noe som blir tatt høyde for i fremstillingen av empiri. Den andre er intern konsistens, som omhandler evnen til å produsere like resultater ved å benytte et annet utvalg for å måle det samme fenomenet under samme tid. Ved at vi inkluderte til sammen fire virksomheter øker det sannsynligheten for en styrket intern konsistens. Samtidig er vi klar over at størrelsen på de ulike virksomhetene varierer noe. Dette kan være med på å skape en usikkerhet i resultatene, noe vi har tatt i betraktning. Den tredje er feilmargin, hvor feilmargin og usikkerhet i svarprosenten har mye å si på om en spørreundersøkelse er pålitelig. I denne spørreundersøkelsen hadde vi en svarprosent på 67,4%, noe som tilsier en høy svarprosent fordelt på de fire virksomhetene. Det eksisterer flere virksomheter i Norge som gjør det samme. På den måten eksisterer det en usikkerhet i tallene for å kunne generalisere til hele kraftsektoren, selv om funnene basert på metodens triangulering er generaliserbare.

Spørreundersøkelsen ble gjennomført før gruppeintervjuene. Dermed valgte vi å inkludere flere spørsmål i intervjuguiden vår om funn som skilte seg ut i spørreundersøkelsen. Ved å konfrontere informantene med det vi som forskere har kommet frem til er med på å validere funnene våre (Jacobsen, 2005). Ved å inkludere spørsmål om dette i gruppeintervjuene fikk vi spurt informantene hva de tenker rundt resultatene. På denne måten fikk de mulighet til å fortelle rundt hva de tenkte omkring det. De funnene vi presenterte i gruppeintervjuene ble forklart av alle fire virksomhetene at det ofte er usikkerhet bak begrepsbruken og omfanget av spørsmålsstillingene, og at flere i virksomhetene ikke kan definisjoner på eksempelvis

«kontinuitetsplaner», og derfor eksisterer det usikkerhet i målingene. Selv om vi inkluderte begrepsforklaring før spørreundersøkelsen.

Validitet og reliabilitet i gruppeintervjuene

Når det kommer til gruppeintervjuene, kan validiteten ha blitt påvirket på ulike måter. Vi har tatt utgangspunkt i teorigrunnlaget i RE og driftskontinuitet. Dermed har vi oversatt spørsmål fra engelsk til norsk, som kan være en utfordring fordi det norske språket er «fattigere» enn det engelske språket. Dette har vi tatt i betraktning når vi har utformet spørsmålene i intervjuguiden. For å øke validiteten til spørsmålene gjennomførte vi pilottest med en gruppe, og på den måten undersøkte vi at spørsmålene ga mening på den måten vi har valgt å oversette det til. Det kan sies at vi også her har gjennomført en *face validity* (Saunders et al., 2019). Når det kommer til overførbarheten og den eksterne gyldigheten har vi valgt å inkludere hele fire gruppeintervju fordelt på fire virksomheter. Ved å inkludere fire virksomheter kan resultatene generaliseres i sammenheng med metodens triangulering. Alle intervjuobjektene regnes som valide til spørsmålene fordi alle hadde kjennskap til SCADA-systemet og flere av informantene hadde stillinger som arbeidet med dette systemet til daglig.

Dataene vi samlet inn via gruppeintervjuene har en styrket reliabilitet ettersom informantene våre er valgt med relevans i henhold til konteksten vi befinner oss i. Det vil si at vi har valgt å gjennomføre intervjuer med mennesker med relevante stillinger, erfaring og kompetanse i henhold til konteksten som oppgavens formål og forskningsspørsmål har basert seg på (Johannessen et al., 2021). Intervjuobjektene er også vurdert til å ha nødvendig (grundig) kjennskap til kraftsektoren og de fagområdene som vi ønsker å rette oppgaven mot. Det at vi har valgt å gjennomføre gruppeintervju er også noe som kan gi oss en svekket reliabilitet dersom vi opplever at intervjuobjektene holder tilbake på informasjon fordi de uttaler seg annerledes blant annet på bakgrunn av at de befinner seg i gruppe med andre kollegaer. Dette var ikke noe vi fikk et inntrykk av, men man kan aldri være helt sikkert. Reliabiliteten kan også svekkes ved at intervjuobjektene gir oss svar på spørsmålene som er fordelaktig for virksomheten deres, men som dermed ikke gjenspeiler den faktiske sannheten (Jacobsen, 2005). Gjennom gruppeintervjuene fikk vi ikke inntrykk av at de holdt informasjon tilbake, eksempelvis hvis lederen var til stede. Det kan nevnes at noen var stillere enn andre og ikke tok like lett til ordet som andre. Likevel var det overordnede inntrykket at ingen holdt tilbake informasjon og alle var villige til å lære mer omkring temaet oppgaven problematiserer. Noe som også hjelper å styrke reliabiliteten er hvordan intervjueren påvirker intervjuobjektet

(Jacobsen, 2005). Det har vært viktig for oss, som forskere og intervjuere, å opptre på en måte som gjør at intervjuobjektene følte seg ivaretatt, at de fikk muligheten til å svare åpent og ikke følte seg presset til å svare i en spesifikk retning basert på spørsmålene vi stilte dem. Det var samtidig viktig for oss å intervjue informantene våre i en naturlig setting (Jacobsen, 2005). Gjennomføringen av intervjuene foregikk på Microsoft Teams, noe som allerede er en innarbeidet og naturlig setting for de fleste i arbeidslivet. Samtidig kan det påvirke reliabiliteten dersom intervjuobjektet har fått mye tid på å forberede seg, noe som vi tok hensyn til i prosessen (Jacobsen, 2005). Intervjuobjektene fikk sette seg inn i scenarioet vi hadde utarbeidet for å sikre at alle informantene kunne svare på spørsmål i henhold til dette. Intervjuobjektene fikk ikke forberede seg på spørsmålene i forkant ettersom det ville medføre en svekket reliabilitet i henhold til det vi ønsket å få ut av intervjuene.

Etiske betraktninger

Denne masteroppgavens tematikk er sendt inn og godkjent av Kunnskapssektorens tjenesteleverandør (Sikt). Alle informanter som har deltatt i dette forskningsprosjektet har blitt anonymisert. I henhold til spørreundersøkelsen kan ingen spores tilbake på bakgrunn av lenken til spørreundersøkelsen ble sendt videre fra våre kontaktpersoner i hver virksomhet, på den måten delte vi ikke ut spørreundersøkelsen direkte til informantene. Når det kommer til gruppeintervjuene, ble alt av transkribert materiale slettet og alle informantene er anonymisert. Eneste kategorisering som er gjort i henhold til dette er hvorvidt det er informanter i et produksjonsselskap (P1 og P2) eller nettselskap (N1 og N2), og hvilken type stillingstitler som er inkludert i gruppeintervjuene. Alle informantene i gruppeintervjuene har signert samtykkeerklæringen fra Sikt, og på den måten vet de om sine rettigheter. Videre ble alle informert før intervjustart om at det ville bli tatt lydopptak, noe alle samtykket til. Ingen personlige opplysninger ble utlevert. Basert på godkjenningen fra Sikt, anses denne oppgaven som etisk forsvarlig.

4.8 Fordeler og ulemper

Avslutningsvis kan vi peke på fordeler og ulemper ved valgt metode. Ved å velge MMA inkluderer man både en kvalitativ- og kvantitativ tilnærming, kan det sies at de utfyller hverandre og veier opp for svakhetene som er forbundet med å benytte en metode. Som også kalles metodetriangulering (Jacobsen, 2005). Ved å både inkludere spørreundersøkelse, gruppeintervju og dokumentanalyse brukes det både primær-, sekundær- og tertiærdata. På denne måten tar vi i bruk allerede eksisterende materiale fra ulike offentlige dokumenter og

lover, samtidig som vi produserer vår egen. Dette kan sies å være med på å styrke oppgavens metodevalg. Ved å gjennomføre en kvantitativ tilnærming før gruppeintervju, kan disse fungere som kritiske tester for hverandre. Spørreundersøkelser kan føre til uklare forhold som vi har utdypet i gruppeintervjuet. Ved å inkludere spørsmål i intervjuguiden om spørreundersøkelsen kan dette være med på å eksplorere og intervjudeltakerne kan utdype hvilke tanker de hadde rundt spørreundersøkelsen. Gjennom bruken av både kvalitativ- og kvantitativ tilnærming gir det en ekstern gyldighet der funnene fra datainnsamlingen kan generaliseres (Jacobsen, 2005). På denne måten kan datamaterialet fra denne undersøkelsen generaliseres til kraftsektoren, med forbehold om usikkerhetene som er diskutert rundt validitet og reliabilitet.

Oppgavens størrelse og omfang har i valg av tilnærming vært utfordrende. Ved å inkludere både kvalitativ og kvantitativ tilnærming fordelt på til sammen fire ulike virksomheter har størrelsen på datamaterialet vært utfordrende å håndtere. Selv ved hjelp av Nvivo og SurveyXact, har oppgavens tidsbegrensinger og omfang vært krevende. Dette kan ha utpreget seg i forhold til presentasjonen av empiri. På denne måten har avgrensning i forhold til datamaterialet for oppgaven vært av en større størrelse. Dette har vi vært oppmerksomme på i behandlingen av datamaterialet. En annen ulempe ved valget på metode baserer seg på hvor utfyllende vi kan gjennomføre både den kvalitative- og kvantitative tilnærmingen. Ved å velge en metodisk triangulering, kan det være vanskelig at metodene utfyller hverandre på en fullstendig måte.

4.9 Oppsummering

I dette kapittelet har vi sett nærmere på den metodologiske trianguleringen. Denne har inkludert både kvantitativ spørreundersøkelse og kvalitative gruppeintervju og dokumentanalyse. På denne måten kunne vi på en utfyllende måte hente ut informasjon av informanter innen kraftsektoren ved ulike hjelpemidler, og se dette i sammenheng med sentrale dokumenter. Det skal videre presenteres empiri fra datainnsamlingen gjennom spørreundersøkelsen og gruppeintervjuene og sett opp mot tilhørende teori gjennom RE og driftskontinuitet.

5. Presentasjon av empiri

Dette kapittelet skal oppsummere funnene fra datainnsamlingen og presentere det. Det skal først sees nærmere på kartleggingen av resiliens gjennom RAG. Videre skal det redegjøres for og presenteres funn fra gruppeintervjuene, der vi skiller mellom egenskapene i RE og driftskontinuitet. Det er nevneverdig at masteroppgaven skrives på et ugradert nivå. Dette betyr at sårbarheter og sensitiv informasjon ikke er inkludert i diskusjonen og ikke reflektert i

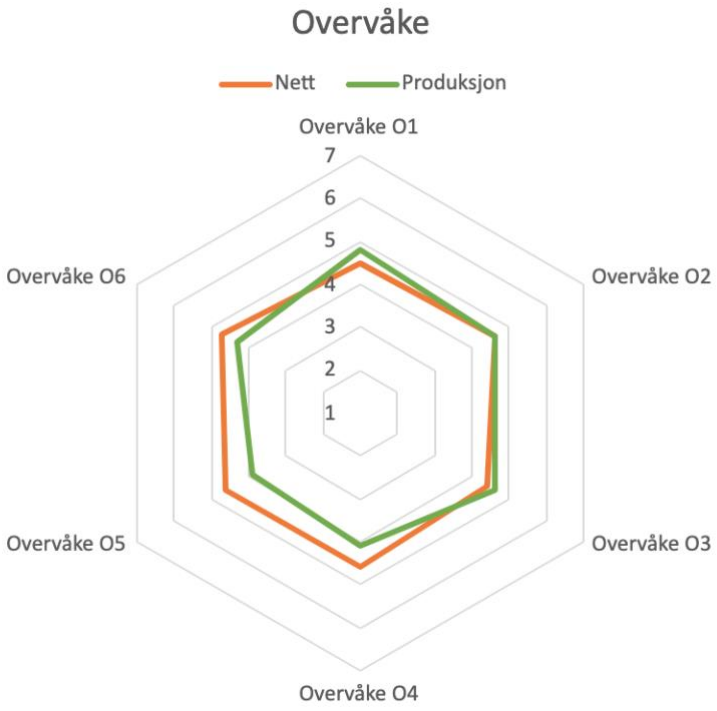
funnene. Vårt formål er å se på et overordnet systemnivå hvordan aktørene arbeider med RE-prinsippene og driftskontinuitet i henhold til SC.

5.1 Kartlegging av resiliens i kraftforsyningen gjennom RAG

Det skal i denne delen redegjøres for spørreundersøkelsens funn. Det skal visuelt fremstilles gjennom prinsippene i RE, hvor resiliensen i virksomhetene skal kartlegges gjennom RAG ut ifra prinsippene: overvåke, forutse, respondere og lære. Gjennom RAG som et teoretisk grunnlag er det fremstilt noen generiske spørsmål som kan tallfeste hvordan de ulike aktørene i kraftforsyningen arbeider med prinsippene i RE. Systemet som Hollnagel (2011) refererer til er, i sammenheng med denne oppgaven, resiliens og driftskontinuitet i kraftforsyningen. Driftskontinuitet har vært med på utformingen av spørreundersøkelsen i samsvar med det teoretiske grunnlaget i RAG. Dette er også med vår forståelse av S1 i henhold til Beer's (1984, 1985) VSM. Systemet som skal kartlegges er «resiliens og driftskontinuitet i kraftforsyningen», som består av kraftforsyningens aktører (nett- og produksjonsselskap).

5.1.1 Forklaring av tabell og radardiagram

Det skal nærmere forklares hvordan man skal lese tabellene og radardiagrammene som er visualisert i empirien. Ved kartleggingen av resiliens gjennom å visualisere det på denne måten kan beslutningstakere se hvilke prinsipper av RE de burde fokusere på og eventuelt hvilke tiltak som kan iverksettes for å forbedre dette. Tabellene er organisert på en slik måte at påstandene fra spørreundersøkelsen er organisert etter ulike nivå, eksempelvis «O» for «Overvåke» og «O1-O6» for å illustrere hvilken påstand det er fra 1-6. Det samme gjelder de andre prinsippene, hvor enkeltbokstavene med tall illustrerer hvilket prinsipp de er i RE og hvilken nummerering påstanden har. Radardiagrammet brukes for å illustrere de ulike nivåene av «resiliens», nivåene er fra 1-7 basert på hva informantene svarte på spørreundersøkelsen. På denne måten er «nivå 1», det nederste nivået og kan tolkes som det «dårligste», mens «nivå 5» er det øverste nivået og det «beste». Nivå 6 og 7 er nøytrale og vil diskuteres nærmere i avsnittet under. De ulike virksomhetene er delt inn etter «nett» og «produksjon». Hvor «nett» er bestående av N1 og N2 sine svar på spørreundersøkelsen, og «produksjon» er P1 og P2 sine svar. På denne måten skiller vi ikke mellom hver enkel virksomhet, fordi oppgaven har større nytte av å prøve å kartlegge resiliens på et systemnivå fremfor et individuelt nivå bestående av hver virksomhet. Målingene illustreres gjennom fire datasett, bestående av fire ulike tabeller med tilhørende visualisering gjennom radardiagrammet.



Figur 15 15 Eksempel på visualisering av radardiagram (overvåke).

Tabellen illustrerer separate målinger på «produksjon» og «nett», og under disse vises en samlet måling. Den samlede målingen fra alle påstandene hos både nett- og produksjonsselskapene vil illustreres øverst i tabellen sammen med gjennomsnittet fra både «produksjon» (grønn) og «nett» (oransje) sine målinger. Disse målingene er illustrert vedsiden av radardiagrammene i tabellen. Videre i tabellen er de forskjellige påstandene illustrert med målinger, og foreslåtte tiltak fra spørreundersøkelsen og kartlagt styrke i funksjonen illustrert horisontalt. Det teoretiske grunnlaget bak påstandene er forklart nærmere i metodekapittel 4.5.2. Snittet på målingene er plassert under «N» for «nett» og «P» for «produksjon» og dermed den samlende målingen under.

Tabell 9 Utsnitt av tabell for kartlegging av å overvåke

Spørsmål om overvåking fra spørreundersøkelse. Relevans for RE i praksis.	**Snitt**		**Foreslåtte tiltak fra spørreundersøkelse.**	**Kartlagt styrke i funksjonen.**
	N	**P**		
O1: Indikator Virksomheten overvåker systemet daglig og ser etter avvik fra normal tilstand	4,5	4,8	Styrke arbeidet med overvåking internt i egen virksomhet.	Generelt god overvåking hos alle virksomheter.
	4,65			

Gjennom presentasjonen av kartleggingen og målingen av resiliens i tabellene bruker vi et graderingsnivå fra 1-5. Nivåene som vises under i tabellen er koblet opp mot ytelsen til virksomheten i arbeidet med den spesifikke påstanden.

Tabell 10 Gradering av ytelse av egenskap

Nivå 1	Nivå 2	Nivå 3	Nivå 4	Nivå 5
Svært god	Generelt god	God	Noe forbedringspotensial	Forbedringspotensial

5.1.2 Usikkerhetsmoment bak visualisering

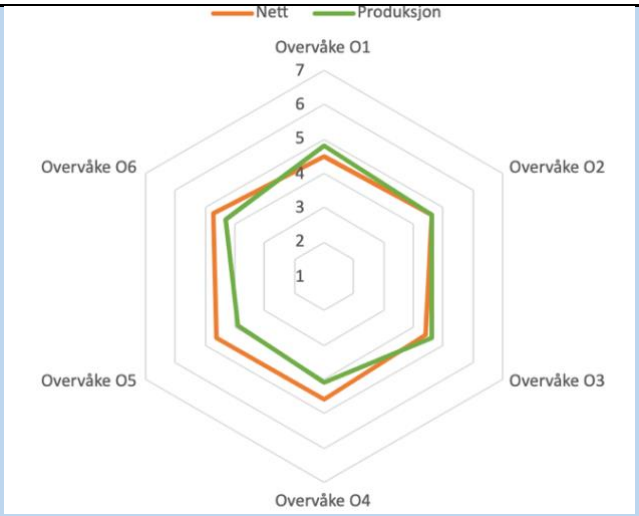
Kartleggingen av resiliens foregår gjennom visualisering gjennom et radardiagram. Det må tas i betraktning at radardiagrammet som presenterer kartleggingen av funnene fra spørreundersøkelsen, er nivå 6 «*vet ikke*» og nivå 7 «*ikke relevant*». Dette betyr at jo nærmere målingene er nivå 5, som er «*helt enig*», kan det være noe usikkerhet i fremstillingen. Det er nevneverdig å inkludere at ingen av svarene på undersøkelsen var på nivå 7 «*ikke relevant*», og dermed bortfaller usikkerhet bak den visuelle fremstillingen relatert til dette. Videre er det ikke flere en svært få personer (1-2 personer) som har svart nivå 6 «*vet ikke*», på noen påstander. Dette ser ikke vi på som utslagsgivende for fremstillingen gjennom radardiagrammet, men vises som en høyere grad av resiliens. Dermed vises det gjennom fremstillingen at flere av målingene på påstandene er nærmere nivå 5 «*helt enig*», enn det i utgangspunktet er siden noen svært få personer har svart «*vet ikke*». Det er to påstander som har en høyere prosentandel på nivå 6 «*vet ikke*». Den første påstanden er F4 med 19%, og L7 med 12% (se påstandene delkapittel 5.1.3). Denne prosentandelen er en samlet svarprosent fra både nett- og produksjonsselskapene. Når det kommer til F4 har nettselskapene en svarprosent på 17% på «*vet ikke*», og produksjon 25%. Når det kommer til L7 har nettselskapene en svarprosent på 18%, og produksjonsselskapene har 0% som har svart «*vet ikke*». Disse prosentandelene er en prosentvis fordeling på alle som har svart «*vet ikke*» i de ulike virksomhetene. På denne måten er det usikkerhet i funnene som er visualisert gjennom radardiagrammet på akkurat på disse to påstandene. Dette er noe vi er klar over og usikkerhetsmomentet rundt dette vil tas i betraktning. Begge påstandene har «*» bak for å visualisere usikkerheten.

Usikkerhetsmomentet vil være større i svarene fra P1 og P2. Dette er fordi utvalget er lavere hos dem (10 personer), enn ved utvalget hos N1 og N2 (19 personer). På denne måten er det forskjell i fra hvor pålitelige svarene fra P1 og P2 er sammenlignet med N1 og N2. Selv om det er en høyere svarprosent hos produksjonsselskapet totalt sett enn hos nettselskapet, er det fremdeles færre i produksjonsselskapene som har gjennomført spørreundersøkelsen. Dette tas i betraktning i presentasjonen av empirien og i drøftingen.

5.1.3 Kartlegging og måling av de fire egenskapene i RE

Nedenfor er det fire tabeller, med tilhørende radardiagram som er fordelt på de fire egenskapene til RE. Dette er kjernen i kartleggingen av resiliens, og er en stor del av FS2, men enkelte deler vil også fremstilles i FS1 og FS3. Fremstillingen er enkel og skal på et overordnet nivå vise enkle målinger gjort for å kartlegge resiliens.

