# Informasjonssikkerhet i kraftforsyningen

**Marie Røyksund**


**UNIVERSITETET I STAVANGER**
**Masteroppgave 2011**

**MASTERGRADSSTUDIUM I**

**SAMFUNNSSIKKERHET**

**MASTEROPPGAVE**

**SEMESTER:**

**Vårsemester 2011**

---

**FORFATTER:**

**Marie Røyksund**

**VEILEDER:**

**Ole Andreas Engen og Ruth Ø. Skotnes**

---

**TITTEL PÅ MASTEROPPGAVE:**

***Informasjonssikkerhet i kraftforsyningen***

---

**EMNEORD/STIKKORD: Kraftforsyningen, Driftskontrollsystem, Cyberkriminalitet, ROS-analyser, Risikopersepsjon, Kollektiv sensemaking**

---

**SIDETALL: 89 (inkludert litteraturliste og vedlegg)**

**STAVANGER, 15. juni 2011** **…….**

# Forord

Med denne oppgaven markeres slutten på to kjekke og lærerrike år av masterstudiet i samfunnssikkerhet.

Ved Universitetet i Stavanger (UiS) foregår det for tiden et doktorgradsarbeid, av Ruth Østgaard Skotnes, som omhandler ”risiko og sårbarhet ved bruk av IKT i kraftforsyningen”. I forbindelse med dette prosjektet, var det ønskelig at noen undersøkte hvordan kraftselskapene selv oppfatter trusselen om dataangrep. Jeg synes dette virket som en spennende utfordring, og ble svært glad da jeg ble gitt anledning til å bidra. Arbeidet har vært interessant, nyttig og krevende. Jeg har dessuten lært mye om norsk kraftforsyning, og har stor respekt for den jobben som blir utført i denne sektoren. Inntrykket

Jeg vil særskilt takke de ti informantene som velvillig delte av sin tid og kompetanse. Uten deres bidrag, hadde ikke denne oppgaven vært mulig å gjennomføre. I tillegg må det nevnes at den absolutt triveligste delen av prosjektet, var å besøke de ulike virksomhetene.

Videre vil jeg rette en stor takk til mine veiledere, Ole Andreas Engen og doktorstipendiat Ruth Ø. Skotnes, for alle råd og konstruktive tilbakemeldinger som dere har gitt i denne perioden. Det har til tider vært en frustrerende prosess, og da har det vært godt å få med noen oppmuntrende ord på veien.

De siste tre månedene har jeg fritt disponert et kontor hos Elektro Comfort AS. Tusen takk til Tor Gunnar Frafjord for gjestfriheten! Jeg vil også takke min far, Karstein Dragsund, som har stått for den omfattende korrekturlesingen.

Mine kjære medstudenter (dere vet hvem dere er); hjertelig takk for et fabelaktig godt samarbeid gjennom hele studiet.

Til sist, men ikke minst, vil jeg rette en ekstra stor oppmerksomhet til min mann og to barn, som tålmodig har talt ned dagene til at mamma skal bli ferdig på skolen…

Marie Røyksund

Stavanger, 15. juni 2011

# Sammendrag

**Bakgrunn:** I de siste tiårene har det skjedd et radikalt teknologisk skifte i samfunnet. Kraftforsyningen er således intet unntak. Mens det tidligere var de ansatte som overvåket og betjente kraftstasjonene, fjernstyres anleggene i dag av komplekse IKT-systemer. Denne utviklingen har imidlertid utvidet trusselbildet, ved at eventuelle "angrep kan gjennomføres når som helst, mot hvem som helst og fra hvor som helst" [13]. Faktum er at norske virksomheter og samfunnskritiske funksjoner, stadig oftere utsettes for kriminelle handlinger via de logiske kanalene [43]. Samtidig rapporteres det fra flere hold at informasjonssikkerheten er sviktende i mange bedrifter [45 og 46].

**Formål:** Hensikten med dette studiet har vært å få innblikk i hvordan kraftforsyningen opplever og håndterer cybertrusselen, hvilket utgjorde følgende problemstilling:

> ***Hvordan oppfatter kraftbransjen risikoen for angrep på driftskontrollsystemene, og hvilke faktorer kan ha betydning for valg av informasjonssikkerhetstiltak?***

**Metode:** For å svare på problemstillingen, er det valgt et eksplorativt forskningsdesign. Det er gjennomført seks dybdeintervjuer med aktører fra nettselskapene, samt et intervju med to representanter fra NVE.

**Resultat:** Informasjonssikkerhet har i økende grad fått oppmerksomhet i kraftsektoren, mye p.g.a. at tilsynsmyndighetene har større fokus på denne sikkerhetsutfordringen. Kraftbransjen har dessuten dannet et sikkerhetsforum på eget initiativ, hvor spørsmål relatert til informasjonssikkerhet behandles.

Kraftsektoren domineres av to yrkesdisipliner; IT og Elkraft. Empirien indikerer at de respektive fagtradisjonene har en ulik tilnærming til informasjonssikkerhet. Respondenter med IT-faglig bakgrunn rangerte bl.a. effekten av bevisstgjørende tiltak betydelig høyere enn de med Elkraft-faglig bakgrunn. Sistnevnte uttrykte derimot større tiltro til de teknologiske barrierene.

**Konklusjon:** Kraftbransjen oppfatter det som lite sannsynlig at driftskontrollsystemet vil bli utsatt for målrettede dataangrep. Valg av informasjonssikkerhetstiltak foretas på bakgrunn av de ROS-analysene som foreligger, samt myndighetskrav og interne retningslinjer. I tillegg vil det aktuelle trusselbildet enkelte ganger være avgjørende for hvorvidt et tiltak blir iverksatt eller ikke. Bransjen etterlyser i den forbindelse mer effektive varslingsrutiner fra myndighetene. Det anbefales derfor at gjeldende praksis blir gjennomgått og vurdert – fortrinnsvis i samarbeid med kraftselskapene.

# Innholdsfortegnelse

## Appendiks I - V

# 1 Innledning

## 1.1 Problembeskrivelse

Sommeren 2010 ble det for første gang oppdaget en utspekulert og avansert dataorm[1] (Stuxnet) som hadde til hensikt å sabotere og ødelegge samfunnskritiske mål. Stuxnet var skreddersydd for å angripe de styrings- og kontrollsystemene som benyttes bl.a. i norsk kraftforsyning og i oljesektoren. Eksperter har uttalt at Stuxnet demonstrerte muligheten som finnes til å *skape* noe som kan føre til skade på liv og helse [18 og 23]. En omfattende undersøkelse utført av McAfee [18], bekrefter at Stuxnet angrep et stort antall datamaskiner verden over. Av 200 respondenter fordelt på 14 land, svarte 40 % at de oppdaget Stuxnet-viruset i sine datasystemer. Iran ble spesielt hardt rammet av denne ormen, og president Ahmedinejad innrømmet i desember i fjor at landets atominnstallasjoner var påvirket [14]. Nasjonal sikkerhetsmyndighet (NSM) rapporterte i forbindelse med Stuxnet om målrettete angrep mot interne prosess- og styringssystemer også her til lands, deriblant kraftforsyningen [18].

Det levnes liten tvil om at cyberkriminalitet[2] er en aktuell problemstilling i vår tidsalder. I rapporten ”eNorge - Nasjonal strategi for informasjonssikkerhet” påpekes det at IKT[3]-utviklingen har utvidet risikobildet i samfunnet ved at eventuelle ”angrep kan gjennomføres når som helst, mot hvem som helst og fra hvor som helst” [13]. I dette utsagnet ligger det en erkjennelse av at trusselbildet også har endret seg ved at man ikke lenger vet hvem *trusselaktørene* er og hvilke *motiver* som ligger bak et angrep. Tidligere forbandt man dataangrep med mindre alvorlige handlinger som ble utført av ”script-kiddies” og ”amatør hackere” (jf. Appendix I). Dette er imidlertid ikke lenger en realitet. Storbritannias statsminister, David Cameron, rangerer

1 Ormer er en ondsinnet kode som er i stand til å spre seg via nettverket, og gjerne uten brukerinteraksjon. (jfr. Appendiks I)

2 Med cyberkriminalitet forstås ”kriminelle handlinger som er rettet mot data og datasystemer, samt kriminalitet hvor datautstyr benyttes som verktøy for å begå mer tradisjonell kriminalitet” [15].

3 Informasjon – og kommunikasjonsteknologi

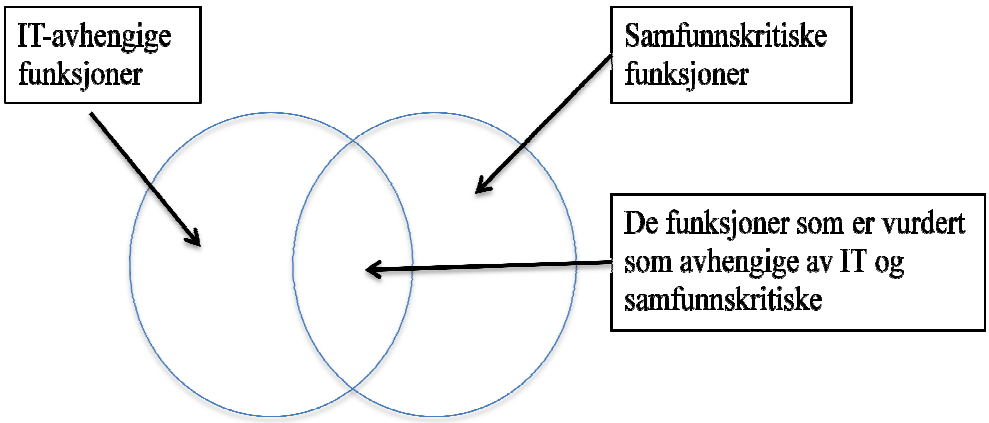
cyberkriminalitet som den mest alvorlige trusselen mot nasjonen, nest etter terrorisme [44]. Omfanget av politiske og økonomiske motiverte angrep på IT-systemene øker, og handlingene blir i større grad utført av svært kompetente "hackere" eller fagspesialister som tilbyr tjenester til organiserte (og gjerne kriminelle) grupperinger. Teknikkene og virkemidlene blir dessuten stadig mer avanserte og sofistikerte [14]. Mange har spekulert i hvem som er ansvarlige for Stuxnet-angrepet, mye pga at "ormen" var så målrettet og kompleks av natur. USA og Israel har blant andre blitt anklaget for å stå bak ugjerningen [45]. Realiteten er at stadig flere nasjoner utvikler cyberkrigføring som militær strategi, deriblant Kina og Russland [45]. Fremmede nasjoner er altså å regne som mulige trusselaktører når det gjelder bruken av datateknologiske virkemidler [14 og 22]. Politiets sikkerhetstjeneste (PST) har uttalt at "det er mer etterretningsvirksomhet mot Norge i dag enn det var under den kalde krigen" [40]. Senest i mai dette året ble Forsvaret utsatt for et massivt, målrettet dataangrep [41]. Flere hundre utvalgte personer mottok den samme e-posten hvor avsenderen tilsynelatende var et norsk direktorat, hvilket ikke var tilfelle. I vedlegget skjulte det seg et datavirus som hadde til hensikt å tappe Forsvarets PCer for informasjon. Denne gangen lyktes de med å stanse angrepet. Trenden er imidlertid klar: norske virksomheter og samfunnskritiske funksjoner blir stadig oftere utsatt for kriminelle handlinger via IT-systemene. Dette bildet bekreftes av Nasjonal sikkerhetsmyndighet[4] (NSM) som har ansvar for håndteringen av alvorlige dataangrep mot samfunnskritisk infrastruktur [43].

> Kritisk infrastruktur innebærer "de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse" [34].

Elektrisk kraft er en av grunnpilarene i det moderne samfunnet, og avhengigheten av en stabil strømforsyning er stor. For det første har den gjennomsnittelige nordmann et høyt forbruk av elektrisitet [12] For det andre er de ulike samfunnssektorene gjensidig avhengige av hverandre [17]. Det innebærer at selv en kortvarig svikt i

4 Nasjonal sikkerhetsmyndighet (NSM) har oversikten over sikkerhetssituasjonen i samfunnskritisk infrastruktur. Hvert år utgir de en rapport med oppdatert IKT- trussel/sårbarhetsbilde.

strømforsyningen kan få store konsekvenser for flere samfunnsfunksjoner, f.eks. telekommunikasjon og finans [12]. De senere år har norsk kraftforsyning i økende grad tatt i bruk komplekse IT-systemer for å overvåke og fjernstyre anleggene (jfr. pkt. 1.4.2). I 2000 foretok Nærings- og Handelsdepartementet [39] en rangering av viktige samfunnsfunksjoner som i tillegg er avhengige av IT Kraftforsyningen var en av de samfunnssektorene som ble vurdert å befinne seg i fellesområdet mellom de to sirklene som vist under:




Figur 1Forholdet mellom samfunnskritiske og IT-avhengige funksjoner [39]

I den samme rapporten ble det konkludert med at ”angrep utenfra er mulig fordi en i dagens kraftforsyning har behov for å knytte sine egne IT-systemer og nettverk sammen med andre aktørers IT-systemer” [39]. Det medfører dermed en mer utstrakt bruk av åpne nettverk. Selv om det er mulig å foreta sikring av en tilknytning mot f eks Internett, gjør den åpne teknologien dette komplisert og vanskelig. Man blir ofte nødt til å inngå kompromisser mellom funksjonalitet og sikkerhet. Det finnes i dag få relevante krav til aktørene som sikrer et adekvat sikkerhetsnivå” [39].

## 1.2 Problemformulering

Forrige avsnitt stadfester at cyberkriminalitet er en realitet. Spørsmålet er hvordan norske bedrifter forholder seg til denne trusselen. Av NSM sin årsrapport for 2010 blir det forebyggende sikkerhetsarbeidet vurdert som utilstrekkelig [46]. Skadelige programvarer (jf. Appendiks I) som angriper prosesskontrollsystemene, forventes å være en av de største sikkerhetsutfordringene det moderne samfunnet står overfor i fremtiden, men det virker som om virksomhetene ikke tar innover seg dette ansvaret. Mye av skylden tillegges manglende ledelsesengasjement og dårlige varslingsrutiner når uønskede hendelser først inntreffer. Resultatene fra Mørketallsundersøkelsen 2010[5] [46] bekrefter funnene i NSM sin rapport: ”sikkerheten er sviktende hos mange” [45]. Virksomhetene blir stadig mer avhengige av IT, men følger ikke opp med sikringstiltak. Mørketallsundersøkelsen 2010 påpeker er at IKT- kompetansen må økes, og da særlig gjelder det for virksomhetsledere.

Med tanke på at ”gapet mellom truslene og sikkerhetstiltakene øker” [46], er det interessant å betrakte hvordan norske bedrifter faktisk opplever trusselen om cyberkriminalitet. Med bakgrunn i at nevnte rapporter har avdekket at det er mangler i forhold til sikringstiltak, kan det derfor være hensiktsmessig å se nærmere på hvilke faktorer som spiller inn når det gjelder valg av sikkerhet. Problemstillingen blir som følger:

***Hvordan oppfatter kraftbransjen risikoen for et angrep på driftskontrollsystemene, og hvilke faktorer kan ha betydning for valg av informasjonssikkerhetstiltak?***

Det er flere grunner til at kraftforsyningen er en interessant aktør å undersøke i denne sammenheng. For det første er det morderne samfunnet svært avhengig av en stabil strømforsyning. For det andre har kraftsektoren vært gjennom en dyptgripende

5 Mørketallsundersøkelsen 2010 er den 7. undersøkelsen som foretas av Næringslivets Sikkerhetsråd (NSR) gjennom Datakrimutvalget. Mørketallsundersøkelsen har en sentral plass i opplysnings- og informasjonsstrategien mot næringslivet og offentlige myndigheter.

teknologisk endring de siste 10-20 årene. Hvor medarbeidere tidligere styrte hvert enkelt anlegg, er det nå prosesstyringssystemer som overvåker og fjernstyrer driften. Kraftbransjen har alltid vært preget av sikkerhetsutfordringer, men sårbarheten har imidlertid blitt ytterligere forsterket ved innføringen av ”ny teknologi, deregulering og strukturell endring i næringen” [22]. Det er derfor interessant å se hvorvidt bransjen har greid å tilpasse seg til de ”nye” sårbarhetene og sikkerhetsutfordringene. Et siste argument er ved å betrakte kraftsektoren, vil studiet være av relevans for et doktorgradsarbeid som for tiden foregår ved Universitet i Stavanger (UiS) under tittelen: *"Risiko og sårbarhet ved bruk av IKT i norsk kraftforsyning”*. Jeg synes det virket som en spennende utfordring da jeg ble forespeilet muligheten for å bidra i dette arbeidet.

## 1.3 Omfang og begrensinger

### 1.3.1 Informasjonssikkerhet

Denne oppgaven er begrenset til å omhandle informasjonssikkerhet i kraftforsyningens drifts- og styringssystemer. Etter beredskapsforskriften § 6-4 gjelder det ”driftssentraler, sambandsanlegg og øvrige anlegg og komponenter som ivaretar driftskontrollfunksjoner” [3]. I fortsettelsen vil disse bli omtalt som driftskontroll-systemer eller SCADA-systemer.

Informasjonssikkerhet i kraftforsyningen omfatter tiltak som ivaretar [4]:

- **Konfidensialitet**: sensitiv informasjon skal kun være tilgjengelig for rettmessig bruker, utstyr eller prosess
- **Integritet**: informasjon er korrekt og pålitelig. Den kan ikke manipuleres
- **Tilgjengelighet**: informasjon og ressurs er tilgjengelig og anvendelig til enhver tid

Informasjonssikkerhet innbefatter all form for informasjon, uavhengig av informasjonsbærer - det være seg opplysninger på papir, samtaler, fotografering og IKT-system etc. Tiltak som skal ivareta informasjonssikkerheten, kan deles inn i organisatoriske og teknologiske tiltak. Disse vil bli behandlet inngående under pkt 2.2.3.

I årene fremover vil kraftsektoren oppleve en formidabel utvikling når det gjelder bruken av it-baserte løsninger. Regjeringen har gått inn for at det skal innføres AMS (avanserte måle- og styresystemer) i kraftforsyningen innen utgangen av 2016, i et forsøk på å stimulere til energisparing og for at kundene skal bli mer bevisste på strømforbruk [11]. Det knyttes mange utfordringer til dette prosjektet, deriblant sikkerhet. Denne oppgaven forholder seg i hovedsak til den gjeldende ikt-strukturen, men utfordringer ved AMS vil så vidt bli berørt i empiri – og diskusjonsdelen.

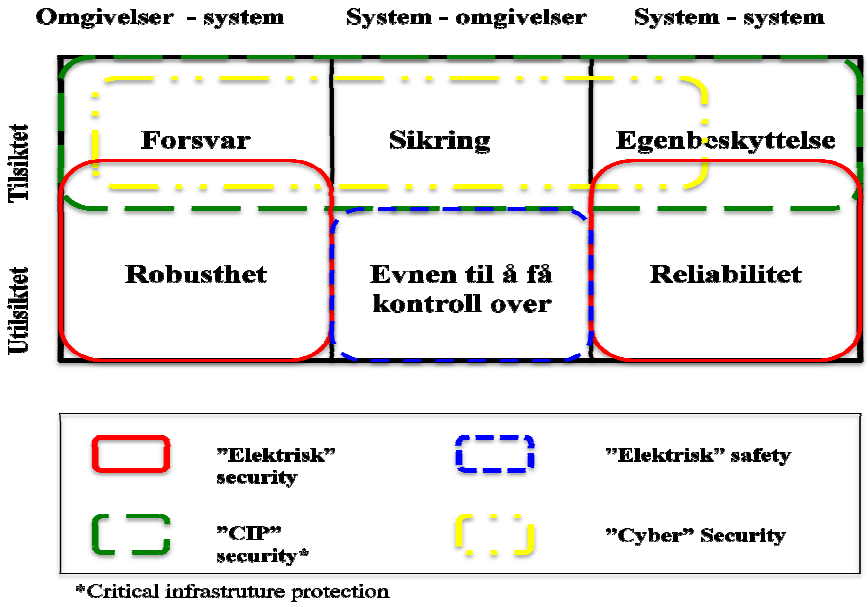
### 1.3.2 Safety vs. security

Når man omtaler sikkerhet, er det vanlig å skille mellom *safety* og *security*. Safety har av enkelte fagmiljø blitt brukt for å beskrive vern mot utilsiktede hendelser, mens security innebærer tiltak og beskyttelse mot villede (ondsinnede) hendelser [5]. Flere har argumentert for at et risikobasert IKT-sikkerhetsarbeid bør inkludere både safety og security- tilnærmingene [5]. Ved kun å betrakte security-relaterte hendelser, står man i fare for å fremstille et feilaktig risikobilde. Dette skyldes at IKT-systemet vil reagere på samme måte, enten det er en tilsiktet eller utilsiktet handling som har utløst feilen. Piètre-Cambacédès og Chaudet [25] har utviklet et rammeverk, SEMA, som ivaretar både safety og security- aspektet. De skiller mellom:

- System (S) vs. omgivelser (E): hvor security innebærer de risikoene som stammer fra omgivelsene og som kan påvirke systemet, mens safety omfatter de risikoen som kan oppstå fra systemet og påvirke omgivelsene
- Ondsinnet (M) vs ulykke (A): her viser security til de ondsinnede (tilsiktet) handlingene, mens safety adresserer kun ulykker (utilsiktet).

I denne forbindelse henviser *systemet* til det ”objektet” som skal studeres, f.eks kraftforsyningen. *Omgivelsene* innbefatter alle de andre systemer som berører ”objektet”, hvis atferd og karakteristikker er mindre kjent og utenfor ”objekteiers” kontroll, det være seg eksempelvis telekommunikasjon og datanettverk. Piètre-Cambacédès og Chaudet [25] har videre foretatt en vurdering av kraftsektoren ved hjelp av SEMA-rammeverket, med utgangspunkt i at denne sektoren består av *”highly technical systems that evolve rapidly and involve diverse security and safety challenges”*. Ifølge dem er safety - begrepet konsekvent benyttet for å beskrive forebygging av tilfeldig skade på menneske og miljø. ”Elektrisk” safety henspeiler på

kraftselskapets evne til å gjenopprette strømforsyningen dersom den skulle falle ut. De øvrige kategoriseringene viser på ulike måter til security-aspektet.




Figur 2 Security og safety i kraftforsyningen. Kilde: Pietre-Cambacedes & Chaudet [25]

Piètre-Cambacédès og Chaudet [25] sier at security-begrepet ut fra et elektroingeniørperspektiv (”Elektrisk” security), forstås som evnen til å takle forstyrrelser slik at kunden ikke blir skadelidende. Som fig. 2 illustrerer, omfatter denne forståelsen i hovedsak utilsiktede hendelser, som f.eks. oversvømmelse eller brann. Tilsiktede hendelser er inkludert, om enn i liten grad. Her kan man forestille seg at Piètre-Cambacédès og Chaudet har tenkt på mulig sabotasje på den fysiske infrastrukturen. De senere års terroranslag, og da spesielt med tanke på 11.september, har aktualisert tilsiktede hendelser mot kraftforsyningen. Av den grunn er security-begrepet utvidet, og omfatter her både ”CIP”- og ”cyber”-security.

### 1.3.3 Tilsiktede vs. utilsiktede hendelser

Litteraturen skiller mellom tilsiktede og utilsiktede handlinger når det kommer til uønskede hendelser [1 og 2]. I et IKT-system oppstår det imidlertid som oftest uønskede hendelser som skyldes menneskelig svikt, fysisk svikt eller miljø/naturhendelser, hvilket kommer inn under betegnelsen ”utilsiktede handlinger” [5]. Ikke-tilsiktede hendelser kan også forårsake store konsekvenser [6].

I dette studiet forstås tilsiktede handlinger som ”angrep eller manipulasjon på IKT-system og tilhørende infrastruktur” [6]. Et angrep mot kraftforsyningens driftskontrollsystem er en villet handling, hvor en eller flere aktivt går inn for å skade, enten det er ”utro tjenere”, amatørhackere, organiserte hacker-grupper eller fremmede nasjoner [14].

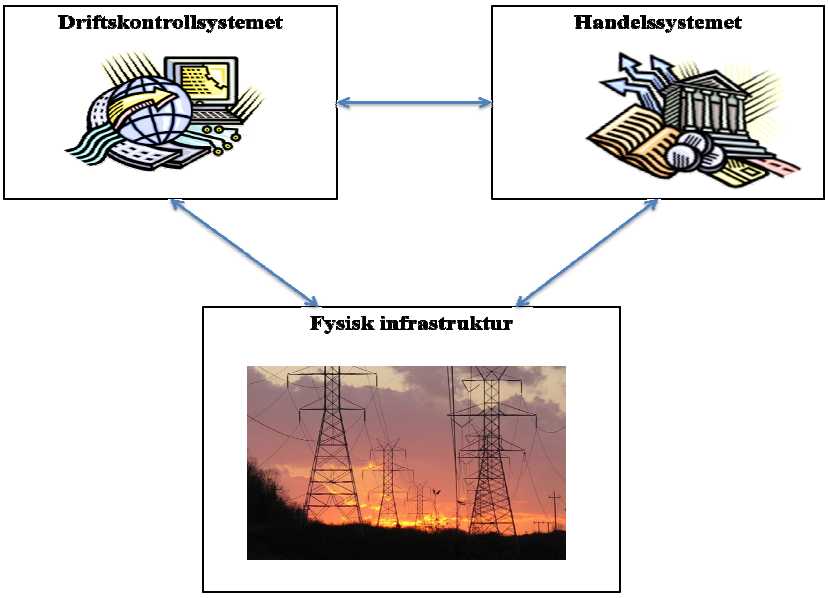
Begrepet *”angrep mot IKT-systemer”* kan forstås på forskjellige måter. En intuitiv tolkning vil muligens være at det dreier seg om et målrettet forsøk på å skade et IT-system. Imidlertid omfatter nesten all statistikk også mer tilfeldige angrep, som f.eks. selvspredende eller automatisk spredende programvare. At tilfeldige og tilsiktede angrep kommer innunder samme kategori, gjør at denne type informasjon nærmest vanskeliggjør arbeidet med å avdekke målrettete angrep mot en virksomhet [5].

## 1.4 Presentasjon av norsk kraftforsyning

Produksjon av elektrisk kraft er i Norge nærmest synonymt med vannkraft. Vannkraftverkene står for om lag 99 % av den innenlandske energiproduksjonen [34]. Spesielt for norsk kraftforsyning er at produksjonsstrukturen er svært desentralisert, hvor da også mottakerne/brukerne befinner seg i et spredt geografisk område [12]. Denne situasjonen har resultert i en omfattende *infrastruktur* (kraftnett) bestående av flere lokale distribusjonsnett, regionalnett og et sentralnett[6]. I egenskap av å være et landsdekkende transportnett, kan sentralnettet karakteriseres som kritisk infrastruktur [34]. *Drifts- og styringssystemer* sørger for en effektiv og sikker overføring og fordeling av elektrisk kraft fra produksjonssentrene til sluttbrukerne. *Handelssystemet* omfatter kjøp og salg av elektrisk kraft, og det er dessuten avhengig av en intakt infrastruktur og en tett kobling til drifts- og styringssystemet.

