DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering:
Master i samfunnssikkerhet

Vårsemesteret, 2022

Åpen / ~~Konfidensiell~~

Forfatter:
Markus Isaksen

.....
(signatur forfatter)

Fagansvarlig:
Ole Andreas Engen

Veileder(e):
Kenneth Arne Pettersen Gould

Tittel på masteroppgaven: Teknologi og organisasjon i likevekt

Engelsk tittel: Technology and Organization in Equilibrium

Studiepoeng: 30

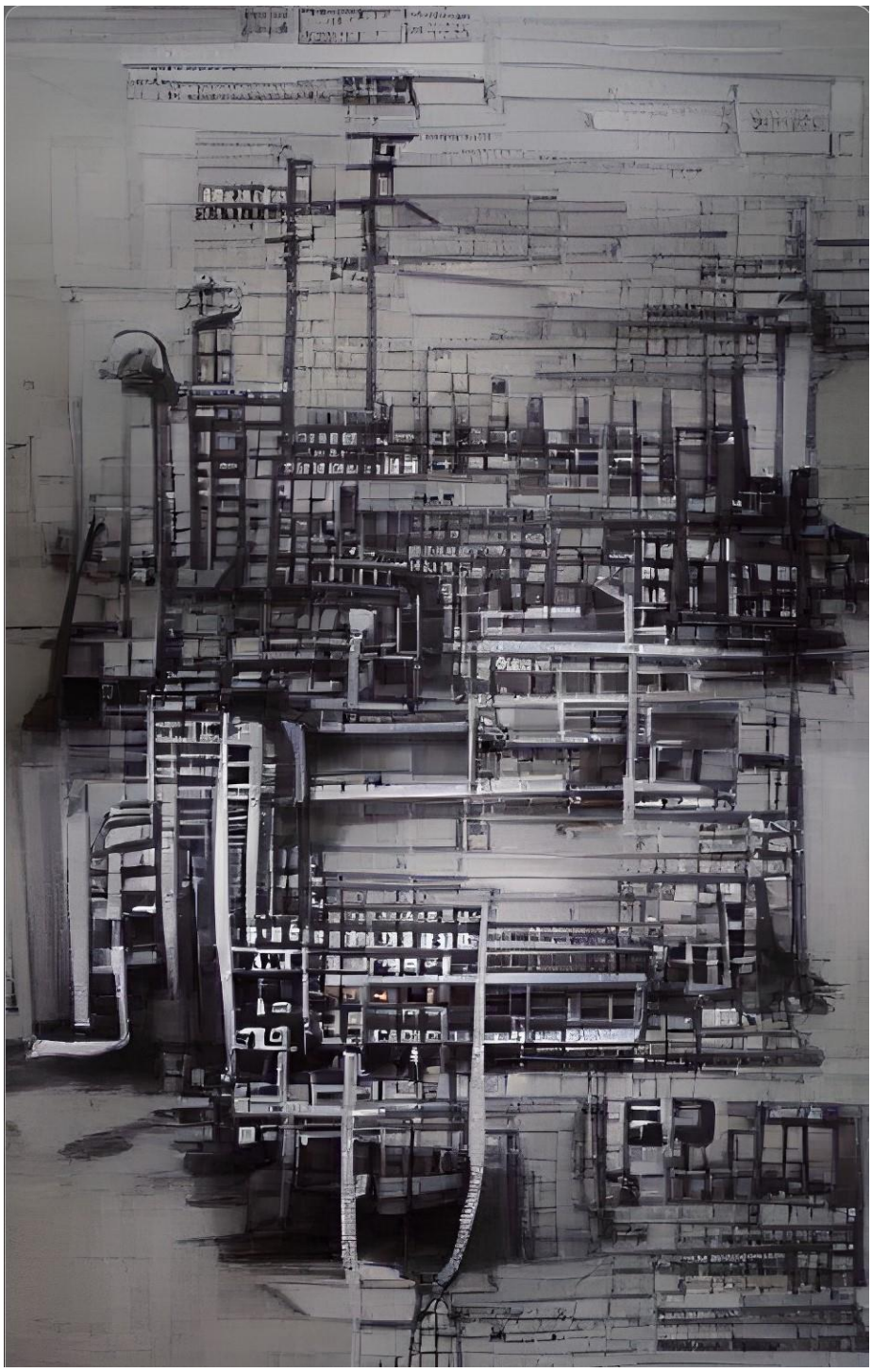
Emneord: sosioteknisk, cyberfysiske systemer, samfunnssikkerhet, smartnett, cyberfysisk systemsikring, sikkerhet

Sidetall: 81

Stavanger, 15.06.2022
dato/år

Teknologi og organisasjon i likevekt

en studie av cyberfysisk systemsikring fra et sosioteknisk perspektiv



Masteroppgave i samfunnssikkerhet
Våren 2022

Universitetet i Stavanger

Markus Isaksen

Forord

«Alt som kan gå galt, vil gå galt på det verste tidspunktet» er det noe som heter, og aldri før har denne påstanden føltes mer passende. Å skrive en masteroppgave kan noen ganger være et slit, andre ganger kan det være ekstremt givende. Det siste halvåret har bydd på rikelig av begge deler.

Å skrive denne masteroppgaven har vært den mest lærerike prosessen jeg har vært gjennom de siste fem årene her på universitetet i Stavanger. I den sammenheng vil jeg gjerne takke min veileder, Kenneth Arne Pettersen Gould. Dine råd og innspill har alltid vært veldig behjelpelig, og veiledningene har bydd på gode og produktive diskusjoner. Jeg vil også rette en takk til alle forelesere, professorer og andre ansatte på instituttet. Å ha vært en del av samfunnsikkerhets-miljøet her på UiS de siste to årene har vært et privilegium.

Jeg vil også takke informantene som stilte opp i en tidlig fase i prosjektet. Kunnskapen og innsikten jeg innhentet gjennom intervjuene har vært uvurderlig. Selv om oppgavens endelige form ikke ble helt som planlagt, setter jeg stor pris på at dere valgte å stille opp.

Til sist vil jeg takke min familie og nærmeste som har vist støtte og tålmodighet under det siste halvåret. Mine venner og medstudenter her på samfunnssikkerhet fortjener også en stor takk. Vi har alle sammen gått gjennom denne prosessen sammen, og støtten og samværet vi har delt har holdt motivasjonen oppe gjennom oppturer og nedturer.

Stavanger, 14. juni 2022
Markus Isaksen

Sammendrag

Denne oppgaven utforsker utviklingen av cyberfysiske systemer med utgangspunkt i kraftsystemet, og forskningen på cyberfysisk systemsikring av smartnett. Dette perspektivet kombineres med sosiotekniske perspektiver på ulykker, hvor organisasjon og teknologi sees i samspill og gjensidighet med hverandre. Oppgaven tilnærmer seg derfor cyberfysisk systemsikring av kraftsystemer fra et sosioteknisk perspektiv gjennom følgende problemstilling:

Hvordan kan utviklingen av cyberfysiske systemer vise seg som sosiotekniske utfordringer for risiko og sikkerhet i organisasjoner?

For å svare på denne problemstillingen tar oppgaven for seg sosioteknisk litteratur og teorier. Dette settes så i sammenheng med resultatene fra en litteraturstudie av 20 artikler om cyberfysisk systemsikring av smartnett. Gjennom en kvalitativ analyse fremhever dette studiet egenskaper ved risiko, systemsvikt og sikkerhet i cyberfysiske systemer slik presentert i forskningslitteraturen på cyberfysisk systemsikring.

Det mest fremtredende funnet fra litteraturstudiet er å vise forskningslitteraturens fokus på nye tekniske sårbarheter som har oppstått i skjæringspunktet mellom digital og fysisk teknologi og nye angrepsstrategier som utnytter sårbarheter, og tilhørende sikkerhetsbarrierer som kan forhindre dette. Cyberfysisk utvikling viser seg i en forstand som nye tekniske utfordringer for organisasjoner, hvor tettere koblinger og komplekse interaksjoner gjør systemene vanskeligere å forstå og håndtere. Denne utviklingen blir også forverret i samspill med stor usikkerhet og tvetydighet knyttet til trusselbildet systemene står overfor.

Vektleggingen av tekniske forhold i cyberfysisk systemsikring er nødvendig for utviklingen og sikringen av systemene, men systemene er stadig avhengig av mennesker og organisasjoner som designer, implementerer og drifter systemene. Oppgaven argumenterer for at sårbarheter, risiko og sikkerhet er konsepter som konstrueres av mennesker og grupper i organisasjoner, og former og formes av organisasjonens omgivelser. Den mest sentrale sosiotekniske utfordringen som diskuteres er: fremstillingen av systemene som cyberfysiske, kan potensielt neglisjere menneskelige og organisatoriske faktorer som samspiller med teknologiens utvikling og drift. Det argumenteres også for at det cyberfysiske systemperspektivet er teknosentrisk, og derfor plasseres ikke organisasjon og teknologi i likevekt.

Innhold

1.0 Innledning

*Cyberfysiske systemer (*CPS) beskriver tekniske systemer hvor fysiske og digitale prosesser utfyller hverandre og preges av tett integrasjon og interaktivitet (Lee, 2008). Fysisk infrastruktur i kraftsystemet har gradvis blitt supplert av digitale styringssystemer; en utvikling drevet av forbedret data- og prosessorkraft, og rimeligere maskinvare og programvare. I kraftbransjen viser cyberfysisk integrasjon seg i *driftskontrollsystemer*, som bidrar til å underbygge og styrke forsyningssikkerheten i det norske kraftsystemet. Denne utviklingen medfører også en endring i risiko- og sårbarhetsbildet til systemene (Hagen, 2018, s. 240). Den operasjonelle driften av kraftsystemet blir stadig mer avhengig av digitale styringssystemer, og kritikaliteten bak kraftsystemet som en kritisk infrastruktur gjør cyberfysiske driftskontrollsystemer attraktive mål for trusselaktører. Cyberfysisk systemsikring handler derfor om å forhindre og håndtere cyberangrep som kan få fysiske konsekvenser på kraftsystemet (Skotnes, 2018, s. 252).

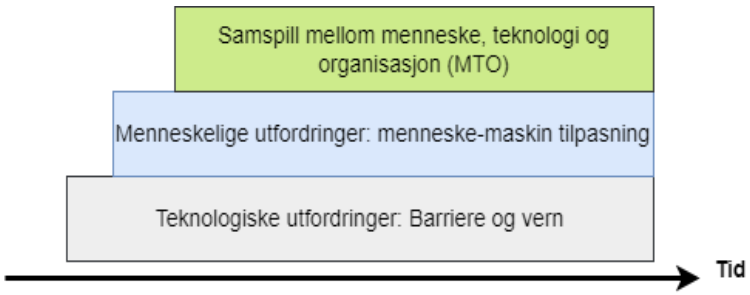
Siden CPS-begrepet først ble myntet i 2006, har det vokst frem et aktivt forskningsfelt rundt cyberfysisk systemsikring. Økt datatrafikk mellom driftskontrollsystemer og andre digitale systemer har bidratt til å effektivisere drift, men har også eksponert disse systemene for cyberdomenet, og dermed har sårbarhetsflaten vokst (Jaatun et al., 2021, s. 12). Forskningen på cyberfysisk systemsikring er derfor drevet av det tekniske; elektro- og dataingeniører og informatikere vektlegger studier av tekniske komponenter og forholdene mellom disse for å avdekke sårbarheter (Baheti & Gill, 2011).

Cyberfysisk teknologi er derimot integrert i et kraftsystem som utvikles og styres av mennesker og organisasjoner. *Systemstrukturen* er et produkt av organisasjoners behov og målsetninger (Leveson, 2011, s. 11; Perrow, 1983); og *prosesser* som ivaretar sikkerhet er grepet av større usikkerhet i møte med kompleks teknologi og mer krevende gjøremål (Turner, 1976; Vaughan, 1996). Dette er to sentrale aspekter inngår i et *sosioteknisk* perspektiv: teknologiske og menneskelige egenskaper vurderes avhengig av hverandre (Fox, 1995, s. 92). Systemsvikt og ulykke i teknologiske systemer er derfor forstått som sosiotekniske hendelser i denne oppgaven: for å forstå hvorfor systemene kan svikte må man se på det tekniske i samspill organisasjonene som designer og drifter systemene (Turner, 1994).

1.1 Sosioteknisk perspektiv i sikkerhetsforskningen

Håndteringen av risiko, sårbarhet og sikkerhet i cyberfysiske kraftsystemer er kontinuerlige prosesser som utføres innenfor rammene av organisasjoner. Et spørsmål som da oppstår, er hvorvidt forskningen på cyberfysisk systemsikring tar over seg sosiale og organisatoriske dimensjoner av sikkerhet i kraftsystemet. Behandles disse aspektene sidestilt med studier av nye cyberfysiske interaksjoner og sårbarheter? Hvilke nye utfordringer skaper cyberfysisk integrasjon for en organisasjon som forvalter denne teknologien? I denne oppgaven vil cyberfysisk systemsikring anvendt mot '*smartnett'* utforskes i sammenheng med sosioteknisk teori og litteratur på risiko, ulykker og systemsvikt.

Studier av ulykker og katastrofer i *høyrisikoteknologiske* systemer har en lang tradisjon. Basert på et studie av Hale og Hovden (1998), beskriver Kongsvik et al. (2018) det de kaller de «ulike tidsaldrene i sikkerhetsforskningen». Trinnvis har forskningen utviklet seg til å vektlegge forskjellige årsaksforklaringer til ulykker, hvor hver av delene bygger over hverandre. Forfatterne viser her til hvordan sikkerhetsforskningen gjennom iterasjon har vokst fra et perspektiv på ulykker kun som et teknisk problem, til et menneskelig, organisatorisk og teknisk problem (MTO) (Kongsvik et al., 2018, s. 39). Figur 1 illustrerer denne iterative utviklingen. I henhold til de innledende spørsmålene er det relevant å vurdere hvor i utviklingstrinnet cyberfysisk sikringsforskning befinner seg. Er det et overordnet fokus på tekniske problemer og påfølgende tekniske løsninger? Senere i oppgaven vil det sosiotekniske perspektivet på sikkerhet og ulykker utforskes. For å svare på de innledende spørsmålene og postuleringene presentert så langt, vil det derfor være nødvendig å utforske forskningslitteraturen på cyberfysisk systemsikring.



Figur 1 Trinnene i sikkerhetsforskning, tilpasset fra Kongsvik et al. (2018)

1.2 Bakgrunn

Cyber-fysisk integrasjon og omfattende digitalisering i industrielle og kommersielle prosesser er en pågående prosess beskrevet som det neste 'steget' i den industrielle revolusjonen: industri 4.0 (Lasi et al., 2014). Gjennom integrasjonen av sensorer, aktuatorer, programvare og nettverksforbindelser, blir teknologien rundt oss stadig mer sammenkoblet. 'Smart' er et moteord som gjerne brukes i denne sammenheng; 'smarttelefoner, 'smarte hus' eller 'smarte strømnett'. Dette beskriver essensielt en form for digital intelligens, hvor et mangfold av systemer utveksler informasjon og utfyller hverandres funksjoner. I industrielle formål tilføyer CPS økt effektivitet gjennom automatisering ved å redusere behov for direkte menneskelig handling. I stedet er prosesser i større grad overvåket og kontrollert gjennom digitale systemer og menneske-maskin grensesnitt (HMI) (Lu, 2017). Smartnettet er ett domene for cyber-fysisk bruk. Gjennom driftskontrollsystemer som SCADA og AMS[1] kan den operasjonelle driften av kraftsystemet i større grad fjernstyres og effektiviseres ved å redusere behov for manuelt arbeid (Frøystad et al., 2018).

1.3 Tidligere forskning

Cyberfysisk systemsikring er et omfattende fagfelt, men ikke mange studier understreker de umiddelbare sosiotekniske utfordringene som økt cyber-fysisk integrasjon innebærer. Frøystad et al. (2018) undersøker risiko- og sårbarhet som følge av økende delsystemintegrasjon, og konkluderer at tettere samspill mellom operasjonell teknologi medfører økt risiko. Humayed et al. (2017) utfører en omfattende studie av relevant CPS-sikkerhetslitteratur i et enhetlig rammeverk. Især vektlegges *komponentheterogenitet* som en viktig kilde til sårbarheter: cyberfysiske systemer bygges gjennom gradvis integrasjon av komponenter, programvare og maskiner som nødvendigvis ikke ble designet med tanke på samspill. Å anvende tekniske løsninger blir derfor stadig vanskeligere ettersom systemene blir mer sammenkoblede og mer avhengige av et utall av komponenter med ulike designforutsetninger (Humayed et al., 2017, s. 1802).

I en doktorgradsavhandling undersøkte Ruth Skotnes (2015) nyoppståtte sikkerhetsutfordringer som følge av digitalisering i kraftsystemet. Forskningen fremhever utfordringer ved regulering av IKT-sikkerhet i bransjen. Avhandlingen viser også til en lav risikooppfatning blant ansatte og ledere for tekniske feil eller dataangrep mot IKT-systemer og driftskontrollsystemer.

[1] Supervisory control and data acquisition (SCADA); Avanserte måle- og styringssystemer (AMS)

Skotnes konkluderer med at kompleksitet påvirker samtlige utfordringer knyttet til IKT-sikkerhet i kraftsystemet (Skotnes, 2015). Økende omfang og kompleksitet i cyberfysiske systemer bidrar til å gjøre sikkerheten i disse systemene mer ubegripelig for aktører uten teknisk kompetanse. For å unngå at sikkerhetsstyringen av driftskontrollsystemer blir redusert til 'skyggesiden' av organisasjoner, argumenterer Zanutto et al. (2017) for at prosessen må løftes opp og likestilles med andre mer 'håndgripelige' arbeidsoppgaver. Studiet fremhever en sosioteknisk utfordring som oppstår i krysningspunktet mellom komplekse tekniske systemer og dysfunksjonelle forhold i organisasjoner som forvalter disse systemene.

1.4 Problemstilling og forskningsspørsmål

Cyberfysisk integrasjon medfører en rekke nye utfordringer for å sikre kritiske systemer fra cyberangrep. Stadig voksende, sammenkoblede cyberfysiske systemer utfordrer systemeieres evne til å avdekke og kartlegge sårbarheter, og disse utfordringene kan også manifesteres som sosiotekniske utfordringer for organisasjonene som forvalter systemene. Det har heller ikke fremkommet vesentlig forskningsbidrag som forsøker å sette cyberfysisk systemsikring i sammenheng med et sosioteknisk perspektiv på systemsvikt og ulykker. Dette er derfor momenter som motiverer og begrunner valg av følgende problemstilling:

Hvordan kan utviklingen av cyberfysiske systemer vise seg som sosiotekniske utfordringer for risiko og sikkerhet i organisasjoner?

Denne problemstillingen vil diskuteres i oppgavens drøftingskapittel (6). Cyberfysisk integrasjon er ikke nødvendigvis en utvikling med iboende potensiale for større risiko. I henhold til problemstillingen må vi forstå dette som en pågående prosess som endrer hvordan et cyberfysisk kraftsystem opptrer og driftes. Målet med studiet er å belyse sosiotekniske utfordringer som oppstår i denne sammenheng. Dette fordrer en redegjørelse av hvilke konsepter og dimensjoner som inngår i et sosioteknisk perspektiv. For å bidra i å svare på den overordnede problemstillingen er derfor følgende forskningsspørsmål formulert:

F1: *Hvordan kan man forstå risiko, systemsvikt og sikkerhet i cyberfysiske systemer fra et sosioteknisk perspektiv?*

Dette forskningsspørsmålet vil utforskes og primært svares på i oppgavens teorikapittel (3), hvor relevant litteratur på ulykker og katastrofer i sosiotekniske systemer vil utforskes og

redegjøres for. I teorikapittelet vil også definisjoner av relevante begreper som risiko og sosioteknisk perspektiv presenteres.

Videre er det også nødvendig å etablere en forståelse av hvilke utordringer for risiko og sikkerhet som har oppstått i cyberfysiske systemer. For å artikulere utviklingen og sikkerhetsutfordringene til CPS, vil en detaljert og kvalitativ litteraturstudie gjennomføres. Derfor tilføyes et ytterligere forskningsspørsmål:

F2: *Hvordan fremstilles egenskaper ved risiko og sikkerhet i cyberfysiske smartnett av forskningslitteraturen på cyberfysisk systemsikring?*

Cyberfysiske systemer er ikke nødvendigvis kun forbundet med kraftbransjen; cyberfysisk integrasjon kan anvendes i mange forskjellige kommersielle og industrielle prosesser. I denne oppgaven vil cyberfysisk integrasjon i kraftsystemet benyttes som et 'case' for å gi en mer håndgripelig dimensjon av denne teknologiske utviklingen. Rollen cyberfysiske driftskontrollsystemer spiller i norsk kraftforsyning bidrar også til å aktualisere denne oppgaven i en samfunnssikkerhetskontekst. Forskningsspørsmål F2 vil utforskes og svares på i oppgavens litteraturstudie (kapittel 5).

1.5 Faglig relevans

Det følger fra den innledende redegjørelsen og påfølgende litteraturstudie at det kan eksistere et gap mellom forskningen på cyberfysisk systemsikring og sosiotekniske perspektiver på sikkerhet i teknologiske systemer. Målet for denne oppgaven er derfor delvis å bidra til brobygging mellom disse to perspektivene, og belyse hvordan cyberfysiske aspekter manifesteres som sosiotekniske utfordringer i organisasjonene som forvalter disse systemene. Oppgavens relevans er derfor rotet i det sosiotekniske perspektivet på systemsvikt og ulykker: uønskede hendelser i teknologiske systemer er ikke enkeltvis tekniske eller menneskelige problemer; samspillet mellom de to skiller suksess fra ulykke (Walker et al., 2008). Ved å utlede organisatoriske utfordringer fra forskningslitteraturen på cyberfysisk systemsikring, tilbyr dette studiet en unik tilnærming til risiko og sikkerhet i en kritisk infrastruktur, og tillater oss å lære om teknologi og organisasjoner fra forskjellige perspektiver.

2.0 Kontekst og systembeskrivelse

Systembeskrivelsen vil i denne oppgaven sikte til å redegjøre for nødvendig bakgrunnsinformasjon og utdype konteksten presentert innledningsvis. Det er nødvendig å danne en felles forståelse av kraftsektoren som en samfunnsfunksjon og verdikjede, nettopp for å belyse hvor i kjeden digitale sårbarheter har oppstått. For å oppnå dette vil det redegjøres for både tekniske og organisatoriske aspekter i verdikjeden. Først vil bakgrunn for kritikalitet i kraftsystemet redegjøres for. Deretter vil en grunnleggende beskrivelse av den fysiske infrastrukturen og den underbyggende digitale teknologien beskrives. Til slutt vil begrepene og konseptene informasjonssikkerhet, IKT-sikkerhet og cybersikkerhet utforskes og settes i sammenheng med det fremvoksende cyberfysiske smartnettet.

2.1 Kritikalitet bak kraftforsyningen

Et strømbrudd som varte i under ett sekund utløste en nedetid av telenettet i 5,5 timer, i Ålesund i 2014 (Hagen, 2018, s. 239). Et omfattende strømbrudd i USA og Canada i 2003 som påvirket 50 millioner mennesker, oppsto på grunn av en kombinasjon av overopphetning i et lokalt strømnett og en programvarefeil som førte til at systemoperatørene ikke hadde tilstrekkelig oversikt over situasjonen (Andersson et al., 2005). Begge hendelsene var preget av komplekse kjedereaksjoner av både menneskelige, teknologiske og organisatoriske avvik hvor ringvirkningene medførte alvorlige konsekvenser i samfunnet for øvrig: konsekvensene av strømbruddet i Nord-Amerika har blitt knyttet til opp mot 90 dødsfall (Bell & Anderson, 2012). I 2015 ble flere regionale strømnett i Ukraina utsatt for cyberangrep som medførte strømbrudd for opptil 225 000 mennesker i flere timer. Angrepet ble innledet med omfattende rekognosering for å finne sårbare nettverk og spre skadevare, før forskjellige angrepsstrategier rettet mot både operasjonell teknologi og menneskelige operatører ble utført (Liang et al., 2017).

Dette illustrerer en kritisk utfordring for samfunnssikkerheten: avhengigheten av elektrisk kraft i alle samfunnslag medfører at risiko for forsyningssvikt i kraftsystemet forplanter seg i andre samfunnsfunksjoner og infrastrukturer (Rinaldi et al., 2001, s. 15). På grunn av den gjennomgripende avhengigheten av kraft har også samfunnets forventing til forsyningssikkerheten økt (Olje- og energidepartementet, 2014, s. 16). Virksomhetene som forvalter strømforsyningen i Norge, har derfor et kritisk ansvar i å ivareta forsyningssikkerheten. Kraftsystemet som en kritisk infrastruktur er av strategisk og nasjonal interesse, og er derfor attraktivt mål for statlige og

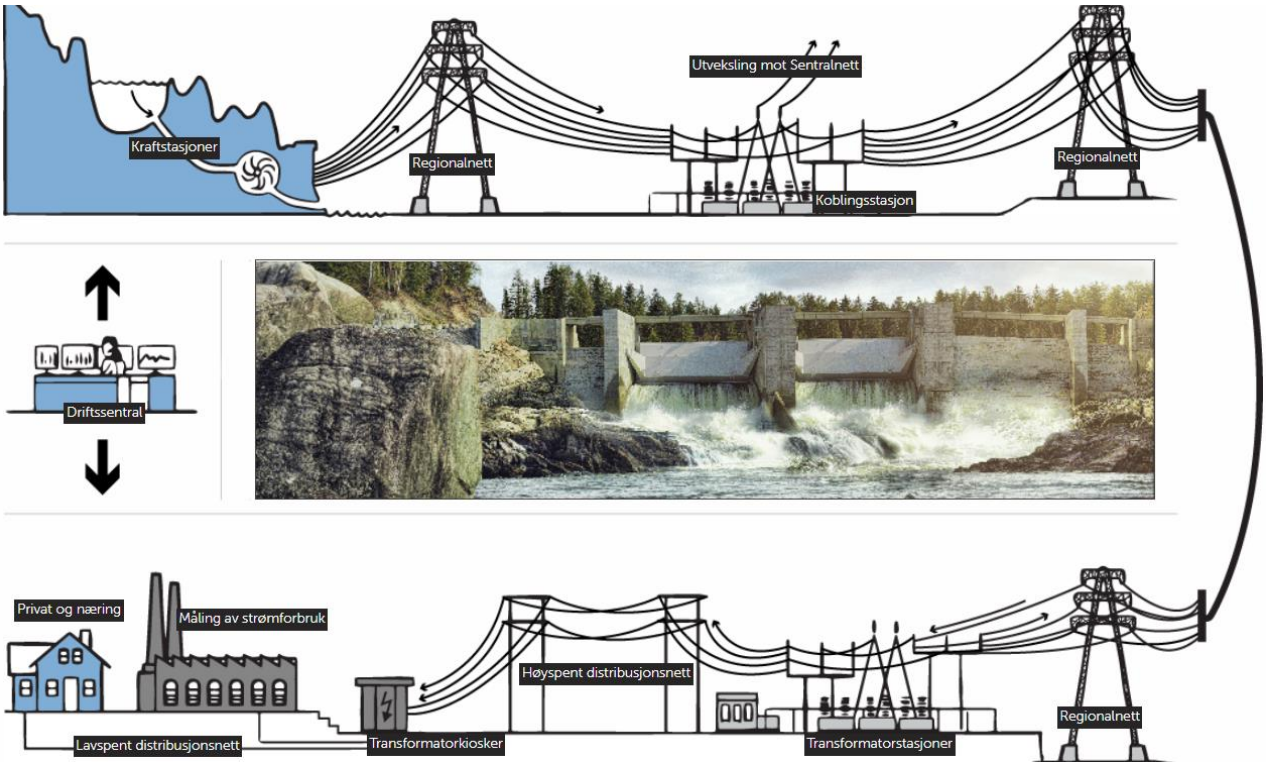
kriminelle trusselaktører. Nasjonal Sikkerhetsmyndighet (NSM) vurderer derfor kraftsystemet som en risikoutsatt sektor (NSM, 2021).

I Stortingsmeldingen 'Kraft til endring – energipolitikken mot 2030' (2015-2016) redegjøres det for flere av utviklingstrekkene som vil prege forsyningssikkerheten det neste tiåret. Her peker regjeringen på at økt elektrifisering av samfunnet også vil øke etterspørsel og belastning på nettet. Befolkningsutvikling, økonomisk vekst, elektrifisering av transportsektoren og større andel *uregulerbar* kraftproduksjon er alle viktige faktorer som kan prege forsyningssikkerheten (Meld. St. 25, 2015-2016 s. 8). Dette er en utvikling som endrer forutsetningene for *kraftbalansen* i strømnettet. Kraftsystemet avhenger enhver tid av en momentan balanse mellom produksjon og forbruk. Dette betyr at økt uttak av elektrisitet i bestemte perioder i døgnet, må kompenseres med økt produksjon i sanntid. Avvik fra denne balansen kan gjøre skade på infrastruktur og utstyr hos sluttbrukeren (Meld. St. 25, 2015-2016, s. 45; Olje- og energidepartementet, 2014, s. 16). Tilpasning av produksjon etter forbruk er forholdsvis enkelt fra regulerbare energikilder som vannkraftverk med magasinkapasitet. I perioder med høyt tilsig av vann, kan dette lagres og benyttes i perioder med lavt tilsig. Dette er ikke mulig med uregulerbar kraftproduksjon som f.eks. vindkraft og solkraft: produksjonsevnen avhenger av de umiddelbare værforholdene (Meld. St. 25, 2015-2016). Utviklingen av kraftsystemet peker derfor mot et større behov for økt fleksibilitet i produksjon og forbruk, og integrasjon i hele verdikjeden fra produksjon til sluttbruker (Olje- og energidepartementet, 2014).

2.2 Systembeskrivelse

Det norske kraftsystemet består av et mangfold av aktører involvert i produksjon, distribusjon, forsyning, tilsyn og forvaltning på flere nivåer. Dagens kraftsektor er organisert som et deregulert marked hvor både offentlige og privateide aktører produserer tjenester for forbrukerne. Likevel er det norske kommuner, fylker og sentrale myndigheter som besitter størst eierandel i både produksjonsselskaper og nettselskaper (Olje- og energidepartementet, 2019). Norsk kraftsektor er derfor underlagt politiske føringer som vedtatt på stortinget, hvorav regjeringen gjennom Olje- og energidepartementet (OED) har overordnet ansvar for forvaltning av kraftsektoren. Underlagt OED finner vi Statnett SF, som besitter et 'systemansvar'. Dette vil si at foretaket er ansvarlig for å tilrettelegge for tilstrekkelig leveringskvalitet i hele landet, koordinering mellom aktører samt å pålegge virksomheter oppgaver og plikter (Statnett, 2021).