Tabell 11 RE egenskap overvåke

<table>
<tr>
<td rowspan="7">FS 2</td>
<td colspan="2"> 
</td>
<td colspan="3">Spørsmål om virksomhetens evne til å overvåke:

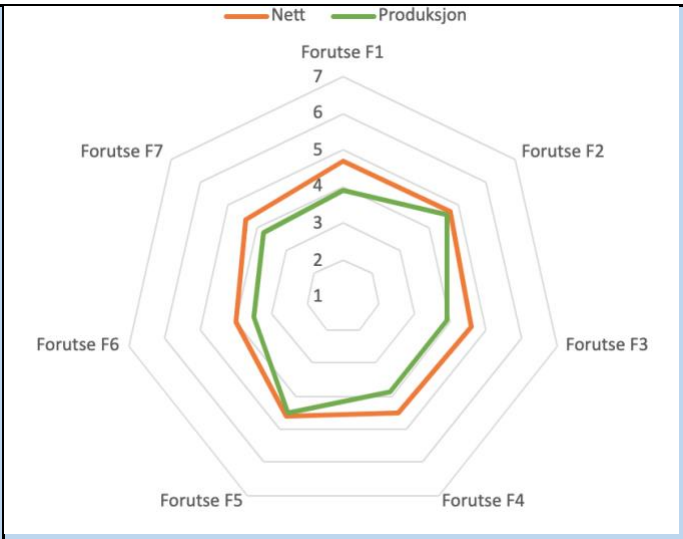
Nettselskap: 4,6

Produksjonsselskap: 4,5

Samlet måling: 4,47</td>
</tr>
<tr>
<td>Spørsmål om overvåking fra spørreundersøkelse.
Relevans for RE i praksis.</td>
<td>Snitt
N P</td>
<td>Foreslåtte tiltak fra spørreundersøkelse.</td>
<td>Kartlagt styrke i funksjonen.</td>
</tr>
<tr>
<td>O1: Indikator

Virksomheten overvåker systemet daglig og ser etter avvik fra normal tilstand</td>
<td>4,5 4,8
4,65</td>
<td>Styrke arbeidet med overvåking internt i egen virksomhet.</td>
<td>Generelt god overvåking hos alle virksomheter.</td>
</tr>
<tr>
<td>O2: Indikator type
Virksomheten iverksetter beredskap på bakgrunn av avvikene for å unngå svikt</td>
<td>4,6 4,6
4,6</td>
<td>Styrke anvendelse av kompetanse rundt beredskap i virksomheten.</td>
<td>Generelt god forståelse rundt iverksettelse av beredskap når avvik oppstår i systemet.</td>
</tr>
<tr>
<td>O3: Validitet
Jeg og mine kollegaer har god kunnskap og forståelse om hvilke risikoforhold vi skal se etter
.</td>
<td>4,4 4,6
4,5</td>
<td>Økt kompetanse om og tydeligere beskrivelser av risiko.</td>
<td>Fremstår som at ansatte har tilstrekkelig kunnskap rundt risikoforhold.</td>
</tr>
<tr>
<td>O4: Målfrekvens
Jeg og mine kollegaer har lav terskel for å rapportere på hendelser og nesten-hendelser</td>
<td>4,6 4,1
4,35</td>
<td>Legge til rette for en lavere terskel hos ansatte for å rapportere på hendelser og nesten-hendelser.</td>
<td>Generelt god forståelse hos ansatte på når det skal rapporteres.</td>
</tr>
<tr>
<td>O5: Stabilitet
Virksomheten har etablert en rapporteringskultur</td>
<td>4,6 3,9
4,25</td>
<td>Etablere en styrket rapporteringskultur, økt kompetanse på når det skal rapporteres rundt avvik/svikt i systemet.</td>
<td>God rapporteringskultur hos nettselskapene. Noe forbedringspotensial hos produksjonsselskapene.</td>
</tr>
<tr>
<td>O6: Verifikasjon/revisjon
Tilsyn på sikkerhet og beredskap i virksomheten jeg arbeider for har ført til endringer til det bedre</td>
<td>4,7 4,3
4,5</td>
<td>Følge opp tilsynsmyndighetens anbefalinger i større grad.</td>
<td>Generelt god oppfølging på anbefalinger fra tilsynsmyndigheten. Noe forbedringspotensial hos produksjonsselskapene.</td>
</tr>
</table>

Tabell 12 RE egenskap forutse

<table>
<tr><td rowspan="8">FS 2</td><td colspan="2"> 
</td><td colspan="3">Spørsmål om virksomhetens evne til å forutse:

Nettselskap: 4,5

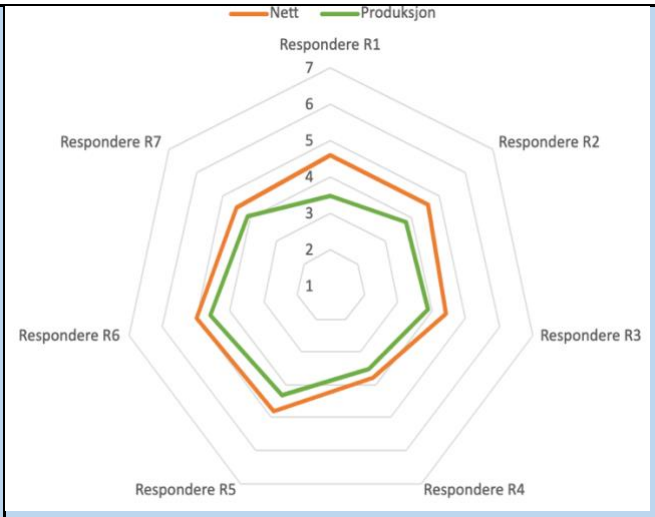
Produksjonsselskap: 4,0

Samlet måling: 4,25</td></tr>
<tr><td>Spørsmål om å forutse fra spørreundersøkelse.
Relevans for RE i praksis.</td><td>Snitt
N P</td><td>Foreslåtte tiltak fra spørreundersøkelse.</td><td>Kartlagt styrke i funksjonen.</td></tr>
<tr><td>F1: Kommunikasjon
Det nåværende trusselbildet kommuniseres til meg og mine kollegaer.</td><td>4,7 3,9
4,3</td><td>Økt kommunikasjon internt rundt trusselbildet til alle ansatte i virksomheten.

Kommuniseres nedover i virksomheten.</td><td>Generelt god kommunikasjon internt hos nettselskapene. Noe forbedringspotensial hos produksjonsselskapene.</td></tr>
<tr><td>F2: Frekvens
Jeg og mine kollegaer rapporterer når vi oppdager uregelmessigheter i systemet.</td><td>4,7 4,6
4,65</td><td>Jevnlig påminnelse rundt når det skal rapporteres.</td><td>Generelt god forståelse hos ansatte når det skal rapporteres uregelmessigheter i systemet.</td></tr>
<tr><td>F3: Antakelser
Beredskapsplanverket er kjent for meg og mine kollegaer i virksomheten</td><td>4,6 3,9
4,25</td><td>Følge opp ansatte i hvor beredskapsplanen er, og hva den innebærer.</td><td>God forståelse om beredskapsplan hos nettselskapene. Noe forbedringspotensial rundt denne forståelsen hos produksjonsselskapene.</td></tr>
<tr><td>F4: Antakelser*
Kontinuitetsplaner er kjent for meg og mine kollegaer i virksomheten</td><td>4,5 3,9
4,2</td><td>Økt kunnskap rundt bruken og utvikling av egne kontinuitetsplaner.</td><td>Nettselskapene virker å ha en større kjennskap til kontinuitetsplaner enn produksjonsselskapene.</td></tr>
<tr><td>F5: Tidsaspekt/forutsigelser
Virksomheten justerer behovet for beredskap basert på dagens trusselbilde.</td><td>4,6 4,5
4,55</td><td>Økt fokus på justeringer rundt beredskap basert på et dynamisk trusselbilde.

Økt frekvens i tilegning av relevant informasjon.</td><td>Generelt god forståelse for behovsjusteringer basert på trusselbildet til kraftsektoren.</td></tr>
<tr><td>F6: Risikoaksept
Virksomheten jeg arbeider for har beskrivelser for risiko som ikke aksepteres.</td><td>4,0 3,5
3,75</td><td>Økt frekvens i kommunikasjon til ansatte rundt hvilke risikoakseptkriterier virksomheten har etablert.</td><td>Forbedringspotensial hos både nett- og produksjonsselskapene.</td></tr>
<tr><td>F7: Årsakssammenheng
Jeg og mine kollegaer er forberedt på hvordan man skal respondere på uønskede hendelser</td><td>4,4 3,8
4,1</td><td>Økt frekvens på kunnskap og øvelse på hva man skal gjøre når en uønsket hendelse inntreffer systemet.</td><td>Generelt god forståelse omkring respondering på uønskede hendelser hos nettselskapene, noe forbedringspotensial hos produksjonsselskapene.</td></tr>
</table>

Tabell 13 RE egenskap respondere



Spørsmål om virksomhetens evne til å respondere:

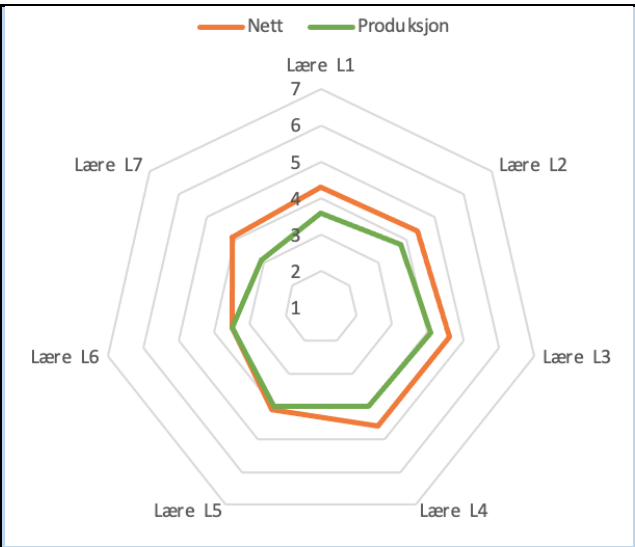
Nettselskap: 4,5

Produksjonsselskap: 4,0

Samlet måling: 4,24

	Spørsmål om å respondere fra spørreundersøkelsen. Relevans for RE i praksis	Snitt N	Snitt P	Snitt	Foreslåtte forbedringer fra spørreundersøkelse.	Kartlagt styrke i funksjonen.
FS 2	**R1: Hendelsesliste** Virksomhetens beredskapsplan har beskrivelser for håndtering av ulike scenarioer	4,6	3,5	**4,05**	Fokus på klare beskrivelser for hvordan man håndterer scenarioene som er beskrevet i beredskapsplanen.	God forståelse rundt beskrivelser for håndtering av scenarioer i planverk hos nettselskapene, noe forbedringspotensial hos produksjonsselskapene.
	R2: Grunnlag Scenarioene i beredskapsplanen er basert på tidsriktig fagkompetanse for kraftsektoren	4,6	3,8	**4,2**	Økt bruk av fageksperter i utarbeidelsen av beredskapsplanen. Fagekspertene burde være oppdaterte på dagens trusselbilde, på den måten ha tidsriktig kompetanse.	I stor grad brukt fagkompetanse i utarbeidelsen av beredskapsplan hos nettselskap. Noe forbedringspotensial hos produksjonsselskapene.
	R3: Terskel for respons Det er kjent for meg og mine kollegaer i virksomheten når beredskap skal iverksettes	4,4	3,9	**4,15**	Økt kommunikasjon og øvelse på når beredskap iverksettes internt i virksomheten.	Noe forbedringspotensial hos produksjonsselskapene på når beredskap skal iverksettes. Tilstrekkelig forståelse rundt dette hos nettselskapene.
	R4: Respons liste Meg og mine kollegaer evner til å håndtere scenarioene i beredskapsplanen blir testet gjennom øvelser	3,8	3,5	**3,65**	Hyppigere gjennomføringer av øvelser på ulike nivå, og hvor alle ansatte blir inkludert. I større grad etablere en øvelseskultur i virksomhetene.	Forbedringspotensial hos både nett- og produksjonsselskap.
	R5: Hurtighet Virksomheten kan mobilisere i henhold til beskrevne scenarioer i beredskapsplanen	4,8	4,3	**4,55**	Økt frekvens i interne øvelser spesifikt rettet mot hurtig mobilisering under en uønsket hendelse.	God forståelse rundt hurtig mobilisering hos både nett- og produksjon.
	R6: Varighet/ressurser Virksomheten har kapasitet til å håndtere en langvarig beredskapshendelse (varer lenger enn 24t)	5	4,6	**4,8**	Øvelser hvor det er fokus på lengre bortfall av grunnleggende funksjoner for systemet.	Grunnleggende funksjoner er godt innarbeidet og sikrer varig mobilisering av ressurser.
	R7: Normalisering Virksomheten har ressurser for hvordan man skal opprettholde drift under en uønsket hendelse	4,5	4,1	**4,3**	Etablering av kontinuitetsplaner.	God forståelse av normalisering under en hendelse hos både nett- og produksjonsselskap. Koordinering etablert med relevante aktører.

Tabell 14 RE egenskap lære



Spørsmål om virksomhetens evne til å lære:

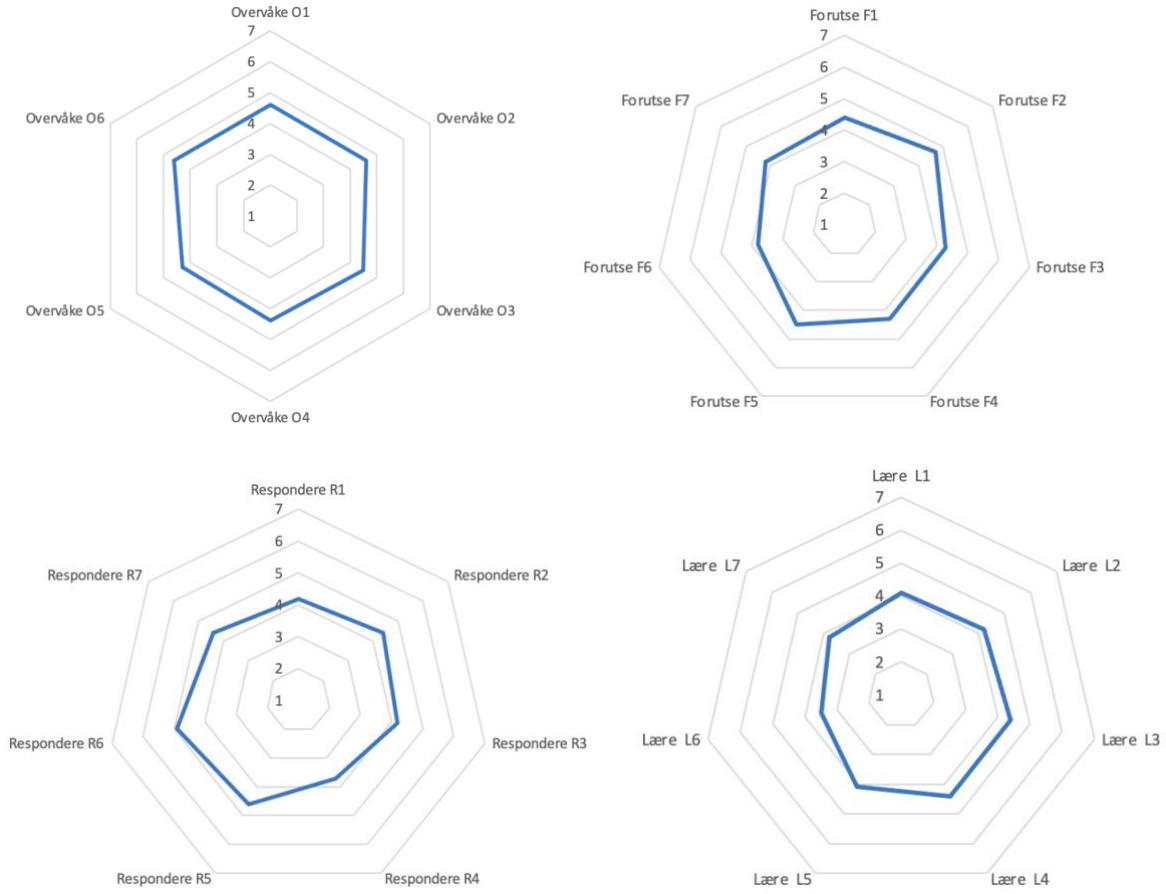
Nettselskap: 4,3

Produksjonsselskap: 3,7

Samlet måling: 3,98

FS 2	Spørsmål om å respondere fra spørreundersøkelsen. Relevans for RE i praksis.	Snitt N	Snitt P	Foreslåtte tiltak fra spørreundersøkelse.	Kartlagt styrke i funksjonen.
	L1: Seleksjonskriterier Virksomheten tar lærdom fra rapportering	4,3	3,6	Utvikle seleksjonskriterier for når virksomheten skal granske rapporteringer. (Alvorlighetsgrad, verdi, etc.)	Tilstrekkelig oppfølging på rapportering hos nettselskapene. Noe forbedringspotensial hos produksjonsselskap.
		3,95			
	L2: Seleksjonskriterier Oppfølging på rapportering fører til forbedret forsyningssikkerhet	4,4	3,8	Styrke oppfølgingen på rapportering (eget utvalg), som arbeider med dette internt i virksomheten.	Fremstår at nettselskapene i større grad oppfatter at oppfølging på rapporteringen hos dem fører til forbedret forsyningssikkerhet.
		4,1			
	L3: Datainnsamling/klassifisering Vi har analytisk kompetanse (intern eller ekstern) til behandling av rapporteringer	4,6	4,2	Økt kompetanse på behandling av rapportering fra eksperter. Tilby kursing for ansatte i virksomheten som arbeider med behandling av rapportering.	Tilstrekkelig grad av analytisk kompetanse hos både nett- og produksjonsselskapene.
		4,4			
	L4: Frekvens Rapportering av avvik eller uønskede forhold har ført til endringer til det bedre	4,6	4,0	Alle typer avvik må gjennomgås og vurderes.	Oppfatningen om endringer til det bedre på bakgrunn av rapportering er god hos både nett- og produksjonsselskapene.
		4,3			
	L5: Læringsmål Virksomheten tilrettelegger for at vi skal lære av hverandre (gjennom intern kursing, samtaler etc.)	4,1	4,0	Økt bruk av ulik kursing med fokus på å lære av hverandre i virksomheten.	Tilstrekkelig fokus hos både nett-og produksjonsselskapene.
		4,05			
	L6: Verifikasjon Virksomheten har gjennomført beredskapsøvelse med alle relevante aktører som er involvert ved en uønsket hendelse i kraftforsyningen, i løpet av de siste 12 mnd	3,5	3,5	Flere storskalaer øvelser hvor alle relevante aktører i forsyningskjeden blir inkludert. Table-top øvelse med forsyningskjeden, inkluderer både berørte produksjon- og nettselskap, og andre naturlige aktører.	Forbedringspotensial hos begge i organisering og gjennomføring av storskala øvelser.
		3,5			
	L7: Læringsmål* Virksomhetens beredskapsøvelser inkluderer ekstreme scenarioer, eksempelvis cyberangrep gjort med hensikt om å ta over kontrollen	4,1	3,1	Flere beredskapsøvelser rundt «worst-case»-type scenarioer.	Forbedringspotensial for utvikling av beredskapsplan som inkluderer «worst-case»-scenarioer, og gjennomføre øvelser basert på disse, hos både nett- og produksjonsselskap.
		3,6			

Avslutningsvis skal det visualiseres den samlede målingen på resiliens fra både N1, N2, P1 og P2. På denne måten kan man enklere illustrere hvordan kraftforsyningen på et systemnivå ligger an i arbeidet med resiliens. Disse radardiagrammene må sees i sammenheng med målingene som er gjort i tabellene. De er basert på den samlede målingen som er vist i de ulike tabellene.



Figur 16 16 Radardiagram over samlet måling av resiliens for de fire egenskapene i RE.

5.1.4 Hovedfunn gjennom kartlegging og måling av resiliens

I tabellen under skal det kort redegjøres for hovedfunnene våre fra kartleggingen og målingen av resiliens.

Tabell 15 Hovedfunn RAG.

Egenskap	Nettselskap	Produksjonsselskap
Overvåke	Samlet sett svært gode resultater fra kartleggingen på denne egenskapen. Ser ut som det er generelt god forståelse hos arbeidere i nettselskapene hvordan de skal arbeide for å oppdage uregelmessigheter i sine interne systemer. Videre også hvordan	Samlet sett gode resultater fra kartleggingen på denne egenskapen. Noe forbedringspotensial. Her kan et økt fokus på rapporteringskultur kan føre til flere rapporteringer av hendelser og nesten hendelser, og på den måten kan

	og hvorfor det skal rapporteres på disse avvikene ser ut som «vanlig» praksis her. Tilsyn internt i virksomhetene har også ført til forbedret forsyningssikkerhet.	virksomhetene bygge seg mer resiliente mot fremtidige uønskede hendelser. En god rapporteringskultur gjenspeiler at virksomhetene vil forbedre seg bedre og tilpasse seg i økende grad endringer i systemet.
Forutse	Samlet sett god forståelse rundt egenskapen forutse. Virker som de fleste ansatte har god forståelse rundt ulike komponenter rundt mulige trusler i systemet. Ser ut som de fleste har god kjennskap til beredskapsplaner og risiko. Noe usikkerhet rundt risikoakseptkriterier. Aspektet rundt kontinuitetsplaner er et begrep og bruksområdet som kan gjøres mer kjent internt i virksomheten, som kan gi en forbedret forsyningssikkerhet og beredskap under uønskede hendelser.	God forståelse rundt hvordan man skal forutse uønskede hendelser (iht. dagens trusselbilde). Noe motsigende resultater her ift. rapportering (overvåke), virker som de fleste rapporterer når man oppdager uregelmessigheter i systemet. Beredskapsplanverket burde kommuniseres internt nedover til alle i virksomheten, på denne måten bidra til forbedret forsyningssikkerhet og at flere internt kan bli en ressurs. Kontinuitetsplaner her noe som kan jobbes videre med. Er noe som ikke er godt kjent for alle internt i virksomheten.
Respondere	Svært god forståelse rundt indikatorene rundt egenskapen til å respondere. Det ser ut som virksomhetene har kapasitet og mulighet til å respondere på små og store (24t) beredskapshendelser og nok ressurser til opprettholdelse drift tross uønskede hendelser. Beredskapsplanverket virker oppdatert og aktuell for kraftsektoren, videre virker det som at ansatte har kompetanse rundt når beredskaps skal iverksettes.	Noe forbedringspotensial rundt egenskapen respondere, men grei forståelse rundt indikatorene under egenskapen. Det kan se ut som at beredskapsplanverket og håndteringen rundt uønskede hendelser ikke er kjent for alle i virksomhetene. Ser ut som virksomhetene har kapasitet og ressurser til å håndtere store (24t) og små beredskapsledelser. Samme gjelder for virksomhetens opprettholdelse av drift under en uønsket hendelse.
Lære	Samlet sett god forståelse rundt denne egenskapen i RE. Virker som det er etablert en forståelse rundt rapportering og hvordan dette har bidrar til forbedringer, som gir en forbedret forsyningssikkerhet. Forbedringspotensial rundt beredskapsøvelser og dens innhold, burde inkludere mer ekstreme scenarioer.	Forbedringspotensial rundt denne egenskapen i RE. Rapportering burde være inkludert som en større del av virksomhetene slik alle ansatte på ulike nivå vet hva og når de skal rapportere på avvik og uønskede hendelser. På denne måten kan det føre til endringer til det bedre slik alle ansatte legger merke til det.

		Ser ut som det trengs et større fokus på beredskapsøvelser og innholdet i disse.