6 Pr. 2008 eide Staten 87 % av sentralnettet. Kommuner og fylkeskommuner eier det meste av regional- og de lokale distribusjonsnettene. Statens eierskap til sentralnettet forvaltes gjennom Statnett SF, som også er systemansvarlig for kraftforsyningen i Norge. Alle de store driftssentralene har rapporteringsplikt til Statnett sin Landssentral.

Norsk kraftforsyning kan illustreres på følgende måte:

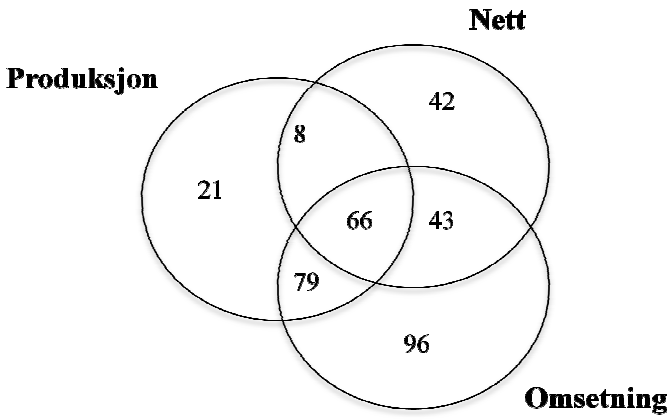



Figur 3 Modell av norsk kraftforsyning, basert på sluttrapporten etter BAS3-prosjektet [12]

Norsk kraftforsyning er et "just-in-time system" [6, 12 og 34]. Det innebærer at det til enhver tid skal være samsvar mellom produksjon og forbruk, noe som krever rask kommunikasjon og informasjonsutveksling mellom flere aktører. Tidligere var det ansatte som styrte den aktuelle installasjonen manuelt på alle kraftforsyningsanleggene, men de senere års teknologiske utvikling har ført til at anleggene nå fjernstyres via et fåtall driftssentraler. Dette gjøres ved hjelp av komplekse IKT-systemer og kommunikasjonssamband. Sistnevnte eies delvis av kraftsektoren selv, men selskapene leier også tjenester fra det offentlige telemarkedet.

### 1.4.1 Myndigheter og regulering

Kraftsektoren blir først og fremst regulert gjennom Energiloven og Vassdragsloven med tilhørende forskrifter og retningslinjer. Konsesjonspraksisen er rådende. Alle som leverer og omsetter elektrisk energi, må eksempelvis ha omsetningskonsesjon [34 og 35], det være seg produksjons-, nett-, eller omsetningsselskaper. Pr. 2008 var det totalt 355 virksomheter som hadde fått omsetningskonsesjon i Norge, med følgende fordeling:



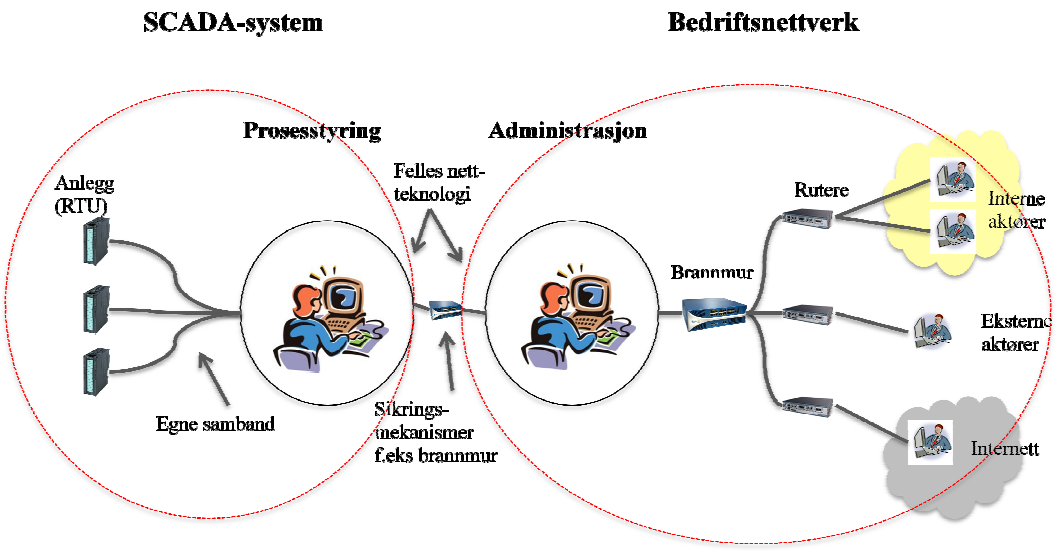

Figur 4 Omsetningskonsesjonærer etter virksomhet. Per 1. januar 2008 [35]

Norges vassdrags- og energidirektorat (NVE) og Direktoratet for samfunnssikkerhet og beredskap (DBS) har fått tildelt et felles ansvar for norsk kraftforsyning [38]. NVE fører tilsyn med nettselskapene i forhold til økonomi, forsyningssikkerhet og beredskap. Her innbefattes krav til leveringskvaliteten og i hvorvidt virksomhetene har tilstrekkelig beredskapsrutiner og ressurser til å ivareta forsyningen under ekstraordinære situasjoner, jf. BfK § 1-1. DSB sitt ansvarsområde omfatter hovedsakelig elsikkerhet og tilsyn av selskapene i forhold til kraftsystemet og komponentenes fysiske og tekniske tilstand. ”Elektriske anlegg skal utføres, drives og vedlikeholdes slik at de ikke frembyr fare for liv, helse og materielle verder” [38].

### 1.4.2 Sårbarhet i kraftforsyningens driftskontrollsystemer

De fleste større aktørene i norsk kraftforsyning opererer med en todeling av sine lokale datanettverk, jfr. fig. 5. Driftssentralens datanettverk består av et prosesstyringsnett (SCADA-system[7]) og et administrativt datanett [12]. Prosesstyringsnettet inneholder datamaskiner og utstyr som er lokalisert i driftssentralen, og via et nettverk koblet opp mot de ulike understasjonene (RTU). Det administrative datanettet (lokalnettet) består av datamaskiner i nettverk med eventuelle eksterne aktører (inkl. internett).

7 Supervisory Control and Data Aquisition (SCADA) system er et databasert prosesskontrollsystem som overvåker og fjernstyrer de tilhørende hjelpesystemer (anleggene, RTU) [37].




Figur 5 Prinsippskisse, SCADA-system vs. Administrativt nettverk [36]

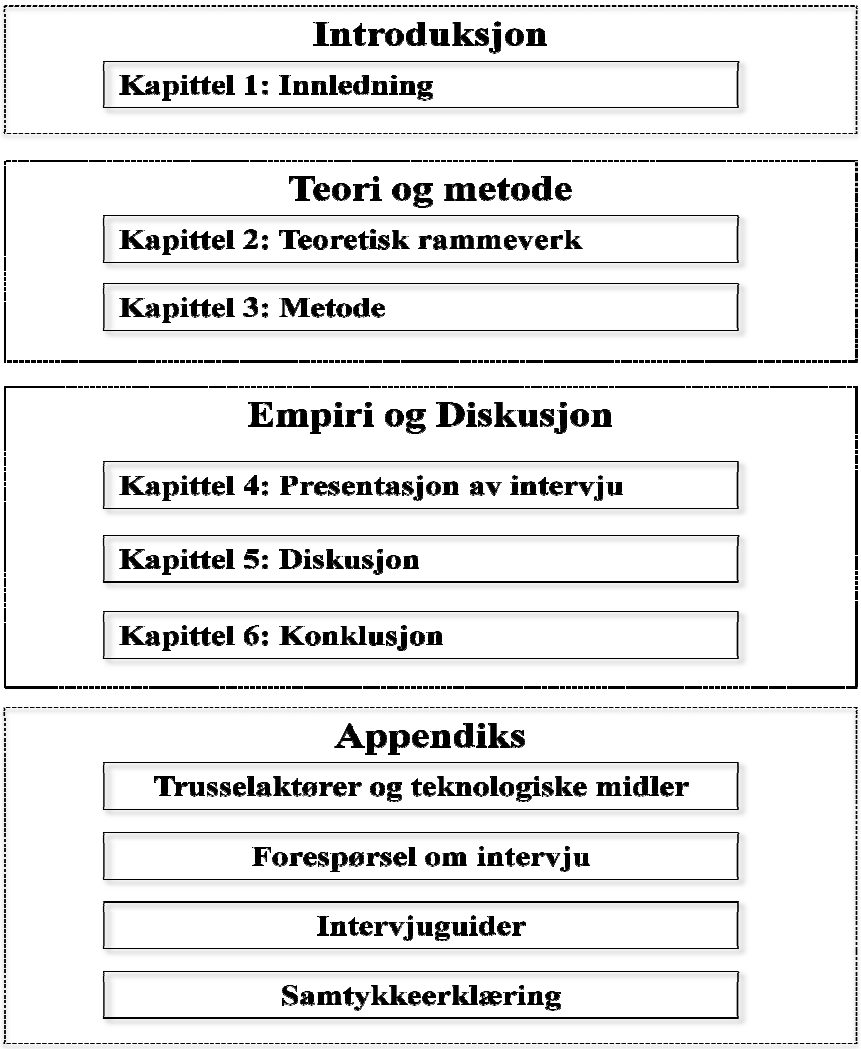
SCADA-systemet fjernstyrer og overvåker ulike prosesser i kraftproduksjonen og nettdriften via dataformidling eller telefoni. Fra driftssentralen hvor "hovedmaskinen" (MTU) er plassert, foregår alle prosessene (kontroll, overvåking og styring) ut mot RTUene som er spredt over et stort geografisk område [37]. Det finnes et alternativ dersom driftskontrollsystemet (SCADA-systmet) svikter. Det er nemlig fullt mulig å overta styringen manuelt i hvert enkelt anlegg, og kommunikasjonen foregår da via telefon eller faks. Det betyr at hvis noen ønsker å oppnå stans i strømforsyningen, krever det vanligvis at vedkommende gjør skade både mot IKT-systemene og den fysiske kraftinfrastrukturen [17].

Prosesstyringsnettet og det administrative datanettet var i utgangspunktet helt separate systemer. SCADA-systemet var således også utviklet som et isolert system med properitær programvare og designet med tanke på å sikre en maksimalisert og stabil strømforsyning [36]. Den teknologiske utviklingen, sammen med kravet om effektivisering og økt funksjonalitet, har imidlertid ført til at SCADA-systemet kobles opp mot administrasjonssystemet via brannmurer. I prinsippet er det kun den administrative delen som skal være tilgjengelig opp mot eventuelle eksterne aktører, men denne koblingen har åpnet muligheten for ekstern tilgang også (bl.a. Internett) til driftssentralen. Utfordringen er at SCADA-systemet i utgangspunktet ikke er utformet med nødvendige sikkerhetsbarrierer. Den fysiske forbindelsen mellom nettverkene øker dermed sårbarheten for logiske angrep (hacking) utenfra, hvilket gjør det mulig for

trusselaktører å utnytte sårbarhetene i systemet [14]. I tillegg har man mindre oversikt over hvem som har tilgang til ulike tjenester internt i virksomheten, hvilket også øker sårbarheten for utro tjenere [36]. Nasjonal sikkerhetsmyndighet (NSM) påpeker at "den kritiske naturen til disse systemene gjør at teknisk personell ikke tør eller ønsker å oppdatere systemene for å tette sårbarheter" [14].

Forsvarets forskningsinstitutt (FFI) har sammen med en rekke andre aktører innenfor sivil beredskap og samfunnssikkerhet, gjennomført studier som inngår i BAS-serien, "Beskyttelse av samfunnet". Kraftforsyningen ble i denne prosjektserien fremhevet med egne studier for å avdekke mulige sårbarheter knyttet til drifts- og styringssystem så vel som fysisk infrastruktur [17]. Det fremkommer av sluttrapportene at "kraftforsyningen *er* sårbar både overfor fysiske påkjenninger og angrep mot sine informasjonssystemer" [12]. FFI har videre bemerket at den økende IKT-avhengigheten i kraftforsyningen medfører en økt sannsynlighet for at dataangrep kan utføres for å skade kraftforsyningens systemer i fremtiden [12 og 17]. NSM har konkludert med tilsvarende: "fra virksomhetenes ståsted fungerer systemene, men fra et nasjonalt ståsted utgjør de en potensiell trussel for terrorslag i overskuelig fremtid" [14].

## 1.5 Oppgavens disposisjon



# Teori og Metode

# 2 Teoretisk rammeverk

Ved hjelp av et utvalg teoretiske bidrag, skal dette studiet forsøke å gi svar på hvordan kraftbransjen oppfatter trusselen om angrep på driftskontrollsystemet. Litteratur om risiko- og sårbarhetsangrepet, samt risikopersepsjon kan således være av relevans for problemstillingen. Målet er deretter å få innblikk i hvilke faktorer som kan være av betydning for valg av informasjonssikkerhetstiltak. Utfordringen er å finne ut hvordan en organisasjon kan komme frem til en felles forståelse av risiko, noe som igjen leder til beslutning om tiltak. Begrepet *kollektiv sensemaking* vil være en sentral bidragsyter for å forklare dette, og man kommer heller ikke utenom litteratur som omtaler risikostyring og risikoanalyser. I tillegg vil ulike informasjonssikkerhetstiltak bli gjort rede for i teorikapittelet. Det finnes helt sikkert andre teoretiske tilnærminger som kunne ha medvirket i denne sammenheng. Det forutsettes likevel at det følgende bidraget vil være tilstrekkelig for å belyse dette studiets problemstilling.

## 2.1 Risiko – og sårbarhetsbegrepet

Ulike fagområder og miljøer kan ha avvikende forståelse av risikobegrepet [1]. Før man kan betrakte hvordan kraftbransjen oppfatter trusselen om et angrep på driftskontrollsystemene, må det derfor avklares hvilket perspektiv på risiko som legges til grunn. I det følgende vil ulike tilnærminger til risiko bli presentert. Videre vil begrepene sårbarhet – og robusthet bli gjort rede for.

### 2.1.1 Risiko

I et forsøk på å betrakte mulige konsekvenser av den fremtidige utviklingen og endringen samfunnet står overfor, blir risikobegrepet benyttet som en analysetilnærming [47]. Det finnes imidlertid mange ulike tilnærminger og definisjoner av risiko. I litteraturen finner man risiko beskrevet som *forventet verdi, sannsynlighetsfordeling,*

*som usikkerhet og som en hendelse.* Aven og Renn [47] har gjennomgått de vanligste definisjonene og kommet frem til følgende to hovedkategorier:

1. Risiko uttrykkes ved hjelp av sannsynligheter og forventingsverdier.
2. Risiko uttrykkes gjennom hendelser/ konsekvenser og usikkerheter.

Den såkalte *tradisjonelle tilnærmingen* henviser til kategori én, og denne har vært fremtredende når risiko omtales [47]. Utfordringen er imidlertid at det i de aller fleste tilfellene er umulig å predikere med sikkerhet hvilket utfall en gitt aktivitet medfører. Risiko handler om fremtiden, og den er ofte ukjent [1]. Løsningen blir at usikkerheten uttrykkes som en sannsynlighet, gjerne ut fra en ”objektiv”, statistisk størrelse. For å komme frem til denne utarbeides estimater basert på tidlige hendelser (historiske data). Det tradisjonelle perspektivet erkjenner likevel at mulige fremtidige uønskede hendelser mange ganger er forbundet med usikkerhet - og særlig dersom det ikke finnes gode nok data [1]. Usikkerheter kan da kalkuleres ut ifra subjektive sannsynligheter eller forventningsverdier [2] . Kritikken mot den tradisjonelle tilnærmingen er at man kan gå glipp av viktige aspekter som er nødvendige for å forstå risikoen av en gitt aktivitet. Særlig gjelder det hvordan usikkerhetsfaktoren behandles [1]. Argumentet er at det ikke finnes en reell, objektiv størrelse, men at det er mer hensiktsmessig å betrakte sannsynlighetene på en alternativ måte, hvilket kan oppnås bl.a. ved å vektlegge ekspertuttalelser når sannsynligheter skal fastsettes. Det alternativet synet på risiko viser til kategori 2 i Aven og Renn sin inndeling [47]. Innholdet i den alternative tilnærmingen kan oppsummeres på følgende måte [8]:

Sett at vi har en hendelse (A), hvor (A) er et vellykket angrep på kraftforsyningens IKT-systemer. (C) innebærer strømstans og er konsekvensene av hendelse (A). Imidlertid vet vi ikke om hendelsen vil inntreffe eller ikke, og hva som blir de faktiske konsekvensene dersom et vellykket angrep på IKT-systemet skulle skje. Det er altså en usikkerhet knyttet til både (A) og (C). Hvor sannsynlig det er at hendelse (A) vil inntreffe og at (C) blir konsekvensene, kan uttrykkes ved hjelp av en sannsynlighet (P). Sistnevnte fastsettes ved hjelp av vår bakgrunnskunnskap (K), og den innbefatter historiske tall, erfaringer og kompetanse/ekspertise.

Til forskjell fra det tradisjonelle synet på risiko, åpnes det altså opp for en videre forståelse av hvordan man kan vurdere usikkerheten ved hjelp av ulike metoder [2]. Ekspertuttalelser blir i det alternative perspektivet en sentral del av risikovurderingen, men i tillegg åpnes det opp for at andre interessenters meninger og opplevelser i enkelte tilfeller bør tas i betraktning [1]. Det er det alternativet synet på risiko som gjør seg gjeldende i denne oppgaven.

### 2.1.2 Sårbarhet og Robusthet

Sårbarhetsutvalget [10] har definert sårbarhet som *"et uttrykk for de problemer et system vil få med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet"*. Systemet kan for eksempel være en stat, den nasjonale kraftforsyningen, en bedrift eller et enkeltstående datasystem. Sårbarhet er i stor grad selvforskyldt. Det går nemlig an å påvirke sårbarheten, begrense og redusere den.

Aven, Wiencke & Røed [8] definerer begrepet sårbarhet på følgende måte:

> Med sårbarheten av et system mener vi kombinasjonen av mulige konsekvenser og usikkerhet, gitt at systemet utsettes for en initierende hendelse.

En initierende hendelse kan være en *trussel, fare og mulighet* [2]. I denne oppgaven vil imidlertid kun tilsiktede hendelser mot kraftforsyningens driftskontrollsystem betraktes. Sårbarhet uttrykkes enkelte ganger som sannsynligheten for at en ønsket funksjon, f.eks. strømforsyningen, svikter gitt en initierende hendelse (f.eks virus).

Robusthet er det motsatte av sårbarhet [8]. Det innebærer at dersom et system omtales som robust, er systemets sårbarhet tilsvarende lav.

## 2.2 Risikostyring

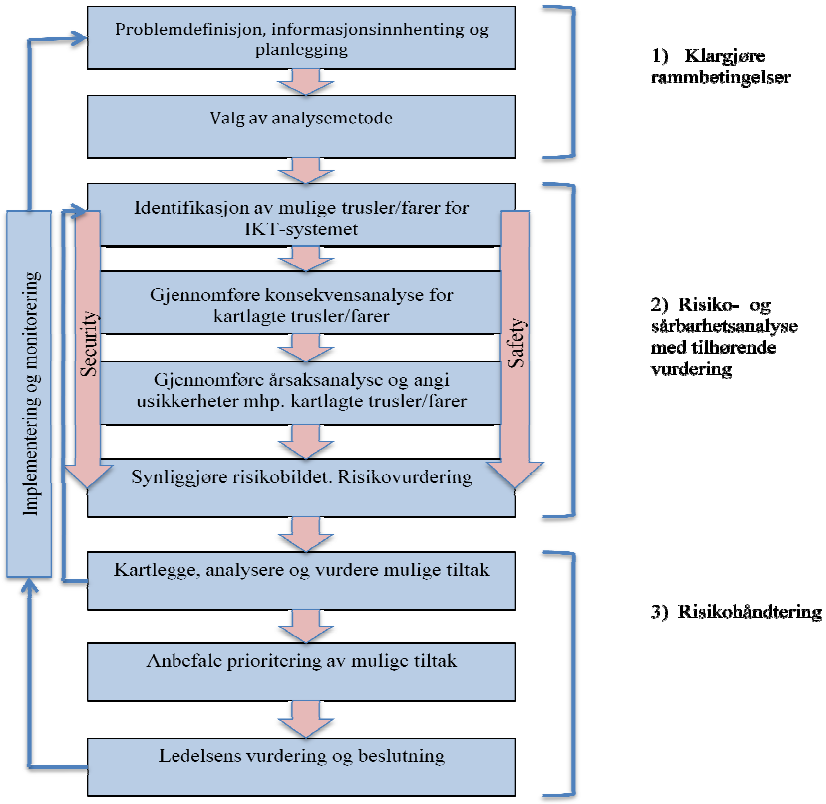
Med risikostyring forstås ”alle aktiviteter og tiltak som gjøres for å styre risiko” [2].

De fleste virksomheter praktiserer en eller annen form for risikostyring. Denne aktiviteten er lovfestet bl.a. i internkontrollforskriften (IK) §2 og §5, hvor virksomhetene pålegges å kartlegge farer og vurdere risiko, samt utarbeide tilhørende risikoreduserende tiltak [19]. For kraftforsyningen forsterkes kravet om risikostyring ytterligere i beredskapsforskriften (BfK) § 1-3 [3]. Forskriften retter særlig fokus på ekstraordinære hendelser som potensielt kan få ”konsekvenser for produksjon, overføring og fordeling av elektrisk kraft”, jmf. BfK § 1-1, herunder trusselen om sabotasje og andre tilsiktede og ondsinnede handlinger. Beredskapsforskriften legger videre opp til at kraftselskapene fortløpende skal foreta risiko- og sårbarhetsvurderinger av driftskontrollsystemene, med tanke på forbygging av uønskede hendelser samt for å planlegge beredskapen slik at gjenoppretting av forsyningen skal skje raskt ved et evtentuelt bortfall. Beredskapsforskriften (BfK) §1-3 stiller krav til at alle KBO-enheter[8] skal ha *”oppdaterte risiko- og sårbarhetsanalyser for å identifisere virksomhetens risikopotensiale og de tiltak som effektivt oppfyller kravene i denne forskriften”* [3]. Det innebærer også at enhetene skal foreta løpende helhetlige vurderinger av informasjonssikkerheten, jf. BfK §6-1. NVE (Norges Vassdrags- og energidirektorat) utgav i 2010 en oppdatert veiledning til hvordan virksomhetene kan gjennomføre risiko- og sårbarhetsanalyser.

Forskningsprosjektet ”Sårbarhet i kritiske IKT-systemer” (BAS 5) har utviklet en metodikk for risikoanalyse av samfunnskritiske IKT-systemer [5]. Rapporten som ble utgitt i etterkant, tar blant annet for seg hvilke utfordringer analysegruppen står overfor når et IKT-system skal risikovurderes. Først og fremst kreves det god oversikt og

8 KBO er en forkortelse for Kraftforsyningens Beredskapsorganisasjon, bestående av NVE og alle enheter som eier eller driver kraftproduksjon med tilhørende vassdragsregulering, overføring og distribusjon av elektrisk kraft og fjernvarme.

kunnskap om det systemet som skal analyseres, det være seg kompetanse om funksjonene systemet skal utføre, komponentene som inngår, programvaren som benyttes og hvilke sikkerhetsmekanismer som tas i bruk [5]. I tillegg må en ha kunnskap om hvilke sårbarheter som finnes i systemet, samt hvilke tilsiktede eller utilsiktede trusler det kan utsettes for. Prosjektet foreslo at følgende risikostyringsprosess danner grunnlaget for risikoanalyser av IKT-system:




Figur 6 Risikostyringsprosesssom presentert i BAS 5-prosjektet [6]

Spesielt for denne risikostyringsprosessen er at den inkluderer både safety - og security-aspektet, jfr. fig.6. Ifølge sluttrapporten til BAS5-prosjektet har det vært en økende interesse for å inkludere tilsiktede handlinger i risikoanalysene [6]. Tilsiktede hendelser er imidlertid et vanskelig tema å behandle i en slik prosess [5]. Det skyldes blant annet at eventuelle trusselaktører og deres intensjoner er ukjent for analysegruppen, og av den grunn er det vanskelig å danne seg en mening om sannsynlighet.

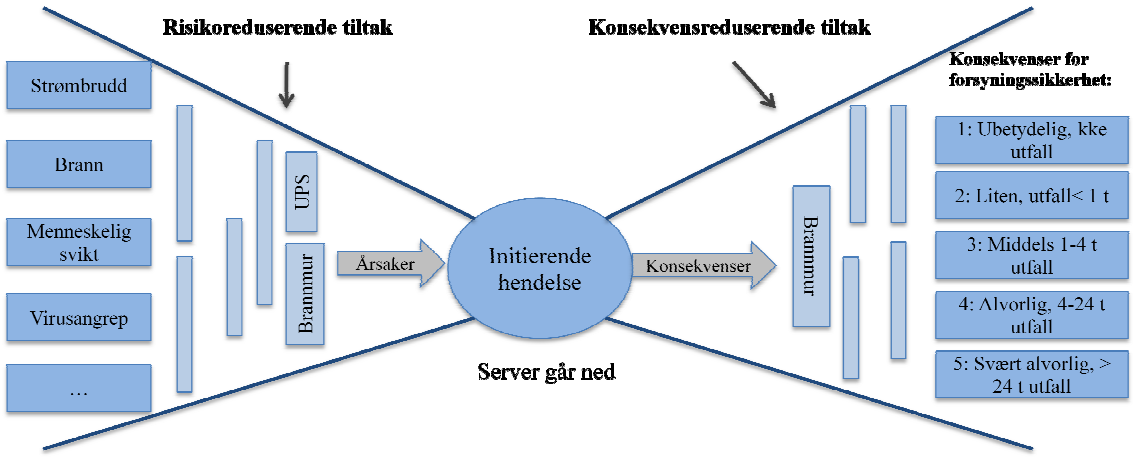
Risikostyringsprosessen er delt inn i tre kategorier:

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

Når det gjelder planlegging, innebærer det bl.a. å definere hva som er hensikten med analysen. Deretter er det viktig å beslutte hvilket nivå konsekvensene av en uønsket hendelse skal måles mot. Her skiller BAS 5 mellom konsekvenser sett mot IKT-systemet, virksomheten eller samfunnet [6]. I tillegg er det nødvendig å avklare rammebetingelser som ligger til grunn, det være seg begrensinger i forhold til budsjett, tid, tilgang til informasjon osv. [6]. Da risikohåndtering, risikoanalyser og beskrivelse av informasjonssikkerhetstiltak anses som mest relevant i forhold til problemstillingen, vil ikke planleggingsfasen behandles ytterligere i denne sammenheng.

