Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: Samfunnsikkerhet	Vårsemesteret, 2011 Åpen
Forfatter: Erlend Jullum Leiknes	…… (signatur forfatter)
Faglig ansvarlig: Ole Andreas Engen Veileder(e): Ole Andreas Engen	
Tittel på masteroppgaven: Informasjonssikkerhet i Komplekse Systemer Engelsk tittel: Information Security in Complex Systems	
Studiepoeng: 30	
Emneord: Komplekse systemer Samfunnsikkerhet Informasjonssikkerhet Systemteori	Sidetall: 49 + vedlegg/annet: 0 Stavanger, 16. juni 2008

Forord

Jeg vil takke informantene for at de kunne stille til intervju hvor de kom med gode innspill som gjorde denne oppgaven mulig. Jeg vil også takke mine klassekamerater for støtte og gode diskusjoner. Til slutt vil jeg takke min bror for hans hjelpsomhet og kunnskaper.

Stavanger, 12 juli 2011

Erlend Jullum Leiknes

Innholdsfortegnelse

Sammendrag

Virksomheter benytter seg av IKT-systemer for å forenkle sin hverdag. Disse systemene har utviklet seg fra å være enkle verktøy til å bli en integrert del i organisasjoner, og er nå ofte svært komplekse systemer som virksomheter er blitt avhengig av.

Ved å analysere de systemegenskaper i IKT-system som gjør dem til komplekse systemer, blir det undersøkt hvilke systemteorier som er best egnet til å forstå IKT-systemer som et kompleks system.

To IT-sjefer i to ulike norske kommuner er blitt intervjuet, hvor temaet var deres sikkerhetsmessige utfordringer.

To hovedteorier om hvordan komplekse systemers egenskaper gjør dem tilbøyelige til ulykker, ble benyttet: *Natural Accident Theory* og *Systems Theory Accident Model and Processes*. Dette både til å analysere deres uttalte forhold til sikkerhet (altså hva de to informantene selv sa) og for å drøfte hvordan disse forholdene (altså hva de selv sa og de slutninger man kan trekke ut i fra dette) er forankret i systemteoriene. I tillegg er organistatoriske faktorer blitt analysert gjennom bruk av *High Reliability Organisation*-teorier.

Ved bruk av *Natural Accident Theory* kommer det frem at forsøk på å forenkle systemene, for å gjøre driften lettere håndterbar, førte til at systeme ble mer komplekse: Dette hadde som konsekvens at eventuelle feil ble mindre transparente. Mindre pessimistisk var *Systems Theory Accident Model and Processes*, hvor det viser seg at kompleksiteten kan håndteres ved å implementere gode sikkerhetsmessige begresninger i de ulike systemkomponentene.

1 Innledning

I dette kapittelet blir bakgrunnen for undersøkelsen presentert. Innledningsvis gis det en beskrivelse av IKT-systemers utvikling i virksomheter. Videre gis det en forklaring på hvorfor det er ønskelig å betrakte IKT-systemer i et systemperspektiv. Deretter blir problemstillingen samt nødvendige avgrensninger og utdypninger presentert.

1.1 Datasystemers innpass i organisasjoner og infrastruktur

Tidligere har IKT-systemer vært ment som et verktøy for å effektivisere og forenkle den normale virksomheten i en organisasjon. Videre har systemene utviklet seg til å bli integrert i organisatoriske prosesser, og er blitt en kritisk del av den normale driften (Sivertsen 2007). Ved et eventuelt frafall av datasystemer hos virksomhetene vil deres evne til løse sine primæroppgaver bli redusert. I løpet av kort tid er de blitt avhengige de ulike IKT-systemene de har tatt i bruk, og systemene utvikler seg fortsatt meget raskt i størrelse og funksjonalitet (Sivertsen 2007). Når systemene vokser i størrelse i form av flere komponenter og større gjensidig avhengighet mellom komponentene, øker kompleksiteten i systemene. Kompleksiteten er en stor utfordring for sikkerhet. Siden systemkomponenter kan ha så mange tilstander, mister man oversikten over hva som skjer med kjente funksjoner når de blir satt inn i nye sammenhenger. Dette er en av årsakene til at sikkerhetshull oppstår (Forskningsrådet 2008). Sikkerheten utvikler seg dessverre ikke i takt med systemet, og kommer ofte som etterskudd i form av tilfeldige sikkerhetsoppdateringer (ibid).

1.2 Hvorfor betrakte IKT-systemer i et systemperspektiv?

Et IKT-system består både av tekniske og ikke-tekniske komponenter. Normalt vil man se for seg et system som består av tekniske komponenter som datamaskiner, skrivere, nettverkskomponenter og lignende. Alle disse tekniske komponentene har sikkerhetsmessige utfordringer, som for eksempel feil i programvare og manglende sikkerhetstiltak. Et annet aspekt i IKT-systemer er de ikke-tekniske komponentene som er i interaksjon med de tekniske komponentene. Brukere av et IKT-system har en viss frihet til å utføre operasjoner i et teknisk system, og noen av handlingene de utfører kan medføre sikkerhetsrisiko for systemet (Reason 1997). Handlingsrommet for et systems brukere blir ofte regulert gjennom organisatoriske virkemidler som reglementer for bruk av IT.

Med alle disse ulike elementene som inngår i et IKT-system, blir dette systemet tolket som et sosioteknisk system hvor menneskelig aktivitet, samt reglementene som er ment for å regulere disse, inngår som en del av det helhetlige systemet. Vi vil i denne undersøkelsen benytte oss av ulike systemteorier for å undersøke hvilke av disse som kan anvedes for å forstå hvordan man kan jobbe for et sikrere IKT-system.

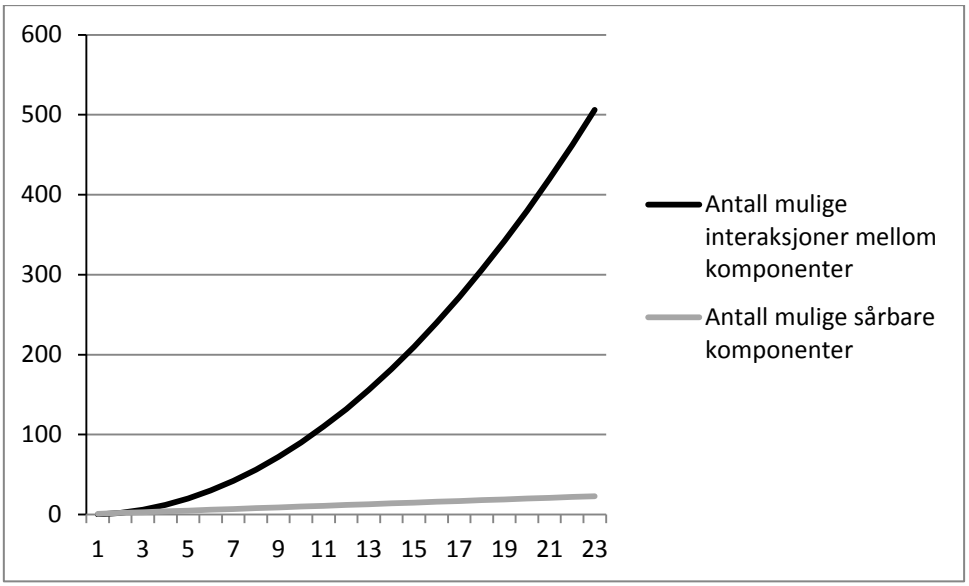
En rask oppsummering av de ulike systemteoriene som benyttes:

- HRO-teorien for *High Reliability Organisations* er typisk anvendt i systemer hvor det er liten vei fra unormal hendelse til ulykke. For å unngå dette må alle leddene i systemet være tilstrekkelig opplært til å kunne håndtere hendelser på riktig måte. Dette innebærer at man må ha full forståelse av det tekniske systemet.
- STAMP begrunner at ulykker i komplekse systemer ikke skyldes kompleksiteten i seg selv, men at ulykker forekommer fordi de ulike systemkomponentene blir integrert i systemene ved manglende sikkerhetsmessige restriksjoner. For å unngå ulykker i

system, er det nødvendig å håndheve disse restriksjonene komponenter er underlagt for å de (komponentene) skal kunne interaktere med andre systemkomponenter på en måte som ikke setter systemet i fare.

- NAT-teorien argumenterer for at ulykker i komplekse systemer er naturlig på grunn av uforutsette interaksjoner. For å kunne gjøre et system sikkert ifølge denne teorien, er det nødvendig å redusere kompleksiteten ved å gjøre sammenkoblingen av systemet mer lineært.

Utgangspunktet til denne undersøkelsen er den pragmatiske holdningen til IKT-sikkerhet hvor en sikkerhetsløsning aldri er bedre enn det svakeste leddet. Den økende veksten av IKT-systemer kommer til å prege virksomheter fremover, og denne praksisen i fremtiden føre til en større sikkerhetsutfordring da IKT-systemer stadig vokser i størrelse og kompleksitet (Forskningsrådet 2008). Hvis vi ser på kompleksitet som funksjon av antall komponetner, vil man se at antall mulige interaksjoner vokser eksponensielt med antall komponenter. Dette er illustrert i Figur 1. Dette viser til at interaksjon kan bli en uhåndterlig utfordring i komplekse systemer. Når IKT-systemene vokser i størrelse i form av flere komponenter og større gjensidig avhengighet mellom komponentene, øker kompleksiteten i systemene. Som figuren viser, kan kompleksiteten bli mer og mer uhåndterlig når systemene vokser i størrelse.