5.2 Empiri fra gruppeintervju

Her skal vi presentere hovedfunnene våre i forbindelse med gruppeintervjuene. Funnene vil presenteres i henhold til relevante kategorier. Vi skiller mellom virksomhetene ved å bemerke dem som P1, P2, N1 og N2. Det henvises til nummerering i sammenheng med sitater, etter kategorier fra intervjuguiden. All empirien baserer seg på prinsippene i RE og driftskontinuitet knyttet opp mot SC samlet inn gjennom gruppeintervjuene. Det vil inkluderes tabeller gjennomgående for presentasjon av sitat gjennom hver enkelt kategori. På den måten kan vi på en ryddig måte henvise til relevante sitat gjennomgående i empirien og senere i drøftingen (kapittel 6).

5.2.1 Funn knyttet til opprettholdelsen av driftskontinuitet

Funnene våre er gjort i henhold til spørsmål stilt generelt om virksomhetenes driftskontinuitet. Dette innebærer deres arbeid med dette, forståelse og anvendelse av kontinuitetsplaner og generelle tanker rundt den helthetlige forståelsen av disse begrepene og bruken av dem i virksomheten. For funnene er det hensiktsmessig å nevne at alle fire virksomhetene forteller oss at de har KBO-enheter i egen virksomhet. Dette er nødvendig å ha i bakhodet på bakgrunn av det da stilles ekstra lovkrav rundt sikkerhet og beredskap i henhold til energiloven og kraftberedskapsforskriften.

Funnene rundt begrepet «kontinuitetsplaner» er tvetydig mellom de ulike virksomhetene. Begrepet er ikke etablert aktivt i sammenheng med alle virksomhetenes interne arbeid (se sitat N1K1, N2K1, P2K1, P2K2). Derav tilsier funnene at det også er uvitenhet rundt om kontinuitetsplaner er noe virksomhetene har og bruker aktivt. Gjennomgående i alle intervjuene er det stort sett de med beredskapsstillinger, eller «høyere» stillinger som kan knyttes til beredskap, som har kjennskap til begrepet kontinuitetsplan og bruken av dem (se sitat N2K2 og P2K1). Det var særlig det ene nettselskapet, N2, hvor beredskapsansvarlig hadde noe vi oppfattet som svært god kontroll på begrepet og bruken av kontinuitetsplaner. Forståelse og klarhet i begrepet manglet likevel hos de øvrige deltakerne på gruppeintervjuet med N2. Det var kun N2 som kunne svare klart ja på at de hadde en overordnet kontinuitetsplan for virksomheten. Det ble påpekt fra N1, N2 og P2 at virksomheten dekker kontinuitetsplaners hensikt i sine beredskapsplaner (se sitat N1K1, N2K1, N2K2, P2K2). P2 nevnte blant annet at de aldri har brukt begrepet kontinuitetsplan, selv om en av informantene hadde noe forståelse rundt begrepsbruken. N1 påpekte særlig at selv om de ikke bruker begrepet aktivt, så betyr det

ikke at virksomheten ikke arbeider med kontinuitet. Når det kommer til P1 var dette et begrep de ikke var særlig kjent med, og de henviste oss videre til deres tilknyttede nettselskap som de deler driftssentral med. Dette kan tyde på at det trengs grundigere kunnskap om forståelsen av beredskapsplan vs. kontinuitetsplan.

Når det kommer til SC er det et overordnet inntrykk at alle virksomhetene er enige i at dette er et «worst case»-scenario. Et funn som kommer fram i forbindelse med driftskontinuitet er at nettselskapene er mindre avhengige av produksjonsselskapene for å opprettholde sin drift under SC. Produksjonsselskapene er dermed mer avhengige av nettselskapene for å opprettholde sin drift (se sitat P1D1 og P2D1). Det kommer gjennomgående fram at dersom SCADA-systemet blir utsatt for cyberangrep, må det skrues av, og da må personer manuelt ut på produksjonsanlegg/nettstasjoner for å betjene disse for å opprettholde forsyningen av strøm. Her får vi likevel en forståelse av at nettselskapene kan forsyne med strøm uten produksjonsselskapene, fordi nettet er selvgående så lenge det er intakt (se sitat N1D2), mens produksjonsselskapene er helt avhengige av nettet for å levere sitt produkt (se sitat P2D1).

Virksomhetenes kontinuerlige arbeid med opprettholdelsen av driftskontinuitet i henhold til cyberangrep, kommer mye tilbake på at virksomhetene er avhengige av andre tjenester. Som også refereres til som «SOC-tjenester». I flere av intervjuene ble det ved flere anledninger nevnt at fokuset på arbeidet med å sikre driften og forsyningen av strøm «ligger i ryggmargen», og at alle ansatte burde ha årvåkenhet og sunn skepsis i det daglige arbeidet med det (se sitat P1KS). Det ble også nevnt at arbeidet med dette ofte ikke forekommer ned på operatørnivå, men for det meste på ledelses-/administrativt nivå.

Helhetlig virker det som at nett og produksjonsselskapene setter pris på at de har «SOC-tjenester», som hjelper de med å overvåke og sikre kontinuitet i leveransene. Videre er produksjonsselskapene avhengige av deres tilknyttede nettselskaps driftssentral, som også kalles en kombi-sentral som er en fusjon mellom nett- og produksjonssentralen. Denne overvåker og hjelper til med å gi beskjed hvis det oppstår noen forstyrrelser i driften hos dem (se sitat N1D1). Generelt svarer alle virksomhetene på at de ikke kunne tenke seg å være for uavhengige av «SOC-tjenestene» og kombi-sentralene, fordi de er avhengige av hverandre for å oppnå en bedre forsyningssikkerhet. Det nevnes gjennomgående i alle intervjuene en tankegang tilknyttet kost-nytte. Alt arbeid med beredskap, øvelser, koordinering o.l. kommer alltid tilbake til et spørsmål om tid, penger og ressurser.

Tabell 16 Sitat driftskontinuitet og kontinuitetsplaner

Virksomhet	Sitat fra gruppeintervju	Tildelt kode	Tema
N1	«For meg er det et kjent begrep, men ikke et begrep som brukes til daglig i N1. Vi snakker mer generelt om beredskapsplaner» (spm. 3).	N1K1	Kontinuitetsplaner
	«Vi som utfører tjenesten, som er drift og overvåking, vi får kjøreplaner for de som sitter på de økonomiske markedene, hos produsentene som vi da følger opp ... også hvis ved eventuelle driftsforstyrrelser eller ting som skjer mot produsentenes komponenter, så har vi ... kontakt med teknisk personale da, som retter opp i det» (spm. 4).	N1D1	Driftskontinuitet
	«Strømmen går ikke fordi om SCADA-systemene går ned, nettet er jo selvgående, det som er vanskelig er å rette eventuelle feil som oppstår, det er det som er kompliserende. Klarer ikke å overvåke» (spm. 13).	N1D2	Driftskontinuitet
N2	«Vi har jo en beredskapsplan med tilhørende innsatsplaner ... som tas fram ved en hendelse som går på forsyningssikkerheten» (spm. 3).	N2K1	Kontinuitetsplaner
	«Men kontinuitetsplaner handler jo om at du har tilstrekkelig med ressurser på de tilstrekkelige rollene vi skal praktisere, og der har vi brukt DSB sin veileder når vi lagde den her kontinuitetsplanen» (spm. 3).	N2K2	Kontinuitetsplaner
P1	«Det blir jo en felles koordinering med nettselskapet, vi kan ikke agere ut fra eget ønske ... vi er litt prisgitte, og avhengige av at noen forteller oss hva vi skal gjøre og hva vi skal laste opp maskinene på ... for å gjenopprette strømforsyningen» (spm. 10).	P1D1	Driftskontinuitet
P2	«... kontinuitetsplan det er jo at hvis noe faller ut hvordan greier vi likevel å opprettholde driften ... joda vi har jo redundans mellom radiolinje sambandet at vi da likevel skal kunne greie oss fint å styre kraftstasjonene ... hvis det også faller ut, så må jo en fysisk person reise opp på kraftstasjonen og kjøre den fra kraftstasjonen» (spm. 3).	P2K1	Kontinuitetsplaner
	«...sånn som for oss da så vil jeg tippe at det som dere kanskje ville ha trukket ut og sagt var en del av kontinuitetsplan det er bare hos oss naturlig i en beredskapsplan» (spørreundersøkelse kontinuitetsplaner).	P2K2	Kontinuitetsplaner

5.2.2 Samhandling og koordinering mellom aktørene i kraftforsyningen

Hovedfunnene våre tyder på at samhandling og koordinering mellom nett- og produksjonsselskap virker å være på et overordnet nivå. Som nevnt over, forstår vi det som at produksjonsselskapene er mer avhengige av nettselskapene enn motsatt på et generelt nivå, også i forbindelse med SC. Det blir påpekt at dynamikken mellom de forskjellige aktørene ikke er veldig strukturert (se sitat P1KS1, P1KS2 og N2KS1). Den daglige samhandlingen mellom aktørene i drift og produksjon forekommer stort sett i økonomiske forhold, hvor produksjonsselskapene sender produksjonsplan til nettselskapet og nettselskapet betaler dem for det de skal produsere. Utover dette har virksomhetene ingen annen kommunikasjon til daglig hvis alt går som det skal.

Det kommer helhetlig fram at det stort sett ikke foreligger felles beredskapsplaner for tilknyttede nett- og produksjonsselskaper. Hvis det skulle oppstå en beredskapssituasjon som også påvirker deres tilknyttede nett- og produksjonsselskaper, er det «naturlig» å inkludere dem (se sitat N1KS2). Under SC har alle virksomhetene påpekt at det ville være naturlig, og en «uskreven, men naturlig praksis» å kontakte og koordinere seg med tilhørende nett- eller produksjonsselskap. Alle virksomhetene påpeker at de innehar informasjon om hvem de skal kontakte ved hendelser.

Koordineringen av drift er ulik mellom de forskjellige virksomhetene. N1 og N2 har en egen driftssentral som driftes av deres ansatte. På denne måten er ikke de like avhengig av deres tilknyttede produksjonsselskaper. Nettselskapene er mer avhengig av «SOC-tjenestene» når det kommer til overvåking av driftsforstyrrelser (se sitat N1KS1). P1 og P2 er tilknyttet sine nettselskapers driftssentral (kombi-sentral), uten at de har egne ansatte der. På denne måten er de avhengige av kontinuerlig overvåking og kommunikasjon som gjelder produksjonsplaner mellom de og sine tilknyttede nettselskaper (se sitat P2KS1). P2 henviser også til at de kjøper eksterne tjenester (SOC-tjenester). P1 nevner at moderselskapet de er en del av har avdeling som driver på med IKT, som også bistår dem med cybersikkerhet. N2 viser til at de deler SCADA-system med et annet produksjonsselskap (se sitat N2KS2). Disse vil de være spesielt tilknyttet under SC. De har likevel ikke noe med hverandre å gjøre til det daglige, men presiserer at de har avtaler mellom seg som sier noe om hvordan de skal hjelpe hverandre å opprettholde forsyningen i et område hvis en linje hos nettselskapet detter ut (se sitat N2KS3). N2 presiserer at de kunne tenke seg at det var noe mer samarbeid mellom dem og det gjeldende produksjonsselskapet for å ha mest mulig kontroll hvis noe skjer.

Tabell 17 Sitat samhandling og koordinering

Virksomhet	Sitat i gruppeintervju	Tildelt kode	Tema
N1	«... Vi utfører den tjenester som er, drift og overvåkning da, og at vi får kjøreplaner fra de som sitter på de økonomiske markedene hos produsentene som vi da følger opp. Og så, hvis ved eventuelle driftsforstyrrelser eller ting som skjer mot produsentenes komponenter, så har vi teknisk, kontakt med teknisk personale da. Som retter opp i det da».	N1KS1	Koordinering og samhandling
	«Det er naturlig at vi, hvis det er en situasjon som påvirker produsentene rundt oss også, at vi tar kontakt med deres beredskapsledelse, slik at de er klar, og vi har vel innsyn i deres beredskapsdokument, slik at vi kan samhandle» (spm. 8).	N1KS2	Koordinering og samhandling
N2	«... Men vi har jo så stabilt og sterkt nett at produksjonen kan gjøre som de vil de, uten at vi må ha noe koordinering med dem» (spm. 4).	N2KS1	Koordinering og samhandling
	«Vi har et samarbeid på dette med SCADA-system da, eller driftskontroll nettverk. Så vi har det samme systemet» (spm. 4).	N2KS2	Koordinering og samhandling
	«Vi har eksempel på avtaler mellom oss, der hvis vi har ensidig forsyning til et område, så kan produksjonen være bakcupen vår, slik at hvis vår linje detter ut, så kan avtalen med produksjonsselskapet til å opprettholde forsyningen i området» (spm. 4).	N2KS3	Koordinering og samhandling
P1	«Dynamikken der, er ikke særlig strukturert som jeg tenker det. Hvis det er krise, eller store kraftverk detter ut, ligger det i ryggmargen vår at vi prøver å gjøre de startklare. Og der må være en dialog med nettselskapet ... det er ikke rutiner på dette ... vi har ikke noe oppskrift på det nei» (spm. 4).	P1KS1	Koordinering og samhandling
	«Da er det om å gjøre å få kontakt ... de tar kontakt med oss, men ingen kjørebok på dette, forekommer en dialog.» (spm. 4).	P1KS2	Koordinering og samhandling
P2	«... Produksjonsplanen blir oversendt til nettselskapet, driftssentralen til nettselskapet. Så det er de som sitter ... og slår av maskinene og styrer at de slår seg inn i produksjonen ... Så dukker det opp noen feil innimellom ... noen ganger så er det driftssentralen som får de feilene, for de sitter tross alt og overvåker, og da varsler de oss» (spm. 4).	P2KS1	Koordinering og samhandling

5.3 Funn knyttet til de fire egenskapene i RE

5.3.1 Evnen til å overvåke og dens effekt på driftskontinuitet

Overordnet er det en forskjell på hvordan de to nettselskapene og de to produksjonsselskapene arbeider med å overvåke systemet med tanke på cyberrelaterte angrep. Alle fire virker å være avhengige av andre tjenester (SOC-tjenester eller tilknyttede nettselskaper) i prosessen med å overvåke.

Gjennomgående hos alle virksomhetene blir det presisert at alle som har tilgang på SCADA-systemet, har begrensede tilganger etter avtale. SCADA-systemet blir vi fortalt er svært sikkert i seg selv og at det skal mye til for å kunne komme seg inn på dette utenifra. For å oppdage uregelmessigheter og feil på systemet, bruker alle virksomhetene tjenester som de kjøper, som spesifikt jobber med overvåkning. Det framkommer også at det er stort sett driftssentralene til nettselskapene som står for overvåkning og oppsett av brannmurer og barrierer o.l. via «SOC-tjenestene» (se sitat P1O1). Dersom det oppdages feil gjennom overvåking av nettselskapene, gjøres dette via SOC-tjenestene (se sitat N1O1, N1O2 og N2O1). Videre blir produksjonsselskapene kontaktet via tilknyttede nettselskaper hvis det er forstyrrelser på deres anlegg (se sitat P2O2). P2 nevner også at de har eksterne aktører som de sender logger til for analyse, og at dette er en måte som brukes for å overvåke systemet (se sitat P2O1).

Tabell 18 Sitat overvåke

Virksomhet	Sitat fra gruppeintervju	Tildelt kode	Tema
N1	«Via driftskontrollrommene, eller via driftssentralen så er vi jo, i den forstand hvis noen klarer å forstyrre systemet så er det da operatørene som oppdager det ... Vi kjøper SOC-tjenester fra andre eksterne aktører som overvåker trafikken da, som skal gi oss beskjed hvis det blir oppdaget unormal aktivitet i nettet eller på klientene» (spm. 6).	N1O1	Overvåke
	«... Vi jobber ikke aktivt med å prøve å finne måte å identifisere eventuelle innbrudd, vi har ikke det, men vi har jo leverandører som leverer tjenester som vi forventer har en organisasjon som kan ha fokus på dette, fordi vi har ikke sånne ressurser internt» (spm. 12).	N1O2	Overvåke
N2	«På IT-siden, som vi nå utvider ... og SCADA-verden, der må vi, eller vi kjøper en tjeneste, en slik SOC-tjeneste, og det er et overvåkningssenter som følger med på våre anlegg om det er trusler som kommer inn og loggfører og følger opp logger og brannmurene våre og de overvåker om noen er i ferd med å angripe oss da» (spm. 5)	N2O1	Overvåke
P1	«Når det gjelder driftssentralen, da er det nettselskapet som har sine brannmurer, og sine systemer ...».	P1O1	Overvåke
P2	«... vi driver og kjøper en god del sikkerhetstjenester ... vi driver og tar alle logger, sann på hva skjer, datatrafikk, logger, på, mellom systemene og spesialt da mot SCADA-systemet også. Også sender vi det inn og så blir dette analysert ...» (spm. 6).	P2O1	Overvåke
	«Vi kjøper tjenester fra nettselskapet. Siden de er døgnbemannet og sitter der og overvåker, og de er jo avhengige av å ha kontroll på dette her også ... så vi kjøper tjenester av de» (spm. 4).	P2O2	Overvåke

5.3.2 Evnen til å forutse endringer og dens effekt på driftskontinuitet

Når det kommer til evnen til å forutse og dens effekt på driftskontinuitet er det likheter hos alle de fire virksomhetene. Gjennomgående likt for alle, svarer de at de holder seg oppdaterte ved hjelp av mange forskjellige organisasjoner, som NSM, PST og KraftCERT (se sitat N1F1, N2F1, N2F2, P1F1, P2F1). Videre ble det nevnt av noen av virksomhetene at organisasjoner som Mnemonic og Telenor Security Operation Center hjelper de å holde seg oppdaterte på dagens trusler, og dette er også sikkerhetstjenester de kjøper for å overvåke sine digitale systemer. På den måten får de mye og relevant informasjon for å kunne holde seg oppdaterte på dagens trusselbilde. Kraftforsyningen er for tiden i en ALFA-beredskapssituasjon, der alle virksomhetene her er en del av KBO. Gjennom KBO har det blitt arrangert en del møter med tanke på dagens trusselbilde (se sitat P1F1). Generelt blir det nevnt at krav fra myndighetene (NVE) er med på å hjelpe virksomhetene til å tenke kontinuerlig på sikkerhet og sikringen av strømforsyning, samt at en av virksomhetene, P2, poengterte at de har interne samlinger årlig hvor det blir gjort en gjennomgang av året og hva som har endret seg og som dermed bør være fokus i henhold til forsyningssikkerhet.

Hovedfunnene her er at produksjonsselskapene og nettselskapene stiller seg ganske likt i forhold til hvordan de holder seg oppdaterte på det nåværende trusselbildet.

Tabell 19 Sitat forutse

Virksomhet	Sitat fra gruppeintervju	Tildelt kode	Tema
N1	«Selv om vi er oppdaterte på det som offentliggjøres, spesielt av sånne trusselvurderinger som kommer, NSM, PST, NVE, KraftCERT, i tillegg så abonnerer vi på daglige oppdateringer fra «ørten» forskjellige instanser» (spm. 5).	N1F1	Forutse
N2	«Vi er jo i jevnlig kontakt med myndighetene, NVE som regulerer oss, og også PST... og får tett informasjon ... Vi har jo også veldig fokus på disse NSM sine grunnprinsipper rundt IT-sikkerhet, og at vi mer eller mindre er i samsvar med de viktigste prinsippene der, så vi har jo hatt en del jobb med det det siste året» (spm. 5). «... I forhold til IT så har vi den der, KraftCERT er vi medlem av».	N2F1 N2F2	Forutse Forutse
P1	«Vi er med i KBO, der kommer det informasjon hele tiden om trusselbildet ... KBO har samarbeid med PST og NSM, så de får informasjon om trusselbilde, og hva de vurderer» (spm. 5).	P1F1	Forutse
P2	«Vi er medlemmer av mange organisasjoner ... vi har mange sanne fagmiljø ... som vi hele tiden får et bilde av hvordan ser situasjonen ut i verden ... også abonnerer vi på noe som heter KraftCERT...» (spm. 5)	P2F1	Forutse

5.3.3 Evnen til å respondere og dens effekt på driftskontinuitet

Når det kommer til evnen å respondere og dens effekt på driftskontinuitet er det tvetydighet i funnene. En ting som alle virksomhetene har til felles, er at dette spesifikke scenarioet er noe de har lite erfaring med. De fleste svarene går ut på hvordan de kunne tenke seg at de ville

respondert i henhold til måten de eventuelt har respondert på andre hendelser tidligere (se sitat N1R1 og P1R1).

Alle virksomhetene forteller at de ville satt beredskap/krisestab i henhold til en slik type hendelse. Roller og ansvar i henhold til beredskapssituasjoner er forhåndsbestemt og nedskrevet i en beredskapsplan, og alle som har en sentral rolle i en slik situasjon er klar over det (se sitat N1R3, N2R1, N2R2 og P2R1). En forskjell på nett- og produksjonsselskapene i denne sammenhengen er at de to produksjonsselskapene vil vente med å starte opp igjen sine kraftverk i påvente av informasjon fra deres tilknyttede nettselskap (se sitat P1R5 og P2R1). De vil også koordinere seg med nettselskapene for å få bekreftelse på at systemene og dens tilhørende problemer er sett nærmere på, og at det vil være trygt å gjenoppstarte de største kraftverkene for å opprettholde driften. På den andre siden så er det ofte slik at nettselskapene får en melding hos en av deres eksterne aktører (SOC-tjenester) som fanges opp i deres driftssentral og på den måten blir det iverksatt beredskap (se sitat N2R1).