### 2.2.1 Risiko – og sårbarhetsanalyser

En risiko- og sårbarhetsanalyse, heretter kalt ROS-analyse, handler i første omgang om å kartlegge hvilke hendelser som kan skje for deretter å vurdere risiko og sårbarhet av de identifiserte hendelsene [1 og 2]. Det er ikke noe i veien for at en risikoanalyse kan avdekke muligheter, altså positive hendelser, men i forhold til problemstillingen er det mest aktuelt å omtale de negative hendelsene, dvs. farer og trusler. Målet med analysen er å gjøre systemet mer robust mot ulike hendelser [5]. I mange sammenhenger benyttes et såkalt bow-tie diagram for å illustrere hva som inngår i en ROS-analyse. Som fig. 7 viser, er det ikke nødvendigvis gitt hva som er årsaken til at den initierende hendelsen inntreffer.




Figur 7 Bow-tie for uønsket hendelse

Det kan være flere grunner til at eksempelvis driftskontrollsystemet svikter. På den venstre siden viser mulige årsaker med tilhørende barrierer (forebyggende tiltak). Dersom det finnes gode barrierer, kan man generelt si at sårbarheten er liten [2]. Godheten til en barriere måes ved å vurdere sannsynligheten for at den svikter, da med tanke på funksjonalitet og pålitelighet. Et eksempel er å betrakte brannmuren som skal sikre driftskontrollsystemet mot angrep. Hvor effektiv er denne når den fungerer som tiltenkt, og hvor sannsynlig er det for at den svikter i en gitt situasjon? På den høyre siden i diagrammet fremgår mulige skadereduserende tiltak som har til hensikt å hindre at det oppstår alvorlige konsekvenser av en uønsket hendelse [4].

ROS-analyser gir en ”systematisk identifisering og kategorisering av risiko og sårbarhet” [1]. For beslutningstakere vil en slik gjennomgang danne et bilde av risikoen ved en gitt aktivitet eller et system, og sådan være et godt verktøy for å kunne fatte ”riktige” beslutninger hva sikkerhet angår.

### 2.2.2 Andre metoder for analyse av IKT-system

Både i sluttrapporten til BAS 5 [6] og i veilederen til NVE [9] benyttes i hovedsak risikoanalyser som metode for å betrakte IKT-systemene, men det finnes også en rekke andre metodikker som bidrar til å ivareta informasjonssikkerheten. Hvorvidt kraftselskapene benytter andre metoder for å vurdere risiko og sårbarheten ved driftskontrollsystemet, vites ikke. Det vil således være interessant å betrakte i hvilken grad de benytter andre metodikker enn den generelle tilnærmingen NVE representerer. Herunder følger en kort innføring i noen av disse.

- Risikoanalyser spesielt utviklet for IKT: Utgangspunktet for disse er at de skal ta hensyn til informasjonssikkerheten, og inkluderer internasjonale standarder. Et eksempel er CORAS-metodikken[9].
- Sjekklister: er et godt hjelpemiddel for å sikre at flere forhold ved informasjons-sikkerhet er tatt vare på. Spesifiserer tiltak, men gjerne ikke i prioritert rekkefølge [5]. Kan dessuten være et nyttig supplement når hendelser skal kartlegges og vurderes.
- Internasjonale standarder og ”beste praksis”: består av forholdsvis omfattende

9 CORAS var et EU-finansiert forskningsprosjekt hvor bl.a. SINTEF og Telenor medvirket.

sjekklister. Ifølge Kalberg [5] er ISO 17799 et styringsrammeverk for IKT-sikkerhet, den mest brukte standarden. ITIL[10] er et prosedyrebasert rammerverk som skal ivareta generell IKT-drift. Denne tar utgangspunkt i en helhetlig sikkerhetstenking som inkluderer både safety og security-aspektet.

- Penetrasjonstesting: tar sikte på å avdekke mulige sårbarheter i et gitt system ved hjelp av en aktiv kartlegging av de enkelte delene i systemet. Ulempen med denne metodikken er at den bare gir negative svar, dvs. sårbarhetene avsløres og kan dermed rettes opp, men man vet ikke hvor mange tilsvarende sårbarheter som finnes. Den gir heller ikke svar på hvordan man kan unngå dem i fremtiden.

### 2.2.3 Risikohåndtering

Neste steg i en risikostyringsprosess (jfr. fig. 2.1.) er å kartlegge og vurdere mulige skadereduserende – og konsekvensreduserende tiltak basert på sårbarhetene som ble avdekket i analysen. I tillegg vil eksisterende sikkerhetsmål, kriterier og krav være retningsgivende for de beslutningene som tas, vedrørende sikkerhet i virksomheten. I beredskapsforskriften stilles det i hovedsak funksjonelle krav til KBO-enhetene [4], hvilket innebærer at myndighetene gjennom lovverket formulerer målsettinger som virksomhetene skal etterleve [20]. Generelt kan man si at målene uttrykker et sikkerhetsnivå som ønskes oppnådd på kort eller lang sikt, det være seg fra samfunnet eller virksomheten selv [1]. Man skiller gjerne mellom ideelle mål (ingen angrep på IKT-systemet) og skadeforebyggende mål (et vellykket angrep på IKT-systemet skal ikke resultere i strømutfall). Mål kan også utformes med hensyn til beredskap, hvilket er tilfellet for kraftselskapene i henhold til BfK §1-1. Kravet som settes her, er at kraftselskapene skal *"optimalisere forebygging og håndtering av alle ekstraordinære hendelser som kan skade eller hindre produksjon, overføring og fordeling av elektrisk kraft"* [3, 4]. Det er opp til hver enkelt KBO-enhet å komme frem til hvordan dette målet skal oppnås. NVE anbefaler imidlertid at virksomhetene utarbeider risikoakseptkriterier [4 og 9], hvilket er å regne som en øvre grense for risiko eksempelvis ift mennesker, miljø og økonomiske verdier. Dersom risikoen vurderes til å falle innenfor "rød sone" i risikomatrisen, er tiltak påkrevd.

10 Information Technology Infrastructure Library (ITIL)

Ifølge Aven [2] foregår det for tiden en debatt i Norge vedrørende bruken av risikoakseptkriterier. Det argumenteres for at dette er en for mekanisk måte å håndtere risiko på. Når det skal foretas beslutninger om hvilke tiltak som skal gjennomføres, mener Aven at det også må tas hensyn til andre forhold som økonomi, hva som er praktisk å få til og hvordan risikoen oppleves for de involverte. I tillegg er det problematisk dersom det blir for mye fokus på å oppnå kriteriet fremfor å rette oppmerksomheten mot forhold som faktisk er viktige for sikkerheten [2]. Det finnes imidlertid en annen måte å vurdere om risikoreduserende tiltak skal iverksettes eller ikke. ALARP (As Low As Reasonably Practicable) innebærer at risikoen skal reduseres så langt det er praktisk mulig [1]. Ifølge Aven, Røed og Wiencke [8] innebærer ALARP-prinsippet en ”omvendt bevisbyrde”, dvs. risikoreduserende tiltak skal gjennomføres, med mindre det er et dokumentert misforhold mellom nytte og kostnader/ulemper.

### 2.2.4 Informasjonssikkerhetstiltak

Det finnes flere typer tiltak som kan benyttes for å oppnå økt robusthet og sikkerhet i IKT-system. I denne oppgaven har jeg valgt å kategorisere informasjonssikkerhetstiltakene etter Hagen, Albrechtsen. [7] sin rapport. Det skilles mellom organisatoriske og teknologiske tiltak, hvorav førstnevnte ytterligere er inndelt i fire grupperinger (pkt 1-4). Teknologiske tiltak fremkommer under pkt 5 som vist på neste side:

1. *Overordnet sikkerhetspolicy*
2. *Metoder og verktøy:* risikoanalyser, rapportering, krav fra myndigheter, interne revisjoner, beredskapsplaner, interne krav
3. *Prosedyrer og kontroll:* retningslinjer for individuell atferd, taushetserklæringer, disiplinære konsekvenser og krav til outsourcing av it-tjenester
4. *Bevissthetsgjørende (awareness) tiltak:* Holdningsskapende kampanjer, opplæring, brukermedvirkning og engasjement fra ledelse.
5. *Teknologiske tiltak*: passord, redundans av kritiske system, anti-virus program, brannmurer, monitorering o.l.

Hagen et al. [7] sin rapport avdekker at norske bedrifter hovedsakelig benytter teknisk-administrative informasjonssikkerhetstiltak som sikkerhetspolicy, prosedyrer og metoder, foruten teknologiske tiltak. Bevisstgjørende tiltak er i mye mindre grad anvendt, selv om denne tiltaksgruppen paradoksalt nok oppfattes som et mer effektivt virkemiddel. Nytteverdien ved å fokusere på eksempelvis brukermedvirkning er stor, fordi den vil kunne forbedre brukervennligheten og funksjonaliteten ved teknologiske informasjonssikkerhetstiltak. I tillegg poengteres det at et slikt tiltak sannsynligvis vil øke den enkeltes bevisstgjøring, motivasjon og forståelse for informasjonssikkerhet, samtidig som det vil forbedre beslutningssituasjonene. Det er likevel en balansegang mellom hvor mye informasjon om systemet den enkelte medarbeider skal få tilgang til ift. need-to – know prinsippet.

## 2.3 Risikopersepsjon

Hensikten med denne rapporten er å forsøke å danne et bilde av hvordan kraftbransjen *oppfatter* risikoen for angrep på driftskontrollsystemene. Tar selskapene trusselen på alvor, eller har de en holdning som tilsier at ”dette er noe som ikke angår oss”? Folk har ofte svært ulik opplevelse og håndtering av risiko og fare. Denne forestillingen om risiko betegnes som *risikopersepsjon* [16] og handler om hvilket perspektiv og bilde man har konstruert av en gitt aktivitet. Risikopersepsjonsforskningen har sitt utspring i kognitiv psykologi [28], men flere andre fagmiljøer har vært opptatt av å studere årsaker til at folk finner en aktivitet som risikofylt eller ikke [1]. Man har gjennom forskning kommet frem til at risikopersepsjon er et resultat av både psykologiske, sosiale og kulturelle faktorer [16]. I dette ligger det en antakelse om at risiko oppfattes ulikt alt etter personlige egenskaper, erfaringer og kunnskap som legges til grunn. I det forestående vil det gis en kort innføring i ulike elementer som påvirker risikopersepsjonen, og som således er relevant for å kunne diskutere kraftbransjens oppfattelse av trusselen om cyberkriminalitet.

Renn [16] skiller mellom *risiko-relaterte mønstre* og *situasjons-relaterte mønstre* hva persepsjon angår. Risiko-relaterte mønstre handler i hovedsak om oppfattet frykt i forhold til konsekvensene av en aktivitet. Folk flest er f.eks. mer redd for å fly enn å kjøre bil, da man vurderer at en potensiell flyulykke alltid vil ha et fatalt utfall, selv om det er statistisk større sannsynlighet for at en bilulykke skal inntreffe. Situasjons-

relaterte mønstre inkluderer aspekter som graden av ”frivillighet” og muligheten for å ha kontroll over aktiviteten [16]. Dersom folk opplever at de kan kontrollere risikoen, er det større sjanse for at de oppfatter den som mindre alvorlig. Den samme effekten oppstår dersom en risikoaktivitet vurderes å kunne gi fordeler/gevinster. I slike tilfeller er man mer tolerante for risikoen, særlig dersom man opplever at aktiviteten er noenlunde frivillig [28].

Forskning viser at menneskelig atferd først og fremst kommer av persepsjon og ikke av den faktakunnskapen som eksempelvis produseres av risikoanalytikere og forskere [16]. Hvordan ”folk flest” vurderer risiko skiller seg ofte fra ekspertenes vurdering [29], som f.eks. i tilfellet ”frykten” for å benytte flytransport fremfor å kjøre bil. Det er mange grunner til at ”lekfolk”og eksperter har ulik risikoforståelse. Sjøberg og Drottz-Sjøberg [29] har bl.a. funnet at *realisme* kan være en forklaring, dvs. at lekfolk er misinformert og at det er ekspertene som er best i stand til å foreta realistiske risikovurderinger. Samtidig er ekspertene vanligvis mer opptatt av sannsynligheter, mens publikum fokuserer mest på konsekvensene av en aktivitet [28 og 29]. En tredje forklaring på forskjellene mellom ekspert og lekfolk er at førstnevnte som regel befinner seg nærmere ”farekilden”, og at de dermed har en større opplevelse av kontroll enn sistnevnte gruppe.

Andre forhold påvirker også den risikooppfatningen hver enkelt har av en gitt situasjon. Media spiller n sentral rolle når det gjelder å informere befolkningen om risikorelaterte forhold [16]. Faktisk utvikler mange holdninger til risikoutsatte aktiviteter og situasjoner, basert på annenhånds-informasjon presentert i media. Journalister samler inn informasjon fra primærkilder, foretar gjerne egne tolkninger basert på erfaring og kunnskap, får så å videreføre informasjonen til mottakerne som igjen foretar fortolkninger. Hvilken innflytelse har så risikopersepsjon? Litteraturen fremhever betydningen av at beslutningstakere tar innover seg ”hvordan folk sosialt og kulturelt skaper sin egen virkelighetsforståelse” [1] når de vedtar hvorvidt en risikoutsatt aktivitet skal gjennomføres eller ikke, samt når risikoreduserende tiltak utvikles og implementeres [16]. Et studie som er gjennomført av Slovic et. al [28], viser at jo høyere en aktivitet scorer på ”fryktfaktoren”, dess høyere er oppfattet risiko og jo mer ønsker folk risikoreduserende tiltak og offentlig reguleringer knyttet til aktiviteten.

Fig. 8 illustrerer noen av de faktorene som påvirker risikopersepsjon.


Figur 8 Faktorer som kan ha innvirkning på risikopersepsjon

Med utgangspunkt i teorier om risikopersepsjon, er det nå mulig å diskutere hvilke mekanismer som ligger til grunn for enkeltpersoners oppfattelse og håndtering av risiko og fare. Det er imidlertid ikke tilstrekkelig til å kunne betrakte hvordan kraftselskapene eller beslutningstakerne kommer frem til en felles forståelse av trusselen om tilsiktede angrep på driftskontrollsystemene. Begrepet *kollektiv sensemaking* står sentralt i forhold til dette spørsmålet, og dette behandles ytterligere i det kommende delkapittelet.

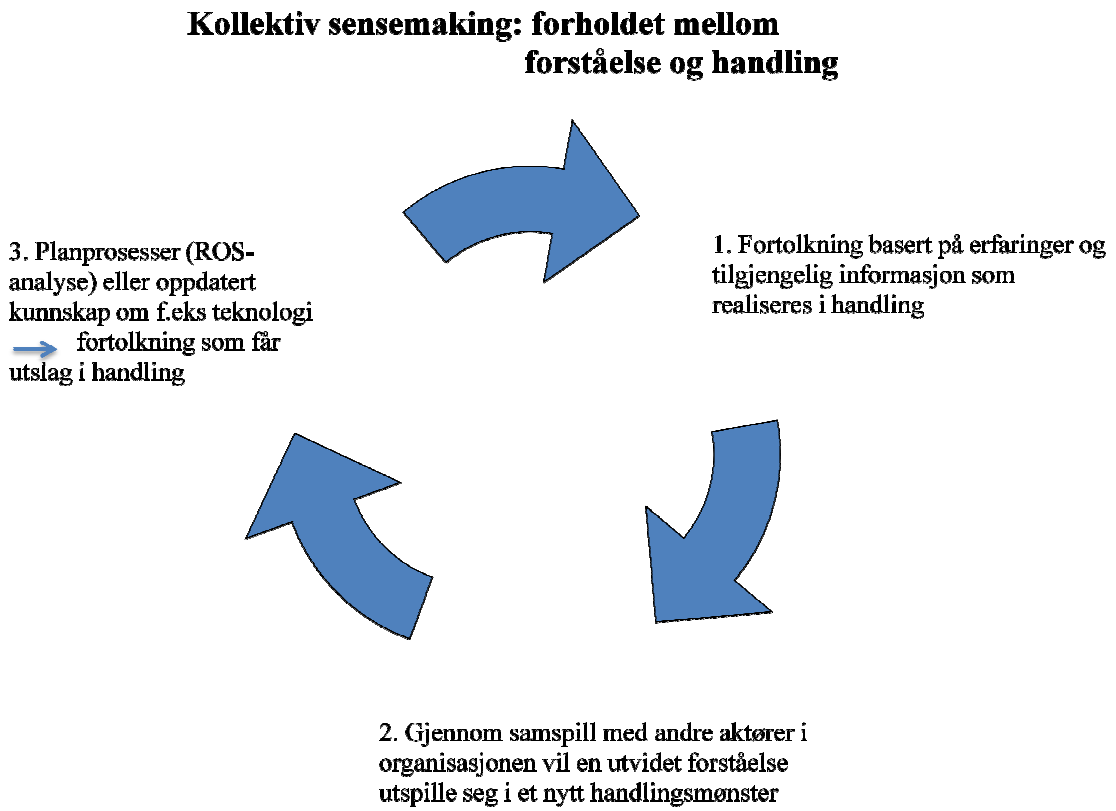
## 2.4 Kollektiv sensemaking

Sensemaking er et sentralt fenomen i enhver organisasjon. Den har noe udefinerbart ved seg og er en sosial, dynamisk og fortløpende prosess [26]. I hovedtrekk handler sensemaking om at aktørene velger bestemte handlingsmønster basert på den meningen de danner seg [24]. Det legges ikke nødvendigvis vekt på at informasjonen er ”sann”, bare den er troverdig og sannsynlig for de involverte. Weick og Sutcliffe [26] påpeker at sensemaking handler om den pågående retrospektive utviklingen av ”rimelige” forestillinger som forklarer folks atferd. Det betyr at de erfaringene man har gjort seg i tidligere sammenhenger, påvirker valg av handlingsmønster i nåtid. Sagt på en annen

måte innebærer sensemaking fortolkning av noe som har skjedd i fortiden og som materialiseres videre i handling.

I en gruppe eller en organisasjon vil det være felles forståelsesprosesser, kollektiv sensemaking, som leder til samkjørte handlinger [24]. Dannelsen av konsensus vedrørende en gitt aktivitet kommer av en dialogbasert interaksjon mellom aktørene [26], hvilket innebærer at man gjennom å kommunisere med andre kan justere en eksisterende oppfatning. Når det gjelder å vurdere all informasjon og alle handlingsalternativene som angår en gitt situasjon, kommer mennesket (og organisasjonen) til kort. Denne begrensingen som ligger i menneskets natur, fører til at virkeligheten forenkles ved hjelp av at man organiserer og kategoriserer den informasjonen som er tilgjengelig på gjeldende tidspunkt. ”Slike fortolkninger kan betraktes som forsøk på å gjøre omgivelsene forståelige og slik sett muliggjøre handling” [24].

En risikostyringsprosess er et eksempel på en arena hvor kollektiv sensemaking utspilles, og grunnlaget for handling eller valg av tiltak legges. De ulike aktørene har ofte egne fortolkninger basert på den kompetansen og erfaringsbakgrunnen de besitter. Ved å dele kompetansen med de andre involverte, vil gruppen gjennom språket danne en ny mening. Den felles forståelsen som kommer ut av en slik prosess, vil kunne være sentral for hvordan organisasjonen utvikles med hensyn til oppfatning av sikkerhetsmål, arbeidsoppgaver, fordeling av ressurser osv. Med dette som utgangspunkt, er det rimelig å anta at dersom organisasjonens oppfattelse av oppgavebetingelser og fordeling av ressurser vil endre seg dersom det fremkommer ny informasjon om en gitt situasjon eller aktivitet [24]. Kollektiv sensemaking kan illustreres ved hjelp av en hermeneutisk sirkel som vist på neste side, da forholdet mellom fortolkning og atferd er en dynamisk og fortløpende prosess.




Figur 9 Kollektiv sensemaking: fremstilt som en hermeneutisk sirkel

Flere underliggende mekanismer kan påvirke dialogen og den kollektive sensemakingen i en organisasjon, det være seg *kontekstuelle forhold*, *skjevheter* (biases) innad i gruppen og *psykologiske faktorer* [31]. Antagelsen er at forhold knyttet til gruppeprosessen kan ha innvirkning på de beslutningene som tas vedrørende handling (f.eks valg av tiltak).

En velkjent problemstilling er at gruppedeltakerne er så opptatt av å komme til enighet at de ikke samler inn tilstrekkelig med informasjon og dermed ikke får oversikt over alle alternativene. Denne formen for ”gruppetekning” ble først beskrevet av Irving Janis tidlig på 1970-tallet og refererer til dårlig begrunnet avgjørelser [31]. En annen ”fallgruve” er at gruppedeltakerne overvurderer graden av likhet, dvs. at man antar at de andre i teamet sitter med den samme oppfatning om situasjonen/informasjonen som en selv. Ross, Greene & House [32] omtalte denne mekanismen som ”falsk konsensus” og beskrev det som at mennesker har en tendens til å:

> ”see their own behavioural choices and judgements as relatively common and appropriate to existing circumstances while viewing alternative responses as uncommon, deviant or inappropriate”

Sagt på en annen måte innebærer ”falsk konsensus” at folk oppfatter sin egen atferd som typisk og dermed tror at andre forstår situasjonen tilsvarende de selv. En tredje bias som Jones og Roelofsma [31] refererer til i sin artikkel, er ”gruppepolarisering”. Det oppstår en gruppepolarisering dersom synspunktene til majoriteten i gruppen er blitt forsterket etter endt diskusjon. Et eksempel er dersom gruppemedlemmene i utgangspunktet generelt er risikosøkende, vil en gruppediskusjon forsterke denne egenskapen ytterlige også på det individuelle plan. ”Gruppeopptrapping” (group escalation) handler om den tendensen individer og grupper har til å støtte et eksisterende handlingssett, til tross for at det finnes bevis som tilsier at noe annet er ”riktig” [31]. Det innebærer at en avgjørelse baseres på tidligere beslutninger selv om denne fikk et negativt utfall.

I sin bok ”Man made disaster”, presenterer Barry Turner [33] begrepet ”inkubasjonsperioden”. I korte trekk beskriver inkubasjonsperioden den fasen hvor en kjede av uregelmessigheter utvikles og akkumuleres ubemerket. Eksisterende kulturelle sikkerhetstiltak kan bli vurdert til å håndtere kjente og klart definerte risikoer, men i løpet av inkubasjonsperioden begynner et sett av vage og uoppdagede farer å lure i kulissene, og som ikke blir tatt med i risikovurderingen. Får denne kjeden av uregelmessigheter anledning til å utvikle seg fritt, kan det i verste fall ende med katastrofe. Gjennom sin forskning avdekket Turner flere kausaliteter som kan forklare hvorfor organisasjoner tillater denne akkumuleringen av farer, og som er relevant i forhold til problemstillingen i denne oppgaven. Dårlig informasjonskommunikasjon eller misoppfatning mellom ulike aktører, er årsaker som er interessante å betrakte opp mot teorier om kollektiv sensemaking og gruppemekanismers innvirkning.

Turner [33] avdekket følgende fire årsaksforhold, som anses aktuelle i forhold til dette studiets problemstilling:

1. Avvikende hendelser ble misforstått eller oversett fordi det var vanskelig å håndtere informasjon i komplekse situasjoner. Det kan f.eks. skyldes at viktige beskjeder forsvant p.g.a. at det var så overveldende mye informasjon, eller at de som skulle overlevere informasjonen, var opptatt med andre oppgaver.
2. Uregelmessigheter ble oversett eller misforstått pga at mennesket har en iboende motvilje mot å frykte det verste. Denne egenskapen gjorde at risikoer ble bagatellisert selv de gangene utbrudd var oppdaget.

3. Dersom formelle sikkerhetstiltak var utdaterte, førte det til at brudd på regler og reguleringer etter hvert ble uformelt akseptert i organisasjonen.

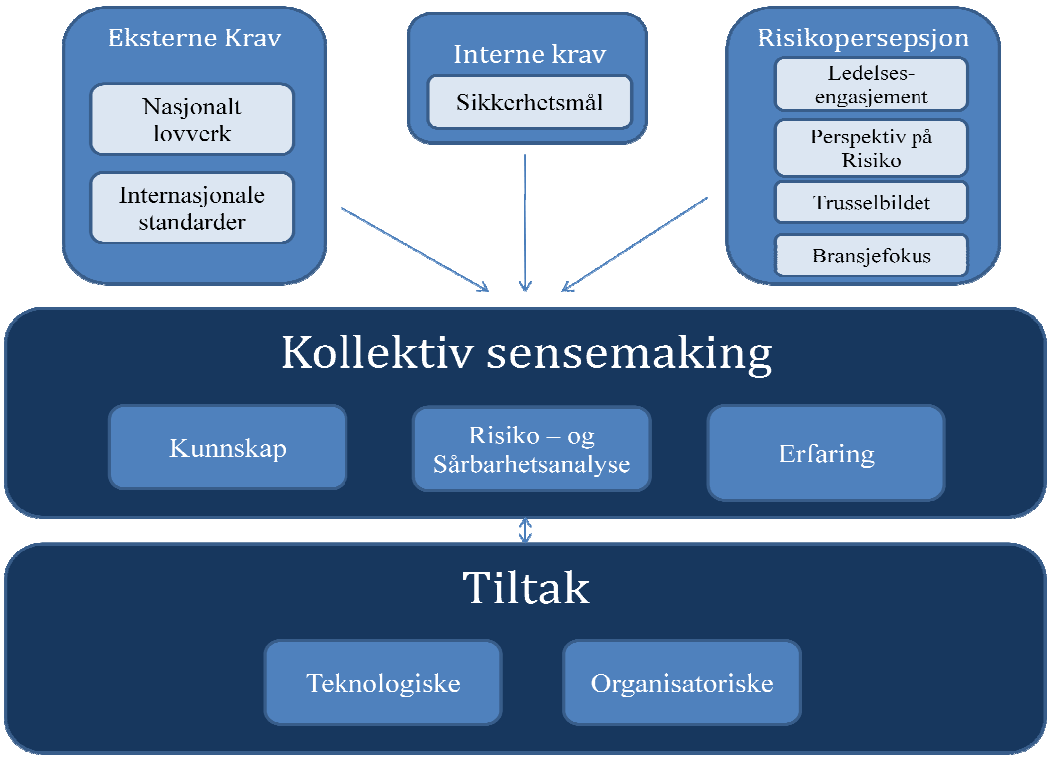
Et av poengene til Turner er at organisasjoner må være bevisste og opptatt av å få frem all relevant informasjon, og på den måten være i stand til å oppdage avvik og dermed hindre at en fare får lov til å utvikle seg [33]. Denne oppgaven omhandler trusler mot kraftforsyningens driftskontrollsystem. I det neste avsnitt vil utfordringer knyttet til ny teknologi bli belyst, da med tanke på hvorvidt mennesket er i stand til å oppfatte og forstå den informasjonen som den komplekse teknologien representerer.