Figur 1 - Eksponensielt voksende interaksjoner

Ved å studere dette fenomenet ved bruk av systemteorier er det ønskelig å finne ut hvordan denne utfordringen blir håndtert sett gjennom et utvalg av systemteorier.

1.3 Problemstilling

Utgangspunktet for denne undersøkelsen er den voksende kompleksiteten IKT-systemer er utsatt for. Trenden er at dette er noe som vil fortsette fremover, og vil være den største sikkerhetsutfordringen i datasystemer (Forskningsrådet 2008). Det er mange likhetstrekk mellom IKT-systemer og andre tradisjonelle komplekse sosiotekniske systemer, noe som gjør det interessant å undersøke hvordan det i praksis blir arbeidet for å håndtere den økende kompleksiteten som organisasjoner må hanskes med. Denne oppgaven har som mål å belyse hvordan kompleksitet i IKT-systemer blir håndtert sikkerhetsmessig gjennom et perspektiv av ulike systemteorier. Med bakgrunn i dette, undersøkes følgende problemstilling:

Hvilke(n) tilnæring(er) til systemteori passer best for å styre sikkerheten i IKT-systemer?

For å få svar på dette, stilles også det følgende forskningsspørsmål:

- Hva slags tilnærming av systemteori benyttes av organisasjoner i praksis?

1.4 Definisjoner

I dette del-kapittelet er de mest sentrale begrepene som er benyttet i oppgaven avklart.

1.4.1 IKT-system

IKT står for Informasjon- og kommunikasjonsteknologi. I denne undersøkelsen er IKT-systemer sett på som sosiotekniske systemer, hvor altså mennesker spiller sin rolle i systemet. Informasjonssikkerheten vil gjelde uavhengig av informasjonsbærer. Et IKT-system vil derfor også inkludere organisatoriske prosedyrer som påvirker bruken av deres system. De tradisjonelle tekniske komponentene inngår også i vår definisjon av et IKT-system. Med dette menes rent teknisk utstyr.

1.4.2 Sikkerhet

I det norske språket er ordet ”sikkerhet” tvetydig da det både kan gjelde tiltak mot tilsiktende hendelse og tilfeldige uønskede hendelser. Det engelske ordet “safety” referer til vern mot ikke-intenderte uønskede hendelser, mens “security” referer til vern mot intenderte uønskede hendelser (Vinje 2006). Både tilsiktede og ikke-tilsiktede handlinger vil kunne føre til brudd på de tiltakene som er satt til å ivareta informasjonssikkerheten. Det er derfor nødvendig å presisere at videre i denne undersøkelsen så vil ordet ”sikkerhet” bli benyttet både om tilsiktende og ikke-tilsiktende hendelser som påvirker informasjonssikkerheten. Med informasjonssikkerhet menes da de tiltakene som er benyttet for å sikre at de følgende tre kriterier blir oppfylt vedrørende den informasjonen som skal beskyttes: *konfidensialitet*, *integritet* og *tilgjengelighet*. Det samme vil også gjelde for IT-funksjonene som overfører og behandler informasjon (Vinje 2006).

1.4.3 Ulykke

Teoriene som er valgt i denne undersøkelsen, benytter et ulykkesbegrep som viser til skade på produksjon, menneske og miljø. Hva som betegnes som en systemulykke, er avhengig av hva man velger som et overordnet system. En ulykke er i denne undersøkelsen derfor definert som de situasjoner hvor informasjonssikkerheten ikke lenger ivaretatt. I sikkerhetsdefinisjonen over er det tre ulike kriterier som avgjør om informasjonssikkerheten er ivaretatt. Denne ulykkesdefinisjonen vil bli videre utarbeidet i teorikapittelet da det har forankring i valgt systemmodell.

1.4.4 Tiltak

Under tiltak vil vi benytte oss av harde og myke tiltak, eller barrierer.

Med myke tiltak menes de regulerende tiltakene som er ment for å styrke menneskers handlingsrom (Reason 1997). Eksempel på disse er regler, opplæring, regulering, tilsyn o.l.

Med harde tiltak referes det til tekniske innrettninger som er ment for å hindre farlige handlinger (Ibid). I en IKT-sammenheng, omfatter dette blant annet tilgangskontroll, brannmurer, fysiske sperringer o.l.

1.5 Antagelser

De systemteoriene som er anvendt i denne undersøkelsen, er utviklet med hensyn til utilsiktede hendelser. Innen informasjonssikkerhet er det ofte slik at systemfeil og –ulykker er forårsaket av gjerningspersoner. For å kunne anvende disse teoriene er det nødvendig å anta at disse også er gyldige for hendelser som er tilsiktet. Dette gjøres på bakgrunn av at samtlige teorier argumenterer for at systemulykker ikke kan oppstå på grunn av individuelle feil, men på grunn av systemegenskaper som tillater dette.

1.6 Avgrensninger

Undersøkelsen benytter seg av eksisterende systemteorier som har klare forklaringer for hva som er årsakene til ulykker i et komplekst system. Det er derfor nødvendig å avgrense oppgaven til å inkludere de ulike organisatoriske faktorene som kan belyses ved bruk av disse teoriene:

- Undersøkelsen fokuserer på organisasjoner som benytter seg av IKT-systemer som et verktøy for å utføre sin virksomhet.
- Undersøkelsen vil kun inkludere de delene av et IKT-system som organisasjonen har mulighet til å påvirke gjennom myke eller harde barrierer.
- Undersøkelsen vil betrakte hvordan organisasjoner håndterer den komplekse utfordringen ved å belyse de strategiske valgene som blir utført av organisasjonens IT-ledelse.

2 Metode

Dette kapittelet omhandler forskningsprosessen, begrunnelse for de metodiske valgene og hvordan disse påvirket undersøkelsens kvalitet. De første delene i kapittelet omhandler fasene i forskningsprosessen.

2.1 Forundersøkelse

Den innledende fasen bestod i å få en oversikt over det temaet som skulle undersøkes gjennom dokumentstudier og studie av tidligere arbeid som er blitt gjort innen dette området. Dette ble hovedsaklig gjort gjennom litteraturstudie. Forundersøkelsen viste at det tidligere ikke var gjort en tilsvarende undersøkelse. Det ble tidlig etablert at det var nødvendig å utvikle en egen modell for å klassifisere IKT-systemer som et komplekst sosioteknisk system. Det ble videre valgt å utføre undersøkelsen på en eksplorerende måte.

Informantene ble valgt på bakgrunn av det kriterium at de har en besluttningstakende myndighet i deres organisasjon hva angår IKT-sikkerhet.

De teoriene som er blitt valgt, dreier seg om risikostyring i tekniske og sosiotekniske systemer.

2.2 Valg av informanter

Under forundersøkelsen var det satt fokus på å benytte nettleverandører i kraftindustrien, men på grunn av et naturlig monopol i de regionene de tilhører, viste det seg at potensielt tilgjengelige informanter var ytterst få.

Det ble så valgt å benytte IT-sjefer i ulike kommuner som informanter. Grunnen til at dette valget ble tatt, var at det her fantes flere av den samme type organisasjoner med tilsvarende like oppgaver og problemer. Valget å undersøke to lignende organisasjoner ble tatt på

bakgrunn av et ønske om å styrke empiriens reliabilitet (Jacobsen 2005). Dette ved å få flere synspunkter på de samme spørsmålene i lignende kontekst.

To kommuner sa seg villig til å la seg intervjue. I og med at de ikke ønsket at utenforstående skulle kunne dra nytte av eventuelle svakheter som kunne bli avdekket, ønsket de å være anonyme.

2.3 Undersøkelsesmetode

Det ble valgt å foreta en kvalitativ undersøkelse. Dette ble gjennomført ved å foreta intervjuer av to kommuner. Det ble valgt å ha en åpen intervjustil. Dette for å la informantene gå inn på de temaene de selv synes er viktige (Jacobsen 2005). For å kunne styrke datagrunnlaget på samme tema fra flere kilder ble det i forkant utarbeidet en intervjuguide for å kunne lede de to ulike informantene inn på de samme temaene. Under intervjuene ble det benyttet båndopptaker. Dette ble så transkribert og anonymisert.

2.4 Valg av teorier

De teoriene som ble valgt, har følgende kriterier som benyttes i undersøkelsen:

1) De er utviklet for å kunne analysere hvordan ulykker og komplekse systemer henger sammen.
2) De har en forklaring på hvilke systemegenskaper som fører til systemulykker.
3) De er egnet til å benyttes i sosiotekniske systemer.

Modellen som er blitt utviklet for å modellere hvordan et IKT-system opptrer som et komplekst system, er basert på Charles Perrows NAT-modell. Dette er en generisk modell som har formelle definisjoner som gjør det mulig å tilpasse det til de fleste tekniske og sosiotekniske systemer. At denne modellen bygger på teori om hva som forårsaker ulykker i

komplekse systemer, gjør at den egnet til å benyttes i tolkning av IKT-systemer. Levesons STAMP-teori bygger videre på denne modellen presentert i NAT, men har en annen forståelse for hvorfor ulykker i systemer oppstår samt hvordan man unngår ulykker i komplekse systemer. HRO er en modell som er benyttet til å forklare organisatoriske egenskaper som er i stand til å håndtere komplekse systemer på en trygg måte.

2.5 Undersøkelsens kvalitet

2.5.1 Reliabilitet

Det ble valgt å undersøke to organisasjoner med tilsvarende virkeområde, hvor de har lignende arbeidsoppgaver og problemer. Jacobsen viser til at begrepet reliabilitet snarere er knyttet til kvantitativ og positivistisk tradisjon (Jacobsen 2005). I begge intervjuene kommer flere av de samme poengene frem, noe som kan tyde på at en empirisk samsvar. Dette ble benyttet veiledende spørsmål for å bevege informantene inn på de samme temaene. Imidlertid stod de fritt til å besvare dem i den retning de ønsket.