Når det kommer til rollefordelingen og ansvar rundt beredskapshendelser er det som nevnt likheter hos de ulike virksomhetene, likevel eksister det noen nyanser hos dem. N2 viser til at ansatte som ikke har like god kjennskap til beredskapsarbeidet internt i virksomheten, ikke har like god forståelse rundt sin rolle i denne typen arbeid (se sitat N2R2). Videre presiseres det at virksomheten har litt å hente i forhold til trening i å forstå det fulle og hele formelle ansvaret rundt disse rollene (se sitat N2R3). I håndteringen av en hendelse kommer det fram at det «ville være naturlig» å kontakte tilhørende produksjonsselskap, og spesielt de som nettselskapet eventuelt deler SCADA-system med (se sitat N2R4). Når det kommer til N1 reflekterer de ikke noe mer rundt enn at de forhåndsbestemte rollene er satt og forstått av dem det gjelder. Vi fikk også inntrykk av at N1 ikke er særlig tilknyttet noen produksjonsselskap i sitt daglige arbeid. De forteller likevel at de har tett dialog med sine kunder og vil kontakte dem hvis det oppstår en beredskapshendelse som også påvirker dem (se sitat N1KS2). Videre viser P1 til at de er avhengige av deres tilknyttede nettselskap for å iverksette beredskap, og har i en slik situasjon bare fysisk kontroll på kraftverkene ved SCADA-systemets bortfall (se sitat P1R2, P1R3 og P1R4). P2 nevner noe av det samme som P1, hvor de nevner at de ville nok ha kontaktet deres tilknyttede nettselskap for å koordinere driften (se sitat P2R2). Avslutningsvis har alle virksomhetene kommet frem til at løsningen under SC vil være å respondere på den måten ved å skru av hele systemet og manuelt betjene stasjoner (trafostasjoner, større kraftverk o.l.) (se sitat N1R4). Da vil ofte kommunikasjonen mellom aktørene foregå ansikt til ansikt, via samband eller telefon (se sitat N1R2).

Tabell 20 Sitat respondere

Virksomhet	Sitat fra gruppeintervju	Tildelt kode	Tema
N1	«Dette har vi ikke veldig mye erfaring med det scenariet der da, for å si det sånn. Men det ville jo bli satt beredskap, som vi kaller det» (spm. 7).	N1R1	Respondere
	«Intern kommunikasjon vil nok skje på stedet i driftssentralen, face to face eller via nødnett eller mobiltelefoni» (spm. 7)	N1R2	Respondere
	«Vi har en beredskapsorganisasjon ut ifra beredskapsforskriften som er satt med folk som innehar en rolle og at det er stedfortredere på de viktige rollene» (spm. 7).	N1R3	Respondere
	«... Hvis de kan styre brytere på kraftverk og sånn så er det, ja, absolutt worst case. Ja, da går SCADA ned... Da må vi betjene lokalt i kraftverkene» (spm. 8).	N1R4	Respondere
N2	«Ja, vi kan jo si hvis vi har en alvorlig hendelse så vil det ofte gå ut en melding fra driftssentralen hos oss, eller det vil gå en melding fra en ekstern aktør som fanges opp internt, også går det ut en melding på beredskapsgruppen i (N2), og jeg som beredskapsleder tar jo en vurdering i, gjerne i lag med andre og ser hvor alvorlig er dette og kritikaliteten i hendelsen også etablerer vi en beredskapsstab på nivået alt ettersom hva behov og følger saken tett» (spm. 7).	N2R1	Respondere
	«Jeg tror akkurat på beredskaps- og kriseledelse i forhold til hendelser så tror jeg vi har ganske god struktur og rolleforståelse, men jeg kan vel si at vi har en del nye folk som ikke er så kjent med å drive beredskap, og det å skjønne rollen sin fullt ut... Er nok mange som tror at beredskap betyr at jeg er ansvarlig, men kraftberedskapsforskriften er jo ganske tydelig på hvilke ansvar som ligger til roller både på forebyggende beredskap og reaktiv beredskap» (spm. 7).	N2R2	Respondere
	«Det nok, vi har jo øvelser, men det nok mye trening i å forstå det fulle og hele formelle ansvaret. Det er nok litt å hente på det» (spm. 7).	N2R3	Respondere
	«Vi har jo felles SCADA-system med (tilhørende produksjonsselskap) da. Så de vil jo være rammet de og, av det samme... Da ville det typisk, de ville satt sitt beredskapsbord, og vi setter vårt, og vi ville hatt kommunikasjon mellom de to beredskapsorganisasjon, som har satt beredskap begge to» (spm. 8).	N2R4	Respondere
P1	«...et cyberangrep på SCADA og at det går ned da, det er nytt, det er ikke ett tilfelle, det er nytt for oss i denne sammenhengen, men hvor sannsynlig det er og alt det der er andre som må se nærmere på» (spm. 7).	P1R1	Respondere
	«...går SCADA ned så er vi «blindet» da, vi ser ikke totaliteten. Vi har kun kontroll på det som måtte være ute i våre kraftverk» (spm. 7).	P1R2	Respondere
	«Veldig viktig bryter i alle situasjoner som heter *fjernstyring på – av*, da må du fysisk ut å switche den og koble av SCADA og alt i hop» (spm. 7).	P1R3	Respondere
	«Vi må prøve å få kontakt med stasjonen og hvis det ikke er mulig må vi få ut folk dit, også må de stå å klø seg i hodet for å finne ut av hva som ikke fungerer, dette er jo noe som vi ikke har tenkt så mye på da» (spm. 7).	P1R4	Respondere
	«Vi agerer ikke før med mindre nettselskapet sier vi skal det da. Vi kan ikke starte opp noen kraftverk å håpe på, det går ikke» (spm. 8).	P1R5	Respondere
P2	«Vi har jo faste roller hvis det skjer en hendelse ... det blir jo satt en sånn, kriseorganisasjon da ... vi har gjort en del ganger med øvelser og sånt». (spm. 7).	P2R1	Respondere
	«Jeg tror hvis vi hadde hatt en hendelse hvor dette skjedde, og vi satt da en krisestab, så tror jeg vi ville ha kalt inn noen fra nettselskapet ... Da ville de ha blitt hentet inn...» (spm. 8)	P2R2	Respondere

5.3.4 Evnen til å lære og dens effekt på driftskontinuitet

Når det kommer til evnen å lære og dens effekt på driftskontinuitet har vi undersøkt hvorvidt virksomhetene deler erfaringer og lærdommer med hverandre. Videre har vi også inkludert

aspekter rundt cyber-relaterte beredskapsøvelser og hvorvidt de har spesifikke planer på hvordan man skal håndtere en slik hendelse. Det kan være relevant å nevne at det virker som at alle virksomhetene ikke har noen formell opplæring i SCADA-systemet. Likevel sier de aller fleste at dette systemet er noe de har jobbet med hver dag i flere tiår. Etter behov for de som ikke kan seg på dette systemet, får de hjelp av noen som har jobbet med SCADA-systemet i en lengre periode og kan det i sin helhet.

Til felles har alle virksomhetene etablert en form for evaluering/gransking av beredskapshendelser som oppstår. Det kommer fram hos alle at erfaringer av dette deles intern i egen virksomhet (se sitat N1L1, N1L2, N1L3, N2L1, P1L2, P2L1). På spørsmål om de deler disse erfaringene med eksterne aktører svarer de at det ikke er noe de er pålagt å gjøre, eller har nedskrevet i en rutine, men at der hvor det er naturlig vil de utveksle læring og erfaring med aktuelle eksterne aktører (se sitat N2L2). Dermed blir det vurdert ut ifra hendelsens alvorlighetsgrad hvorvidt andre eksterne virksomheter blir kontaktet eller ikke. I forhold til vår beskrivelse av SC, finner vi at alle virksomhetene mener det er en alvorlig nok hendelse hvor det hadde vært naturlig å kontakte tilknyttede nett- og produksjonsselskap. P1 beskriver i tilknytning til dette at hvis det er krise må det etableres en «dialog og få kontakt» med nettselskapet for å utrede situasjonen. N2 presiserer også at de har et IKT-sikkerhetsråd som brukes internt hos seg, men også sammen med et tilknyttet produksjonsselskap hvor IKT-sikkerhet er hovedtema for læring og informasjonsutveksling. De fleste sier at det «hadde vært naturlig» med inkludering av andre virksomheter under en hendelse, men ikke er noe som er nedskrevet i en rutine.

Når det kommer til beredskapsøvelser relatert til cyberangrep er dette noe de ulike virksomhetene fikk en tankevekker rundt. Ingen av virksomhetene hadde hatt øvelser på nivået med SC som er beskrevet (se sitat P2L3). Flere kan likevel fortelle at de har hatt mindre øvelser tilknyttet cyber ved bruk av skrivebordsøvelser, men har ikke inkludert et «worst-case»-scenario som er beskrevet i denne oppgaven. Ofte blir sånne typer øvelser noe som skrives ned, men noe som ofte er krevende å gjennomføre i henhold til planlegging, i tillegg til at det er ressurskrevende (se sitat N2L5, P2L2, P2L3). N2 forteller oss at en øvelse som tar for seg «bortfall av SCADA-systemet» er blitt anbefalt av NVE for aktører i kraftforsyningen (se sitat N2L3), og at dette er noe som burde prioriteres. NVE har også kommentert N1 sitt arbeid med beredskapsøvelser tilknyttet cyberangrep, hvor de hadde fått påpekt at de ikke hadde spesifikke nok planer på akkurat denne typen scenario (se sitat N1L5). Både N1 og N2 har påpekt at under SC så ville det blitt inkludert medlemmer fra SOC-tjenestene de kjøper, og dermed ville de

også blitt inkludert i denne typen øvelse. N1 påpeker at i en eventuell øvelse på dette så er det en «liten klikk» som er med, og ikke hele organisasjonen (se sitat N1L4). På spørsmål til N2 om de burde inkludere produksjonsselskapet som de deler SCADA-system med, i en sånn type øvelse relatert til SC, svarer beredskapsansvarlig at dette er «allerede notert det på blokken min» som et resultat av intervjuets fokusområde (se sitat N2L4). I tillegg presiserer N2 at å gjennomføre en slik øvelse, som NVE egentlig har anbefalt å gjøre når de eventuelt blir satt til BETA-beredskap, er noe de ønsker å gjøre allerede nå «så har vi faktisk gjort noe før vi må». Både P1 og P2 påpeker at denne typen scenario hadde vært «et kjempeproblem» og «hvis det hadde skjedd så hadde det gått både armer og ben her». P1 og P2 kunne tenke seg å bli inkludert i en større øvelse hvor deres tilknyttede nettselskap inkluderte dem (se sitat P1L1). P1 beskriver seg selv som en «forlenget arm» til nettselskapets beredskapsorganisasjon under SC. I sammenheng med dette forteller P1 oss at deres tilknyttede nettselskap har tendenser til en «ovenfra og ned holdning», der deres fokus er på sin egen virksomhet. Vi har et inntrykk av at nettselskapene ikke har et stort fokus på tilknyttede produksjonsselskap i koordineringen av beredskapsplaner og øvelser. Helhetlig får vi et inntrykk av at alle mener SC er et «worst-case»-scenario som er en stor trussel som de burde fokusere mer på (se sitat P1L3, P1L4, N2L4).

Tabell 21 Sitat lære

Virksomhet	Sitat fra gruppeintervju	Tildelt kode	Tema
N1	«Det skal rapporteres til myndighetene når hendelser oppstår, underveis og en evaluering i ettertid selvfølgelig» (spm. 9).	N1L1	Lære
	«Jeg tror det blir vurdert fra gang til gang jeg. Hvor mye dette egentlig påvirker dem og hva det vil bety ... Men i en sånn situasjon som dette her ville det vært helt naturlig å holde dem (produksjonsselskapet) oppdaterte da. Det er klart» (spm. 9).	N1L2	Lære
	«Det står ingen plass at det er viktig for oss å involvere produsentene i vår evaluering av hendelser, det står det ikke» (spm. 9).	N1L3	Lære
	«... Det er ikke alle som, spesielt når man tenker på cyber-relaterte ting, så er det ikke noe en involverer store deler av organisasjonen vår igjennom på det da. Liten klikk, som er på sånne øvelser» (spm. 11).	N1L4	Lære
	«Det er jo et scenario vi også har fått påpekt fra NVE om at vi ikke har spesifikke nok beredskapsplaner for å håndtere cyber, altså vi har en innsatsplan som sier at relevant personell skal involveres som i stor grad er leverandørene våre, og det er sannsynligvis ikke spesifikt nok da» (spm. 11).	N1L5	Lære
N2	«Vi har jo egentlig en obligatorisk rutine for evaluering, men ikke for å dele denne evalueringer eksternt, det har vi nok ikke skrevet i vår rutine» (spm. 9).	N2L1	Lære
	«Men om vi har skrevet den i rutinen så vil det være helt naturlig for oss å gjøre det med den aktøren som vi snakker om her som vi deler SCADA-system med da ... Vi må jo også rapportere dette inn til myndighetene, for læring da» (spm. 9).	N2L2	Lære
	«Den hendelsen her er jo kanskje «worst-case», men den er ikke verre enn at myndighetene har beskrevet den i en anbefalt øvelse til oss for, hvis vi	N2L3	Lære

	skulle havne i BETA-beredskap, altså neste nivå på alvorligheten på nasjonal sikkerhetsvurdering, så har de beskrevet en øvelse med bortfall av SCADA-systemet og hva vi gjør da» (spm. 7). «Jeg tenker kanskje dette med, kanskje gjøre øvelser mye tettere, at vi er mer trente på å håndtere en sånn type drift som er ute av balanse, det tror jeg vi må ta innover oss» (spm. 13). «Vi venter litt for lenge. Vi tar oss ikke tid til å øve, det blir ofte sånne skipper-tak at nå må vi ta en øvelse» (spm. 13).	N2L4 N2L5	Lære Lære
P1	«Det er en god case, da må nettselskapet være med, driftssentralen der». (spm. 11) «Vi må jo ha sånne evalueringer i ettertid, ikke sant» (spm. 9). «Jeg vil jo tro at cyber-angrep ... det er det verste som kan skje. Og det er jo kanskje det neste som skjer» (spm. 9)	P1L1 P1L2 P1L3	Lære Lære
P2	«Gransking. Når man har store hendelser så er det gransking ... som egentlig er erfaringsutveksling i etterkant» (spm. 7). «Jeg tror at man er flink til å ha en del øvelser på sin enhet. Men når du skal lage en øvelse som involverer hele kjeden, så er det veldig krevende. Vi har hatt det noen ganger... men det krever masse planlegging og det krever mye tid. Nå stilles det jo krav om at du skal ha hatt øvelser, og trent på sånn, men min oppfatning er at det er veldig enkle øvelser, gjerne bare redusert til din enhet og du «mister» den kjeden da» (spm. 11). «Det har vi hatt på blokken at vi skal ha akkurat en sånn øvelse, men vi har ikke gjennomført det» (spm. 11). «... det er den største trusselen vi har da, det går bra for oss og sånt, og det eneste som kan ødelegge det, det er et cyberangrep» (spm. 9).	P2L1 P2L2 P2L3 P1L4	Lære Lære Lære

5.4 Oppsummering

I denne delen har vi systematisk presentert de viktigste empiriske funnene våre gjort ved hjelp av en spørreundersøkelse og fire gruppeintervju. Funnene fra spørreundersøkelsen er presentert i henhold til de fire egenskapene i RE. Funnene fra gruppeintervjuene er presentert i henhold til driftskontinuitet samt de fire egenskapene i RE. Disse funnene skal brukes til å drøfte i henhold til forskningsspørsmålene våre, i samsvar med relevante dokumenter og oppgavens teoretiske utgangspunkt.

6. Drøfting

I denne delen skal funnene fra spørreundersøkelsen og gruppeintervjuene basert på det teoretiske grunnlaget og informasjonen innhentet gjennom dokumentanalysen, diskuteres og drøftes sett i sammenheng med forskningsspørsmålene. Gjennom å besvare alle forskningsspørsmålene får vi et utfyllende svar på oppgavens problemsstilling. På denne måten skal vi svare på hvordan prinsippene i RE og opprettholdelsen av driftskontinuitet kan benyttes til å forbedre arbeidet med forsyningssikkerhet i kraftsektoren. Dette sees da nærmere på gjennom et systemnivå ved hjelp av VSM. Det er nevneverdig å påpeke at alle egenskapene i RE er relatert til hverandre og dermed kommer det til å brukes sitater fra ulike egenskaper på tvers av hverandre gjennom drøftingen.

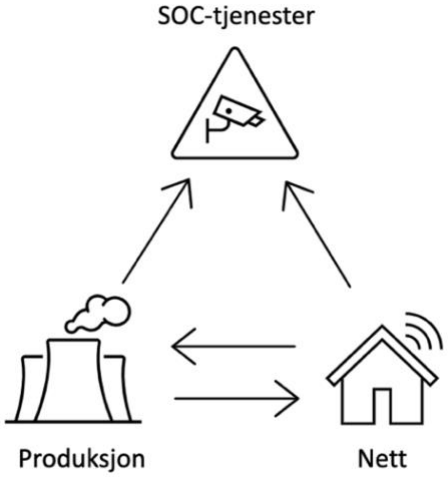
6.1 FS1: På hvilken måte er nett- og produksjonsselskapene avhengige av hverandre og eksterne aktører i arbeidet med cybersikkerhet?

Besvarelsen på FS1 vil gi oss en forståelse rundt kontinuitetsplaner og hvordan koordinering og samarbeid med eksterne aktører og internt faktisk utspiller seg hos de fire virksomhetene. Videre skal det avslutningsvis sees på rolleforståelsen rundt og i håndteringen av SC som de ulike virksomheten har og hvordan de stiller seg til å dele erfaring internt og eksternt.

Når det kommer til driftskontinuitet og kontinuitetsplanlegging er det tvetydighet i forståelsen rundt begrepsbruken. Det var inkludert i den innledende informasjonen til spørreundersøkelsen definisjoner og forklaringer av begreper. Ett av disse begrepene var kontinuitetsplaner, der DSB (2020) sin definisjon av kontinuitetsplaner er inkludert. Denne forståelsen går ut på at man kan bruke kontinuitetsplaner som metode for å redusere sannsynligheten for stopp i produksjonen og finne løsninger på hvordan virksomhetene kan opprettholde driften på et akseptabelt nivå, uansett hvilken ekstraordinær hendelse som inntreffer. Likevel kan man se gjennom spørreundersøkelsen usikkerhet rundt F4, hvor en stor andel av nettselskapene har svart «*vet ikke*», og nett- og produksjonsselskapene har en stor andel også svart «*helt uenig*», «*delvis uenig*» og «*verken enig eller uenig*». Dette er målinger som ikke kommer godt frem i visualiseringen gjennom radardiagrammet på bakgrunn av antallet som har svart «*vet ikke*». Selv om visualiseringen ikke viser det, tyder det på at ansatte i både nett- og produksjonsselskapene er usikre på hva kontinuitetsplaner er og hvorvidt dette er noe de praktiserer i deres virksomhet. Dette blir ytterligere underbygget gjennom gruppeintervjuene, hvor det er forskjeller mellom de ulike virksomhetene. Overordnet virker det som de fleste har noe kjennskap til kontinuitetsplaner, men at det ikke er noe som de anvender i stor grad i virksomhetene. P1 stilte seg uforståelige til begrepsbruken, og henviste seg videre til de som sitter på driftssentralen til deres tilknyttede nettselskap (se sitat P1D1). Både P2, N1, N2 viser til en forståelse rundt kontinuitetsplaner, men at dette ofte sees på i sammenheng med beredskapsplanverket og at kontinuitetsplanens hensikt blir dekket av denne og ved tilhørende innsatsplaner (se sitat N1K1, N2K1, P2K2). Ifølge energiloven (1990) og kraftberedskapsforskriften (2012) er ikke kontinuitetsplaner noe som er lovpålagt, men forståelsen og innholdet i dette kan sies å være omfavnet av lovkravene. Dette kommer blant annet til uttrykk i §1-1 i kraftberedskapsforskriften, som sier at KBO-enhetene skal sikre at forsyningen gjenopprettes på en effektiv og sikker måte *i* og etter ekstraordinære situasjoner kraftberedskapsforskriften (2012). Her henviser altså lovverket til at man også skal sikre drift *under* en uønsket hendelse, noe som er essensielt i kontinuitetsplanlegging og dermed også

kontinuitetsplaner. Beredskapsansvarlig i N2 utviste særlig god kontroll på forståelsen og bruken av kontinuitetsplaner og henviste til DSB (2020), noe som er svært positivt. Likevel, påpekes det av N2 at det som regel er de som jobber med beredskap i virksomhetene som kan noe om dette, og at det er noe som burde jobbes mer med for å dele kunnskapen videre i virksomheten. I henhold til kontinuitet i strømforsyningen, vil det være essensielt å kunne opprettholde driften for å ha en god forsyningssikkerhet. Dette kan gjøres ved hjelp av kontinuitetsplaner som et verktøy, i tillegg til beredskapsplanverket. Ved at kontinuitetsplaner er ukjent av flere ansatte og ikke brukt på tilstrekkelig nivå, kan det utgjøre at virksomhetene får en økt risiko og sårbarhet når det kommer til å opprettholde driften til tross for uønskede hendelser, som cyberangrep. Dette vil bli ytterligere diskutert i avsnittene under.

Når det kommer til koordineringen og samarbeidet i S1 og S3* eksisterer det en avhengighet. I henhold til driftskontinuitet burde det være en form for koordinering mellom aktørene i kraftforsyningskjeden. Her vil produksjonsselskapenes interessenter blant annet være de tilhørende nettselskapene som de deler driftssentral med og eventuelle SOC-tjenester. Videre er interessenter av nettselskapene blant annet deres tilhørende produsenter og SOC-tjenester. Samlet sett kan denne avhengigheten illustreres i figur 17. Produsentene (P1 og P2) leverer en produksjonsplan til deres tilknyttede nettselskap som de deler driftssentral med. Nettet til nettselskapene (N1 og N2) er selvgående og ikke i seg selv avhengig av produsentene, på den andre siden har ikke nettselskapene noe produkt å levere uten produsentene. På denne måten kan man se at nett- og produksjonsselskapene er gjensidig avhengige av hverandre for å levere det endelige produktet (strøm). Videre er noen av virksomhetene avhengige av eksterne leverandører, såkalte SOC-tjenester. Denne avhengigheten kan tenkes å være ensidig, da virksomhetene trenger SOC-tjenestene for å kunne overvåke sine systemer når det kommer til cyberangrep (se pilene i figur 17). Dermed ser man at avhengigheten til eksterne aktører/tjenester er noe alle virksomhetene har.



Figur 17 17Aktørenes avhengighet.

