Er det behov for nytenkning og utvikling av nye risikoanalysemetoder for å håndtere risiko i det moderne informasjonssamfunn?

Risikostyring og sikkerhetsledelse

UiS Pluss

Forfatter: Tore Hartvigsen

14.10.2013

UNIVERSITETET I STAVANGER

MASTERGRADSTUDIUM I
RISIKOSTYRING OG SIKKERHETSLEDELSE

MASTEROPPGAVE

SEMESTER: Høst 2013

FORFATTER: Tore Hartvigsen

VEILEDER: Roger Flage

TITTEL PÅ MASTEROPPGAVE:

Er det behov for nytenkning og utvikling av nye risikoanalysemetoder for å håndtere risiko i det moderne informasjonssamfunn?

EMNEORD/STIKKORD:

Risiko, risikostyring, risikoanalyser, analysemetoder, informasjonssystemer, IT, sikkerhet, ulykkesperspektiver, høypålitelige organisasjoner, HRO.

SIDETALL: 104

STAVANGER 14.10.2013

DATO/ÅR

FORORD

I det erfaringsbaserte studie *Master i risikostyring og sikkerhetsledelse* ved Universitetet i Stavanger (UiS) har de forskjellige teoretiske perspektivene på hvorfor ulykker skjer, samt hva som gjør enkelte organisasjoner mer robuste enn andre, vært et sentralt tema. Etter å ha jobbet med informasjonssystemer i mange år, både i olje- og gassindustrien, det offentlige og i Forsvaret, har den nye kunnskapen om ulykkesperspektivene vært en inspirasjon til en spennende ny måte å betrakte ulykker som kan skje med informasjonssystemer på. I arbeidet med sikkerhet i informasjonssystemer har fokus i stor grad vært på teknologiske aspekter. Ulykkesperspektivene fokuserer i like stor grad på menneskelige og organisasjonsmessige forhold. Samspillet mellom mennesker, teknologi og organisasjon skaper muligheter, men også nye trusler. Større ulykker skjer oftest plutselig og uvarslet og de skjer sjeldent. Min mening er at ulykkesperspektivene vil kunne tilføre kunnskap og perspektiv som kan være til hjelp for å forstå, analysere og styre risiko også med informasjonssystemer. Dette er bakgrunnen for valg av tema for denne masteroppgaven.

Studiet ved UiS har vært en berikelse både personlig og faglig. Jeg er takknemlig for at min arbeidsgiver, Det Norske Veritas, har gitt meg denne muligheten. Jeg er også stor takk skyldig til min veileder ved UiS, Roger Flage, for kritiske, positive og svært lærerike tilbakemeldinger under arbeidet med oppgaven. Ikke minst vil jeg takke min familie for tålmodigheten de har vist og for at jeg har fått bruke så mye av vår felles tid på dette prosjektet.

Tore Hartvigsen

Høvik 14.10.2013

SAMMENDRAG

Metoder for risikoanalyse har lenge blitt benyttet i organisasjoner med store komplekse systemer innen bransjer som atomkraft, fly- og romfart, forsvar, olje- og gass og offentlig virksomhet. Informasjonssystemer har blitt betraktet som integrert i slike systemer og blitt analysert som en del av disse. De siste tyve årene, spesielt etter introduksjon av Internett, har det skjedd en endring av informasjonssystemenes rolle i mange bransjer. For mange organisasjoner er nå informasjons-systemene blitt de viktigste. I tillegg har informasjonssystemer blitt en sentral og viktig ingrediens i mange menneskers privatliv. Det har manglet en bred diskusjon hvor risiko med informasjonssystemer har vært i fokus. I oppgaven diskuteres det om de eksisterende risikoanalyse-metoder er anvendelige også for informasjonssystemer, om det er spesielle egenskaper ved informasjonssystemer som gjør at det er behov for nytenkning og hva slags risikoanalysemetoder det i så fall er behov for.

De mest kjente teoretiske perspektivene på hvorfor ulykker skjer gir oss et grunnlag for å avlede typiske karakteristikker på ulykker som også vil kunne skje i informasjonssystemer. Energi-/barriereperspektivet gir oss at feil og mangler som ligger latente i systemet kan bli utløst dersom tilstrekkelige barrierer ikke er etablert. Informasjonsprosesseringsperspektivet gir oss at ulykker kan skje når eksisterende informasjon ikke blir gjort kjent for de som har bruk for den, eller når informasjon ikke blir kommunisert på en effektiv måte. I henhold til Normal ulykkesperspektivet må en forvente, og være forberedt på å håndtere ulykker i kompliserte systemer. Jo mer komplekst systemet er, desto mindre oversikt har en, og jo større grunn er det til å forvente at en ulykke vil kunne skje. Hensiktsmessig organisasjonsform må velges for å være best mulig forberedt på å håndtere hendelser som kan inntreffe. Høypålitelig organisasjon-perspektivet gir oss at bedrifter som praktiserer en stor grad av årvåkenhet, er mindre utsatt for ulykker enn de som ikke gjør det. Forebygging av ulykker kan skje gjennom å utvikle en velfungerende organisasjon. Målkonflikt-perspektivet forteller oss at ulykker skjer når en organisasjon ikke prioriterer ferdigstillelse, verifisering, sikkerhet og robusthet i forhold til andre mål. Fra perspektivet om Menneskelige faktorer avleder vi at ulykker kan skyldes enten bevisste villede handlinger, eller handlinger som for eksempel skyldes manglende prosedyrer eller enkeltpersoners etterlevelse av disse.