2.5.2 Validitet

Undersøkelsen baserer seg på hvordan informantene opplever problemer som har med datasikkerhet å gjøre. Det er altså ikke en direkte undersøkelse av datasikkerheten, men dreier seg om hvordan deres organisasjon forholder seg til de komplekse i IKT-systemer, og deres personlige syn på dette. Synspunktene til de to ulike informantene synes å stemme godt overens, noe som kan tyde på at dette også ville (kunne) være tilfelle om undersøkelsens omfang ble utvidet. Det synes relevant å nevne at de i denne undersøkelsen er anonyme.

2.5.3 Overførbarhet

Denne undersøkelsen er knyttet opp til den empiri som ble funnet innen kommunal sektor. Som vi vet, kan ofte denne type organisasjoner være ressursmangel, både økonomisk og kapasitetsmessig. I eksempelvis privat sektor hvor dette kan være et mindre problem, vil man derfor sannsynligvis kunne finne andre synspunkt på hvordan de håndterer komplekse systemer. Modellen som ble benyttet, er imidlertid ment til å kunne analysere IKT-system uavhengig av dets opprinnelige funksjon, og burde derfor være mulig å utføre på forskjellige organisasjoner. Konklusjonen vil likevel være knyttet til den type organisasjon som er blitt undersøkt. I de organisasjoner som har lignende drift- og sikkerhetsmessige utfordringer, kan det forventes at lignende konklusjoner kan bli trukket ved bruk av en tilsvarende undersøkelse.

3 Teori

I dette kapittelet presenteres det teoretiske fundamentet som ligger til grunn i undersøkelsen. Innledningsvis skal vi se hvordan IKT-systemet kan betraktes som et komplekst system. Deretter vil de tre ulike teoriene undersøkelsen bygger på, bli benyttet for å analysere funnene. Dette er henholdsvis *Natural Accidents Theory* (NAT), *Systems Theory Accident Model and Processes* (STAMP) og *High Reliability Organization* (HRO).

3.1 Sårbarheter i sosiotekniske systemer

Innledningsvis ble det vist til at kompleksitet er en økende faktor i IKT-systemer og at denne må håndteres for å kunne unngå ulykker inntruffet på bakgrunn av dette. Dette vises det også til i artikkelen *Detecting Chains for Vulnerabilities in Industrial Networks* (Cheminod, Bertolotti et al. 2009). Her kommer det frem at når kompleksiteten i nettverk øker, så er det snakk om diskré og uforutsette interaksjoner mellom tilsynelatende urelaterte sårbarheter. Faren med dette er at inntrengere kan benytte seg av en sårbarhet til å utnytte andre sårbarheter. Dette omtales som en kjede av sårbarheter (Cheminod, Bertolotti et al. 2009). Med dette som et utgangspunkt på hvorfor kompleksitet i datanettverk er en av hovedutfordringene med tanke på sikkerheten, vil vi videre se på teorier som har som mål å hindre ulykker i komplekse systemer.

Et IKT-system er et sosioteknisk system. Dette innebærer at mennesker også inngår i et slikt system, og at sikkerheten i et slikt system ikke bare er avhengig av tilstanden til de tekniske komponenter. Brukere av systemene interakterer også med IKT-systemer, og kan da også gjøre dette på uforutsette måter. Dette beskrives som individers handlingsrom, hvor de vil kunne utføre utrygge handlinger som kan føre til systemfeil. Organisatoriske prosesser er det som begrenser handlingsrommet (Reason 1997). Reglement og sikkerhetskultur fungerer

som myke barrierer og er et virkemiddel for å styre IKT-sikkerheten i en organisasjon (Ibid). Disse blir også derfor en naturlig del av hvordan vi velger å betrakte et IKT-system.

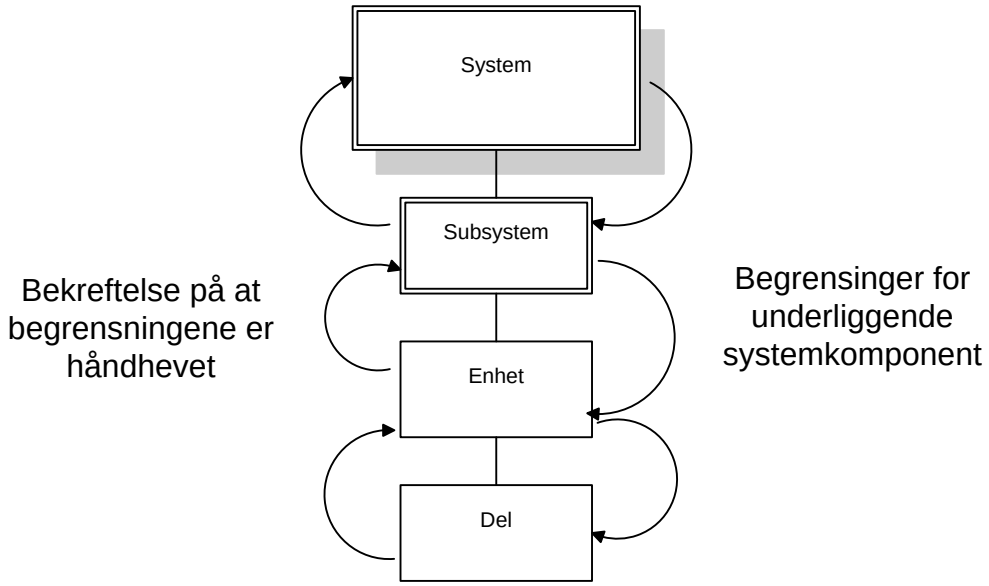
3.2 Natural Accidents Theory

Ifølge NAT vil ulykker forekomme *naturlig* i komplekse systemer. Det er to systemegenskaper som forårsaker dette: Den første egenskapen dreier seg om i hvor høy grad systemets komponenter har mulighet til å interaktere med andre systemkomponenter. Dette gjelder både for uforutsette og forutsette interaksjoner. Den andre systemegenskapen for et ulykkesutsatt system dreier seg om hvor tett systemkomponentene er koblet sammen. Det kan oppstå feil i komponenter i et system, slik at de oppfører seg på uforutsette måter. Dette kan føre til at komponentene interakterer med andre komponenter på uforutsette måter. Kaskadefeil kan oppstå hvor flere komponenter vil bli berørt som følge av dette. Systemer med høy grad av interaktiv kompleksitet har høyere mulighet til å forårsake uforutsette interaksjoner. Disse interaksjonene kan føre til systemfeil, og hvor store konsekvenser disse vil ha, er avhengig av hvor tett koblet systemfeilene er. Systemer med tette koblinger vil kunne få større konsekvenser enn de som er løst koblet. I et tett koblet system er det mindre avstand mellom årsak og virkning som kan føre til et systemuhell. Det blir derfor mindre tid til å reagere før feilen får mulighet til å materlialiseres som et uhell (Perrow 1999) (Hanseth and Ciborra 2007). Denne systemteorien foreslår at man ved å redusere kompleksitet og dermed ved å gjøre de mer lineære samt gjøre systemet løsere koblet, så vil systemet være mindre utsatt for ulykker (Perrow 1999).

3.3 Systems Theory Accident Model and Processes

I komplekse systemer vil interaksjoner ofte forårsake ulykker, selv når komponentene utfører den oppgaven de er satt til. Systemets komponenter kan være pålitelige, men det

medfører verken at totalsystemet er pålitelig eller sikkert. Med dette sier teorien at sikkerhet ikke er en komponentegenskap, men en systemegenskap. Sikkerhet må derfor kontrolleres på et systemnivå, hvor de ulike systemkomponentene har visse sikkerhetsmessige begrensninger og forutsetninger. For hvert nivå i systemet må det være kontroll-løkker som ser at disse sikkerhetsbegrensningene er ivaretatt. Eksempel på hvordan kontroll-løkkene i et system er vist i Figur 2. Figuren benytter seg av systemmodell som er presentert i kapittel 3.6.



Figur 2 – Kontroll-løkker for begrensninger og håndheving av disse

Sikkerhet blir derfor sett på som et kontrollproblem hvor man må ta hensyn til de forutsetningene og begrensningene som de underliggende komponentene har, og det miljøet de er satt til å operere i. Komponentbegrensningene oppstår allerede ved design av de ulike komponentene, og disse må da tas hensyn til ved produksjon. Dette gjelder videre for implementasjon av komponentene i et system.

Et eksempel på en situasjon hvor pålitelighet og sikkerhet ikke er en komponentegenskap gis: En dør på et fly kan være pålitelig. Man kan åpne og lukke døren, men med en gang det

er mulig å utføre dette når flyet er i luftrommet, vil totalsystemet kunne bli utsatt for en større ulykke. Selv om komponenten utfører sin funksjon pålitelig, er ikke de sikkerhetsmessige begrensningene ivaretatt, og systemet som en helhet vil være usikkert. Mangel på sikkerhetsmessige begrensninger og kontrollmekanismer sees derfor som på årsaken til en eventuell ulykke.

STAMP-teorien hevder at det ikke er komponentfeil som forårsaker ulykker, men manglende kontroll og håndhevelse av sikkerhetsrelaterte begrensninger gjennom design, utvikling og implementasjon av de ulike komponentene som utgjør systemet. Ulykker forekommer når komponentfeil, eksterne virkninger og/eller dysfunksjonelle interaksjoner mellom komponenter ikke blir tilstrekkelig håndtert (Leveson 2011).