### 2.4.1 Sensemaking og ny teknologi

Weick [27] har gjennom artikkelen ”Technology as Equivoque” problematisert sensemaking i forhold til nye teknologier. Her blir særlig IKT-systemer fremhevet som et eksempel på ny teknologi. ”Equivoque” kan oversettes med ”tvetydighet” og innebærer at noe tillater flere mulige tolkninger. I likhet med Weick, har Leveson [30] satt fokus på de utfordringene som IKT-systemer medfører. Hun sier at ny teknologi kjennetegnes ved graden av kompleksitet og tette koblinger. I tillegg eksisterer det mange ukjente faktorer, samtidig som teknologien gjerne er forbigående med mange hurtige systemendringer. Alt dette gjør det svært vanskelig for de menneskene som forsøker å sette seg inn i hvordan systemene fungerer, å forstå hvorfor eksempelvis datasystemene svikter [27]. Weick hevder at komplekse systemer gir redusert mening fordi det er så lite som er synlig, samtidig som de tette koblingene kan modelleres på mange ulike måter og dermed forårsake mange og ukjente virkninger[27]. Videre påpeker han at denne teknologiens tvetydighet krever fortløpende organisering og sensemaking dersom den skal la seg styre, men det forutsetter at de perseptuelle modellene tilsvarer de faktiske teknologiske prosessene i størst mulig grad.

## 2.5 Analysemodell

Formålet med denne oppgaven er som tidligere nevnt, å undersøke hvordan kraftbransjen oppfatter trusselen om angrep på driftskontrollsystemene, og i hvilken grad det har betydning for informasjonssikkerheten. Følgende analysemodell gir en oppsummering av teorien som er presentert i kapittel 2, samt danne utgangspunkt for diskusjonen i kapittel 4.




Figur 10 Analysemodell

### 2.5.1 Forklaring til analysemodellen

Myndighetskrav som fremkommer av regelverk og forskrifter, vil alltid ligge til grunn for risikostyringen i en virksomhet [1]. I tillegg kan internasjonale standarder, som f.eks ISO 17799, ha innvirkning på den aktiviteten som foregår i en bedrift. Interne krav er gjerne basert på nasjonalt lovverk, men kan også utvides med egne formuleringer og sikkerhetsmål [1]. Risikopersepsjon utgjør en sentral del av problemstillingen.

Forskning viser at persepsjon blant annet dannes av erfaring, sosial og kulturell påvirkning og grad av frivillighet [16]. I denne sammenheng har jeg valgt å legge særlig vekt på ledelsen (engasjement), hvilket sikkerhetsfokus som eksisterer i bransjen for øvrig, det nasjonale trusselbildet og medias dekning av cyberkriminalitet som faktorer som påvirker risikopersepsjonen. Eksterne krav, interne krav og risikopersepsjon danner grunnlaget for hvilken prioritering sikkerhetsutfordringer knyttet til ikt-systemene gis i virksomheten. Dette forholdet illustreres med piler ned til kollektiv sensemaking.

*Kollektiv sensemaking* foregår hovedsakelig i risikostyringsprosessen og inkluderer risiko- og sårbarhetsanalyser, samt deltakernes kompetanse (kunnskap og erfaring). Videre kan ulike gruppeprosesser påvirke den felles forståelsen av, i dette tilfellet trusselen om cyberkriminalitet, som fører til beslutninger om valg av tiltak. Tiltak er delt inn i organisatoriske og teknologiske tiltak. Det er en toveis-pil mellom ”kollektiv sensemaking” og ”tiltak”, hvilket indikerer at de erfaringene man gjør seg av de tiltakene som er iverksatt, igjen vil påvirke sensemakingen i neste omgang.

Analysemodellen kunne dessuten ha involvert forhold knyttet til *etterlevelse*, hvilket innebærer hvorvidt virksomhetene følger opp de tiltakene som iverksettes. Når dette elementet er utelatt, skyldes det et bevisst valg om ikke å berøre forhold som kan betegnes som sensitiv informasjon etter BfK § 6-2.

# 3 Metode

Dette kapittelet tar for seg de metodiske valgene som er foretatt i henhold til studiets problemstilling.

## 3.1 Forskningsdesign

I følge Blaikie [49] refererer forskningsdesignet til den prosessen som sammenfatter problemstilling, empiri og konklusjon. Videre bør det henvise til det som skal undersøkes, hvorfor det skal bli studert og hvilken metode som skal benyttes. I dette studiet er formålet å avdekke hvordan kraftbransjen forholder seg til trusselen om cyberkriminalitet, og hvilke faktorer som kan ha betydning for valg av informasjonssikkerhet. Omfattende litteratursøk har vært en nødvendig forutsetning for å tilegne seg nok bakgrunnskunnskap om blant annet kraftforsyningen, IKT-systemer og cyberkriminalitet. Både nasjonal og internasjonal forskning har inngått i litteratursøket.

Et case-studie, hvor flere enheter (nettselskaper) inngår, ble ansett som en hensiktsmessig tilnærming til problemstillingen. Et case-studium vil være godt egnet når man ønsker en større forståelse av et fenomen som er tilfellet her [48]. Ved å gå i dybden kan det hende at man finner forhold som man ikke var klar over på forhånd.

## 3.2 Kvalitativ undersøkelse

Problemstillingen er av en eksplorativ karakter, dvs. at hensikten ikke er å forstå, men forklare [51]. Kvalitativ datainnsamlingsmetode vurderes som en mest egnet fremgangsmåte. En kvantitativ metode ville ha drevet frem kunnskap i bredden [48], mens dette studiet har til hensikt å gå i dybden. Det åpne individuelle intervjuet egner seg godt når få enheter skal undersøkes, og når man ønsker å få kunnskap om hvordan den enkelte ”fortolker og legger mening i et spesielt fenomen” [48]. Slike intervjuer spiller en vesentlig rolle i case-studier [51].

### 3.2.1 Intervju

På tross av en tid - og kostnadskrevende prosess, ble intervjuene hovedsakelig gjennomført ansikt til ansikt. Bakgrunnen for valget var et ønske om å treffe informantene i sine egne omgivelser, samt at det er enklere å skape en fortrolighet i intervjusituasjonen når man fysisk sitter overfor hverandre [48]. En samtale ble utført via telefon, da det ikke var anledning å oppsøke vedkommende på det aktuelle tidspunktet. Med unntak av telefonintervjuet, ble alle samtalene tatt opp på bånd. Dette var avtalt med informantene på forhånd, og en samtykkeerklæring ble underskrevet av begge parter før oppstart (Jfr. Appendiks V). Intervjuene kan karakteriseres som dybdeintervju, og hver enkelt samtale varte mellom en og to timer.

I forkant av intervjuet fikk samtlige informanter tilsendt bakgrunnsinformasjon om studiet, intervjuguide og samtykkeerklæring (Appendiks II, III og IV), med unntak av en kandidat som ikke hadde mottatt denne. Vedkommende fikk anledning å lese igjennom guiden før intervjuet startet. Intervjuguiden var relativt omfattende. Den var tematisk oppbygd med utgangspunkt i problemstilling og utvalgt teori. Spørsmålene ble ikke fulgt slavisk under intervjuene, men var likevel aktivt i bruk - dette for å sikre at samtlige kommenterte de temaene som var ansett som relevante for problemstillingen. Det finnes imidlertid fordeler og ulemper ved å la informantene få tilgang til intervjuguiden på forhånd. På den ene siden kan man i større grad oppnå reflekterte svar, ulempen er at man går glipp av den spontane responsen på spørsmålene. Valget om å sende intervjuguiden på forhånd, er hovedsakelig begrunnet i at mange forhold som omhandler driftskontrollsystemene, karakteriseres som sensitiv informasjon. Formålet med å opprette en åpen dialog allerede i forkant av samtalene, var at respondentene formodentlig ville være trygge på at spørsmålene ikke ville involvere informasjon av sensitiv karakter.

### 3.2.2 Valg av informanter

I dette studiet består utvalget av seks respondenter og en informant. *Respondenter* omfatter personer som har direkte kunnskap om et fenomen, og som representerer den gruppen som skal undersøkes [48]. Her er det kraftbransjen, nærmere bestemt nettselskaper av en viss størrelse, som utgjør respondentene. *Informanter* har god kjennskap til gruppen eller fenomenet uten å være en del av den, og består i denne sammenheng av en tilsynsmyndighet (NVE). Det er kun NVE som vil bli identifisert i

dette studiet. De resterende behandles konfidensielt etter avtale – dette for å unngå at informasjonen blir å anse som sensitiv i henhold til Energilovens krav. I empirikapittelet og i diskusjonen vil imidlertid begrepene informant og respondent bli brukt om hverandre.

Samtlige som deltok i undersøkelsen, kan karakteriseres som nøkkelinformanter [50]. Fire av respondentene fungerer som nettselskapets IKT-sikkerhetsleder i henhold til BfK 6-1. Den femte respondenten har koordinert risikoanalysen av driftskontrollsystemet i virksomheten. NVE har bidratt med å tilføye bredde og variasjon i utvalget. Nettselskaper av mindre størrelser, er ikke representert i dette studiet. Valget kan begrunnes med at de kandidatene som karakteriseres som nøkkelpersoner, ikke nødvendigvis finnes i små enheter, hvor lederen gjerne samtidig ivaretar rollen som beredskapsleder og ikt-sikkerhetsleder. Respondentene ble valgt fordi de ansees å kunne tilføre informasjon som vil være nyttig for forskningen [50 og 48]. I tre av intervjuene var det to personer fra virksomheten til stede. Da intervjuene ikke tilfredsstiller kriteriene som inngår i et gruppeintervju, behandles disse på lik linje med individuelle samtaler.

Det vil alltid være spørsmål om det burde vært flere respondenter involvert i studiet, noe som også er vurdert her. Med hensyn til tiden som har vært til rådighet, antas det imidlertid at utvalget har vært tilstrekkelig for å belyse de forhold som har vært viktige for å kunne besvare problemstillingen.

## 3.3 Fortolkning av data

Jacobsen [48] fremhever at det ofte går et skille mellom det som betegnes som analyse av enkelt-caser og analyser hvor man sammenligner flere caser. I dette studiet er det kraftbransjen som skal studeres. Enkeltpersoners oppfattelse fokuseres derimot ikke her. Som tidligere nevnt, var intervjuguiden inndelt i emner. Analyse på tvers av caser innebærer at svarene fra de ulike respondentene sammenlignes med hensyn til hver enkelt kategori. Hensikten har vært å avdekke hvordan flere aktører vurderer trusselen om cyberkriminalitet, samt hvorvidt forhold ved eksempelvis en risikoanalyseprosess varierer i de ulike virksomhetene.

Det er alltid mulighet for feiltolkning av de dataene som foreligger. Til sammenligning finnes det ulike meninger om f.eks. betydningen av forkunnskaper i forhold til et

dybdeintervju [50]. Noen mener at det i en utspørring kan være en fordel å ikke ha så mye kunnskap om det som skal studeres, fordi intervjueren ikke blir forstyrret av forutinntatthet. På den andre siden kan manglende kunnskap føre til at forskeren misoppfatter det som blir sagt under intervjuet, hvilket resulterer i redusert forståelse og oversikt over intervjusituasjonen [50]. Tilsvarende kan også forekomme når data skal analyseres. Mangelfull oversikt over feltet som studeres, kan forårsake at man ikke klarer å fange opp de funnene som måtte være der. En annen feilkilde kan imidlertid være at egen forutinntatthet bidrar til at forskeren kun oppdager det han vet om emnet fra før, og dermed overser man kanskje interessante sammenhenger. Dette er noe forfatteren har hatt et bevisst forhold til under analysen av dataene, men samtidig må det erkjennes at det vil være vanskelig å gå inn i en slik prosess uten en viss forutinntatthet. Problemet er imidlertid først når en lar egne verdier og forutinntatthet styre objektiviteten, noe som er forsøkt unngått i denne analysen.

## 3.4 Reliabilitet og Validitet

Reliabilitet innebærer at den informasjonen som innhentes, skal kunne etterprøves [51]. I et forsøk på å øke reliabiliteten har det blitt benyttet en semi-strukturert intervjuguide. Hensikten var å skape en noenlunde tilsvarende intervjusituasjon for samtlige respondenter. Erfaringer fra det første intervjuet med et av nettselskapene, tilsa at det i utgangspunktet var for mange spørsmål, og intervjuguiden ble som følge av det noe forkortet. For ytterligere å styrke reliabiliteten, har alle data blitt lagret på en forsvarlig måte [52]. De intervjuene som ble tatt opp på bånd, er transkribert. Det ble ikke foretatt noen notater underveis i samtalene, med unntak av telefonintervjuet. Her ble notatene ”finskrevet” og sendt til respondenten, som bekreftet at vedkommende var oppfattet riktig.

Har forskningen gitt et korrekt svar på problemstillingen? For å kunne besvare dette spørsmålet, må intern og ekstern gyldighet (validitet) vurderes [48]. Førstnevnte innebærer om resultatene oppfattes som ”sanne”, i den grad et fenomen er befestet med en objektiv sannhet. Etter at empirikapittelet var ferdig formulert, ble det sendt til samtlige respondenter (og informanter), for at de skulle få anledning til å komme med

innvendinger eller kommentarer. Fire av syv har gitt en tilbakemelding. En av dem ønsket å presisere og utdype noen opplysninger som ikke var kommet tydelig nok frem. Argumentet var at dersom endringer ikke ble foretatt, stod dokumentet i fare for å avsløre sensitiv informasjon i henhold til Energilovens krav. Ytterligere en respondent ønsket at et sitat ble omformulert. Denne endringen fikk ikke betydning for innholdet. Det forutsettes at de respondentene som ikke har gitt tilbakemelding, ikke hadde noen innvendinger til innholdet i empirikapittelet.

Hva med den eksterne gyldigheten? Jacobsen [48] presiserer at formålet med kvalitative metoder vanligvis ikke er ”å generalisere fra utvalget av enheter til en stor gruppe enheter”. Problemstillingen har til hensikt å avdekke hvordan kraftbransjen oppfatter trusselen om angrep på driftskontrollsystemene, og hvilke faktorer som kan ha betydning for valg av informasjonssikkerhetstiltak. Det kan tenkes at utvalget er for lite til å kunne trekke en generell konklusjon om en hel bransje. Særlig er det vanskelig å uttale seg om hvorvidt de små og mellomstore nettselskapene vurderer trusselen om cyberkriminalitet. På den andre siden er NVE benyttet som informant, blant annet med tanke på å ”kvalitetssikre” resultatene. De kan med sin tilsynserfaring og kjennskap til bransjen bidra med å bekrefte eller avkrefte de funnene som kom frem av intervjuene med nettselskapene.

## 3.5 Etiske betraktninger

Kraftforsyningen er en av de viktigste kritiske infrastrukturene vi har i landet. Et tilsiktet angrep vil kunne være svært alvorlig, enten det er de fysiske komponentene eller angrepet er rettet mot ikt-systemene. Energiloven, Sikkerhetsloven og Beredskapsloven har klare retningslinjer til hva som karakteriseres som sensitiv informasjon og hvordan denne skal behandles av de enkelte aktørene i kraftsektoren. Med hensyn til de kravene som foreligger, har de temaene og spørsmålene som ble omtalt i intervjuene unngått å berøre informasjon som kan betegnes som sensitiv. Denne begrensingen har tilsynelatende vært styrende for hvilke svar som har blitt gitt.

I dette studiet er det av den grunn særlig vektlagt at alle opplysninger blir behandlet konfidensielt. Hensikten er at ingen skal kunne gjenkjenne verken personer eller den virksomheten vedkommende tilhører. Materialet som blir brukt, skal ikke være til skade

eller ulempe for informantene eller virksomhetene. Dette blir ivaretatt ved at ingen blir navngitt i teksten. Etter skriftlig samtykke (Appendiks V) fra respondentene kan imidlertid informasjon benyttes i den grad at vedkommende ikke blir gjenkjent. Sitat som benyttes refererer til ”Respondent 1” , ”Respondent 2” osv. Betegnelsene er tilfeldig valgt og kan ikke spores tilbake til samtalene. Unntaket er intervjuet med NVE som en offentlig tilsynsmyndighet. Personene som representerte NVE, er ikke navngitt, men kommentarer og sitat refererer til organisasjonene.

Lydopptak som er gjort i forbindelse med intervjuene, er kun beregnet for denne masteroppgaven. Disse vil bli slettet etter at sensur er falt.

# Empiri og Diskusjon

## 4 Presentasjon av intervjuer

Hensikten med empiriske undersøkelser er først og fremst å utvikle ny kunnskap, enten man er ute etter å *beskrive* et fenomen eller man ønsker å *forklare* sammenhenger [48]. Denne oppgaven legger vekt på å skildre hvordan kraftbransjen oppfatter trusselen om angrep på driftskontrollsystemene. I tillegg er det interessant å studere hvilke faktorer som kan ha betydning når virksomhetene velger hvilke informasjonssikkerhetstiltak som skal iverksettes.

Seks store selskaper innenfor kraftsektoren har deltatt i undersøkelsen. En spørsmålsguide (jf. appendiks III og IV) dannet utgangspunktet for samtalene. I tillegg ble to representanter fra NVE intervjuet. Det var interessant å iaktta hvilket inntrykk tilsynsmyndighetene har av bransjen, samt å avdekke forhold hvor NVE og virksomhetene var av ulik oppfatning. Jeg har valgt å kategorisere og sammenfatte de svarene som er kommet frem av intervjuene. I flere tilfeller er informantene rimelig samstemte, og jeg har da forsøkt å formidle hovedessensen. De gangene informantene presenterte ulike syn, kommer det frem av teksten. Deler av datamaterialet er utelatt da det ble vurdert som mindre relevant for problemstillingen. Hver kategori etterfølges av en oppsummerende anmerkning. Empirikapittelet avsluttes med en kommentar til hovedfunnene fra denne undersøkelsen

I kapittel 5 foregår drøftingen av utvalgt teori og det datamaterialet som foreligger. Analysemodellen som er presentert i kapittel 2, danner utgangspunkt for diskusjonen. Forhold som kommer innunder følgende kategorier vil bli omtalt:

- Risiko og persepsjon
- Kollektiv sensemaking i kraftforsyningen
- Fra felles forståelse til handling

## 4.1 Organisering og ansvar

Felles for virksomhetene er at de er ansvarlige for og drifter anlegg som tilhører klasse 3 i henhold til bfK § 5-3 og energiloven § 8-3. Alle har en IKT-sikkerhetsleder etter BfK 4-1, men ikke alle har øremerket en hel stilling til dette formålet. To av informantene oppgav at funksjonen som IKT-sikkerhetsleder var redusert til henholdsvis en halv stilling i det ene selskapet og en halv stilling fordelt på nettselskapet og konsern i det andre selskapet. Denne ordningen gikk på bekostning av at man ikke fikk gjennomført alle arbeidsoppgavene som ønsket. Videre varierte det hvordan energiselskapene har valgt å organisere seg for øvrig. Enkelte av selskapene hadde ikke en egen IT-ansvarlig i enheten, men samarbeidet da med IKT-sikkerhetsleder på tvers av datterselskapene i konsernet. På spørsmål om hvordan IKT-systemet organiseres, valgte en informant å beskrive de ulike rollene som ble benyttet i virksomheten, det være seg *overordnet systemeier, systemeier, systemansvarlig og driftsansvarlig*. Tre av respondentene kjente seg igjen i denne type inndeling, mens to andre representerte en annen ordning. I det ene selskapet var det en egen IKT-avdeling som hadde ansvar for planlegging og drift av alle systemene. Noe tilsvarende gjaldt også for det andre selskapet. Her fantes et eget it-datterselskap i konsernet, men selve driftssentralen ble administrert av folk som ikke var tilknyttet it-avdelingen. Samtlige informanter poengterte at driftskontrollsystemet, dvs. SCADA-systemet er et forholdsvis lukket system. Det finnes et fåtall (en til to) porter som er koblet til det administrative systemet via brannmurer.

Fem av seks informanter svarte at de ikke benytter seg av outsourcing av IT-oppgaver. Da har de sett bort ifra systemleverandører som ABB og Siemens, som gis tilgang til driftskontrollsystemene f.eks. ved oppgradering av systemene eller for å utføre oppgaver som nettselskapene ikke har kompetanse til selv. En forklaring på at systemleverandøren ikke ble betraktet som outsourcingspartner, var at de ikke er inne i den daglige driften av systemet. NVE har sikkerhetsavtaler med en del av de store aktørene som leverer tjenester til kraftbransjen, men hvert enkelt selskap kan inngå egne sikkerhetsavtaler. Dette ble i liten grad gjort av de selskapene som er undersøkt i denne rapporten. En informant uttalte at de følger de kravene som settes til sikkerhetsavtaler i beredskapsforskriften.

Tre av informantene har svart at systemleverandørene kan gis tilgang eksternt, altså at de har mulighet å sitte på et rom hos seg selv og logge seg inn på driftskontrollsystemet.

Dette skjer under kontrollerte former, f.eks. ved å gi en tidsbegrenset tilgang med automatisk lukking via egne modemforbindelser eller 2-komponentløsninger (brukernavn og passord som tilsvarer det som benyttes til nettbank). Systemleverandørene kan også få tilgang ifra driftssentralen, hvor SCADA-systemene er fysisk plassert. Det er uklart hvorvidt dette gjelder alle, men flere påpekte at systemleverandøren har følge når de går inn i det "aller helligste". En informant presiserte at selskapet alltid har kontroll over tid, ressurs og innsyn ved tilgang (f.eks. logging). Vedkommende må også skrive under på erklæringer om konfidensialitet. En informant påpekte at man ikke har oversikt over systemleverandørens sikkerhetsrutiner:

> **"Hvordan vet vi at den maskinen de logger seg inn med er sikker og ikke tar med ulumskheter. Vi vet ikke om deres ressurser er sikret "** (Respondent 3).

På den andre siden er det viktig å fokusere på å bygge robusthet i egne system. NVE gav uttrykk for at det etter hvert har blitt en viss grad av bevissthet omkring outsourcing. Men de fleste kraftselskapene er små sammenlignet med leverandørene, og disse stiller gjerne ikke krav da de forutsetter at "leverandøren kan dette".

> **"For eksempel spurte jeg et stort selskap om deres interne sikkerhetsregime vedrørende driftskontrollsystemet var kjent for leverandøren deres, om de hadde noen systemer for å sikre seg at leverandøren var kjent med og fulgte det. Nei, det hadde de ikke. Men de trodde nok ikke at han var kjent med det."** (NVE)

En informant problematiserte at enkelte systemleverandører mangler fokus på sikkerhet. Mange løsninger kommer som resultat av systemutvikling i samarbeid med systemeier. Dette er ikke spesielt for kraftbransjen. Problemet er gjerne da at systemeier (f.eks nettselskapet) ikke har tilstrekkelig kunnskap om systemene - og av den grunn ikke vet hvilke sikkerhetsforutsetninger som bør legges til grunn.

*FUNN:*

- *To av respondentene opplyste at ikt-sikkerhetslederen kun var tildelt en 50 % stilling, hvilket kan tolkes dit hen at ledelsen ikke prioriterer dette.*
- *Systemleverandører ble ikke vurdert som outsourcingspartner. De fleste oppgav at de hadde god kontroll på tilgangen som gis til vedkommende som foretar oppgradering av systemene (fra leverandør), særlig når aktiviteten foregikk i*

*driftssentralens lokaler. Når systemleverandøren får fjerntilgang, var det mindre kontroll. Det virket som om flesteparten ikke opplevde dette som et sikkerhetsproblem. En informant problematiserte imidlertid at leverandørbransjen ikke er gode nok på det IKT-sikkerhetsfaglige.*

## 4.2 Risikostyring (ROS-analyser)

*Med risikostyring forstås "alle tiltak og aktiviteter som gjøres for å styre risiko" (Aven, 2007). Informantene har i hovedsak fått spørsmål knyttet til risiko – og sårbarhetsanalyser, samt forhold knyttet til selve arbeidsprosessen.*

Samtlige har gjennomført ROS-analyser av IKT-systemene, herunder driftskontrollsystemet. Det varierte hvor ofte og hvor grundige analysene var. To av dem benyttet en frekvens på hvert tredje år, mens enkelte rapporterte at de har som mål å gjennomføre ROS-analyser hvert annet år. Felles for flere var at de foretok en revisjon eller ny vurdering ved endringer som var av betydning, f.eks ved oppgradering av systemet. ROS-analyser ble oppfattet som et hensiktsmessig verktøy når IKT-systemene skulle vurderes, særlig dersom analysegruppen klarte å tenke kreativt og ta med "det utenkelige". Samtidig var det viktig at analysedokumentet er brukervennlig og "jordnært".

> **"Vi var veldig klar på at vi ikke ønsket store ROS-analyser med ukjente og svære begrep. (…) Vi ville ikke ha noen problemer tilbake som vi ikke klarer å løse. Det funket for oss."** (Respondent 3)

Fire av informantene har benyttet standard ROS-analyser, dvs en grovanalyse som ender opp i matriser med fargekoder som beskriver nivå for sannsynlighet og konsekvens. Det varierte i hvilken grad eksterne konsulenter har vært delaktige i prosessen. To av informantene benyttet egenutviklede analysemetodikker. En informant mente at CORAS er den beste metoden når det gjelder synliggjøring av gjensidig avhengigheter i IKT-systemet. Fire respondenter nevnte bruken av sjekklister, men da gjerne i forbindelse med å komme frem til hvilke uønskede hendelser som skal analyseres (fareidentifikasjon). Samtlige svarte at erfarne folk deltar i risikoanalysene, eventuelt sammen med eksterne konsulenter. Brainstorming eller workshops dannet grunnlag for hvilke objekter som skal analyseres. Samtidig ble det poengtert at den

erfaringen og kompetansen som analysegruppen besitter, var det viktigste utgangspunktet for den videre prosessen. De vet ”hvor skoen trykker” og hvor systemet er mest sårbart. Utfordringen ved å vurdere risiko knyttet til IKT-systemer, er at det består av mange usikkerhetsmomenter og ukjente faktorer.

> **”Det er jo det som er utfordringen her, å finne det ukjente. Finne det som ingen har tenkt på før og sette det i et system.”** (Respondent 4)

På spørsmål om bakgrunnen for fastsettelse av sannsynlighet og konsekvens, var det to respondenter som svarte at de benyttet en tradisjonell teknisk utregning, hvor risiko = sannsynlighet x konsekvens. De var imidlertid ikke så opptatt av tallene, men ”mageføleIsesverdien” var mer retningsgivende. Det samsvarte med de øvrige informantenes oppfatning av at ”common sense”-vurderinger eller erfaring og kjennskap til feltet danner grunnlaget for beregning av sannsynligheter. En informant poengterte at det endog ikke var mulig å benytte kvantitativ sannsynlighetsberegning, da det ikke finnes statistikk når det gjelder IKT-systemer. Det var altså de kvalitative vurderinger som må ligge til grunn for fastsettelse av sannsynlighet og konsekvens. I tillegg ble det sagt at det er nødvendig å være fremsynte i forhold til hva som kan skje.