Som Hodges & Larraaga (2021) påpeker burde virksomhetene kartlegge sine avhengigheter og på den måten sikre en tryggere drift under forstyrrelser, som SC. Basert på denne gjensidige avhengigheten og generell avhengighet til SOC-tjenester, kan det i SC gjøre virksomhetene sårbare og ha økt risiko for sammenbrudd. Som vist i empirien har ingen av virksomhetene noe særlig erfaring eller kunnskap omkring større cyberangrep som SC. Gjennom et overordnet inntrykk kan det virke som om security-trusler, slik som SC, får et mindre fokus enn safety-trusler. Dette inntrykket er basert på at flere av virksomhetene trekker frem safety-relaterte eksempler, som steinras og orkan i nærheten av deres anlegg, når de nevner hendelser og erfaring/håndtering av disse. På denne måten kan man tenke seg at de har mer erfaring og kunnskap rundt safety-trusler fremfor security-trusler, spesielt når det kommer til trusler relatert til cyber. Dette kommer også frem ved at NVE, som følge av tilsyn, har påpekt mangler i beredskapsplanverket hos virksomhetene når det kommer til cyberangrep (se sitat N1L5). Dette kan også trekkes til og sees i sammenheng med lovkravene i forskriften, hvorav §7-8 henviser til at alle virksomhetene skal ha beredskap og forberedte tiltak for fortsatt drift av anlegg ved svikt i driftskontrollsystemet (SCADA-systemet) (Kraftberedskapsforskriften, 2012). Dermed vil det være hensiktsmessig og i tråd med loven for virksomhetene å ha klare planer for håndtering av cyberangrep som forårsaker bortfall av SCADA. Flere av virksomhetene har selv påpekt at dette er noe de har tenkt å følge opp, men noe de ikke har fått gjort i tilstrekkelig grad enda. Med tanke på avhengigheten mellom virksomhetene som har blitt illustrert, vil det også være hensiktsmessig å ha kontinuitetsplaner og eventuelle felles beredskapsplaner mellom nett- og produksjonsselskapene. Dette kan tenkes å gjelde spesielt for de som deler driftssentral, og dette er hensiktsmessig for å gjøre virksomhetene mer

resiliente i møte med uønskede hendelser som SC. Dette kommer også tydelig frem i kraftberedskapsforskriften (2012) §2-4 som i andre ledd forteller at beredskapsplanverket skal, innenfor rammene i kap. 6 om informasjonssikkerhet, samordne planverket med andre relevante virksomheter, deriblant andre KBO-enheter.

Når det kommer til de ulike virksomhetenes rolleforståelse rundt SC og hvordan de hadde respondert og delt erfaring i etterkant eksisterer det forskjeller. Før den uønskede hendelsen (SC) inntreffer (førkrisefasen), kommer det frem at de har lite erfaring og øvelser som baserer seg på cyberangrep. I kraftberedskapsforskriften (2012) kap. 5 oppsummerer forskriften ulike hensyn som særlig skal tas i betraktning når det kommer til ekstraordinære forhold, en av disse er «innbrudd, hærverk, sabotasje og andre kriminelle handlinger» jfr. §5-1 fjerde ledd. SC kan i denne sammenhengen kategoriseres som «sabotasje», på denne måten er cyberangrep noe som virksomheter i kraftsektoren burde ha større kjennskap til og erfaring rundt. Videre er øvelser noe som er lovpålagt å gjennomføre med slikt innhold og omfang at enheten vedlikeholder og utvikler kompetanse i å håndtere alle de aktuelle ekstraordinære situasjonene (Kraftberedskapsforskriften, 2012). Dette vil da også inkludere cyberangrep som SC. Tre av virksomhetene (P1, N1, og N2) koordinerer seg ikke med deres tilknyttede nett- eller produksjonsselskap når det kommer til beredskapsøvelser. P2 nevner at de har hatt enklere øvelser noen ganger med deres tilhørende nettselskap, som de deler driftssentral med. Øvelser generelt er noe som virksomhetene påpeker blir gjort iblant. Likevel, blir det påpekt at øvelsene som gjennomføres ofte er enkle (gjerne skrivebordsøvelser), og gjerne redusert til egen enhet. På den måten mister man den helhetlige forsyningskjeden (se sitat P2L2). Som man også ser basert på spørreundersøkelsens L7, er gjennomføring av beredskapsøvelser som inkluderer ekstreme scenarioer som cyberangrep noe det eksisterer usikkerhet rundt. Dette vises gjennom at det er flere som har svart «*vet ikke*» på denne påstanden. Gjennom gruppeintervjuene kommer det frem at cyber-relaterte øvelser, dersom det blir gjennomført, ofte blir med en liten gruppe i ledelsen (se sitat N1L4). Dette kan forklare hvorfor det ikke er tilfredsstillende målinger, fordi det er en liten enhet som inkluderes i denne typen øvelser og dermed er det ikke kjent for alle. Ved å ha enkle øvelser på sin enhet oppfyller virksomhetene lovkravet om øvelser, men et overordnet innrykk er at det ofte gjennomføres på denne måten nettopp for å oppfylle lovkravet og at potensialet for læring dermed ikke blir fullstendig utnyttet.

Under den uønskede hendelsen som beskrevet i SC (underkrisefasen), beskriver alle virksomhetene at det hadde vært naturlig å inkludere tilknyttede nett- og produksjonsselskap, på bakgrunn av omfanget av scenariobeskrivelsen. Det påpekes at det ikke er noe fast rutine

som er nedskrevet, men at det vil være naturlig å få kontakt med hverandre under SC. Det kan overordnet tenkes at virksomhetene ikke har tilstrekkelige beredskapsplaner rundt å respondere på SC (se sitat N1L5). Alle virksomhetene svarer klart på at de har nedskrevne roller i henhold til beredskap som er forutbestemte i deres virksomhet. På bakgrunn av dette ser man at alle har forutbestemte roller og ansvar, men at disse kanskje ikke er fult så klare når det kommer til håndteringen rundt SC. Det kommer også frem at rollefordelingen mulig ikke er tilfredsstillende i henhold til SC, blant annet på bakgrunn av avhengigheten til SOC-tjenestene. Dette skyldes at det er disse tjenestene som sitter på mesteparten av kunnskapen rundt cyberangrep som SC.

Etter den uønskede hendelsen har inntruffet og alt har gått tilbake til normalt (etterkrisefasen), sier alle virksomhetene at det hadde vært vanlig praksis å dele erfaringer og lærdommer med sine tilknyttede nett- eller produksjonsselskap til tross for at dette ikke er noe som er nedskrevet i en rutine. Virksomhetene gjør det klart i gruppeintervjuene at det etter SC, basert på dens omfang, ville vært naturlig for dem å dele erfaring og lærdommer med hverandre. Dette gjelder spesielt virksomhetene som deler driftssentral og eventuelt deler SCADA-system. Det kommer frem at nettselskapene er mindre avhengig av produsentene under SC. Helhetsinntrykket som kan trekkes fra dette tyder på at tankene rundt å ha en felles koordinering av planverk og øvelser framstår som mindre nødvendig for nettselskapene, enn hos produksjonsselskapene. Det påpekes videre i resiliens litteraturen i artikkelen til Colabianchi et al. (2021) hvor de har gjennomgått flere hundre dokumenter som blant annet omhandler integreringen av cyber-fysiske systemer i kritisk infrastruktur, hvor et funn er at et fåtall av disse problematiserer etterkrisefasen og hvordan disse komplekse systemene kommer seg etter at forstyrrelsen oppstår. Dette kan tyde på at siden det eksisterer mindre forskning på akkurat dette, er det vanskeligere for slike sektorer, som kraftforsyningen, å etablere faste rutiner og planer på hva denne etterkrisefasen skal inneholde. Basert på dette er det kanskje ikke uvanlig at nedskrevne rutiner ikke er noe som eksisterer på hvordan de skal dele erfaring og lærdommer internt og ekstern i virksomhetene. Avslutningsvis kan vi poengtere at ved spørsmål om felles koordinering med tilhørende nett- eller produksjonsselskap av en øvelse basert på SC og dens omfang, er det noe som alle virksomhetene stiller seg positive til.

6.2 FS2: Hvordan arbeider nett- og produksjonsselskapene med prinsippene i RE, sett opp mot SC?

Gjennomgående i FS2 skal vi systematisk gå igjennom de fire egenskapene i RE. Disse skal utforskes med funn fra spørreundersøkelsen og gruppeintervjuene fra empirien i kapittel 5, og

dokumentene som er presentert i metodekapittel 4.6.1. Vi skal på den måten knytte egenskapene i RE opp mot funnene vi har gjort. På den måten får vi presentert og knyttet sammen relevant teori og funn på en ryddig og presis måte.

Overvåke

Når det kommer til egenskapen overvåke, er et sentralt aspekt at virksomhetene gjennomfører analyser for risikoakseptkriterier. Dette kan gjøres på forskjellige måter og målet er å finne fram til indikatorer på hva virksomhetene skal se etter når de overvåker systemet. I sammenheng med de to aktørene vi tar utgangspunkt i (nett- og produksjonsselskaper) fra kraftforsyningen, er dette systemet SCADA-systemet. NVE gjennomfører også årlig en vurdering av nettselskapenes risikokategorier, der IKT-sikkerhet er inkludert (Meld. St. 25 (2015-2016)). På bakgrunn av dette er det viktig at både nett- og produksjonsselskapene etablerer risikoakseptkriterier i egen virksomhet. Når det kommer til kartleggingen gjennom RAG ser vi at egenskapen overvåke er noe både nett- og produksjonsselskapene samlet sett er svært gode på. Dette vises blant annet igjennom målingene fra O1-O6. Vi ser i påstand O3 og F6 at de som arbeider i nett- og produksjonsselskapene har god forståelse og kunnskap rundt hvilke risikoforhold de skal se etter på et generelt nivå. Dette tyder på at virksomhetene har indikatorer på hvilke risikoer de skal se etter og overvåke, og hva som aksepteres og ikke. I forhold til SC ser vi gjennom gruppeintervjuene at i overvåkingen av systemet, er de helt avhengige av andre leverandører (SOC-tjenester) som arbeider for dem på bakgrunn av manglende kunnskap i egen virksomhet. I henhold til sitat N1O2 og N2O1, ser vi at begge nettselskapene forventer at de eksterne tjenestene har fullt fokus på arbeidet med å overvåke trafikken i SCADA-systemet deres. På bakgrunn av dette presiseres det at dette ikke er noe de arbeider med selv i sitt daglige arbeid. Både P1 og P2 er avhengige av sine tilknyttede nettselskaper for denne typen overvåkning, samt eksterne SOC-tjenester. Dette kan tyde på at virksomhetene ikke har tilfredsstillende egne rutiner på å oppdage uregelmessigheter i systemene sine i forhold til cyberangrep. På den måten overvåker de ikke selv sine egne systemer i sammenheng med cyberangrep og cyber-relaterte trusler. Ut ifra dette kan det sies at virksomhetene har full tillit til at de eksterne tjenestene de kjøper rapporterer uregelmessigheter videre til dem. Helhetsinntrykket vårt er at virksomhetene til en viss grad har tenkt over cyberangrep på et generelt nivå. Det kan likevel sees ut ifra gruppeintervjuene at omfanget i SC er noe virksomhetene ikke har forestilt seg i stor grad. På bakgrunn av dette virker det som at virksomhetene har etablert en form for risikoforståelse rundt cyberangrep, men som Wreathall (2011) påpeker kan risikoakseptkriterier komme til kort når man skal

håndtere sikkerhet i fremtiden. Basert på SC's omfang kan det tenkes at virksomhetenes risikoforståelse ikke er tilstrekkelig. I henhold til VSM er det essensielt at et system har en evne til å tilpasse seg og forberede seg på enderinger i miljøet. Dette påpekes også av Wreathall (2011) som sier at miljøet rundt virksomhetenes og deres interne prosesser er dynamiske, og da kan fjorårets eller gårsdagens sikkerhet og risikoforståelse være svake i møte med morgensdagens risikoer. Også i henhold til VSM må et system kunne tilpasse seg fremtidige trusler og forbygge og overvåke disse for å være levedyktig over tid.

I sammenheng med egenskapen overvåke finnes det et klassisk kontrollregime. Kontrollregimet kan styres på to forskjellige måter, reaktivt og proaktivt (Wreathall, 2011). I henhold til kartleggingen gjennom RAG, kan det tenkes at alle virksomhetene har en form for proaktiv styringsform. Blant annet fordi målingene er overordnet svært gode for denne egenskapen og på den måten virker de årvåken på et generelt nivå. O1 viser at de overvåker systemet daglig og ser etter avvik. På bakgrunn av dette kan det tenkes at de får inn indikatorer på forstyrrelser i systemet og på den måten har forutsetninger for å forhindre svikt. Imidlertid vises det gjennom gruppeintervjuene at i sammenheng med SC framstår styringsformen mer reaktiv. Det vil si at avvik i sikkerheten vil endres etter at en slik hendelse har skjedd. Dette vises gjennom at omfanget rundt beskrivelsen av SC, i stor grad ikke er noe som er tenkt på i virksomhetene, og dermed vil det ikke være mulig for dem å være proaktive i møte med SC. Dette påpekes blant annet gjennom sitat N1L5, hvor det kommer frem at de har fått påpekt fra NVE at beredskapsplanverket har mangler i forhold til cybersikkerhet. Dette kan også trekkes og sees i sammenheng med VSM, hvor man kan tenke at det bør vektlegges en proaktiv styringsform for at et system skal være levedyktig over tid. På samme måte legger RE til grunn at man må ha en proaktiv styringsform for å oppnå en resilient virksomhet. På bakgrunn av dette kan vi si at virksomhetene burde bli mer proaktive i sin styringsform i møte med cyber-relaterte hendelser som SC. Som vist gjennom målingene i RAG er dette noe de har kapasitet til, siden de kan klare å være proaktive på et generelt nivå.

Forutse

Når det kommer til evnen å forutse er en sentral del systemets evne til å tilpasse seg og svare på kravene som det vil møte i fremtiden. Dette kan også refereres til som systemets adaptive kapasitet (Woods, 2011), som her er hvor adaptive de fire virksomhetene er. For å oppnå dette kreves det at virksomhetene gjør endringer som krever respons og justeringer. Det skal sees nærmere på de seks ulike mønstrene for hvordan resiliente systemer kan forutse at den adaptive

kapasiteten feiler i henhold til empirien vi har hentet inn. For denne oppgavens formål er det relevant å diskutere noen av mønstrene sammen med hverandre. Det første mønsteret omhandler at resiliente systemer har evnen til å oppdage at den adaptive kapasiteten er i ferd med å feile eller er uregelmessig (Woods, 2011). Det andre mønsteret som beskrives rundt å forutse er at resiliente systemer burde være i stand til å gjenkjenne om det trues av at ressursene brukes mer enn det man har buffere til (Woods, 2011). Disse nevnes om hverandre i diskusjonen i dette avsnittet. Ved å oppdage feil i systemet kan virksomhetene unngå dekompensasjon. Når det kommer til kartleggingen gjennom RAG, kan det tenkes at de har generelt god forståelse rundt evnen å forutse. Målingene viser gjennom F5 at de klarer å justere behovet for beredskap basert på dagens trusselbilde. Det å være oppdaterte på dagens trusselbilde er svært viktig i henhold til endringer for kraftsektoren som utfordrer driftssikkerheten, også når det gjelder IKT-sikkerhet (Meld. St. 25 (2015, 2016), NOU, 2023:3). Det kan videre virke som alle virksomhetene på et generelt nivå klarer å oppdage uregelmessigheter spesielt i henhold til endringer i trusselbildet, og på den måten justere og tilpasse seg etter dette. Gjennom gruppeintervjuene kommer det frem at produksjonsselskapene er avhengige av tilknyttede nettselskap og SOC-tjenester for å oppdage uregelmessigheter i SCADA-systemet. På samme måte er nettselskapene avhengige av SOC-tjenestene for å oppdage at den adaptive kapasiteten er i ferd med å feile i forhold til cyberangrep. N1 nevner at de har reserve buffere i den forstand at de har nettet skrevet ut på papir. På denne måten kan det tenkes at de har en form for redundans og da kan tilpasse seg en ny normal. Det samme gjelder at de må manuelt ut på stasjonene og kraftanleggene for å betjene dem, uten å fjernstyre på bakgrunn av SCADA-systemets bortfall gjennom SC. Den adaptive kapasiteten kan også sies å være en grunnsten i VSM, fordi man må kunne tilpasse seg miljøet rundt, også når det skal kunne forekomme endringer.

Det tredje og fjerde mønstret for forutsigelser handler om hvorvidt resiliente systemer er i stand til å gjenkjenne når de burde skifte prioriteringer og endre perspektiver, som kan være en motsetning fra det som representerer den daglige normen (Woods, 2011). Begge disse mønstrene viser til at virksomhetene må kunne endre perspektiv ved målkonflikter. En virksomhet som gir avkall på produksjonsmål til fordel for sikkerhetsmål, når det er nødvendig, er en prioritet for å oppnå resiliens. I henhold til kartleggingen gjennom RAG, kan det tenkes at virksomhetene justerer behovet for beredskap når det er nødvendigheter for det (F5). På den måten kan man gjennom kartleggingen tenke at de klarer å prioritere sikkerhetsmål når det oppstår målkonflikter. Når det kommer til gruppeintervjuene som er knyttet opp mot SC,

nevner flere av virksomhetene at det alltid vil være et spørsmål om kost-nytte når det kommer til å prioritere spesielt større øvelser rundt SC's omfang (se sitat P2L2). På denne måten kan det tenkes at de ikke har endret sine prioriteringer eller perspektiver rundt akkurat dette, selv om det er noe NVE har påpekt i lignende scenarioer hvor SCADA-systemet bortfaller og spesielt med tanke på dagens trusselbilde som poengteres i NOU 2023:3 og melding til stortinget nr. 25 (se sitat N1L4, N1L5) (Meld. St. 25 (2015, 2016), NOU, 2023:3).

De siste to mønstrene for forutsigelser i resiliente systemer kan diskuteres sammen. Det femte mønstret omhandler hvorvidt systemet er i stand til å navigere gjennom funksjonsavhengigheter på tvers av roller, aktiviteter og nivåer (Woods, 2011). Dette er et av de sentrale aspektene i VSM, hvor koordineringen, levedyktigheten og selv-organiseringen av kraftforsyningen som en helhet avhenger av de enkelte systemene (S1-S5) arbeider sammen på alle nivåer. Ifølge Woods (2011) burde de ulike nivåene i virksomhetene tilpasses hverandre på eksempelvis strategisk, taktisk og operativt nivå. Funksjonene på de ulike nivåene må da tilpasses hverandre. Det kan tenkes at de ulike virksomhetene gjør dette ved at de har forutbestemte roller og ansvar når det kommer til beredskapsarbeidet, og dette er noe de personene som er inkludert er klar over (se sitat N1R3, N2R1, N2R2, P2R1). Dette kan foregå på tvers av nivåer intern i virksomhetene. Likevel, påpeker N2 at ansatte som ikke har like godt kjennskap til virksomhetens beredskapsarbeid ikke har like god forståelse rundt rollen sin i denne typen arbeid, og dermed har behov for å trene på rolleforståelsen omkring dette (se sitat N2R2 og N2R3). I enkelte tilfeller vil det også kreves koordinering gjennom disse nivåene på tvers av virksomhetene i henhold til beredskapsarbeidet. Videre kan det tenkes at de ulike systemene i S1 har mangler når det kommer til samarbeid og koordinering mellom seg. Dette er sett nærmere på i FS1 og skal utdypes i henhold til øvrig teori i FS3. Når det kommer til det sjette mønstret som omhandler at systemet er i stand til å gjenkjenne behovet for å lære nye måter å tilpasse seg på, befinner resiliensen seg i hvordan systemet lærer (Woods, 2011). Dette kan tolkes i retningen av hvordan virksomhetene arbeider med det dynamiske risikobildet og hvordan de kan lære fra dette for å tilpasse seg. Nesten alle virksomhetene virker å være opptatt av årvåkenhet og sikkerhet rundt cyberrelaterte angrep. Alle nevnte at de har en sikkerhetstankegang hvor de er påpasselige rundt generell IKT-sikkerhet på arbeidsplassen og på den måten kan det tenkes at de ser et behov for å lære nye måter å tilpasse seg digitale trusler. På den andre siden kan det sees ut som at ingen av virksomhetene har sett for seg et «worst-case»-scenario som SC, og på den måten kan man tolke det som at virksomhetene ikke

har sett behovet for å lære seg å respondere på større cyberangrep. Noe som kan sies å være kritikkverdig.

Respondere

Når det kommer til egenskapen respondere omhandler dette virksomhetens evne til håndtere det aktuelle (Pariés, 2011). Dette betyr at virksomheten må kunne vite hva som skal til for å respondere på en hendelse hvor det har oppstått et avvik. Pariés (2011) mener at evnen til å respondere på riktig tidspunkt er viktig for å optimalisere eller redusere virkningene av hendelsen. Beredskapen i sammenheng med å respondere baserer seg på to strategier, en proaktiv- og en reaktiv tilnærming til beredskap. I sammenheng med kartleggingen gjennom RAG er det splittede målinger på ulike spørsmål fra spørreundersøkelsen. Generelt kan det trekkes frem her at evnen til å respondere er generelt god, og på denne måten kan det sies at virksomhetene arbeider med proaktiv beredskap. Det er noe forskjell fra nettselskapene og produksjonsselskapene. Nettselskapene har bedre målinger når det kommer til beredskapen rundt å respondere og håndtere hendelser som er beskrevet i scenarioer i planverk, dette kommer frem i R1-R3 og R5-R7. På den måten kan man si at nettselskapene har en form for generell tilnærming til proaktiv beredskap. På den andre siden viser målingene til produksjonsselskapene at det er noe forbedringspotensialet, som vist gjennom R1-R4. Videre har de gode målinger på R5-R7. Dette kan tyde på at ikke alle ansatte i produksjonsselskapene er særlig involvert i beredskapsplanverket, men at flere har mer forståelse rundt responsen på mobilisering og ressurser omkring beredskap. I sammenheng med produksjonsselskapenes generelle forståelse rundt beredskap, forteller både P1 og P2 i gruppeintervju at det er noen få i visse stillinger som har god kontroll på dette, og dermed ikke en generell kunnskap hos alle ansatte i produksjonsselskapene. Dermed kan man si at produksjonsselskapene har en form for generell proaktiv tilnærming til beredskap, men noe forbedringspotensial med tanke på videreformidling rundt økt beredskapsbevissthet.