STAMP-teorien bygger på samme systemmodell som NAT, og gir andre forklaringer på hvorfor ulykker i komplekse system oppstår. Det er derfor interessant å se hvordan sikkerhet i IKT-systemer blir sett på som tilstedeværelse av de prosessenene Leveson mener er nødvendige for å ha et sikkert system.

3.4 High Reliability Organization

HRO-teorien beskriver organisasjoner som har klart å utføre sin virksomhet i en årrekke uten å ha vært utsatt for katastrofale uhell, dette tross for at de håndterer systemer som gjenkjennes som komplekse (Hanseth and Ciborra 2007).

Definisjonen av en HRO-organisasjon er mer omfattende enn de to ovenstående teoriene, som er klare systembeskrivelser. En HRO-organisasjon er en sikkerhetskultur, noe som består av følgende underkulturer:

- Rapporterende kultur

- Rettferdig kultur
- Fleksibel kultur
- Lærende kultur

Vi vil gå dypere inn de to underkulturene *rapporterende kultur* og *fleksibel kultur*. Karakteristikker som fremhever disse underkulturene vil senere bli benyttet for å undersøke om de organisasjonene som er gjenstand for denne undersøkelsen, har nettopp karakteristikker som stemmer overens med HRO-teorien.

Fleksibilitet er en av de definerende egenskapene til en HRO-organisasjon. En studie viser at HRO-organisasjoner har følgende karakteristikker (Reason 1997):

- Organisasjonene er store, er dynamiske og har i perioder høy interaksjon.
- De utfører komplekse og eksakte oppgaver under høyt tidspress.
- De har utført oppgavene med lav feilrate og uten katastrofale ulykker i en årrekke.

Strategiene disse organisasjonene benytter seg av, er de følgende (Hanseth and Ciborra 2007):

- Ansatte i organisasjonen får opplæring til å kunne håndtere potensielt farlige situasjoner kjapt og korrekt, uten å måtte bli veiledet av overordnede
- Når kompleksiteten blir for stor for en person å håndtere, benyttes uformelle nettverk som består av seniorer, tekniske spesialister og rådgivere
- Bruk av redundante enheter og personer hvor den ene vil kunne overta hvis den andre gjør en feil eller svikter
- Evne til å forstå kompleksiteten av teknologien de benytter, ved å lære av tidligere feil og annen erfaring

I en rapporterende kultur kommer det frem fem ulike faktorer som en nødvendige for at et rapporteringssystem i en *rapporterende kultur* skal fungere (Reason 1997):

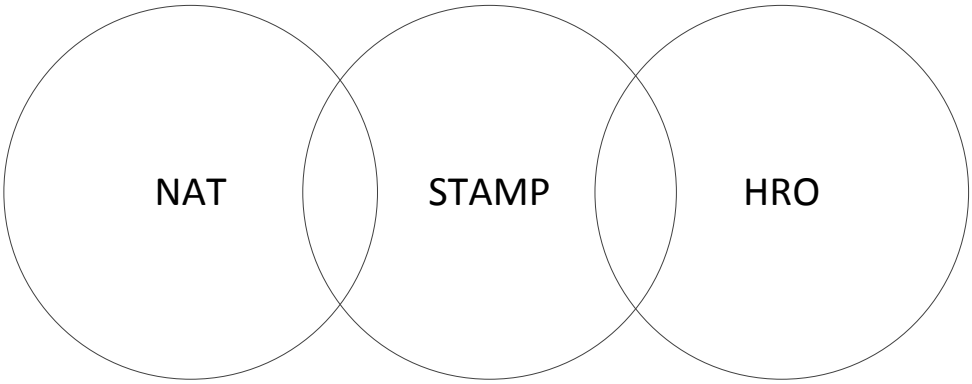
- Garantier mot disiplinere tiltak
- Konfidensialitet og anonymisering
- At de som samler inn og behandler rapportene ikke er de samme som har myndighet til å fremme disiplinerende tiltak
- Relevant tilbakemelding som viser at rapporteringer blir tatt hensyn til
- Enkelt system for innrapportering

En ulykke ifølge HRO sies å ha årsak i organisatoriske faktorer. På utsiden kan det ofte virke som om det er farlige handlinger som er utført av individer, men går man dypere inn i det, viser det seg ofte at lokale faktorer har vært en medvirkende årsak til ulykken. Videre vil man finne at disse er forankret i organisatoriske faktorer.

3.5 Sammensetting av de ulike teoriene

De ulike teoriene som er presentert ovenfor beskriver forskjellige systemegenskaper som enten gjør systemer robuste eller usikre. Felles for samtlige teorier er at systemulykker ikke forekommer på grunn av enkeltfeil. I NAT kommer det frem at ulykker vil opptre naturlig i systemer som har en ulineær sammensetning og tette koblinger. Måten å gjøre systemet mer robust på er å gjøre systemene mer lineære, og implementere buffere for å få et løsere koblet system. STAMP baserer seg på at det er de samme systemegenskapene som forårsaker ulykker, nemlig interaksjoner som oppstår uforutsett mellom systemkomponenter, men at den forutliggende årsaken er mangel på kontroll- og håndhevingsmekanismer som ivaretar de sikkerhetsmessige begrensningene de ulike komponentene har. HRO viser til en rekke organisatoriske egenskaper de organisasjoner som

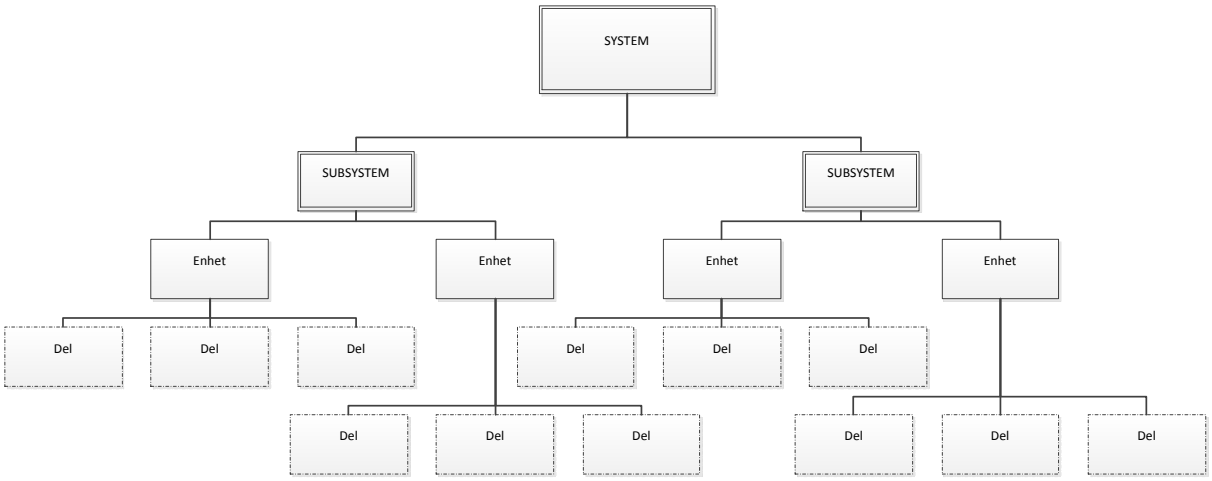
har vist å kunne håndtere komplekse systemer uten større ulykker over lang tid, har til felles. De ulike faktorene som slike organisasjoner besitter, er blant annet dyp teknisk forståelse av systemet de håndterer og klare definisjoner på hva som er riktige handlinger (Hanseth and Ciborra 2007). Dette berører også STAMP, hvor man må forstå de sikkerhetsmessige begrensningene som må ivaretas for at et system kan opptre sikkert. Som Figur 3 viser, er systemteoriene delvis overlappende.



Figur 3 - Årsaker til systemulykker iht. systemteoriene

3.6 Systemmodell

Modellen som presenteres her, er basert på systemdefinisjonen i Natural Accidents Theory. Denne modellen benytter fire nivå: System, Subsystem, Enhet og Del. Eksempel på den hierarkiske sammensettingen av et slikt system illustreres i Figur 4.



Figur 4 - Systemmodell basert på systemmodell fra NAT

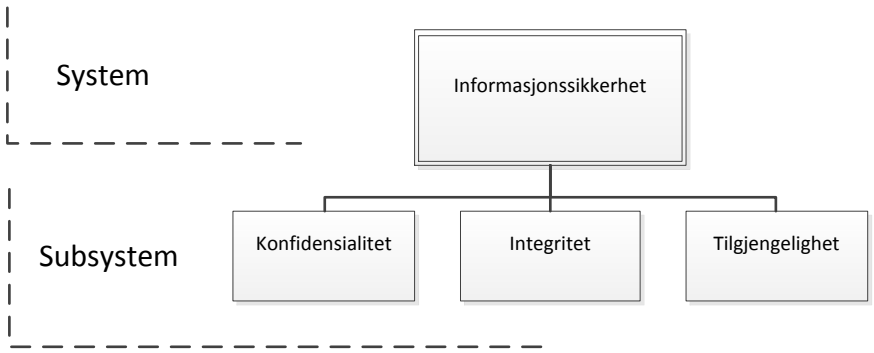
Hva som velges som totalsystem og som undersystem, er avhengig av hvordan systemet som helhet blir rammet hvis en av disse svikter. En ulykke er en svikt i et system eller undersystem som fører til at en eller flere deler av systemet blir skadet, og den pågående driften av systemet stanses.