I Norge er ca. 98% av kraftproduksjonen fornybar, hvor mesteparten av dette kommer fra vannkraft (Meld. St. 25 (2015-2016). Det er hos kraftprodusentene denne verdikjeden begynner. Elektrisk energi fra produksjon og import overføres via *transmisjonsnettet* på tvers av hele landet. Energien når forbrukerne gjennom *regional*- og *distribusjonsnettene*, som distribuerer strøm til lokale husholdninger og næring. For å transportere energi over lange avstander må transformatorstasjoner øke *spenningen* i transmisjonsnettet og deler av regionalnettet. Før strømmen distribueres til forbrukeren må transformatorstasjoner og transformatorkiosker igjen redusere spenningen. Figur 2 illustrerer denne verdikjeden (Glitre Energi, 2022). kraftsystemet er organisert etter formål og funksjon til de enkelte tjenestene i verdikjeden. Kraftprodusentene er markedsutsatte virksomheter og aktører som selger strøm til forbrukere. Strømnettet er et naturlig monopol, ettersom transmisjon og distribusjon ikke kan konkurranseutsettes. Det er derfor lovpålagt å ha et selskapsmessig og funksjonelt skille mellom konkurranseutsatt produksjon og salg og nettdrift (Olje- og energidepartementet, 2014, s. 33).



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

Transmisjonsnettet er primært eid og forvaltet av Statnett SF, et statsforetak underlagt Olje- og energidepartementet. Statnett har systemansvar for kraftsystemet. Dette innebærer å opprettholde kraftmarkedet gjennom overvåkning av spenningsnivå, frekvensnivå og momentan balanse, koordinering av drift og håndtering av utenlandsforbindelser (Meld. St. 25 (2015-2016) s. 45). Regional- og distribusjonsnettene forvaltes og eies av nettselskapene som får konsesjonsrettigheter til å utbygge og forvalte nettet innenfor et geografisk område. Nettselskapene er hovedsakelig eid av kommunene og fylkeskommunene i områdene nettselskapene drifter (Almklov, et al., 2008). Skillet mellom monopolvirksomhet (nett) og markedsvirksomhet (produksjon, salg) medfører at nettselskapene driftes selvstendig fra kraftprodusentene og leverandørene. Leverandør og nettselskap er ofte organisert under samme konsernledelse derimot, hvor nettselskapene eksisterer som selvstendige rettssubjekt (Olje- og energidepartementet, 2014).

Verdikjeden bindes sammen i driftssentralene, hvor produksjon, transmisjon og distribusjon kan overvåkes og styres. Driftssentralen er et viktig digitaliseringsområde i kraftbransjen, hvor nye digitale løsninger gir nettselskaper og kraftprodusenter bedre oversikt over systemtilstanden og raskt kan respondere dersom det oppstår avvik (Meld. St. 25 (2015-2016). Det lovpålagte skillet mellom monopolvirksomhet og markedsvirksomhet innebærer også at driftskontrollsystemer og driftssentraler for distribusjon opereres selvstendig fra produksjon og transmisjon. Dette betyr at nettselskapene ofte har sin egen driftssentral som overvåker og styrer deres strømnett og transformatorstasjoner, og disse er selvstendige fra driftssentraler for transmisjon og produksjon. I tillegg til dette er kraftsystemet i Norge koblet opp både fysisk og digitalt til det nordiske kraftmarkedet 'Nord Pool' (Meld. St. 25 (2015-2016), s. 32). Primært har driften av produksjon, transmisjon og distribusjon vært overvåket og styrt gjennom et system som kalles *Supervisory Control and Data Acquisition* (SCADA), men de siste årene har også andre typer teknologier blitt integrert i kraftsystemet (NOU 2015:13, 2015, s. 137). SCADA er et sentralt verktøy i det man kaller driftskontrollsystemer. Det er denne typen digitale styringssystemer som har bidratt til å binde verdikjeden i kraftsystemet tettere sammen. Digitale styringssystemer har åpnet opp for mer effektiv drift, større grad av automatisering og redusert behov for nye investeringer i strømnettet (Meld. St. 25 (2015-2016), s. 144).

2.3 'Smartnettet'

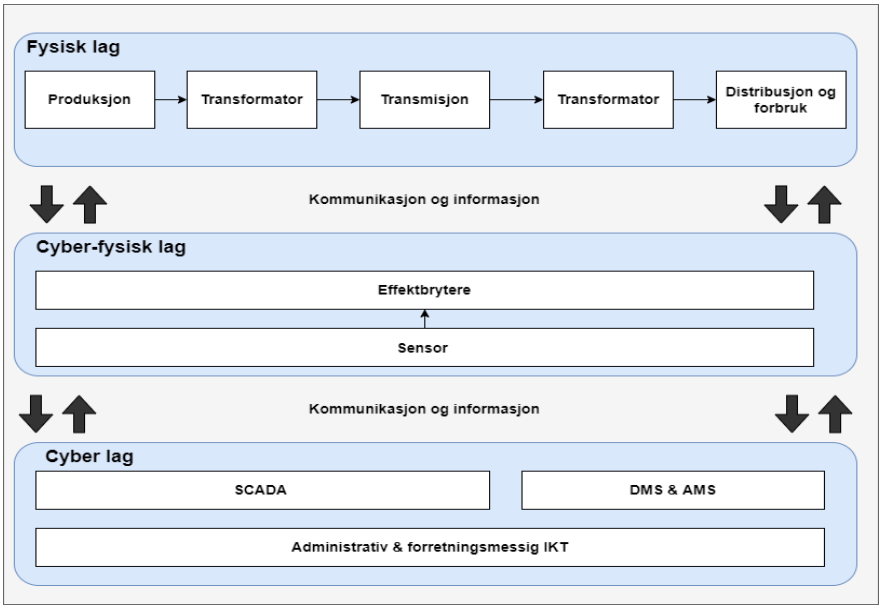
'Smartnettet' som en betegnelse beskriver et kraftsystem som imøtekommer behovet for tettere samspill i verdikjeden gjennom 'smart' bruk av IKT-systemer. Med 'smart' menes det en dypere integrasjon mellom fysisk infrastruktur og IKT for å overvåke og tilpasse produksjon og forbruk i sanntid (Harrison et al., 2010, s. 8). Ved å utplassere sensorer eller målestasjoner hos sluttbrukere og infrastrukturinstallasjoner kan relevant informasjon samles inn i sanntid og benyttes til å tilpasse systemdriften etter behov. Forbedringer i programvare, fastvare og databehandlingsevne utgjør også en mulighet til å automatisere og dermed effektivisere prosesser som tidligere krevde manuell behandling. Digitale systemer benyttes i alle vesentlige prosesser i dagens kraftsystem: alt fra å opprette nye strømkunder, styre åpne- og lukkemekanismer i et produksjonsanlegg, eller overvåke spenningsnivå og momentan balanse.

Behovet for tettere integrasjon i hele kraftsystemets verdikjede har ført til økt integrasjon mellom IKT og *operasjonell teknologi*; driftskontrollsystemer som blant annet SCADA. I sammenheng med den digitale transformasjonen av samfunnet, har industrielle prosesser som tidligere ble overvåket og styrt fysisk og manuelt, eller gjennom elektromekaniske driftssystemer, over tid blitt erstattet med digitale styringssystemer (Hagen, 2018, s. 241). I kraftbransjen har tilgang til kostnadseffektive og standardisert fastvare og programvare ført til en tettere integrasjon mellom IKT og driftskontrollsystemer. Driftskontrollsystemer har historisk sett vært lukkede systemer, og derfor var ikke sikkerhet en prioritet når systemene ble designet og implementert. Siden har mange av disse driftskontrollsystemene blitt koblet opp mot IKT-systemer, og dermed også administrative funksjoner og internettforbindelser (NOU 2015:13, s. 137). Denne utviklingen har medført at driftskontrollsystemene er mindre isolerte fra utsiden og dermed får sikringen av IKT-systemene langt større betydning enn tidligere (Skotnes, 2015, s. 11).

2.4 AMS og SCADA-systemer

Driftskontrollsystemer er en form for cyberfysiske systemer som er godt integrert i det norske kraftsystemet (Skotnes, 2018, s. 257). Avanserte måle- og styringssystemer (AMS), også kalt 'smarte målere' er målere som registrerer forbruk, overvåker spenningsnivå og oppdager avvik. Dette har bidratt til å effektivisere bruken av nettet og redusert fremtidige investeringskostnader (Meld. St. 25, 2015-2016, s. 144). AMS-systemet har også bidratt til å redusere manuell behandling av måledata, slik at kraftselskaper lettere kan forvalte flere kunder uten å vesentlig øke antallet ansatte. Data og oversikt over forbruk i sanntid samspiller også med andre

operasjonelle systemer som SCADA. SCADA-systemer muliggjør fjernstyring og overvåkning av strømnett, produksjonsanlegg og andre fysiske prosesser. Åpne- og lukkemekanismer i et produksjonsanlegg eller effektbrytere i et distribusjonsnett kan fjernstyres og tilpasses basert på sanntidsinformasjon. Gjennom et brukergrensesnitt på en datamaskin kan disse prosessene overvåkes og kontrolleres. En samling av sensorer, aktuatorer, fastvare og programvare bidrar til at fysiske prosesser kan utføres i sanntid, ubetinget av geografisk avstand (Frøystad et al., 2018). SCADA-systemer sitter på skjæringspunktet mellom det fysiske og digitale, og skiller seg fra tradisjonelle IKT-systemer i sin cyberfysiske funksjon og kompleksitet (Skotnes, 2018, s. 257).



Figur 3 Modell av lagene i et smartnett

Figur 3 viser en forenklet fremstilling av hvordan smartnettet nå driftes ved hjelp av cyberfysiske systemer. Det 'fysiske laget' er fortsatt gjenkjennelig ved den lineære prosessen fra produksjon til forbruk. I enkleste forstand innebærer dette systemet sensorer og målere som samler inn data fra det fysiske laget. Effektbrytere og aktuatorer er manipulerbare brytere som muliggjør fjernstyring av det fysiske laget. Sammen utgjør dette det cyberfysiske laget. Data i form av målinger oppfattes i det fysiske laget via det cyberfysiske, og sendes til driftssentraler hvor operatører overvåker og styrer systemene gjennom HMI. Det cyberfysiske systemet er derfor preget av kontinuerlig flyt av informasjon og kommunikasjon mellom lagene i sanntid. Informasjon basert på datainnsamlingen kan så benyttes i organisasjonens administrative og forretningsmessige aktiviteter, og motsatt; produksjon i et vannkraftverk kan for eksempel økes eller reduseres basert på forventede variasjoner i strømpriser.

IKT underbygger derfor arbeidet med å opprettholde kraftbalansen og dermed også forsyningssikkerheten. Det enorme mangfoldet og potensialet til informasjonslagring og databehandling IKT besitter, samt evnen til å samhandle med og dele denne informasjonen i sanntid, utgjør en del av 'smartheten' som imøtekommer behovet for tettere samspill i nettet. Langs hele kraftsystemets verdikjede; fra produksjon, til transmisjon og distribusjon, blir tidligere analoge prosesser og funksjoner supplert, erstattet og effektivisert av informasjons- og kommunikasjonsteknologi (IKT) (Engen et al., 2021, s. 244; Meld. St. 25 (2015-2016), s. 144). Risikobildet til kraftsystemet har således endret seg og IKT-sikkerhet har blitt mye viktigere i kraftbransjen som følge av digitaliseringen (Skotnes, 2018, s. 253). Skillelinjene mellom IKT-sikkerhet og forsyningssikkerhet blir dermed mer tvetydig når IKT blir mer integrert i daglig drift.

2.5 Informasjonssikkerhet

Sikkerhet i det digitale rom blir ofte beskrevet med flere ulike utrykk. Begreper som datasikkerhet, digital sikkerhet, informasjonssikkerhet, cybersikkerhet og IKT-sikkerhet er ofte brukt om hverandre uten en tydelig avklaring. Det kan ses på sikkerhet knyttet til de fysiske komponentene (hardware), programvare som kjøres på de fysiske komponentene (software), samt andre tjenester som eksempelvis sky- og lagringstjenester. IKT-systemer betegnes ofte som informasjonssystemer, og derfor blir *informasjonssikkerhet* brukt av mange som begrep for sikkerhet i disse systemene (Lundgren et al., 2019).

Kjernen i informasjonssikkerhet ligger i å bevare og beskytte *informasjon* fra uautoriserte. Dette innebærer informasjon og data i seg selv, men også IKT-infrastrukturen som oppbevarer, distribuerer og behandler data, enten det er fastvare, programvare eller skytjenester. Skade på informasjonsverdier knyttes ofte til informasjonens konfidensialitet, integritet og tilgjengelighet (KIT). KIT-sikkerhetsmålene har siden begynnelsen av 2000-tallet blitt brukt som en bransjestandard for informasjonssikkerhet (von Solms & van Niekerk, 2013). En vanlig definisjon av informasjonssikkerhet knyttes til opprettholdelse av disse sikkerhetsmålene: informasjonen er sikker dersom konfidensialiteten, integriteten og tilgjengeligheten opprettholdes (Lundgren et al., 2019). Konfidensialitet handler om å kontrollere adgang til informasjon og forhindre at uautoriserte personer får tilgang. Integritet kan omfatte både dataintegritet; at data ikke blir endret eller slettet, og systemintegritet; at prosesser og funksjoner som oppbevarer og behandler data ikke manipuleres av uautoriserte. Tilgjengelighet betyr at autoriserte personer har tilgang til og kan benytte seg av data og digitale funksjoner ved behov (Jøsang, 2021).

I utgangspunktet omfatter informasjonssikkerhet også beskyttelse av fysisk og analog data som arkiver og papirdokumenter. Informasjonslekkasjer, spionasje og «utro tjenere»; ansatte som bevisst deler informasjon for egen gevinst, utgjør også brudd på KIT og vil derfor falle inn under informasjonssikkerhet. Informasjonssikkerhet favner derfor et bredt spekter av risikoer og sikkerhetsløsninger. Fysisk sikring, kryptering, brannmurer, regelverk, rutiner, ressurser, prioriteringer, organisatoriske egenskaper, psykologi, atferd og bevissthet hos ansatte er bare et utvalg at faktorer som har blitt studert i sammenheng med informasjonssikkerhet (Diesch et al., 2020). Det er nettopp dette tverrfaglige mangfoldet som har gjort informasjonssikkerhet til et attraktivt forskningsfelt, men dette medfører også at begrepet blir svært omfattende.

Data som utgjør informasjon i et kraftsystem, kommer i mange forskjellige typer og lagringsmåter. sensorer i feltet samler inn data om spenningsnivåer og frekvensnivåer nettet; tilsig i vassdrag, issmelting i fjellet måles og formidles til systemoperatører som gjør tilsvarende handlinger basert på denne informasjonen. Data i form av kundeopplysninger, forbruk og adresser inngår i kraftselskapene kunderegistre. Interne styringsdokumenter, beredskapsplaner, lister over personalia, etc. Denne dataen er igjen lagret på forskjellige måter: lokale harddisker, i sky, papirdokumenter eller i ansattes hukommelse. Konfidensialitet, integritet og tilgjengelighet beskriver ulike aspekter av sikkerheten ved denne dataen: hvordan er den skjermet fra utenforstående og hvilke konsekvenser kan det ha hvis KIT for denne dataen brytes? Kritikaliteten bak en bestemt type data varierer etter dataens formål, for eksempel prisdata på elektrisitet. Dette er offentlig tilgjengelig informasjon, og derfor er konfidensialitet ikke et problem. Dersom man vurderer integritet imidlertid: manipulering av prisdata kan forårsake alvorlige ringvirkninger for systemet og samfunnet for øvrig. Forbrukerne justerer forbruket og kraftselskapene justerer produksjon basert på prising (Attia et al., 2018).

2.6 IKT-sikkerhet og Cybersikkerhet

Omfattende digitalisering av samfunnet har medført at IKT-systemer i dag gjennomsyrer stadig flere domener. Utviklingen har medført at systemer som tradisjonelt har blitt kontrollert og overvåket fysisk, nå blir styrt via digital kommunikasjonsteknologi. Disse cyberfysiske systemene har fundamentalt endret hvordan vi interagerer med den fysiske verden rundt oss: det åpner for nye muligheter, effektivitet og produktivitet, men skaper også nye sårbarhetsflater (Rajkumar et al., 2010). Det digitale risikobildet har utviklet seg til å omfatte mer sofistikerte trusler. Bruken av digitale systemer til operasjonell drift av kraftsystemet har som tidligere beskrevet gjort forsyningssikkerheten sårbar for cyberangrep. Det digitale risikobildet har utviklet seg til å omfatte mer sofistikerte trusler. I lys av denne utviklingen har fagfolk påpekt at informasjonssikkerhetsbegrepet ikke tilstrekkelig omfavner disse farene (Yin et al., 2020). Cybersikkerhetsbegrepet har oppstått i denne sammenheng. Begrepet beskriver sikringen av det såkalte "cyberspace", et noe mer diffust begrep, men det er nettopp behovet for å benytte et begrep som omfatter et stadig ekspanderende nettverk av systemer og maskiner samt menneskene som samhandler med disse systemene (Langø, 2013; Langø & Sandvik, 2013). Cybersikkerhet er derfor ikke synonymt med informasjonssikkerhet eller IKT-sikkerhet, men disse konseptene kan heller betegnes som underliggende sårbarheter i cybersikkerhetslandskapet (von Solms & van Niekerk, 2013).

Operasjonell teknologi har lenge eksistert for å fungere under utfordrende værforhold, for eksempel på oljeplattformer i Nordsjøen eller infrastruktur ute i landskapet. Etter hvert som OT-systemer i større grad integreres med IKT for driftseffektivisering eller administrasjon, gjør dette også systemene sårbare for cybertrusler (Jaatun et al., 2021). Digitale sårbarheter i driftskontrollsystemer benyttet i kraftsystemet utgjør en risiko for forsyningssikkerheten, og dermed også en risiko for liv, helse eller materielle verdier i samfunnet. Denne risikoen strekker seg forbi grensene til KIT-sikkerhetsmålene i den forstand at informasjonsverdiene i seg selv ikke er den kritiske sikkerhetsverdien, men heller tilstanden til systemet som underbygges av informasjonssystemet (von Solms & van Niekerk, 2013). KIT-sikkerhetsmålene benyttes fortsatt som kriterier for sikkerhet i cyberfysiske systemer, men konsekvensene av KIT-brudd er forlenget til å omfatte uønskede fysiske tilstander i systemet (Gunduz & Das, 2020). Cyberbegrepet slik det blir anvendt i denne oppgaven beskriver derfor ikke kun sårbarheter i informasjonsverdier, men **alt** som er sårbart gjennom tilknytning til cyberdomenet (von Solms & van Niekerk, 2013, s. 100).

2.7 IKT-sikkerhetstilstanden i det norske kraftsystemet

I en rapport fra 2021 konkluderte Riksrevisjonen at tilsyn av IKT-sikkerhet og beredskap mot IKT-angrep i kraftbransjen ikke er god nok (Riksrevisjonen, 2021). Kritikken er rettet mot Norges Vassdrags- og Energidirektorat; tilsynsmyndigheten som gjennom regelverk, kompetansebygging, overvåkning og varsling, ivaretar beredskapen i kraftsystemet. Riksrevisjonens rapport belyser behovet for å fokusere på digital risiko når kraftsystemet i økende grad digitaliseres (NVE, 2021). I en NVE-rapport fra 2021 kartlegges konsekvensene av cyberangrep mot administrative IKT-systemer og industrielle kontrollsystemer: selv om rapporten ikke kan vise til svikt i kraftforsyningen som følge av driftshendelser eller cyberangrep, påpeker den mangelfull kartlegging av enheter og programvare i de voksende cyber-fysiske systemene (Tøien et al., 2021). Lignende rapporter utført forholdsvis av Sintef (Frøystad et al., 2018) og Proactima (Røyksund & Valdal, 2020) på vegne av NVE, belyser også økt integrasjon mellom eldre fysisk infrastruktur og nyere digitale komponenter og systemer. Rapportene konkluderer med et behov for å styrke kompetansen om egne systemer for å forstå risiko og sårbarheter som oppstår når kraftsystemet digitaliseres.

2.8 Organisatoriske forutsetninger for IKT-sikkerhet

Utfordringer knyttet til informasjonssikkerhet kan ikke imøtekommes med tekniske løsninger alene. IKT-systemer gjennomsyrer i dag hverdagslige arbeidsprosesser og det følger at feil oppstår i grensesnittet mellom menneske og maskin. I faglitteraturen blir derfor informasjonssikkerhet fremhevet ved en ledelse- og virksomhetsdimensjon, i tillegg til en teknisk dimensjon (Chang & Ho, 2006; Soomro et al., 2016; von Solms & von Solms, 2004). Denne forankringen forsterkes gjennom forskning som belyser rollen menneskelige faktorer spiller i digitale sikkerhetshendelser (Evans et al., 2019; Kraemer et al., 2009; Kraemer & Carayon, 2007). Menneskelige faktorer kan beskrive enkle hendelser som å sende en e-post til feil mottaker, mangelfull overholdelse av regler eller målrettede angrep som sosialt manipulerer ansatte til bistå i tilsiktede handlinger (Taib et al., 2019).

Konvergeringen av IKT og operasjonell teknologi har gjort forsyningssikkerheten mer avhengig av sikkerhet i digitale systemer. Det er derfor en rekke IKT-sikkerhetsutfordringer aktørene i kraftbransjen må imøtekomme. Digitalisering og utbredelse av standardiserte IKT-systemer for administrasjon og drift har gjort kraftbransjen mer avhengig av eksterne aktører og

leverandører (Selnes et al., 2021). En virksomhet i kraftbransjen vil ofte benytte seg av samtlige leverandører av programvare, fastvare og komponenter som tilhører komplekse og globale verdikjeder. Lange verdikjeder skaper både en avhengighet av ekstern kompetanse og utstyr, men det medfører også sårbarheter når leverandøren i seg selv blir et mål for cyberangrep (Hagen, 2018; Selnes et al., 2021). Digitale systemer kan i denne forstand fremstå som et 'ferdig produkt' virksomheter i kraftbransjen kan anskaffe og dermed også redusere kompetansebyrden på egen organisasjon. En slik utvikling kan også settes i sammenheng med funn som viser at det trolig vil være vesentlig mangel på IKT-sikkerhetskompetanse i Norge frem mot 2030 (Mark et al., 2019). Risikostyring i anskaffelsesfasen får derfor langt større betydning i sammenheng med IKT-sikkerheten i kraftbransjen. Dette er et eksempel på en utfordring som ikke nødvendigvis er grunnet i tekniske sårbarheter, men heller organisatoriske og interorganisatoriske forhold.

Deregulert forvaltningsstruktur i kraftbransjen har også endret organisatoriske forutsetninger for IKT-sikkerhetstjenester. Digitalisering og IKT-systemer har vært en viktig pådriver for bestiller- utfører modellen som preger kraftbransjen, hvor tjenesteutvikling 'moduliseres' og konkurranseutsettes (Almklov, et al., 2008;Almklov & Antonsen, 2010). Digitalisering, deregulering, privatisering og transnasjonal markedsutsetning er pådrivere for globaliseringen som i gjengjeld også former høyteknologiske systemer og organisasjonene som forvalter systemene (Le Coze, 2021, s. 105). IKT-tjenester reduserer 'avstanden' mellom mennesker og organisasjoner og utfordrer tradisjonelle byråkratiserende idealer blant annet ved outsourcing av kompetanse. Rask digitalisering har etterlatt et gap mellom behovet for IKT-sikkerhetskompetanse og den kompetansen som samfunnet produserer (Mark et al., 2019). Mangel på IKT kompetanse er også en utfordring for virksomheter i kraftbransjen og et fokusområde for NVE (Tøien et al., 2021). Eksemplene illustrerer dermed et mer komplekst og sammensatt sikkerhetsbilde for kraftsystemet.

3. Teori

Hensikten med teorikapittelet er å utforske forskningsspørsmålet: *Hvordan kan organisatoriske og sosiotekniske forhold påvirke risiko og sikkerhet i cyberfysiske systemer?* Teorikapittelet er todelt: først vil det redegjøres for den teoretiske bakgrunnen til relevante begreper som risiko, usikkerhet og sikkerhet. En ytterligere beskrivelse av begrepet cyberfysiske systemer følger også. I den andre delen vil relevant litteratur om ulykker og katastrofer i sosiotekniske systemer redegjøres for. Målet med teorikapittelet er derfor å etablere en forståelse av samspillet mellom teknologi, menneske og organisasjon i sammenheng med risiko og sikkerhet.

3.1 Risiko, sikkerhet og usikkerhet

3.1.1 Risiko og usikkerhet

Tilnærmingene til risiko og risikobegrepet er mangfoldige, men grunnleggende kan man peke til begrepet som et uttrykk eller beskrivelse av mulige *fremtidige* hendelser eller tilstander (Engen, et al., 2016; Solberg & Njå, 2012). Ingeniører og teknologer uttrykker ofte risiko som et produkt av sannsynlighet og konsekvens ved en uønsket hendelse (Lupton, 2013). Et slikt perspektiv på risiko er også vanlig innenfor IKT-sikkerhet, hvor statistiske analysemodeller, simulasjoner og andre teknisk-vitenskapelige metoder benyttes for å tallfeste sannsynligheter (Ciborra, 2007). Lupton (2013) Beskriver dette som et 'realistisk' risikoperspektiv: risiko er et reelt og objektivt fenomen og ved å anvende vitenskapelige metoder kan denne risikoen avdekkes. Risikoforskning innen dette perspektivet er derfor mer opptatt av normative, ideelle modeller og metoder for å måle og kalkulere risiko (Lupton, 2013).

Dette perspektivet er ofte kontrastert med det *konstruktivistiske* perspektivet på risiko. Utrykk for risiko er en *vurdering* av hva som kan skje i fremtiden. I denne vurderingen benyttes kunnskap, erfaringer og oppfatninger av virkeligheten. Risiko uttrykkes også i sammenheng med noe vi verdsetter; liv og helse, miljø og materielle og immaterielle verdier (Renn, 2008). Fremtiden er også beheftet av *usikkerhet*; vi kan ikke med visshet si hvordan den vil utfolde seg. Risiko og usikkerhet er i denne forstand sammenvevde konsepter (Aven, 2016; Pettersen, 2016). Usikkerhet kan omfatte ufullstendig kunnskap eller tvetydighet knyttet til hvordan kunnskapen skal fortolkes. Det kan også råde usikkerhet rundt hvilken risiko man kan akseptere, hvordan man skal forholde seg til ulike risikoer og hvilke virkemidler man skal benytte (Renn, 2008). Vurdererens faglige, sosiale eller politiske kontekst kan prege hvordan kunnskap om risiko genereres og fremstilles. Risiko er avhengig av den sosio-kulturelle konteksten

bedømmeren befinner seg i (Lupton, 2013); vurderingen er et resultat av vurdererens subjektive virkelighetsforståelse (Aven, 2016).

Dette vil også være den rådene forståelsen av risiko i denne oppgaven. Aven, m.fl. har definert risiko som «konsekvensene av en aktivitet og tilhørende usikkerhet i sammenheng med noe mennesker verdsetter» (Aven & Renn, 2009, s. 6; Aven & Thekdi, 2022). I denne oppgaven vil risikobegrepet forstås deretter. Risiko er en vurdering av mulige fremtidige hendelser og konsekvensene av disse. Dette er vurderinger beheftet av usikkerhet; vi vet ikke hva som vil skje og hva konsekvensene vil være. Vi vurderer dette i sammenheng med verdier man ønsker å beskytte. Uttrykk og kunnskap om risiko er formet av den sosiale og institusjonelle konteksten den befinner seg i, og er derfor et produkt av bedømmeren. Det burde også merkes at Avens tilnærming til risiko presentert her, mer korrekt kan betegnes som en *svak konstruktivisme*. Farer kan ifølge Aven og Renn (2009) eksistere uavhengig av vår erfaring. Det er først når faren oppfattes at den viser seg som en risiko for bedømmeren. Diskusjoner om risikoens ontologi begrenses til dette; det viktigste å poengtere i denne sammenheng forståelsen av risiko som en vurdering av usikkerhet knyttet til fremtidige hendelser.

3.1.2 Hva er sikkerhet?

Aven (2009) presenterer sikkerhet (safety) som antonymet til risiko, hvor lav risiko betyr høy grad av sikkerhet og fravær av stor farepotensiale. Det er derimot ikke mulig å redusere risiko til null; det vil alltid eksistere en usikkerhet om hva som vil skje i fremtiden. Hva som er 'sikkert nok' er derfor en subjektiv vurdering, hvor aktørene som vurderer risikoen også er ansvarlige for å identifisere hvilken grad av risiko som er akseptabel (Aven, 2009). Systemeiere kan benytte seg av risikoanalysemodeller eller andre kunnskapsbaserte verktøy for å beskrive eller tallfeste denne risikoen i systemet, men ifølge Aven kan ikke de samme redskapene avklare hvilken risiko man skal akseptere eller om gevinsten utveier eventuelle negative konsekvenser. Sikkerhet og trygghet er derfor underlagt kunnskapen om konsekvenser og tilhørende usikkerhet knyttet til en aktivitet eller handling. Risiko og sikkerhet henger ifølge Aven og Renns (2009) definisjon, konseptuelt sammen (Aven, 2009). I denne forstand betyr sikkerhet 'frihet' fra uakseptabel risiko, og sikkerhet som en tilstand er en ikke-hendelse eller fravær av negative hendelser (Hollnagel, 2014).

Digitaliseringen har medført at IKT-systemer nå gjennomsyrer organisasjoner til det punktet hvor et skille mellom teknologi og organisasjon ikke lenger er hensiktsmessig (Hanseth, 2007;

Werlinger et al., 2009). Dette påvirker også hvordan man forstår risiko og sikkerhet i digitale systemer; risiko er preget av interaksjonen mellom menneskelige, organisatoriske og teknologiske faktorer (Lundgren et al., 2019). Kalkulert risiko kan uttrykke hvor trolig en fremtidig hendelse er basert på historisk data, men den kan ikke fortelle oss hvordan man skal respondere på denne risikoen. Kvantitative uttrykk for risiko forutsetter også at man har et stort nok omfang av historisk data å basere analysen på. Tilgang på slik data er ofte en utfordring knyttet til tilsiktede handlinger, på grunn av den relativt lave frekvensen av slike hendelser (Jore, 2017). Sosiotekniske systemer gjennomsyret av IKT har også blitt større og mer komplekse, mindre forutsigbare og håndterbare (Hollnagel, 2014). Dette gjør sammenhenger mellom årsak og virkning mindre lineære, og modelleringer av dette blir vanskeligere.