> **”De fem punktene som ikke er med i ROS-analysene som vi ikke vet om, men som burde vært der. De er viktige fremover.”** (Respondent 3)

En annen kommenterte usikkerhetene knyttet til IKT-systemer på følgende måte:

> **”Det ene er at IKT-systemene har mye kortere levetid enn et vanlig tradisjonelt kraftsystem. (…) Det andre er at skal bruke statistikk og hendelser. Da kan du se om det har skjedd i vårt område, i Norge eller om vi har hørt om det en eller annen gang. Men du kan ikke bare se bakover, du må også se fremover. Hva kan en forvente. (…), og da er den plasseringen inn i matrisen avhengig av personene du har inne og hva de klarer å se fremover.”** (Respondent 5)

Det var noe variasjon i hvordan virksomhetene forholdt seg til fastsettelse av akseptabelt risikonivå. To av informantene poengterte at man må ha grep om verdier knyttet til 1) tap av liv og helse, 2) tap av omsetning / utfall med store samfunnsmessige konsekvenser og 3) tap av omdømme før akseptabelt risikonivå kan fastsettes. Da vil gjerne myndighetskrav, interne krav og hva virksomheten anser som akseptabelt risikonivå bakes inn i det. To informanter understreket betydningen av at akseptabelt risikonivå fastsettes på forhånd, altså før resultatene fra ROS-analysen presenteres.

> **”Jeg har sett tilfeller hvor man tar risikoanalyser, og så justere akseptnivået når man ser konsekvensene av analysen. For da passer det inn i økonomien.”** (Respondent 1)

> **”Vi hadde senest en diskusjon i går, hvor en hendelse stod igjen på rødt etter at tiltak var vurdert. Det ble veldig mye diskusjon rundt den ene hendelsen, og det blir litt feil i mitt hode. Noen hendelser er røde, du kommer ikke bort fra det.”** (Respondent 5)

Det kom altså an på hvilken risikoappetitt en skal legge seg på, og gjerne også hvorvidt den uakseptable situasjonen var midlertidig eller endelig. Dersom en hendelse befant seg i rødt, var det i en virksomhet opp til systemeier eller ansvarlig beslutningstaker å avgjøre hvorvidt tiltak skulle gjennomføres eller ikke. I et annet selskap kom det frem at det manglet et overordna prinsipp ifra konsernledelsen som gikk ned til nivåene under. Risikomatrisene som ble benyttet var utdatert og avvek i forhold til tankegangen i dag.

Ifølge informantene får risiko knyttet til IKT-systemene, i økende grad oppmerksomhet i kraftbransjen. En informant medgav at det tradisjonelt har vært lite fokus på dette, men at man befinner seg i en ”oppvåkningsperiode”. En av grunnene som ble nevnt, er at myndighetene har mer fokus på dette. To av informantene antok at minst like mye oppmerksomhet ble rettet mot IKT-systmene som til fysisk infrastruktur, mens tre respondenter mente at den fysiske infrastrukturen fremdeles tillegges mest vekt i deres enhet.

> **”Det er nok mer fokus på fysisk infrastruktur, og det er nok riktig prioritering også. Folk skal ha strøm selv om kontrollsystemer svikter.”** (Respondent 6)

### 4.2.1 Varslingsrutiner

Informantene var rimelig unisone i opplevelsen av at varslingsrutinene fra myndigheten ikke fungerer tilfredsstillende. De fikk spørsmål knyttet til hvilke erfaringer de hadde av Stuxnet-viruset sommeren 2010. Fem av seks respondenter stilte seg kritiske til varslingen av denne spesifikke hendelsen. Et av problemene var at de fikk kjennskap til trusselen gjennom media eller via intern rapportering i bransjen, mens NVE kom på banen først flere uker i etterkant. Ifølge en informant hadde de allerede sikret seg mot trusselen da de mottok varslingen fra myndighetene. En informant antok at NVE har for stor tillit til den etablerte kjeden de har gjennom beredskapskoordinatorene. Bransjen

mente altså at det må en betydelig forbedring til dersom varslingen skal ha en hensikt. Følgende ble foreslått:

- Tettere dialog mellom myndighetene og bransjen
- Varslene må sendes så raskt så mulig etter at de er kjent. Bedre samarbeid med NorSis kan forbedre dette.
- Varslene må sendes til riktige mottakere i kraftselskapene: IT-sikkerhetsleder og beredskapskoordinatorer (viktig med oppdatert kontaktinformasjon).

Representantene fra NVE var av en helt annen oppfatning. De forklarte at når varsler om ulike former for alvorlige trusler (IKT, klimatiske, kriminalitet og lignende) er tilgjenglig, gir de direkte beskjed til alle direkte berørte KBO-enhetene pr epost (ofte fulgt opp med en telefonsamtale), + e-post og fax til distriktsjefene ,som igjen følger opp sine selskaper. Implisitt i rutinen ligger det også at alle mottakerne skal gi tilbakemelding om at de har mottatt varslet. Varslene går til de kontaktpersoner (beredskapskoordinatorer, IKT-sikkerhetsleder og lignende) som virksomhetene selv har utpekt. Videre påpekte NVE at når vedkommende er valgt til å inneha disse funksjonene, er de også ansvarlig for effektiv intern-informasjon i eget selskap.

Flere av informantene nevnte at bransjen har etablert et forum som kalles FSK-forum, blant annet fordi det var et behov for å arbeide for en tettere dialog med myndighetene. Forumet består anslagsvis av de femten største nettselskapene, og har samlinger to ganger i året. Tema som gjennomgås er relatert til informasjonssikkerhet, eksempelvis at myndigheter og leverandører bør være mer åpne om sårbarheter de har oppdaget selv og sørge for samtlige energiselskap blir orientert.

*FUNN:*

- *Hovedtendensen var at virksomhetene benyttet en kvalitativ tilnærming til risiko. Samtlige trakk frem erfaring og kompetanse som den viktigste egenskapen ved fastsettelse av sannsynlighet og konsekvens.*
- *Alle hadde gjennomført grundige ROS-analyser av IKT-systemet, hvor de skilte mellom tilsikta og utilsikta hendelser. Det er ikke sikkert at dette funnet er representativt for hele kraftbransjen, noe NVE også bekreftet. De sa at det var*

*stor forskjell på kvaliteten på disse analysene, noe som gjerne hadde sammenheng med størrelsen på selskapet og hvilket security-fokus som var i organisasjonen.*

- *Samtlige fremhev betydningen av at kompetente og erfarne medarbeidere deltok i analyseprosessen, og at brainstorming var nødvendig for å få frem ulike scenarioer. Bortsett fra sjekklister, er det uklart hvorvidt rapporter (NSM) og internasjonale standarder ble benyttet i denne prosessen. Inntrykket er at denne formen for grunnlagsdokumenter i liten grad er tatt i bruk.*
- *Tendensen er at sikkerhetsutfordringer knyttet til IKT-systemene i økende grad får oppmerksomhet. Fremdeles får fysisk infrastruktur mest fokus hos tre av informantene. To aktører oppgav at de var minst like opptatt av IKT-systemene og fysisk infrastruktur. Sistnevnte kan ha sammenheng med at informantene hadde IKT-faglig bakgrunn., hvilket antyder at IT-sikkerhetsledere som har relevant utdanning og kompetanse, naturlig nok er opptatt av forhold knyttet til sitt fagfelt.*
- *Den mest interessante oppdagelsen er misforholdet mellom bransjen og myndighetene når det kommer til varslingsrutiner. Informantene kritiserte den eksisterende praksisen, mens NVE opplevde at ordningen fungerte tilfredsstillende.*
- *Bransjen har etablert et sikkerhetsforum (SFK), hvor femten nettselskaper deltar. Her blir ulike tema om informasjonssikkerhet behandlet i årlige seminar.*

## 4.3 Hvilke tanker har informantene om risikoen for angrep på IKT-systemene?

*Informantene fikk mange spørsmål som omhandlet forhold knyttet til risikopersepsjon. Hensikten var å få innblikk i hvilke oppfatninger kraftbransjen har til trusselen om cyberkriminalitet.*

Respondentene var forholdsvis samstemte når det gjaldt forståelsen av begrepet ”angrep på ikt-systemene” - det være seg inntrenging, tjenestenekt eller trussel mot systemets integritet. Flesteparten forstod angrep på ikt-systemet enten som en villet handling utenfra eller at en ”intern utro tjener” foretok en ondsinnet gjerning.

Imidlertid var den en informant som formulerte det slik:

> **”Angrep på ikt-systemene har i seg interne trusler. Enten tjenestenekten ift. administrative nettet skyldes et uhell med en minnepinne eller at den er plantet der, kan effekten være den samme.” (**Respondent 3)

Det kan tyde på at vedkommende i tillegg inkluderte de utilsiktede hendelsene som gjerne kommer av mangel på kunnskap eller ”uforsiktighet”. Dette synet samsvarer med NVE sin forståelse av begrepet. De mener at dersom man kun ser på dataangrep ”utenfra og inn” begrenser man trusselbildet, da angrepet ikke nødvendigvis kommer via de logiske kanalene. BfKs bestemmelse av informasjonssikkerhet innbefatter ”fysisk sikring av rom, sentraler, datarom og overføringslinjer” (NVE).

På spørsmål om virksomheten har vært utsatt for angrep, svarte en informant ”ja” uten å utdype ytterligere. To oppgav at det ikke har vært angrep på SCADA- systemet, men mot virksomhetens IKT-system for øvrig. Flere rapporterte at de stadig ble angrepet av såkalt ”portscanninger”, som kan sammenlignes med at ”noen prøver å bryte seg inn, men blir stoppet ved ytterdøren” (NVE). En av virksomhetene fortalte at den siste måneden hadde de mottatt 310 virusinfiserte mail, og at ¾ av epostene var såkalt ”spam”. Under intervjuene ble det nevnt at det har vært snakk om å etablere et KraftCert, tilsvarende NSM, hvor informasjon fra hele kraftbransjen samles for å betrakte alle forsøk på angrep utenfra. Svakheten med en slik sektorbasert analyse, er at man kun vil få avdekket angrep via internett. Ifølge NVE har kraftselskapene plikt til å varsle dersom de opplever systematiske angrep fra en eller flere IP-adresser. Det finnes ikke mange slike rapporter, hvilket kan skyldes at slike angrep ikke fremkommer i loggene før i etterkant, og de blir dermed ikke blir oppdaget - alternativt at kraftselskapene faktisk ikke kontrollerer loggene.

Det var tilsynelatende en sprikende oppfatning av hvem trusselaktørene er. Flere nevnte ”gutteromshackere” eller terrorister og statsmakter som vil lage kaos. En respondent trakk frem at Norge sin innsats i Midtøsten kan hende øker sjansen for terrorisme. En informant poengterte at vi ikke nødvendigvis kan vite hvem trusselaktørene er:

> **”Cyberdomenet, da vet jeg ikke lenger hva de grensene betyr. Det behøver ikke være nasjoner som er trusselen, det kan også være miljøer. Det å lamme distribusjonsnettet kan ha en verdi for noen”** (Respondent 3).

I tillegg til at det er noe ulik oppfatning av hvem trusselaktørene er og hva motivet kan være, så virker det som om enkelte av informantene ikke opplevde dette som særlig aktuelt for deres virksomhet. En informant uttalte at det gjerne er tilfeldigheter som er avgjørende for om et system blir angrepet eller ikke. En annen vurderte det som mer sannsynlig at trusselaktøren i stedet ville angripe Statnett dersom de ønsket å ramme strømforsyningen, noe som kan få konsekvenser for hele landet. To av informantene vurderte sannsynligheten for angrep på IKT-systemene som ”svært liten”. Tre svarte ”lav sannsynlighet”, og en informant satte sannsynligheten til ”under en gang pr 50 år”. I den siste enheten ble sannsynligheter benyttet for å rettferdiggjøre sikkerhetstiltak. Å gi et generelt svar på sannsynlighet var ikke så interessant, da deres enhet er ”like interessante som alle andre virksomheter” (Respondent 3). Dette synet på sannsynlighet samsvarer med NVE, som også påpeker at sannsynlighet er vanskelig å ta stilling til. Det viktigste er å ha blikket rettet mot konsekvensene av et angrep på IKT-systemene.

> **”Vi skal vurdere konsekvensaspektet, sannsynligheten ligger og svever litt i bakgrunnen og korrigerer litt hvilket nivå du er. Man skal ikke ha overfokus på den delen (NVE).**”

Når det gjelder hvilke konsekvenser informantene tror et potensielt vellykket angrep på IKT-systemene vil medføre, svarte to av informantene at det var avhengig av hvor omfattende angrepet var. Frafall av nett er en stor konsekvens hvor det i verste fall kan være fare for liv og helse. Andre konsekvenser kan være at uvedkommende henter ut sensitiv informasjon, kobler ut forbruk, samt lammer infrastrukturen. En oppfatning er at det verste som kan skje, er at noen kobler ut og inn på driftskontrollsystemet, for potensielt å ødelegge et anlegg. Det kan i så fall ta lang tid å få det fikset, men stasjonene kan i mellomtiden bemannes manuelt uavhengig av IKT-systemene.

Halvparten av informantene oppgir at menneskelig svikt er den største trusselen mot IKT-systemene. Det kan f.eks. skyldes mangel på kunnskap.

> **”Så lenge det er mennesker inne i systemer, er det alltid en risiko for menneskelig svikt” (NVE).**

Virus kan også bli ”utilsikta overført ved patcher eller at nye filer skal inn i systemet” (Respondent 6). Særlig ved oppgradering og rekonfigurering kan det oppstå uønskede hendelser. Systemets kompleksitet med sine gjensidige avhengigheter kan dessuten føre til at:

> **”Man ser kanskje ikke konsekvensen før man er oppe i en kritisk situasjon, hvor systemet skulle reagert på den og den måten, og ikke gjør det” (Respondent 1).**

En informant trakk frem at ”hull i barrierer via interne, åpne kanaler” kan være en trussel mot IKT-systemene. Selv om det finnes et fåtall forbindelser mot omverdenen, kan det finnes hull/performering her. NVE rangerte EMP-trusselen som en av de med størst konsekvens. Denne oppfatningen ble ikke delt av de øvrige informantene, noe som vil bli belyst ytterligere under pkt. 4.3.1.

Samtlige respondenter karakteriserte gjeldende driftskontrollsystemer som tilstrekkelig sikre. En av forklaringene var at kraftbransjen har vært konservative når det gjelder å koble SCADA-systemet opp mot internett. Videre benyttes teknologiske løsninger etter ”beste praksis” som sikrer driftskontrollsystemene mot inntrenging, samt at anleggene EMP-sikres. I tillegg er det redundans i systemene ved at det eksempelvis finnes 2-3 servere. En informant svarte at systemene er tilstrekkelig sikre med tanke på ønsket funksjonalitet. Ny fremtidig teknologi vil imidlertid kreve mer investering i sikkerhetstiltak. NVE sa noe av det samme. Teknologiutviklingen har eskalert de siste 10-15 årene, og utfordringen blir at ”kraftselskapene får forståelse for hvilke teknologier de kaster seg på, slik at de ikke tråkker utover kravene regelverket tilsier” (NVE).

Selv om samtlige mente at driftskontrollsystemene er sikre, kom det indirekte frem hos fire av informantene at det var forhold ved systemene som ikke var optimalt behandlet. Det gjaldt eksempelvis mangelfull oppdatering av driftskontrollsystemene, mangelfull kontroll på hvordan leverandører ivaretar sikkerhet ved fjernstyring og manglende bevisstgjøring (holdningskampanjer), for å hindre ondsinna programvarer som de ansatte utilsiktet tar med inn i IKT-systemet. En informant innrømmet at gjeldende driftskontrollsystem har sikkerhetsutfordringer ved seg, men da dette skulle skiftes ut i løpet av de neste årene ville ikke ”hullene” bli tettet med tiltak. Ifølge NVE finner de mange avvik hver gang de er på tilsyn, hvilket impliserer ”at driftskontrollsystemene

ikke er tilstrekkelig sikre". At det er så mange aktører i kraftforsyningen, skaper likevel en viss robusthet.

> **"(…), med mindre de virkelig store faller ut. Oslo kan hjelpe mange, men det er ikke så mange som kan hjelpe Oslo" (NVE).**

Ved innføringen av AMS vil kraftforsyningen oppleve store teknologiske endringer. Informantene uttrykte bekymring for hvorvidt sikkerhetsutfordringer er tilstrekkelig forstått og ivaretatt. Det avhenger av hvor mange tilleggsfunksjoner som legges til, men åpnes det opp for en tredjepart, vil det særlig kunne øke sårbarhetene i systemet. Den ene informanten påpekte at man potensielt vil kunne møte på noen av de samme utfordringene som for et SCADA-system. Det betyr at en eventuell inntregning på AMS- systemet kan gjøre like stor skade og kanskje til og med større. Informantene, inklusiv NVE, var tilsynelatende samstemte i at sikkerhetstankegangen må ligge langt fremme i forhold til fremtidige teknologiske utfordringer.

### 4.3.1 Hvor "flinke" er kraftsektoren når det kommer til sikring?

NVE har i flere sammenhenger uttalt at kraftbransjen generelt er gode på sikring, men at det er mangler når det gjelder å planlegge for ekstraordinære hendelser med potensielt store konsekvenser. To av informantene sa seg enige i dette, men det ble samtidig nevnt at det er så stor variasjon over begrepet "ekstraordinære hendelser", hvilket vanskeliggjorde både å definere og planlegge for hendelsene. Tre informanter sa seg "litt uenig" i påstanden. Den ene begrunnet det med at det er viktigere å se på hvorvidt man er i stand til å ivareta en stabil og sikker strømforsyning, noe man er gode på. En av dem antydet at problemet er en mangelfull dokumentasjon av den beredskapen som faktisk finnes i organisasjonen. "Det er veldig mye beredskap oppi hodene på folk" (Respondent 1). En annen sa som følgende:

> **"Vi opplever nok at de er flinkere til å male fanden på veggen enn oss. Det er vår oppfatning, men sånn må del vel være skal noen gå foran."** (Respondent 4)

Kravet om EMP-sikring ble trukket frem av flere. Informantene opplever at de bruker mye ressurser på å tilfredsstille dette kravet. En sa at det var bortimot umulig å oppnå dette i eksisterende bygg, og at en må ”nesten bygge nye bygg” for å imøtekomme vilkårene.

> **”Hvis det er å være godt sikret, å ha store nye EMP-rom, ja så er vi kanskje godt sikret mot noe som ikke er så veldig sannsynlig. Så på en måte underkjenner jeg den innledende uttalelsen der.”** (Respondent 3)

*FUNN:*

- *Respondentene var relativt samstemte når det gjaldt hva de la i begrepet ”angrep på ikt-systemene”. Flesteparten forstod det som bevisste, ondsinnede handlinger utført av eksterne eller interne (utro tjenere) aktører. To informanter inkluderte utilsiktede hendelser, med bakgrunn i at konsekvensen er den samme. Dette synet samsvarte med NVE sin oppfatning.*
- *Det kan synes som om majoriteten ikke opplevde trusselen om angrep på ikt-systemene som en særlig prekær problemstilling. Denne påstanden viser blant annet til den enkeltes sannsynlighetsvurdering, og til noen av uttalelsene som peker i den retning. Det var imidlertid tre av respondentene som uttrykte seg mer ”positive” til at cybertrusselen er reell. Felles for disse var at menneskelig svikt tas med i risikobildet, dvs. manglende kunnskap eller utilsikta handlinger i forbindelse med oppgradering/konfigurering.*
- *En virksomhet rapporterte at de har opplevd angrep på ikt-systemene uten å utdype det ytterligere. Utover det opplyste samtlige at de ofte blir utsatt for ”portscanninger”. NVE har mottatt få meldinger om at selskaper har opplevd angrep. Det kan også skyldes at angrepene ikke blir oppdaget.*
- *Driftskontrollsystemet (SCADA-systemet) oppfattes som tilstrekkelig sikre system. NVE finner mange avvik hver gang de er på tilsyn, så de konkluderte med at det systemet ikke er sikre nok. At det er så mange aktører på markedet, utgjør en viss robusthet med mindre de store nettselskapene faller ut.*

## 4.4 Informasjonssikkerhetstiltak

*For å betrakte hvilke forestillinger kraftbransjen har til informasjonssikkerhetstiltak ble Hagen et al. [7] sin kategorisering benyttet, for på denne måten å unngå å berøre informasjon som var av sensitiv karakter. Det skilles mellom følgende organisatoriske og teknologiske tiltak:*

1. Sikkerhetspolicy
2. Metoder og verktøy
3. Prosedyrer og kontroll
4. Bevisstgjørende tiltak
5. Teknologiske tiltak

Figur 11 Organisatoriske og teknologiske tiltak

Samtlige kjente seg igjen i og var komfortable med denne type inndeling av tiltak, selv om de ikke foretok tilsvarende systematisering i egen virksomhet. Bakgrunnen for valg av tiltak var myndighetskrav, interne krav og resultat fra ROS-analyser. En informant trakk frem at det er viktig å ha grep om sannsynlighet, ”er det realistisk at vi kan bli utsatt for den type trussel, eller er det litt for eksotisk” (Respondent 3)? Oppgradering av IKT-systemet eller innføring av ny type kommunikasjon, samt eventuelle varsler om eksterne trusler vil også ha betydning for valg av tiltak.

Alle virksomhetene som deltok i denne undersøkelsen, oppgav at de har en sikkerhetspolicy som var forankret i ledelsen. Det er noe ulik praksis i hvilken grad denne policyen blir formidlet nedover i organisasjonen. Enkelte informanter svarte at innholdet i denne ble tatt opp på eksempelvis avdelingsmøter eller formidlet gjennom linjeorganisasjoner. Hos andre lå dokumentet tilgjengelig på intranett. NVE tilføyde i denne sammenheng at de ser stor forskjell når det gjelder ledelsesengasjement. Enkelte ledere er ”ildsjeler” og er brennende opptatt av det som angår informasjonssikkerhet, mens andre har en mer delegerende holdning.

To av virksomhetene har gjennomført holdningskampanjer internt, e-læringskurs, for alle ansatte. Tilbakemeldingen har vært meget positiv. Ytterligere en informant har fremmet forslag om å gjennomføre tilsvarende kampanjer, men hadde ikke fått

tilbakemelding fra konsernledelsen på daværende tidspunkt. Når det kommer til *kompetanseheving*, gis de ansatte anledning til å delta på seminar og konferanser. Tendensen når det gjelder *bevisstgjørende tiltak*, er at dette er et område som ikke følges opp systematisk i kraftbransjen. De ansatte har selv plikt til å sette seg inn i eksisterende brukerinstrukser og sikkerhetshåndbøker. Et interessant funn er at de informantene som har gjennomført e-læringskurs, også har satt bevisstgjørende tiltak høyt oppe på listen da de ble bedt om å rangere de ulike kategoriene (jf fig. 4.1.) Tilsvarende har de informantene som ikke gjennomførte systematiske holdningsskapende kampanjer, rangert slike tiltak langt nede på listen.

Samtlige tok i bruk taushetserklæringer både overfor medarbeidere og eksterne aktører som gis tilgang til IKT-systemene eller får kjennskap til forhold som betegnes som sensitiv informasjon. Taushetserklæringer ble ikke nødvendigvis oppfattet som et beskyttende tiltak i seg selv.

> **"Det er viktig å sette krav til hva man kan gjøre og ikke, og som kan brukes som et verktøy dersom personellet ikke oppfyller kravene" (Respondent 6).**

I tillegg benyttet virksomhetene kontrollfunksjoner, som logging av aktiviteten på driftskontrollsystemene, avvikssystem, prosedyrer og adgangskontroll til bygget. En informant påpekte at det var "for svakt med kontroller". Utover det var den generelle oppfatningen at virksomhetene hadde tilstrekkelig med prosedyrer og kontrollfunksjoner. NVE hevdet at mange selskaper har gode prosedyrer for å beskytte eksempelvis dataanleggene, men at bevisstheten ikke nødvendigvis er så stor utover det. De påpekte at mange vil ha god nytte av å utføre interne revisjoner.

> **"I og med at vi finner så mye avvik, så er det jo et tegn på at det burde være bedre interne systemer og kontroller" (NVE).**

Sikkerhetskulturen beskrives som god hos de fleste. En informant påpekte at de var i en modningsprosess og at de ikke har hatt nok fokus på sikkerhet. En annen sa følgende

> **"Det kunne sikkert vært bedre, men vi ivaretar sikkerheten på en god måte ift. samfunnsoppgaven vår som er levere sikker strømforsyning (Respondent 2).**

NVE fikk æren for at sikkerhetskulturen ansees som god, da de som tilsyn har skapt en kultur over mange år. Ifølge NVE sin respons, er det tilsynelatende en betydelig tilgjengelighetskultur som går på at "anleggene skal virke". Men de opplever at

sikkerhetskulturen og oppmerksomheten mye lavere i kraftbransjen ift. trusselen om cyberkriminalitet.

Det var en blandet oppfatning om hvorvidt konsernledelsen var opptatt av denne type trusler. To av informantene opplevde sterkt engasjement fra ledelsen, mens andre merket ikke så mye til dette i det daglige. En informant sa det slik:

> **"Hvis du spør dem svarer de nok ja. Å merke noe av det til daglig, det er ikke lett. Det blir ikke prioritert (Respondent 4)"**

En annen informant opplevde at ledelsen var raskt på banen dersom det oppstod kritiske situasjoner, som f.eks. Stuxnet. Utover det ble ansvaret gitt til de som driver med det til daglig, hvilket samsvarer med NVE sin oppfatning.

På spørsmål om hvorvidt teknologiske eller organisatoriske tiltak anses som mest effektive barrierer mot cyberkriminalitet, svarte de fleste at det er kombinasjonen som skaper det beste resultatet. Man trenger altså begge deler. En informant var imidlertid tydelig på at organisatoriske tiltak er det mest effektive.

> **"Det hjelper ikke hvor mye tiltak som brannmurer, IDS eller IPS (…), du klarer å hacke deg inn i Pentagon og da sier det litt om de teknologiske barrierene" (Respondent 1).**

En annen påpekte at man ikke må se seg blind på tekniske løsninger, for systemene er sårbare for det som skjer fra innsiden - eksempelvis av menneskelig svikt. NVE tilføyde i denne sammenheng at det er viktig at de ansatte forstår hvorfor tiltakene er der, og lojalt følger dem for at en skal oppnå effekt.