Med dette til grunn vil vi i neste delkapittel benytte denne ulykkesdefinisjonen for å konstruere et totalsystem hvor informasjonssikkerhet vil bli definert som systemets hovedfunksjon.

3.6.1 Informasjonssikkerhet som system

Et IKT-system er som nevnt i innledningen, ment som et verktøy for å forenkle og effektivisere den normale virksomheten i en organisasjon. Når organisasjoner er blitt avhengige av IKT-systemer som et verktøy for å utføre den normale virksomheten, er gjerne systemene blitt uunnværlige for organisasjonen. Informasjonen som virksomheten behandler, kan være av sensitiv art, være avhengig av korrekt informasjon og at informasjonen er tilgjengelig. Derfor har IKT-systemer utover de vanlige funksjonene også en oppgave i å opprettholde *konfidensialitet*, *integritet* og *tilgjengelighet*. Dette blir også omtalt som de tre grunnpilarene i informasjonssikkerhet (Lacey 2009).

Når vi betrakter et IKT-system som et komplekst sosioteknisk system, benytter vi NATs systemdefinisjon hvor det overordnede systemet er ensbetydende med begrepet Informasjonssikkerhet. *Konfidensialitet*, *integritet* og *tilgjengelighet* er systemets undersystemer for å tilfredsstille systemmodellens definisjon på systemulykke.



Figur 5 - Informasjonssikkerhet som overordnet system

3.6.2 Ulykker i vår systemmodell

Etter vår systemmodell er altså systemets funksjon å opprettholde *konfidensialitet*, *integritet* og *tilgengelighet*. Når et system opprettholder konfidensialitet, er det beskyttet mot uautorisert tilgang til informasjon som skal beskyttes. Integriteten til et system er opprettholdt når det er beskyttet mot uautoriserte endringer i systemets informasjon. Med tilgjengelighet menes at kun autorisert personell er gitt tilgang til systemet (Jones, Kovacich et al. 2002). Et datainnbrudd i et IKT-system vil berøre en eller flere av disse elementene, og vil derfor kunne bli beskrevet som en ulykke. I vår systemmodell er disse elementene blitt kategorisert som undersystemet til informasjonssikkerhet, og når disse er blitt brutt, har det oppstått en ulykke i informasjonssikkerhet som system (Perrow 1999).

Det er nødvendigvis ikke synlige hendelser da datainnbrudd i sin natur kan være subtile hendelser hvor det vil ta tid å oppdage innbruddet, hvis det i det hele tatt blir oppdaget. Det er derfor et skille mellom spionasje og sabotasje mot et system.

Selv om et IKT-system er blitt utsatt for et vellykket datangrep, kan det fortsatt utføre sin oppgave hvis hensikten ikke har vært å sabotere den pågående driften. Det er derfor nødvendig å definere hva som menes med en ulykke i et IKT-system.

IKT-system er ofte ment som et effektiviserende verktøy i en virksomhet. Et frafall av *tilgjengelighet* vil føre til at systemet ikke lenger kan utføre det arbeidet det er ment å utføre.

Som sagt er i vår kontekst et IKT-systems oppgave å ivareta *konfidensialitet*, *integritet* og *tilgjengelighet*. Dette er de tre grunnpilarene som må være der for å kunne ha et sikkert IKT-system. Vi ser da bort ifra systemets egentlige funksjon, utenom det selvfølgelige kravet at det skal være tilgjengelig for brukerene.

4 Emperi

Dette kapittelet er delt inn etter de ulike komponentene som kan berøre sikkerheten i et informasjonssystem. De to informantenes tanker og meninger som fremgått fra intervjuene, vil her komme til uttrykk underlagt denne inndelingen. Som nevnt i innledningen, dreier det seg om to representanter fra to forskjellige kommuner, her henholdsvis kalt (informant) i kommune A og (informant) i kommune B. Fra intervjuene vil det bli trukket frem aktuelle temaer som kan være med å gi svar på undersøkelsens forskningsspørsmål og problemstilling.

4.1 Ansvar for sikkerhet

Informantene er IT-ledere i sine respektive organisasjoner. De har et overordnet ansvar for IT-sikkerhet, og de har egne ansatte som har ansvar for sikkerheten. Informant i kommune A presiserer at de er pålagt å ha en sikkerhetsansvarlig og at dette ansvaret ikke skal ligge hos IT-sjefen. Dette for at toppledelsen i kommunen, altså rådmannen, skal ha to forskjellige rapporteringsveier. I denne kommunen har en ansatt i personalavdelingen sikkerhetsansvaret, et ansvar som kommer som et tillegg til de ordinære pliktene hans/hennes. For at hver etat skal være representert i de valgene de tar, og for å avlaste sikkerhetsansvarlige, har de derfor valgt å danne en gruppe med medlemmer fra de forskjellige etatene hvor totalansvaret for sikkerhet ligger. Kommune B har i likhet med kommune A dannet en styringsgruppe for informasjonssikkerhet. Også denne er representert av alle de ulike etatene i organisasjonen.

4.2 Brukere i et IKT-system

På spørsmål om hvorvidt de ansatte blir kurset innen sikker bruk av IT, svarer de det følgende: Informant i Kommune B kan foretelle at brukere får formell opplæring av bruk av

IT, og at det er avtaledokumenter hva gjelder datasikkerhet som må signeres når man blir ansatt. Kommunen viser spesielt til at helsesektoren er spesielt flinke på dette punktet, da det jo er de som sitter på mest sensitiv data. De kjører en del holdningsskapende arbeid, og informanten viser blant annet til at det fins musematter med påminnelse om sikker bruk av IT. I tillegg fins informasjon på intranett slik at de stadig skal bli minnet på de reglene som fins med tanke på sikkerhet.

Informant fra kommune A nevner at mye av deres sikkerhetsarbeid går på bevisstgjøring og opplæring av ansatte, og viser til et eksempel med bruk av passord:

> ”Det har jo siden tidens morgen vært sånn at [om] lager du et passord sjøl, blir det ikke nødvendigvis godt, og får du oppgitt et passord av andre som kanskje er godt, teknisk godt, har det en tendens til å bli skrevet på en gul lapp som blir lagt under tastaturet.”

Informant i kommune B forteller at den største sikkerhetsmessige utfordringen dreier seg om brukerholdninger. De har 9000 ansatte i en bedrift som har tilgang til ulike sensitive systemer; man må derfor sørge for at de ansatte oppfører seg på en forsvarlig måte. Informanten viser til at man tidligere ofte fant gule lapper med brukernavn, passord og diverse annet. Dette endret seg fordi regimet endret seg.

Informant fra kommune B sier følgende, noe da også informanten fra kommune A snakket om:

> ”Hvis du går rent teoretisk på sikkerheten, så hvor mer kompleks og hvor fortere du skifter det, jo bedre er det. Men i praksis er det ikke sånn. I praksis må du gjøre passordene sånn at de kan lage sekvenser slik at de kan huske de. Så du å må ikke være for strikt på reglene. Dessuten må du også la passordene leve litt lenger enn hva teorien sier. For du må ikke skifte for ofte. Da forsvinner de gule lappene…”

Når det kommer til interne trusler, forteller informanten at avviksrapporteringen benyttes generelt. Når brukere for eksempel får tilgang til systemer de ikke skal ha tilgang til, skal dette rapporteres. Som en del av kvalitetssystemet i kommunene er de pliktet til å føre avviksrapportering av hva de oppfatter som feil. Helse og omsorgssektoren er spesielt flink på dette området, kan informanten i kommune A berette. Brukere i kommunene har også et ansvar hvis de oppdager uregelmessigheter i datasystemer. En del av dette fanges opp gjennom dette kvalitetssystemet, men informanten betoner at de ønsker å bli flinkere på dette området: ”Sånn som jeg ser det, er det en av de viktigste måtene å jobbe internt, med interne trusler (…).”

For hvert system kommune A benytter seg av, har de en egen systemansvarlig. Vedkommende har her opplæringsansvar for brukere av systemet. IT-sjefen forteller at han er veldig klar på at når de anskaffer et nytt system, så må de sørge for de nødvendige kurs. Dette er, ifølge ham, en veldig liten del av totalkostnadene, og er absolutt ikke noe som bør spares på.

Dette eksempelet vil drøftes med tanke på uforutsett interaksjon mellom brukeres adferd og organisasjonens reglement for bruk av IT. Opplæring av systemets brukere står sentralt i HRO-teorien, og vil derfor også drøftes.

4.3 Ansvar for IKT-systemer

På spørsmål om det er blitt benyttet mye *outsourcing*, forteller begge kommune-informantene at de drifter og vedlikeholder det meste av sine egne systemer. Begge viser til ta deres informasjonside på Internett blir driftet av et eksternt selskap, men at de selv er ansvarlige for å vedlikeholde informasjonen.

For de systemene de selv drifter, har de respektive systemene egen systemansvarlig. Disse har ansvar for blant annet å ha kontakt med leverandører og for å få informasjon om nye utgaver av deres løsninger. Dette videreformidles til IT-avdelingen, hvor de får beskjed om nye oppdateringer og hvordan de vil ha det installert.

4.4 Anbud

På spørsmål om hvilke krav de stiller under anbud til systemer som behandler sensitive opplysninger, forteller kommune B at de ikke er så mye inne på den tekniske sikkerheten i produktene de kjøper. De bygger den tekniske sikkerheten rundt de produktene de velger. Når det kommer til sikkerhetskrav hos programleverandører, viser de til de gjeldene lover og regler. De krever at produktene de kjøper er utprøvd og selvsagt at sikkerheten er godt gjennomtenkt, men stiller ikke krav til at ting må løses på den ene eller andre måten. Informanten forteller videre:

> ”Men for å si det sånn, hvis du er en aktør som leverer pasientjournal-system, og ikke har bakt inn sikkerhet i produktet, så er du ikke en aktør på det markedet. Det er store leverandører som leverer til sykehus.”