3.1.3 Trussel, sårbarhet og verdi: cyberrisiko

Engelskspråklig litteratur benytter oftest ulike begreper; hvor 'security' (sikring) refererer til tilsiktede handlinger og 'safety' (sikkerhet) refererer til ikke-tilsiktede hendelser (Smith & Brooks, 2013). Jore (2017) tilskriver sikring et ytterligere kriterie ved å være ondsinnet i tillegg til tilsiktet. Det skilles derfor mellom risikokilder (Blokland & Reniers, 2020); hvor sikringsrisiko kan være hackerangrep, sabotasje eller terrorisme, mens en sikkerhetsrisiko kan være en arbeidsulykke, komponentsvik, eller skade påført som følge av naturhendelser. En komponentsvikt kan utløses av upålitelighet i selve komponenten, skade påført fra omgivelser eller mennesker som interagerer med den, enten tilsiktet eller ikke-tilsiktet. En handling eller hendelse kan dermed ha samme eller lignende konsekvenser, men forskjellig risikokilde. På norsk blir begrepet sikkerhet brukt både i sammenheng med tilsiktede handlinger og ikke-tilsiktede hendelser (Engen, et al., 2016). Aven og Renns (2009) risikodefinisjon skiller ikke mellom tilsiktet og ikke-tilsiktete hendelser, så lav risiko kan anses som anonymet til sikkerhet både i safety og security forstand (Aven, 2014). Skillet mellom safety/security kan tilskrives som en karakteristikk av risikoen, og dette kan ha implikasjoner for hvordan man responderer og styrer risikoen.

Når risiko vurderes som sannsynlighet x konsekvens slik det realistiske perspektivet ofte gjør, fordrer dette at man har et tilstrekkelig datagrunnlag å beregne sannsynligheten ut ifra. Dette er ikke alltid tilfellet med tilsiktede hendelser. I vurderingen av sikringsrisiko brukes ofte trefaktormodellen: risiko er en vurdering av trussel, verdi og sårbarhet (Bruvoll et al., 2020). Trussel beskriver i denne sammenheng evnen og intensjonene til en *trusselaktør*. Tilsiktede hendelser er preget av en ytterligere usikkerhetsdimensjon ved at trusselaktører er rasjonelle og hemmelighetsfulle. Konsekvensene av en tilsiktet hendelse kan derfor være svært alvorlig, og i tillegg

vanskelig å oppdage (Martin, 2019). Trusselaktører målsetter seg mot verdier; noe mennesker, organisasjoner og samfunn verdsetter, for eksempel kraftforsyning. Når disse verdiene er utsatt for fare fra trusselaktører, er de sårbare. Sårbarheter beskriver muligheter for trusselaktører til å skade verdiene (Martin, 2019).

Vurderinger av sårbarheter er ikke nødvendigvis det samme som en vurdering av risiko. En sårbarhetsvurdering beskriver hvordan for eksempel et teknologisk system et mottakelig for en bestemt hendelse, som et cyberangrep. Sårbarhet er først og fremst en beskrivelse av en tilstand i nåtiden, i motsetning til risiko som beskriver mulige hendelser i fremtiden (Smith & Brooks, 2013). Studier av sårbarheter er gitt mye vekt i CPS-sikkerhetslitteraturen, ettersom nye interaksjoner og økt eksponering av driftskontrollsystemer mot cyberdomenet har produsert nye sårbarheter. Driftskontrollsystemer som blir utsatt (sårbare) for trusselaktører gjennom cyberdomenet, kombinert med aktører som besitter tilstrekkelig evne og hensikt til å utnytte disse sårbarhetene til å skade kraftforsyningen (verdien), utgjør derfor en risiko. Cyberrisiko kan i forlengelse av dette forstås som prosesser og aktiviteter som gjennom cyberdomenet er sårbart for trusler mot informasjonsverdier, IKT-systemer, fysiske systemer og ytterligere materielle og immaterielle verdier (Strupczewski, 2021). Med andre ord er cyberrisiko vurderinger og tilhørende usikkerhet av uønskede hendelser som kan påvirke våre verdier gjennom sårbarheter i digitale systemer.

Leveson (2020) argumenterer for at skillet mellom safety og security er mindre hensiktsmessig når man vurderer hvordan man best kan sikre informasjonssystemer. Om en programvarefeil utløser et strømbrudd fordi en operatør feiltolker situasjonen, eller om et hackerangrep rettet mot driftskontrollsystemer forstyrrer forsyningssikkerheten, er konsekvensene det samme ifølge Leveson (Leveson, 2020). Et virkemiddel i styringen av sikringsrisiko for eksempel er overvåkning av trusselbildet. Avdekke å stanse kriminelle og terrorister før de begår en tilsiktet handling er en kontinuerlig pågående prosess. I samsvar med digitalisering og sammensmeltning av IKT og operasjonelle prosesser, har derimot skillet mellom sikkerhet og sikring blitt mer tvetydig. Organisasjoner har begrenset evne til å overvåke og bekjempe trusselaktørene selv, og må heller rette blikket mot sikkerhet i eget system. Levesons argumentasjon henger sammen med en utvikling innen sikkerhetsfeltet hvor sikkerhet og sikring stadig konvergeres sammen (Kongsvik et al., 2018). Leveson anser denne konvergeringen som et kontrollproblem: systemeiere og operatører må heller rette blikket mot egenskaper innad i eget system og graden av kontroll over interaksjoner mellom komponenter i systemet (Leveson, 2011, 2020).

3.2 Cyberfysisk system

Utviklingen av smartnettet slik beskrevet tidligere sammenfaller med større utviklingstrender i industrielle og teknologiske systemer og betegnes som cyberfysiske systemer (Baheti & Gill, 2011). Som navnet impliserer, er ikke systemene forstått enestående som fysiske eller digitale, men integrerte systemer i samarbeid med hverandre. Gjennom sensorer, kameraer og måleapparater kan relevant informasjon samles inn og kommuniseres videre i sanntid. Et mangfold av sensorer og målere i et utstrakt område danner et felles kommunikasjonsnettverk som kan overvåkes fra en sentralisert driftssentral (Ashibani & Mahmoud, 2017). Brytere og aktuatorer gjør at operatørene kan utføre fysiske funksjoner basert på sanntidsinformasjonen. Gjennom menneske-maskin grensesnitt (HMI) kan systemoperatører overvåke og kontrollere fysiske funksjoner utenfor umiddelbar rekkevidde. Deler og komponenter som tidligere var atskilt både fysisk og sekvensielt i systemet, er nå i økende grad koplet sammen i et omfattende nettverk (Ashibani & Mahmoud, 2017). Det grunnleggende konseptet bak cyberfysiske systemer er derfor samhandling mellom digitale systemer og fysiske systemer i sanntid og i 'feedback loops' med hverandre, hvor informasjon og data kontinuerlig utveksles mellom og innad i systemene (Xu et al., 2018; Lee, 2008).

Stadig flere samfunnsfunksjoner, redskaper og teknologier drar nytten av digitale systemer i samspill med fysiske prosesser. Fra omfattende systemer som et kraftsystem, til biler og husholdningsapparater; i sin mest generiske forstand kan CPS-begrepet anvendes mot et stort antall objekter og systemer (Humayed et al., 2017). Törngren, et al. (2017) argumenterer for at gjennomsyringen av IKT i samfunnet som følge av digitalisering, gjør det vanskeligere å skille ut hvilke systemer som *ikke* er cyberfysiske. Forfatterne presenterer derfor fire aspekter av CPS-begrepet, for å ytterligere avgrense det fra andre liknende begreper (Törngren et al., 2017).

(1) Det *tekniske* perspektivet er rådende innen CPS-studier, og beskriver integrasjonen mellom IKT og fysiske systemer. Især vektlegges designaspekter og synergi mellom fysiske og digitale komponenter.
(2) Cyberfysisk integrasjon tilbyr mange teknologiske og forretningsmessige fordeler, men integrasjonen ilegges også begrensninger. *Systemegenskaper* er egenskaper ved systemet som en helhet; sikkerhet, regulering, lovgivning og organisatoriske målsetninger. Systemegenskaper påvirker systemet som en helhet og former utviklingen av systemet.

(3) *Automasjonsnivået* beskriver grad av automatisering av aktiviteter i systemet. 'Smartheten' i cyber-fysiske systemet henger sammen med grad av automasjon, hvor prosesser og funksjoner i større grad løsrives fra direkte menneskelig kontroll. Gjennom positive feedback loops kan delsystemer interagere og utfylle hverandres funksjoner med minimal innblanding fra operatører.
(4) *Levetid* beskriver integrasjonen av CPS-funksjoner i sammenheng med et bestemt formål. Dette aspektet kan beskrive kostnad-nytte og andre økonomiske dimensjoner av cyber-fysisk integrasjon, eller hvilke konsekvenser integrasjonen vil ha for systemets operasjonelle evne (Törngren et al., 2017).

Drevet av forbedret effektivitet i dataenheter og prosessorer, lavere kostnader i komponenter og i samspill med internettets utbredelse, har CPS-teknologi integrert seg i flere kritiske samfunnsfunksjoner og infrastruktur. Cyber-fysisk integrasjon medfører en økning i antall digitale komponenter og redskaper i systemet. Systemet er igjen også avhengig av interaksjon mellom disse komponentene for å utøve sin tiltenkte funksjon. Denne avhengigheten forordner informasjonssikkerhet som et systemkrav, når en kritisk prosess som elektrisitetsoverføring blir avhengig av cyber-fysisk interaksjon. Systemtrygghet og sikring har dermed vært en prioritet i CPS-litteraturen fra begynnelsen (Lee, 2008; Rajkumar et al., 2010). Disse nye avhengighetene har delvis motivert vektleggingen av teknisk analyse og komponentinteraksjon innenfor CPS-fagfeltet (Törngren et al., 2017). CPS er et relativt ungt forskningsfelt, og har siden begynnelsen vært nedbrutt i teknologiske og ingeniørmessige domener som forsker på og utvikler ulike aspekter av et cyberfysisk system. Ved å oppstykke og analysere programvare, nettverkskommunikasjon eller elektroteknikk hver for seg, har komponentegenskaper og interaksjoner dominert fagfeltet (Baheti & Gill, 2011).

Cyberfysisk systemsikring tilnærmer seg sikkerhet i systemene på tilsvarende vis. Fra sikringsperspektivet har utviklingen beskrevet over medført en rekke nye sårbarheter. Disse sårbarhetene får en stadig større betydning i en samfunnsmessig kontekst etter hvert som hverdagslige produkter som 'smarthus', medisinsk utstyr eller 'smarte biler', samt industrielle prosesser som 'smartnett' integrerer cyberfysisk teknologi (Humayed et al., 2017). Denne utviklingen motiverer derfor studier av sårbarheter i systemene fra det nederste nivået; fastvare, komponenter og programvare; og opptil systemene som en helhet (Wurm et al., 2017).

Stuxnet viruset som i 2010 forstyrret Irans atomprogram ved å angripe sentrifuger i urananrikningsanleggene, anses ofte som et vendepunkt for cyberfysisk systemsikring. Angrepet viste at selv lukkende SCADA-systemer ikke nødvendigvis er trygge, og at konvensjonelle IKT-sikkerhetskonsepter om konfidensialitet, integritet og tilgjengelighet ikke trenger å krenkes for å utgjøre en skade mot fysiske prosesser (Langner, 2011). Siden industrielle kontrollsystemer som SCADA typisk sett har vært lukkede systemer, har heller ikke sikkerhet vært en prioritet. Men etter hvert som systemene har blitt mer åpne, bredere anvendt og lettere tilgjengelig for omverdenen, har dette sårbarhetsbildet endret seg (Jaatun et al., 2021). Det som derimot er interessant, er at Stuxnet-angrepet mot Iran trolig ble gjennomført ved bruk av insidere, sosial manipulasjon gjennom e-poster eller uaktsomme ansatte som ubevisst deltok i angrepet (Lindsay, 2013). Eksempelet fremhever at hendelsen som kan ha signalisert et paradigmeskifte innen cyberfysisk systemsikring, også er tilknyttet til det menneskelige og organisatoriske. Med andre ord kan også dette angrepet anses som en sosioteknisk svikt.

3.3 Sosiotekniske systemer

Teknologi omfatter de materielle objekter og redskaper vi benytter oss av, men også kunnskapen som er nødvendig for å anvende redskapet og organisere denne prosessen i riktig kontekst (Olsen & Lindøe, 2009). Som et teknologisk system består kraftsystemet av materielle objekter; elektrisk lys, transformatorer, generatorer og overføringsnett. Men det består også av organisering i bruken av disse redskapene; produksjonen, finansieringen og formalisering av kunnskap om systemet (Hughes, 2012). Systemene består av en menneskelig del (sosio) og en teknisk del, derved det *sosiotekniske* systemet. Begrepet impliserer derfor en innbyrdes sammenheng mellom menneske og teknologi. Ifølge Walker et al. (2008) bygger det sosiotekniske perspektivet på to grunnleggende premisser: 1) det er interaksjonen mellom menneske og teknologi som er avgjørende for systemets suksess eller uhell. 2) fellesoptimalisering mellom menneske og teknologi er nødvendig, fordi menneske og maskin opptrer fundamentalt forskjellig. Mer avansert eller effektiv teknologi skaper ikke nødvendigvis organisatoriske og menneskelige optimaliseringer, og motsatt (Fox, 1995; Walker et al., 2008).

Å forstå risiko i teknologiske systemer avhenger derfor også av å forstå hvordan mennesker samhandler med teknologien og hvordan disse prosessene organiseres (Le Coze, 2016). Dette er essensielt et sosiologisk perspektiv: det handler om å forstå organisasjonsstrukturer mennesker skaper i fellesskap og hvordan dette igjen former atferd og ideer hos individer (Hopkins, 2016, sitert i Hopkins, 2021, s. 25). Et cyberfysisk kraftsystem kan forstås som sosioteknisk i

denne sammenheng. Utviklingen av CPS er knyttet til ambisjoner om effektivisering og optimalisering av fysiske prosesser gjennom digitalisering, til formål for organisasjonen og samfunnet. For å sitere Charles Perrow: «*det finnes ikke et teknologisk imperativ tilsier at vi må ha energi eller våpen fra kjernefysisk fisjon eller fusjon*» (Perrow, 1999, s. 11). Perrow refererer her til bruken av kjernekraft, men det samme gjelder utviklingen av cyberfysiske systemer. Teknologien er stadig underordnet organisasjonene som utvikler og forvalter systemet; systemstrukturen er ikke tilfeldig, men heller et resultat av menneskene og organisasjonene som utviklet teknologien i en bestemt kontekst (Olsen & Lindøe, 2009). Teknologien anvendes til formål for organisasjonen, og teknologiens utforming kan anses som et produkt av organisasjonsstrukturen og omgivelsene den tilhører (Perrow, 1983).

Dette betyr derimot ikke at risiko i sosiotekniske systemer kun tilskrives menneskelige og organisatoriske egenskaper. Studier av risiko i sosiotekniske systemer fremhever utfordringer som oppstår i grensesnittet mellom menneske, organisasjon og teknologi. Teknologiske systemer som kjernekraft og kjemisk industri er ofte assosiert med alvorlige konsekvenser og en iboende fare. Disse systemene beskrives ofte som *høyrisikoteknologier*. Menneskelig eller miljømessig eksponering for radioaktivitet eller kjemikalier utgjør en stor fare, og risikostyring av disse systemene er dermed kritisk. Samfunnets avhengighet av elektrisk energi, IKT-teknologi, helsetjenester og finansielle institusjoner har også medført at svikt i disse funksjonene kan få alvorlige og langvarige samfunnsmessige konsekvenser (Gould & Macrae, 2021). Konsekvensene av en uønsket hendelse i et petrokjemisk industrianlegg kan eksempelvis være mer umiddelbare: omfattende branner og eksplosjoner med stort skadepotensiale. Risikoen ved omfattende strømbrudd er mer *systemisk*; risikoen og de potensielle konsekvensene forplanter seg i andre systemer og samfunnslag som er avhengig av elektrisk energi (Schweizer, 2021).

Perspektivet innebærer også at konstruerte systemer og mennesker i seg selv er ufullkomne. Det forekommer alltid begrensninger i tilgjengelig tid eller menneskelig og materiell knapphet, som resulterer at ingen systemer eller sikkerhetsløsninger er perfekte (Hollnagel, 2014, s. 127). Prosesser som ivaretar sikkerheten i sosiotekniske systemer er tilbøyelig for dysfunksjonaliteter, og kan produsere feil tillater at den iboende faren i teknologiske systemer blir utløst. Mennesker er ofte gjenstand for feil, uhell eller omsorgssvikt for arbeidsoppgavene de utfører. Dette er derimot ikke et perspektiv som 'peker' fingre om menneskelige feil som årsaken til ulykker i tekniske systemer. Det handler om å illustrere hvordan det ga mening for menneskene i den situasjonen å «gjøre det slik» (Dekker, 2014, s. 7). Tekniske løsninger kan være nødvendig for

å forhindre at systemene vi er avhengig av svikter. Fra et sosioteknisk perspektiv vil det derimot vært en feilslutning å anta at man 'designe' seg ut av enhver risiko i systemene. Tekniske sikkerhetsbarrierer og forsvarsmekanismer er stadig menneskeskapte og er utsatt for de samme hverdagslige feil alle mennesker begår. Disse feilene blir ikke nødvendigvis synlig før barrieren utsettes for fare (Reason, 1997). Det sosiotekniske perspektivet utfordrer oss derfor til å se på egenskapene i systemet: hvordan er teknologien uregjerlig eller uforutsigbar, eller hvordan konstrueres forestillinger av risiko og sikkerhet i organisasjonen som forvalter systemet? For å svare på dette vil vi videre utforske to dimensjoner av sosiotekniske systemer: *Systemstruktur* og *prosesser.*

3.4 Systemstruktur: komplekse systemer

3.4.1 Kompleksitet og 'systemiske ulykker'

Ifølge Perrow (1999) finnes det høyteknologiske systemer hvor ulykker er uunngåelige. Teknologiske systemer er ifølge Perrow delt inn i fire nivåer: *komponenter* [2] er de minste delene i systemet som er hensiktsmessig å identifisere. Samtlige sammenkoblede komponenter utgjør *enheter,* som i flertall utgjør *delsystemer* og til slutt har vi *systemet* som består av flere delsystemer. Perrow definerer svikt i deler og enheter som 'hendelser', mens ulykker inntreffer når forstyrrelser eller stans påvirker delsystemer eller hele systemet (Perrow, 1999, s. 65). Det Perrow kaller 'normale' eller 'systemiske ulykker' inntreffer når hendelser oppstår og interagerer med hverandre på uventet vis og dermed forårsaker stans i systemet som en helhet.

Nøkkelen til å forstå Perrows beskrivelse av systemiske ulykker ligger i systemenes komplekse interaksjoner. Komplekse interaksjoner, i motsetning til lineære interaksjoner, oppstår mellom komponenter i uventet sammenheng og er ikke tiltenkt i designprosessen. I følge Perrow består de fleste systemer av lineære interaksjoner; interaksjoner som er forventet og synlige (Perrow, 1999, s. 78). Alle systemer har deler og enheter som interagerer med hverandre og interaksjoner mellom disse alene er ikke nødvendigvis nyttig å studere, ifølge Perrow. Derimot når systemer stadig vokser i størrelse og utgjør et mangfold av funksjoner for samfunnet rundt seg, vokser også antallet koblinger innad i systemet og til andre systemer. Deler og enheter vil også i større grad være multifunksjonelle; dette leder til mer effektive systemer, men reduserer også lineariteten til systemet og gjør det dermed mer komplekst. Systemets interaksjoner er i økende grad

[2] Perrow bruker opprinnelig ordet 'parts' som oversettes til 'deler', for å beskrive de minste delene av systemet. I denne oppgaven vil 'komponent' benyttes synonymt med 'deler'.

også preget av feedback loops, som kan virke forvirrende for systemoperatører. I følge Perrow leder dette til mer uforståelige eller uforutsigbare interaksjoner.

Den andre egenskapen ved systemer som gjør de utsatt for systemiske ulykker, er tette koblinger. Dette beskriver Perrow som mangel på buffer mellom to eller flere systemaspekter. Perrow (1999, s. 93) fremhever fire egenskaper som preger tette koblinger: 1) systemet har tidsavhengige prosesser som krever kontinuerlig drift eller produksjon. Kraftsystemet er et godt eksempel på dette, hvor tilstanden til strømnettet er basert på den momentane balansen mellom produksjon og forbruk. 2) produksjonssekvenser er konstante; B må følge A før det kan gå videre til X. 3) tett koblete systemer har ingen alternativer for å oppnå sin tiltenkte funksjon. 4) tett koblete systemer mangler buffer og krever derfor presisjon. Perrow argumenterer for at systemer preget av disse egenskapene, er mer utsatt for systemsvikt dersom en feil oppstår i systemet. På grunn av avhengighetsforholdene mellom delsystemene (2) (3), må sikkerhetsmessige hensyn imøtekommes i designfasen til systemene; det er mindre rom for improviserte eller supplerende sikkerhetstiltak i allerede tettkoblete systemer. Tette koblinger bidrar også til å gjøre systemene mindre gjennomsiktige og komponenter og delsystemer mindre tilgjengelig for manuelle handlinger. Dette medfører igjen at hendelser og mindre avvik i komponenter forblir uoppdaget frem til feilen har forplantet seg gjennom hele systemet (Perrow, 1999).

Denne redegjørelsen munner ut i Perrows 'Normal Accident Theory' (NAT): Ulykker er en iboende egenskap i systemer med komplekse interaksjoner og tette koblinger. Det er ikke de individuelle delsystemene eller komponentene som besitter denne iboende faren, men systemet som en helhet. Tette koblinger medfører at feil i deler og enheter forplanter seg i resten av systemet og påvirker funksjoner til andre delsystemer. Når deler, enheter og delsystemer også interagerer på uventet vis vil samtlige delsystemer svikte på tilsynelatende usammenhengende måte. Dette fører til slutt til fullstendig systemsvikt. Ulykkene er et produkt av systemet slik det er konstruert; systemiske ulykker er en iboende egenskap i systemstrukturen (Le Coze, 2016). Sikkerhetsstyring av komplekse systemer er også beheftet av dilemmaer, hvor tette koblinger og komplekse interaksjoner krever ulike optimaliseringstiltak (Kongsvik et al., 2018, s. 78). Teorien uttrykker en manglende kontroll og forståelighet overfor komplekse systemer som medfører at systemoperatører ikke behersker å forutsi systemfeil.

I møte med komplekse systemer foreslår Perrow tre løsninger: 1) Komplekse systemer hvor ulempene overveier fordelene burde forlates. 2) Komplekse systemer vi ikke kan leve uten, eller er svært fordelaktige for samfunnet burde gjøres tryggere. 3) Komplekse systemer som er

tilstrekkelig selvkorrigerende kan gjøres tryggere uten omfattende innsats (Perrow, 1999, s. 304). Hvis man skulle forsøke å plassere cyberfysiske systemer innenfor disse rammene, kan man postulere at sistnevnte kategori er tilstrekkelig. Derimot burde kunnskapen vår og levetiden til cyberfysiske systemer også vurderes i denne sammenheng. Cyberfysiske systemer er en relativ ny utvikling. Som Perrow selv uttalte om kjernekraftverk da 'Normal Accident' ble skrevet på begynnelsen av 80-tallet: katastrofepotensialet i systemene har ennå ikke fullstendig avslørt seg (Perrow, 1999, s. 32). Perrows NAT er derfor en teknologideterministisk teori katastrofepotensialet i komplekse systemer. Ulykker og systemsvikt kan og vil inntreffe, og vi har begrenset evne til å styre sikkerheten gjennom sikkerhetsbarrierer eller dybdeforsvar (Perrow, 1999, s. 43).

3.4.2 Systemteori og trygge systemstrukturer

Systemteoretikeren Nancy Leveson deler Perrows perspektiv om at systemer må beskrives ut ifra koblinger og interaksjoner mellom delsystemer som utgjør en samlet helhet (Leveson, 2011, s. 63). Leveson uttrykker aspekter av kompleksitet gjennom *fremvoksende egenskaper*. En komponent eller enhet kan være mer eller mindre pålitelig, men dette beskriver kun komponentens evne til å utøve sin tiltenkte funksjon. For å identifisere sikkerhetsnivået i et system, holder det ikke kun å se på sikkerhet og pålitelighet i eksempelvis en effektbryter i distribusjonsnettet. Sikkerhet er en fremvoksende egenskap ved systemet som en helhet. Dersom man ikke studerer interaksjonene til effektbryteren; hvordan enheten blir påvirket av, og påvirker mennesker, maskiner og omgivelsene sine, kan man heller ikke danne et presist bilde av hvordan den enkelte enhet eller delsystem fungerer. Å forbedre påliteligheten til komponenten lar seg isolert sett gjøre, men å si at sikkerheten forbedres på samme vis har ingen betydning (Leveson, 2011).

Å bygge sikre systemstrukturer vil ifølge Leveson kreve at komponenter og delsystemer ilegges *begrensninger* i handlingsrom for å kontrollere systemets interaksjoner (Leveson, 2011, s. 64). Ved å begrense interaksjoner som kan lede til uønskede hendelser, kan systemets sikkerhetsnivå forbedres. Kontroll av systemet avhenger igjen av kommunikasjon. Systemoperatørene må motta relevant informasjon som igjen skal benyttes til å manipulere systemet i riktig retning og dermed skape en positiv feedback loop. Dette er nødvendig i åpne og dynamiske systemer som påvirker, og påvirkes av omgivelsene. Kontroll nødvendiggjør kommunikasjon, som til gjengjeld skaper en likevekt og stabilitet i systemet som sikrer at det utøver sin tiltenkte funksjon og opprettholder et forsvarlig sikkerhetsnivå (Leveson, 2011).

Selv om Perrow og Levesons teorier oppsto fra forskjellige perspektiver (henholdsvis sosiologi og ingeniørfag), uttrykker begge teorier om hvordan systemstrukturer er avgjørende for sikkerheten til et teknologisk system. Perrow sporer dilemmaer i styringen av høyrisikosystemer helt tilbake til sosial maktdynamikk og metanarrativer som kapitalisme (Perrow, 1999, Kapittel 9). Levesons teori er rotet i ingeniørperspektiver opptatt av utvikling av rasjonelle verktøy og prosesser som tilskriver mening til stadig mer komplekse systemer i et dynamisk samfunn (Leveson, 2011, s. 463). Perrow kan forstås som mer pessimistisk til tekniske løsninger på sikkerhetsproblemer; Leveson ser på inngrep i systemstrukturen som en nødvendighet for sikkerheten. Av den grunn må man være forsiktig med å likestille de to perspektivene. Det vi imidlertid kan utlede er at disse teoriene er opptatt av systemet som helhet, og hvordan strukturen og driften av systemet indikerer dets suksess eller fiasko (Dekker, 2014, s. 133). Teoriene anvendes også for å etablere en forståelse av tekniske systemstrukturer og implikasjoner dette kan ha på sikkerheten i høyrisikosystemer. Ideen om systemstrukturer må derimot ikke begrenses til kun det tekniske; hierarkier, beslutningsstrukturer og organiseringen av arbeidsprosesser er således å se som kritisk for ivaretakelse av sikkerheten i systemene.

Motsigelsen mellom en deterministisk tolkning av Perrows Normal Accident Theory, og den rådende definisjonen av risiko, som sier at fremtidige utfall er ukjente (Aven & Renn, 2009), burde også poengteres her. Teknologideterminismen Perrows NAT impliserer, har blitt gransket og senere avvist av mange (Le Coze, 2021, s. 4). Blant argumentene for dette finner vi at Perrow ikke presenterer kriterier for å måle kompleks interaktivitet eller tette og løse koblinger, og flere eksempler som benyttes for systemiske ulykker ikke matcher Perrows beskrivelse av komplekse systemer (Hopkins, 1999, 2001). En utvidet tolkning av NAT presentert av Jean-Christophe Le Coze (2015, 2021) derimot, ser Perrows verk som en beskrivelse av komplekse og dynamiske sosiotekniske forhold i organisasjoner (Le Coze, 2015, s. 277). Ulykker i sosiotekniske systemer er derfor ikke å anse som ‘normale’ fordi den underliggende teknologien er uhåndterbar; ulykker er normale fordi de fortsetter å inntreffe til tross innsatsen som ilegges for å forhindre de (Le Coze, 2021, s. 29). For å utforske dette perspektivet må vi se nærmere på prosesser i organisasjoner som konstruerer forestillinger om risiko og sikkerhet og hvordan disse svikter. I følgende delkapittel dette perspektivet utforskes.

3.5 Prosessuelle teorier – svikt i organisasjoner

3.5.1 Fra struktur til prosess

Drevet av ambisjoner om effektivisering gjennom automatisering, blir cyberfysiske systemer koblet tettere sammen, og flere interaksjoner skapes på tvers av systemene. Dette medfører at cyberfysiske systemer også blir mer komplekse. Denne utviklingen henger sammen med prosesser i organisasjoner som former og forvalter teknologiske systemer. I følge Leveson krever sikker drift av høyrisikoteknologiske systemer forskjellige typer begrensninger avhengig av hvilket delsystem eller nivå av systemet som reguleres. På et komponentnivå ilegges tekniske begrensninger, men 'lenger opp' i hierarkiet må operatørers og organisasjoners handlingsrom også begrenses (Leveson, 2011, s. 67). Det Levesons modeller ikke nødvendigvis forklarer er hvordan selve kontrollmekanismene og sikkerhetsbegrensningene svikter. Enten begrensninger innføres av reguleringsmyndigheter, eller organisasjonen selv; kontrollmekanismer er aldri perfekte, og implementeringen er avhengig av rådende perspektiver i organisasjonen og dens omgivelser (Dekker, 2014, s. 135). I det Perrow beskriver som feilfremkallende systemer, er det en rådene mangel av kontroll over teknologien som er rotet i organisatoriske og menneskelige faktorer (Perrow, 1999, s. 172). Høyrisikoteknologier som kraftsystemet har produksjon av elektrisitet som overordnet mål, og dette målet legger føringer på hvordan funksjonaliteten i teknologien utvikles og anvendes. Samtidig ilegges det også begrensninger på systemet i form av sikkerhetskrav. Sikkerhetsbegrensninger kan være både hemmende eller forsterkende for organisasjonens overordnede mål, men resultatet er at sikkerhet sjeldent er hovedformålet med driften av systemet (Leveson, 2011, s. 11).