Sett i sammenheng med SC og hvordan virksomhetene responderer på dette scenarioet kan det sies at alle har en reaktiv tilnærming til beredskap. Dette kommer av at en virksomhet forteller oss at de har ikke nok erfaring rundt denne typen scenario (se sitat N1R1). Gjennomgående virker det ikke som at noen av virksomhetene har hatt øvelse på nivå med SC, og heller ikke planverk som tilsier hvordan man skal respondere på en slik hendelse (se sitat P2L3, N1L5). Dette vil si at hvis SC blir en realitet, vil alle virksomhetene reagere med å være ad-hoc. I sammenheng med tidsperspektivet for utviklingen av hendelsen/krisen er det ledelsen som må

etablere gode beredskapsplaner og planlegge øvelser (i fortid), og på den måten kan deres ansatte og dem respondere på en riktig og effektiv måte (i nåtid), samtidig som man klarer å opprettholde beredskapen og totaliteten i levedyktigheten til systemet (i fremtid). Dette omhandler synkrone og diakrone tidsperspektiver, som også kan sees i sammenheng med Krukes (2012) krisefaser: før, under og etter krisen. Tidsperspektivet her kan sees i forhold til det Pariés (2011) beskriver som «resiliens i øyeblikket» der den «butte enden» (administrasjon og ledelse) burde sikre de nødvendige ressursene som personell, utstyr og kompetanse i tide før den uønskede hendelsen inntreffer deres virksomhet. På denne måten kan man se at tidsperspektivet er relevant i forhold til hvordan man skal forberede seg, håndtere og lære av den uønskede hendelsen.

Lære

Når det kommer til egenskapen lære er det ifølge RE tre betingelser som må være oppfylt (Hollnagel, 2011c). Den første og andre betingelsen handler om at det eksisterer rimelige muligheter for å lære og at situasjonen kan la seg generalisere, ved at de er like i sin natur. Denne egenskapen hos både nett- og produksjonsselskapene har noen ulikheter i kartleggingen gjennom RAG. Vi ser at nettselskapene har en god forståelse rundt denne egenskapen, selv om det er forbedringspotensial rundt beredskapsøvelser. I sammenligning med produksjonsselskapene er det svakheter rundt rapportering og beredskapsøvelser som krever forbedringspotensial. Begge har forbedringspotensial rundt beredskapsøvelser med eksterne aktører og øvelser som omhandler ekstreme scenarioer som cyberangrep (L7). Målingene gjennom RAG er svake som vist i L7, og kan tyde på at flere internt i virksomhetene er usikre rundt om beredskapsøvelser i dette omfanget er noe som er gjort eller ikke. Når det kommer til gruppeintervjuene vises det at det også er et forbedringspotensial rundt beredskapsøvelser, spesielt knyttet til tematikken i SC. Ved å ikke ha denne typen øvelser eksisterer det ikke rimelige nok muligheter på hvordan man kan respondere på en slik type hendelse. Da får ikke ansatte muligheten til å lære. På samme måte vil denne situasjonen gjennom en beredskapsøvelse ikke kunne la seg generalisere, fordi de ikke har erfart dette i en tilstrekkelig grad. Det kommer frem i intervjuet med N1 at det er en liten gruppe mennesker som sitter på denne kunnskapen som blir inkludert i mindre øvelser (skrivebordsøvelser) (se sitat N1L4). Dette kan forklare hvorfor flere ansatte ikke vet om de har gjennomført denne typen øvelser, fordi det er få inkludert i akkurat dette. Det overordnede inntrykket er at flere har mindre øvelser når det kommer til generell IKT-sikkerhet, som eksempel ukritisk klikk på eksterne lenker (phishing). Når det kommer til den tredje betingelsen omhandler den at det skal være

tilstrekkelig mulighet til å verifisere at de riktige lærdommene er trukket ut av situasjonen, denne betingelsen er en sammenkobling mellom de to forutgående betingelsene. Som diskutert ovenfor ser man at denne betingelsen ikke lar gjennomføre på bakgrunn av manglende erfaring og kunnskap rundt håndtering av SC, på grunnlag av mangelfulle læremuligheter basert på cyberangrep hvor det kan oppstå læring i virksomhetene.

6.3 FS3: Hvordan kan et fokus på driftskontinuitet og RE hos nett- og produksjonsselskapene være med på å forbedre forsyningssikkerheten i kraftsektoren?

I denne delen skal de to forutgående forskningsspørsmålene knyttes sammen, og på den måten besvare oppgavens problemsstilling. Det skal gjennomgående drøftes prinsippene i RE og driftskontinuitet, og hvordan disse utfyller hverandre sett i sammenheng med et systemnivå av kraftforsyningen gjennom VSM. Gjennom diskusjonen i FS1 og FS2 kan man utpeke tre diagnostiske problem i forhold til VSM, som skal utdypes gjennomgående i FS3. Dette er diagnostiske problemer som kan true systemets levedyktighet over tid. Det skal også her sees nærmere på løsningene til disse diagnostiske problemene.

Tabell 22 Oversikt over diagnostiske problem.

Nr.	Beskrivelse av identifisert problem
1.	Mangelfull koordinering og samarbeid mellom aktørene i S1.
2.	Manglende kunnskap og erfaring rundt cyberangrep som SC.
3.	Aktørene i S1's prioriteringer av produksjonsmål vs. sikkerhetsmål.

Det første diagnostiske problemet som skal utredes er mangelfull koordinering og samarbeid mellom nett- og produksjonsselskapene (S1), sett i sammenheng med SOC-tjenestene (S3*). En grunn til at dette kan være et diagnostisk problem kan være hvor avhengige aktørene i S1 er av hverandre og SOC-tjenestene (S3*). Som vist i FS1 ser man hvor lite koordinering og samarbeid de har i henhold til cybertrusler, på tross av den avhengigheten de allerede har til hverandre. I OEDs rapport påpeker de at en mer kompleks drift av nettet som følge av endringer i produksjon- og forbruksmønstre, gir et økt behov for koordinering mellom blant annet nett- og produksjonsselskaper (Olje- og energidepartementet, 2014). Statnett SF påpeker også en utfordring ved mange aktører i kraftforsyningskjeden, som igjen kan påvirke systemansvaret (Olje- og energidepartementet, 2014). Denne økte kompleksiteten kan også tenkes å skape et større behov for koordinering mellom nett- og produksjonsselskaper i henhold til dagens trusselbilde. Avhengigheten mellom aktørene kan medføre en økt sårbarhet for sammenbrudd

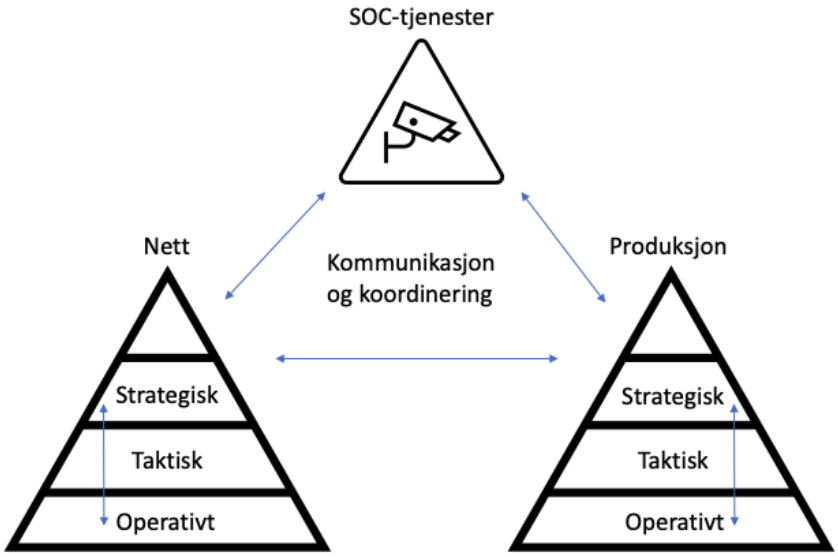
i SCADA-systemet, som kan kreve en tettere koordinering. Ved å kartlegge sine avhengigheter og samordne seg med hverandre kan de på en enklere måte effektivisere håndteringen av dynamiske og usikre miljøer (Hodges & Larraaga, 2021). For å redusere denne sårbarheten, kan man bruke ulike metoder for å gjøre håndteringen og arbeidet med cybertrusler enklere og på den måten bygge en mer resilient virksomhet. En metode som diskutert i FS2 er å etablere en mer proaktiv styringsform og proaktiv beredskap (Pariés, 2011; Wreathall, 2011). Gjennom kartleggingen av RAG ser man at både nett- og produksjonsselskapene behersker en proaktiv styringsform og proaktiv beredskap på en tilfredsstillende måte, selv om det er noe forbedringspotensial rundt produksjonsselskapenes videreformidling om beredskapsbevissthet. Det kommer frem at de på et generelt nivå klarer å ha en proaktiv styringsform og proaktiv beredskap, men når det kommer til cyber-relaterte hendelser ser man at dette ikke er tilfredsstillende. Dermed kan en løsning på dette problemet være å etablere en mer proaktiv styringsform og proaktiv beredskap, som kan inneholde å ha et tettere samarbeid med SOC-tjenestene og tilknyttede nett- og produksjonsselskap som deler driftssentral. I henhold til dette er det mulig å ha egne interne ansatte hos den felles driftssentralen, der noen fra produksjon- og nettselskapene sitter og overvåker SCADA-systemet. På samme måten kan man intern i egen virksomhet utpeke 1-2 personer som har ansvaret for informasjonsflyten mellom de og SOC-tjenestene. Her burde man bli opplært i hvordan man skal etablere et godt samarbeid, hvor man alltid er tilgjengelig hvis forstyrrelser inntreffer SCADA-systemet deres. Man kan på en mer effektiv måte overvåke og se etter avvik i forhold til cyber-relaterte trusler, gjennom en god koordinering og samarbeid mellom disse tre aktørene. De kan da kommunisere svikt i SCADA-systemet raskt gjennom kraftforsyningskjeden til de ulike aktørene, og forhindre forstyrrelser.

Det å etablere et tett samarbeid her er essensielt for å bygge en resilient virksomhet og på den måten styrke arbeidet med opprettholdelsen av driftskontinuitet på tvers av aktører i kraftforsyningskjeden. Dette kan videre eksempelvis etableres gjennom beredskapsøvelser som involverer tilknyttede nett- og produksjonsselskap og SOC-tjenester. På denne måten kan man ved en faktisk cyber-hendelse håndtere situasjonen på en koordinert og tilfredsstillende måte. Det samme gjelder felles planverk, i form av kontinuitetsplaner og beredskapsplaner, på den måten reduserer man sårbarheten under et angrep. Dermed kan man sikre en felles koordinering og forhindre at aktørene arbeider mot hverandre. På denne måten kan virksomhetene også oppfylle lovkravet i kraftberedskapsforskriften (2018) §2-4 om samordning med andre relevante virksomheter. Med tanke på felles øvelser og planverk burde

disse være generelle, på den måten kan man bruke det ved flere cyber-relaterte hendelser, og ikke bare ett spesifikt scenario. Dette kan sees i sammenheng med Hollnagel (2011a) sin andre betingelse av læring, der øvelser og planverk burde inneholde tilstrekkelig like komponenter for å la seg generalisere. På denne måten kan man sikre at man lærer det nødvendige før man responderer på en faktisk cyber-hendelse.

En annen løsning på det første diagnostiske problemet kan basere seg på det femte og sjette mønstret for forutsigelser i resiliente systemet. Ifølge det femte mønstret som omhandler navigering mellom funksjonsavhengigheter på tvers av aktiviteter, roller og nivåer (Woods, 2011), kan dette sees i sammenheng med både intern og eksternt samarbeid på tvers av hver virksomhet og nivåer intern i virksomheten. Som sett på tidligere i FS1 og FS2 er det som regel en liten gruppe eller de som arbeider med beredskap som sitter på kunnskapen om beredskap, i henhold til cybertrusler intern i egen virksomhet. Dette kan være en ulempe når det kommer til større hendelser som SC, som vil påvirke hele virksomheten og dens tilknyttede nett- og produksjonsselskap. Det kommer også frem gjennom gruppeintervjuene at der det er naturlig vil deres tilknyttede nett- og produksjonsselskap bli kontaktet, og at de ikke har noe fast rutine på når de skal kommunisere med hverandre i større hendelser. På denne måten kan det være nødvendig med en koordinering og samarbeid mellom internt strategisk, taktisk og operativt nivå, som horisontal koordinering og samarbeid mellom virksomhetene i kraftforsyningskjeden (se figur 18). Som følge av dette må de tilpasses hverandre og det burde eksistere en informasjonsflyt, og dette kan gjøres som nevnt gjennom felles planverk og øvelser. På denne måten er det ikke godt nok at virksomhetene anser noe som «naturlig», men burde ha en fast rutine på hvordan dette eventuelt skal gjøres. Dette er viktig for å unngå misforståelser rundt roller og ansvar, og vil gi et bedre grunnlag for sikrere drift i henhold til SC's omfang. På den måten kan man oppnå en sikrere opprettholdelse av driftskontinuitet. Det sjette mønstret for forutsigelser omhandler at virksomhetene gjenkjenner behovet når de må tilpasse seg nye måter å lære på (Woods, 2011). Selv om de gjensidige avhengighetene og andre avhengigheter eksisterer, burde virksomhetene etablere en større evne til å reflektere over denne kompleksiteten og på den måten gjenkjenne forandringer som burde føre til nye prosesser og metoder. Det tyder på i FS2 at nesten alle virksomhetene hver for seg har en sikkerhetstankegang, men denne tankegangen burde også koordineres basert på avhengighetene. Dette påpekes også av Hodges & Laarraga (2021) hvor den interaktive kompleksiteten til systemet som i denne sammenhengen er kraftforsyningen burde få en større forståelse rundt systemhelheten og dens avhengigheter, og på den måten skape et komplekst

adaptivt system. På denne måten kan disse to betingelsene være med på å bygge en mer resilient virksomhet i møte med cyber-relaterte trusler og redusere sårbarheten for sammenbrudd. Dette vil også være med på å styrke opprettholdelsen av driftskontinuiteten og arbeidet med dette i fremtiden. På den måten kan virksomhetene bli mer resiliente i møte med SC.



Figur 18 18 Horisontal og vertikal koordinering eksternt og internt.

Det andre diagnostiske problemet tar for seg manglende kunnskap og erfaring knyttet til cyber-relaterte angrep som SC hos virksomhetene. En grunn til at dette kan være et diagnostisk problem er at det på bakgrunn av gruppeintervjuene kommer frem at det på et overordnet nivå eksisterer mangler på kunnskapen og erfaring rundt cyber-relaterte trusler. På den måten kan man si at virksomhetene ikke har en tilfredsstillende forutsetning for å kunne håndtere SC. For å kunne løse dette diagnostiske problemet kan man se nærmere på ulike metoder. En løsning kan basere seg på det første og andre mønstret for forutsigelser (Woods, 2011), og en dynamisk risikoforståelse (Wreathall, 2011). Det første og andre mønstret kan kort omhandle hvordan virksomhetene oppdager at den adaptive kapasiteten er i ferd med å feile og at de burde være i stand til å gjenkjenne når systemet trues av at ressursene er i ferd med å ikke lenger være tilstrekkelig nok. I forhold til kartleggingen av egenskapen forutse gjennom RAG, kan det tyde på at de klarer å forhindre at den adaptive kapasiteten feiler og klarer også da å gjenkjenne når ressursene deres utmattes. På denne måten ser vi at selv om nett- og produksjonsselskapene har noe ulike målinger, er de generelt gode. Dette vil si at evnen eksister internt i virksomheten, men når det kommer til cyber-relatere trusler som SC, kan det tyde på at de har mindre kontroll over at den adaptive kapasiteten er i ferd med å feile og ressursene uttømmes. På bakgrunn av dette kan man se at den gjensidige avhengigheten (S1) og avhengigheten (S3*) kan gjøre at

virksomhetene internt ikke har tilstrekkelig kontroll når det kommer til cyberangrep. Basert på at overvåkningen og tilpasningen i virksomhetene overlates til tilknyttede nettselskaper og videre til SOC-tjenester, kan dette tyde på at virksomhetene internt mangler en egen kompetanse på cyber-relaterte trusler. På den måten kan det eksistere hull i kompetansen rundt denne tematikken som trengs for å håndtere og respondere på SC. Dette vil også påvirke evnen til å kunne opprettholde driften under SC. Selv om avhengigheten på overvåkning av SCADA-systemet eksisterer, burde dermed virksomhetene utvikle relevant risikoakseptkriterier i henhold til cybertrusler. På denne måten kan en videre løsning på dette problemet være å skape en større risikoforståelse rundt denne typen trusler. Overordnet kan det tyde på at nett- og produksjonsselskapene er klar over denne trusselen, men at de ikke har fokusert nok på cybertrusler i egen virksomhet. Dette kan sees i sammenheng med den adaptive kapasiteten, der virksomhetene er klar over dagens trusselbilde, men kanskje ikke har gjort nok for å tilpasse seg en dynamisk endring i forhold til det. Videre kan dette knyttes til Gierczak & Blake Messmer (2022), der det påpekes selv hvor oppdaterte virksomhetene kan være i henhold til planverket, krever fremtidig risiko og et dynamisk trusselbilde kontinuerlig årvåkenhet og tilpasning. På denne måten burde de ifølge VSM og Wreathall, (2011) tilpasse seg miljøet rundt virksomhetene, og på den måten kan de videreutvikle en felles dynamisk risikoforståelse rundt cybertrusler. Dette kan bidra til en forbedret driftskontinuitet i kraftforsyningskjeden. I sammenheng med resiliens litteraturen hvor Patriarca et al. (2021) påpeker økt forståelse blant ansatte og konteksten de arbeider i sosio-tekniske systemer. Her kan et økt fokus på å bygge kunnskap internt i egen virksomhet føre til mer pålitelige aktører i virksomheten. Når et cyberangrep inntreffer som SC, vil da aktører kunne håndtere og tilpasse systemet på en raskere måte på bakgrunn av en økt risikoforståelse. En videre løsning på dette kan trekkes til samme konklusjon som nevnt i første diagnostiske problemet, der felles øvelser og planverk står sentralt. Det som kan legges på er at de burde ha egne ansatte som arbeider aktivt med å tilpasse virksomheten i henhold til nye trusler og videre det dynamiske trusselbilde.

En annen løsning på det andre diagnostiske problemer kan utdypes gjennom første, andre og tredje betingelse for at læring skal finne sted (Hollnagel, 2011c). Den første og andre betingelsen omhandler at det eksisterer rimelige muligheter for å lære og at situasjonen kan la seg generalisere. Som vist i kartleggingen gjennom RAG, er både nett- og produksjonsselskapene generelt gode på egenskapen lære. Selv om det fins nyanser i målingene som diskutert tidligere. Noe som kan trekkes frem i henhold til dette er at både nett- og produksjonsselskapene har forbedringspotensial rundt beredskapsøvelser når det kommer til

ekstreme scenarioer, som cyberangrep (L7). Dette kommer også frem gjennom gruppeintervjuene, der cyber-relaterte beredskapsøvelser er noe som ikke har en stor nok prioritering hos virksomhetene. Hvis denne typen øvelser gjennomføres er det en liten gruppe som er med. Basert på disse funnene, kan det tyde på at de som blir inkludert ikke får rimelige nok muligheter til å faktisk kunne lære seg det godt nok. På bakgrunn av omfanget av cyber-relaterte øvelser de har hatt, som ofte da har vært små og mindre hyppige. Av denne grunn kan det tenkes at de få øvelsene ikke lar seg generalisere til hverandre, kanskje også fordi det gjennomføres sjeldent. På samme måte kan dette trekkes mot at ingen av virksomhetene har noen gang gjennomført en fullskala øvelse relatert til cyberangrep med sine tilhørende nett- eller produksjonsselskap og SOC-tjeneste. Dermed kan et scenario som SC påvirke virksomhetene i stor grad og den overordnede driftskontinuiteten. På bakgrunn av dette kan det tenkes at de ikke har hatt nok læring rundt denne typen øvelser. Dette gir mindre kunnskap og etablering av erfaring rundt denne tematikken. Dette kan sees i sammenheng med den tredje betingelsen, som omhandler at det skal være tilstrekkelig mulighet til å verifisere at de riktige lærdommene er trukket ut av situasjonen. Det vil være vanskelig å verifisere riktige lærdommer, når man sjeldent gjennomfører øvelser som kan verifisere de riktige lærdommene. Dermed burde virksomhetene prioritere det å gjennomføre beredskapsøvelser og trekke lærdommer og erfaringer ut av disse, for å forberede seg på et fremtidig cyberangrep. På denne måten kan virksomhetene etablere en bedre forutsetning for å opprettholde driftskoninuiteten når en slik hendelse inntreffer.

Det tredje diagnostiske problemet omhandler hvorvidt virksomhetene prioriterer produksjonsmål fremfor sikkerhetsmål. En grunn til at dette kan være et diagnostisk problem er at det gjennomgående i gruppeintervjuene kom frem et overordnet inntrykk av en kost-nytte-tankegang. Dette kan ha forhindret virksomhetene i å gjennomføre øvelser i et større omfang, hvor det også kunne ha blitt inkludert flere relevante aktører. Dette kommer også frem via karleggingen av RAG, hvor L6 viser utilfredsstillende målinger når det kommer til beredskapsøvelser som inkluderer alle relevante aktører som er involvert i en uønsket hendelse i kraftforsyningen. Her kan man se at dette ikke er noe som er prioritert i virksomhetene. Dette underbygges i gruppeintervjuene med at arbeidet med beredskap, øvelser og koordinering mellom hverandre kommer alltid tilbake til spørsmålet rundt tid, penger og ressurser (se sitat P2L2). Spesielt i henhold til større øvelser, på nivået med SC, som gjerne skulle inkludert flere enn egen virksomhet. Overordnet er inntrykket at de fleste gjennomfører mindre øvelser på sin enhet, og på den måten mister man det helhetlige perspektivet i kraftforsyningskjeden. På

denne måten kan arbeidet med driftskontinuitet i kraftforsyningskjeden falle bort. En løsning på dette problemet kan først sees igjennom det tredje og fjerde mønstret for forutsigelser. For å oppnå resiliens i virksomheten må de være i stand til å gjenkjenne når det burde skiftes prioriteringer og endre perspektiver, som kan være i motsetning fra det som representerer den daglige normen (Woods, 2011). Det kan gjennom gruppeintervjuene se ut som at alle virksomhetene er innforstått med at cyberangrep er en reell trussel, og muligens det neste som skjer (se sitat P1L3 og P2L4). Til tross for at virksomhetene er godt oppdaterte på dagens trusselbilde og et økt fokus på denne typen trusler i kraftsektoren generelt, er det ingen av virksomhetene som er noe godt forberedt internt på omfanget rundt SC. Dermed kan man se at de ikke prioriterer godt nok denne typen trussel når det kommer til erfaring og læring på hvordan man skal håndtere dette. På denne måten burde virksomhetene, på bakgrunn målkonflikter, prioritere større øvelser og kontinuitet i beredskapen for å forberede seg og ha erfaring rundt denne typen trussel. En beslektet løsning ifølge resiliens litteraturen kommer frem av Patriarca et al. (2022) der et cyber-resiliens perspektiv kan tas i bruk sammen med en vurdering av resiliens som er gjort i denne oppgaven. I sammenheng med dette foreslår de en stimuleringsbasert vurdering av cyber-resiliensen til virksomheten, på den måten kan virksomheter ha øvelser hvor de får stimulert et cyberangrep mot sine systemer, som SCADA. På denne måten kan virksomhetene få en bredere erfaring i å håndtere cybertrusler. Dette vil påvirke driftskontinuitet på en positiv måte, på den måten er de forberedt på hvordan de skal opprettholde forsyningen til tross for hindringer og at de effektiv klarer å forhindre forplantning i kraftforsyningskjeden.