4.5 Tekniske løsninger – nettverksstruktur og teknologivalg

Informant i kommune A viser til en situasjon hvor de møtte på en begrensning i infrastrukturen som førte til at systemene ikke var tilgjengelig for noen skoler. Feilen lå i at maskinene på disse skolene ikke fikk tildelt IP-adresser og ikke kunne komme seg på kommunens nettverk. De påpeker at de som mange andre kommuner har begrenset økonomi og at de ikke skifter ut utstyr før det må skiftes ut. Etter mye brainstorming fant de ut at problemet lå i en eldre brannmur hvor aksesstabellene var fulle, og kunne derfor ikke tildele IP-adresser til klientene.

Dette er et av eksemplene som viser til en form for kompleksitet hvor eldre utstyr ikke lenger klarer å holde tritt med de nye behov.

4.5.1 Virtualisering av nettverk

I begge organisasjoner var det benyttet seg av virtualiseringsteknologi. Denne type teknologi ble benyttet på grunn av økonomiske og driftsmessige årsaker. Denne teknologien blir benyttet som virtualisering av nettverk og informasjonstjenere.

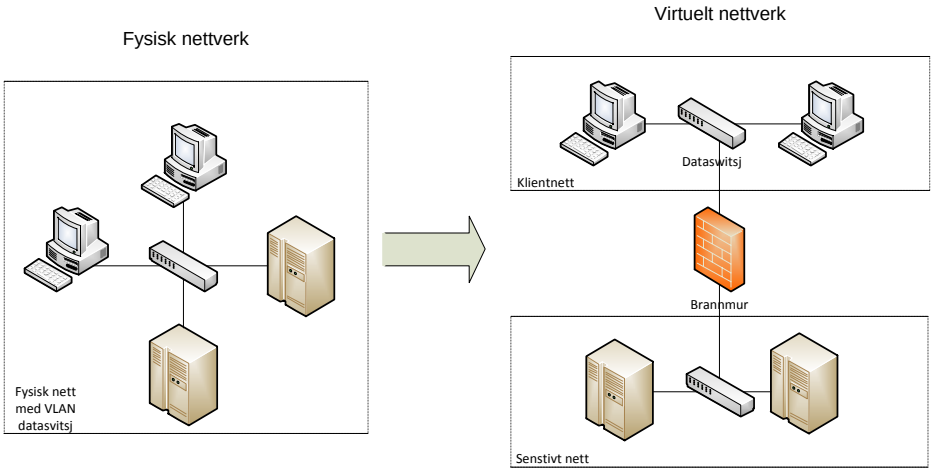
I kommunene som ble undersøkt, var separering av nettverkssoner blitt benyttet. Det kom frem at det var to ulike soner. Klientnettet hvor brukere fritt kunne koble seg til uten noen form for tilgangskontroll, og et sensitivt nett brukere må koble seg på gjennom terminalløsninger.

Tidligere var disse to sonene fysisk separert, hvor det var egne kabler for hver av disse sonene. Dette er nå blitt byttet ut med virtuelle nettverk hvor sonene blir separert virtuelt. Informant i kommune B forteller:

> "Jeg tror ikke det er en eneste bedrift i dag som ikke kjører sensitiv- og ikke-sensitiv på de samme nettverkskablene."

Tidligere ble ulike nettverkssoner fysisk separert ved kabling, som Figur 6 viser. Dette er i dag blitt byttet ut med virtualiseringsløsninger (VLAN), hvor senstive og åpne systemer er på samme fysiske nettverk, men blir virtuelt separert ved hjelp av virtuelle nettverk. Videre forteller informanten:

> "Vi har troen på at teknologien er sikker nok i forhold til å holde ting adskilt".



Figur 6 – Skille mellom ulike soner ved bruk av virtuelle nettverk

Dette vil bli drøftet i forbindelse med NAT-teorien hvor ulykker i systemer unngås ved å redusere interaksjon.

4.5.2 Virtualisering av tjenere

Tjenerparker hos organisasjonene har benyttet seg av virtualisert maskinvare. Dette gjøres av økonomiske og driftsmessige årsaker. De økonomiske årsakene er at det ikke lenger er nødvendig med dedikert maskinvare for hver tjener som benyttes i virksomheten. Blant de driftsmessige årsakene var muligheten for å flytte virtuelle tjenere over til ny maskinvare ved behov nevnt. Informant i kommune A forteller at han var blitt pålagt av sikkerhetsgruppen å foreta en risikoanalyse over hva som vil skje hvis serverrommet de har, skulle gå i lufta, brenne eller bli ødelagt på et eller annet vis. De har derfor vurdert mulighetene for å kunne speile alle systemene til et nytt bygg i kommunen hvis det skulle skje noe drastisk.

Kommune B forteller at sensitive og ikke-sensitive tjenester benyttet samme maskinvare, men var adskilt virtuelt i begge kommunene som ble undersøkt. Her er det også tillit til at virtualiseringssystemene klarer å holde de sensitive og ikke-sensitive systemene adskilt. Begge anerkjente at dette er en sikkerhetsutfordring. Informanten i kommune B forteller:

”Det betyr at sensitive og ikke-sensitive systemer i større grad skal kobles sammen. Hvis vi ikke har tungen rett i munnen i den prosessen der, og i alle de type prosesser, så kommer man til å gjøre noen blemmer.”

4.5.3 Tynne terminaler

Tynne terminaler er datamaskiner som ikke benytter seg av harddisk. Når en tynn terminal starter opp, henter den operativsystemet fra en sentral tjener. Fra starten hvor kommune A har benyttet seg av datanettverk, forteller informanten at de har benyttet seg av tynne klienter. Dette innebærer at hvis en slik maskin ryker, er ikke harddisk-problematikk involvert. Maskinen inneholder bare konfidensielle data i det øyeblikket skjermbildet er oppe på skjermen.

”Det er egentlig en god måte på å kjøpe seg fri fra den problematikken at en PC kan bli stjålet.”

4.6 Fysisk sikkerhet

Samtlige kommuner viser til fysisk sikkerhet som en del av den totale sikkerheten for deres IKT-systemer. Kommune A viser til at sist gang det ble ført tilsyn i organisasjonen, var det fysisk sikring de påpekte. Kommune B viser til at studenten, altså undertegnede, måtte gjennom flere tilgangskontroller før han kom inn i IT-avdelingen, og at det fremdeles var en vei å gå for å komme til serverrommet.

“ (...) det med fysisk sikkerhet taes på alvor, og vi har jo ingen servere som er distributert ut på lokasjoner. Alt er sentralisert, og det er bare noen få folk som har adgang til det aller helligste.”

4.7 Håndtering av systemlogger

Ved spørsmål om hva slags kapasitet de hadde til å gå gjennom systemlogger som blir generert av de forskjellige maskinene, kommer de frem at det ikke er kapasitet til å gjennomgå alle systemloggene som ble generert.

De systemene som ble daglig overvåket, var brannmur og innbruddsdeteksjonssystemer. Disse ble benyttet for å oppdage angrep fra utsiden mot interne systemer.

I begge kommunene var det også benyttet seg av stikkprøver på de mer sensitive systemene for å undersøke om det har forekommet uønskede hendelser. Disse stikkprøvene forekommer oftest når det er mistanke om at noe er galt. Kommune A forteller at de oppbevarer systemloggene såpass lenge at de kan benyttes som bevis hvis det noe skulle bli oppdaget i etterkant. "Vi har brukt logger for å finne ut ting som vi har trengt å finne en forklaring på", forteller han.

Det er også blitt vurdert å benytte seg av eksterne selskaper som gjennomgår disse systemloggene, og det er blitt vurdert å benytte seg av programvare som kan automatisere denne oppgaven.

5 Drøfting

I dette kapittelet vil vi drøfte empirien mot valgte teorier.

5.1 Systemegenskaper

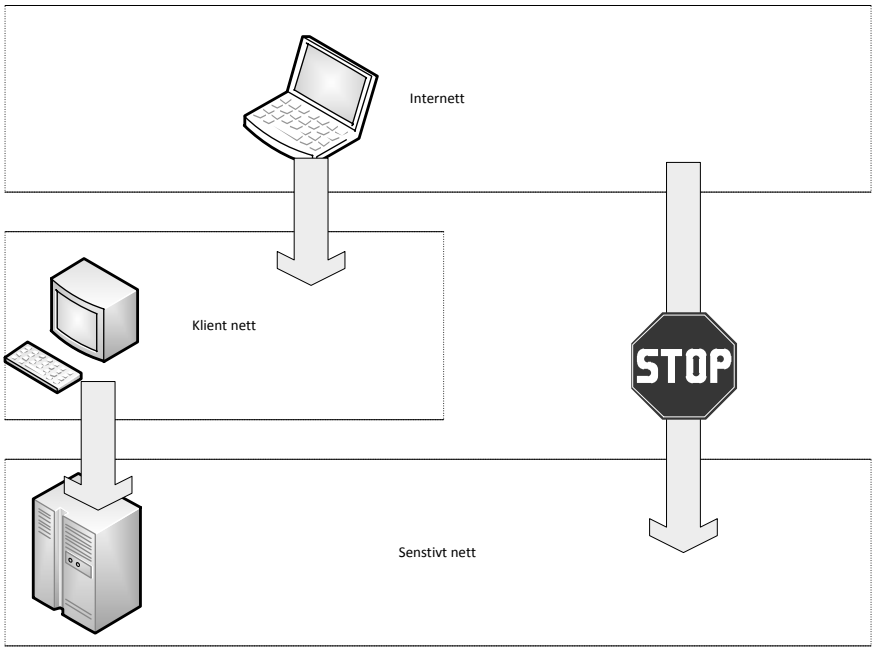
5.1.1 Tiltak som er ment for å redusere kompleksitet

I kapittel 3.2 ble Natural Accidents Theory beskrevet, hvor årsaken til ulykker i komplekse systemer er kompleksiteten i seg selv. Komplekse systemer har den egenskap at det vil oppstå uforutsette interaksjoner eller uhåndterte interaksjoner, da man aldri vil kunne få en total oversikt over alle de ulike tilstandene de ulike systemkompontener, kan ha. Dette gjelder spesielt i IKT-systemer, hvor systemets innkjøper verken har tilgang eller resurser til å få en fullstendig innsikt i systemets virkemåte.