De mest vanlige metodene for risikoanalyse blir diskutert og funnet egnet til analyse også av informasjonssystemer. Metodene CORAS og VAM er spesielt utviklet for analyse av risiko i informasjonssystemer og blir funnet å kunne ha stor anvendelighet. Noen metoder fra data-

kvalitetsområdet blir vurdert og funnet å kunne være hjelpemidler både til risikoidentifikasjon og som barrierer, så lenge det finnes representative data som kan undersøkes.

Oppbyggingen av et informasjonssystem hvor det finnes etterprøvbare krav eller regler som spesifiserer hvordan systemet skal fungere, er ikke ulikt andre komplekse systemer. Dette gjelder både for det som i oppgaven betegnes som strukturerte informasjonssystemer og for referansebaserte (semantisk) strukturerte informasjonssystemer. For ustrukturert informasjon, som utgjør den aller vesentligste del av informasjonsmengden i det moderne informasjonssamfunn, er situasjonene ikke den samme. Her finnes ikke regler som kan etterprøves eller strukturer som kan følges, og man må se på andre metoder. Såkalt *mining* etter gjenkjennbare mønstre i store informasjonsmengder blir foreslått som en metode som med fordel kan videreutvikles og anvendes i større grad i risikoanalysesammenheng.

Informasjonssystemets rolle i et utvalg større ulykker er analysert og beskrevet i oppgaven. For å få bredde i diskusjonene er eksemplene hentet fra romfart (Ariane 5, Mars Climate Orbiter), fra olje- og gassbransjen (Deepwater Horizon, Sleipner-A), fra politi og etterretning (9/11 i USA, og 22/7 i Oslo og på Utøya), fra finans (Barings Bank kollapsen) og fra helsevesenet (tilfellet «David»). Eksemplene blir relatert til ulykkesperspektivene, for så å bli diskutert i forhold til analyse-metodene. Basert på denne diskusjonen foreslås et rammeverk for styring og analyse av risiko i informasjonssystemer. Konklusjonen er at mange av de store ulykkene hvor informasjonssystemer har vært sentrale, ikke skyldes mangel på eller mangler i analysemetoder, men at risikoanalyser ikke har blitt tilstrekkelig gjennomført eller ikke er gjennomført i det hele tatt. I gjennomgangen av eksemplene er det ikke i noen av dem identifisert beskrivelse av utførte risikoanalyser.

Ved å trekke lærdom fra ulykkesperspektivene og de erfaringer og den tenkning som ligger bak perspektivene, kan kunnskap om hvordan informasjonssystemer kan gjøres mer robuste avledes. Det er behov for å tenke nytt og se på nye metoder for risikoanalyse i lys av menneskelige og organisasjonsmessige sider. Et utgangspunkt kan være å se risikoanalyse i sammenheng med etablerte metoder og teknikker fra blant annet kvalitetsstyringsområdet.

Generelt gjelder at forhold som har med samspillet mellom mennesker, teknologi og organisasjon (MTO) å gjøre, er viktige for å oppnå robuste informasjonssystemer. Det kreves en velfungerende organisasjon som tar de riktige beslutningene og gjør de riktige prioriteringene. Formålet med risikoanalysen er å bidra med et beslutningsgrunnlag slik at dette blir oppnåelig.

INNHOLDSFORTEGNELSE

FIGURLISTE

TABELLISTE

INNLEDNING OG PROBLEMBESKRIVELSE

1.1 BAKGRUNN

Det moderne informasjonssamfunnet er i en rivende utvikling. Mengden informasjon som lagres elektronisk fordobles hver 40. måned (Datatilsynet og Teknologirådet 2013). Internett er allemannseie og har fått en enorm utbredelse. Utviklingen av Internett er ikke sentralt styrt. Det stilles spørsmål om feiltoleranse, pålitelighet og konsekvenser dersom en hendelse skulle skje i nettet som rammer en sentral del (ENISA 2011). Ny teknologi skaper nye muligheter men introduserer også nye farer. Risiko handler om hendelser og konsekvenser, og tilhørende usikkerhet. Hendelser kan også ha positive konsekvenser. Årsaker til hendelser i informasjonssystemer kan være mangler og defekter eller manglende eller utilsiktet bruk av tilgjengelig informasjon. Risiko-analysen skal identifisere de initierende hendelsene og få frem årsaks- og konsekvensbildet.

I dag er det ikke noe alternativ for en organisasjon ikke å ta informasjonssystemer i bruk i stor grad. Bill Gates, Microsofts grunnlegger sier at (Gates 1999 s.1-2):

> *«How you gather, manage and use information will determine whether you win or lose. The best way to put distance between you and the crowd is to do an excellent job with information».*

En kan trekke paralleller til de endringer som skjedde i samfunnet da elektrisiteten og senere telefonen ble allemannseie. De organisasjoner som raskest tok teknologien i bruk var de som fikk forretningsmessige fordeler mens organisasjoner som ikke forsto eller sent tok i bruk de nye muligheter, ble borte. Gates (1999 s.37) sier:

> *«The Internet is enabling a new way of life that I call «the web lifestyle». The Web lifestyle, like the electricity lifestyle, will be characterized by new things happening quickly. The infrastructure for high-speed communication is producing new software and hardware that will change people's lives».*

Hele 80 % av den norske befolkning er nå medlem av et sosialt nettverk hvor Facebook er det desidert største. 79 % av alle kvinner og 72 % av alle menn er medlem. Det er nå omtrent 800 millioner medlemmer av Facebook i hele verden. Det har blitt vanlig at folk i alle aldre deler feriebilder og bursdagshilsener med venner og «ukjente» på nettsamfunnet, eller «sjekker inn» for å vise hvor de befinner seg akkurat nå. Seks av ti deler innhold som kommentarer, lenker, bilder og filmer på sosiale nettsamfunn ukentlig (Datatilsynet og Teknologirådet 2013).