Økt kompleksitet som følge av interaktivitet og automasjon kan bidra til å gjøre tekniske systemer mindre gjennomsiktige og mer uforståelig. Organisasjoner og individer som samhandler med systemet kan derfor i varierende grad ha ufullkommen kunnskap om hvordan systemet fungerer og er satt sammen. For å imøtekomme kompleksitet konstruerer vi modeller og beretninger om strukturer og systemfunksjoner. Individer og grupper oppfatter, tolker og konstruerer en sosial virkelighet i møte med vesentlig usikkerhet eller tvetydighet i komplekse systemer (Perrow, 1999, s. 176). I følge Perrow vil systemoperatører ignorere kompleksitet og tette koblinger når de konstruerer en kognitiv forståelse av systemet (Perrow, 1999, s. 214). Derved formes en forståelse av systemet som sikter til å redusere vår usikkerhet (Vaughan, 1999, s. 279).

Systemoperatører som jobber lokalt med komponenter og enheter i systemet forholder seg til tilstanden ved de bestemte delene eller enhetene og kan ikke ut ifra dette utlede den helhetlige sikkerheten i systemet. Derfor kan lokale beslutninger være 'riktige', men ha motsatt effekt på systemet som en helhet, når kompleksiteten ikke inkluderes i den lokale beslutningen (Leveson, 2011). Det blir dermed et dilemma når en operatør ikke er i stand til å besitte fullstendig kunnskap systemets komplekse interaksjoner, samtidig som at tette systemkoblinger fordrer at sekvensielle og tidsavhengige prosesser respekteres (Perrow, 1999, s. 10). Nye teknologiske løsninger og sikkerhetsbarrierer som tar sikte på å redusere feilprosenten eller ulykkesrisikoen, oppnår da det motsatte, ettersom tilstedeværelsen av mer avansert teknologi fører til at operatører blir villige til å ta større risiko, mens den underliggende kompleksiteten forblir (Perrow, 1999, s. 230).

Det sosiotekniske perspektivet fordrer at vi forstår samspillet mellom teknologi og organisasjon. Derfor må vi også rette blikket mot organisasjonen som styrer komplekse systemer. I kraftsystemet for eksempel, er kraftselskapene konkurranseutsatte markedsaktører som er avhengig av profitt for å overleve. Økonomisk gevinst kontrastert av sikkerhetstiltak som begrenser effektivitet kan skape målkonflikter som igjen fører til at sikkerhetsbegrensninger ikke respekteres. Selv om virksomhetene verdsetter og prioriterer sikkerhet, vil de likevel 'tøye strikken' for sikker drift, for å tilfredsstille andre interesser (Perrow, 1999, s. 123). Sikkerhetsbegrensninger kan i denne sammenheng ha motsatt effekt enn tiltenkt, hvor overskridelse eller brudd av rutiner eller barrierer har ingen umiddelbar negativ effekt. Hva som anses som trygg atferd i organisasjonen utvides derfor og over tid og forvitrer den helhetlige sikkerheten i organisasjonen (Rasmussen, 1997, s. 190). Operatørers atferd kan derfor bli feilfremkallende når deres konstruerte virkelighet er i strid med det systemet de faktisk opererer (Le Coze, 2021, s. 23).

3.5.2 Informasjonssvikt og menneskeskapte katastrofer

Vi kan utdype dette perspektivet på organisatorisk sammenbrudd med Barry Turners studie av ulykker. Turners formative verk *Man-Made Disasters* (1997) teoretiserte om årsaker til ulykker og katastrofer som en følge av sammenbrudd i kommunikasjon og informasjonsflyt innad og mellom organisasjoner (Hopkins, 2021; Pidgeon & O'Leary, 2000). Turner argumenterte for at svikt i sosiotekniske systemer uttrykker en mangel av kontroll over tekniske aspekter. Dette betyr derved ikke at systemsvikt kan tilstrekkelig beskrives kun ut ifra det det tekniske aspektet (Turner, 1994, s. 215). Ulykker og katastrofer forutsettes av mindre avvik, misforståelser og

feilkommunikasjon som forblir ubemerket av organisasjonen i det Turner kaller 'inkubasjonsfasen'. Systemsvikt inntreffer når en utløsende hendelse møter de dysfunksjonelle forholdene i organisasjonen. Etter hendelsen blir misforhold mellom forestillinger om risiko forut for ulykken, og den virkelighetssituasjonen organisasjonen befant seg i, åpenbart (Pidgeon & O'Leary, 2000; Turner, 1994).

Ifølge Turner er det flere kjennetegn på informasjonssvikt i organisasjoner forut for ulykker (Pidgeon & O'Leary, 2000, s. 19): 1) kritisk informasjon om risikoindikatorer i systemet blir ikke fanget opp organisasjonen. Dette kan være fordi indikatorene peker mot hendelser som aldri har inntruffet før, og de blir dermed feiltolket og underrepresentert (Kongsvik et al., 2018, s. 81). 2) Informasjon om risiko fanges opp, men er spredt blant mange aktører i organisasjonen. Kommuniseringen av risiko går tapt i organisasjoner som håndterer flere interesser og målsetninger samtidig. 3) Avvik fra sikkerhetsrutiner eller regler blir ikke satt i sammenheng med potensialet for større ulykker. 4) Selv om informasjon om risiko er tilgjengelig i organisasjonen, blir denne risikoen minimert eller neglisjert fordi det ikke passer inn i organisasjonens fortolkningsrammer (Kongsvik et al., 2018, s. 81; Pidgeon & O'Leary, 2000, s. 20). Ifølge Turner er dette noen av egenskapene organisasjoner viser i inkubasjonsfasen forut for en ulykke. Dysfunksjonelle forhold i organisasjonene fører til at kritisk informasjon og kommunikasjon går tapt, dermed unnlater organisasjonen å foreta forebyggende tiltak som begrenser farepotensialet i teknologiske systemer. Sikkerhet i sosiotekniske systemer er derfor ifølge Turner et ledelsesproblem; ledelsen i organisasjoner mislykkes i å adressere de underliggende kjennetegnene på informasjonssvikt som plager organisasjonen, fordi disse kjennetegnene er inngrodd i organisasjonens daglige praksis og drift (Turner, 1994).

3.6 Risiko, systemsvikt og sikkerhet i et sosioteknisk perspektiv

Komplekse systemer er en beskrivelse av systemstrukturen og implikasjonene dette kan ha for sikkerheten i systemene. Følger vi Turners tilnærming til systemsvikt, rettes også blikket mot prosesser i organisasjoner genererer dysfunksjonelle forhold. Her korrelerer usikkerheter om teknologi og usikkerheter om organisasjoner i produksjonen av systemsvikt (Le Coze, 2016, s. 161). Både Perrow og Turners teorier om ulykker er sosiotekniske i denne forstand; man kan ikke redusere risikoen i sosiotekniske systemer ved kun å adressere enten teknologi eller organisasjon og lederskap (Turner, 1994). Samspillet mellom teknologi og menneske er derfor nøkkelen til å forstå ulykke og systemsvikt i sosiotekniske systemer.

Organisasjoner jobber mot målsetninger som økonomisk gevinst eller produksjonskrav. De er i denne forstand målrettede, sosiale organismer hvor eksempelvis økonomisk gevinst og produktivitet forsikrer organisasjonens kontinuerlige eksistens (Woll & Eriksson-Zetterquist, 2014). Tekniske og organisatoriske sikkerhetsbarrierer implementeres for å styre risikoen i organisasjonen, men dette skaper også mer byråkrati og flere interaksjoner mellom systemdelene. Dette tilføyer heller den underliggende kompleksiteten i systemet, fremfor å gi systemeieren større grad av kontroll (Dekker, 2014, s. 132). Disse sikkerhetsbegrensningene kan derimot også virke hemmende på organisasjonens overordnede mål, som effektivitet eller produktivitet. Konkurrerende perspektiver, målkonflikter eller fravær av ulykker kan over tid føre til at sikkerhet blir nedprioritert i organisasjonen (Rasmussen, 1997; Turner, 1994). Fravær av ulykker kan over tid kan også innpode et falskt inntrykk av at sikkerhetsbarrierene er effektive. Dermed reduseres forestillingen om risiko organisasjonen står overfor (Reason, 1997). De underliggende tekniske systemene organisasjonen tillattes derfor større handlingsrom, fordi organisasjonen oppfatter at de opererer innenfor en akseptabel risiko. Over tid 'drifter' forestillingen av risiko i organisasjonen til det punktet hvor det som tidligere ble ansett som risikofylt, nå blir den nye 'normalen' (Dekker, 2014). Dette er en prosess som dermed normaliserer avvik til den grad at avvikene blir et forventet produkt av organisasjonens daglige drift (Vaughan, 1999). Denne prosessen av 'drift' mot større fare gjennom organisasjoners dagligdagse og 'normale' prosesser er grundig beskrevet av Diane Vaughan i hennes bok: *The Challenger Launch Decision* (1996).

Vaughans analyse av Challenger-ulykken (1996) utfordret den etablerte årsaksforklaringen bak ulykken. Challenger-romfergen eksploderte kort tid etter oppskytning, og årsaken ble tilskrevet en upålitelig komponent i raketten. Forut for oppskytningen hadde en gruppe ingeniører uttrykt bekymringer for risiko knyttet til denne komponenten, men etter den formaliserte analyseprosessen ble det konkludert å klassifisere dette som en akseptabel risiko. Beslutningen som ble gjort av NASA-ledelsen var i denne forstand i 'tråd' med normen i organisasjonen (Vaughan, 1996, s. 82). Som Vaughan beskriver det; organisasjonen (NASA) hadde gjennom ordinære og tilsynelatende rasjonelle prosesser utviklet seg til å «se», men samtidig «overse». Informasjon om faresignaler og indikasjoner på risiko ble 'dempet' i risikoakseptprosessen, fordi beslutningstakerne trodde usikkerheten ble korrekt målt og dermed justert (Pidgeon & O'Leary, 2000; Vaughan, 1996, s. 394–397). Etter ulykken kom det frem at organisasjonen opererte under betydelig økonomisk press og effektivitetsmål, som hadde bidratt til at ledelsen valgte å undertrykke og ignorere risikoindikatorer forut for oppskytningen (Vaughan, 1996, s. xii).

Ingeniørene og ledelsen hadde alle sammen de beste intensjoner om at oppskytningen skulle lykkes, men som Vaughans analyse viser; uønskede utfall inntreffer selv i organisasjoner som er konstruert for å forhindre dem (Vaughan, 1996, s. XV).

Vaughans studie av Challenger-ulykken illustrerer hvordan teknologisk og organisatorisk usikkerhet samspilte og til slutt ledet til katastrofe. Forfatteren undersøkte hvordan fremstillinger av risiko og fokus på sikkerhet ble undertrykt av rutinene som skulle ivareta nettopp dette. Vaughan påpeker at Challenger-ulykken kan beskrives som en 'normal accident' i tråd med Perrows teori (Vaughan, 1996, s. 415), men rammene for analysen utvides til å også omfatte organisasjonen og de organisatoriske omgivelsene som preget risikovurderingen forut for oppskytningen (Le Coze, 2021, s. 4). På samme måte som ulykker er 'normale' i komplekse systemer, vokser dysfunksjonelle prosesser frem gjennom organisasjoners dagligdagse handlinger og beslutninger. Vaughan kaller dette den 'skyggesiden' av organisasjoner: normalisering av avvik (1999).

3.7 Oppsummering av kapittel

Teorikapittelet har som mål å svare på: *hvordan kan man forstå risiko, systemsvikt og sikkerhet i cyberfysiske systemer fra et sosioteknisk perspektiv?* Teorien og litteraturen redegjort for i denne kapittelet kan derfor bidra til å svare på dette spørsmålet.

Utviklingen av cyberfysiske systemer har vekket interessen å studere og forstå nye former for systeminteraksjoner og komponentegenskaper. Cyberfysiske systemer er likevel å anse som sosiotekniske systemer: utformingen, driften og sikkerheten er avhengig av menneskene og organisasjonene som eier og opererer systemene.

Risiko og sikkerhet som to sammenvevde konsepter er i denne forstand konstruerte og subjektive virkelighetsoppfatninger hos individer og grupper, formet av organisasjonsmiljøet og omgivelsene det sosiotekniske systemet befinner seg i. Risikoanalyseprosesser kan fremstå som vitenskapelige og rasjonelle, men de er stadig konstruksjoner i en sosial, politisk og institusjonell kontekst. Menneskene og organisasjonene som utvikler og former teknologi, analysemodeller eller sikkerhetsrutiner, er utsatt for de samme menneskelige feilene og dysfunksjonalitetene som oppstår i møte med kompleks teknologi og sammensatte organisasjonsmiljøer. De samme menneskene utfolder seg også i organisasjoner og samfunn som former og formes av systemet.

Cyberfysiske systemstrukturer kan være mer eller mindre komplekse, og denne graden av kompleksitet kan ha en betydning for organisasjoners evne til å forhindre at systemsvikt inntreffer. Å ilegge begrensninger mellom komponentinteraksjoner kan forhindre at farlige tilstander sprer seg i systemene, men avhengig av hvordan disse begrensningene utformes kan de bidra til systemkompleksiteten fremfor å redusere den. Implementasjonen av sikkerhetsbegrensninger avhenger igjen av organisasjonens oppfatninger og fremstillinger av fare. Prosessene som oppdager, systematiserer og vurderer risiko og sikkerhet i organisasjoner kan utvikle seg til å bli kontraproduktive, og likevel forblir dette skjult fordi det over tid blir en dagligdags og 'normal' del av organisasjonens liv og virke.

Å forstå risiko, systemsvikt og sikkerhet i cyberfysiske systemer fra et sosioteknisk perspektiv, innebærer derfor å ta over seg samspillet mellom teknologi og organisasjon. Hvordan er forestillinger om risiko og tilhørende sikkerhetsbarrierer konstruert av aktører og organisasjoner som interagerer med disse systemene? Hvordan fungerer prosessene som avdekker og følger opp risikovurderinger? Hvordan er den underliggende systemkompleksiteten oppfattet og forstått av organisasjonen som forvalter systemet? Dette er spørsmål som forsøker å sette organisasjon, menneske og teknologi i forenelighet med hverandre.

Fra et sosioteknisk perspektiv er det egenskaper ved systemstrukturen til cyberfysiske systemer som kan gjøre systemene vanskeligere å forstå, styre og håndtere. I denne forstand kan systemenes kompleksitet også påvirke hvordan organisasjoner oppfatter og konstruerer fremstillinger av risiko i systemene. Fremstillinger av risiko og systemsvikt er igjen konstruert i innenfor en fortolkningsramme. Formet av organisasjoners målsetninger, eller faktorer fra organisasjonsomgivelsene; konsepter som risiko, systemsvikt og sikkerhet er betinget av organisasjonens fortolkningsrammer. Egenskaper som dermed definerer eller utgjør organisasjoners fortolkningsrammer vil igjen påvirke hvordan risiko, sårbarheter og sikkerhetstiltak kommuniseres, utredes og implementeres i systemet.

4. Metode

For å utforske sosiotekniske problemstillinger knyttet til risiko og sikkerhet i cyberfysiske systemer, vil det gjennomføres en litteraturstudie av utvalgte vitenskapelige artikler. Metodisk litteratur har bistått i å gjøre denne prosessen systematisk og transparent, og i følgende kapittel vil denne prosessen beskrives i detalj. Problemstillingen og forskningsspørsmålenes relevans knyttes til problematiseringen presentert innledningsvis: hvorvidt tar forskningen på cyberfysisk systemsikring over seg de sosiotekniske faktorene som påvirker risiko og sikkerhet? Med utgangspunkt i denne problemstillingen er det derfor nødvendig å gjennomføre en litteraturstudie. Den metodiske tilnærmingen til litteraturstudiet vil derfor vektlegges i dette kapittelet. Problemstillingen for oppgaven lyder som følger:

Hvordan kan utviklingen av cyberfysiske systemer vise seg som sosiotekniske utfordringer for risiko og sikkerhet i organisasjoner?

I sammenheng med problemstillingen må det presiseres at det undersøkes sosiotekniske utfordringer slik det fremstår fra forskningslitteraturen på cyberfysisk systemsikring. 'Utfordringene' som det er refereres til stammer dermed fra forskningslitteraturen på cyberfysisk systemsikring. Det er ikke gjennomført empiriske undersøkelser i organisasjoner for å svare på problemstillingen eller forskningsspørsmålene. Datagrunnlaget er begrenset til artikkelutvalget som presenteres under. I en tidlig fase av dette prosjektet ble tre intervjuer ble gjennomført. Intervjuene har fungert som kunnskapsstyrkende for forfatteren, og har bidratt til å etablere kontekst som har informert utformingen av systembeskrivelse i kapittel 2. Sitater eller konkret informasjon som fremkom i intervjuene har ikke direkte blitt anvendt i oppgaven.

Forskningsspørsmålene for denne oppgaven er:

F1: *Hvordan kan man forstå risiko, systemsvikt og sikkerhet i cyberfysiske systemer fra et sosioteknisk perspektiv?*
F2: *Hvordan fremstilles egenskaper ved risiko og sikkerhet i cyberfysiske smartnett av forskningslitteraturen på cyberfysisk systemsikring?*

Forskningsspørsmål F1 har allerede blitt redegjort for i kapittel 3 av denne oppgaven. I den påfølgende redegjørelsen av litteraturstudiet vil forskningsspørsmål F2 svares på.

4.1 Litteraturstudiet

Litteraturstudiet består av en kvalitativ analyse av et utvalg på 20 artikler. Antallet artikler i utvalget er av vesentlig betydning for kvaliteten på studiet (Bandara et al., 2015). Lenger nede vil det utdypes nærmere om omfanget ved litteratur på CPS. I et litteraturstudie er det vesentlig at utvalget er representativt for forskningen som studeres (Larsen et al., 2019). Med et antall på 20 artikler kan dette utgjøre en potensiell svakhet i fange opp 'helheten' eller fullstendigheten i forskningsfeltet. Samtidig må også antallet tilpasses etter kapasitet og behov. Artiklene i dette studiet gjennomgår en tidkrevende og detaljert kvalitativ analyse. Kvaliteten på dette studiet avhenger også på forfatterens evne til å integrere innsikten fra litteraturen inn i en sammenfattet studie (Bandara et al., 2015, s. 165). Et relevant spørsmål er dermed: på hvilket punkt er utvalget 'mettet' og grunnlaget er tilstrekkelig for analyse. Målet med utvalget er først og fremst å danne et tilstrekkelig grunnlag for analyse; ikke å tilfredsstille et forskrevet krav. Derfor fremstår det som hensiktsmessig å begrense utvalget til 20. Dette tallet dekker et bredt utvalg av artikler som lar seg analyseres innenfor tidsbegrensningene og omfanget av denne masteroppgaven.

Hensikten med litteraturstudiet er todelt:

1) fremheve forskningstemaer og utfordringer belyst i litteraturen på cyberfysisk systemsikring.
2) sette disse forskningstemaene og utfordringene i sammenheng med det sosiotekniske perspektivet redegjort for i teorikapittelet.

For å oppnå et tilfredsstillende resultat ved målsetning 1) er det hensiktsmessig å fremheve konseptuelle aspekter ved studiene. Funnene presentert i kapittel 5 er derfor en syntetisert fremstilling av artiklene, systematisert etter relevante teoretiske konsepter. Begrunnelsen for dette er flerfoldig: det er hensiktsmessig å unngå at litteraturstudiet har et 'forfatterfokus', hvor individuelle artikler redegjøres for uavhengig av hverandre. Ved å ha et konseptuelt fokus fremfor et forfatterfokus, lykkes studiet med å trekke essensen ut av forskningen. Videre er det også nødvendig å unngå at litteraturstudiet kun fremstår som en lang liste av referanser (Webster & Watson, 2002). Ved å sammenfatte innholdet i en samlet syntese, innebærer dette også å gjøre forenklinger i forskningen som redegjøres for. Dette kan spesielt være en utfordring med tanke på at en vesentlig andel av forskningen i dette studiet er teknisk, kvantitativ og kompleks. I praksis betyr dette at detaljnivået i artiklene ikke kan redelig gjengis her. Nyanser i den opprinnelige forskningen vil derfor gå tapt i overføringen i dette studiet (Watson & Webster, 2020). Det er viktig å poengtere dette som et bevisst og metodisk valg, fremfor tilfeldig utelatelse.

4.2 Teoretisk operasjonalisering

For å svare på problemstillingen krever det at de to aspektene av det sosiotekniske perspektivet operasjonaliseres. Gjennomgangen i teorikapittelet er forholdsvis abstrakt, og konseptene eller dimensjonene systemstruktur og prosesser kan være uklare. Operasjonaliseringen skal bøte på dette ved å gi konseptene mer håndgripelige dimensjoner. Samtidig må det merkes at en streng operasjonalisering ikke er målet, ettersom dette studiet ikke sikter til å måle eller tallfeste graden av disse konseptene. Som beskrevet over er det også hensiktsmessig å forsøke å fange essensen av forskningen som studeres. Selv om analysen gjennomføres med et bestemt sosioteknisk perspektiv, handler dette om å uttrykke egenskapene ved forskningen innenfor det gitte teoretiske perspektivet.

Systemstruktur: denne dimensjonen er primært interessert i strukturelle beskrivelser av teknologiske systemer. Konseptet baseres menneskelig forståelse av komplekse systemstrukturer og konsekvenser dette kan ha på organisasjoners evne til å ivareta sikkerhet i systemene. Det må merkes at Perrow og Levesons teorier ikke er begrenset til kun teknologiske strukturer; Leveson beskriver organisatoriske og interorganisatoriske forhold; og Perrow er opptatt av maktdynamikk, organisasjonsstrukturer og omgivelser i tillegg til egenskapene beskrevet i teorikapittelet (Leveson, 2011; Perrow, 1999). Tesene som systemstrukturer er kritisk til denne oppgaven ettersom teoriene bistår med å bygge broer mellom ingeniørfagmessige tilnærminger og sosiologiske tilnærminger til ulykke og katastrofe. Denne dimensjonen av det sosiotekniske perspektivet vil derfor sikte til å beskrive og forstå funksjonelle forhold i systemene gjennom komponentinteraksjoner, fremtredende sårbarheter og tekniske sikkerhetsbarrierer. Gjennom analyse og redegjørelse av disse egenskapene i litteraturen, kan det skapes et inntrykk av hvordan cyberfysiske systemers systemstruktur påvirker konstruksjonen av risiko og sikkerhet i organisasjoner.

Prosesser: Slik beskrevet av utvalgt litteratur er hovedsakelig organisatoriske og menneskelige dimensjoner av ulykker og katastrofe i sosiotekniske systemer. Disse egenskapene er derimot tydelig *etter* en hendelse har inntruffet. Som Turner indikerer kan organisasjoner vise tegn på dysfunksjonelle forhold i inkubasjonsfasen, men det fremstår ikke nødvendigvis som feilfremkallende prosesser forut for en ulykke (Turner, 1994). Egenskapene som Turner og Vaughan setter i sammenheng med ulykke er forstått slik i ettertid, og er i denne forstand årsaksforklaringer for ulykke og systemsvikt. Derfor er man nødt å utøve en viss varsomhet ved å bruke disse perspektivene i sammenheng med litteraturutvalget. Artiklene tar ikke utgangspunkt i

analyser av tidligere hendelser; og de har ikke organisatoriske og menneskelige faktorer som sitt primære analyseobjekt. Måten de prosessuelle teoriene er forstått og anvendt i denne oppgaven er derfor slik: rasjonelle prosesser som risikoanalyse, risikostyring og trusler er med på å skape fortolkningsrammer og konstruksjoner av risiko, systemsvikt og sikkerhet. For å svare på problemstillingen trenger vi å etablere en forståelse av hvilke egenskaper risiko og sikkerhet tilskrives i forskningslitteraturen, ettersom dette er med på å 'skape' utfordringene cyberfysiske systemer står overfor.

4.3 Litteratursøk

Basert på Bandara et al. (2015) trinnvise tilnærming til grundige søkeprosesser begynte litteraturstudiet med generelle og eksperimentelle søk for å etablere grunnleggende oversikt over nyttige søkeord og databaser. Utvalg av artikler ble gjort systematisk med den hensikt å fange opp de mest sentrale studiene på cyber-fysiske systemer. For å etablere en kontekst: et søk på Google Scholar etter «cyber-physical systems» gir 218 000 treff, Scopus produserer 22 414 treff og IEEE Xplore gir 10 863 treff. Legger vi til «security» i dette søket reduseres treffene ytterligere. På denne måten filtreres søket for å utelukke irrelevante artikler og fremheve de mest ønskelige artiklene. Søkeprosessen er også iterativ: flere ulike kombinasjoner av søkeord og filtre ble benyttet og deretter ble søket lagret og dokumentert i kildereferanseverktøyet Zotero. Det samlede utvalget ble så vurdert, og deretter ble tilpasninger ved søket foretatt og prosessen ble gjennomført på nytt (Bandara et al., 2015). I tillegg til dette ble også referanser i artiklene studert, og artikler som ble hyppig referert til ble vurdert etter gjeldende kriterier og inkludert i studiet. Dette bidrar til å gjøre utvalget mer representativt for fagfeltet (Bandara et al., 2015; Webster & Watson, 2002).

Det endelige søket som ble benyttet var:

"cyber-physical systems" AND "smart grid" safety OR security

Søket velger ut artikler som bruker «cyber-physical systems» og «smart grid» i sin helhet og i tillegg bruker ordet 'safety' eller 'security'. Dette søket viste seg å være mest effektiv på å fremkalle studier som eksplisitt omhandler sikkerhet i et smartnett med et cyber-fysisk perspektiv. Ytterligere ble søket begrenset til å kun omfatte artikler fra journaler. Dermed blir konferansebidrag eller andre publikasjonsformater utelukket. Selv om konferansebidrag kan være nyttig å ta med i en litteraturstudie, ble det besluttet å ekskludere dette ettersom de ikke er fagfellevurdert. Mangelen på fagfellevurdering krever at man er mer kritisk og nøyaktig i utvelgingen (Bandara et al., 2015, s. 163). Dette er derimot vanskelig å gjennomføre i praksis når man tilnærmer seg et helt nytt fagfelt og mangler relevant bakgrunnskunnskap. Det er derimot gode argumenter for at konferansebidrag også burde inkluderes i systematiske litteraturstudier: konferansebidrag presenterer ofte de nyeste utviklingene innen et fagfelt og bidragene er mindre preget av metodisk konformitet (Larsen et al., 2019; Webster & Watson, 2002). Eksklusjonen av dette kan derfor fremstå som en potensiell svakhet ved datagrunnlaget i dette studiet.

4.5 Utvalget

Deretter ble søket anvendt i hovedsakelig tre databaser. Resultatene er gjengitt i tabell 1. I tillegg til søket over, ble også 'NOT IEEE' lagt til søket på Scopus for å unngå vesentlig overlapp i treff. Dette fordi Scopus også gir treff i IEEE Xplore sin database, noe som blir gjennomført i et selvstendig søk. Til slutt ble søket avgrenset til perioden 2010-2022 for å fange opp et bredt tidsspenn. Begrepet «cyber-physical systems» ble myntet i 2006 av amerikaneren Hellen Gill (Skilton & Hovsepian, 2018, s. 9) og er dermed et relativt nytt begrep i teoretisk forstand. Tidsbegrensingen ble likevel innført for å utelukke eldre, irrelevante treff i IEEE Xplore og Sciencedirect databasen. Tidsbegrensningen hadde ingen effekt på søket i Scopus. Som søkertallene indikerer, er omfanget på fagfeltet stort og en form for 'fullstendighet' blir derfor svært krevende. Med en strabasiøs og nøye beskrevet utvelgingsprosess bidrar dette til å styrke validiteten og reliabiliteten i oppgaven; det forsikrer at utvalget er representativt for en del av CPS-litteraturen, at utvalget kan reproduseres og dermed relevant for oppgavens forskningsspørsmål (Furseth, 2020). Det endelige utvalget er listet i tabell 2.

Database	**Treff**
Scopus	435
Science Direct	81
IEEE Xplore	1639

Tabell 1 antall treff per database for endelig søk

Artikkel	Tidsskrift
(Sridhar et al., 2012)	Proceedings of the IEEE
(Woodard et al., 2021)	Reliability Engineering and System Safety
(Khazaei & Amini, 2021)	International Journal of Critical Infrastructure Protection
(Leszczyna, 2018)	Computers & Security
(Attia et al., 2018)	Computers and Electrical Engineering
(Khurana et al., 2010)	IEEE Security Privacy
(Kim & Tong, 2013)	IEEE Journal on Selected Areas in Communications
(Friedberg et al., 2017)	Journal of Information Security and Applications
(Hahn et al., 2013)	IEEE Transactions on Smart Grid
(Ouchani, 2021)	Journal of Systems Architecture
(Humayed et al., 2017)	IEEE Internet of Things Journal
(Sun et al., 2018)	Electrical Power and Energy Systems
(Mo et al., 2012)	Proceedings of the IEEE
(Gunduz & Das, 2020)	Computer Networks
(Marashi et al., 2021)	Reliability Engineering and System Safety
(Rodríguez et al., 2021)	Microprosessors and Microsystems
(Liu et al., 2014)	IEEE Transactions On Smart Grid
(Ericsson, 2010)	IEEE Transactions on Power Delivery
(Bretas et al., 2019)	Electrical Power and Energy Systems
(Zonouz & Haghani, 2013)	Computers & Security

Tabell 2 Liste over endelig utvalg og tilhørende journal

4.6 Destillering av utvalget

For å redusere antall treff til en håndterbar mengde, ble de mest relevante manuelt vurdert. Målet med denne destilleringen er å velge ut artikler av høy kvalitet og relevans og redusere dette til en håndterbar mengde. Denne prosessen innebærer å sette grenser rundt den aktuelle forskningen, men samtidig unngå å ekskludere artikler for arbitrære og forutinntatte grunner (Larsen et al., 2019). Det er også innforstått at ulike akademiske bakgrunner, institusjoner og publikasjoner har vidt forskjellige kriterier til 'akademisk kvalitet'. Å fastslå grad av kvalitet på en artikkel er dermed en komplisert prosess uten 'riktige svar' (Bandara et al., 2015). Dette impliserer at subjektivitet påvirker utvalget. Det er derfor viktig å dokumentere, begrunne og presentere prosessen grundig for å bekrefte validiteten til studiet (Furseth, 2020). Denne vurderingen ble gjort basert på flere kriterier:

1) *Tittel og nøkkelord:* Den første filtreringen ble gjort basert på artikkelens tittel og nøkkelord. Her ble artikler som innehold søkeordene «cyber-physical system», «smart grid» sammen med «security», «safety» eller lignende uttrykk som «cyber security», «ICT-security» og lignende prioritert.