5.1.1.1 Nettverk

Det kontinuerlige kappløpet viser at IKT-systemer stadig blir mer komplekse (Forskningsrådet 2008). Ved å redusere kompleksiteten i IKT-systemer vil man ifølge NAT kunne hindre at datainnbrudd forekommer som følge av mulighet til å interaktere med andre systemkomponenter, og vil derfor kunne gjøre et system mindre sårbart for systemulykker. Ifølge ulykkesdefinisjonen i kapittel 1.4.3 og 3.6.2 betrakter vi ikke feil i enkeltkomponenter som systemulykker, og hendelsen vil være isolert til en enkeltkomponent. De tiltakene som ble observert hos de undersøkte organisasjonene, var blant annet sone-inndelingen i nettverk. Dette var tiltak som satt klare begrensninger på hvilke systemkomponenter som kunne interaktere med andre. Spesielt var det satt et skille mellom det adminsitrative nettet hvor klientene hadde tilgang, og det sensitive nettet hvor sensitive systemer som pasientjournaler og lignende befant seg. Illustrasjonen i Figur 7 viser til at det kun er klienter som befinner seg i den administrative sonen, som har tilgang til

sensitive systemer. Interaksjon fra systemer utenfor denne sonen vil bli blokkert av brannmurene. Tilgang til den sensitive sonen var ytterligere begrenset ved at man bare kan benytte sensitive tjenester ved å logge seg på gjennom terminalløsninger.



Figur 7 - Restriksjoner på kommunikasjon mellom ulike deler av systemet

I kommune A var det benyttet tynne terminaler mot de sensitive systemene. Disse terminalene er diskløse, og innebærer at de ikke inneholder sensitive opplysninger hvis de skulle komme på avveie. Dette kan også sees på som en reduksjon av uforutsett interaksjon hvor systemkomponenter medfører en sikkerhetsrisiko selv etter endt livsløp.

5.1.1.2 Virtualisering

Det kommer frem at begge kommunene benytter seg av virtualiseringsteknologi, blant annet for å separere de sensitive og ikke-sensitive systemene uten å ha behov for to fysiske nettverk. Hvis vi ser tilbake på hvordan dette er blitt gjort tidligere, kan det være tydelig at virtualiseringen er blitt gjort med tanke på økonomi, hvor man ikke lenger benytter seg av dedikert maskinvare og kabling for å drifte to separate soner. Kommune B viser også til at

det tidligere var tilstrekkelig å finne riktig nettverksplugg, for å komme innen den sikre sonen. Ved hjelp av virtualiseringsteknologi skal det ikke være mulig å komme seg inn uten å benytte terminalløsningen.

VLAN Security White Paper fra Cisco går gjennom de fleste tekniske sårbarhetene og har fått et eksternt sikkerhetsfirma til å teste disse mot deres produkter. Konklusjonen deres var at virtuelle nettverk er mer robuste mot sårbarheter enn det som tidligere er antatt, men at de er avhengige av korrekt implementasjon og konfigurasjon for å kunne utføre sitt arbeid sikkert (Cisco Systems 2002). Kommune B sier at virtualising og logisk separering av de ulike sonene er et valg de har gjort. Dette sees på som et tiltak for å redusere kompleksiteten for å kunne utnytte de systemressursene som er tilgjengelige. Informanten sier også at det å forenkle nettverksstrukturen er en måte å forenkle tilgangen på. Dette kan tyde på at kommunen ønsker å redusere kompleksiteten i deres nettverksstruktur, men har valgt en løsning som er avhengig av å være riktig konfigurert for å holde systemet sikkert. På den måten har man byttet ut én form for kompleksitet med en annen hvor det er nødvendig å konfigurere nettverket med korrekte begrensninger og tilgangskontroller. Denne form for systemsikring har en større forankring i STAMP-teorien hvor man oppnår et sikkert system ved å implementere og håndheve sikkerhetsbegrensninger i systemkomponentene.

5.1.2 Systemets koblinger

Når et system er tett koblet, går det kortere tid mellom hendelse og konsekvens. For å gjøre et system sikrere må man iht. NAT bevisst bygge inn buffer slik at operatører får tid til å reagere på hendelser som kan utvikle seg til systemulykker. Imidlertid er dette ikke gjennomførbart for alle typer systemer. I IKT-systemer er det ofte ønskelig at informasjon blir behandlet umiddelbart, og det er derfor ikke alltid rom for å implementere buffere. I

denne sammenhengen virker det som om redundans er en mer gunstig løsning, selv om NAT presiserer at redundante systemer øker kompleksiteten og derfor kan virke mot sin hensikt.

I kommune A var det snakk om å gjøre hele IT-avdelingens systemer redundante hvor hele systemet skal kunne bli speilet til et annet bygg om det skulle være nødvendig. Dette var et tiltak som kom frem i en risikoanalyse hvor scenarioet innebar fysisk skade på driftslokaler og utstyret som er involvert. Bruk av redundante systemer er et av kjerneprinsippene innen HRO, men i dette tilfelle er redundansen knyttet opp til driftslokaler og maskinvare. Feil i programvare hos det tekniske systemet vil også kunne bli speilet og eksistere i det redundante systemet.

Et annet poeng som kom frem under intervjuet, var at inntrengere utenfor kommunens nettverk må forsere to brannmurer for å kunne trenge inn til se sensitive systemene. Dette er således et eksempel på hvordan et IKT-system kan ha løse koblinger, hvor et sikkerhetsbrudd ikke nødvendigvis vil føre til tap av integritet eller konfidensialitet i sensitive systemer. For at inntrengeren skal kunne komme seg videre inn i systemet må nye sårbarheter kartlegges og utnyttes, noe som vil de systemansvarlige tid til å oppdage og reagere på problemet.

5.1.3 Ansvarsforhold for implementasjon av sikkerhetsbegrensninger

Kommune B viser til at ansvaret for de ulike systemdelene ligger hos den respektive systemansvarlige. Retting av sikkerhetshull og nye funksjoner er blant noe av innholdet i programvareoppdateringer fra leverandører. Det kommer frem i empirien at ansvaret for å tilse at programvareoppdateringene er på plass, ligger på innkjøpere av systemet da det er kommunene som må hente informasjon om dette fra leverandører. Det kan tenkes at flere

leverandører varsler sine kunder om nye oppdateringer, men empirien viser ikke til at dette faktisk er tilfelle.

Dette er et aspekt som strider mot STAMP-teorien, hvor det er nødvendig med en tilbakekoblingssløyfe som skal sørge for at de nødvendige forutsetningene er blitt implementert. Det kommer ikke frem hvorfor dette ikke blir gjort, og et tankekors er hvorvidt dette er et ansvar som burde ligge på leverandøren av programvare. Pasientjournaler ble trukket frem som eksempel på et av disse systemene med krav fra bl.a. personvernslovgivning. Selv om det ikke er en såkalt tilbakekoblingssløyfe (altså en bekreftelse på at sikkerhetsbegrensninger er implementert) mellom produsent og innkjøper som bekrefter at sikkerhetskravene er fulgt, er det mulig at dette fins mellom myndigheter og produsent gjennom etterfølging av pålegg av lover og regler. I kommune A kommer det frem at både IT-sjefen og sikkerhetsansvarlig har rapporteringsplikt til rådmannen. Dette kan tyde på at systemegenskapen for å implementere komponenter riktig i et system ifølge STAMP, er fulgt indirekte lovmessige krav fra myndighetene til slike typer systemer.

På spørsmål om hvordan sikkerhet blir betraktet som en del av anbudsprosessen, kommer det frem at det er visse krav til gjennom gjeldende lover og regler. Det kan tolkes som en tilbakekoblingssløyfe hvor brukere og innkjøpere samt datatilsynet vil reagere hvis produkter som behandler pasientdata, ikke følger disse lovene. Det vises imidlertid ikke til formelle tilbakemeldinger på hvorvidt systemene følger de gitte lovverkene eller ei.

Brukere er pålagt å rapportere hendelser som oppleves som unormale. Eksempelvis viser kommune B til at ansatte er pliktet til å rapportere hendelser gjennom avvikssystemet dersom det oppdages brudd på deres sikkerhetsreglement. Dette det kan se ut som om dette fungerer som en annen type indirekte tilbakekoblingssløyfe, hvor brukere jo faktisk

rapporterer det som ikke synes å være riktig implementert. Ifølge STAMP skal de antagelsene og begrensningene som er utført under implementasjonen, rapporteres tilbake, men i dette tilfelle blir det altså rapportert når det ikke er tilfelle.