Mengden informasjon som skapes i det moderne informasjonssamfunnet er akselererende. Datatilsynet og Teknologirådet (2013) referer til Mark Zuckerberg, Facebooks grunnlegger, som i 2007 spådde at informasjonsmengden ville fordoble seg hvert år i fremtiden. I 2012 ble det produsert 2,5 kvintillioner bytes data (det er 18 nuller) på Internett. Hele 90 % av alt innhold på Internett har blitt produsert de siste to årene. Muligheten for å samle inn, lagre og kommunisere informasjon blir stadig bedre. Det samme gjelder muligheter for å kombinere informasjon på

forskjellige måter. Et sosialt medium er også et informasjonssystem. Pressen skriver ofte om nettmobbing, identitetstyveri, misbruk av personlig informasjon som rammer enkeltindivider. Skoleopptøyene i Gøteborg like før jul 2012, er et eksempel på hvilke konsekvenser en handling som sannsynligvis var ment som en uskyldig spøk skapte nær sagt lynsjestemning. Den jenta som ble beskyldt for å ha lagt ut bildene på bildedelingssystemet Instagram og som ble truet på livet, viste seg senere å være uskyldig. En 15 år gammel jente blir nå beskyldt for å ha lagt ut bildene. Den jenta som først ble beskyldt for publiseringen ble tvunget til å flytte, de som fikk bilder av seg publisert må leve med at disse bildene aldri blir borte. 15 åringen som forårsaket det hele må leve med en politisak hengende ved seg hele livet (Lang 2013).

Opplysninger om vårt bevegelsesmønster forteller mye om oss. Slike opplysninger er attraktive for mange ulike aktører. På den ene siden kan det være organisasjoner som ønsker å selge oss en tjeneste eller å forbedre sitt produkt. På den andre siden kan det være myndighetene som ønsker tilgang til slike data for å kontrollere at vi ikke bryter loven eller misbruker felles samfunnsgoder. Det kan gi grunn til bekymring at mer omfattende lagring av elektroniske spor bidrar til at bevisbyrden ovenfor myndighetene på sett og vis snur. Siden sporene allerede ligger der, blir det den registrerte som må sannsynliggjøre sin uskyld (Datatilsynet og Teknologirådet 2013).

1.2 EKSEMPLER PÅ RISIKO I INFORMASJONSSYSTEMER

For å belyse hva som menes med risiko i informasjonssystemer i denne oppgaven, gjengis det i dette avsnitt kort eksempler på ulykker hvor informasjon eller informasjonssystemer har hatt en sentral rolle. Noen av eksemplene vil bli grundigere beskrevet og analysert i empiri delen av oppgaven (kapittel 4).

- På den storpolitiske arena har det inntruffet hendelser hvor feil informasjon eller manglende informasjon har vært en vesentlig faktor. 26.9.1983 melder den russiske spionsatellitten *Kosmos 1382* at en rakett er skutt ut fra en amerikansk atombase. Informasjonssystemene slår alarm og melder at om 25 minutter vil raketten slå ned i Sovjetunionen. Like etterpå melder samme satellitt at flere andre raketter er på vei. Kun logisk resonnement av ansvarshavende offiser, Stanislav Jevgrafovitsj Petrov, avverger en atomkrig. Han skjønner at informasjonen fra satellitten må være feil og iverksetter derfor ikke prosedyren som ville ha startet et gjengjeldelsesoppdrag mot USA. Ingen vet hvor mange liv en atomkrig i september 1983 ville ha kostet. Anslag går ut på 750 millioner døde. Store deler av den nordlige halvkule ville ha blitt liggende i en kjernefysisk ruinhaug. Eksemplet viser hvordan menneskelig dømmekraft var den endelige barrieren som hindret en uendelig stor katastrofe. Petrov blir i dag feiret som en

helt både i vesten og i Russland. Feilen var sannsynligvis at informasjonssystemene hadde tolket sollys som ble reflektert fra skyer, til å være atomraketter (Tjønn 2013).

- 8.5.1999, under krigen i Bosnia, bombet NATO den kinesiske ambassaden i Beograd på grunn av feil i NATOs databaser og kart (Al-Hakim 2007).
- Etter terroristangrepene på Twin Towers og Pentagon i USA 11.9.2001 påpekte den såkalte 9/11-kommisjonen at en rekke terroristadvarsler var blitt ignorert og tilgjengelig kollektiv informasjon ikke hadde blitt kommunisert og delt (Al-Hakim 2007).
- 22. juli-kommisjonen i Norge kritiserer politiets manglende bruk av informasjonsteknologi og tilgjengelig informasjon etter hendelsene i Oslo og på Utøya 22.7.2011. Politiets sikkerhets-tjeneste hadde begrensede muligheter til å søke i egne informasjonssystemer, viktig informasjon om gjerningsmannens bilnummer nådde ikke ut i tide og politipatruljene kunne ikke motta tekst, bilder eller kartopplysninger. Norsk politi må, i følge kommisjonen, begynne å utnytte potensialet i informasjons- og kommunikasjonsteknologien bedre (NOU 2012).
- Finansbransjen er den bransjen som kanskje har utnyttet informasjonsteknologien best. Også her har det skjedd ulykker. Selskapet Mizuho Securities la ut 610,000 aksjer til salgs for 1 yen per aksje. Selskapet hadde tenkt å selge 1 aksje for 610,000 yen. På grunn av dette fikk selskapet et tap på 21,6 USD Milliarder (Al-Hakim 2007).
- Reason (1997) beskriver hvordan den 203 år gamle engelske Barings Bank, den lengst eksisterende forretningsbanken i *City of London* (etablert i 1792), kollapset etter at en illojal medarbeider, Nick Leeson, manipulerte bankens informasjonssystemer for å kunne gjøre egne disposisjoner med bankens penger. Leeson fabrikkerte falske interne rapporter for å skjule sin virksomhet. Leesons virksomhet pågikk i flere år uten å bli oppdaget. Først etter at han tapte enorme pengesummer ble virksomheten oppdaget av en intern revisjon i selskapet.
- NASA sin Mars Climate Orbiter forsvant 11.12.1998 da den skulle lande på planeten Mars. Det viste seg at man hadde brukt både metriske og engelske måleenheter i parallell under utviklingen av romfartøyet uten at dette var blitt oppdaget (NASA 1999).
- Det europeiske romfartøyet Ariane 5 eksploderte 39 sekunder etter utskytning 4.6.1996. Undersøkelseskommisjonen konkluderte med at feilen skyldtes en feil i romfartøyets *Flight Control System* etter at en gammel programvaremodul var integrert med nyutviklet programvare uten at totalløsningen var testet godt nok (ESA 1996).
- Sleipner-A-ulykken, hvor hele betongunderstellet gikk i stykker under trykktesting i Gandsfjorden, skyldes designfeil ved at kraftpåvirkninger ble underestimert. Dette førte igjen til beregninger og konstruksjon av for svak støttestruktur. Beregningene var gjort med informasjonssystemer som man tidligere hadde benyttet for en rekke tilsvarende konstruksjoner av betongunderstell. Det viste seg å ikke være feil i informasjonssystemene men i