*FUNN:*

- *Fire informanter mente at sikkerhetspolicy bør være det "første" tiltaket som implementeres i bedriften. Policyen var forankret i ledelsen hos alle, men hvordan denne ble formidlet nedover i systemet, fortonet seg ulikt.*
- *Tre aktører vurderte effekten av bevisstgjørende tiltak (f.eks. holdningskampanjer) som nr to. Ikke overraskende er det de samme virksomhetene som enten har erfaring med et slikt tiltak, eller har ønske om å gjennomføre en kampanje, som plasserte dette tiltaket "høyest" på rangeringen.*

*To informanter har vurdert bevisstgjørende tiltak som det informasjonssikkerhetstiltaket med lavest effekt.*

- *Taushetserklæringer og øvrige prosedyrer var implementert hos alle de undersøkte.*
- *I og med at det er så få porter som kobler sammen SCADA-systemet og det administrative systemet, virker det som om virksomhetene i stor grad hadde tiltro til at de teknologiske tiltakene (f.eks. brannmurene), stanser det meste av angrep som måtte komme mot IKT-systemene via det administrative nettverket.*
- *Kun to informanter oppgav at ledelsen var engasjert i risiko knyttet til IKT-systemene. De resterende merket ikke så mye til dette i det daglige.*
- *Fem respondenter oppgav at det er kombinasjonen av teknologiske og organisatoriske tiltak som utgjør det beste resultatet. Det var kun en som mente at organisatoriske tiltak er det viktigste.*

## 4.5 Oppsummerende kommentar

Det er tilsynelatende store variasjoner blant de undersøkte selskapene av hvor opptatt man er av cyberkriminalitet, og hvorvidt man anser det som en realistisk trussel eller ikke. Enkelte av informantene var svært engasjerte, og mange av svarene deres gav uttrykk for at også ledelsen tok problemstillingen på alvor. Ut fra empirien er det grunn til å spekulere i hvor stor grad den faglige bakgrunnen har betydning for hvordan man betraktet risikoen for angrep på IKT-systemene. De informantene som hadde en it-faglig bakgrunn, var formodentlig mest dedikerte overfor problematikken. I tillegg var de rimelig samstemte i forhold til hvilke sikkerhetsutfordringer kraftbransjen står overfor. Menneskelig svikt ble vurdert som en av hovedtruslene mot IKT-systemet, og bevisstgjøring og kompetanseheving av de ansatte ble sett på som nødvendige virkemidler for å forebygge denne type utilsiktede hendelser. Dataene som foreligger, viser at personene med Elkraft-faglig bakgrunn tilsynelatende uttrykte større tiltro til de teknologiske barrierene. I tillegg var de ikke så bekymret for at svikt i IKT-systemene nødvendigvis ville ha betydning for forsyningsevnen, da anleggene kan driftes manuelt ved behov.

Det var noen uoverensstemmelser mellom hvordan myndighetene (NVE) og bransjen tenkte omkring følgende:

- Når NVE førere tilsyn, finner de mange avvik i forhold til driftskontrollsystemene, hvilket tyder på at sikkerheten ved systemene ikke tilfredsstiller vilkårene i beredskapsforskriften. Bransjen derimot, oppfattet systemet som tilstrekkelig pålitelige, ut fra ønsket funksjonalitet.
- NVE trakk frem konsekvensene av en EMP-hendelse som en av de største utfordringer for driftskontrollsystemet. Denne rangeringen og prioriteringen ble ikke delt av respondentene.
- Ifølge respondentene ble gjeldende varslingsrutiner oppfattet som lite effektive, blant annet fordi de opplevde at varslingen kom for sent, og gjerne til feil mottaker i selskapet. NVE på sin side mente at rutinene fungerte tilfredsstillende. De kommenterte at dersom det er svakheter ved selskapenes interne viderevarsling, så er dette forhold som må sees nærmere på.
- Med ett unntak opplyste informantene at sikkerhetskulturen i virksomheten ble ansett som tilfredsstillende. NVE var enige i at *tilgjengelighetskulturen* er god, men at det er forbedringspotensial ved sikkerhetskulturen og oppmerksomheten knyttet til cyberkriminalitet.

# 5 Diskusjon

I dette kapittelet vil de empiriske funnene som foreligger, sees opp mot utvalgt teori. Hensikten er å drøfte de elementene som anses for relevante i forhold til å kunne svare på problemstillingen. Diskusjonsdelen er tredelt og tar utgangspunkt i analysemodellen som ble presentert under pkt. 2.5. I den første delen drøftes forhold som bidrar til å forklare hvordan kraftselskapet vurderer trusselen om cyberkriminalitet. Hvilken tilnærming virksomhetene har til risiko, samt ulike sider ved risikopersepsjon vil være aktuelt å kommentere i denne sammenheng.

I del to vil jeg diskutere ulike aspekter ved risikostyringsprosessen opp mot teori om kollektiv sensemaking og gruppeprosesser. I tillegg vil jeg videreføre den pågående debatten om bruken av risikoakseptkriterier i ROS-analysene, med utgangspunkt i hvorvidt den forhåndsbestemte kategoriseringen fremmer eller hemmer kollektiv sensemaking.

Den tredje og siste delen tar for seg ulike faktorer som kan være gjeldende for valg av informasjonssikkerhetstiltak. I tillegg er det interessant å betrakte hvilke tanker informantene hadde i forhold til teknologiske og organisatoriske tiltak, sett i lys av Hagen et al. sin artikkel ”Implementation and effectiveness of organizational information security measures” [7].

## 5.1 Risiko og persepsjon

Under dette punktet, diskuteres forhold som kommer innunder den stiplete sirkelen i analysemodellen.


Figur 12 Analysemodell: Risikopersepsjon

Risikopersepsjon handler om hvilken mental forestilling man har av en gitt aktivitet. Som forklart i teorikapittelet (jfr. pkt. 2.3), er mange forhold med på å forme denne mentale konstruksjonen, det være seg psykologiske, sosiale eller kulturelle faktorer. Det empiriske materialet gir kun opplysninger om hvilken fagbakgrunn informantene har. Informantene blir derfor betraktet som representanter for kraftselskapet, og det forutsettes at de uttaler seg på vegne av virksomheten og ikke i lys av sin egen person. I denne sammenheng omtales kun de elementene som er listet opp i analysemodellen. Korrelasjonen mellom risikopersepsjon og kollektiv sensemaking illustreres med en pil i analysemodellen (jfr.fig.12). Denne indikerer at forhold som omtales i dette delkapittelet, ansees å ha innvirkning på den kollektive sensemakingen som foregår i kraftselskapet.

### 5.1.1 Utfordringen med å beregne sannsynlighet og konsekvens

Risikobegrepet ble omtalt og definert tidligere i oppgaven. Her ble forskjellen mellom den tradisjonelle[11]- og alternative[12] tilnærmingen til risiko tydeliggjort (jfr. pkt. 2.1.1). Det er vanskelig å konkludere med hvordan kraftbransjen oppfatter trusselen om cyberkriminalitet, dersom man ikke har grep om hvilket perspektiv på risiko som legges til grunn. Samtlige informanter fikk derfor spørsmål om hvordan de fastsetter sannsynlighet og konsekvens i sine risikoanalyser av driftskontrollsystemene. I en risikoanalyseprosess er det gjerne flere ulike fagmiljøer og tradisjoner representert, hvilket kan være en utfordring når de skal samarbeide om problemstillinger som omhandler risiko [2].

Den tradisjonelle tilnærmingen til risiko legger stor vekt på tidligere hendelser (historiske data) når sannsynlighet skal beregnes [1]. I denne sammenheng kan historiske data forstås som de erfaringene den enkelte virksomhet har med dataangrep, bransjen for øvrig eller hvorvidt den internasjonale kraftsektoren har vært rammet av cyberkriminalitet. Hvilke erfaringer har deltakerne i denne undersøkelsen av dataangrep? En informant opplyste at de hadde opplevd angrep på IKT-systemene uten å utdype dette ytterligere. En annen sa at virksomheten, men ikke datakontrollsystemet, hadde vært utsatt for datakriminalitet. De øvrige deltakerne formidlet at de ofte opplevde portscanninger, dvs. at noe eller noen ”der ute i cyberspace” prøvde å finne hull som gav tilgang til systemet. Portscanninger ble imidlertid ikke oppfattet som angrep. Det er altså registrert få tilfeller av sabotasjehandlinger mot norsk kraftforsyning, både den fysiske infrastrukturen og ikt-systemene [17]. Selv om det finnes eksempler på at kraftforsyningen i andre land har vært utsatt for hacking, deriblant Stuxnet-angrepet, er det likevel få historiske data knyttet til angrep på driftskontrollsystemene [21]. Aven et al. [1] fremhever at manglende målinger (data) gjør at beregning av sannsynlighet og konsekvens gir etter det tradisjonelle perspektivet, svært usikre estimater.

11 Tradisjonell tilnærming: Risiko= sannsynlighet x konsekvens

12 Alternativ tilnærming: Risiko= kombinasjonen av mulige konsekvenser og tilhørende usikkerhet

Dette studiet fokuserer på trusselen om cyberkriminalitet, hvilket forstås som tilsiktede uønskede hendelser mot IKT-systemene. Å betrakte risiko ut ifra det tradisjonelle synet når det gjelder målrettede angrep vil være problematisk, p.g.a. at sannsynlighet og konsekvens er beheftet med stor usikkerhet. Eksempelvis er den potensielle angripers motiver og muligheter (ressurser) for å ramme kraftforsyningen, ukjent for analysegruppen. Risikobegrepet må altså tilnærmes på en annen måte, en oppfatning samtlige informanter tilsynelatende deler. En informant uttrykte eksempelvis at de benyttet en tradisjonell tilnærming til risiko, men at de ikke var så opptatt av tallene. "Mageføelelsesverdien" var mer retningsgivende. Kompetanse og erfaring ble ansett som de viktigste elementene i vurderingen av sannsynlighet og konsekvens. I tillegg var det nødvendig å være fremsynte og forsøke å tenke ut "det ukjente". Dette stemmer overens med Sivertsen [5] som poengterer at det er spesielt vanskelig å vurdere sannsynlighet for de IKT-systemene som opereres med i kraftforsyningen, da "en angripers muligheter for å utnytte et system i verste fall baserer seg på totalt ukjente sårbarheter".

Selv om det ikke nødvendigvis var et bevisst valg, kan det virke som om respondentene i praksis benyttet en variant av Aven sin alternative tilnærming, der risiko forstås som "en kombinasjon av mulige konsekvenser (utfall) og tilhørende usikkerhet" [2 og 47]. På grunn av at det i liten grad finnes erfaringsdata knyttet til cyberkriminalitet, samt at komplekse ikt-systemer kjennetegnes av mange ukjente faktorer [27 og 30], er det alternative synet mest egnet i denne sammenheng.

### 5.1.2 Dataangrep eller ikke dataangrep?

Ledelsesengasjement er den første faktoren som ventes å kunne påvirke risikopersepsjonen. Her ligger det en antakelse om at hvorvidt ledelsen prioriterer og setter cyberkriminalitet på dagsorden, har betydning for hvordan medarbeidere på lavere nivå betrakter denne trusselen. Av de kraftselskapene som ble undersøkt, var tilsynelatende både sterkt ledelsesengasjement og mindre involvert ledelse representert, noe som samsvarer med det inntrykket NVE har av bransjen. De hevdet at enkelte toppledere fremstår som ildsjeler i forhold til beredskap generelt, mens andre har et mer delegert forhold og har tiltro til de som er ansvarlige nedover i systemet. To av informantene var kun ansatt i en 50 % - stilling, hvilket kan tolkes dit hen at ledelsen ikke prioriterte denne aktiviteten. Begge opplevde at de ikke hadde nok tid til å følge

opp alle arbeidsoppgaver som var ønskelig. En informant gav uttrykk for at ledelsen kom raskt på banen dersom det skjedde noe ekstraordinært, men i det daglige var ansvaret lagt på de som driftet SCADA-systemet. Felles for de to informantene som opplevde et sterkt ledelsesengasjement, var at begge hadde gjennomført holdningskampanjer for alle de ansatte i virksomheten. Av de seks undersøkte, var det også disse som tilsynelatende vurderte muligheten for at noe tilsiktet eller utilsiktet kunne tilfalle IKT-systemene høyest. Risikopersepsjon formes av de erfaringene man har av den gitte aktiviteten [16]. Et av selskapene hadde som tidligere nevnt, opplevd angrep på IKT-systemene, hvilket kan bidra til å forklare det sterke ledelsesengasjementet. Funnet indikerer samtidig at dersom ledelsen setter informasjonssikkerhet høyt på dagsorden, vil det også kunne påvirke hvordan organisasjonen forøvrig vurderer muligheten for et dataangrep.

Har gjeldende trusselbilde betydning for hvordan kraftsektoren oppfatter risikoen for cyberkriminalitet? I hovedsak er det to etater som holder fortløpende oversikt med trusselnivået i Norge. Først og fremst har Politiets sikkerhetstjeneste (PST) en sentral rolle i denne sammenheng, blant annet ved å utarbeide generelle og periodiske trusselvurderinger[13]. I tillegg har Nasjonal sikkerhetsmyndighet (NSM) ansvar for å holde oversikt med sikkerhetssituasjonen for samfunnskritisk infrastruktur. Årlige rapporter fra PST og NSM kan gi informasjon om hvordan trusselen om cyberkriminalitet mot kraftforsyningen vurderes. NSM utgir i tillegg rapporter som beskriver status for sikkerhetsnivået i norske bedrifter [14]. Empirien viser imidlertid at slike rapporter i liten grad benyttes som grunnlag for ROS-analysene. En informant påpekte at de offentlige og tilgjengelige rapportene var ubrukelige for deres del. Det var imidlertid andre respondenter som opplevde det nyttig de gangene NSM deltok på sikkerhetskonferanser som arrangeres av og for kraftbransjen. På den måten fikk virksomhetene informasjon om trusselbildet, som igjen ble tatt til betraktning i ROS-analysene.

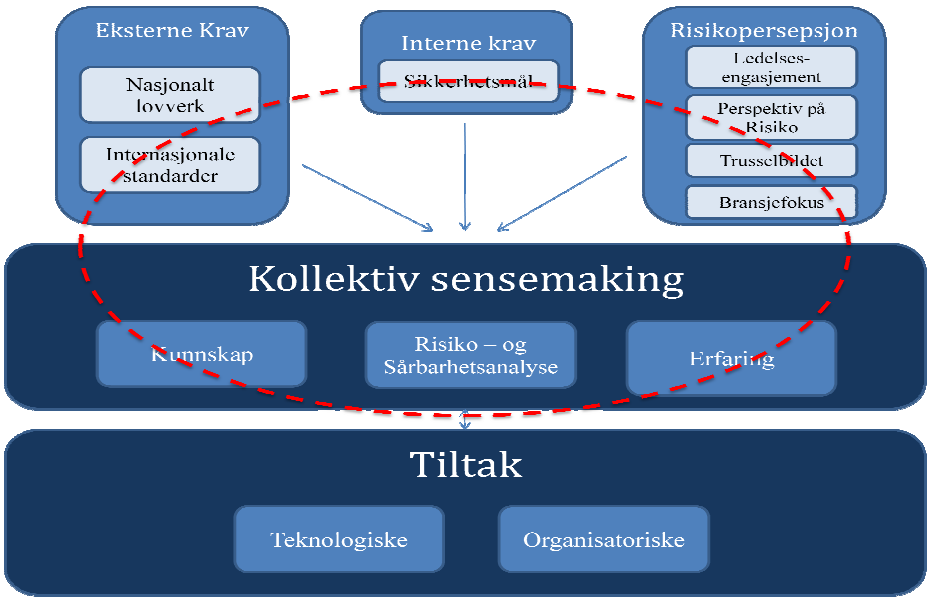
13 http://www.pst.politiet.no/PST/Templates/Article____387.aspx

Litteraturen fremhever medias rolle som formidler av risiko [16]. Bortsett fra en informant som opplyste om at de fikk kjennskap til Stuxnet først gjennom media, gir empirien angivelig ingen svar på hvorvidt kraftbransjen lar seg påvirke av den informasjonen som formidles via mediekanalene. Uavhengig av om det er media eller myndighetene som opplyser om mulige trusler mot IKT-systemene, har trusselbildet tilsynelatende innvirkning på hvordan kraftselskapene forholder seg til risikoen. Flere informanter sa at dersom det ble endring i trusselbildet, ble det gjennomført en oppdatering av ROS-analysen. I en bedrift innførte de sikringstiltak i det øyeblikket de fikk kjennskap til Stuxnet-angrepet, selv om denne trusselen ikke var dirkete rettet mot norske virksomheter. Dette funnet kan sees i lys av Slovic et al. [28] sin forskning, som viser at ”fryktfakoren”, dvs. graden av oppfattet risiko, har sammenheng med ønsket om å iverksette risikoreduserende tiltak.

Det kom frem av intervjuene at risiko knyttet til IKT-systemene har fått økt fokus i kraftforsyningen de senere år. I analysemodellen finnes det et punkt under risikopersepsjon som er kalt ”bransjefokus”, hvilket involverer tilsynsmyndighetenes rolle og et bransjestyrt sikkerhetsforum. Fokuset tilsynsmyndighetene har på informasjonssikkerhet, ble tilegnet mye av æren for at kraftsektoren var opptatt av dette. De følger opp virksomhetene i forhold til sikkerhet og beredskap etter gjeldende lovverk, og har de senere årene hatt særskilt fokus på forhold ved informasjonssikkerhet. Bransjen har dessuten valgt å danne et sikkerhetsforum bestående av om lag femten av de største nettselskapene i kraftsektoren. Hensikten er å behandle relevante problemstillinger, som f.eks hvordan myndighetenes varslingsrutiner kan bli bedre. En informant påpekte at forumet var en av hans viktigste arenaer for kompetanseheving i forhold til jobben som it-sikkerhetsleder. Her deltar personer med både IT-faglig og Elkraft-faglig bakgrunn, hvilket kan bidra til å skape en felles forståelse av de utfordringene bransjen står overfor. På en måte kan man si at det foregår en kollektiv sensemaking i forumet på tvers av organisasjoner, noe den enkelte representant kan videreføre i egen virksomhet.

## 5.2 Kollektiv sensemaking i kraftforsyningen

Hensikten med denne oppgaven er å forsøke å avsløre hvordan kraftbransjen oppfatter risikoen for angrep på driftskontrollsystemene, samt å betrakte hvilke faktorer som kan påvirke valg av informasjonssikkerhetstiltak. Kollektiv sensemaking er således relevant da teorien i hovedsak handler om de prosessene som fører til at en gruppe eller organisasjon kommer frem til en felles forståelse av en gitt aktivitet, og som materialiseres i handling [16].




Figur 13 Analysemodell: kollektiv sensemaking

Som fig. 13 illustrerer, forutsettes det at den kollektive sensemakingen drives frem av risikopersepsjon, samt de interne og eksterne kravene som foreligger. Den kollektive sensemakingen avgrenses til å foregå i risikoanalyseprosessen, hvor deltakernes kompetanse (kunnskap og erfaring) tillegges en sentral rolle.

### 5.2.1 Risikostyringsprosessen som arena for kollektiv sensemaking

Med hjemmel i BfK § 6-1 pålegges virksomhetene å foreta fortløpende helhetlige vurderinger av informasjonssikkerheten. Videre skal risikoanalyser danne grunnlaget for valg av tiltak, jfr. BfK § 1-3. Kraftselskapene bestemmer selv hvordan de ønsker å gjennomføre slike analyser, og NVE medgir at det er store forskjeller på hvor omfattende ROS-analysene av ikt-systemene er. Det har gjerne sammenheng med

størrelsen på selskapet og hvor profesjonelle organisasjonene er på IKT-området. Samtlige informanter har gjennomført risikoanalyse av driftskontrollsystemene. Selv om de til dels har tatt utgangspunkt i ulike metodikker, virker det som om alle har et reflektert forhold til selve analyseprosessen. Målet med en risikoanalyse er å gjøre systemet mer robust mot uønskede hendelser [5]. Utfordringen er å komme på alle ting som kan tilfalle SCADA-systemet, noe informantene tilsynelatende var svært bevisste på. For det første skilte de mellom tilsiktede og utilsiktede hendelser, hvilket samsvarer med de anbefalingene som fremkommer av BAS 5-rapporten [5]. I tillegg var de tydelige på at det var viktig å tenke kreativt og inkludere ”det usannsynlige” i denne prosessen. Det var noe variasjon av hvor mange som deltok i ROS-analysen. I en virksomhet var det kun en til to deltakere, mens de øvrige respondentene gav uttrykk for at analysegruppen bestod av erfarne og kompetente folk fra ulike nivå i organisasjonen.

Samtlige informanter oppgav at de gjennomførte en brainstorming når fareidentifikasjon skulle fastsettes. Gruppedeltakerne fikk dermed bruke den erfaringen og kompetansen de hadde, for å belyse hvilke hendelser SCADA-systemet kan utsettes for. Brainstorming kan betraktes som en del av den dialogbaserte samhandlingen kollektiv sensemaking legger vekt på [26]. Gjennom kommunikasjonen avdekkes ulike fortolkninger basert på hvilke erfaringer man har gjort seg i tidligere sammenhenger, og gruppen kan deretter bli enige om hvilke uønskede hendelser som skal analyseres i fortsettelsen. En informant påpekte at det var viktig Forutsatt at de involverte engasjerer seg og utnytter den kompetansen som finnes i gruppen, kan en risikoanalyseprosess være en arena hvor informasjon blir presentert og ivaretatt. Imidlertid finnes det underliggende mekanismer som kan forstyrre informasjonsflyten. Ofte kan gruppedeltakerne være så opptatt av å komme til enighet at relevant informasjon ikke blir lagt merke til. Turner [33] var tydelig på at mangler ved kommunikasjonen kan føre til at nødvendig informasjon blir misforstått eller ikke når frem til riktig mottaker. I en ROS-analyse kan dette føre til at man ikke har oversikt over alle alternativer, og dermed iverksetter de feil tiltak som følge av det. Empirien avslører ingen forhold som kan bekrefte eller avkrefte hvilke mekanismer som har vært gjeldende i risikoanalyseprosessen. For å få tilgang til den informasjonen måtte man ha gjennomført en deltakende observasjon av gruppemøtene, samt foretatt individuelle intervjuer med alle de involverte. Først da kunne man ha uttalt seg om eksempelvis ”gruppepolarisering” eller ”falsk konsensus” som styrende for gruppeprosessen [31].

Analysegruppen benytter den kunnskapen og erfaringen som er tilgjengelig på gjeldende tidspunkt for å komme frem til en felles forståelse av risikoer, og som deretter realiseres i handling [24].

### 5.2.2 Et kraftsystem – to fagdisipliner

I henhold til BfK § 6-1 skal det utpekes en *datakyndig* IT-sikkerhetsleder, men det stilles ingen krav om at vedkommende skal ha en formell IT- kompetanse. Av de virksomhetene som ble undersøkt, hadde om lag halvparten av it-sikkerhetslederne en elkraft-faglig bakgrunn. Samtlige respondenter opplever driftskontrollsystemene som tilstrekkelige sikre system, og de vurderer sannsynligheten for et målrettet angrep som svært liten. Ut i fra det empiriske datamaterialet kan det likevel virke som at de ulike fagtradisjonene har en noe avvikende oppfatning av hvilke trusler som følger av IKT-systemene. En tendens er at vedkommende med IT-faglig kompetanse la størst vekt på risikoen for menneskelig svikt, og han pekte på at driftskontrollsystemet vil reagere på samme måte uavhengig av om svikten skyldes en tilsiktet eller utilsiktet handling. Det virker som informantene i tillegg vurderte konsekvensene ulikt når det gjaldt potensiell svikt i SCADA-systemet. Etter forfatterens mening kan det virke som om informantene med elkraft-faglig bakgrunn i større grad gav uttrykk for at det finnes redundans i systemet, ved at kraftanleggene kan driftes manuelt dersom det skulle oppstå svikt i driftskontrollsystemet. En mulig forklaring er at de har solid kunnskap til damanleggenes funksjonalitet og oppbygging, samt at deres kunnskap om systemene strekker seg tilbake til tiden før IKT-systemene overtok overvåking og fjernstyringen av anleggene.

Sjøberg og Drottz-Sjøberg [29] har funnet at det ofte er misforhold mellom hvordan eksperter og lekfolk oppfatter risiko av en gitt aktivitet eller situasjon, noe som kan tilskrives graden av oppfattet kontroll eller hvor mye kunnskap man har om risikoen. I dette tilfellet kan verken den IT- eller elkraft-faglige medarbeideren karakteriseres som ”lekmann”, da begge har mye kunnskap om kraftsystemet. Begge partene kan derimot betegnes som ekspert innen sitt kompetanseområde. Det spesielle med kraftforsyningen er at både IKT-systemet og den fysiske infrastrukturen er avhengig av hverandre, noe som forutsetter et godt samarbeid og god dialog mellom fagdisiplinene.

### 5.2.3 Utfordringer i risikoanalysen av driftskontrollsystemet

Egenskaper ved den komplekse IKT-teknologien utfordrer ROS-analysen av driftskontrollsystemet. Tidligere var det ansatte ved hvert kraftforsyningsanlegg som overvåket og betjente installasjonene, og kompetansen omkring "den gamle" teknologien fikk utvikle seg over lang tid på bakgrunn av "lessons learnt" [12]. Nå står kraftbransjen imidlertid overfor hurtige teknologiske endringer som dermed representerer nye og ukjente farer [30]. Innføring av AMS[14] og smartgrid[15] er eksempler på it-løsninger som vil bli en del av de fremtidige tjenestene i kraftsektoren [11]. Weick [27] fremhever at nyere teknologi vanskeliggjør sensemakingen, blant annet fordi den består av usikkerheter og mange ukjente faktorer. Det skyldes at mennesket ikke nødvendigvis er i stand til å konstruere mentale modeller som stemmer overens med teknologien. Denne utfordringen ble også problematisert under intervjuene, blant annet med tanke på den forestående innføringen av AMS. Samtlige informanter uttrykte bekymring for hvorvidt sikkerhetsutfordringene er tilstrekkelig forstått og ivaretatt. Særlig dersom det åpnes for tredjepart, vil det kunne øke sårbarhetene i systemet. Videre fremhevde en respondent at systemleverandørene tradisjonelt ikke hadde hatt nok fokus på sikkerhet, men at dette hadde bedret seg noe. Likevel kan man undre seg over om de som faktisk utvikler IKT-systemene som benyttes i kraftforsyningen, fremdeles er mer opptatt av funksjonalitet fremfor sikre løsninger. Dette er forhold som kraftselskapene må være svært bevisste på i tiden fremover.