2) *Abstrakt:* etter at tittelen ble vurdert som relevant, ble abstraktet lest og studert. Sammendraget presenterer mer relevant informasjon og presenterer en kortfattet oppsummering av studiet, og er dermed en utmerket måte å fange opp studiets relevans.

3) *Innledning og konklusjon:* Til slutt ble artikkelens innledning og konklusjon lest for å bedre fange opp essensen i artikkelen. Denne prosessen gjør det lettere å vurdere om artikkelen lar seg analysere. En vesentlig andel av artiklene fra søket er svært tekniske, og disse tekniske analysene er ubegripelig uten en relevant bakgrunnskunnskap. Dette utgjør en potensiell svakhet i litteraturstudiet, hvor denne forfatteren ikke besitter tilstrekkelig teknisk kunnskap til å analysere og forstå disse aspektene. Disse artiklene er likevel relevante ved å belyse artikkelforfatternes betraktninger rundt egne funn og fremstillinger av egen forskning.

4) *Ulike databaser og journaler:* Søket ble gjennomført i tre ulike databaser: Scopus, Sciencedirect og IEEE Xplore. De tre ulike databasene henter fra et forskjellig utvalg av journaler med ulik tematikk og fokus. IEEE har et sterkt teknisk og teknologisk fokus (IEEE, 2022); Scopus og Sciencedirect favner et bredt utvalg av fagfelt som i større grad representerer samfunnsvitenskapelig litteratur. Scopus overlapper med både IEEE og Sciencedircet (Elsevier, 2022). Derfor ble det ansett som hensiktsmessig å hente artikler fra flere databaser og journaler, og variere utvalget mellom journalene. På denne måten unngår utvalget å bli overrepresentert av tekniske og kvantitative studier. Spesifikt ble det også vektlagt å hente artikler fra journalen «Reliability Engineering and System Safety», ettersom denne journalen hovedsakelig inneholder artikler med et ‘safety’ fokus. I utvalgsfasen kom det frem at artikler med et cybersikkerhetsfokus var overrepresentert i utvalget. Prioritert utvalg fra denne journalen ble da benyttet for å forsikre at ‘safety’ perspektivet ble sterkere representert.

4.7 Styrker og svakheter

Avslutningsvis kan det pekes tilbake til flere styrker og svakheter ved metodevalgene i denne oppgaven:

Størrelsen på utvalget: Det er ikke nødvendigvis noe som tilsier at resultatene av litteraturstudiet hadde blitt drastisk påvirket hvis utvalget var større. Kvalitative innholdsanalyser er tidkrevende, og forskeren må derfor forholde seg til et antall som er overkommelig og gjennomførbart i praksis. I henhold til problemstillingen og det relevante forskningsspørsmålet var det nødvendig å studere artiklene nøye for å fange essensen av forskningen. Det fremstår heller som en styrke at utvalget har blitt grundig analysert og presentert. Utvalget kunne vært større, men dette valget inngikk i kompromisset alle forskere er nødt til å imøtekomme for å gjennomføre prosjekter i praksis.

Avgrensning av utvalget: Utelatelse av konferansebidrag ble diskutert grundig tidligere, og argumentene trengs ikke gjentas her. Om dette var en nødvendig avgrensning er vanskelig å konstatere og poengterer det faktum at forskerens subjektivitet vil påvirke utvalget og dermed også det endelige litteraturstudiet. Argumentene for å utelate bidragene fremstår derimot som forsvarlige, og det virker ikke nødvendigvis som en styrke eller svakhet at det ble ekskludert. Andre måter subjektivitet påvirket utvalget var det faktum at enkelte artikler måtte ekskluderes fra den endelige analysen fordi innholdet i artikkelen ikke lot seg analyseres innenfor rammene etablert i dette studiet. I denne forstand fungerer også det teoretiske rammeverket som en veileder for hvilke artikler som inkluderes i analysen. Artikler som ikke bidro til å svare på forskningsspørsmålet innenfor de teoretiske konseptene ble derfor ekskludert. Dette kan være en potensiell svakhet i den forstand at subjektiviteten påvirker representativiteten av utvalget.

Forenkling av forskningslitteraturen: Forenkling av forskningen i litteraturstudiet var en nødvendighet fordi denne forfatteren ikke besitter tilstrekkelig kunnskap i å vurdere det tekniske innholdet. Dette fremstår som den mest uttalte svakheten i dette studiet. Cyberfysisk systemsikring er et forskningsfelt preget av tekniske analyser og det er derfor krevende for en forsker med samfunnsvitenskapelig bakgrunn å sette seg inn i denne forskningen. Likevel er det ikke de tekniske aspektene som er i fokus i analysen, men heller konteksten *rundt* analysen. Dette baserer seg på konseptualiseringene av risiko, farer, sårbarheter og sikkerhetsbarrierer som forfatterne presenterer. Resultatene av kvantitative analyser er ikke nødvendigvis i fokus, og alle artiklene i utvalget inneholder tilstrekkelig kvalitative beskrivelser som tillater at artikkelen kan

analyseres. En potensiell styrke ved dette studiet er derimot at litteraturen på cyberfysisk systemsikring utforskes fra et sosioteknisk perspektiv; en tilnærming som fremstår som unik i sammenheng med sikkerhetslitteratur og andre masteroppgaver skrevet om samfunnssikkerhet.

Oppgavens omfang og avgrensning: En av oppgavens styrker er den grundige analysen og forskningen som har inngått i hvert kapittel i denne oppgaven. Vesentlig mengder med teoretisk forskning og litteratur på sikkerhet ble gjennomført for å sette sammen oppgavens teorikapittel. Både intervjuer og dokumentanalyse har bidratt til å sette sammen en systembeskrivelse og kontekst som supplerer oppgavens forskningsspørsmål og problemstilling. Dette har vært en utfordrende prosess som har bidratt til tverrfaglig innsikt og kompetanse. En styrke ved denne studien har også vært å påvise at anvendelsen av klassisk teori innenfor sikkerhet og ulykker, blant annet Perrow og Turners verk, fortsatt er hensiktsmessig å anvende 40 år etter de ble skrevet. Dette er ikke nødvendigvis en selvfølge når man studerer samspillet mellom menneske og teknologi, hvor den teknologiske utviklingen har akselerert drastisk siden den tid.

Litteraturanalysen: Verktøy som Zotero for kildebehandling, og Nvivo for kryssanalyse av nøkkelord og konsepter, har bistått i å gjøre analyseprosessen mer effektiv. I den enkleste forstand innebærer analysen likevel å sette seg grundig inn i hver enkelt artikkel for å forsøke å utlede relevante egenskaper i samsvar med det teoretiske rammeverket. Innenfor rammene av dette prosjektet fremstår det derfor som en styrke at de ulike delene av oppgaven blir utforsket grundig og blir satt i sammenheng gjennom hele oppgaven.

5.0 Litteraturstudie

5.1 Systemstruktur

Cyber-fysiske smartnett er omfattende systemer med mangfoldige komponenter i samspill med hverandre. Et gjennomgående fokus i studiene er derfor sårbarheter som oppstår i enkelte komponenter eller kritiske komponentinteraksjoner. Ved å analysere og kvantifisere funksjonelle forhold, beskrive angrepsstrategier og kaskadeeffekter på systemet, presenterer artiklene tekniske sikkerhetsutfordringer i cyberfysiske systemer. Basert på dette kan vi utlede egenskaper ved systemstrukturen i cyberfysiske smartnett. I henhold til den teoretiske redegjørelsen i kapittel 3, er det hensiktsmessig å identifisere nivåer av interaktivitet og koblinger for å fastslå kompleksiteten i systemene. Kompleksiteten i systemene er en avgjørende egenskap for organisasjoners evne til å regulere og håndtere teknologien.

5.1.1 Innledning

Artiklene utvalgt i dette studiet besitter rikelige beskrivelser av nye sårbarheter som oppstår gjennom cyberfysisk integrasjon. I denne forstand er studiene primært opptatt av (dys)funksjonelle forhold mellom komponenter som en kilde til sårbarhet. Risiko oppstår derfor i skjæringspunktet mellom det ønskelige funksjonelle forholdet i systemet (sikkerhet), og en uønsket tilstand som kan oppstå i fremtiden. Integrasjon av IKT i kraftsystemet gjør driften av operasjonelle systemfunksjoner avhengig av digitale systemer og forutsetningene for sikkerhet endrer seg dermed med denne digitaliseringsprosessen (Friedberg et al., 2017). For å styre risiko i cyber-fysiske systemer er det nødvendig å forstå sårbarheter i sammenheng med risikokilden. Svikt og avvik blir behandlet uavhengig fra cybertrusler i noen av artiklene, men majoriteten forholder seg til trusselaktører og angrepsstrategier som utnytter sårbarheter i systemene.

En av forutsetningene for smartnettet er samspill mellom forskjellige systemfunksjoner; operasjonelle funksjoner kan forbedres gjennom administrativ eller forretningsmessig integrasjon og vice versa. Administrative og operasjonelle systemer utfører forskjellige funksjoner, og har derfor også ulike funksjonelle krav og sikkerhetsbehov. Ericsson påpeker at denne koblingen mellom administrative og operasjonelle IT-systemer kan være en kilde til risiko, ettersom sårbarheter i IT-systemer kan utnyttes til å påføre skade på infrastruktur. Eksempelvis kan sikkerhetshull i Microsoft programvare gjøre SCADA-systemer sårbare hvis de er basert på eller samspiller med systemer basert på denne programvaren (Ericsson, 2010, s. 1503). Koblingene og

interaksjonene mellom de ulike komponentene og funksjonene er i denne forstand utgangspunktet for nye sårbarheter.

5.1.2 Analyse av funksjonelle forhold

Smartnettet er et iterativt system hvor nye digitale komponenter integreres og 'bygges over' eksisterende systemer fremfor å designes sammen fra bunnen. Avhengighetsforhold mellom digitale og fysiske funksjoner kan utgjøre en kritisk sårbarhet når ny, moderne teknologi bygges 'over' eldre teknologi som ikke lenger støttes eller oppdateres av produsenten (Humayed et al., 2017; Rodríguez et al., 2021). Komponentene utøver funksjoner i samspill med hverandre, men stammer ofte fra ulike leverandører og produsenter. Komponenter levert av ulike produsenter kan ha vidt forskjellige designforutsetninger før de blir integrert i smartnettet, og dermed kan det oppstå både sårbarheter og usikkerhet om hvordan komponenter i systemet vil interagere med hverandre. Mangfoldet av heterogene komponenter og deres interaksjoner utvider systemets sårbarhetsflate og kan bidra til flere innganger for cyberangrep. Økt interaktivitet mellom heterogene komponenter fremstår dersom som en kritisk kilde til sårbarhet i cyber-fysiske systemer (Humayed et al., 2017, s. 1810).

Hahn et al. (2013) og Liu et al. (2014) vektlegger derfor studier av hvordan bestemte angrepsvektorer kan utnytte funksjonelle forhold mellom systemkomponenter for å påvirke systemtilstanden. Woodard et al. (2021) og Marashi et al. (2021) bygger også analyser basert på spredning av avvik gjennom cyber-fysiske interaksjoner, men behandler komponentsvikt uavhengig fra cyberangrep. Forfatterne vektlegger analyser av hvordan avvik i kritiske komponenter kan forplante seg og forårsake systemsvikt. Cyber-fysiske interaksjoner har særegne tekniske utfordringer, og derfor må risikobaserte analyser utvikles med et detaljnivå som tilstrekkelig favner tekniske komponentegenskaper (Liu et al., 2014). Forhold mellom cyber-fysiske komponenter åpner opp for at digitale avvik eller cyberangrep kan ha fysiske konsekvenser på infrastrukturen i smartnettet. Identifiseringen av sårbarheter fremstår derfor som en essensiell del i analyseprosesser av cyberfysiske systemer.

Woodard et al. (2021) sin studie gjennomfører en kvantitativ analyse av systemytelse i et smartnett med hensikt å identifisere sårbare komponenter. Komponenter med høyest feilfrekvens og mest alvorlig konsekvens som følge av svikt, ble identifisert som sårbare. Analysen tar utgangspunkt i to mål for systemytelse: andelen av kunder som mottar strøm og gjennomsnittlig avvik fra forventet spenningsnivå. Deretter gjennomføres simulerte undersøkelser for å

demonstrere hvordan avvik i komponenter påvirker den samlede systemytelsen. Dette er forholdsvis digitale avvik; korrupsjon eller tap av data, ukorrekte kommandoer utført av systemet og uoppdagete kommunikasjonsfeil (Woodard et al., 2021). Marashi et al. (2021) sin kvantifisering av gjensidige avhengigheter mellom systemkomponenter benyttes også for å identifisere sårbare komponenter hvor svikt kan forplante seg videre (Marashi et al., 2021).

Friedberg et al. (2017) sin systemanalyse tar utgangspunkt i et mikronett hvor produksjon, transmisjon og distribusjon ligger i umiddelbar fysisk nærhet av hverandre. I utgangspunktet vil dette mikronettet være selvforsynt, men er i tillegg koblet opp mot hovednettet dersom ytterligere kapasitet er nødvendig. En effektbryter kan åpne og lukke denne tilkoblingen, men dette avhenger av at kraftmålinger (spenning, frekvensnivå) mellom mikronettet og hovednettet er synkronisert (Friedberg et al., 2017). Analysen identifiserer dette som den underliggende sårbarheten i systemet som analyseres: hvis påkobling gjennomføres uten tilstrekkelig synkronisering i kraftmålingene, kan dette påføre skade på infrastrukturen. I Mo et al. (2012) sin systemteoretiske analyse identifiserer også de mest kritiske sårbarhetene i systemkomponentene, og fremhever dermed hvor sikkerhetstiltak burde prioriteres. I følge forfatterne kan analysen i denne forstand avdekke optimale mottiltak mot cyberangrep, nettopp ved å prioritere sikkerhetstiltak mot de mest sårbare komponentene (Mo et al., 2012, s. 207). Analyse for å avdekke sårbare komponenter er et gjennomgående trekk i samtlige studier, hvor blant annet Liu et al. bemerker at deres studie har påvist hvor enkelt det kan være å destabilisere et strømnett ved å utnytte digitale sårbarheter i én enkelt type komponent (Liu et al., 2014, s. 1183).

5.1.3 Tekniske sårbarheter

Avskjæring av kommunikasjon, sårbare sikkerhetsprotokoller, standardisert programvare og omfattende interaktivitet mellom systemkomponenter som typiske digitale sårbarheter i CPS (Humayed et al., 2017). Økt interaktivitet mellom komponenter tilskriver nettverksbasert kommunikasjon innad i systemet en økt kritikalitet og en viktig forutsetning for nye sårbarheter i informasjonsbaserte systemer. Man kan skille mellom sanntidsbasert operasjonell kommunikasjon i f.eks. SCADA-systemer, sensorer og tilhørende operativsystemer; operasjonell-administrativ kommunikasjon som ikke er sanntidskritisk; og administrativ kommunikasjon innad og mellom organisasjoner og virksomheter (Ericsson, 2010). Sårbarhetene beskrevet i utvalget kan oppsummeres under følgende kategorier:

Nettverksinntrengning:

Ved å kompromittere nettverk gjennom sårbare brannmurer, kan trusselaktører få tilgang til administrative og forretningsmessige systemer og i forlengelsen operative systemer som er tilknyttet samme nettverk. Ved å oppnå denne tilgangen kan trusselaktører installere skadevare og virus som kan sabotere IT-infrastrukturen og tilknyttede OT-systemer (Mo et al., 2012). Nettverksinntrengning kan også oppnås gjennom sosial manipulasjon av autentiserte brukere av et nettverk, for eksempel phising-lenker og vedlegg i e-poster. Svake passord kan knekkes og gi trusselaktører mulighet til å maskere seg som autentiske brukere i nettverket. I tillegg til skadevare kan trusselaktører få tilgang til sensitiv informasjon om nettverk og IT-systemer, og dermed bruke dette som et springbrett til å utføre andre angrepsstrategier. En skadevareinfeksjon i kritiske systemer kan ha konsekvenser som spenner fra brudd på kunders personvern gjennom informasjonslekkasje, til potensielle strømbrudd dersom underbyggende digital infrastruktur svikter (Gunduz & Das, 2020).

Tidsforsinkelse

Tidsforsinkelse beskriver sårbarheter hvor forsinkede signaler kan føre til at enheter ikke reagerer på riktig tidspunkt eller responderer på en ikke-reell endring som kan skade delsystemet (Gunduz & Das, 2020; Liu et al., 2014; Mo et al., 2012). Tidsavhengighet mellom cyber-fysiske interaksjoner er et kritisk aspekt. Industrielle kontrollsystemer er sanntidssystemer med liten eller ingen tidsmessig slakk eller buffer mellom kommando og respons. Dette betyr at når operatøren utløser en bryter må den tilhørende funksjonen reagere tilnærmet umiddelbart. Forsinkelser i slike prosesser kan ha alvorlige konsekvenser på systemets funksjonalitet. Denial of Service (DoS) angrep kan i denne sammenheng benyttes til å desynkronisere tidsforholdet mellom komponenter og forstyrre operasjonell drift (Sridhar et al., 2012). Et DoS-angrep rettet mot AMS kan forårsake mangelfull eller forsinket informasjon om forbruk. Dette kan føre til gale beslutninger av systemoperatører, som f.eks. å produsere strøm uten en reell etterspørsel, og dermed påføre kraftselskapet økonomiske tap. Forsinket styringsinformasjon kan også påføre skade på infrastrukturen dersom en operatør utfører en handling på feil tidspunkt (Attia et al., 2018). Liu, et.al (2014) vektlegger kritikaliteten bak tidsforsinkelse ved å inkludere en tidsdimensjon i modellering og analyse av sikkerhet i CPS.

Dataavskjæring, manipulasjon og injeksjon

Nettverkskommunikasjon kan kompromitteres og dermed tillatte at trusselaktører kan få tilgang til sensitiv informasjon som kan benyttes til andre tilsiktede formål (Mo et al., 2012).

Muligheten til å avskjære informasjonspakker og signaler betyr at trusselaktører kan manipulere informasjon som presenteres til systemoperatører. Gjennom nærhet til enhetene kan signaler fra måleenheter forstyrres uten at trusselaktører nødvendigvis har 'tilgang' til nettverkssystemer (Sun et al., 2018). Den manipulerte informasjonen kan dermed medføre at operatøren begår gale beslutninger basert på informasjonen tilgjengelig (Gunduz & Das, 2020). Informasjonsavskjæring kan manipulere strømpriser og dermed redusere strømregninger og forårsake økonomisk tap på kraftselskapet. Attia et al (2018) studerer prismanipulasjon som sikter til å endre sluttbrukerens forbruksmønster ved å manipulere den reelle strømprisen. Forfatterne hevder at på grunn av strømprisens elastiske markedseffekt, vil lave strømpriser under forbruksintensive perioder føre til overbelastning på produksjonsanlegg og distribusjon. Dette vil bryte momentanbalansen i nettet og kan dermed føre til svikt i infrastruktur.

Kim & Tong (2013) beskriver et «*Man in the middle*» angrep som utnytter mangelfull autentifisering av brukere i et system, som dermed lar en trusselaktør å sende forfalsket informasjon til systemoperatører. Uten mulighet til å avdekke at informasjonen er manipulert, kan systemets reelle tilstand skjules for operatøren, eller manipuleres slik at operatøren selv påfører systemet skade. Studiet redegjør for tester av 'uoppdagelige angrep' som manipulerer målerdata og nettverksdata samtidig, som derved gjør den manipulerte informasjonen uadskillelig fra autentisk informasjon. Konsekvensene av denne typen angrep kan være alvorlige økonomiske tap for strømselskapene, og i verste tilfelle kan det påføre skade på den fysiske infrastrukturen. Angrep som retter seg mot integriteten til operasjonelle data er dekket av flere studier, og tilsvarende mottiltak rettet mot datamanipulasjonsavdekking (Bretas et al., 2019; Khazaei & Amini, 2021).

Endringer / oppdateringer

Nye installasjoner eller oppdateringer av eksisterende komponenter, programvare og enheter kan endre forutsetninger for interaksjoner og dermed påvirke systemegenskaper. Oppdateringer eller 'patcher' av programvare er spesielt viktig, hvor for eksempel Windows programvare regelmessig oppdateres for å lukke sikkerhetshull (Humayed et al., 2017). Endringer ved å installere nye komponenter eller ta i bruk nytt programvare kan potensielt utgjøre en sårbarhet. Nye sårbarheter kan oppstå hvis sikkerheten ikke ivaretas i de nye komponentene, men sårbarheter kan også reduseres ved å erstatte eldre, sårbare komponenter. Sridhar et al. påpeker eksempelvis at muligheten til å fjerninstallere og oppdatere fastvare i AMS også innebærer en potensiell angrepsvektor som kan utnyttes av trusselaktører (Sridhar et al., 2012, s. 218). Samtidig så kan slike oppdateringer være hensiktsmessig for å forlenge levetiden til fastvaren, fikse

programvarefeil og sikkerhetshull. Små og store endringer i systemstrukturer vil kreve grundig revisjon og vurdering av potensiell risiko og konsekvenser som oppstår ved integrasjon eller tettere kobling (Rodríguez et al., 2021).

5.1.4 Test bed

Et sentralt virkemiddel for å validere sårbarhetsmodelleringer og foreslåtte mottiltak, er å gjennomføre praktiske eksperimenter i 'test beds'. Dette er anlegg som kombinerer fysiske og digitale systemer og modellerer og simulerer cyber-fysiske smartnett (Hahn et al., 2013). Dette er både virtuelle simulasjoner og SCADA-laboratorium som i varierende grad lar forskere utforske cyberfysiske interaksjoner i praksis (Sridhar et al., 2012). Samtlige studier utøver tester av ulike angrepsstrategier mot et simulert cyberfysisk smartnett. Slike tester tilbyr muligheter til å utforske sårbarheter, angrepsstrategier og potensielle fysiske konsekvenser på systemet i et isolert miljø. Effektiviteten til sikkerhetsbarrierer kan også testes i sammenheng med målrettede angrep (Sun et al., 2018). Fysiske konsekvenser i det simulerte strømnettet; spenningsnivåer og strømforsyning kan overvåkes og måles, og gir forskerne et inntrykk av fysiske konsekvenser ved cyberangrep eller komponentsvikt i operasjonelle systemer (Woodard et al., 2021). Forfatterne utforsker også muligheten for at testbed miljøer kan bidra til å validere etablerte bransjestandarder eller reguleringsforskrifter (Hahn et al., 2013). Testene kan dermed indikere om valgte sikkerhetsløsninger tilfredsstiller stipulerte reguleringskrav og om disse kravene også tilstrekkelig dekker funksjonelle sikkerhetskrav.

Det er imidlertid ulemper med disse testmiljøene som har implikasjoner på gyldigheten av angrepsstrategier og tilsvarende mottiltak beskrevet i disse studiene. Det er en utfordring å skape test-systemer som tilstrekkelig modellerer og simulerer virkelige smartnetts funksjonaliteter, og denne utviklingen er også begrenset av økonomiske midler til forskning (Sridhar et al., 2012). Kompromisser i forskningen må ofte inngås; det kan være mangel på tilgjengelig cyberfysisk infrastruktur å teste på, eller begrensninger i eksperimentene må innføres for sikkerhetsgrunner eller konfidensialiteten til systemet som forskes på (Friedberg et al., 2017). Modeller og simulasjoner er også basert på forenklinger av virkeligheten; modeller kan ikke fange virkeligheten 'som den er'. Simulering av komponentsvikt for eksempel, uttrykkes som en binær størrelse hvor komponenten enten virker eller ikke (Woodard et al., 2021). Virkelige systemer er i større utsatt for ukvantifiserbar 'støy'; uforutsette variabler og variasjoner som ikke modelleres. Det vil derfor oftest forekomme avvik mellom modellerte systemer og virkelige systemer (Mo et al., 2012).

5.1.5 Tekniske sikkerhetsbarrierer

Såkalte *Intrusion Detection Systems* (IDS) får mye oppmerksomhet i artiklene i dette studiet. IDS beskriver programvare og komponenter som er i stand til å automatisk oppdage inntrengere i nettverk og varsler om kritisk informasjon og data blir avskjært og manipulert av uautoriserte brukere. IDS er et redskap som bidrar til å skape situasjonsforståelse og oversikt over databehandlingen til cyber-fysiske systemer; en prosess som i praksis er umulig å gjennomføre manuelt når dataomfanget i systemene vokser (Zonouz & Haghani, 2013). Samtlige artikler presenterer algoritmer som sikter til å avdekke koordinerte cyberangrep og integritetsangrep (Attia et al., 2018; Khazaei & Amini, 2021; Sun et al., 2018), og modeller for å automatisk korrigere manipulert data (Bretas et al., 2019). Sikkerhetstiltak som beskytter informasjon og kommunikasjon fra å bli avskjært, manipulert eller forstyrret blir presentert som en kritisk nødvendighet, ettersom at smartnettene stadig blir mer avhengige av informasjon og data for å driftes sikkert (Sun et al., 2018, s. 54).

Humayed et al. (2017) påpeker at omfanget og mangfoldet av komponenter i smartnettet gjør utviklingen av pålitelig IDS svært komplekst og utfordrende (Humayed et al., 2017, s. 1821). Særegne systemegenskaper ved smartnettet vil trolig også kreve mer spesialiserte behov, og stadig mer komplekse IDS-løsninger (Sridhar et al., 2012). For å automatisere et IDS må ønskelige systemtilstander kvantifiseres, og programmene må være i stand til å identifisere og skille denne ønskelige tilstanden fra andre tilstander. Algoritmene og programvaren er ikke perfekt, og gir ofte falske utslag, og systemoperatører må behandle disse varslene manuelt (Zonouz & Haghani, 2013). Sanntidssystemer tilføyer et ytterligere krav at IDS gjennomfører dataanalysen uten vesentlig tidsforsinkelse som kan forstyrre den operasjonelle driften.

Brannmurer er en viktig sikkerhetsbarriere som hindrer at inntrengere får tilgang til systemnettverk. Feilkonfigurering av brannmurer er en sårbarhet som hyppig blir utnyttet til å skaffe tilgang til konfidensielle systemer (Mo et al., 2012). Brannmurene må konfigureres riktig, slik at de holder inntrengere ute og lar autorisert kommunikasjon passere gjennom nettverket. Konfigurering burde spesielt prioriteres i operasjonelle kontrollsystemer. Sun et al. fremhever her en usikkerhet hos systemoperatørene: Å avdekke sårbarheter i brannmurer på forhånd kan være utfordrende, fordi det forutsetter at systemoperatørene har 'fullstendig' kunnskap om systemet og kommunikasjonsflyten i nettverket (Sun et al., 2018, s. 48). sikkerhetskrav for brannmurer er omfattende dekket av cybersikkerhetsstandarder for smartnett (Leszczyna, 2018).

Ericsson (2010) foreslår et nødvendig skille mellom operasjonelle IT-systemer som drifter SCADA og administrative IT-systemer. Tett integrasjon og åpenhet mellom administrative IT-systemer og driftskontrollsystemer gjør kraftsystemet mer sårbart fordi det presenterer flere innganger og muligheter til å forstyrre, manipulere eller avskjære kritisk informasjon og data i driftskontrollsystemene (Ericsson, 2010, s. 1503). En sikker systemarkitektur er et nødvendig sikkerhetstiltak for å forhindre nettverksinntrengning og opprettholde KIT (Mo et al., 2012). Avkobling mellom administrative og operasjonelle IT-systemer henger sammen med en sikkerhetsstyringsstrategi som bryter IKT-sikkerhet ned i 'domener' fremfor komponenter og delsystemer. Å avgrense administrativ IT, driftskontrollsystemer, produksjonssystemer og telekommunikasjon til distinkte domener vektlegger at de ulike digitale og fysiske teknologiene som benyttes innenfor hvert domene har ulike egenskaper og funksjonskrav, og dermed krever ulike sikkerhetsløsninger. Spesifikke lovverk og retningslinjer for sikkerhet kan derfor anvendes til hvert enkelt domene, og sikkerheten kan styres basert på risikovurderinger for hvert enkelt domene (Ericsson, 2010, s. 1505). Dette innebærer også at man kan stille strengere krav til sikkerhet i operasjonelle systemer, uten å begrense administrative eller forretningsmessige systemer på samme måte.

5.1.6 Oppsummering av systemstruktur – egenskaper ved risiko og sikkerhet

Funksjonalitet og interaksjon i og mellom cyber-fysiske komponenter er en egenskap i CPS-litteraturen som får betydelig fokus. Det underliggende premisset i disse studiene er forholdet mellom cyberdomenet og det fysiske domenet, og konsekvenser som kan oppstå gjennom cyber-fysisk konvergering. Cyberangrep som utnytter sårbarheter i komponenter og delsystemer utgjør en risiko for å påføre den fysiske infrastrukturen skade, og dermed er dette også en risiko for forsyningssikkerheten. I denne forstand utnyttes funksjonelle forhold mellom komponenter til å skape dysfunksjonelle tilstander i systemet. Disse dysfunksjonelle tilstandene uttrykkes som underliggende sårbarheter som, når de utsettes for svikt indusert ved et uhell eller ekstern kraft, kan forplante seg og påvirke delsystemet eller hele systemet. Det fremkommer derfor fra litteraturstudiet at omfattende sårbarheter har oppstått i skjæringspunktet mellom fysisk- og cyber integrasjon. Man kan også fastslå en grad av økende kompleksitet som følge av hyppige interaksjoner og tett kobling på tvers av hele systemet. En kilde til denne kompleksiteten stammer fra komponentheterogeniteten i cyberfysiske systemer.

Validiteten av forskningen; hvorvidt angrepsstrategier fungerer i praksis, og effekten av presenterte sikkerhetsbarrierer, gjøres gjennom simulasjoner i 'test bed'. Test bed simulasjoner

gjennomføres også i sammenheng med forplanting av feil uavhengig av cyberangrep. Disse lukkede testing miljøene tilbyr forskere en måte å utøve teorier i praksis, men det forekommer også at modelleringer og scenarier gjennomført i test bed er forenklinger av virkelige cyberfysiske kraftsystemer. Avvik mellom resultater i testene og implementasjon i praksis kan derfor oppstå.

Avskjæring, manipulasjon og korrupsjon av data som sendes fra sensorer og målinger til sentrale driftskontrollsystemer fremheves som en sentral sårbarhet. Derfor får også utviklingen av algoritmer, programvare og komponenter som er i stand til å avdekke og korrigere denne typen angrep vesentlig fokus i forskningslitteraturen. Fordelene med slike sikkerhetsbarrierer er blant annet å overvåke av datatrafikk i for uregelmessigheter og behandle større mengder data automatisk. Utfordringer med denne typen barrierer er at kravene til sikkerhet i CPS blir stadig mer omfattende, som igjen krever mer sofistikerte verktøy.