beregningene som var gjort. Resultatene fra beregningene ble ikke kvalitetssikret godt nok (Jakobsen 1994).

- Også innenfor helsebransjen har det skjedd alvorlige ulykker som kan relateres til feil bruk av informasjonssystemer. Informasjon om to kvinner med samme fornavn og samme diagnose (brystkreft) ble forbyttet på et sykehus. Den ene kvinnen døde etter 9 måneder (Al-Hakim 2007).
- *«David» dør av kreft etter datafeil* var overskriften på en artikkel i Aftenposten 11.3.2013. En feil i systemet som administrerte henvisninger til undersøkelse, gjorde at pasienter som ble feilregistrert ble «glemt» i systemet. I det omtalte tilfellet utviklet kreftsykdommen seg til å bli dødelig på grunn av manglende oppfølging fra helsevesenet (Vedeler og Eggesvik 2013).
- Av mer nasjonale hendelser kan nevnes Altinn-systemet som feilet ved utlegging av skatteoppgjøret våren 2012. Skatteoppgjøret til en navngitt person ble vist til flere som var pålogget Altinn. Feilen viste seg å skyldes en programmeringsfeil i en underleverandørs kode men også dårlig testing av Altinn-systemet for å klare den forventede belastningstoppen som systemet fikk når skatteoppgjøret for 2012 ble publisert elektronisk. En gjennomgang gjort av Det Norske Veritas, på oppdrag fra Nærings- og Handelsdepartementet, hadde påpekt vesentlige svakheter i Altinn systemet (Hartvigsen mfl. 2011).
- I august 2001 opplevde EDB Fellesdata problemer i ca. en uke, som førte til at anslagsvis 2 millioner nordmenn ikke hadde forbindelse med sine nettbanker. Feilen oppstod under en test av nye sikkerhetsløsninger hvor innholdet på flere disker ble slettet ved en operatørfeil (Digi.no(2001) i Sivertsen 2007).

Det skjer i tillegg en rekke ulykker i organisasjoners interne informasjonssystemer uten at dette når ut til offentligheten av frykt for å skade bedriftens renommé eller kunderelasjoner. Dette begrenser muligheten til å lære av andres feil. Noen informasjonssystemer er kritiske for at vårt moderne informasjonssamfunn skal fungere. Tidligere har dette vært begrenset til systemer som regulerer offentlige tjenester som vann og kraftforsyning, kommunikasjon, media etc. Utfall av slike samfunnskritiske systemer kan få store konsekvenser for befolkningen. En stadig omlegging av tjenester til selvbetjente informasjonssystemer, for eksempel for banktjenester, har ført til at samfunnet er avhengig av at informasjonssystemene er kontinuerlig tilgjengelige. Trafikkselskapene ønsker å gå vekk fra papirbilletter og penger som betalingsmiddel. Fremtidig betaling av reiser skal skje med elektroniske billetter for eksempel via mobiltelefonen som er direkte forbundet med selskapenes informasjonssystemer (Datatilsynet og Teknologirådet 2013).

Enkelte organisasjoner baserer nå hele sin virksomhet på salg via Internett. Datafirmaet Dell var et av de som var først ute. I Norge er Yr.no, Finn.no og Komplett.no eksempler på suksess-organisasjoner som utnytter mulighetene i Internett. Bokhandlernes nettbutikker som for eksempel

Amazon.com tilbyr raske og billige leveranser av varer direkte i postkassen slik at kundene ikke trenger å oppsøke butikkene lengre.

1.3 FORSKNINGSSPØRSMÅL

Forskningsspørsmålene som diskuteres i oppgaven er:

1 Hva karakteriserer risiko i informasjonssystemer og hvordan kan slik risiko styres?

2 Kan de vanlige risikoanalysemetoder også anvendes for risiko i informasjonssystemer eller er det behov for nytenkning?

3 Hva slags metoder er det i så fall behov for?

Metoder som er valgt for å besvare disse spørsmål er beskrevet i oppgavens metodekapittel (kapittel 3).