Gjennomgående i FS3 har de to forutgående forskningsspørsmålene blitt koblet sammen og på den måten besvarer oppgavens problemsstilling. Det har blitt utarbeidet tre diagnostiske problemer, som ved hjelp av flere mulige løsninger kan være med på å forbedre forsyningssikkerheten i kraftsektoren på et systemnivå gjennom VSM. Løsningene som er foreslått er basert på oppgavens teoretiske grunnlag, spesielt knyttet til prinsippene i RE og driftskontinuitet. Hvis løsningene som er foreslått etableres kan det øke resiliensen i virksomhetene, spesielt når det kommer til cyberangrep som SC og på den måten forsterke levedyktigheten til det totale systemet. Samlet sett kan dette være med på å forbedre forsyningssikkerheten i kraftforsyningskjeden.

6.4 Oppsummering av drøfting

Oppgavens drøfting har ledet oss fram til følgende funn som vil bli presentert gjennom de ulike forskningsspørsmålene. FS1 viser at nett- og produksjonsselskapene er avhengige av hverandre

og SOC-tjenestene når det kommer til arbeidet med cybersikkerhet. Det kommer frem at produsentene er mer avhengige av nettselskapene de deler driftssentral med, enn nettselskapene er avhengige av sine produsenter når det kommer til håndteringen av SC. Dette til tross for at de er gjensidig avhengige av hverandre for å levere det endelige produktet (strøm). Både nett- og produksjonsselskapene er igjen avhengige av eksterne tjenester, SOC-tjenester, for å kunne overvåke sine systemer når det kommer til cyberangrep. Basert på den gjensidige avhengigheten mellom virksomhetenes tilknyttede nett- og produksjonsselskaper, og avhengigheten til SOC, kan virksomhetene under SC være sårbare og ha økt risiko for sammenbrudd. Dette baserer seg på at de ikke internt har tilstrekkelig kunnskap om cyberangrep, eller nødvendig erfaring og håndtering rundt denne typen uønskede hendelser. Dette fører da til at virksomhetene ikke har godt nok oppdaterte og koordinerte planverk basert på cyber-relaterte trusler med tilknyttede nett- og produksjonsselskap.

Når det kommer til FS2 ser vi hvordan nett- og produksjonsselskapene arbeider med prinsippene i RE, også sett i sammenheng med SC. Gjennomgående i henhold til kartleggingen av resiliens gjennom RAG vises det generelt gode målinger, men motsigende resultater kommer fram av egenskapene i henhold til SC. Når det kommer til egenskapen *overvåke*, ser man at målingene er både svært gode og gode. Her er nettselskapene mer årvåken når det kommer til rapportering av avvik, videre kan det sies at både nett- og produksjonsselskapene vet når beredskap skal iverksettes på bakgrunn av avvik. I henhold til SC, ser man at de overlater overvåkingen til SOC-tjenestene når det kommer til cybertrusler. Når det kommer til egenskapen å *forutse* er målingene generelt gode. Det eksisterer noen nyanser i målingene innenfor denne egenskapen hos både nett- og produksjonsselskapene, overordnet kommer nettselskapene bedre ut enn produksjonsselskapene her. Både nett- og produksjonsselskapene viser svært gode målinger på at de justerer behovet for beredskap basert på dagens trusselbilde og rapportere uregelmessigheter internt. Videre er det noe forbedringspotensial rundt forståelsen av risikoakseptkriterier hos begge. I henhold til SC, ser man under denne egenskapen at virksomhetene på et generelt nivå er gode til å oppdage endringer i trusselbilde og justere seg etter dette. På den andre siden kan det sees ut som at virksomhetene prioriterer produksjonsmål fremfor sikkerhetsmål, og på den måten ikke prioriterer et sikkerhetsperspektiv i forhold til omfanget av SC. Når det kommer til egenskapen *respondere* er det et lite skille mellom nett- og produksjonsselskapene. Nettselskapene har noe som ser ut til å være en svært god forståelse rundt når beredskap skal iverksettes, og håndteringen av langvarige beredskapshendelser. På den andre siden har produksjonsselskapene noe

forbedringspotensial basert på å videreformidle beredskapsplanverket til alle i virksomheten. Videre er det generelt gode målinger på det som omhandler det å mobilisere i henhold til planverket og håndtere langvarige beredskapshendelser. I henhold til SC, kommer det frem at virksomhetene har en reaktiv tilnærming til beredskap. Når det kommer til egenskapen å *lære* er dette den egenskapen hvor både nett- og produksjonsselskapene har lavest målinger. Begge har forbedringspotensial rundt beredskapsøvelser og inkludering av ekstreme scenarioer i beredskapsplanverket. I henhold til SC, kommer det frem at det sjeldent gjennomføres beredskapsøvelser som omhandler tematikken i SC. På et overordnet nivå kan man trekke frem at målingene gjennom RAG er gjennomgående gode på et generelt nivå basert på kartlegging av resiliens i virksomhetene. Videre er det forbedringspotensial rundt egenskapene når det kommer til SC. Disse motsigelsene fra kartleggingen gjennom RAG og egenskapene basert på SC, ble sett nærmere på i de tre diagnostiske problemene i FS3.

FS3 knytter sammen de to forutgående forskningsspørsmålene og presenterer oppgavens hovedfunn gjennom de tre diagnostiske problemene vi har kartlagt ved hjelp av VSM og sett i sammenheng SC. Det første diagnostiske problemet baserer seg på mangler i koordinering og samarbeid mellom nett- og produksjonsselskapene (S1) samt SOC-tjenestene (S3*) i direkte sammenheng med SC. Det eksisterer en gjensidig avhengighet mellom disse og denne avhengigheten øker sårbarheten for bortfall av SCADA-systemet, som da også vil påvirke tilknyttede nett- og produksjonsselskap. Det er ikke nok at kommunikasjon mellom disse anses som «naturlig». En løsning er at det burde bli nedfelt i virksomhetenes rutiner hvordan denne kommunikasjonen skal foregå for å sikre en tilfredsstillende felles koordinering. Dette sikrer at aktørene jobber med hverandre for å redusere sårbarheten under et angrep. I tillegg kan problemet løses ved å sikre større informasjonsflyt og informasjonsutveksling på tvers av virksomhetenes nivåer internt og eksternt, eksempelvis gjennom felles planverk og øvelser. Det andre diagnostiske problemet viser at det er en manglende kunnskap og erfaring knyttet til cyberrelaterte trusler hos virksomhetene. Som igjen viser til at virksomhetene har dårlige forutsetninger for å håndtere slike angrep på en tilfredsstillende måte. Løsninger på dette presenteres gjennom å etablere en god risikoforståelse gjennom relevante risikoakseptkriterier i henhold til cybertrusler basert på dagens trusselbilde. Dette vil ha en direkte påvirkning på virksomhetenes adaptive kapasitet og dermed også deres evne til å opprettholde driften under et angrep. Da vil de få mulighet til å tilpasse systemet på en tilfredsstillende måte og dermed sikre en bedre håndtering av hendelsen. Dette problemet kan også løses ved å tilrettelegge for at virksomhetene skal lære seg å håndtere slike hendelser spesifikt gjennom å gjennomføre

beredskapsøvelser med et omfang som vil dekke SC eller lignende. Det siste diagnostiske problemet tilsier at virksomhetene tilsynelatende prioriterer produksjonsmål fremfor sikkerhetsmål når det kommer til cybertrusler. Det vises gjennom at det ikke har blitt gjennomført øvelser i større omfang, som eksempelvis SC, på bakgrunn av at det er ressurs- og tidkrevende. Vi mener dermed at tankegangen hos virksomhetene må endres på en slik måte at sikkerhet blir prioritert i henhold til å gjennomføre større øvelser som gjør virksomhetene mer resilient i møte med et cyberangrep. Løsningene på de diagnostiske problemene vil bidra til en forbedret forsyningssikkerhet i kraftforsyningen.

7. Konklusjon

Oppgaven har søkt å svare på følgende problemstilling, sett i sammenheng med SC:

Hvordan kan prinsippene for «Resilience Engineering» og opprettholdelsen av driftskontinuitet benyttes til å forbedre forsyningssikkerheten hos aktører i kraftforsyningen på et systemnivå?

SC: Cyberangrep på SCADA-system (hos både nett- og produksjonsselskap)

Gjennom de tre forskningsspørsmålene våre presentert over i kapittel 6 kan vi hente ut svaret på oppgavens problemstilling. Svaret på dette befinner seg i det tredje forskningsspørsmålet som kobler sammen FS1 og FS2. Her har det har blitt utarbeidet tre diagnostiske problemer som det tilhørende har blitt foreslått løsninger på for å forbedre forsyningssikkerheten i kraftsektoren. Det første diagnostiske problemet omhandler mangelfull koordinering og samarbeid mellom nett- og produksjonsselskapene. Det andre diagnostiske problemet viser en manglende kunnskap og erfaring rundt cyberangrep. Det tredje diagnostiske problemet viser til at nett- og produksjonsselskapene tilsynelatende prioriterer produksjonsmål fremfor sikkerhetsmål. Gjennom løsningene på disse diagnostiske problemene kan vi konkludere med at virksomhetene i kraftforsyningen kan anvende RE-prinsippene gjennom en praktisk tilnærming, som presentert i oppgavens drøfting. Ved anvende RE-prinsippene (overvåke, forutse, respondere og lære) og fokusere på opprettholdelsen av driftskontinuitet gjennom økt koordinering, samarbeid og felles planverk, vil dette gjøre de mer resilient i møte med cybertrusler, som SC. Dette har blitt utforsket på et systemnivå gjennom VSM. Systemnivå i henhold til VSM kan sees i sammenheng med at det er basert på en systemisk diagnose av levedyktigheten til et system, som i denne oppgaven er kraftforsyningen.

Gjennomgående i oppgaven har det blitt brukt VSM. Ved hjelp av VSM har vi blant annet visualisert kraftforsyningen som et helhetlig levedyktig system bestående av fem sub-systemer. VSM legger til grunn at resiliente systemer må ha kapasitet til å tilpasse seg sine dynamiske miljøer. Dette er også sentrale aspekter av RE og driftskontinuitet når det kommer til systemets adaptive kapasitet. VSM blir på den måten nyttig i å kunne kartlegge komplekse systemer, dets nivåer og hvordan systemet på beste måte kan være levedyktig over tid gjennom tilpasning til et forandrende miljø og koordinering mellom de forskjellige nivåene. Denne oppgaven har forholdt seg til system 1 og dets subsystemer (to nettselskaper og to produksjonsselskaper) og S3* (SOC-tjenester). Endringer i miljøet for kraftforsyningen knyttes til endringer i trusselbildet. Endringer i trusselbildet kan føre med seg behov for store endringer i hvordan virksomhetene handler før, under og etter hendelser. Med tanke på den interaktive kompleksiteten i den økte andelen av cyber-fysiske systemer som kraftforsyningen er, kreves det nye metoder for å utarbeide planverk og øvelser som omfatter cyber-relaterte hendelser som SC. Disse må dermed gjennomføres på en måte som gir et større utbytte i henhold til læring, for å sikre en tilstrekkelig tilpasning og dermed mer resiliente virksomheter. Det vil være vanskelig å oppnå en perfekt resilient virksomhet, men det er ikke umulig dersom man arbeider systematisk med løsningene som denne oppgaven har lagt til grunn. Det innebærer at virksomhetene i kraftforsyningen tar til seg løsningene som har blitt presentert i henhold til de tre diagnostiske problemene. I henhold til VSM kan det sees på som en trussel for kraftsektorens levedyktighet over tid dersom de diagnostiske problemene vi har identifisert ignoreres, og våre løsninger på dem ikke blir tatt til betraktning i større grad. Dermed kan vi avslutningsvis si at ved å arbeide med prinsippene i RE og opprettholdelsen av driftskontinuitet, burde virksomhetene kunne justere sine funksjoner både før, under og etter forstyrrelser, og dermed vil de kunne opprettholde sine nødvendige funksjoner i koordinering med relevante aktører. Dette vil videre kunne bidra til en forbedret forsyningssikkerhet blant aktørene i kraftforsyningen.

Forslag til videre forskning

Denne oppgaven har hatt et fokus på systemnivå av kraftforsyningen hvor det har blitt inkludert totalt fire virksomheter. Til videre forskning hadde det vært svært interessant å inkludere de tilhørende SOC-tjenestene, og se på den eksisterende avhengigheten til disse mer i dybden. I denne oppgaven er det ikke inkludert noen informanter fra SOC-tjenestene, fordi dette var noe som ble kjent for oss underveis i datainnsamlingen. I sammenheng med dette kunne det også vært interessant å utforske på et mer individuelt nivå hvordan ulike virksomheter i kraftsektoren

kartlegger systemhelheten og dens påvirkningsfaktorer, og hvordan forbedringer rundt dette kan gjøre hele systemet mer resilient i fremtiden (Hodges & Larraaga, 2021). Videre hadde det vært interessant å sett på hvordan flere aktører i kraftforsyningen arbeider med prinsippene i RE og opprettholdelsen av driftskontinuitet både direkte og indirekte. På den måten kunne man fått et større bilde over sektoren. VSM som metodisk rammeverk har vist seg å være svært nyttig for å studere store komplekse systemer, slik som vi har gjort med kraftforsyningen. Det vil også være svært interessant å benytte VSM for å studere andre komplekse systemer, som for eksempel samferdselssektoren eller olje-og energisektoren. Videre kunne man sett på de andre systemene i VSM enn de vi har hatt som hovedfokus (S1 og S3*), som myndighetsnivåene (OED og NVE), for å skape et større bilde over kjeden som en helhet.

8. Litteraturliste

Aven, T., & Renn, O. (2010). *Risk Management and Governance: Concepts, Guidelines and Applications* (2010., Bd. 16). Springer Berlin Heidelberg : Imprint: Springer.

Aven, T., & Thekdi, S. (2021). *Risk Science: An Introduction*. Routledge. https://doi.org/10.4324/9781003156864

Beer, S. (1984). The Viable System Model: Its Provenance, Development, Methodology and Pathology. *The Journal of the Operational Research Society*, *35*(1), 7–25. https://doi.org/10.1057/jors.1984.2

Beer, S. (1985). *Diagnosing the system for organizations*. Wiley.

Blaikie, N., & Priest, J. (2019). *Designing social research: The logic of anticipation: Bd. 3.* Polity Press.

Buckl, S., Matthes, F., & Schweda, C. M. (2009). A viable system perspective on enterprise architecture management. *2009 IEEE International Conference on Systems, Man and Cybernetics*, 1483–1488. https://doi.org/10.1109/ICSMC.2009.5346262

Busmundrud, O., Maal, M., Kiran, Jo. H., & Endregard, M. (2015). *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger* (Nr. 2015/00923; FFI-rapport). Forsvarets forskningsinstitutt (FFI). https://www.ffi.no/publikasjoner/arkiv/tilnaerminger-til-risikovurderinger-for-tilsiktede-uonskede-handlinger

Colabianchi, S., Costantino, F., Di Gravio, G., Nonino, F., & Patriarca, R. (2021). Discussing resilience in the context of cyber physical systems. *Computers & Industrial Engineering*, *160*, 107534. https://doi.org/10.1016/j.cie.2021.107534

Danermark, B., Ekström, M., Jakobsen, L., & Karlsson, J. C. (2002). *Explaining society: Critical realism in the social sciences*.

DSB. (2016). *Samfunnets kritiske funksjoner: Hvilken funksjonsevne må samfunnet opprettholde til enhver tid?* (KIKS 2-rapport). Direktoratet for samfunnssikkerhet og beredskap (DSB).

DSB. (2020). *Veileder i kontinuitetsplanlegging* (978-82-7768-504-5 HR-nummer: 2430). DSB. https://www.dsbinfo.no/DSBno/2019/veiledning/veileder-i-kontinuitetsplanlegging/

Energiloven. (1990). *Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m* (LOV-1990-06-29-50). Olje- og energidepartementet. https://lovdata.no/dokument/NL/lov/1990-06-29-50#KAPITTEL_9

Engen, O. A. H., Kruke, B. I., Lindøe, P., Olsen, K. H., Olsen, O. E., & Gould, K. A. P. (2021). *Perspektiver på samfunnssikkerhet* (2. utg.). Cappelen Damm akademisk.

Eriksen, J., Rake, E. L., & Sommer, M. (2021). *Beredskapsanalyse*. Cappelen Damm Akademisk.

Fernandes, A., & Tribolet, J. (2019). Enterprise Operating System: The enterprise (self) governing system. *Procedia Computer Science*, *164*, 149–158. https://doi.org/10.1016/j.procs.2019.12.167

Gierczak, M., & Blake Messmer, J. (2022). How to build more resilient businesses and communities: A proposal. *Journal of Business Continuity & Emergency Planning*, *15*(4), 330–341.

Grønmo, S. (2004). *Samfunnsvitenskapelige metoder*. Fagbokforl. https://www.nb.no/search?q=oaiid:"oai:nb.bibsys.no:999617985804702202"&mediatype=bøker

Gundel, S. (2005). Towards a New Typology of Crises. *Journal of Contingencies and Crisis*

Management, *13*(3), 106–115. https://doi.org/10.1111/j.1468-5973.2005.00465.x

Harrison, C., Eckman, B., Hamilton, R., Hartswick, P., Kalagnanam, J., Paraszczak, J., & Williams, P. (2010). Foundations for Smarter Cities. *IBM Journal of Research and Development*, *54*(4), 1–16. https://doi.org/10.1147/JRD.2010.2048257

Hegghammer, T. (2012). Islamism: Contested Perspectives on Political Islam Edited by RICHARD C. MARTIN and ABBAS BARZEGAR. *Journal of Islamic Studies (Oxford, England)*, *23*(2), 252–254. https://doi.org/10.1093/jis/ets004

Hodges, L. R., & Larraaga, M. D. (2021). Emergency management as a complex adaptive system. *Journal of Business Continuity & Emergency Planning*, *14*(4), 354–368.

Hollnagel, E. (2011a). Epilogue: RAG - The Resilience Analysis Grid. I E. Hollnagel, J. Pariés, & D. D. Woods, *Resilience Engingeering in Practice: A guidebook*. Ashgate.

Hollnagel, E. (2011b). prologue: The Scope of Resilience Engineering. I E. Hollnagel, J. Pariés, D. D. Woods, & J. Wreathall, *Resilience Engingeering in Practice: A guidebook*. Ashgate.

Hollnagel, E. (2011c). To Learn or Not to Learn, that is the Question. I E. Hollnagel, D. D. Woods, J. Pariés, & J. Wreathall, *Resilience engineering in practice: A guidebook*. Ashgate.

Hollnagel, E., Woods, D. D., & Leveson, N. (2006). *Resilience engineering: Concepts and precepts*. Aldershot, UK: Ashgate.

Jacobsen, D. I. (2005). *Hvordan gjennomføre undersøkelser?: Innføring i samfunnsvitenskapelig metode* (2. utg.). Høyskoleforlaget. https://www.nb.no/search?q=oaiid:"oai:nb.bibsys.no:990514650864702202"&mediatype=bøker

Johannessen, A., Christoffersen, L., & Tufte, P. A. (2021). *Introduksjon til samfunnsvitenskapelig metode* (6. utgave.). Abstrakt forlag.

Jore, S. H. (2015). Challengers of Building Societal Resilience through Organizational Security Risk Management. *Working on Safety, Portugal*.

Jore, S. H. (2017). The Conceptual and Scientific Demarcation of Security in Contrast to Safety. *European Journal for Security Research*. https://doi.org/10.1007/s41125-017-0021-9

Kraftberedskapsforskriften. (2012). *Forskrift om sikkerhet og beredskap i kraftforsyningen* (FOR-2012-12-07-1157). Olje- og energidepartementet. https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157

KraftCERT. (2023, mars 14). *Sikring av prosesskontrollsystemer mot digitale angrep*. https://www.kraftcert.no/no/#tjenester

Kripos. (2023). *Politiets trusselvurdering 2023*. Kripos. https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/politiets-trusselvurdering-ptv/politiets-trusselvurdering-2023.pdf

Kruke, B. I. (2015). Planning for crisis response: The case of the population contribution. I *Safety and reliability of complex engineered systems: Proceedings of the 25th European Safety and Reliability Conference* (s. 177–185). Taylor & Francis.

Kruke, B. I. (2012). *Samfunnssikkerhet og krisehåndtering: Relevans for 22.juli 2011* (Notat: 7/12). til 22-juli kommisjonen.

Lay, E. (2011). Practices for Noticing and Dealing with the Critical. A Case Study from Maintenance of Power Plants. I *Resilience Engingeering in Practice: A guidebook*. Ashgate.

Lun, Y. Z., D'Innocenzo, A., Smarra, F., Malavolta, I., & Di Benedetto, M. D. (2019). State of the art of cyber-physical systems security: An automatic control perspective. *The Journal of Systems and Software, 149*, 174–216. https://doi.org/10.1016/j.jss.2018.12.006

Martin, P. (2019). *The rules of security: Staying safe in a risky world* (s. 272 s.). Oxford University Press.