5.2 Prosesser

Den underliggende kompleksiteten i systemstrukturen bør vurderes i takt med forhold som skaper, former og hemmer forestillinger om risiko og sikkerhet i organisasjoner. Artiklene i dette studiet har primært tilnærminger fra elektroingeniørfag, nettverksteknologi og informatikk. Derfor er ikke organisatoriske og menneskelige aspekter ved risiko og sikkerhet uttrykt like entydig som tekniske forhold og strukturer. Det er imidlertid aspekter ved risikostyring, analyse og risikokilden som er relevant i denne sammenheng. Målet for dette delkapittelet er å fremheve egenskaper ved risiko og sikkerhet som presenteres i litteraturen; med fokus på egenskaper som kan relateres til hvordan organisasjoner konstruerer og fremstiller risiko og sikkerhet.

5.2.1 Innledning

Integrasjon og større grad av interaktivitet mellom delsystemer er en essensiell egenskap i det cyber-fysiske smartnettet. Den fysiske infrastrukturen ute i feltet overvåkes kontrolleres av sensorer og aktuatorer, som styres fra et sentralt driftssenter, som igjen i varierende grad samspiller med virksomheters administrative og forretningsmessige systemer (Humayed et al., 2017). Denne sammenkoblingen har i en forstand ‘åpnet opp’ systemene, skapt større sårbarhetsflater og gjort systemene mer tilgjengelig for outsiderangrep. Omfattende cyber-fysisk integrasjon assosieres også med større grad av kompleksitet, som igjen utfordrer systemoperatørenes evne til å vurdere sikkerheten i eget system (Friedberg et al., 2017). Tekniske analyser av

konsekvenser (impact) mot fysiske prosesser som følge av cyberangrep, er også en utfordring i systemer med mangfoldige koblinger og interaktivitet (Hahn et al., 2013). Evnen trusselaktører har til å påvirke cyber-fysiske system fra utsiden, er en vesentlig usikkerhetsfaktor som påvirker risikostyringsprosesser av cyberfysiske systemer.

Sammenlignet med det tradisjonelle kraftsystemet, er smartnettet preget av toveis flyt av både informasjon og elektrisitet (Attia et al., 2018), hvor sanntidsinformasjon forbedrer effektiviteten og forbrukere i større grad også blir produsenter. Toveisflyt av informasjon og forbedret funksjonalitet i prosessorer og programvare tillater større grad av automatisering, som igjen bidrar til å effektivisere operasjonell drift av kraftsystemet (Rodríguez et al., 2021). Effektivisering gjennom automatisering er et viktig kjennetegn ved smartnettet, for eksempel ved at produksjon tilpasses etter forbruk med minimal innblanding av operatører (Rodríguez et al., 2021). AMS-systemet muliggjør også en grad av automatisering ved å redusere behov for manuelle målinger, og systemets evne til oppdage tekniske avvik umiddelbart er også reliabilitetsstyrkende (Sun et al., 2018). Dette krever også omfattende interaktivitet mellom systemet som en helhet og skaper gjensidige avhengigheter mellom delsystemer. Studie av tett cyber-fysisk integrasjon har vist at omfattende avhengighetsforhold ikke nødvendigvis har geografiske, logiske, fysiske eller digitale sammenhenger (Marashi et al., 2021, s. 10). Å fastslå sikkerhetstilstanden til systemet er derfor en stadig mer utfordrende prosess.

5.2.2 Risikostyring

Artiklene i dette studiet varierer mellom seg når det kommer til tematikk og tilnærming til analyse og risikostyring. Det følger også at artiklene som vektlegger forhold mellom cyber-fysiske komponenter, prioriterer å styre cyberrisikoen ved å redusere sårbarheter i komponentinteraksjoner. Tekniske sikkerhetsbarrierer ble presentert i forrige delkapittel som et aspekt av systemstrukturen, og disse barrierene er også å anse som risikostyringstiltak. For å unngå repetisjon vil ikke momenter fra tidligere redegjørelse gjentas her.

Et underliggende premiss i analysene av komponentinteraksjoner redegjort for i forrige delkapittel, er at det forekommer flere uoppdagede sårbarheter som først blir åpenbare etter en hendelse. Rodríguez et al. (2021) knytter dette til lav risikooppfatning av cybertrusler og sårbarheter i organisasjonene. Manglende bevissthet om cyberrisiko medfører at nødvendige sikkerhetsrutiner og sikkerhetskrav ikke implementeres. Forfatterne tilnærmer seg derfor sårbarheter i CPS gjennom revisjon og regulering. Et mangfold av enheter og komponenter i smartnettet kan

være sårbare, og risiko kan minimeres ved å gjøre tilstrekkelig revisjon og regulering i henhold til bransjestandarder på IT-sikkerhet (Rodríguez et al., 2021, s. 2). Ericsson peker til en historisk utvikling, hvor bevissthet rundt cyberrisiko var lav hos systemeiere i kraftbransjen på 90-tallet. Dette førte til at IKT-systemer og driftskontrollsystemer ble designet til å være åpne og tett integrerte, fordi dette var fordelaktig og ga effektiviseringsmuligheter for kraftbransjen (Ericsson, 2010, s. 1503). IKT-systemer som tidligere ikke har vært utsatt for cyberangrep, har ofte ikke sikkerhet som en designforutsetning (Gunduz & Das, 2020).

Utformingen av interne policyer, regelverk og retningslinjer kan derimot være utfordrende i sammenheng med komplekse cyberfysiske systemer (Ouchani, 2021). Komponentheterogenitet krever særegne sikkerhetsløsninger og dette innebærer at sikkerhetsbarrierene som innføres kan være like komplekse som systemet det beskytter (Rodríguez et al., 2021). I sammenheng med dette er det også et mangfold av standarder og 'beste praksis'-dokumenter som dekker sikkerhetstiltak i ulike aspekter av systemstrukturen, samt organisatoriske og ledelsesmessige praksiser. Ulike funksjonaliteter i OT og IT systemer krever igjen ulike standarder. Resultatet er et landskap av standarder som i seg selv kan være vanskelig å navigere (Leszczyna, 2018).

Kraftsystemet har svært mange interessenter: leverandører, administratorer, systemoperatører, politikere, byråkrater og kunder; og disse grupperingene kan påvirke kraftsystemet og trekke det i forskjellige retninger. Å koordinere sikkerhet under endringsprosesser er derfor kritisk; når teknologien endrer seg, må sikkerheten følge etter for å unngå å introdusere nye sårbarheter (Humayed et al., 2017, s. 1824). En vesentlig del av denne utfordringen ligger i å utvikle kostnadseffektive sikkerhetsløsninger som kan anvendes i alle nivåer av et smartnett (Humayed et al., 2017, s. 1826).

Sårbarheter i leverandørkjeder overlapper med samtlige tekniske sårbarheter redegjort for over. Disse sårbarhetene utnyttes derimot hos leverandøren av tjenester og produkter til det cyber-fysiske systemet. Trusselaktører kan potensielt installere ‘bakdører’ i programvare eller fastvare hos leverandøren, som kan utnyttes når komponentene er implementert i systemet (Mo et al., 2012). Rodríguez et al. (2021) fremhever denne sårbarheten fra et organisatorisk perspektiv, som nødvendiggjør interne rutiner, retningslinjer og revisjoner av leverandører og produsenter. Utbredelse av generisk IKT i samfunnet har medført lavere kostnader på disse produktene og dermed blir integreringen av slike teknologiske løsninger også mer vanlig i cyber-fysiske systemer (Sun et al., 2018). Dette kan for eksempel bety at sårbarheter som oppstår i Windows programvare også blir en sårbarhet for kraftsystemet hvis IT-infrastrukturen benytter seg av

denne programvaren. Ericsson poengterer i denne sammenheng at «kunder får det de ber om» fra sine leverandører; hvis de ikke ber om IKT-sikkerhet, så får de det ikke (Ericsson, 2010, s. 1503).

Cyber-fysiske systemer er informasjonsbaserte systemer. Svikt i informasjons- og kommunikasjonssystemene reduserer derfor systemoperatørers oversikt og situasjonsforståelse, som igjen muliggjør at selv små avvik kan forplante seg videre i systemet og forårsake systemsvikt (Woodard et al., 2021). Tettere integrasjon mellom delsystemer åpner opp for kaskadeeffekter hvor uønskede tilstander sprer seg fra et delsystem til et annet, og cyberangrep blir beskrevet som tilskynder av slike hendelser (Khurana et al., 2010). Organisatorisk oppstykking og geografiske avstander i kraftsystemet og mellom infrastrukturinstallasjoner kan ha en betydning hvordan systemsvikt utfoldes og håndteres. Koordinerte angrep mot et geografisk vidstrakt område kan være vanskelig å håndtere, fordi beredskap og sikkerhet i strømnettene er håndteres lokalt. Aktive strømbrudd kan også føre til kommunikasjonsproblemer mellom systemoperatører som ikke befinner seg i samme lokasjon, og dermed kan operatørenes situasjonsforståelse reduseres og restitusjonstiden i systemet forlenges (Sun et al., 2018).

5.2.3 Risikoanalyse

Analyse av cyber-fysiske systemer utfordres av stadig voksende omfang av systemene, både i geografisk og teknisk utbredelse og påfølgende kompleksitet ved å kontrollere og overvåke systemene (Friedberg et al., 2017; Zonouz & Haghani, 2013). Et gjentagende argument fra flere studier, er at analysemetoder må tilpasses omfattende interaktivitet og koblinger mellom fysisk infrastruktur og underbyggende cyberinfrastruktur (Friedberg et al., 2017; Mo et al., 2012; Sridhar et al., 2012). Forfatterne viderefører dette ved å presentere nye risiko- og sikkerhetsanalysemetoder som er nødvendig for å imøtekomme denne utviklingen. Ved å identifisere de mest fremtredende sårbarhetene i et system, kan vil dette også belyse hvor det er mest nødvendig med sikkerhetsinvesteringer (Friedberg et al., 2017; Mo et al., 2012). Systemanalyser og risikoanalyser er ikke bare en nødvendighet for å forstå systemenes sårbarheter, men det kan også informere beslutningsprosesser og veilede investeringsprosesser.

Mangelen på historisk data av storskala koordinerte cyberangrep reduserer gyldigheten av kvantitative risikoanalyser, og krever derfor ulike tilnærminger til risikostyring. Game Theory presenteres av Gunduz & Das (2020) som et effektivt virkemiddel for å simulere forhold mellom systemforsvar og angripere. Spillteori kan i denne sammenheng simulere trusselaktører

som angripere og systemoperatører som forsvarer; hvor ulike forsvarsmekanismer og ledelsesstrategier stilles opp mot kjente angrepsstrategier. I følge forfatterne kan en slik metode bidra til å avdekke optimale beslutninger og forsvarsstrategier ved fravær av pålitelige risikoanalyser (Gunduz & Das, 2020, s. 12).

Artiklene benytter forskjellige analysemetoder, men kommer frem til lignende konklusjoner: etablerte analysemetoder for sikkerhet er ikke tilstrekkelig for å identifisere forholdet mellom cyberdomenet og den fysiske infrastrukturen. Sikkerhetskravene til smartnett er omfattende, ettersom samfunnet forventer kontinuerlig strømforsyning, og kraftsystemet blir stadig større og mer komplekst når den underbyggende IKT-infrastrukturen utvikler seg (Mo et al., 2012, s. 207). Det er derfor behov for analyseverktøy som tilstrekkelig omfavner de cyber-fysiske sikkerhetsforholdene til kraftsystemet (Sridhar et al., 2012, s. 222) og som fremhever fysiske konsekvenser av digitale sårbarheter på en forståelig måte til ledere og beslutningstakere (Friedberg et al., 2017, s. 195). Det kan også utledes fra utvalget at det ikke er en ensartethet ved metodene som benyttes, og de varierer mellom kvantitative og kvalitative uttrykk.

5.2.4 Tillitt til maskinen

Mo et al (2012) Fremhever en utfordring ved å oppdage skadevare som har infisert et systemnettverk: hvis en antivirusprogramvare ikke oppdager et virus, er dette fordi systemet er virusfritt, er viruset uoppdaget av programvaren eller fordi viruset har deaktivert antivirusprogramvaren? (Mo et al., 2012, s. 202). Forfatterne belyser i denne sammenheng en utfordring som oppstår i grensesnittet mellom menneske og maskin. Begrenset innsikt i systemtilstanden er en vesentlig usikkerhetsfaktor. Systemoperatører har en implisitt tillitt til operasjonelle kontrollsystemer, og at informasjonen som presenteres for dem gjennom brukergrensesnitt er korrekt og resulterer i en tilsvarende korrekt handling (Khurana et al., 2010). Denne sårbarheten gjenspeiles også i artikkelen til Sun et al. (2018): dersom trusselaktører får tilgang til brukergrensesnittet til SCADA-systemer, kan informasjonen som presenteres for systemoperatører manipuleres og dermed lede til gale beslutninger med konsekvenser for drift. Angrep mot AMS kan også føre til personvernbrudd og at forfalsket informasjon om forbruk og priser blir distribuert til sentralen eller kunden (Sun et al., 2018, s. 49). Manipulasjon av for eksempel strømprisen som vises til kunden kan igjen føre til endringer i forbruksmønstre, som kan ha økonomiske og fysiske konsekvenser på kraftsystemet (Attia et al., 2018).

5.2.5 Risikokilden: tilsiktet og ikke-tilsiktede hendelser

Analyser av cyberangrep baserer seg på antagelser om at trusselaktører besitter nødvendig kunnskap og vil gjennomføre rasjonelle og målrettede angrep mot komponenter og delsystemer. Hahn et al. (2013), Kim & Tong, (2013) og Liu et al. (2014) analyser av spesifikke angrepsstrategier baserer seg på en 'worst-case' tilnærming hvor det antas at trusselaktører har 'universell' kunnskap nødvendig for å gjennomføre angrepet. Kim & Tong bemerker her at kunnskapsgraden angriperen besitter er en avgjørende variabel for potensielle konsekvenser og forsvarsevnen til systemoperatørene (Kim & Tong, 2013, s. 1294). Studiene beskriver ideelle forhold og nødvendige kriterier for å gjennomføre et slikt angrep og setter dette i sammenheng med sårbare tilstander i systemene. Ikke alle artiklene i utvalget tar utgangspunkt i universell kunnskap hos trusselaktøren; de fleste plasserer trusselaktørens kunnskaper på et spektrum. Kraftsystemer og strømnett er heller ikke ensartet på tvers av landegrenser eller regioner. Trusselaktørens kunnskap vil derfor begrenses av systemet de målsetter seg mot (Khazaei & Amini, 2021). Kompleksitet og kunnskap om systemet er også et tveegget sverd: komplekse systemer krever kompetanse og ressurser hos systemoperatører for å analysere og sikre systemet, men det samme kreves også av potensielle trusselaktører for å lykkes i et angrep (Mo et al., 2012, s. 207).

Humayed et.al (2017) redegjør for en helhetlig tilnærming til trusselaktører, hvor forfatterne bryter ned sikkerhetstrusler hvor: 1) ondsinnede individer, organisasjoner eller stater, (2) målretter seg mot CPS komponenter og sårbarheter, med (3) distinkte motiver som spionasje, sabotasje, terrorisme eller vinningskriminalitet og (4) distinkte angrepsvektorer som vil gi de tilgang til verdiene til systemet (Humayed et al., 2017, s. 1807). Sun et al. (2018) argumenterer for at kraftsystemer er designet for å være sikre og robuste, og begrensede cyberangrep vil tvilsomt kunne påvirke operasjonell drift av systemet (Sun et al., 2018, s. 51). Det ligger en utfordring i omfattende og koordinerte angrep som kombinerer ulike angrepsstrategier (Gunduz & Das, 2020). Disse angrepene begynner gjerne flere måneder i forveien, hvor trusselaktører sonderer sikkerhetsbarrierer og infiltrerer nettverk forut for et konsentrert angrep. Ressurssterke og kompetente trusselaktører utgjør derfor en større risiko for cyberfysiske systemer.

Insidere eller utro tjenere kan potensielt ha bedre innsikt i systemet dermed ha bedre forutsetning for å utføre angrep (Hahn et al., 2013). Insidere refererer til aktører innenfor organisasjonen som benytter tilganger og kunnskap om systemet til å påføre skade mot verdier. Insidere kan utnytte systemkunnskap til å omgå sikkerhetsbarrierer, og har derfor bedre forutsetning for

å gjennomføre angrep (Kim & Tong, 2013; Mo et al., 2012). Rodríguez et al (2021) knytter også insidertrusler til antallet interessenter i organisasjonen og systemet; flere interessenter kan skape en høyere risiko for insiderangrep. I tillegg kan det være vanskelig å forsvare seg mot fordi insidere utnytter tillitten man gjerne tilskriver sine medansatte, og derfor er man mindre varsom (Humayed et al., 2017, s. 1824; Sun et al., 2018). Tekniske sikkerhetsbarrierer som brannmurer og kryptering har liten til ingen effekt mot insiderangrep, ettersom aktøren allerede har tilgang til nettverk og systemer (Sridhar et al., 2012). Informasjon er en kritisk verdi i cyber-fysiske systemer, og informasjonslagring i slike systemer kommer i mange forskjellige former; Digital, analog, men også i ansattes hukommelse. Ansatte er informasjonsbærere i denne forstand. Gode tekniske og sosiotekniske sikkerhetstiltak og regelverk som ivaretar dette er derfor en vesentlig utfordring i cyber-fysiske systemer (Ouchani, 2021). En potensiell sikkerhetsbegrensning kan derfor være systemsikring; triviell personell burde ikke ha tilgang til systemkritiske komponenter (Mo et al., 2012).

Kun to av artiklene i studiet har utelukkende studert sårbarheter i cyber-fysiske systemer uavhengig fra angrepssvektorer og trusselaktører (Marashi et al., 2021; Woodard et al., 2021). Studiene vektlegger komponentpålitelighet, interaksjoner og stabilitet i cyber-fysiske systemer. Flere feiltilfeller i komponenter velges ut og deretter simuleres feilene for å vise hvordan komponentsvikt forplanter seg og påvirker systemet. Analysene illustrerer dermed hvordan komponenter interagerer med hverandre i en feilsituasjon og kan predikere feilscenarioer som kan bidra til å fremheve riktige sikkerhetstiltak (Marashi et al., 2021). Studiene sikter i denne forstand til å observere de svakeste 'leddene' i systemet. Disse studiene har et mindre proksimalt fokus sammenlignet med studiene av angrepsvektorer og tilsvarende sårbarheter. Komponentinteraksjoner og avhengigheter i systemet er fortsatt sentralt, men analysen skifter fra spesifikke sårbarheter i komponenter og avdekker heller sårbarheter på tvers av systemet gjennom avhengighetsforhold.

Utvalgte artikler analyserer også sikkerhet/sikringshendelser i en samlet analysemodell (Friedberg et al., 2017; Mo et al., 2012). Resultatene fremhever avhengigheter mellom cyber-fysisk systemsikring og systemsikkerhet. Forfatterne analyserer hvordan cyberangrep påvirker systemsikkerhet, stabilitet og pålitelighet. Studiene kombinerer både safety og security perspektiver i en samlet analysemodell. Forfatterne begrunner denne tilnærmingen ved cybersikkerhets manglende evne til å redegjøre for fysiske konsekvenser, og systemteoretiske modeller vektlegger systemstabilitet og systemtrygghet. Mangler ved de to ulike tilnærmingene (safety og

security) imøtekommes dermed ved å kombinere analyseformene (Friedberg et al., 2017; Mo et al., 2012). I denne forstand kan man anse systemsikkerhet som en egenskap eller verdi som blant annet, er avhengig av cyberfysisk systemsikring (Gunduz & Das, 2020; Humayed et al., 2017). Tilsiktede og ikke-tilsiktede hendelser kan få konsekvenser for systemets trygghet og evne til å opprettholde forsyningssikkerheten. Artiklene som studerer systemsikring, og artikler som studerer systemsikkerhet og pålitelighet kommer frem til lignende konklusjoner: forhold mellom cyber-fysiske komponenter er kritiske for sikkerheten. Distinksjonen mellom 'safety' og 'security' blir mer tvetydig i denne sammenheng.

5.2.6 Oppsummering av prosesser – egenskaper ved risiko og sikkerhet

Dette underkapittelet har dekket et bredt område av egenskaper som kan spille inn i prosesser som konstruerer og former organisasjoners fremstillinger av risiko, systemsvikt og sikkerhet. Prosesser som risikostyring og risikoanalyse er formaliserte prosesser som kan forstås som bidragsytere til organisasjoners fortolkningsrammer. I denne forstand spiller analysene en rolle i hvordan forestillinger om risiko blir konstruert og formet i litteraturen. Hensikten med litteraturstudiet er også å fremstille utfordringer for risiko og sikkerhet i cyberfysiske systemer. Derfor har gjennomgangen vektlagt å påpeke utfordringer slik fremhevet av artikkelforfatterne.

Kompleksiteten i cyberfysiske systemer er fremtredende, og utfordrer og begrenser anvendeligheten av tidligere analysemetoder. Hovedfunnet i dette delkapittelet illustrerer at fremstillinger av risiko, systemsvikt og tilhørende sikkerhetstiltak primært er rotet i systemtekniske analyser. Sofistikerte analysemetoder som tar for seg kompleksiteten og samspillet mellom cyberfunksjonalitet og fysisk funksjonalitet er nødvendig. Disse analysene kan bidra organisasjoner med å identifisere kritiske sårbarheter og dermed prioritere sikkerhetstiltakene sine deretter. Risikostyringsstrategier er ikke en egenskap som dekkes uttømmende av artiklene i utvalget, og er primært fokusert på tekniske sikkerhetsbarrierer presentert i forrige delkapittel. Videre ble også egenskaper ved tilsiktede og ikke-tilsiktede hendelser presentert. Kunnskapsgrunnlaget hos trusselaktører får størst oppmerksomhet, og spesifikke angrepsvektorer beskrives i detalj. Både tilsiktede og ikke-tilsiktede årsaker til systemsvikt studeres av artiklene, og det fremstår som et mer tvetydig skille mellom sikring og sikkerhet i litteraturen på cyberfysisk systemsikring.

6.0 Drøfting

Med den sosiotekniske teorien og litteraturstudiet av cyberfysisk systemsikring nå redegjort for, kan vi igjen tilnærme oss oppgavens problemstilling: *Hvordan viser utviklingen av cyberfysiske systemer seg som sosiotekniske utfordringer for risiko og sikkerhet i organisasjoner?* Dette kapittelet vil gjennomgå relevante aspekter i et forsøk på å belyse denne problemstillingen. Kapittelet er fordelt i to delkapitler som samsvarer med de to sosiotekniske dimensjonene redegjort for i teorien. Samtlige utfordringer vil derfor belyses underveis i diskusjonen.

6.1 Systemstruktur

6.1.1 Det svakeste leddet

I delkapittel 5.1.2 ble det rådende perspektivet på cyberfysiske komponentinteraksjoner fra litteraturen redegjort for. Cyberfysisk integrasjon i kraftsystemet innebærer at digitale systemer bygges 'over' den etablerte fysiske infrastrukturen for å skape et samspill mellom digitale og fysiske funksjoner. Litteraturstudiet viser blant annet at cyberfysiske systemer preges av komplekse interaksjoner og tette koblinger mellom komponenter og delsystemer (Marashi et al., 2021). Effektivisering gjennom automatisering er blant faktorene som driver frem flere cyberfysiske interaksjoner og tettere koblinger på tvers av hele kraftsystemets verdikjede. Driftssentralen for eksempel, fungerer som et samlingspunkt for flere delsystemer og funksjoner. SCADA-systemer lar operatører overvåke og kontrollere systemaspekter ubetinget av geografisk avstand, og disse funksjonene samles og benyttes gjennom systemets HMI.

Dette kan analyseres fra en menneske-maskin-dimensjon, hvor operatørens systemforståelse er begrenset til hva de faktisk kan 'se' foran seg. Systemet består fortsatt av flere interaksjoner, både lineære og komplekse, som foregår skjult for systemoperatørenes direkte påsyn (Perrow, 1999, s. 79). En av effektiviseringsmålene til cyberfysiske systemer er større løsrivelse fra direkte menneskelig kontroll. Ved å skape positive feedback loops av informasjon blir systemene 'smarte' nok til å fatte enkle beslutninger på egenhånd (Lu, 2017). Disse informasjonsbaserte feedback loops kan sammenlignes med det Perrow kaller tette koblinger (Perrow, 1999). Tidsavhengige prosesser i SCADA tillater liten eller ingen tidsforsinkelse, og krever korrekte målinger og ukorrupt datagrunnlag for å unngå at systemoperatører påfører systemet skade. Sårbarheter i sanntidssystemer og informasjonsintegritet er godt beskrevet i litteraturstudiet. Dette er koblinger med lite slakk eller buffer mellom komponenter og delsystemer (Perrow, 1999). Tette koblinger kan derimot forstås som et overordnet designmål for cyberfysiske systemer som

muliggjør effektivisering og automatisering (Törngren et al., 2017). Implikasjonene av dette vil diskuteres videre i neste delkapittel. Utfordringer tettere systemkoblinger kan medføre er redusert gjennomsiktighet og umiddelbar forståelighet av systemene. Dette aspektet av systemstrukturen kan potensielt bidra til å redusere operatørers evne til å umiddelbart bryte inn og forhindre av mindre avvik forplanter seg i resten av systemet.

Funksjonelle og dysfunksjonelle cyberfysiske interaksjoner som litteraturstudiet redegjør for, bidrar til å analysere og teste potensielle kontrollbegrensninger, og derved styrke sikkerheten i systemet. Å undersøke dysfunksjonelle komponentinteraksjoner er delvis også motivert av den tette koblingen mellom delsystemer i smartnettet, hvor individuelle sårbarheter i komponenter kan utnyttes til å utløse en kaskadeeffekt på systemet (Liu et al., 2014). For å unngå kaskadeeffekter ved komponentsvikt må redundans eller sikkerhetsmekanismer inkluderes i designfasen ifølge Perrow (Perrow, 1999). Et av funnene fra litteraturstudiet viser at komponentheterogenitet utfordrer dette prinsippet. Cyberfysisk integrering over tid, og på tvers av delsystemer innebærer at komponenter med ulike designforutsetninger, fra ulike leverandører interagerer med hverandre (Humayed et al., 2017). En oppgave for systemoperatører og systemeiere er derfor å forsikre at komponenter og delsystemer ilegges tilstrekkelige begrensninger mellom seg, slik at interaksjonene ikke gir opphav til dysfunksjonelle systemtilstander. Dette kan derimot bli en utfordring når ulike komponenter og delsystemer har forskjellige designforutsetninger, og systemene blir mer komplekse. Vi kan vise til HMI igjen for å illustrere hvorfor dette kan bli en utfordring i stadig mer komplekse systemer.

En HMI forstås som en multifunksjonell og tett integrert komponent; dens hensikt er å skape kontinuitet gjennom hele systemet. Vi kan benytte en bilfører metafor for å bedre forstå dette: å betjene HMI tilsvarer å sette en operatør i førersetet i 'bilen'; en oppgave som ikke krever inngående kjennskap til motoren som driver bilen fremover. Egenskapene (interaksjonene) til det tekniske som ligger 'under panseret' kan reduseres til de delene operatøren sanser og interagerer med. I denne forstand er det kompleksitetsreduserende og forenklende for operatøren, men samtidig bidrar det også til å redusere gjennomsiktigheten til systemet. Systemoperatører kan besitte evnen til å 'kjøre bilen' i denne sammenheng, men har ikke nødvendigvis samme kunnskap om hvordan bilen (systemet) er satt sammen. Manglende evne til å forstå og begrense systemets komplekse interaksjoner utgjør delvis det Leveson (2011) forstår som farepotensialet i teknologiske systemer, og det som gjør systemsvikt tilsynelatende uforståelig, men likevel et forventet resultat av systemet, ifølge Perrow (1999). Det kan derimot fremstå som

hensiktsmessig å styrke funksjonaliteten til komponenter som HMI. Det gir systemoperatører bedre oversikt og kontroll over systemet, og forenkler selve arbeidsprosessen og interaksjonene med systemet. Derimot hvis denne utviklingen medfører å gjøre flere interaksjoner 'usynlige' for systemoperatørene (Perrow, 1999) ved å skjule de under 'panseret', er systemkompleksiteten kun skjult, ikke redusert. Systemsvikt vil derfor likevel være uforståelig og vanskelig å begrense.

Videre indikerer litteraturstudiet at kompleksitet er et voksende problem i cyber-fysiske systemer. Automatisering fordrer tettere koblinger og flere interaksjoner mellom systemet som en helhet. Samtidig gjør økende kompleksitet og omfang systemene ugjennomsiktige og vanskeligere å håndtere (Perrow, 1999). Dette er organisatorisk-tekniske faktorer som utfordrer systemoperatører og systemeieres evne til å forstå, analysere og kommunisere risiko i eget system. Sikkerhetstiltak eller inngrep i systemet for eksempel, krever ressurser ofte tilegnet gjennom sentrale beslutningsprosesser i organisasjoner. Tiltakene må fremstå som kostnadseffektive og hensiktsmessige for grupperinger i organisasjonen som ikke nødvendigvis besitter teknisk kompetanse, samtidig som at tiltakene konkurrerer mot andre prioriteringer og behov. Kompleksitet som en fremvoksende egenskap i cyberfysiske smartnett krever at systemeiere og operatører forplikter mer ressurser og oppmerksomhet mot kompleksitetsreduksjon og analyse av egne systemer (Leveson, 2011; Perrow, 1999). Det kan derimot fremstå som en motsigelse å forsøke å redusere systemkompleksitet samtidig som systemene skal effektiviseres. Tettere kobling og interaktivitet på tvers av systemene er ikke nødvendigvis synonymt med effektivitet, men som vist til tidligere i oppgaven er det mange krefter som trekker kraftsystemer mot tettere cyberfysisk integrasjon. En relevant utfordring for cyberfysiske systemer kan derfor være at utviklingen av sikkerhetsbarrierer blir mer utfordrende når systemene også blir mer komplekse. I tillegg til dette kan også de organisatoriske prosessene som beslutter, utvikler og implementerer barrierene være preget av tvetydighet og usikkerhet når teknologien også blir mer kompleks.