1.4 OMFANG OG UTDYPNINGER I FORHOLD TIL FORSKNINGS-SPØRSMÅLENE

Rapporten avgrenses til å se på karakteristikker i informasjonssystemer som kan relateres til de teoretiske ulykkesperspektivene som er gjennomgått ved studiet *Master i risikostyring og sikkerhetsledelse* ved UiS i perioden 2011 og 2012. Disse representerer de mest kjente perspektivene og gir en god bredde i beskrivelsen av type ulykker som kan skje. I henhold til ISO (ISO 2009b s.2) karakteriseres risiko ofte med referanse til mulige hendelser og konsekvenser eller en kombinasjon av disse. Denne definisjonen legges til grunn i oppgaven, men en vurdering av usikkerhet i forhold til både om hendelse vil kunne inntreffe og om hva de mulige konsekvenser kan være, er også nødvendig å inkludere for å knytte karakteristikkene til den definisjon av risiko som er valgt å bruke i oppgaven.

Med «de vanlige risikoanalysemetoder» menes de risikoanlysemetoder som er gjennomgått i fagene *Risikoanalyse del I* og *Risikoanalyse del II* ved UiS våren 2012. I tillegg blir nytten av å benytte noen metoder som er særskilt utviklet for analyse av sikkerhet i informasjonssystemer (CORAS og VAM), noen metoder som benyttes innenfor kvalitetssikring av informasjon (metoder basert på ISO-8000 og dataprofilering) samt datamining og bruk av nettverksanalyse, vurdert. Målet med utvelgelsen av analysemetoder har vært å finne lett tilgjengelige metoder som skiller seg ut fra andre. Det er også et ønske å presentere bredden i egenskaper i tilgjengelige analysemetoder. Det antall metoder som kan bli gjennomgått, begrenses av omfanget på oppgaven. Det samme gjelder detaljgraden på gjennomgangen av metodene. Gjennomgangen er begrenset til overordnede

egenskaper og karakteristikker ved analysemetodene. For flere detaljer henvises til det refererte kildemateriale.

Vurdering av hva slags nye metoder det vil være behov for i fremtiden er styrt av det fokuset som er valgt på ulykkesperspektivene og behov som kan relateres til disse.

1.5 RAPPORTENS OPPBYGGING

Struktur og disposisjon på rapporten er som beskrevet under:

Kapittel 2, som er oppgavens teoridel, gir en generell teoretisk introduksjon til sentrale begreper som brukes i oppgaven. Teoretiske ulykkesperspektiver og de utvalgte risikoanalysemetodene blir gjennomgått. Metodekapittelet (kapittel 3) beskriver metoder som er valgt benyttet i oppgaven og en diskusjon av alternative fremgangsmåter som kunne ha vært benyttet.

Et utvalg hendelser, hvor informasjonssystemer eller informasjon har hatt en vesentlig rolle, gjennomgås i kapittel 4, oppgavens empiridel. Informasjonssystemenes rolle er i fokus i disse eksemplene. For å få en oversiktlig og stringent form på presentasjonen av eksemplene er disse modellert i henhold til MTO-metodikken (Vedlegg A gir en kortfattet introduksjon til MTO-metodikken, og til de diagram og symboler som er brukt).

I kapittel 5 drøftes og relateres hendelsene i eksemplene til ulykkesperspektivene. Et rammeverk for valg av analysemetoder blir foreslått. Argumentasjonen som ligger bak den subjektive vurderingen av analysemetodenes egnethet er tatt med i vedlegg B. Det diskuteres hvilken virkning rammeverket kunne ha hatt, dersom det var blitt anvendt, og hvilke analysemetoder som ville ha vært best egnet å benytte i forhold til hendelsene i eksemplene. Rammeverket benyttes også som basis for diskusjon om hvilke områder (relatert til ulykkesperspektivene), hvor det er mangelfull metodedekning og behov for nytenkning.

Svar på forskningsspørsmålene gis som en oppsummering og konklusjon i kapittel 6 som også avrunder oppgaven med forslag til hvordan man kan komme videre med forskningsspørsmålene.

2 TEORI

Dette kapittelet definerer og diskuterer de sentrale begreper som brukes i oppgaven.

2.1 DATA, INFORMASJON, KUNNSKAP, VISDOM - DIKV- HIERARKIET

I oppgaven skilles det mellom begrepene data, informasjon, kunnskap og «visdom»[1]. DIKV-hierarkiet er sentralt som referansegrunnlag i IT-bransjen. Definisjonene er mange og delvis sprikende. Aven (2013a) har en interessant diskusjon om knytningen mellom risikokonseptet og elementene i DIKV-hierarkiet. For denne oppgavens formål er det funnet hensiktsmessig å definere begrepene som IFIP[2] har gjort i sin FRISCO rapport:

Data

FRISCO (1998 s.66) definerer data som:

> *«any set of representation of knowledge, expressed in a language»*

Med dette menes at beskrivelse av ting, hendelser, aktiviteter og transaksjoner som er registrert, klassifisert og lagret, ikke er organisert på en slik måte at beskrivelsen isolert sett gir noen mening. Språk (*language*) kan i denne forbindelse være numerisk, alfanumerisk, tekst, figurer, lyd eller bilde.

Informasjon

FRISCO (1998 s.68) definerer informasjon som:

> *«the personal knowledge increment brought about by a receiving action in a message transfer, i.e. it is the difference between the conceptions interpreted from a received message and the personal knowledge before the receiving action»*

Informasjon er derfor data som er organisert på en slik måte, transformert til et format og presentert slik at det gir mening for mottakeren.

Kunnskap

Forskjellen mellom kunnskap og informasjon har lenge vært et sentralt spørsmål i filosofien. Like fullt gis det i dag ingen klar definisjon. For denne oppgavens skyld velges å definere kunnskap som kontrollert og verifisert informasjon i henhold til. FRISCO rapporten (1998 s.66):

> *«a relatively stable and sufficiently consistent set of conceptions possessed by single human actors.»*

[1] Det engelske ordet «*wisdom*» er her oversatt til det norske ordet visdom. Alternativt kunne ordet klokskap vært brukt.