5.1.4 Opplæring av brukere

Sentralt i HRO, er at brukere skal kunne utføre riktige valg uten veiledning av overordnede. De skal altså ha tilstrekkelig kunnskap innen IT til å unnlate å foreta usikre handlinger. I kommune A vises det til bruk av kvalitetssystemer for å kunne tilpasse seg de avvikene som blir oppdaget. Kommunen har således en *rapporterende kultur*, som er en de sub-kulturene som utgjør hva som kalles en *sikkerhetskultur* (Reason 1997). Det kommer ikke frem om organisasjonen aktivt søker rapportering, men kommune B kan fortelle om mistanke om underrapportering. Dette kan type på at organisasjonen er av *byråkratisk* type hvor slik avviksrapportering blir tatt imot, men ikke blir aktivt etterspurt. Med hensyn til informasjonssikkerhet og de systemene rundt dette produserer systemene en mengde systemlogger over hendelser som inntreffer. Dette gjør det mulig at organisasjonen ikke er avhengig av rapportering av de tekniske aspektene i et IKT-system, hvor rapporteringen skjer automatisk. Det er da også slik at det er ressurskrevende å tolke disse systemloggene, og kommune A har vurdert å benytte seg av programvare som gjør dette automatisk. Dette innebærer likevel at organisasjonen må benytte seg av ressurser for å gjennomgå rapportene som blir produsert av et slikt system.

Begge kommunene viser til bruk av eksterne spesialister for å dekke de kompetanseområdene de selv enten ikke har ressurser til dekke, og viser ikke til kompetanseheving på disse områdene. Da årsaken til bruk av spesialkompetanse har røtter i

ressursmangel og berører daglig drift, gjør det vanskelig å belyse dette gjennom bruk av HRO-teori.

Ved ansettelse må brukere signere avtaledokumenter som avklarer hvilke spilleregler de har å forholde seg til med tanke på sikker bruk av IKT-systemer. Iht. STAMP kan dette tolkes som en del av kontroll-sløyfen hvor det blir satt sikkerhetsmessige begrensninger på brukeres handlingsrom. Da dette er en myk barriere, kan denne begrensningen ikke håndheves med mindre det er satt en hard barriere som hindrer de handlingene som er sett på som uønsket.

5.2 Systemteorier

I dette delkapittelet blir det oppsummert hvordan de ulike funnene presentert ovenfor forholder seg til systemteoriene presentert i teorikapittelet.

5.2.1 NAT

Flere av de tiltakene som er ment for å forenkle de driftsmessige konspetene, har ført til mer komplekse systemer. Bruk av virtualiseringsteknologi, både for nettverk og på tjenerparker, kan ha bidratt til å øke kompleksiteten. Dette annerkjenner informanten i kommune A idet han forteller at det er blitt mer utfordrene å feilsøke da det fins så mange mulige feilkilder. Organisasjonenes nettverk har gått fra å være fysisk adskilt til å bli virtuelt adskilt, noe som har ført til driftsmessige konsekvenser hvor man må være bevist på hvordan man skiller sensitive systemer fra de mer åpne nettverkene. Teorien viser det er kompleksiteten i seg selv som er problemet (Perrow 1999). De løsningene som er blitt valgt, har altså gjort problemene større idet de ble mer komplekse.

5.2.2 STAMP

I kapittel 5.2.1 ovenfor kommer det altså frem at virtualisering av nettverk kan føre til ytterligere kompleksitet. Dette er ofte gjort for å gjøre hverdagene til driftsansvarlige enklere. En konsekvens av dette kan imidlertid være at systemet da blir mer sårbart overfor uforutsette interaksjoner. STAMP-teorien har derimot en forklaring på hvordan dette problemet kan håndteres selv i et ikke-reduserbart komplekst system, hvor problematikken ligger i at systemets komponenter må ha gitte begrensninger på hvordan de kan interaktere med resten av systemet.

Årsaken til systemulykker ligger i mangel på kontroll og håndhevelse av de sikkerhetsmessige begrensninger. Dette kommer frem i eksempelet som dreier seg om virtualisering av nettverk hos organisasjonene. De har valgt å benytte seg av teknologi som krever ytterligere begrensninger, og er avhengig av korrekt konfigurasjon for å operere på en sikker måte. Det er derfor her nødvendig med de korrekte sikkerhetsbegrensningene for å unngå interaksjon mellom sensitive og ikke-sensitive systemer som opptrer på uønskede måter.

Videre så vi på et eksempel på hvor STAMP blir anvendt som en myk barriere i form av avtaledokumenter for sikker bruk av IT. Dette er da ment som en begrensning på hva som er tillatt av handlinger mot et IKT-system. I dette tilfellet ble det ikke foretatt noen direkte kontroll/håndhevelse av at disse begrensningene faktisk blir utført.

5.2.3 HRO

Samtidig som virtualiseringsteknologi har medført at IKT-systemer er blitt mer komplekse, er de også blitt mer fleksible i den forstand at det er mulig å endre konfigurasjonen til en infrastruktur etter organisasjonens behov. Da HRO er ment for å beskrive de egenskapene en organisasjon har for å vellykket kunne betjene komplekse systemer, må IKT-systemet

også sees på som en del av organisasjonen og som et hjelpemiddel som tillater organisasjonen å opptre mer fleksibelt. For å kunne tilpasse seg utfordringene organisasjonen står ovenfor, er det viktig å ta lærdom fra tidligere hendelser. Det kom frem at det var dannet egne grupper for å ta valg innenfor rammene av sikkerhetsproblematikk. Dette kan tolkes dithen at de er istand til å ta avgjørelser på et kollektivt grunnlag med det ønskede resultat at det fører til en bredere systemforståelse.

Gjennom begge kommunenes kvalitetssystem er det tilrettelagt for en rapporterende kultur, men det vises ikke i empirien til funn som kan indikere på at de faktorene for å ivarta en vellykket rapporteringskultur er tilstede. Dette kan imidlertid skyldes valg av intervjumetode, da jo dette ikke var var et spesifikt tema, eller spesifikt spørsmål i intervjusituasjonen.

6 Konklusjon

Denne undersøkelsen har hatt som målsetning å utforske hvilke tilnærminger av systemteori som passer best for styre sikkerheten i IKT-systemer. For å oppnå en forståelse av dette har det vært nødvendig å betrakte hvilke systemspesifikke egenskaper et IKT-system har med tanke på det som er blitt definert som en ulykke i et IKT-system.

For å tilfredsstille ulykkesdefinsjonen iht. den valgte systemmodellen, er *informasjonssikkerhet* blitt sett på sett på det overordnende systemet med *tilgjengelighet*, *konfidensialitet* og *integritet* som de underornede systemene.

Tre teorier er blitt benyttet for å beskrive to organisasjoners IKT-systemer. To av disse, henholdsvis *Natural Accidents* og *Theory Systems Theory Accident Model and Processes*, har fokusert på de spesifikke systemegenskapene som beskriver hvorfor ulykker forekommer i komplekse systemer samt hvilke tiltak som bør benyttes for å hindre ulykker.

HRO-teorien har bidratt med å undersøke hvilke organistoriske faktorer som må være tilstede i organisasjoner som gjennom empiri har vist seg å kunne håndtere komplekse systemer over lang tid uten katastrofale ulykker.

Flere av løsningene som er blitt benyttet av organisasjonene undersøkt i denne oppgaven, er blitt valgt for å tilfredsstille andre hensyn enn de sikkerhetsmessige. Ved å ta i bruk *Natural Accidents The*ory har vi sett hvordan forenkling av tiltak kan føre til økt kompleksitet. Dette innebærer at systemene vil opptre mer uhåndterlig grunnet økt mulighet for uforutsett interaksjon.

Systems Theory Accident Model and Processes åpner for løsninger hvor man kan sette inn tiltak for å forhindre ulykker i komplekse systemer ved å implementere nødvendige

sikkerhetsmessige begrensninger. Det ble funnet tilnærminger på bruk av denne teorien blant annet i sikkerhetskrav til sensitive løsninger og i bevisstgjøring av brukeres holdninger gjennom reglement.

7 Referanser

Cheminod, M., I. C. Bertolotti, et al. (2009). "Detecting Chains of Vulnerabilities in Industrial Networks." Ieee Transactions on Industrial Informatics: 181-193.

Cisco Systems, I. (2002). "VLAN Security White Paper." fra http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/vlnwp_wp.pdf. Sist oppdatert: 2002. Benyttet: 07.07.2011

Forskningsrådet (2008) IKT-sikkerhet: Det kontinuerlige kappløpet.

Hanseth, O. and C. Ciborra (2007). Risk, complexity and ICT. Cheltenham, Edward Elgar.

Jacobsen, D. I. (2005). Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode. Kristiansand, Høyskoleforlaget.

Jones, A., G. L. Kovacich, et al. (2002). Global information warfare: How businesses, governments, and others achieve objectives and attain competitive advantages. Boca Raton, Auerbach Publications.

Lacey, D. (2009). Managing the human factor in information security: How to win over staff and influence business managers. Chichester, John Wiley & Sons.

Leveson, N. G. (2011). "Applying systems thinking to analyze and learn from events." Safety Science 49: 55-64

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

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

Sivertsen, T. K. (2007). "Risikoanalyse av samfunnskritiske IKT-systemer."

Vinje, F.-E. (2006). "Når sikkerhet er viktigst."

http://www.regjeringen.no/nb/dep/jd/dok/nouer/2006/nou-2006-6/22.html?id=157694.

Sist oppdatert: 2006. Benyttet: 15.06.2011

8 Figurer