6.1.2 Den 'perfekte' barrieren

Utstedelse av sikkerhetsbegrensninger på komponentinteraksjoner ble presentert i delkapittel 5.1.5. Flere av analysemetodene som benyttes av artikkelforfatterne sikter til å avdekke optimale eller ideelle løsninger for dysfunksjonelle komponentforhold (Mo et al., 2012), eller fremheve det 'svakeste leddet' ved å analysere komponentinteraksjoner (Woodard et al., 2021). Dataintegritet i driftskontrollsystemer er fremhevet som en sentral sårbarhet i et cyberfysisk

smartnett, og IDS [3] er presentert som et nødvendig motverge. Hensikten med et slikt system er å oppdage manipulerte data og korrigere dem i sanntid, og dermed unngå potensielle driftsfeil som kan skade infrastrukturen (Zonouz & Haghani, 2013). En IDS skal i utgangspunktet bidra en systemoperatør som samhandler med systemet i å oppdage og forhindre avvik som kan resultere i driftsstans.

Litteraturstudiet viser at å produsere algoritmer og programvare som tilfredsstiller sikkerhetskravene til et cyberfysisk smartnett er krevende. Flere av studiene viser til egne løsninger på disse utfordringene, og validerer metodenes positive testresultater gjennom simulasjoner og 'test beds' (Attia et al., 2018; Bretas et al., 2019; Khazaei & Amini, 2021; Zonouz & Haghani, 2013). Det er ikke ønskelig å underdrive betydningen av IDS, og mangler i design og programmering bør håndteres og rettes opp. Men hvis vi refererer tilbake til poenget fra mo et al (Mo et al., 2012, s. 202): programvare og komponenter som automatisk oppdager uregelmessigheter som skadevare og datatukling er avhengig av forhåndsvurderinger av disse uregelmessighetene. Slike redskaper vil derfor også ha begrenset nytte hvis for eksempel skadevaren ikke er gjenkjennbar, eller angrepsmetoden som benyttes gjør den manipulerte dataen uadskillig fra autentisk data (Kim & Tong, 2013). En annen begrensning i algoritmer og programvare er tiden som kreves for å beregne innkommende data. Inkludere programvare som sikkerhetsbegrensninger mellom to komponenter innebærer også å skape tidsforsinkelse i denne prosessen (Leveson, 2011, s. 94). Som vist tidligere er det mindre rom for tidsmessig slakk eller buffer i driftskontrollsystemer, noe som stiller strengere krav til utformingen av IDS.

Beholder vi bilførerallegorien fra tidligere, vil en IDS forsikre føreren at motoroljelampen kun lyser når oljenivået er lavt. Forhindres lampen fra å varsle føreren, risikeres det at motoren skades ved kontinuerlig bruk. Hvis lampen ofte gir falske positive advarsler, vil føreren til slutt lære og ignorere disse advarslene, og akseptere dem som "normale". Litteraturstudiet viser at dataintegritet er kritisk i operasjonelle systemer for å unngå at operatører påfører systemet skade. Sårbarheten ligger derfor i et misforhold mellom den presenterte og 'reelle' tilstanden til systemet. Å operere et cyberfysisk smartnett fra en driftssentral medfører at operatøren kun kan påvirke systemet gjennom forutinntatte kontrollmekanismer på et 'høyere' nivå (Perrow, 1999, s. 81). De har ikke nødvendigvis umiddelbar tilgang til komponenter i den skarpe enden, og er derfor avhengig av informasjon som overføres gjennom digitale systemer. Avstanden mellom operatøren og komponentene de opererer blir derfor større, og i en forstand også

[3] Intrusion Detection System

abstrahert ved å forenkle kontrollen over systemet. Resultatet av tettere koblinger i systemet er potensielt at systemoperatørene kan konstruere forenklede mentale modeller av underliggende teknologien, som igjen gjør forekomsten av tekniske uregelmessigheter eller avvik mer forvirrende (Perrow, 1999).

Problemet som da tydeliggjøres, er et risikobilde med mer sofistikerte trusler og angrepsvektorer, mer komplekse systemer og tilsvarende komplekse tekniske sikkerhetsbarrierer. Innenfor rammene av en vitenskapelig artikkel om cyberfysisk systemsikring, er det logisk når man presenterer en spesifikk sårbarhet, at man også presenterer en tilsvarende løsning. Det man derimot kan utlede som et potensielt problem fra utvalget av litteraturen, er at vesentlig fokus rettes mot å utvikle ideelle eller perfekte sikkerhetsbarrierer som 'lukker' sårbarheten, og dermed eliminerer eller minimerer risikoen. Man bør også vurdere at løsninger på en enkelt komponent eller en type komponent ikke kan regnes som et sikkerhetsforbedrende tiltak, men heller som pålitelighetsstyrkende (Leveson, 2011). Systemet som en helhet, og dets primære funksjon (pålitelig kraftforsyning) kan fortsatt være mer eller mindre beskyttet hvis lignende konsekvenser kan oppnås ved ganske enkelt å målsette seg mot en annen type komponent eller funksjonalitet.

Dette er tekniske barrierer; algoritmer, programvare og komponenter som avdekker, eliminerer og korrigerer datamanipulasjon og skadevare. Sofistikerte algoritmer med økende kompleksitet og "intelligens" virker tiltalende, men disse formlene er fortsatt menneskeskapte artefakter, og er derfor utsatt for samme feilscenarioer i design, implementering og vedlikehold som enhver annen teknisk komponent (Leveson, 2011). Design av disse tekniske sikkerhetsbarrierene er også basert på forutinntatte trusler, noe som etterlater en usikkerhet hos systemoperatørene om de tekniske sikkerhetsbarrierene er i stand til å stanse angrepsvektorer og trusler man ikke har kjennskap til. Et av Levesons grunnleggende prinsipper er derimot at systemeiere og operatører i større grad kan 'designe' seg ut av tekniske problemer ved å begrense interaksjoner innad i systemet. Hun utvider også denne analysen til å omfatte organisatoriske styringsmekanismer som opprettholder kontrollen av prosesser som ivaretar sikkerhet (Leveson, 2011). Å utstede kontroll over systemet vil da innebære å kontrollere komponentinteraksjonene, så vel som designprosesser, implementasjon og vedlikehold av tekniske systemer. Neste delkapittel vil bidra til å belyse hvordan; til tross for gode intensjoner og rasjonelle styringsprosesser; er organisasjoner utsatt for ulykke og systemsvikt (Vaughan, 1996). Vi kan derimot kan konstatere så langt: selv om tekniske systembegrensninger er nødvendig; og mer sofistikerte sikkerhetsbarrierer ser appellerende ut, bør man utøve varsomhet med å konkludere at risikoen i cyberfysiske

systemer kan tilstrekkelig styres ved å begrense komponentinteraksjoner eller bygge komplekse sikkerhetsbarrierer 'over' allerede komplekse systemer. Implementasjonen av IDS eller andre tekniske sikkerhetsbarrierer burde derfor ikke enkeltvis anses som å gjøre systemene tryggere.

6.1.3 Systemstruktur og organisasjoner

Det sosiotekniske perspektivet uttrykker ideen om symbiose mellom menneske, organisasjon og teknologi. Systemstrukturen i cyberfysiske systemer kan således forstås som et resultat av organisasjoners målsetninger og prioriteringer; strukturer som igjen former organisasjoners konseptualiseringer av risiko og sikkerhet. Uttalelsen fra Perrow tidligere presentert kan også tolkes i sammenheng med cyber-fysiske systemer: det eksisterer ikke et teknologisk imperativ som tilsier at systemene må kobles tettere sammen (Perrow, 1999). Tettere cyberfysisk integrasjon og sammenkobling er heller en av byggeklossene i overordnede utviklingstrender i industri 4.0 (Lasi et al., 2014); hvor omfattende digitalisering muliggjør effektivisering av stadig flere prosesser og funksjoner i samfunnet. Effektivisering gjennom automatisering er et kjennetegn ved smartnett som repeteres i samtlige studier i utvalget. Muligheten for kommunikasjon og automatisering innad og på tvers av systemet; mellom mennesker, organisasjoner og komponenter utgjør essensen av systemets 'smarthet' (Attia et al., 2018; Ericsson, 2010). Faktorer som stammer fra organisasjoners omgivelser; eksempelvis forventninger om effektivisering, bedre integrasjon av fornybar energi og pålitelig forsyningssikkerhet til samfunnet her i Norge (Meld. St. 25 (2015-2016); Olje- og Energidepartementet, 2014); er faktorer som driver utviklingen av CPS i en bestemt retning.

Det kan dermed fremstå at det er en forståelse i litteraturen for at cyberfysiske smartnett i økende grad er komplekse systemer preget av interaktivitet, gjensidig avhengighet og tette koblinger. Det overordnede perspektivet på funksjonelle komponentforhold i litteraturen uttrykker en grad av usikkerhet rundt interaksjoner innad og utenfra systemet. Mangfoldet og heterogeniteten i komponentene medfører også at omfattende cyberfysiske systemer har mange komplekse interaksjoner. Dette er ifølge Perrow (1999), systemegenskaper som er knyttet til systemsvikt. For å oppsummere denne delen av diskusjonen, kan det pekes til at vesentlig kompleksitet i systemstrukturen bidrar til å gjøre cyberfysiske systemer risikoutsatte. Risiko som et uttrykk for usikkerhet om potensielle konsekvenser på systemets verdier (Aven & Renn, 2009), blir derfor forstørret i møte med forvirrende og ugjennomsiktige systemstrukturer. Dette reduserer systemeiere og systemoperatørers evne til å forestille seg potensielle sårbarheter og sviktscenarioer, og tettere koblinger reduserer også systemoperatørers evne til å reagere

umiddelbart på mindre avvik som potensielt kan forplante seg videre i systemet (Perrow, 1999). En konsekvens av dette kan være at hendelser og avvik i komponenter og enheter, enten utløst av komponentsvikt eller et cyberangrep, kan forårsake at kritiske styringsfunksjoner i systemet svikter. Den ultimate konsekvensen av dette kan være systemets evne til å opprettholde forsyningssikkerheten reduseres.

6.2 Prosesser

Cyber-fysiske smartnett er sosiotekniske systemer, og kan ikke redelig skilles fra organisasjonene og menneskene som aktivt deltar i systemets aktiviteter. Detaljerte og tekniske sikkerhetsløsninger må følges opp av en organisasjon som prioriterer sikkerhet, besitter kompetansen til å utrede eget system og implementere tiltak hvor nødvendig. Sikkerhetstiltak må også være kostnadseffektive og gjennomførbare i praksis. Andre faktorer, som lovgivning og regulering spiller også en vesentlig rolle i å forme den teknologiske utviklingen i kraftsystemet. Så langt har systemkompleksitet og tekniske sikkerhetsbarrierer blitt diskutert. Egenskapene ved den tekniske systemstrukturen og implikasjoner dette har for risiko og sikkerheten til systemene har blitt diskutert. I følgende delkapittel vil utfordringer knyttet til prosesser som ivaretar eller hemmer sikkerheten i cyberfysiske systemer diskuteres.

Tidligere presenterte aspekter ved cyberfysisk integrasjon; blant annet tette koblinger og kompleks interaktivitet reduserer gjennomsiktigheten og den umiddelbare evnen til å forstå feil når de oppstår i systemet. Flere organisatoriske faktorer forverrer også denne dynamikken. Ingen enkeltperson besitter fullstendig kunnskap om systemet, og alle dets finurligheter. Kunnskap deles mellom flere personer innenfor en organisasjon eller grupperinger i organisasjonsmiljøet. De som potensielt har den beste forutsetningen for å forstå teknologien er de som opererer med den hver dag i den ‘skarpe enden’. Beslutningstakere som står utenfor dette domenet av organisasjonen, vil alltid ha ufullstendig kunnskap om prosessene som foregår på et lavere nivå i organisasjonen (Vaughan, 1999). Ifølge Turner vil formidlingen av kunnskap og informasjon være kritisk for å unngå at dysfunksjonelle forhold får rotfeste i organisasjonen. Mer spesifikt handler det om å etablere prosesser som kommuniserer riktig mengde og type informasjon, som er avgjørende for sikkerheten til systemet (Turner, 1994). En potensiell utfordring i møte med økende kompleksitet, er å kommunisere og videreformidle kritisk informasjon mellom operatører og beslutningstakere.

Vi kan vurdere denne utfordringen i sammenheng med et argument presentert av Perrow: i møte med kompleksitet vil systemoperatører konstruere mentale modeller av systemene som reduserer kompleksiteten fremfor å omfavne den (Perrow, 1999). Systemstrukturen korrelerer i denne forstand med tilbøyeligheten organisasjoner har til å mislykkes ved å formidle kritisk informasjon og kunnskap mellom domener eller grupperinger innad i organisasjoner. Vaughan gjenspeiler dette poenget ved å sette teknologisk kompleksitet i sammenheng med uønskede hendelser: usikkerhet og tvetydighet om teknologiske egenskaper bidrar til suboptimal beslutningstaking i organisasjoner (Vaughan, 1999). En av måtene dette kommer til syne i litteraturen, er vektleggingen av analysemodeller som avdekker kritiske sårbarheter og dermed identifiserer hvor sikkerhetsinvesteringer er mest nødvendig. Det er ikke en enhetlighet i analysemodeller, og mangfoldet av sårbarhetene som beskrives er bredt. Dette viser en vesentlig grad av «tolkningsfleksibilitet» i forskningslitteraturen, slik Vaughan viser til (ibid.). Det er ikke nødvendigvis slik at artikkelforfatterne uttrykker forenklede modeller av cyberfysiske systemer slik Perrows argument i denne konteksten antyder. Derimot sikter dette heller til grupperinger innad i organisasjoner som opererer komplekse tekniske systemer. Dette leder til spørsmål om denne usikkerheten og tvetydigheten også er til stede i organisasjoner som faktisk former og drifter cyberfysiske systemer.

6.2.1 Komponentheterogenitet og leverandører

En av de sentrale kildene til kompleksitet og sårbarheter er komponentheterogeniteten i CPS (Humayed et al., 2017). Den trinnvise oppbygningen av cyberfysiske systemer medfører at bred diversitet mellom komponentene som integreres i systemet, og at disse komponentene ikke nødvendigvis ble designet med tanke på samspill i et større system. Avhengigheten av eksterne leverandører og produsenter spiller inn i denne sammenheng. Sårbarheter i allestedsnærværende programvare som Windows interagerer i varierende grad med AMS eller SCADA-systemer. Som Stuxnet viruset illustrerte, kan de allmenne funksjonene i denne programvaren utnyttes av trusselaktører til å bli en sårbarhet, og dermed gi tilgang til operasjonelle og administrative systemer (Langner, 2011). Dette er en utfordring for organisasjonene som styrer cyberfysiske systemer, fordi komponenter og programvare som er ikke-proprietære er designet, implementert og vedlikeholdt av underleverandører. Å styre disse sårbarhetene kan til en viss grad være utenfor rekkevidde av organisasjonen som kjøper og benytter seg av disse tjenestene.

Premissene for å styre risikoen i leverandørkjeder og innkjøpte tjenester og produkter er derfor annerledes fra cyberfysisk systemsikring. Den underliggende sårbarheten kan godt være teknisk

i den forstand at et sikkerhetshull eller funksjonalitet i programvare eller fastvare kan utnyttes; men en organisasjon som forvalter et cyberfysisk system kan ikke 'designe' seg ut av problemet slik kanskje Leveson ville fremstilt det. Sikkerhetshull i Windows programvare for eksempel, må lukkes av leverandøren; ikke organisasjonen. Programvareoppdateringer har tidligere blitt fremhevet som en kilde til sårbarhet; oppdateringer kan lukke sikkerhetshull og potensielt skape nye (Humayed et al., 2017); muligheten til å oppdatere fastvare kan forlenge levetid i komponenter, men det kan også fungere som angrepsvektorer (Sridhar et al., 2012). Selv om oppdateringer eller endringer i systemet kan lukke sikkerhetshull og sårbarheter, fordrer dette at organisasjonen påser at dette blir tilstrekkelig gjennomført i alle systemer som kan være sårbare. Større oppdateringer og endringer kan også potensielt bryte kontinuiteten i systemet og introdusere nye sårbarheter. Grundige vurderinger av risiko som følge av integrasjon er derimot en utfordring i stadig mer omfattende og komplekse systemer (Rodríguez et al., 2021).

Om forhold mellom leverandør og kjøper påpeker Ericsson: «kunden får det de ber om» (Ericsson, 2010, s. 1503). Et passende spørsmål kan da være; vet kunden hva de skal spørre om fra leverandøren? NVE har kartlagt flere av disse problemstillingene i det norske kraftsystemet gjennom en rapport som understreker nødvendigheten av bestillerkompetanse og kjennskap til behovene i eget system (Selnes et al., 2021). Leverandører konkurrerer seg imellom for å sikre kontrakter på anbud, og innkjøperen (organisasjonene) balanserer valg av leverandør på nytteverdien, kostnaden og potensiell risiko det innebærer å integrere produktet i deres system. Det vi kan lære av Vaughans analyse av Challenger-ulykker er at selv om underleverandører eller systemeiere kan ha de beste intensjoner om å ivareta sikkerheten når de anskaffer ny teknologi, er også innkjøpsprosesser gjenstand for organisatorisk "støy". Ideer om kostnadseffektivitet, produksjonspress og tvetydighet knyttet til teknologisk ytelse og usikkerhet; dette er faktorer som former og konstruerer oppfatninger av risiko i beslutningsprosesser. Utfordringen ligger ikke dermed i at organisasjonene må implementere perfekte rutiner som kontrollerer innkjøpsprosesser, men heller at rutiner og prosesser ikke kan fullstendig avverge at sårbarheter 'importeres' når nye komponenter eller digitale systemer integreres i et cyberfysisk system.

6.2.2 Usikkerhet og det ukjente

Rollen trusler og trusselaktører spiller som pådriver for potensiell systemsvikt, er en kilde til omfattende usikkerhet og tvetydighet. Litteraturutvalget er forholdsvis kortfattet i vurderinger av trusselaktører; diskusjonen er primært avgrenset til kunnskapen aktøren må besitte for å utføre et bestemt angrepsscenario. Derfor gjenstår ikke et veldig klart bilde av hvem som

potensielt kan utføre angrepene, og heller ikke hva deres evne er til å utføre. Ericsson (2010) peker til behovet for å koordinere sikkerheten i SCADA-systemer med nasjonale sikkerhetstjenester, som kan ha større innsikt i det bredere trussellandskapet (Ericsson, 2010, s. 1504). Vi kan sette disse momentene i sammenheng med en overordnet utvikling innenfor sikkerhetsfaget, hvor sikkerhet og sikring i større grad konvergeres (Kongsvik et al., 2018, s. 279). Trusselbildet som et aspekt av sikringsrisiko, er hovedsakelig utenfor 'grensene' av hva en organisasjon eller virksomhet i kraftbransjen kan kontrollere. En organisasjon som styrer risiko i et cyberfysisk system, er derfor begrenset til tiltak som sikrer eget system.

Ifølge Leveson derfor, bør det prioriteres å redusere sårbarheter gjennom begrensninger på komponentinteraksjoner (Leveson, 2020). Basert på litteraturstudiet, ser dette også ut til å være det rådende perspektivet innen cyber-fysisk systemsikring. Historiske hendelser som cyberangrepene mot ukrainske strømnett i 2015 (Liang et al., 2017), eller Stuxnet-skadevaren som spesifikt angriper og omprogrammerer SCADA-systemer (Langner, 2011), er hendelser som motiverer studiene innenfor cyberfysisk systemsikring. Disse historiske hendelsene er absolutt av betydning; å beskytte SCADA-systemer i et strømnett mot skadelig programvare som ligner på Stuxnet er en nødvendighet. Det som derimot tilskriver Stuxnet vesentlig betydning i en historisk kontekst, er hvordan viruset brøt etablerte konvensjoner om skadevare og sikkerhet i driftskontrollsystemer. Viruset benyttet selve funksjonaliteten programvaren leverte, og var ikke nødvendigvis et sikkerhetshull som kunne tettes igjen gjennom bedre sikring (Langner, 2011). I tillegg til det var viruset også en helt ukjent trussel, og dermed ikke forutsatt av etablerte sikkerhetskriterier og analyseverktøy.

I følge Leveson kunne skaden påført av viruset mot de iranske atomreaktorene vært avverget hvis sentrifugene i reaktoren hadde blitt ilagt en kontrollbegrensning i form av maks rotasjonshastighet (Leveson, 2020, s. 20). Problemet med denne analysen er derimot at 'problemet' defineres etter at hendelsen har inntruffet. De iranske ingeniørene og operatørene hadde ikke nødvendigvis oppfattet dette som et problem i det hele tatt; SCADA-systemene i anleggene var lukkede systemer, så beskyttelse mot skadevare er ikke en prioritet (Langner, 2011). En begrensning ved Levesons tilnærming til komponentbegrensninger blir derfor at sårbarhetene og tilsvarende sikkerhetsløsninger defineres innenfor rammene av det vi allerede har kjennskap til (Bieder & Gould, 2022). Levesons strategi til sikkerhetsstyring er potensielt hensiktsmessig i møte med kjente trusler, men etterlater ikke organisasjoner med verktøy for å imøtekomme det ukjente.

Dette betyr derimot ikke at forbedringer innen antivirus, brannmurer eller IDS er meningsløst. Som flere av forfatterne fra litteraturstudiet har påpekt: den største trusselen mot operasjonell drift av kraftsystemet er omfattende og koordinerte cyberangrep, som også er sjeldne (Gunduz & Das, 2020; Sun et al., 2018). Selv om man ikke riktig vet hvem som sto bak Stuxnet, har det blitt spekulert at virusets sofistikerte design og operasjonen nødvendig for å installere skadevaren i de lukkede systemene, krevde ressurser og kompetanse kun nasjonale sikkerhetstjenester besitter (Kushner, 2013). Stuxnet som et 'worst-case' scenario for et cyberfysisk strømnett vil praktisk talt sette umulige standarder for sikkerheten til systemene. Uten rimelige grunner til å anta at systemene er utsatt for denne typen angrep, vil sikringen mot det også fremstå som lite hensiktsmessig og kostbart. Enklere angrep motivert av for eksempel vinningskriminalitet eller personvernbrudd kan i større grad også forhindres gjennom enkle inngrep i etablerte sikkerhetsbarrierer. Håndteringen av det ukjente derimot, er en begrensning ved denne typen barrierer, slik diskutert i forrige delkapittel.

Organisasjoner som forvalter cyberfysiske systemer, står derfor overfor en utfordring: sikring av eget system krever til en viss grad også kunnskap om ukjente størrelser i trussellandskapet en virksomhet i kraftbransjen ikke har forutsetninger for å styre. Foruten dette vil det også gjenstå en vesentlig usikkerhet om hvordan ukjente angrepsvektorer kan påvirke systemene i fremtiden. Det burde ikke være en selvfølge at fremtidige katastrofer vil utartes på samme vis som den forrige. Dette betyr selvsagt ikke at organisasjoner ikke burde strekke seg lenger for å unngå potensielle tilstander som kan føre til systemsvikt, men som Vaughan advarer: vi burde være klar over begrensningene ved å anvende kjente løsninger mot ukjente problemer (Vaughan, 1996, s. 416). Det man derfor kan vurdere, er om stadig omfattende cyberfysisk integrasjon også medfører en tilsvarende vekst i sårbarhetene til systemet. Dersom dette er tilfellet, virker det urimelig å anta at uønskede hendelser rettet mot driftskontrollsystemer ikke på sikt vil kunne påvirke forsyningssikkerheten; hovedoppgaven til enhver organisasjon i kraftsystemet.

6.2.3 Vurdering av risiko og sårbarhet

Turner ville i denne sammenheng utfordret organisasjonen til å spørre seg selv om motsigelser mot de etablerte fortolkningsrammene tillates i organisasjonen. Et av faretegnene i inkubasjonsfasen er nettopp det at alternative tolkninger som bryter med de dominerende oppfatningene i organisasjonen undertrykkes (Turner, 1994). Organisasjoner som møter risiko beheftet av usikkerheter og motstridende fortolkninger, kan ende opp med å underrepresentere denne risikoen

eller avvise den som irrelevant og lite sannsynlig (Pidgeon & O'Leary, 2000). Vaughan (1996) viste eksempelvis at det var en felles oppfatning i NASA forut for Challenger-ulykken, at risiko ikke fullstendig elimineres; det var derfor et spørsmål om hvilken risiko man kan akseptere. Oppskytningen var et svært krevende teknisk prosjekt, og forventningene til pålitelighet i komponentene var høye. Hver systemdel eller komponent ble vurdert etter risikoakseptkriterier; en formell og rasjonaliserende prosess som stilte krav om å gripe inn dersom risikoen var uakseptabel (Vaughan, 1996, s. 81). Kvantitative utregninger og eksperimenter med teknologien tilskrev en tillitt til at systemet ville opptre som forventet, og større avvik kunne korrigeres gjennom risikostyringsprosessen (Vaughan, 1996, s. 79–85).

Vi kan trekke analogier mellom Vaughans analyse, og litteraturgjennomgangen i denne oppgaven. Litteraturstudiet viste for eksempel et mangfold av ulike analysemetoder og tilnærminger til å avdekke sårbarheter i cyberfysiske systemer. Det poengteres også i denne sammenheng at det er utfordrende å utvikle analyseverktøy som tilstrekkelig fanger opp geografisk og teknisk utbredelse av cyberfysiske strømnett (Friedberg et al., 2017; Mo et al., 2012; Sridhar et al., 2012). Forfatterne imøtekommer dette blant annet gjennom test beds og eksperimenter, som bistår til å validere artikkelforfatternes presenterte angrepsvektorer og sikkerhetsbarrierer. Flere svakheter ved 'test bed' ble trukket frem i delkapittel 5.1.4; basert på dette vil det være rimelig å forvente avvik mellom resultater produsert i kontrollerte og vitenskapelige omgivelser, og anvendelse i de faktiske systemene. Egenskapene som litteraturen på cyberfysisk sikring beskriver; systemstruktur og komponentinteraksjoner; analysemodeller av angrepsvektorer, sårbarheter og tekniske sikkerhetsbarrierer; dette er teknisk-rasjonaliserende prosesser som imøtekommer risiko gjenspeilet av kjente trusler og sårbarheter. Hva Vaughans analyse kan vise oss, er at til tross for intensjoner om å styre risikoen i cyberfysiske systemer gjennom systemsikring, gjenstår det et vesentlig usikkerhetsmoment om teknologien vil opptre som forventet, spesielt når den opererer i krevende omgivelser slik kraftsystemet gjør.

6.2.4 Organisatoriske fortolkningsrammer – teknosentrisk?

Turner og Vaughans berettelser av ulykke og katastrofe er tilknyttet hvordan forestillinger om risiko er konstruert og forvandlet gjennom organisasjoners ordinære prosesser. I denne forstand kan bekymringer om ukjente trusler eller sårbarheter potensielt forsvinne i 'støyen' av organisasjoners dagligdagse gjøremål (Turner, 1994). Sikkerhetsledere kan for eksempel være opptatt av å forsikre at forskrifter og regelverk følges av organisasjonen. Selv om forskrifter og regelverk følges til punkt og prikke, utgjør ikke dette nødvendigvis at risikoen er tilstrekkelig

redusert. Som vist i litteraturstudiet er utformingen av regelverk og rutiner i komplekse cyber-fysiske systemer en utfordring (Ouchani, 2021; Rodríguez et al., 2021). Utformingen av styringsdokumenter kan også være preget av en systemisk treghet som ofte hemmer sentrale forvaltningsorganer (Rasmussen, 1997, s. 186). Overdreven regulering bidrar også til normalisering av avvik, da det skaper mer arbeid for sikkerhetsledere og reduserer deres evne til å oppdage problemer (Vaughan, 1996, s. 420). Regelverk kan derfor ha en begrenset evne til å styre risikoen av et dynamisk risikolandskap beheftet av usikkerhet. Likevel er styringsdokumenter med på å etablere fortolkningsrammene for sikkerheten i organisasjoner; de hjelper organisasjoner med å forstå hva som anses som risikabelt, og hva som anses som trygt.

Fortolkningsrammene for virksomhetene i kraftbransjen formes i stor grad av omgivelsene. Både private og offentlige aktører i kraftbransjen; konkurranseutsatte eller monopolbaserte virksomheter streber etter å være økonomisk bærekraftig og effektive (Almklov et al., 2008). Digitalisering og industri 4.0 som henger tett sammen med utviklingen av CPS; tilhører overordnede globaliseringsprosesser som igjen former organisasjoner og teknologiske systemer (Le Coze, 2021, s. 103). Virksomhetene og organisasjonene i kraftbransjen har derfor incentiver for cyberfysisk integrasjon. Tidligere i oppgaven ble utviklingen av automasjon og tettere koblinger i systemstrukturer knyttet til disse overordnede utviklingstrendene. Man kan diskutere om Perrow ville advart om at denne utviklingen som selvskadende på systemene ved å gjøre de mer utsatt for systemsvikt. Samtidig er dette en utvikling som samsvarer med organisasjoners målsetninger om forbedret effektivitet eller konkurranseevne som forsikrer deres kontinuerlige eksistens. Selv om cyber-fysisk integrasjon potensielt utvider sårbarhetsflater og endrer risikoen for systemsvikt, vil det å avstå fra cyberfysisk integrasjon på samme måte fremstå som en risiko for organisasjonens økonomiske eller politiske levedyktighet.

Å forstå prosessene som konstruerer og forvandler risikofremstillinger innad organisasjoner handler ikke derfor bare om oppfatninger av fare og tilstrekkelige reaksjoner. Som Vaughans beretning detaljerer: dette er en komplisert prosess som utfolder seg over lang tid, involverer mange aktører og motstridende perspektiver og målsetninger. Som Turner også påpeker, vil ikke konsekvensene av nåværende systemstrukturer og sikkerhetsprosesser nødvendigvis vise seg før etter en katastrofe inntreffer (Dekker, 2014, s. 138). Målet med denne argumentasjonen er ikke å likestille driften av cyberfysiske systemer med romfergeprosjektene til NASA; derimot handler det om å se svikt i organisatoriske og teknologiske systemer i sammenheng med hverandre. Videre følger det også fra dette hvorvidt det cyberfysiske systemperspektivet også

omfavner de menneskelige og organisatoriske dimensjonene som spiller en sentral rolle for systemsikkerheten. Litteraturstudiet viser at cyberfysisk systemsikring som et fagfelt ikke er blottet for betraktninger om menneskelige og organisatoriske faktorer. Det fremstår derimot at egenskapene som vektlegges i studiene primært er fokusert på den teknologiske dimensjonen av systemene.