[2] FRISCO rapporten er et resultat fra IFIP WG 8.1 sin arbeidsgruppe «FRISCO». FRISCO er et akronym for "FRamework of Information System COncepts" og IFIP er den «International Federation for Information Processing", en ikkekommersiell og ikkestatlig organisasjon med 48 nasjonale dataforeninger og universiteter som medlemmer.

.

Visdom

Begrepet visdom innbefatter forståelsen for hva kunnskap betyr og hvordan kunnskap best kan anvendes. Rowley (2006 i Aven 2013a s.31) definerer visdom som:

> *«wisdom is the capacity to put into action the most appropriate behaviour, taking into account what is known (knowledge) and what does the most good (ethical and social considerations).»*

FRISCO rapporten har ikke noen definisjon av begrepet visdom. Rowleys definisjon blir brukt i denne oppgaven.

2.2 INFORMASJONSSYSTEMER

Informasjon er et produkt av et informasjonssystem. Input til dette systemet er data (English 1999). Et informasjonssystem angår bruk av informasjon av personer eller organisasjoner (Frisco 1998). I informasjonssamfunnet assosierer vi ofte et informasjonssystem med et system som kan benyttes gjennom en datamaskin. For diskusjonene i oppgaven er det funnet hensiktsmessig å gruppere informasjonssystemer i tre grupper etter hvordan informasjonen er strukturert. Gruppene er beskrevet i de påfølgende delkapitler. Dette er funnet hensiktsmessig fordi reglene for behandling av informasjon vil være forskjellig i de tre forskjellige strukturene. Konsekvent bruk av begrepet *informasjonssystem* er bevisst. Alternativt kunne begrepene *datasystem* eller *kunnskapssystem* vært brukt. Datasystem er ikke brukt siden dette blir forbundet med et teknisk system som forvalter data. Fokus ville da ha blitt risiko knyttet til forvaltning og drift. Kunnskapssystem og informasjons-system har ikke noen klar avgrensning. Det er mulig at en del av de problemstillinger som tas opp i denne oppgave relaterer seg til det mange vil si bør innbefattes i et kunnskapssystem.

2.2.1 Strukturert informasjon

Med strukturert informasjon menes informasjon som er identifiserbar siden den er organisert etter definerte regler. Den mest vanlige måten å strukturere informasjon på er i en database. Her organiseres data i henhold til et databaseskjema som gir struktur og regler for sammenhenger mellom de forskjellige dataelementer. Begrepet datavarehus brukes også om en streng organi-sering av data i henhold til fast definerte databaseskjema. Datamodeller som er vanlige her betegnes ofte stjernemodeller, *snow flakes* modeller eller informasjonskuber. Siden datastrukturene er faste og dataene som skal analyseres må legges inn i de faste strukturene, har en kunnet lage avansert analyseverktøy som kan gjenbrukes i mange organisasjoner. *OLAP* (*On Line Analytical Processing*) er et begrep som ofte benyttes sammen med datavarehus som begrep på metoder for å navigere i, kombinere og prosessere data. Streng organisering av data gjør også at applikasjoner som opererer på disse strukturene kan gjenbrukes i forskjellige sammenhenger (Han 2012).

2.2.2 Ustrukturert informasjon

Ustrukturert informasjon har ingen regelbasert fast struktur og har heller ikke noe skjema som gjør det mulig å plassere informasjon inn i tradisjonelle tabellstrukturer. De kan kun brukes i den applikasjonen som de er laget med eller kan konverteres til (Daconta 2003). *Big data* er et moteord som brukes i det moderne informasjonssamfunn om den enorme datamengden som skapes i dag. Den største økningen av informasjon som skapes i dag er ustrukturert informasjon som bilder, video, tekst, sensorinformasjon av forskjellig slag (Datatilsynet og Teknologirådet 2013).

2.2.3 Referansebaserte (semantiske) strukturer

XML (*eXtended Markup Language*) er basisen for det som refereres til som semantisk web. Tim Berners-Lee, Internetts oppfinner, hadde to visjoner for sitt arbeid. Det første var å lage et medium for samarbeid. Det andre var å lage et medium som var forståelig og dermed prosesserbart av datamaskiner. Uheldigvis er relasjoner mellom ressurser ikke tilstrekkelige for intelligent prosessering, slik de defineres i dag. Skal Berners-Lees intensjon om et prosesserbart Internett realiseres, må eksisterende data kompletteres med *metadata*[3] som viser definisjoner og sammenhenger mellom ressurser. Dette er formålet med semantisk web – å legge på definisjoner og metadata som gjør dataene kombinerbare – dette gjelder både for strukturerte og ustrukturerte data (Daconta 2003).