I tillegg til å forstå driftskontrollsystemet, skal analysegruppen vurdere hvilke eksterne trusler systemet potensielt står overfor [4]. Beredskapsforskriften § 6-1 krever at kraftselskapene planlegger for ekstraordinære hendelser med potensielt store konsekvenser [3]. NVE er av den oppfatning at bransjen ikke ivaretar dette kravet på en tilfredsstillende måte, noe informantene i varierende grad var enige i. Det ble blant annet kommentert at begrepet "ekstraordinære hendelser" favner så stort, at det er

14 AMS: avanserte måle- og styringssystemer

15 Smartgrid: AMS gir grunnlag for intelligente strømstyringstjenester og toveisfunksjonalitet, gjerne kalt smartgrid/smartnett

vanskelig både å definere og planlegge for hendelsene. NVE har i sin veileder til ROS-analysene utarbeidet flere sjekklister som kan benyttes i disse prosessene [4]. Det kan være hensiktsmessig å benytte sjekklister og andre rapporter for å justere eller legge til farer som kan utgjøre en sårbarhet i et IKT-system [5]. Ifølge dataene som er samlet inn, brukte de fleste virksomhetene sjekklister for å identifisere objekter som skulle analyseres. Offentlige rapporter (f.eks. NSM og PST) og ISO-standarder ble i liten grad benyttet i ROS-analysen. Kun en informant oppgav at de tok utgangspunkt i ISO-standarder i risikoanalysen av IKT-systemet. Det empiriske grunnlaget avdekker ikke noen tydelige årsakssammenhenger til den manglende utnyttelsen av slike dokumenter.

### 5.2.4 Risikoaspektkriterier – til hjelp eller hinder?

Som nevnt i teorikapittelet foregår det for tiden en debatt om bruken av risikoakseptkriterier. Aven [2] hevder at denne metoden er for instrumentell og tar verken hensyn til folks opplevelse, eller om risikoreduserende tiltak i det hele tatt er mulig å gjennomføre. NVE, på sin side, anbefaler virksomhetene å fastsette en øvre risikogrense [4]. Begge synene var representert blant informantene. Grunnen til at risikoakseptkriterier dedikeres med et eget avsnitt i denne sammenheng, er spørsmålet om hvilken betydning denne type kategorisering har for kollektiv sensemaking.

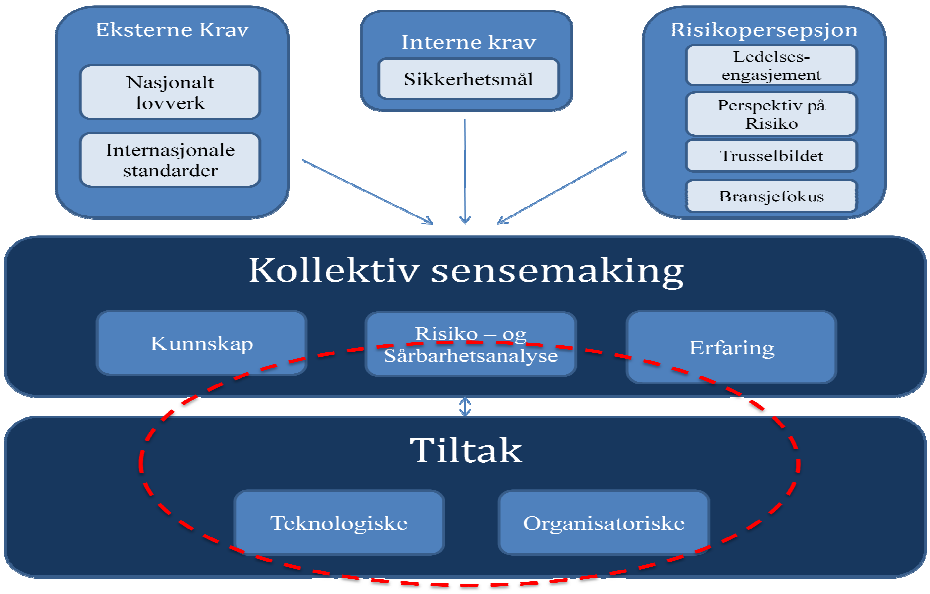
Sensemaking handler i stor grad om å organisere og kategorisere den informasjonen som finnes på det gjeldende tidspunktet [24]. Dersom myndighetskrav, interne krav og ledelsens oppfatninger ligger til grunn for fastsettelsen av risikoakseptnivå, kan slike forhåndsbestemte kategorier muligens hjelpe gruppen til å komme frem til en felles forståelse av risiko. Det forutsetter imidlertid at risikoakseptkriteriene er fastsatt på forhånd. En informant fortalte at han hadde opplevd ganger der grensene ble justert etter at resultatene av analysen forelå. Motivasjonen var å tilpasse risikobildet ut ifra økonomiske hensyn. Denne praksisen er helt mot sin hensikt, noe også Aven påpeker. Dersom deltakerne blir for opptatt av å unngå å falle i den ”røde sonen”, kan det gå på bekostning av sikkerheten [2]. NVE har også presisert i sin veiledning til ROS-analyser, at virksomhetene må ”sette inn innsatsen der hvor risikoen er høyest, og man oppnår størst risikoreduserende effekt av å sett inn tiltak” [4].

I en annen virksomhet manglet det et overordnet prinsipp om akseptabelt risikonivå som gikk fra ledelsen og nedover i organisasjonen. De retningslinjene som fantes, var utdaterte og reflekterte ikke hvordan man tenker omkring risikostyring i dag.

Respondenten gav et eksempel på en risikoanalyse hvor en hendelse ble stående igjen på rødt etter at tiltak var vurdert, noe som resulterte i en omfattende diskusjon i analysegruppen. Mangelfulle retningslinjer kan forklare hvorfor det oppstod debatt omkring en enkelthendelse. Her ble analysegruppen utfordret i det å komme frem til en felles forståelse av hvor de analyserte objektene skulle plasseres i risikomatrisen. Den kollektive sensemakingen ble dermed en tilsynelatende mer krevende og langvarig prosess. Informanten gav uttrykk for at det var ”helt feil” å bruke så mye tid på en hendelse som en muligens kanskje bare måtte akseptere havnet på rødt.

## 5.3 Fra felles forståelse til handling

Kollektiv sensemaking handler om hvordan den felles forståelsen i organisasjonen kommer til uttrykk gjennom handling. I forhold til problemstillingen er det aktuelt å belyse hvilke faktorer som har betydning for valg av informasjonssikkerhetstiltak.




Figur 14 Analysemodell: Tiltak

Som illustrert i fig. 14, omfatter tiltak både teknologiske og organisatoriske tiltak. Det er et bevisst valg å la den stiplete sirkelen inkludere kollektiv sensemaking, ut fra kunnskapen om at de erfaringene som virksomheten har av tiltak, vil ha innvirkning på den kollektive sensemakingen i neste omgang [24].

### 5.3.1 Risikoanalyser som beslutningsstøtte. Hva mer?

Det empiriske materialet gir ingen klare indikasjoner på hvorvidt ROS-analysene som er utført av de undersøkte kraftselskapene, kan karakteriseres som ”god” eller ”dårlig”. Flere nevnte at de hadde benyttet eksterne konsulenter i risikoanalysen, noe som ikke nødvendigvis er synonymt med kvalitet. NVE påpekte at det er store forskjeller i kvaliteten på ROS-analysene i kraftsektoren generelt. Dette hadde ofte sammenheng med størrelsen på selskapet og ikt-avdelingen, samt hvilket security-fokus som var i enheten. Erfaringer fra BAS 5-prosjektet støtter utsagnet til NVE. Det kommer frem av sluttrapporten at mange aktører utfører risikoanalyser av ikt-systemer, men av svært varierende karakter [6]. En årsak kan være at folk mangler kompetanse på hvordan de skal anvende metodene. Sivertsen [5] trekker frem at det er viktig at deltakerne er motivert og har, ikke minst, godt kjennskap til systemet som skal undersøkes.

Analysemodellen (fig. 14) illustrerer at det finnes både eksterne og interne krav til virksomhetene for hvordan informasjonssikkerheten og forsyningssikkerheten skal ivaretas. Når det gjelder eksterne krav innebærer, det eksempelvis Energiloven og Beredskapsforskriften [34]. Generelt for beredskapsforskriften er at det hovedsakelig stilles funksjonelle krav til virksomhetene [4]. Det innebærer at det er opptil hver virksomhet å bestemme hvordan dette kravet eller målet skal oppnås [20]. Empirien avslørte flere forhold hvor tilsynsmyndighetene og selskapene var på kollisjonskurs, deriblant kravet om EMP-sikring. Flere informanter gav uttrykk om at de brukte ufordelaktig mye ressurser på å oppfylle dette kravet, og det kan synes som om dette ikke ville blitt prioritert i så stor grad hvis ikke forskriften krevde det.

### 5.3.2 Teknologiske eller organisatoriske informasjonssikkerhetstiltak?

Det finnes som tidligere nevnt, flere ulike barrierer som kan bidra til å øke sikkerheten og robustheten i et IKT-system. I dette studiet er tiltakene delt inn i organisatoriske og teknologiske tiltak (jfr.fig.11). Førstnevnte innebærer følgende kategorier: *sikkerhetspolicyer, metoder* og *verktøy, prosedyrer* og *kontroll,* samt *bevisstgjørende tiltak.* Teknologiske tiltak involverer blant annet bruken av passord, brannmurer og anti-virus program for å nevne noen [7]. En respondent uttalte at organisatoriske tiltak var de mest effektive barrierene mot cyberkriminalitet, mens de resterende uttrykte at det er kombinasjonen av organisatoriske og teknologiske tiltak som utgjør det beste resultatet. I dette ligger det en forståelse av at ”det ene ikke utelukker det andre”. Respondentene

ble deretter bedt om å rangere effekten av de ulike tiltakskategoriene. Hensikten var å sammenligne resultatet med Hagen et al. [7] sin studie av norske bedrifter, hvor sikkerhetspolicyer, prosedyrer og kontroll, samt teknologiske barrierer ble oppgitt som de mest brukte informasjonssikkerhetstiltakene. Av rapporten til Hagen et al. kom det frem at effekten av bevisstgjørende tiltak ble vurdert på lik linje med teknologiske tiltak [7]. Paradoksalt nok ble bevisstgjørende tiltak i liten grad gjennomført i de bedriftene som deltok i undersøkelsen.

Når det gjelder kraftselskapene, var det noe variasjon i hvordan informantene valgte å rangere effekten av informasjonssikkerhetstiltakene. Fire av seks satte sikkerhetspolicy øverst på listen. Dette funnet samsvarer ikke med Hagen et al., noe som kan forklares med at spørsmålene kan være ulikt formulert i de to respektive undersøkelsene. En alternativ tolkning er at kraftselskapene kan ha oppfattet spørsmålet på en annen måte enn det som var intensjonen fra forfatterens side. Tre av seks informanter satte imidlertid bevisstgjørende tiltak som nr to, mens de øvrige plasserte teknologiske tiltak på en andre plass. I motsetning til Hagen et al. [7], hadde informantene som vurderte effekten av bevisstgjørende tiltak høyt, også gjennomført eller ønsket å iverksette holdningsskapende kampanjer for alle de ansatte i bedriften. To av de informantene som hadde rangert teknologiske tiltak høyt, hadde tilsvarende plassert bevisstgjørende tiltak på en sisteplass.

Finnes det en plausibel forklaring på hvorfor informantene vurderte effekten av tiltak så ulikt? En mulig tolkning av den empirien som foreligger, er at informantene med en it-faglig bakgrunn anså menneskelig svikt som den største trusselen mot ikt-systemet. De påpekte at medarbeidere eksempelvis utilsiktet kan åpne opp for virus i systemet via minnepinner, eller at de gjør en feilhandling som får konsekvenser for systemet. Jevnlig fokus på sikkerhet og opplæring vil kunne øke kompetansen og bevisstheten hos de ansatte, hvilket antas å ha en preventiv effekt [7]. Felles for de øvrige informantene var at de hadde en elkraft-faglig bakgrunn, samt at de tilsynelatende viste en større tiltro til de teknologiske barrierene.

# 6 Konklusjon

***"Hvordan oppfatter kraftbransjen risikoen for et angrep på driftskontrollsystemene, og hvilke faktorer kan ha betydning for valg av informasjonssikkerhetstiltak?"***

Hensikten med dette studiet har vært å danne et bilde av hvordan norsk kraftforsyning opplever trusselen om cyberkriminalitet. Videre er risikoanalyseprosessen fremhevet som en arena, hvor grunnlaget for hvilke tiltak som blir gjennomført i virksomheten, etableres. Seks nettselskaper er benyttet som case. Utvalget er for lite til å kunne generalisere for en hel bransje. Likevel anses funnene som interessante også for den øvrige kraftforsyningen, med tanke på at IKT-baserte styrings- og kontrollsystemer benyttes i hele sektoren.

Med utgangspunkt i det empiriske materialet, kan det tyde på at virksomhetene oppfatter risikoen for et *dataangrep* på SCADA-systemet, som lite sannsynlig. Ut fra et historisk perspektiv, finnes det få eksempler på sabotasjeforsøk mot norsk kraftforsyning [12]. I tillegg hadde nettselskapene i liten grad opplevd at driftskontrollsystemene var blitt forsøkt angrepet, hvilket kan forklare hvorfor de ikke anså trusselen som særlig prekær. Teorien bekrefter dermed at risikopersepsjon har sammenheng med hvilke erfaringer man har av en gitt aktivitet [16 og 29]. Videre har kraftsektoren vært restriktive ved å koble driftskontrollsystemet opp mot det administrative nettverket, samt at bransjen tilsynelatende har hatt tillit til at systemleverandørene ivaretar den nødvendige sikkerheten.

Funnene tilsier likevel at det er en økende grad av bevissthet omkring informasjonssikkerhet i kraftbransjen. For det første har tilsynsmyndighetene et større fokus på ROS-analyser generelt - og informasjonssikkerhet spesielt. For det andre har bransjen selv tatt initiativ til å danne et sikkerhetsforum (FSK-forum), hvor problemstillinger relatert til informasjonssikkerhet behandles. Det har i tillegg vært snakk om å etablere et KraftCert, tilsvarende NSM for kraftbransjen, for å registrere alle forsøk på angrep utenfra. Selv om oppmerksomheten har blitt større, er det samtidig forhold som indikerer at IKT-relaterte aktiviteter tillegges noe ulik prioritering i nettselskapene. Utvalget er for lite til å trekke noen generelle konklusjoner, med det kan likevel være nyttig å bemerke mulige fellesnevnere.

Empirien viste en koherens mellom ledelsesengasjement og vektlegging av informasjonssikkerhet. I to selskaper var IT-sikkerhetsleder ansatt i 50 % stilling, hvilket ikke var i overensstemmelse med antatt arbeidsmengde. Etter forfatterens mening, er det noe kritikkverdig at nettselskaper av en slik størrelse, ikke har ansatt en IT-sikkerhetsleder i full stilling. Motsatt har de virksomhetene som opplevde sterkt ledelsesengasjement, også gjennomført omfattende organisatoriske tiltak, som f.eks. holdningsskapende kampanjer for alle de ansatte.

Kraftforsyningen ble opprinnelig driftet av personell med elkraft-faglig bakgrunn [12]. Når IKT-baserte løsninger ble implementert i systemene, fikk også IT-faglig personell tildelt en viktig rolle i kraftsektoren. I henhold til BfK § 6-1 skal alle enheter i KBO utnevne en datakyndig IT-sikkerhetsleder. Det stilles imidlertid ingen krav til utdanningsbakgrunn, så i praksis blir også elkraft- faglig personell tilsatt i en slik posisjon. Det finnes ingen dekning i empirien for å konkludere med at den ene fagdisiplinen er å foretrekke foran det andre. Likevel finner man noen forskjeller. Det ene er at IT-faglig personell i størst grad anerkjente problemstillingen om cyberkriminalitet. Samtidig var de mest opptatt av at menneskelig svikt er den største trusselen mot driftskontrollsystemet, og dermed fremhevet organisatoriske tiltak som mest effektive. På den ene siden uttrykte elkraft-faglig personell større tiltro til de teknologiske barrierene, og de rangerte dessuten bevisstgjørende kampanjer med minst effekt. På den andre siden har de elkraft-faglige større erfaring og kompetanse med det tradisjonelle kraftsystemet. ”De har gjennom utbygging, prøving og feiling lært seg teknikker for raske improvisasjoner og utbedringer ved svikt” [12], noe som kan forklare hvorfor elkraft-faglig personell ikke vurderte svikt i driftskontrollsystemet nødvendigvis som kritisk. Det finnes redundans i å betjene anleggene manuelt.

Valg av tiltak foretas med bakgrunn i eksterne krav, interne krav (sikkerhetsmål) og ROS-analyse. Kost/nytte-perspektivet har selvfølgelig stor betydning, men ble utelatt i denne sammenheng. I dette studiet er hovedsakelig risikoanalysen av driftskontrollsystemet tillagt stor vekt. Bakgrunnen for dette var antakelsen om at organisasjonen gjennom en risikoanalyseprosess, kommer frem til en felles forståelse av risiko som materialiseres i handling eller tiltak (kollektiv sensemaking) [24]. Empiren bekrefter at resultatet fra ROS-analysene, sammen med eksterne og interne krav (sikkerhetsmål), har stor betydning for valg av tiltak i de virksomhetene som er

undersøkt. Det finnes imidlertid ingen dekning for å avgjøre hvorvidt disse risikoanalysene er av en god kvalitet eller ikke, noe som kan betraktes som en svakhet med dette studiet. I den innledende kontakten med respondentene, ble tilgang til ROS-analysene etterspurt. Beklageligvis ble det ikke gitt innsyn til disse i denne omgang. NVE bekreftet imidlertid at det er store variasjoner i kvalitet og omfang av ROS-analysene som utføres i norsk kraftforsyning. Hvorvidt det gjelder noen av de undersøkte virksomhetene, vites ikke.

## 6.1 Forslag til videre forskning

Det er enkelte forhold som ikke blir tilstrekkelig ivaretatt i dette studiet, og som hadde vært givende å studere mer inngående. For det første kunne det vært svært interessant å belyse kollektiv sensemaking ytterligere, dvs. hvilke mekanismer som gjør seg gjeldende når analysegruppen skal diskutere seg frem til en felles forståelse av risikoen for dataangrep. Da kunne det ha vært hensiktsmessig å gjennomført en deltakende observasjon av analysemøtene, samt foretatt individuelle intervju med den enkelte deltaker.

Skjæringspunktet mellom de to dominerende fagdisiplinene, IT og Elkraft kunne også vært spennende å undersøke nærmere. Sistnevnte har en lang tradisjon og kultur for forsyningssikkerhet, noe NVE bekrefter at bransjen er god på. Samtidig fører IKT-teknologi med seg nye sikkerhetsutfordringer og farer. Det kunne vært interessant å betrakte hvordan samarbeidsklimaet, deriblant kommunikasjon og forståelse, er mellom de to fagkulturene.

Dette studiet har heller ikke tatt hensyn til *etterlevelse.* Empirien gav ikke så mye konkret informasjon om hvordan nettselskapene fulgte opp tiltak og reguleringskrav. Samtidig var det et bevisst valg og ikke å belyse etterlevelse i denne sammenheng, særlig for å unngå å komme i konflikt med kravet om sensitiv informasjon. NVE påpekte imidlertid at de finner mye avvik når de er fører tilsyn med kraftselskapene. Det viser at problemstilling er aktuell, og således kunne den vært interessant å forfølge.

# 7 Referanser


[1] Aven, T., Boyesen, M., Njå, O., Olsen, K.H. & Sandve, K. (2008) *Samfunnssikkerhet.* 3.utgave. Oslo, Universitetsforlaget.

[2] Aven, T. (2007) *Risikostyring*. Oslo, Universitetsforlaget

[3] Beredskapsforskriften (2002) *Forskrift om beredskap i kraftforsyningen.* FOR-2002-12-16-1606. Tilgjengelig fra:http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20021216-1606.html [nedlastet 1.mars 2011]

[4] Norges vassdrags- og energidirektorat (2003) *Veiledning til forskrift om beredskap i kraftforsyningen* [Internett] Oslo Tilgjengelig fra: http://www.kunnskapsnettverk.no/sites/kis/Offentlige%20dokumenter/Beredskapsveiledning_v6b.pdf [nedlastet 1.mars 2011]

[5] Sivertsen,T.K. (2007) *Risikoanalyse av samfunnskritiske IKT-systemer-Teknologiske erfaringer*. FFI/Rapport-2007/00910. Forsvarets forskningsinstitutt http://rapporter.ffi.no/rapporter/2007/00910.pdf [nedlastet 25.februar 2011]

[6] Fridheim, H. & Hagen, J. (2007) *Beskyttelse av samfunnet 5: Sårbarhet i kritiske IKT-systemer – sluttrapport.* FFI/Rapport-2007/01204. Forsvarets forskningsinstitutt Tilgjengelig fra: http://rapporter.ffi.no/rapporter/2007/01204.pdf [nedlastet 25.februar 2011]

[7] Hagen, J.M., Albrechtsen, E. & Hovden, J. (2008) *Implementation and effectiveness of organizational information security measures.*Information Management & Computer Security, Vol. 16, no. 4, s. 377-397

[8] Aven, T., Røed, W. & Wiencke, H.S. (2008) *Risikoanalyse.* Oslo. Universitetsforlaget

[9] Norges vassdrags- og energidirektorat (2010) *Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen* Oslo, Norges vassdrags- og energidirektorat

[10] Justis- og politidepartementet (2002) *Samfunnssikkerhet. Veien til et mindre sårbart samfunn. St.meld. nr. 17 (2001-2002) Oslo, Justis- og politidepartementet*

[11] Hamnes, L. (2011) IT invaderer kraftbransjen. Artikkel, *Teknisk ukeblad.* 23.februar 2011 [Internett] Tilgjengelig fra: http://www.tu.no/it/article279234.ece [nedlastet 5. mai 2011]

[12] Fridheim, H., Hagen, J. & Henriksen, S. (2001) *En sårbar kraftforsyning-sluttrapport etter BAS3.* FFI/Rapport-2001/02381. Forsvarets forskningsinstitutt http://www.nve.no/PageFiles/850/Sluttrapport.pdf?epslanguage=no [nedlastet 25. februar 2011]

[13] Forsvarsdepartementet, Nærings- og handelsdepartementet & Justis- og politidepartementet (2003) *eNorge- Nasjonal strategi for informasjonssikkerhet- Utfordringer, prioriteringer og tiltak.* Tilgjengelig fra: http://www.kunnskapsnettverk.no/sites/kisarbeidsrom/Offentlige%20dokumenter/Nasjonal%20strategi%20for%20informasjonssikkerhet.pdf [nedlastet 23. februar 2011]

[14] Onerød, J.T. (2006) *Sårbarheter og trusler mot informasjonssystemer*. NSM temahefte 1/2006. Oslo, Nasjonal sikkerhetsmyndighet

[15] Justis – og politidepartementet (2008) *Om lov om endringer i straffeloven 20. mai 2005 nr. 28 (siste delproposisjon - sluttføring av spesiell del og tilpasning av annen lovgivning)* Ot.prp. 22 (2008-2009) Oslo, Justis- og politidepartementet

[16] Renn, O. (2008) *Risk Governance. Coping with Uncertainty in a Complex World.* London. Earthscan

[17] Rodal, K. (2001) Sårbarhet i kraftforsyningens drifts- og styringssystemer FFI/RAPPORT- 2001/04278. Forsvarets forskningsinstitutt. Tilgjengelig fra: http://rapporter.ffi.no/rapporter/2001/04278.pdf [nedlastet 25. februar 2011]

[18] Hamnes, L. (2010) Cyberkrigen er i gang. Artikkel, *Teknisk ukeblad*. 8. oktober 2010 [Internett] Tilgjengelig fra: http://www.tu.no/iphone/article261873.ece [nedlastet 5. mai 2011]

[19] Internkontrollforskriften (1996) *Forskrift om systematisk helse- og miljø- og sikkerhetsarbeid i virksomheter* FOR-1996-12-06-1127. Tilgjengelig fra: http://www.lovdata.no/cgi-wift/wiftldles?doc=/app/gratis/www/docroot/for/sf/ad/ad-19961206-1127.html&emne=forskrift%20om%20systematisk%20helse*%20og& [nedlastet 4. april 2011]

[20] Kirwan, B., Hale, A. & Hopkins, A. (2002) *Changing Regulation. Controlling Risks in Society.* Amsterdam. Pergamon

[21] Rege- Patwardhan, A. (2009) *Cybercrimes against critical infrastructures:a study of online criminal organization and techniques.* Criminal justice, 22:3, s. 261-271

[22] Investigate research for infrastructure (2002) *Cyber security of the electric power industry.* IRIA. Tilgjengelig fra:http://www.ists.dartmouth.edu/library/218.pdf [nedlastet 28. februar 2011]

[23] Baker, S., Filipiak, N. & Timlin, K. (2011) *In the dark. Crucial Industries Confront Cyberattacks.* MacAfee & Center for Strategic and International Studies [Internett] Tilgjengelig fra: http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf [nedlastet 12. mai 2011]

[24] Valaker, S. (2007) *Kollektiv sensemaking og informasjonsstruktur i nettverksbaserte operasjoner. Et human factor perspektiv.*FFI/Rapport-2007/02251. Tilgjengelig fra: http://rapporter.ffi.no/rapporter/2007/02251.pdf [nedlastet 29. april 2011]

[25] Pietre- Cabcedes, L. & Chaudet, C. (2010)*The SEMA referential framework: Avoiding ambiguities in the terms "security" and "safety"*. International journal of Critical Infrastructure protection, 3 (2010) s. 55-66

[26] Weick, K.,Sutcliffe, K.M. & Obstfeld, D. (2005) *Organizing and the process of sensemaking.* Organization Science, Vol. 16.No 4.July-August 2005. s, 409-421

[27] Weick, K. (1990) *Technology as Equivoque: Sensemaking in New Technologies.* I Goodman, P.et al. (Ed.). Techology and organizations, s. 1-44. San Francisco: Jossey-Bass

[28] Slovic, P., Fischhoff, B. & Lichtenstein, S. (1982) *Why Study Risk Perception?* Risk Analysis, Vol 2, no. 2, s. 83-92

[29] Sjøberg, L. & Drottz-Sjøberg, B.-M. (2001) *Fairness, risk and risk tolerance in the sitting of a nuclear waste repository*. Journal of Risk Research, Vol 4, s. 75-101

[30] Leveson, N. (2004) *A New Accident Modell for Engineering Safer Systems.* Safety Science,Vol. 42, no. 4, s. 230-270

[31] Jones, E.P. & Roelofsma, H.M.P.P (2000) *The Potential for social contextual and group biases in team decision-making: biases, conditions and psychological mechanisms.* Ergonomics, vol.43, no.8, 1129-1152

[32] Ross, L., Greene, D. & House, P. (1977) *"The false consensus effect": an egocentric bias in social perception and attribution process,* Journal of Experimental Social Psychology, 13, 279-301