Litteraturen presentert på cyberfysisk systemsikring er ment å tilby løsninger på nye tekniske problemer, men etterlater ikke leseren med særlige inntrykk på hvordan organisasjoner som drifter systemene også må tenke nytt for å bidra til systemenes sikkerhet. Ser man helheten i argumentene presentert i denne diskusjonen, er det ingen grunn til å anta at et cyberfysisk smartnett som et sosioteknisk system, **ikke** er utsatt for det samme potensialet for organisatorisk dysfunksjonalitet eller normalisering av avvik. Samtidig er det mest sannsynlig idiosynkratiske trekk ved den underliggende teknologien, organisasjonsstrukturer og samfunnsomgivelser som skiller disse systemene fra andre sosiotekniske systemer studert tidligere. Derfor er ikke hensikten å ugyldiggjøre cyberfysisk systemsikring som et fagfelt. Et sosioteknisk system består stadig av en teknisk dimensjon, og dette fordrer at man også imøtekommer tekniske problemer. Så langt i diskusjonen har det blitt presentert samtlige grunner til at et teknosentrisk perspektiv på sikkerhet i cyberfysiske systemer kan være problematisk. Slik presentert i dette studiet kan man argumentere for at den største utfordringen organisasjoner står overfor som forvaltere av sikkerheten i cyberfysiske systemer, er å redusere helheten av systemet til det cyberfysiske. Et cyberfysisk systemperspektiv kan føre til at tekniske forestillinger om sårbarheter og risiko får en overvekt innen organisasjoners fortolkningsrammer. Dermed risikerer organisasjoner å neglisjere menneskelige og organisatoriske faktorer som innkapsler teknologien og påvirker dens utforming.

7.0 Konklusjon

Målet for denne oppgaven har vært å utforske utviklingen av cyberfysiske systemer og forskningen på cyberfysisk systemsikring. Ved å ramme inn forståelsen av disse systemene som sosiotekniske systemer, har oppgaven forsøkt å belyse hvordan cyberfysisk utvikling viser seg som sosiotekniske utfordringer for risiko og sikkerhet i organisasjoner. I teorikapittelet etableres en forståelse av sosiotekniske systemer, hvor menneske og teknologi er i samspill og gjensidighet med hverandre. Ytterligere beskrives hvordan systemenes strukturer og organisatoriske prosesser bidrar til å etablere fortolkningsrammer og forståelser av risiko, systemsvikt og sikkerhet. Denne forståelsen utvides også til cyberfysiske systemer, som forstås som sosiotekniske i den forstand at teknologien stadig er underlagt menneskelig og organisatoriske premisser. Fremstillinger av risiko, sårbarheter og sikkerhet er således forstått som konstruksjoner av en konkret sosial, politisk og institusjonell kontekst.

Dette premisset settes i sammenheng med forskningslitteratur på cyberfysisk systemsikring, som har bidratt til å fremheve egenskaper ved risiko og sikkerhet i cyberfysiske systemer. Det mest fremtredende funnet denne oppgaven har gjort er å vise et rådende teknosentrisk perspektiv på sikkerhet i forskningslitteraturen på cyberfysiske systemer. Cyberfysisk utvikling viser seg i en forstand som nye tekniske utfordringer for organisasjoner, hvor tettere koblinger og komplekse interaksjoner gjør systemene vanskeligere å forstå og håndtere. Denne utviklingen blir også forverret i samspill med usikkerhet og tvetydighet knyttet til trusselbildet systemene står overfor. Å styre risikoen av det ukjente er derfor en utfordring.

I en annen forstand kan man forstå utviklingen av cyberfysiske systemer i sammenheng med en fortolkningsramme hvor tekniske systemforhold er rådende. Sårbarheter, risiko systemsvikt og sikkerhet er derfor innkapslet av de tekniske forholdene, og danner en fortolkningsramme rundt disse konseptene. En sentral utfordring for organisasjoner kan derfor være at fremstillingen av systemene som cyberfysiske, neglisjerer menneskelige og organisatoriske faktorer som samspiller med teknologiens utvikling og drift. Tekniske sikkerhetsløsninger vil trolig fortsatt være en nødvendighet, men disse burde forstås i sammenheng med organisatoriske egenskaper og prosesser. En utfordring ved et cyberfysisk systemperspektiv kan derfor være at det blir teknosentrisk, og forholdet mellom teknologi og organisasjon er derfor ikke i likevekt.

7.1 Videre forskning

Dette studiet har vist momenter av det sosiotekniske perspektivet som er relevant i sammenheng med cyberfysisk integrasjon. Videre kunne det vært relevant å utforske menneskelige og organisatoriske aspekter ved ansatte og operatører i kraftbransjen som forholder seg til cyberfysiske systemer i praksis. Studier av for eksempel kommunikasjon og informasjonsformidling innad i organisasjoner i sammenheng med risikostyringsprosesser, ville vært en relevant studie i denne sammenheng.

Cyberfysisk teknologi har fordelen ved å være allestedsværende, og kan integreres i utallige systemer og funksjoner. Mer utbredt cyberfysisk integrasjon i samfunnet rundt oss, vil trolig bare styrke nytten av et sosioteknisk perspektiv, ettersom stadig flere mennesker og organisasjoner vil interagere med denne teknologien. Det kan derfor være relevant å utforske lignende problemstillinger i sammenheng med cyberfysisk integrasjon i andre virksomheter og systemer.

Litteraturliste

Almklov, P. G., & Antonsen, S. (2010). The Commoditization of Societal Safety. *Journal of Contingencies and Crisis Management*, *18*(3), 132–144. https://doi.org/10.1111/j.1468-5973.2010.00610.x

Almklov, P. G., Antonsen, S., Fenstad, J., Jacobsen, E., Nybø, A., & Kjølle, G. (2008). *Fra forvaltning til forretning – Restrukturering av norske nettselskaper og konsekvenser for samfunnssikkerhet*. https://sintef.brage.unit.no/sintef-xmlui/handle/11250/2367658

Andersson, G., Donalek, P., Farmer, R., Hatziargyriou, N., Kamwa, I., Kundur, P., Martins, N., Paserba, J., Pourbeik, P., Sanchez-Gasca, J., Schulz, R., Stankovic, A., Taylor, C., & Vittal, V. (2005). Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance. *IEEE Transactions on Power Systems*, *20*(4), 1922–1928. https://doi.org/10.1109/TPWRS.2005.857942

Ashibani, Y., & Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security*, *68*, 81–97. https://doi.org/10.1016/j.cose.2017.04.005

Attia, M., Senouci, S. M., Sedjelmaci, H., Aglzim, E.-H., & Chrenko, D. (2018). An efficient Intrusion Detection System against cyber-physical attacks in the smart grid. *Computers & Electrical Engineering*, *68*, 499–512. https://doi.org/10.1016/j.compeleceng.2018.05.006

Aven, T. (2009). Safety is the antonym of risk for some perspectives of risk. *Safety Science*, *47*(7), 925–930. https://doi.org/10.1016/j.ssci.2008.10.001

Aven, T. (2014). What is safety science? *Safety Science*, *67*, 15–20. https://doi.org/10.1016/j.ssci.2013.07.026

Aven, T. (2016). The reconceptualization of risk. I *Routledge Handbook of Risk Studies*. Routledge.

Aven, T., & Renn, O. (2009). On risk defined as an event where the outcome is uncertain. *Journal of Risk Research*, *12*(1), 1–11. https://doi.org/10.1080/13669870802488883

Aven, T., & Thekdi, S. (2022). *Risk science: An introduction* (1 Edition). Routledge.

Baheti, R., & Gill, H. (2011). Cyber-physical Systems. *Impact Control Technology*, 1–6.

Bandara, W., Furtmueller, E., Gorbacheva, E., Miskon, S., & Beekhuyzen, J. (2015). Achieving Rigor in Literature Reviews: Insights from Qualitative Data Analysis and Tool-Support. *Communications of the Association for Information Systems*, *37*(1). https://doi.org/10.17705/1CAIS.03708

Bell, M. L., & Anderson, G. B. (2012). The Mortality Of A Major Power Outage: Case Study Of The 2003 Blackout In New York, New York, USA. I *D61. RESPIRATORY CLINICAL EPIDEMIOLOGY* (Bd. 1–315, s. A6058–A6058). American Thoracic Society. https://doi.org/10.1164/ajrccm-conference.2012.185.1_MeetingAbstracts.A6058

Bieder, C., & Gould, K. P. (2022). *The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice*. https://www.crimrxiv.com/pub/mkbhf12k

Blokland, P. J., & Reniers, G. L. (2020). The Concepts of Risk, Safety, and Security: A Fundamental Exploration and Understanding of Similarities and Differences. I C. Bieder & K. Pettersen Gould (Red.), *The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice* (s. 9–16). Springer International Publishing. https://doi.org/10.1007/978-3-030-47229-0_2

Bretas, A. S., Bretas, N. G., & Carvalho, B. E. B. (2019). Further contributions to smart grids cyber-physical security as a malicious data attack: Proof and properties of the parameter error spreading out to the measurements and a relaxed correction model. *International Journal of Electrical Power & Energy Systems*, *104*, 43–51. https://doi.org/10.1016/j.ijepes.2018.06.039

Bruvoll, J., Brattekås, K., & Nystuen, K. O. (2020). Funksjonsbasert risikovurdering. I *Digital sikkerhet—En innføring*. Universitetsforlaget.

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, *106*(3), 345–361. https://doi.org/10.1108/02635570610653498

Ciborra, C. (2007). Digital Technologies and Risk: A Critical Review. I *Risk, Complexity and ICT*. Edward Elgar Publishing. https://ideas.repec.org/h/elg/eechap/4062_2.html

Dekker, S. (2014). *The field guide to understanding «human error»* (Third edition). Ashgate.

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security*, *92*, 101747. https://doi.org/10.1016/j.cose.2020.101747

Elsevier. (2022, mai 30). *About ScienceDirect*. Elsevier. https://www.elsevier.com/solutions/sciencedirect

Engen, O. A., Gould, K. P., Kruke, B. I., Hempel Lindøe, P., Olsen, K. H., & Olsen, O. E. (2021). *Perspektiver på samfunnssikkerhet*.

Engen, O. A. H., Kruke, B. I., Lindøe, P., H., Olsen, K., H., Olsen, O. E., & Pettersen, K., A. (2016). *Perspektiver på samfunnssikkerhet* (1. utg.). Cappelen Damm akademisk.

Ericsson, G. N. (2010). Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure. *IEEE Transactions on Power Delivery*, *25*(3), 1501–1507. https://doi.org/10.1109/TPWRD.2010.2046654

Evans, M., He, Y., Maglaras, L., & Janicke, H. (2019). HEART-IS: A novel technique for evaluating human error-related information security incidents. *Computers & Security*, *80*, 74–89. https://doi.org/10.1016/j.cose.2018.09.002

Fox, W. M. (1995). Sociotechnical System Principles and Guidelines: Past and Present. *The Journal of Applied Behavioral Science*, *31*(1), 91–105. https://doi.org/10.1177/0021886395311009

Friedberg, I., McLaughlin, K., Smith, P., Laverty, D., & Sezer, S. (2017). STPA-SafeSec: Safety and security analysis for cyber-physical systems. *Journal of Information Security and Applications*, *34*, 183–196. https://doi.org/10.1016/j.jisa.2016.05.008

Frøystad, C., Jaatun, M. G., Bernsmed, K., & Moe, M. (2018). *Risiko- og sårbarhetsanalyse for økt integrasjon mellom AMS, DMS og SCADA* (s. 41). NVE. http://publikasjoner.nve.no/eksternrapport/2018/eksternrapport2018_15.pdf?fbclid=IwAR32I2lhxK-wCjsXcFNA86mY3kJla6dphpxXtG6Go0oxS9YY8DtVayBJZLo

Furseth, I. (2020). *Masteroppgaven: Hvordan begynne—Og fullføre* (3. utgave.). Universitetsforlaget.

Glitre Energi. (2022, april 27). *Kraftsystemmodellen*. Glitre Energi Nett AS. https://www.glitreenergi-nett.no/om-glitre-energi-nett/

Gould, K. P., & Macrae, C. (2021). Hazardous Technological Systems from the Inside Out: An Introduction. I *Inside Hazardous Technological Systems*. CRC Press.

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*, *169*, 107094. https://doi.org/10.1016/j.comnet.2019.107094

Hagen, J. (2018). Standarder for IKT-sikkerhet—Nytte i regelutvikling og tilsyn i norsk kraftforsyning. I P. H. Lindøe & G. S. Braut (Red.), *Regulering og standardisering—Perspektiver og praksis*.

Hahn, A., Ashok, A., Sridhar, S., & Govindarasu, M. (2013). Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid. *IEEE Transactions on Smart Grid*, *4*(2), 847–855. https://doi.org/10.1109/TSG.2012.2226919

Hale, A. R., & Hovden, J. (1998). Management and culture: The third age of safety. A review of approaches to organizational aspects of safety, health and environment. I *Occupational Injury*. CRC Press.

Hanseth, O. (2007). Introduction: Integration–Complexity–Risk – The Making of Information Systems Out-of-Control. I *Risk, Complexity and ICT*. Edward Elgar Publishing. https://ideas.repec.org/h/elg/eechap/4062_1.html

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

Hollnagel, E. (2014). *Safety-I and Safety-II: The Past and Future of Safety Management*. Taylor & Francis Group. http://ebookcentral.proquest.com/lib/uisbib/detail.action?docID=1661242

Hopkins, A. (1999). The limits of normal accident theory. *Safety Science*, 10.

Hopkins, A. (2001). Was Three Mile Island a 'Normal Accident'? *Journal of Contingencies and Crisis Management*, *9*(2), 65–72. https://doi.org/10.1111/1468-5973.00155

Hopkins, A. (2016). *Quiet Outrage: The Way of a Sociologist*.

Hopkins, A. (2021). Turner and the Sociology of Disasters. I *Inside Hazardous Technological Systems* (s. 19–32). CRC Press.

Hughes, T. P. (2012). The Evolution of Large Technological Systems. I *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. MIT Press. http://ebookcentral.proquest.com/lib/uisbib/detail.action?docID=3339458

Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-Physical Systems Security—A Survey. *IEEE Internet of Things Journal*, *4*(6), 1802–1831. https://doi.org/10.1109/JIOT.2017.2703172

IEEE. (2022, mai 30). *About IEEE Xplore*. IEEE Xplore. https://ieeexplore.ieee.org/Xplorehelp/overview-of-ieee-xplore/about-ieee-xplore

Jore, S. H. (2017). The Conceptual and Scientific Demarcation of Security in Contrast to Safety. *European Journal for Security Research*, *4*(1), 157–174. https://doi.org/10.1007/s41125-017-0021-9

Jøsang, A. (2021). *Informasjonssikkerhet—Teori og praksis*. Universitetsforlaget.

Jaatun, M. G., Wille, E., Bernsmed, K., & Kilskar, S. S. (2021). *Grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer* (2021:00055). SINTEF. https://sintef.brage.unit.no/sintef-xmlui/bitstream/handle/11250/2835081/ID4+rapport+Ptil+IKT-sikkerhet+-+Robusthet+2020.pdf?sequence=2

Khazaei, J., & Amini, M. H. (2021). Protection of large-scale smart grids against false data injection cyberattacks leading to blackouts. *International Journal of Critical Infrastructure Protection*, *35*, 100457. https://doi.org/10.1016/j.ijcip.2021.100457

Khurana, H., Hadley, M., Lu, N., & Frincke, D. A. (2010). Smart-grid security issues. *IEEE Security Privacy*, *8*(1), 81–85. https://doi.org/10.1109/MSP.2010.49

Kim, J., & Tong, L. (2013). On Topology Attack of a Smart Grid: Undetectable Attacks and Countermeasures. *IEEE Journal on Selected Areas in Communications*, *31*(7), 1294–1305. https://doi.org/10.1109/JSAC.2013.130712

Kongsvik, T., Albrechtsen, E., Antonsen, S., Herrera, I., Hovden, J., & Schiefloe, P. M. (2018). *Sikkerhet i arbeidslivet*. Fagbokforl.

Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics*, *38*(2), 143–154. https://doi.org/10.1016/j.apergo.2006.03.010

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security*, *28*(7), 509–520. https://doi.org/10.1016/j.cose.2009.04.006

Kushner, D. (2013). The real story of stuxnet. *IEEE Spectrum*, *50*(3), 48–53. https://doi.org/10.1109/MSPEC.2013.6471059

Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security & Privacy*, *9*(3), 49–51. https://doi.org/10.1109/MSP.2011.67

Langø, H.-I. (2013). Den akademiske debatten om cybersikkerhet. *Internasjonal Politikk*, *71*(02), 229–240. https://doi.org/10.18261/ISSN1891-1757-2013-02-06

Langø, H.-I., & Sandvik, K. B. (2013). Cyberspace og sikkerhet. *Internasjonal Politikk*, *71*(02), 221–228. https://doi.org/10.18261/ISSN1891-1757-2013-02-05

Larsen, K. R., Hovorka, D., Dennis, A., & West, J. (2019). Understanding the Elephant: The Discourse Approach to Boundary Identification and Corpus Construction for Theory Review Articles. *Journal of the Association for Information Systems*, *20*(7). https://doi.org/10.17705/1jais.00556

Lasi, H., Fettke, P., Kemper, H.-G., Feld, T., & Hoffmann, M. (2014). Industry 4.0. *Business & Information Systems Engineering*, *6*(4), 239–242. https://doi.org/10.1007/s12599-014-0334-4

Le Coze, J.-C. (2015). 1984–2014. Normal Accidents. Was Charles Perrow Right for the Wrong Reasons? *Journal of Contingencies and Crisis Management*, *23*(4), 275–286. https://doi.org/10.1111/1468-5973.12090

Le Coze, J.-C. (2016). Risk management: Sociotechnological risks and disasters. I *Routledge Handbook of Risk Studies*. Routledge.

Le Coze, J.-C. (2021). *Post normal accident: Revisiting Perrow's Classic*.

Lee, E. A. (2008). Cyber Physical Systems: Design Challenges. *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, 363–369. https://doi.org/10.1109/ISORC.2008.25

Leszczyna, R. (2018). A review of standards with cybersecurity requirements for smart grid. *Computers & Security*, *77*, 262–276. https://doi.org/10.1016/j.cose.2018.03.011

Leveson, N. (2011). *Engineering a safer world: Systems thinking applied to safety*. MIT Press.

Leveson, N. (2020). Safety and Security Are Two Sides of the Same Coin. I *The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice*. Springer International Publishing. https://dspace.mit.edu/handle/1721.1/137069

Liang, G., Weller, S. R., Zhao, J., Luo, F., & Dong, Z. Y. (2017). The 2015 Ukraine Blackout: Implications for False Data Injection Attacks. *IEEE Transactions on Power Systems*, *32*(4), 3317–3318. https://doi.org/10.1109/TPWRS.2016.2631891

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, *22*(3), 365–404. https://doi.org/10.1080/09636412.2013.816122

Liu, S., Chen, B., Zourntos, T., Kundur, D., & Butler-Purry, K. (2014). A coordinated multi-switch attack for cascading failures in smart grid. *IEEE Transactions on Smart Grid*, *5*(3), 1183–1195. https://doi.org/10.1109/TSG.2014.2302476

Lu, Y. (2017). Industry 4.0: A survey on technologies, applications and open research issues. *Journal of Industrial Information Integration*, *6*, 1–10. https://doi.org/10.1016/j.jii.2017.04.005

Lundgren, B., Link to external site, this link will open in a new window, & Möller, N. (2019). Defining Information Security. *Science and Engineering Ethics*, *25*(2), 419–441. http://dx.doi.org.ez-proxy.uis.no/10.1007/s11948-017-9992-1

Lupton, D. (2013). *Risk* (2nd ed). Routledge.

Marashi, K., Sarvestani, S. S., & Hurson, A. R. (2021). Identification of interdependencies and prediction of fault propagation for cyber–physical systems. *Reliability Engineering & System Safety*, *215*, 107787. https://doi.org/10.1016/j.ress.2021.107787

Mark, M. S., Tømte, C. E., Næss, T., & Røsdal, T. (2019). Leaving the windows open—Økt mangel på IKT-sikkerhetskompetanse i Norge. *Norsk sosiologisk tidsskrift*, *3*(03), 173–190. https://doi.org/10.18261/issn.2535-2512-2019-03-02

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

Meld. St. 25 (2015-2016). (2016). *Kraft til endring—Energipolitikken mot 2030*. Olje- og energidepartementet. https://www.regjeringen.no/no/dokumenter/meld.-st.-25-20152016/id2482952/

Mo, Y., Kim, T. H.-J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., & Sinopoli, B. (2012). Cyber–Physical Security of a Smart Grid Infrastructure. *Proceedings of the IEEE*, *100*(1), 195–209. https://doi.org/10.1109/JPROC.2011.2161428

NOU 2015:13. (2015). *Digital sårbarhet—Et sikkert samfunn*. Justis- og beredskapsdepartementet.

NSM. (2021). *RISIKO 2021 – helhetlig sikring mot sammensatte trusler*. https://nsm.no/aktuelt/risiko-2021-helhetlig-sikring-mot-sammensatte-trusler

NVE. (2021, mars 23). *NVE fortsetter innsatsen for å sikre kraftforsyningen mot dataangrep—NVE*. https://www.nve.no/nytt-fra-nve/nyheter-sikkerhet-og-energiforsyningsberedskap/nve-fortsetter-innsatsen-for-a-sikre-kraftforsyningen-mot-dataangrep/

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

Olje- og energidepartementet. (2019, januar 3). *Eierskap i kraftsektoren*. Energifakta Norge. https://energifakta-norge.no/om-energisektoren/eierskap-i-kraftsektoren/

Olsen, O. E., & Lindøe, P. H. (2009). Risk on the ramble: The international transfer of risk and vulnerability. *Safety Science*, *47*(6), 743–755. https://doi.org/10.1016/j.ssci.2008.01.012

Ouchani, S. (2021). A security policy hardening framework for Socio-Cyber-Physical Systems. *Journal of Systems Architecture*, *119*, 102259. https://doi.org/10.1016/j.sysarc.2021.102259

Perrow, C. (1983). The Organizational Context of Human Factors Engineering. *Administrative Science Quarterly*, *28*(4), 521–541. https://doi.org/10.2307/2393007

Perrow, C. (1999). *Normal accidents: Living with high-risk technologies*. Princeton University Press.

Pettersen, K. (2016). Understanding uncertainty: Thinking through in relation to high-risk technologies. I *Routledge Handbook of Risk Studies*. Routledge.

Pidgeon, N., & O'Leary, M. (2000). Man-made disasters: Why technology and organizations (sometimes) fail. *Safety Science*, *34*(1), 15–30. https://doi.org/10.1016/S0925-7535(00)00004-7

Rajkumar, R., Lee, I., Sha, L., & Stankovic, J. (2010). Cyber-physical systems: The next computing revolution. *Design Automation Conference*, 731–736. https://doi.org/10.1145/1837274.1837461

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science*, *27*(2), 183–213. https://doi.org/10.1016/S0925-7535(97)00052-0

Reason, J. T. (1997). *Managing the risks of organizational accidents*. Ashgate.

Renn, O. (2008). *Risk governance: Coping with uncertainty in a complex world*. Earthscan.

Riksrevisjonen. (2021). *Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen* (3:7 (2020−2021)). https://www.riksrevisjonen.no/rapporter-mappe/no-2020-2021/undersokelse-av-nves-arbeid-med-ikt-sikkerhet-i-kraftforsyningen/

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

Rodríguez, M. Á. S., Higuera, J. B., Higuera, J. R. B., Montalvo, J. A. S., & Crespo, R. G. (2021). A systematic approach to analysis for assessing the security level of cyber-physical systems in the electricity sector. *Microprocessors and Microsystems*, *87*, 104352. https://doi.org/10.1016/j.micpro.2021.104352

Røyksund, M., & Valdal, A. K. (2020). *Kartlegging av bruk av tingenes internett (IoT/ IIoT) i norsk kraftforsyning* (Nr. 2/2020). Norges vassdrags- og energidirektorat. https://www.nve.no/nytt-fra-nve/nyheter-sikkerhet-og-energiforsyningsberedskap/nve-kartlegger-hvordan-tingenes-internett-brukes-i-dagens-kraftforsyning/

Schweizer, P.-J. (2021). Systemic risks – concepts and challenges for risk governance. *Journal of Risk Research*, *24*(1), 78–93. https://doi.org/10.1080/13669877.2019.1687574

Selnes, S. H., Moen, S. R., Ji, S. E., & Njå, O. (2021). *Kraftbransjens leverandørkjeder—Digital sikkerhet og sårbarhet i globaliseringens tidsalder* (Nr. 18/2021). Norges vassdrags- og energidirektorat.

Skilton, M., & Hovsepian, F. (2018). The 4th Industrial Revolution Impact. I M. Skilton & F. Hovsepian (Red.), *The 4th Industrial Revolution: Responding to the Impact of Artificial Intelligence on Business* (s. 3–28). Springer International Publishing. https://doi.org/10.1007/978-3-319-62479-2_1

Skotnes, R. (2015). *Challenges for safety and security management of network companies due to increased use of ICT in the electric power supply sector* [Doktorgradsavhandling, University of Stavanger, Norway]. Universitetet i Stavanger. https://uis.brage.unit.no/uis-xmlui/handle/11250/2374441

Skotnes, R. (2018). Regulering og standardisering av IKT-sikkerhet i kraftsektoren – holdninger, fordeler og ulemper. I P. H. Lindøe & G. S. Braut (Red.), *Regulering og standardisering—Perspektiver og praksis*.

Smith, C. L., & Brooks, D. J. (2013). *Security science: The theory and practice of security*. Elsevier, BH.

Solberg, Ø., & Njå, O. (2012). Reflections on the ontological status of risk. *Journal of Risk Research*, *15*(9), 1201–1215. https://doi.org/10.1080/13669877.2012.713385

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Sridhar, S., Hahn, A., & Govindarasu, M. (2012). Cyber–Physical System Security for the Electric Power Grid. *Proceedings of the IEEE*, *100*(1), 210–224. https://doi.org/10.1109/JPROC.2011.2165269

Statnett. (2021, oktober 13). *Om systemansvaret*. Statnett. https://www.statnett.no/for-aktorer-i-kraftbransjen/systemansvaret/om-systemansvaret/

Strupczewski, G. (2021). Defining cyber risk. *Safety Science*, *135*, 105143. https://doi.org/10.1016/j.ssci.2020.105143

Sun, C.-C., Hahn, A., & Liu, C.-C. (2018). Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems*, *99*, 45–56. https://doi.org/10.1016/j.ijepes.2017.12.020

Taib, R., Yu, K., Berkovsky, S., Wiggins, M., & Bayl-Smith, P. (2019). Social Engineering and Organisational Dependencies in Phishing Attacks. I D. Lamas, F. Loizides, L. Nacke, H. Petrie, M. Winckler, & P. Zaphiris (Red.), *Human-Computer Interaction – INTERACT 2019* (s. 564–584). Springer International Publishing. https://doi.org/10.1007/978-3-030-29381-9_35

Turner, B. A. (1976). The Organizational and Interorganizational Development of Disasters. *Administrative Science Quarterly*, *21*(3), 378–397. https://doi.org/10.2307/2391850

Turner, B. A. (1994). Causes of Disaster: Sloppy Management. *British Journal of Management*, *5*(3), 215–219. https://doi.org/10.1111/j.1467-8551.1994.tb00172.x

Turner, B. A. (1997). *Man-made disasters* (2nd ed.). Butterworth-Heinemann.

Tøien, F. K., Fagermyr, J., Treider, G., & Remvang, H. (2021). *IKT-sikkerhetstilstanden i kraftforsyningen 2021* (Nr. 19/2021). Norges vassdrags- og energidirektorat. https://publikasjoner.nve.no/eksternrapport/2021/eksternrapport2021_19.pdf

Törngren, M., Asplund, F., Bensalem, S., McDermid, J., Passerone, R., Pfeifer, H., Sangiovanni-Vincentelli, A., & Schätz, B. (2017). Chapter 1—Characterization, Analysis, and Recommendations for Exploiting the Opportunities of Cyber-Physical Systems. I H. Song, D. B. Rawat, S. Jeschke, & C. Brecher (Red.), *Cyber-Physical Systems* (s. 3–14). Academic Press. https://doi.org/10.1016/B978-0-12-803801-7.00001-8

Vaughan, D. (1996). *The Challenger launch decision: Risky technology, culture, and deviance at NASA*. University of Chicago Press.

Vaughan, D. (1999). The Dark Side of Organizations: Mistake, Misconduct, and Disaster. *Annual Review of Sociology*, *25*(1), 271–305. https://doi.org/10.1146/annurev.soc.25.1.271

von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, *23*(5), 371–376. https://doi.org/10.1016/j.cose.2004.05.002

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Walker, G. H., Stanton, N. A., Salmon, P. M., & Jenkins, D. P. (2008). A review of sociotechnical systems theory: A classic concept for new command and control paradigms. *Theoretical Issues in Ergonomics Science*, *9*(6), 479–499. https://doi.org/10.1080/14639220701635470

Watson, R. T., & Webster, J. (2020). Analysing the past to prepare for the future: Writing a literature review a roadmap for release 2.0. *Journal of Decision Systems*, *29*(3), 129–147. https://doi.org/10.1080/12460125.2020.1798591

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, *26*(2), xiii–xxiii.

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*, *17*(1), 4–19. https://doi.org/10.1108/09685220910944722

Woll, K., & Eriksson-Zetterquist, U. (2014). *Organisasjonsteori*. Cappelen Damm akademisk.

Woodard, M., Marashi, K., Sarvestani, S. S., & Hurson, A. R. (2021). Survivability evaluation and importance analysis for cyber–physical smart grids. *Reliability Engineering & System Safety*, *210*, 107479. https://doi.org/10.1016/j.ress.2021.107479

Wurm, J., Jin, Y., Liu, Y., Hu, S., Heffner, K., Rahman, F., & Tehranipoor, M. (2017). Introduction to Cyber-Physical System Security: A Cross-Layer Perspective. *IEEE Transactions on Multi-Scale Computing Systems*, *3*(3), 215–227. https://doi.org/10.1109/TMSCS.2016.2569446

Yin, L., Fang, B., Guo, Y., Sun, Z., & Tian, Z. (2020). Hierarchically defining Internet of Things security: From CIA to CACA. *International Journal of Distributed Sensor Networks*, *16*(1), 1550147719899374. https://doi.org/10.1177/1550147719899374

Zanutto, A., Shreeve, B. O., Follis, K., Busby, J. S., & Rashid, A. (2017). *The shadow warriors: In the no man's land between industrial control systems and enterprise IT systems*. https://eprints.lancs.ac.uk/id/eprint/86729/

Zonouz, S., & Haghani, P. (2013). Cyber-physical security metric inference in smart grid critical infrastructures based on system administrators' responsive behavior. *Computers & Security*, *39*, 190–200. https://doi.org/10.1016/j.cose.2013.07.003