2.3 RISIKO

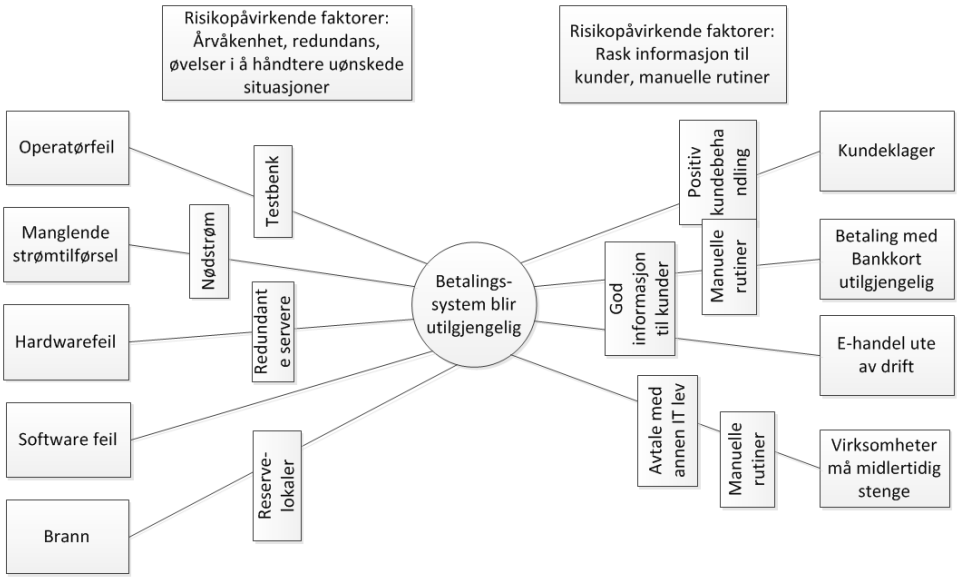
Risiko handler om mulige fremtidige hendelser (A) og om hva konsekvensene (C) av slike hendelser kan være. Som ved alt som har med fremtid å gjøre er det usikkerhet knyttet til de mulige konsekvensene. Konsekvenser kan være både positive og negative (Aven 2007). Det har vært gjort mange forsøk på å komme frem til entydige definisjoner på risikobegrepet. Forskjellige kulturer, bransjer, organisasjoner har egne definisjoner og bruker begrepet ulikt. Risiko defineres i denne oppgaven til å være kombinasjonen av hendelser (A) i eller med et informasjonssystem og konsekvenser (C) av disse, og tilhørende usikkerhet (vil hendelsen inntreffe og hva blir i så fall konsekvensene).

Det mest brukte verktøy til å beskrive usikkerhet er sannsynlighet (P). Aven (2012) har en detaljert diskusjon av hvordan risiko som konsept har utviklet seg over tid og hva som per i dag er de mest vanlige definisjoner av risiko. Sannsynligheten (P) for at hendelsen kan inntreffe kan betraktes på forskjellige måter. Såkalte frekventister vil alltid tolke en sannsynlighet som den relative frekvensen etter et uendelig antall forsøk. Såkalte subjektivister vil alltid tolke en sannsynlighet som graden av tro på om hvorvidt hendelsen vil inntreffe eller ei (Løvås 2004). Aven (2013b) diskuterer

[3] Metada defineres som data om data. Dvs. data som beskriver hvordan dataelementer er organisert, formater og hva de beskriver.

fundamenter for sannsynlighetskonseptet i en risikoanalyse og sikkerhetskontekst. Han setter spørsmålstegn ved eksistensen av objektive sannsynligheter i en slik kontekst da et uendelig antall like forsøk er vanskelig å oppnå i en risiko- og sikkerhetssammenheng. Sannsynligheten kan være den samme i to situasjoner, men kunnskapen som ligger til grunn for sannsynlighetsangivelsene, kan være fullstendig forskjellige. En beslutningstager kan bli villedet hvis ikke kunnskapen som ligger bak sannsynlighetsbedømmingen tas med i betraktningen. En annen faktor er at sannsynligheter alltid er betinget av en rekke forutsetninger. Slike forutsetninger kan skjule viktige aspekter av risiko og usikkerheter (Aven 2013c). Aven (2013c) sier videre at sannsynlighet bare er et av flere verktøy for å beskrive usikkerhet og at risikokonseptet ikke må begrenses til kun dette verktøyet.

I eksemplet i figur 1, som er illustrert med et såkalt «*bow-tie diagram*», er den initierende hendelsen (A) at et betalingssystem går ned og blir utilgjengelig. Mulige årsaker til at dette kan skje er angitt som bokser på venstre side i diagrammet (Operatørfeil, manglende strømtilførsel, osv.). Kundeklager, betaling med bankkort ikke mulig lengre, e-handel som er ute av drift og virksomheter som må midlertidig stenge er mulige prediksjoner (C*) av konsekvenser(C). «*Bow-tie*» er en hensiktsmessig måte å illustrere og kommunisere mulige årsaker og konsekvenser av en initierende hendelse på og kan med fordel anvendes i en risikoanalyse.



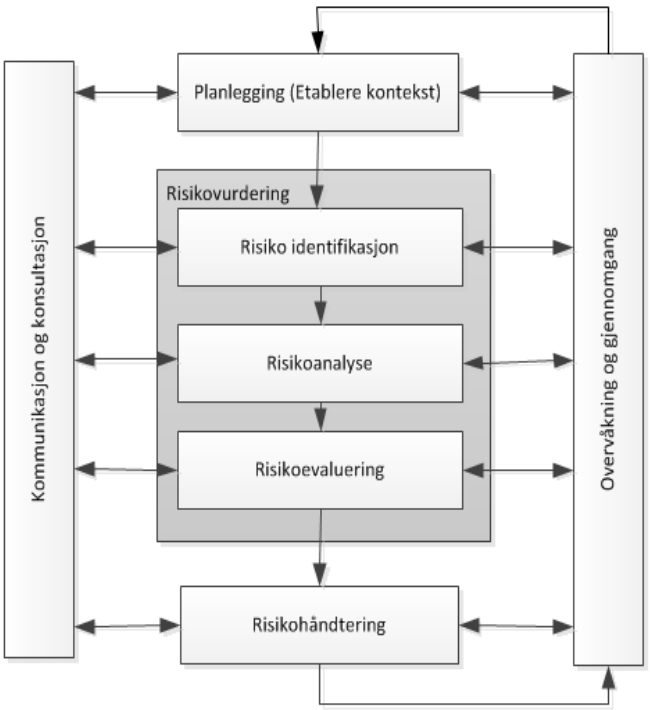
Figur 1: "Bow-Tie" diagram illustrert med et eksempel

Barrierer er de tiltak vi enten iverksetter for å hindre at den initierende hendelse skal skje (sannsynlighetsreduserende) eller de tiltak som vi planlegger å iverksette dersom den initierende hendelsen inntreffer (konsekvensreduserende). Et resultat av en risikoanalyse kan være forslag til barrierer som bør etableres eller forsterkes for enten å gjøre informasjonssystemene mer robuste, eller for at muligheter lettere skal kunne utvikles. Dette gjøres ved å etablere eller styrke barrierer

som kan påvirke usikkerheten om en hendelse kan inntreffe, eller påvirke konsekvensene etter at hendelsen eventuelt har inntruffet. Eksempler på barrierer er vist i «bow-tie» diagrammet.