Marx, A., Rihoux, B., & Ragin, C. (2014). The origins, development, and application of Qualitative Comparative Analysis: The first 25 years. *European Political Science Review*, *6*(1), 115–142. https://doi.org/10.1017/S1755773912000318

Meld. St. 25 (2015-2016). *Kraft til endring—Energipolitikken mot 2023*. Olje- og energidepartementet. https://www.regjeringen.no/contentassets/31249efa2ca6425cab08130b35ebb997/no/pdfs/stm201520160025000dddpdfs.pdf

Meld. St. 38 (2016-2017). *IKT-sikkerhet: Et felles ansvar*. Justis- og beredskapsdepartementet.

Meld.St.5 (2020-2021). *Samfunnssikkerhet i en usikker verden*. Justis- og beredskapsdepartementet. https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm202020210005000dddpdfs.pdf

Njå, O., Sommer, M., Rake, E. L., & Braut, G. S. (2020). *Samfunnssikkerhet: Analyse, styring og evaluering*. Universitetsforlaget.

Norsk Standard. (2019). *Sikkerhet og resiliens – systemer for kontinuitetsledelse*. NS-ISO 22301:2019. https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=1124802

NOU. (2000:24). *Et sårbart samfunn—Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet*. Justis- og beredskapsdepartementet. https://www.regjeringen.no/contentassets/1c557161b3884335b4f9b89bbd32b27e/no/pdfa/nou200020000024000dddpdfa.pdf

NOU. (2006:6). *Når sikkerhet er viktigst—Beskyttelse av landets kritiske infrastruktur*. Justis- og beredskapsdepartementet. https://www.regjeringen.no/contentassets/c8b710be1a284bab8aea8fd955b39fa0/no/pdfs/nou200620060006000dddpdfs.pdf

NOU. (2022:6). *Nett i tide—Om utvikling av strømnettet*. Olje- og energidepartementet. https://www.regjeringen.no/contentassets/9dabbb7fb58e4bb297f4388696570460/no/pdfs/nou202220220006000dddpdfs.pdf

NOU. (2023:3). *Mer av alt—Raskere* (Energikommisjonen). Olje- og energidepartementet. https://www.regjeringen.no/contentassets/5f15fcecae3143d1bf9cade7da6afe6e/no/pdfs/nou202320230003000dddpdfs.pdf

NSM. (2023a). *Risiko 2023—Økt uforutsigbarhet krever høyere beredskap*. Nasjonal sikkerhetsmyndighet. https://nsm.no/getfile.php/1312547-1676548301/NSM/Filer/Dokumenter/Rapporter/Risiko%202023%20-%20Nasjonal%20sikkerhetsmyndighet.pdf

NSM. (2023b). *Sikkerhetsfaglig råd—Et motstandsdyktig Norge*. Nasjonal sikkerhetsmyndighet. https://nsm.no/getfile.php/1312994-1683615611/NSM/Filer/Dokumenter/Rapporter/Sikkerhetsfaglig%20råd%20-%20Et%20motstandsdyktig%20Norge.pdf

NVE. (2011). *Veiledning til forskrift om beredskap i kraftforsyningen* (Nr. 1). Norges vassdrags- og energidirektorat. https://publikasjoner.nve.no/veileder/2011/veileder2011_01.pdf

NVE. (2022a, januar 7). *Kraftforsyningens beredskapsorganisasjon (KBO)*. Kraftforsyningens beredskapsorganisasjon (KBO). https://www.nve.no/energi/tilsyn/kraftforsyningsberedskap-og-kbo/kraftforsyningens-beredskapsorganisasjon-kbo/

NVE. (2022b, april 13). *Kraftforsyningsberedskap og KBO - NVE*. Kraftforsyningsberedskap og KBO. https://www.nve.no/energi/tilsyn/kraftforsyningsberedskap-og-kbo/

Nygård, A. R. (2004). *Risk management in SCADA-system* [Masteroppgave, Kungliga Tekniska Høgskolan (KTH)]. https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/143918/nygÃ¥rd_-_Risk_management_in_SCADA-_system.pdf?sequence=1

Olje- og energidepartementet. (2014). *Et bedre organisert strømnett* (Y-0125 B). Olje- og energidepartementet. https://www.regjeringen.no/globalassets/upload/oed/pdf_filer_2/rapport_et_bedre_organisert_stroemnett.pdf

Olje- og energidepartementet. (2019, mars 1). *Eierskap i kraftsektoren*. Energifakta Norge. https://energifaktanorge.no/om-energisektoren/eierskap-i-kraftsektoren/

Pariés, J. (2011). Resilience and the Ability to Respond. I E. Hollnagel, J. Pariés, D. D. Woods, & J. Wreathall, *Resilience engineering in practice: A guidebook*. Ashgate.

Patriarca, R., Falegnami, A., Costantino, F., Di Gravio, G., De Nicola, A., & Villani, M. L. (2021). WAx: An integrated conceptual framework for the analysis of cyber-socio-technical systems. *Safety Science*, *136*, 105142. https://doi.org/10.1016/j.ssci.2020.105142

Patriarca, R., Simone, F., & Di Gravio, G. (2022). Modelling cyber resilience in a water treatment and distribution system. *Reliability Engineering & System Safety*, *226*, 108653. https://doi.org/10.1016/j.ress.2022.108653

Perrow, C. (2011). Complexity, Coupling and Catastrophe. I *Normal Accidents: Living with high.risk technologies* (s. 62–100). Princeton Univeristy Press.

Pollock, K., & Steen, R. (2021). Total Defence Resilience: Viable or Not During COVID-19? A Comparative Study of Norway and the UK. *Risk, Hazards & Crisis in Public Policy*, *12*(1), 73–109. https://doi.org/10.1002/rhc3.12207

PST. (2023). *Nasjonal trusselvurdering 2023*. Politiets sikkerhetstjeneste. file:///Users/kristine/Downloads/_globalassets_ntv_2023_ntv_2023_nor_web%20(1).pdf

Qu, S. Q., & Dumay, J. (2011). The qualitative research interview. *Qualitative Research in Accounting and Management*, *8*(3), 238–264. https://doi.org/10.1108/11766091111162070

Riksrevisjonen. (2021). *Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen* (Dokument 3:7 (2020-2021); ISBN-978-82-8229-504-8). https://www.riksrevisjonen.no/globalassets/rapporter/no-2020-2021/nves-arbeid-med-ikt-sikkerhet-i-kraftforsyningen.pdf

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, *21*(6), 11–25. https://doi.org/10.1109/37.969131

Ringdal, K. (2018). *Enhet og mangfold: Samfunnsvitenskapelig forskning og kvantitativ metode* (4. utg.). Fagbokforl.

https://www.nb.no/search?q=oaiid:"oai:nb.bibsys.no:999919953189802202"&mediatype=bøker

Rosenthal, U., Charles, M. T., & t'Hart, P. (1989). *Coping with crises. The management of distasters, riots and terrorism*. Charles C. Thomas.

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2019). *Research methods for business students* (Eighth Edition.). Pearson.

Sellevåg, S. R., Brattekås, K., Bruvoll, J. A., Buvarp, P. M. H., Fardal, H., Farsund, B., Fykse, E. M., Gisnås, H., Hellesø-Knutsen, K., Kirkhorn, S., Nystuen, K. O., Olsen, R., & Seehuus, R. A. (2020). *Samfunnssikkerhet mot 2030 – utviklingstrekk* (Nr. 20/00530). FFI.

Shah, A., Ganesan, R., Jajodia, S., & Cam, H. (2018). A methodology to measure and monitor level of operational effectiveness of a CSOC. *International Journal of Information Security*, *17*(2), 121–134. https://doi.org/10.1007/s10207-017-0365-1

Standard Norge. (2019). *Sikkerhet og resiliens—Systemer for kontinuitetsledelse—Krav (ISO 22301:2019) = Security and resilience business continuity management systems requirements (ISO 22301:2019)—Universitetsbiblioteket i Stavanger*. https://bibsys-almaprimo.hosted.exlibrisgroup.com/primo-explore/fulldisplay/BIBSYS_ILS71589279760002201/UBIS

Statkraft. (2023, januar 18). *Vår virksomhet*. https://www.statkraft.com/var-virksomhet/

Statnett. (2018, oktober 19). *Slik fungerer kraftsystemet*. https://www.statnett.no/om-statnett/bli-bedre-kjent-med-statnett/slik-fungerer-kraftsystemet/

Stavland, B., & Bruvoll, J. A. (2019). *Resiliens – hva er det og hvordan kan det integreres i risikostyring?* (Nr. 19/00363). FFI.

Steen, R., Ingvaldsen, G., & Patriarca, R. (2021). Engineering resilience in a prison's performance management system. *Safety Science*, *142*, 105367-. https://doi.org/10.1016/j.ssci.2021.105367

Weiss, R. S. (1994). *Learning from strangers: The art and method of qualitative interview studies*. Free Press.

Westrum, R. (1999). Faint hearts and faint signals—How organizations manage signs of trouble. I *1999 Workshop of the Senter for Human Performance in Complex Systems.* University of Wisconsin.

Woods, D. D. (2011). Resilience and the Ability to Anticipate. I E. Hollnagel, J. Pariés, D. D. Woods, & J. Wreathall, *Resilience Engingeering in Practice: A guidebook*. Ashgate.

Woods, D. D., & Hollnagel, E. (2006). Prologue: Resilience Engineering Concepts. I E. Hollnagel, D. D. Woods, & N. Leveson, *Resilience Engineering: Concepts and Precepts*. Ashgate.

Wreathall, J. (2006). Properties of Resilient Organizations: An Initial View. I E. Hollnagel, D. D. Woods, & N. Leveson (Red.), *Resilience engineering: Concepts and precepts*. Ashgate.

Wreathall, J. (2011). Monitoring—A Critical Ability in Resilience Engineering. I E. Hollnagel, J. Pariés, D. D. Woods, & J. Wreathall, *Resilience Engineering in Practice: A guidebook*. Ashgate.

Aanensen, T. (2022, juni 29). *Tidenes høyeste krafteksport i 2021*. SSB. https://www.ssb.no/energi-og-industri/energi/statistikk/elektrisitet/artikler/tidenes-hoyeste-krafteksport-i-2021

Vedlegg 1: Intervjuguide

Faktaspørsmål:

1. Hva er deres stilling og hva innebærer den?
2. Har dere kurs eller utdanning knyttet til SCADA-systemer eller arbeid med dette?

Introduksjonsspørsmål:

3. Kjenner dere til at dere har kontinuitetsplan for virksomheten?

- *Oppfølgingsspørsmål*: hva tenker dere om F4 fra spørreundersøkelsen?

Overgangsspørsmål:

4. Kan du fortelle oss hvordan koordineringen av driften som er mellom aktørene i forsyningskjeden foregår/ivaretas?

- *Oppfølgingsspørsmål*: Hvordan sikrer dere samsvar mellom hvordan dette gjøres i praksis og hvordan det er beskrevet i planverk, kontrakter, avtaler, regelverk etc.
- *Oppfølgingsspørsmål*: Hvordan vil du si dette påvirker forsyningssikkerheten hos dere?

Kjernespørsmål:

5. Kan dere fortelle om hvordan dere holder dere oppdatert på dagens trusselbilde, og eventuelt hvordan dere tilpasser dere dette?
6. Før SC inntreffer, kan dere fortelle om hvordan dere arbeider med å oppdage cyber-relaterte angrep på SCADA-systemet?
7. Når SC inntreffer, kan dere fortelle hvordan kommunikasjonen foregår internt i egen virksomhet for å unngå misforståelser av roller og ansvar?
8. Når SC inntreffer, kan dere fortelle hvordan kommunikasjonen mellom nett- og produksjon foregår for å opprettholde drift under en hendelse?
9. Etter SC har inntruffet, hvordan deler aktørene erfaringer og lærdommer med hverandre for å kunne forberede seg (bedre) til den neste hendelsen?
    - *Oppfølgingsspørsmål*: Har dere eksempelvis noen debrief/samtale etter slike hendelser?
    - *Oppfølgingsspørsmål*: Hva tror du/dere dette har å si for forsyningssikkerheten?
10. Når SC inntreffer, hvordan sikrer dere forsyning av strøm på tross av utfordringer med SCADA-systemet? Eksempelvis hvis det skulle lamme systemet?

Spørsmål basert på svar på spørreundersøkelsen:

11. Gitt svaret i spørsmål L6 og L7 i undersøkelsen. Hvilke tanker har dere omkring dette? Er det bra nok?

Avslutningsspørsmål:

12. Hvordan jobber dere systematisk for å forbedre opprettholdelse av driften og sikre forsyningen av strøm for fremtidige eventuelle cyberangrep?
13. Hvilke forbedringsområder ser du med tanke på å opprettholde driften og sikre forsyningen av strøm for fremtidige eventuelle cyberangrep?

Vedlegg 2: Forespørsel om å delta i mastersamarbeid

Denne våren skal vi skrive vår masteroppgave i samfunnssikkerhet og i den anledning er vi svært interessert i å komme i kontakt med deres virksomhet. Formålet med oppgaven er å se hvordan resiliens og opprettholdelsen av driftskontinuitet kan benyttes til å forbedre arbeidet med forsyningssikkerhet hos aktører i kraftforsyningen. Dette skal sees nærmere på gjennom et overordnet nivå. Vi ønsker å se nærmere på den overordnede verdikjeden (forsyningskjeden) og samhandlingen de involverte aktørene har (fra produksjon og til sluttbruker). Dermed ønsker vi å komme i kontakt med produksjonsselskaper og nettselskaper, hvor vi metodisk skal inkludere både spørreskjema og intervju. Vi ønsker svar innen syv dager, altså **tirsdag 14/2** på om dette er noe dere kunne tenkt dere. Nærmere avtale gjøres etter dette.

Kort om prosjektet:

Bakgrunnen for valget på denne sektoren baserer seg på at kraftforsyning er en kritisk samfunnsfunksjon. Vi skal spesifikt se på forsyningen av strøm. Videre er forsyningssikkerhet i kraftsektoren et relevant og viktig tema, med tanke på dagens utfordringer. Dette har gjort at det har blitt et større fokus på forsyningssikkerhet og generell sikkerhet rundt kritiske samfunnsfunksjoner. Problemsstillingen til studien er som følger (med forbehold om endringer):

- *Hvordan kan prinsippene for «Resilience Engineering» og opprettholdelsen av driftskontinuitet benyttes til å forbedre forsyningssikkerheten hos aktører i kraftforsyningen?*

Ved hjelp av sentrale teorier innen resiliens og et nyere konsept i norsk sammenheng, driftskontinuitet (fra det engelske business continuity), vil vi utforme spørsmål til en spørreundersøkelse som deres medarbeidere kan velge å ta. Spørsmålene er rangert fra *helt uenig* til *helt enig*. Ut ifra denne spørreundersøkelsen vil vi kartlegge resiliens hos deres virksomhet. Dette vil være utgangpunkt for et intervju med 1-3 medarbeidere. Informantene vil bli sikret anonymitet og det samme gjelder deres virksomhet. Navn og personopplysninger vil ikke registreres noe sted og vil kun være kjent for undertegnede. Masteroppgaven er i samarbeid med Safetec Nordic AS, som er en ledende leverandør av tjenester innen risikostyring og risikobasert beslutningsstøtte.

Kort oppsummert:

Hva kan vi tilby dere?

Resultat fra spørreundersøkelse og intervju med spesifikke tilbakemeldinger. Dette kan hjelpe virksomheten med økt sikkerhet i et fremtidig perspektiv. Resultatene kan tilby innsikt i hvordan virksomheten arbeider med resiliens og driftskontinuitet. Alle involverte virksomheter vil få tilgang til den ferdigstilte masteroppgaven som skal avlegges 15.juni 2023.

Hva trenger vi fra dere?

- Utdeling av elektronisk spørreundersøkelse til ansatte i avdeling som hovedsakelig står for drift/vedlikehold/administrasjon av produksjon/distribusjon. Dette kan avtales nærmere med deres virksomhet angående hvilke(n) avdeling(er) som er relevante og hvilket utvalg som skal motta undersøkelsen. Spørreundersøkelsen antas å ha en varighet på 10-15 minutter. Det er valgfritt å svare. Vi trenger å vite hvor mange som er ansatt i avdelingen(e) som spørreundersøkelsen eventuelt skal gis ut til.
- 1-3 informanter til intervju med overordnede stillinger i de(n) aktuelle avdelingen(e), intervjuet vil antas å ta mellom 30-45 minutter. I enkelte virksomheter kan det være aktuelt å intervjue disse informantene samtidig i form av en workshop/gruppeintervju, med varighet på ca. 1-1,5t. Dette vil avtales nærmere.

Definisjoner:

Resiliens: "Den iboende evnen i et system til å justere sine funksjoner i forkant av, under, eller etter endringer og forstyrrelser, slik at det kan opprettholde nødvendige funksjoner under både forventede og uforventede forhold" (Hollnagel, 2011, s. 275).

Driftskontinuitet: "capability of an organization to continue the delivery of product and services within acceptable time frames at predefined capacity during a disruption" (NS-ISO 22301, s. 2)

Med vennlig hilsen

Kristine Pettersen Kofoed og Carina Karlsen
Studenter, master i samfunnssikkerhet ved Universitetet i Stavanger
Mail: xxxx / xxxx
Tlf. Kristine: xxxxxxxx, Tlf. Carina: xxxxxxxx

Vedlegg 3: Samtykkeerklæring

Vil du delta i forskningsprosjektet

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å se hvordan resiliens og opprettholdelsen av driftskontinuitet kan benyttes til å forbedre arbeidet med forsyningssikkerhet hos aktører i kraftforsyningen. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Vi skal skrive masteroppgave i samfunnssikkerhet. Bakgrunnen for valget på kraftsektoren baserer seg på at kraftforsyning er en kritisk samfunnsfunksjon. Videre er forsyningssikkerhet i kraftsektoren et relevant og viktig tema, med tanke på dagens utfordringer. Dette har gjort at det har blitt et større fokus på forsyningssikkerhet og generell sikkerhet rundt kritiske samfunnsfunksjoner.
Problemsstillingen til studien er som følger:

- Hvordan kan prinsippene for Resilience Engineering og opprettholdelsen av driftskontinuitet benyttes til å forbedre forsyningssikkerheten hos aktører i kraftforsyningen på et systemnivå?

Vi skal gjennom denne problemsstillingen ta for oss en scenarioanalyse relatert til cyberangrep på SCADA-systemene som brukes i kraftforsyningen.

Hvem er ansvarlig for forskningsprosjektet?

Universitetet i Stavanger er ansvarlig for prosjektet.

Videre er det etablert et samarbeid med Safetec Nordic AS.

Hvorfor får du spørsmål om å delta?

Vi er interessert i å innhente informanter fra kraftproduksjon- og nettselskaper. Grunnen til at vi vil ha deg er fordi du arbeider i kraftsektoren.

Hva innebærer det for deg å delta?

Det skal gjennomføres et gruppeintervju på 60-90 min, som består av relevante spørsmål tilknyttet vår problemsstilling. Intervjuene vil bli tatt opp av lydopptak og transkriberes. Dette vil slettes etter endt mastergrad.

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket

tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg. Dette vil heller ikke påvirke ditt forhold til arbeidsplassen din.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket. Det er bare forfatterne av masteroppgaven som skal ha tilgang til personlige opplysninger under skriveprosessen, ingen eksterne aktører vil få tilgang til dette. Navnet på vedkommende kommer til å bli erstattet med en kode, eksempelvis «person A fra bedrift C». Videre blir det transkriberte materialet sikret bak passord. Alt skal anonymiseres og bedriftene kommer ikke til å bli gjenkjent på noen som helst måte.

Hva skjer med personopplysningene dine når forskningsprosjektet avsluttes?

Prosjektet vil etter planen avsluttes innen 15. juni 2023. Etter prosjektslutt vil det datamaterialet slettes, inkludert lydopptak og transkribert materialet.

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Universitetet i Stavanger har Sikt – Kunnskapssektorens tjenesteleverandør vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter

Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:

- Universitetet i Stavanger, Kristine Kofoed (tlf: xxxx, mail: xxxx) og Carina Karlsen (tlf: xxxx, mail: xxxx). Veileder Riana Steen (tlf: xxxx, mail: xxxx)

- Vårt personvernombud: Rolf Jegervatn (mail: personvernombud@uis.no)

Hvis du har spørsmål knyttet til vurderingen som er gjort av personverntjenestene fra Sikt, kan du ta kontakt via:

- Epost: personverntjenester@sikt.no eller telefon: 73 98 40 40.

Med vennlig hilsen

Riana Steen (Forsker/veileder)

Kristine Kofoed og Carina Karlsen (studenter)

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *Resiliens i driftskontinuitet*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

☐ å delta i gruppeintervju

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

---

(Signert av prosjektdeltaker, dato)

Vedlegg 4: Godkjenning fra Sikt

Prosjekttittel
Resiliens i driftskontinuitet

Behandlingsansvarlig institusjon
Universitetet i Stavanger / Det teknisk- naturvitenskapelige fakultet / Institutt for sikkerheit, økonomi og planlegging

Prosjektansvarlig
Riana Steen

Student
Kristine Kofoed

Prosjektperiode
01.02.2023 - 15.06.2023

Kategorier personopplysninger
Alminnelige

Lovlig grunnlag
Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Behandlingen av personopplysningene er lovlig så fremt den gjennomføres som oppgitt i meldeskjemaet. Det lovlige grunnlaget gjelder til 15.06.2023.

Meldeskjema

Kommentar
Vår vurdering er at den planlagte behandlingen i dette prosjektet er lovlig, hvis den gjennomføres slik den er beskrevet i meldeskjemaet med dialog og vedlegg og vurderingen her.

OM VURDERINGEN
Sikt har en avtale med institusjonen du forsker eller studerer ved. Denne avtalen innebærer at vi skal gi deg råd slik at behandlingen av personopplysninger i prosjektet ditt er lovlig etter personvernregelverket.

FØLG DIN INSTITUSJONS RETNINGSLINJER
Vi har vurdert at du har lovlig grunnlag til å behandle personopplysningene, men husk at det er institusjonen du er ansatt/student ved som avgjør hvilke databehandlere du kan bruke og hvordan du må lagre og sikre data i ditt prosjekt. Husk å bruke leverandører som din institusjon har avtale med (for eksempel ved skylagring, nettspørreskjema, videosamtale eller liknende).

Personverntjenester legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32).

MELD VESENTLIGE ENDRINGER
Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til oss ved å oppdatere meldeskjemaet. Se våre nettsider om hvilke endringer du må melde: https://sikt.no/melde-endringar-i-meldeskjema

OPPFØLGING AV PROSJEKTET
Vi vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til med prosjektet!