[33] Turner, B.A & Pidgeon, N.F. (1997) *Man Made Disasters,* Oxford, Butterwoth Heineman

[34] Justis- og politidepartementet (2006) *Når sikkerheten er viktigst.* NOU 2006:6. Oslo, Departementenes servicesenter Informasjonsforvaltning

[35] Olje- og energidepartementet (2008) *Fakta 2008. Energi og vannressurser i Norge* [Internett] Tilgjengelig fra:http://www.regjeringen.no/upload/OED/pdf%20filer/Faktaheftet/EVfakta08/Evfakta08_start_no.pdf [nedlastet 19. mai 2011]

[36] Nygård, A.R. (2004) *Risk Management in SCADA-systems.* Masteroppgave, Høgskolen i Gjøvik [Internett] Tilgjengelig fra: http://brage.bibsys.no/hig/bitstream/URN:NBN:no-bibsys_brage_4310/1/nygÃ%C2%83Â¥rd_-_Risk_management_in_SCADA-_system.pdf [nedlastet 25. april 2011]

[37] Patel, S.C. & Sanyal, P. (2008) *Securing SCADA-systems*. Information Management & Computer Security, Vol. 16, no. 4.2008 s. 398-414, Emerald

[38] Justis- og politidepartementet (2008) *Samfunnssikkerhet. Samvirke og Samordning.* St.meld 22 (2007-2008) Oslo, Justis- og politidepartementet

[39] Nærings- og Handelsdepartementet (2000) *Samfunnets sårbarhet som følge av avhengighet til IT* [Internett] Tilgjengelig fra: http://www.regjeringen.no/upload/kilde/nhd/rap/2000/0010/ddd/pdfv/120416-it-saarbarhet.pdf [nedlastet 27. mai 2011]

[40] Hammerstrøm, J.L. (2010) Økt spionasje mot Norge. Artikkel, *NRK Nettutgave,* 4.februar 2010 [Internett] Tilgjengelig fra: http://m.nrk.no/m/artikkel.jsp?art_id=16977384 [Nedlastet 23.mai 2011]

[41] Teknisk ukeblad (2011) *Målrettet dataangrep mot Forsvaret.*19.mai 2011 [Internett] Tilgjengelig fra: http://www.tu.no/it/article286624.ece [Nedlastet 23.mai 2011]

[42] Nasjonal sikkerhetsmyndighet, Politidirektoratet & Politiets sikkerhetstjeneste (2010) *En veiledning: Sikkerhets- og beredskapstiltak mot terrorhandlinger* [Internett] Oslo. Tilgjengelig fra: http://www.pst.politiet.no/Filer/utgivelser/Utgivelser/terror_sikkerhetsveileder.pdf [nedlastet 19. februar 2011]

[43] Krikfjord, T.P. (2010) Cyberkrim er ”det neste Pearl Harbour”. Artikkel, *Dagbladet.* 18. oktober 2010 [Internett] Tilgjengelig fra: http://www.dagbladet.no/2010/10/18/nyheter/datakriminalitet/storbritannia/utenriks/hacking/13891788/ [nedlastet 23. mai 2011]

[44] Hamnes, L. (2010) Stuxnet er et militært våpen. Artikkel, *Teknisk ukeblad.* 1.oktober 2010 [Internett] Tilgjengelig fra: http://www.tu.no/it/article261388.ece [nedlastet 23. mai 2011]

[45] Nasjonal sikkerhetsmyndighet (2010) *Årsrapport 2010. Sikkerhetskultur* [Internett] Tilgjengelig fra: https://www.nsm.stat.no/upload/Publikasjoner/Årsmeldinger/Årsmelding-NSM-2010web.pdf [nedlastet 28. mai 2011]

[46] Næringslivets sikkerhetsråd (2010) *Mørketallsundersøkelsen 2010. Informasjonssikkerhet og datakriminalitet* [Internett] Tilgjengelig fra: http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/morketallsundersokelsen_2010.pdf [Nedlastet 18.februar 2011]

[47] Aven, T. & Renn, O. (2010) *Risk Management and Governance: Concept, Guidelines and Applications*. 1.utgave. Springer Verlag

[48] Jacobsen, D.I. (2000) *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode.* Kristiansand. Høyskoleforlaget

[49] Blaikie, N. (2010) *Designing Social Research*. 2. Utgave. Polity Press

[50] Andersen, S.S. (2006) *Aktiv informantintervjuing*. Norsk statsvitenskapelig tidsskrift, Vol. 22, s. 278-298. Universitetsforlaget

[51] Jacobsen, D. I. (2005). *Hvordan gjennomføre undersøkelser? Innføring i vitenskapelig metode*, 1. Utgave, Kristiansand. Høyskoleforlaget.

[52] Yin, R. K. (2009). *Case study research : design and methods.* 4. Ed. Vol. Applied social research methods series, Los Angeles. Sage

# Appendiks I

## Trusselaktører og teknologiske virkemidler

Det finnes mange ulike rapporter som kategoriserer ulike trusselaktører. Jeg har valgt å referere til en artikkel som har sett på informasjonssikkerhet i kraftsektoren. I følge *"Cyber Security of the electric power industry* [22] utgjør en mulig trussel mot kraftforsyningens driftskontrollsystemer:

1) **Fiendtlige nasjoner**: Det antas at om lag 20 nasjoner utvikler cyberkrigføring som militær strategi, og antallet forventes å øke. Her finnes det ofte mye ressurser, evner og kunnskap til å potensielt gjennomføre mer alvorlig angrep mot kraftforsyningen.

2) **Cyberterrorister:** det finnes ikke eksempler på at terroristiske cyberhandlinger frem til dags dato, i hvert fall ikke som er publisert. Det er likevel liten tvil om at terrorister også utvikler IT-ferdigheter, og at disse kan benyttes til å gjennomføre cyberattack i fremtiden

3) **Hackere**: det finnes mange varianter av hackergrupper. Gutteromshackere vurderes ikke til å ha være en trussel mot kraftforsyningen da de ikke har nok kunnskap til å forårsake store nok ødeleggelser. Men en liten gruppe av teknisk dyktige hackere med detaljert kunnskap om drifts- og styringssystemene utgjør en reell trussel mot kraftforsyningen. Det finnes også noen få miljøaktivister som kan ha motivasjon og ferdigheter til å forstyrre kraftoperasjonene.

4) **Utro tjenere (insidere)**: representerer også en potensiell trussel mot kraftforsyningen da de har betydelig kjennskap til systemene. SCADA-systemene benyttes over hele verden, og det er mye informasjon om systemene på internett. Av den grunn ansees ikke utro tjenere som den "farligste" gruppen, da de besitter mye av den kunnskapen som uansett er forholdsvis lett tilgjenglig.

Nasjonal sikkerhetsmynderi (NSM) påpeker at trusselaktørene utgjør en alvorlig trussel først dersom vedkommende både har motivasjon og evner til å utføre et avansert dataangrep [14] . Det kan være økonomiske eller politiske interesser som ligger bak et angrep. Nysgjerrighet, samt anerkjennelse i enkelte miljø kan også være en motiverende faktor. Sårbarheter er ikke problem i seg selv, det er først når noen velger å utnytte dem at det blir et problem [14].

## Teknologiske virkemiddel

Hvilke metoder finnes for å utnytte de sårbarhetene som forekommer i ikt-systemene? Ondsinnet programvare eller ”malware” er en samlebetegnelse for *virus* og *ormer*, *trojaner* og *bakdører* [5]. Samtlige er teknologiske virkemidler som benyttes for å skade, hindre, styre eller få kontroll over et ikt-system. Felles for disse begrepene er at de inneholder en eller annen form for *ondsinnet kode*, altså ”et sett med instruksjoner som kjører på en datamaskin og utfører operasjoner i henhold til angripers ønske” [14]. Ofte spres ondsinnet programvare via sosial manipulasjon, eksempelvis de selvspredende variantene som sendes som vedlegg til epost [5]. Mottakeren lures til å kjøre filen, og blir dermed infisert av et virus eller en orm. Det er noe forskjell på hvordan de ulike virkemidlene sprer seg, men det vil jeg ikke gå nærmere inn på i denne sammenheng.

Effekten de ondsinnede har er mer relevant å si noe om i denne sammenheng. Dersom en ondsinnet programvare blir installert på en maskin, kan den i verste fall utføre mange av de samme handlingene som brukeren selv. Eksemplene som nevnes her er hentet fra følgende rapport, ”Risikoanalyser av IKT-system” [5].

- All tilgjengelige informasjon gjennomsøkes (kredittkortnr, person-identifiserende informasjon, passord etc)
- Nye programvarer lastes ned og installeres (uten brukers vilje).
- Informasjon kan forandres (f.eks innhold på websider)
- Nettverksforbindelser kan gjenopprettes (for å sende tilbake innhentet informasjon, eller muliggjør for fjernstyring)
- Tilkoblede enheter kan overvåkes og kontrolleres

Figur A.1. gir en oversikt over mulige trusselaktører, deres motivasjon og virkemidler. Dette skjemaet ble opprinnelig brukt i et av BAS5-prosjektene, og er en matrise i en trusselanalyse av et ikt-system. I denne fremstillingen er imidlertid kolonnene for sannsynlighet og konsekvens utelatt.

| **Trusseltype** | | | |
|---|---|---|---|
| **Motivasjon** | **Virkemiddel** | **Aktører** | **Kommentar** |
| Utforsking, nysgjerrighet | logiske | Hackere Kunder | Automatiserte verktøy, manipulering av webinterface og databaser |
| Prestisje | Logiske<br>Sosiale | Hackere | Ukjente sårbarheter i infrastruktur, mangelfulle sikkerhetsrutiner |
| Hevn | Logiske<br>Fysiske<br>Sosiale | Oppsagt ansatt<br>Forvirret ansatt<br>Andre tilknyttede | God kjennskap til interne rutiner og system, ikke tilbaketrukket autorisasjon, kjennskap til passord |
| Økonomiske (direkte eller via utpressing) | Logiske<br>Sosiale | Organisert kriminalitet<br>Enkeltpersoner<br>Ansatte<br>Insidere | Manipulerte databaser til egen fordel, uthenting av informasjon.<br>Trusler om logiske angrep.<br>Insidere med ekstra informasjon |
| Publisitet<br>f.eks ”hactivisme” | Logiske<br>Fysiske | Politiske grupper<br>Terroristgrupper | Angrep som ikke trenger å være ”effektive” |
| Spre kaos og usikkerhet | Fysiske<br>Sosiale<br>Logiske | Terroristgrupper<br>Fremmede stater | |
| Politiske / militære mål | Logiske<br>Fysiske | Terroristgrupper<br>Fremmede stater<br>Utilsiktet skade fra fremmede stater | Rettede angrep mot infrastruktur, angrep fra interne nettverk.<br>Manipulering av applikasjonsdata |

*Tabell A.1. Oversikt over aktørtyper og mulig motivasjon. Utdrag fra en matrise brukt i en trusselanalyse i forbindelse med at av BAS5-casene [5:37]*

# APPENDIKS II

**Til den det måtte angå**

Jeg er masterstudent i samfunnssikkerhet ved Universitetet i Stavanger, og holder for tiden på å skrive den avsluttende oppgaven. Masteroppgaven er tilknyttet et doktorgradsprosjekt ved UiS med temaet sårbarhet, teknologi og organisasjon. Tittelen på dette prosjektet er :" Risiko og sårbarhet ved bruk av IKT i norsk kraftforsyning". I forbindelse med doktorgradsprosjektet var det ønskelig at noen ville skrive en masteroppgave med fokus på hvordan kraftbransjen selv oppfatter trusselen om cyberkriminalitet.

I samråd med doktorstipendiat, har vi kommet frem til at det er mest interessant å betrakte nettselskapene, da et angrep på disse selskapenes IKT-systemer (drifts- og styringssystem) potensielt vil kunne gi størst konsekvenser for kraftforsyningen. Videre ønsker jeg å betrakte hvorvidt gjennomførte tiltak samsvarer med den oppfatningen som eksisterer i virksomhetene. Oppgaven jeg skriver tar utgangspunkt i teori om risikopersepsjon, organisasjonsteori og risikostyring. Planen er å gjennomføre intervju og (evt.) dokumentanalyse av seks nettselskaper, i tillegg til NVE.

Jeg skal etter planen gjennomføre intervjuene i uke 17 og 18. Intervjuet forventes å ha en varighet på ca 1 time. Til informasjon finnes det rutiner for hvordan masterstudenter/universitet skal forholde seg informasjon som er av sensitiv karakter. En praksis er at jeg og mine veiledere kan underskrive en taushetserklæring, samt at selve masterdokumentet kan unnlates offentligheten i x-antall år dersom det er ønskelig.

Jeg setter stor pris på en snarlig tilbakemelding, og vil samtidig understreke at jeg håper at ……. har mulighet til å bidra i prosjektet.

Eventuelle spørsmål kan rettes til meg på tlf …….

På forhånd takk!

mvh Marie Røyksund

# APPENDIKS III

## INFORMASJON OM PROSJEKTET

Meg selv: Jeg er 2-års student ved masterprogrammet i samfunnssikkerhet ved Universitetet i Stavanger (UiS). Har en Bachelor i Sosialfag og er høyskolekandidat i økonomi og administrasjon.

Hensikten med denne masteroppgaven er å kartlegge kraftbransjens egne oppfatninger av trusselen om angrep på IKT-systemene, og hvordan dette påvirker informasjonssikkerheten. Teoretiske bidrag vil ta utgangspunkt i *risikopersepsjon, risikostyring* og organisasjonsteori. Masteroppgaven er tilknyttet et doktorgradsprosjekt som omhandler "Risiko og sårbarhet ved bruk av IKT i norsk kraftforsyning.

Foreløpig problemstillingen er;

**Hvordan oppfatter kraftbransjen risikoen for et angrep på IKT-systemene, og hvilken betydning har dette for informasjonssikkerheten?**

Med cyberkriminalitet forstås kriminelle handlinger som er rettet mot data og datasystemer, samt kriminalitet hvor datautstyr benyttes som verktøy for å begå mer tradisjonell kriminalitet (Ot.prp. 22 (2008-2009)). Denne oppgaven omhandler i hovedsak førstnevnte tilsiktede handling. I denne sammenheng forstås IKT-systemene som de drifts- og styringssystemene som benyttes for å produsere og distribuere kraft.

SPØRSMÅLSGUIDEN ER BASERT PÅ FØLGENDE:

- Veileder til beredskapsforskriften
- NSM, Temahefte 1/2006. *Sårbarheter og trusler mot informasjonssystemer*
- Mørketallsundersøkelsen 2010
- FFI-rapport (2001) *Sårbarhet i kraftforsyningens drift- og styringssystem*
- FFI-rapport (2007) *Risikoanalyser av samfunnskritiske IKT-systemer. Teknologiske erfaringer.*
- Hagen et al. (2008) *Implementation and effectiveness of organizational information security measures*

# SPØRSMÅLSGUIDE (NETTSELSKAPENE)

INNLEDNINGSVIS

1. Respondentens bakgrunn og rolle ift IKT i nettselskapet?

ORGANISERING OG ANSVAR

1. Hvilken klasse tilhører anlegget ift bfK § 5-3 og energiloven § 8-3?
2. Ifølge bfK § 4-1 har enhetens leder ansvar for informasjonssikkerheten, men kan utpeke en til å planlegge og følge opp IKT-sikkerheten. Hvordan er det organisert i hos dere?
3. Hvordan er IKT-systemet organisert i enheten? (Rollebeskrivelse, f.eks. systemeier, systemansvarlig, driftsansvarlig etc)
4. Benytter enheten seg av eksterne it-tjenester (outsourcing av it-oppgaver)? Hvis ja, i hvilken grad stilles det sikringskrav til outsourcingspartner? Og føres det tilsyn / kontroll ift. sikkerhetsrutiner?

RISIKOANALYSER

1. Hvor ofte gjennomfører enheten risikoanalyser av IKT-systemet, jmf bfK § 1-1 og § 1-3 (inkl. oppdatering/revisjon)?
2. Hvilke(n) risikoanalysemetodikk av IKT- systemet benyttes i enheten?
    - Standard risiko- og sårbarhetsanalyser (ROS)
    - Metoder spesielt utviklet for IKT (f.eks KITH, CORAS)
    - Sjekklister
    - Internasjonale standarder og ”best practices”
    - Penetrasjonstesting
    - Tekniske sårbarhetsanalyser
    - Egenutviklede virksomhetsinterne risikoanalysemetodikker
    - Andre?
3. Har dere erfaring med NVE sin veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen som ble utgitt i 2010?
    - Hvis ja, er veilederen et godt hjelpemiddel eller er den vanskelig å bruke i praksis? Begrunn.

- Hvis nei, hvorfor ikke?

4. Hvem deltar i risikoanalyseprosessen?
5. Hvordan kommer dere frem til hvilke uønskede hendelser som skal vurderes i risikoanalysen (fareidentifikasjon)?
6. Skilles det mellom tilsiktede og utilsiktede handlinger i risikoanalysene?
7. Hva er bakgrunn for fastsettelse av sannsynlighet og konsekvens?
8. Hvilke faktorer er av betydning når akseptabelt risikonivå fastsettes? Utdyp.
9. Kan du forsøke å vektlegge hvor mye oppmerksomhet som gis til risiko mot IKT-systemet vs den fysiske infrastrukturen i risikoanalyseprosessen?
10. Opplever dere risikoanalyser som et hensiktsmessig redskap ift. å kartlegge faren for tilsiktede angrep på IKT-systemet? Utdyp.

RISIKO

1. Hva forstår du/dere med begrepet cyberkriminalitet?
2. Hva legger dere i begrepet ”angrep mot IKT-systemer”?
3. Har dere opplevd angrep mot enhetens IKT-system? Ja/Nei
4. Har du/ dere noen tanker om trusselaktørene? ”Hvem” trusselaktørene er og hvilken motivasjon som kan ligge bak et evt. angrep mot kraftforsyningen?
5. Hvordan vurderer dere sannsynligheten for et angrep på IKT-systemet i deres enhet?
6. Hvilke konsekvenser kan et potensielt ”vellykket” angrep få?
7. Hva anser dere som de største truslene mot IKT-systemet, herunder innbefattes alle hendelser (ikke kun målrettede angrep)?
8. Anser du/dere gjeldende drift- og styringssystemer for tilstrekkelig ”sikre” system? Utdyp.
9. Ifølge NVE er kraftbransjen generelt gode på sikring, men det er mangler når det gjelder å planlegge for ekstraordinære hendelser med potensielt store konsekvenser. Enig / Uenig?

ORGANISATORISKE OG TEKNOLOGISKE TILTAK

Jeg har valgt å dele inn informasjonssikkerhets tiltak i følgende 5 kategorier (jmf Hagen, 2008):

(i) *Informasjonssikkerhetspolitikk:* overordnet sikkerhetspolicy

(ii) *Metoder og verktøy:* risikoanalyser, rapportering, krav fra myndigheter, interne revisjoner, beredskapsplaner

(iii) *Prosedyrer og kontroll:* retningslinjer for individuell atferd, taushetserklæringer, disiplinære konsekvenser og krav til outsourcing av it-tjenester

(iv) *Bevissthetsgjørende (awareness) tiltak:* Holdningsskapende kampanjer, opplæring, brukermedverkning og engasjement fra ledelse.

(v) *Teknologiske tiltak*: passord, redundans av kritiske system, anti-virus program, brannmurer, monitorering o.l.

1. Benytter dere andre typer kategoriseringer? I tilfellet, hvilke?
2. Hva er bakgrunnen for valg av tiltak som implementeres i enheten?
3. Er det utarbeidet egne sikkerhetspolicyer for håndtering av informasjonssikkerhet?
    - Hvis ja, hvilket nivå i organisasjonen er denne forankret i?
    - Hvordan blir innholdet i sikkerhetspolicyen formidlet til de som arbeider med IKT-systemet i enheten?
4. Hva med kompetanseheving? Opplæring/kursing?
5. Hvilke prosedyrer og kontroller finnes i virksomheten?
6. Hvordan vil dere beskrive sikkerhetskulturen i nettselskapet?
7. Opplever du/dere at konsernledelsen tar trusselen om cyberkriminalitet på alvor? Utdyp.
8. Har dere noen tanker om hvorvidt teknologiske tiltak eller organisatoriske tiltak er mest effektive barrierer mot cyberkriminalitet? Begrunn.
9. Hvordan vil dere rangere effekten av de ulike tiltaksgruppene som nevnt ovenfor?
10. Opplever du at det er tid og anledning til å holde seg oppdatert vedrørende trusselbilde og regelverk?

TIL SLUTT

1. *Er det andre spørsmål som burde bli stilt for å belyse problemstillingen? Hvilke?*
2. *Er det tema du forventet ville bli omhandlet i intervjuet, som er utelatt? Utdyp.*

# APPENDIKS IV

## SPØRSMÅLSGUIDE (NVE)

ORGANISERING OG ANSVAR

5. Hvor ”gode” er nettselskapene på informasjonssikkerhet etter deres oppfatning? Utdyp.
6. Ifølge BfK § 4-1 har leder ansvar for informasjonssikkerheten i enheten, men kan delegere ansvaret om planlegging og oppfølging av IKT-sikkerheten? Er dette gjennomført i norsk kraftforsyning? Forskjell på små/store aktører?
7. Hvilke tanker har dere ift bruken av outsourcing av it-oppgaver i kraftforsyningen? Blir dette tilstrekkelig fulgt opp med sikringskrav og påfølgende kontroll av sikkerhetsrutiner hos outsourcingspartnere?

RISIKOANALYSER

11. Hvilken oppfatning har dere av de risikoanalysene som blir utført av nettselskapene ift. IKT-systemene (jmf bfK § 1-1 og § 1-3), herunder:
    - *Fareidentifikasjon* (uønskede hendelser som skal behandles i risikoanalysen)
    - Fastsettelse av sannsynlighet og konsekvens
    - Akseptabelt risikonivå
12. Hva er bakgrunnen for at NVE utarbeidet veiledningen i risiko-og sårbarhetsanalyser for kraftforsyningen (2010), og i hvilken grad er denne egnet for å analysere risikoen for tilsiktede hendelser på IKT-systemene?

RISIKO

10. Hva forstår du/dere med begrepet cyberkriminalitet?
11. Hva legger dere i begrepet ”angrep mot IKT-systemer”?
12. Dersom nettselskapene opplever angrep på sine IKT-system, blir dette rapportert til dere?

13. Hvilke varslingsrutiner har dere overfor nettselskapene dersom dere får kjennskap til mulige trusler/angrep mot kraftforsyningen?
14. Har du/ dere noen tanker om trusselaktørene? ”Hvem” trusselaktørene er og hvilken motivasjon som kan ligge bak et evt. angrep mot kraftforsyningen?
15. Hvilke tanker har dere om sannsynligheten for et angrep på kraftforsyningens IKT-system?
16. Hvilke konsekvenser kan et potensielt ”vellykket” angrep få?
17. Hva anser dere som de største truslene mot IKT-systemet, herunder innbefattes alle hendelser (ikke kun målrettede angrep)?
18. Anser du/dere gjeldende drift- og styringssystemer for tilstrekkelig ”sikre” system? Utdyp.
19. Hvilke sikkerhetsutfordringer vil innføringen av smartgrid /AMS i kraftbransjen medføre?
20. Ifølge NVE (f.eks KBO landsmøte, mars -10) er kraftbransjen generelt gode på sikring, men det er mangler når det gjelder å planlegge for ekstraordinære hendelser med potensielt store konsekvenser. Hva er bakgrunnen for denne uttalelsen/oppfatningen?

ORGANISATORISKE OG TEKNOLOGISKE TILTAK

Jeg har valgt å dele inn informasjonssikkerhets tiltak i følgende 5 kategorier (jmf Hagen, 2008):

(vi) *Informasjonssikkerhetspolitikk:* overordnet sikkerhetspolicy

(vii) *Metoder og verktøy:* risikoanalyser, rapportering, krav fra myndigheter, interne revisjoner, beredskapsplaner

(viii) *Prosedyrer og kontroll:* retningslinjer for individuell atferd, taushetserklæringer, disiplinære konsekvenser og krav til outsourcing av it-tjenester

(ix) *Bevissthetsgjørende (awareness) tiltak:* Holdningsskapende kampanjer, opplæring, brukermedverkning og engasjement fra ledelse.

(x) *Teknologiske tiltak*: passord, redundans av kritiske system, anti-virus program, brannmurer, monitorering o.l.

11. Kjenner dere igjen denne formen for kategorisering i kraftforsyningen?
12. Har dere inntrykk av at nettselskapene (ledelsen) tar trusselen om cyberkriminalitet på alvor? Utdyp.
13. Opplever dere at nettselskapene har tilfredsstillende sikkerhetspolicyer forankret på ledelsesnivå? Utdyp.
14. Hva med kompetanseheving? Opplæring/kursing?
15. Er det gode nok prosedyrerer og kontroller for de ansatte i virksomhetene? Utdyp.
16. Hvordan vil dere beskrive sikkerhetskulturen i norsk kraftforsyning?
17. Har dere noen tanker om hvorvidt teknologiske tiltak eller organisatoriske tiltak er mest effektive barrierer mot cyberkriminalitet? Begrunn.
18. Hvordan vil dere rangere effekten av de ulike tiltaksgruppene som nevnt ovenfor?
19. Opplever dere at nettselskapene holder seg oppdatert på regelverk og trusselnivå?

TIL SLUTT

*Er det andre spørsmål som burde bli stilt for å belyse problemstillingen? Hvilke?*

*Er det tema du forventet ville bli omhandlet i intervjuet, som er utelatt? Utdyp*

# APPENDIKS V

## Samtykkeerklæring

I forbindelse med min masteroppgave i Samfunnssikkerhet ved Universitetet i Stavanger, vil jeg gjennomføre flere intervjuer. Formålet med oppgaven er å undersøke hvordan den norske kraftforsyningen oppfatter risikoen for cyberkriminalitet, og hvordan dette har betydning for informasjonssikkerheten. Spørsmål som stilles vil i hovedsak omhandle *risikopersepsjon*, prosesser knyttet til *risikoanalyser*, samt en generell betraktning av *risikoreduserende tiltak*, med hovedvekt på *organisatoriske tiltak.*

Alle opplysninger som blir gitt i intervjuet anonymiseres i oppgaven. Jeg vil benytte båndopptaker for å sikre at jeg får med meg alle opplysninger. Virksomhet og informant (navn) vil bli omtalt som ”respondent 1”, ”respondent 2” osv. Dette for å sikre at alle opplysninger blir behandlet fortrolig og anonymt. I tillegg vil du/dere gis anledning til å godkjenne teksten som er tilknyttet deres svar før det settes en sluttstrek.

Ved å skrive under på denne erklæringen godtar du at opplysninger som gis under intervjuet kan benyttes i masteroppgaven.

……

Marie Røyksund

Masterstudent i samfunnssikkerhet

…….

Respondent