2.4 RISIKOSTYRINGSPROSESSEN

Med risikostyring forstås alle tiltak og aktiviteter som gjøres for å styre risiko. Risikostyring handler om å balansere konflikten mellom det å utforske muligheter på den ene siden og å unngå tap, ulykker og katastrofer på den andre siden (Aven 2008). For styring av risiko i et informasjonssystem vil ISO standard ISO-31000:2009 kunne anvendes siden denne er utviklet som en generell standard og er uavhengig av type anvendelse. Standarden spesifiserer hvilke aktiviteter en bør gjennomføre i en risikostyringsprosess (figur 2).



Figur 2: Risikostyringsprosessen i henhold til ISO-31000:2009 (ISO 2009)

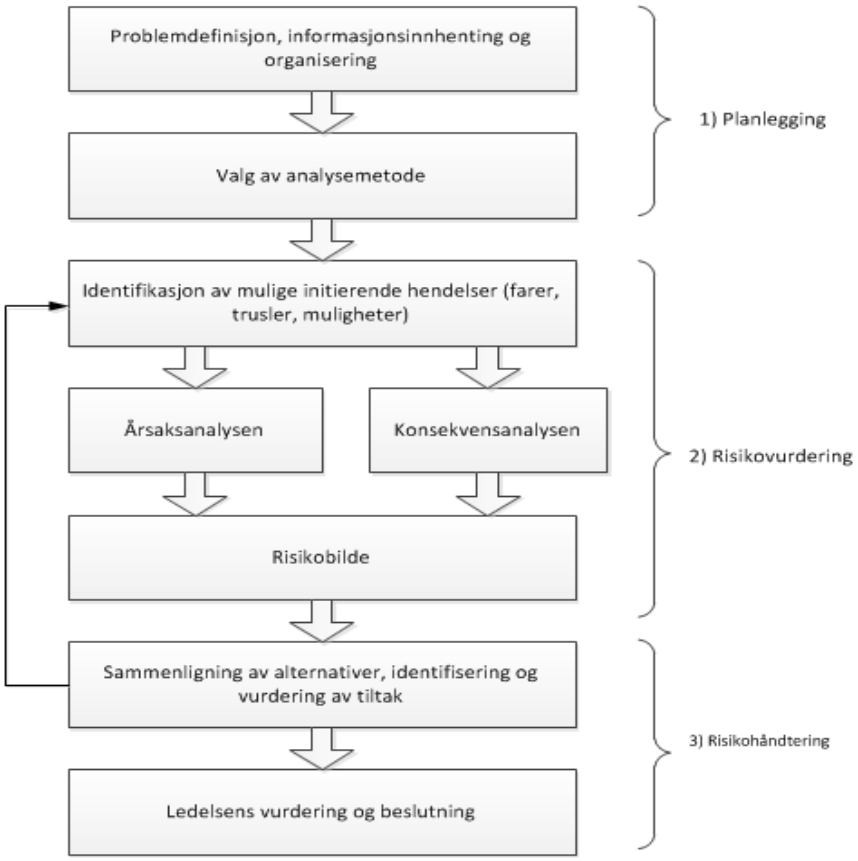
2.5 RISIKOANALYSE AV INFORMASJONSSYSTEMER

De tre hovedaktivitetene (planlegging, risikovurdering, risikohåndtering) som inngår i selve analysen av risiko i informasjonssystemer, vises i referansemodellen i figur 3 (Aven 2008).

Informasjonssystemer er ofte store og komplekse. De kan være vanskelig å avgrense siden de ofte er tett integrert med, bruker eller utveksler felles data med andre informasjonssystemer. Synkronisering av endringer som skjer på de samme data som anvendes i flere parallelle systemer, erfares ofte å være en utfordring. Det er nødvendig med en klar problemformulering slik at analysen

blir fokusert og kan gjennomføres innenfor de rammer som er spesifisert. Informasjon som er samlet inn for å brukes i en kontekst og under gitte forutsetninger, kan gis en ny kontekst eller kombineres med annen informasjon i en annen kontekst, slik at de krav som gjaldt ved innsamlingen til kvalitet og presisjon er uriktige og kan forårsake feil og misforståelser (English 1999).

Identifikasjon av mulige initierende hendelser må gjøres sammen med analyse av mulige årsaker og konsekvenser for å få opp risikobildet. Sammenligning av alternativer, identifisering og vurdering av tiltak vil være et hjelpemiddel for å kunne etablere barrierer. Ofte kan det være hensiktsmessig å presentere resultatet fra en analyse i en risikomatrise eller i en tabell. Formålet med risikoanalysen er alltid å bidra med et beslutningsunderlag for de ledelsesvurderinger og beslutninger som skal tas (Aven 2008).



Figur 3: Risikoanalysens ulike trinn (Aven 2008)

2.6 METODER FOR Å ANALYSERE RISIKO I INFORMASJONS-SYSTEMER

Et utvalg aktuelle analysemetoder blir gjennomgått i dette delkapittel og sett i forhold til risiko i informasjonssystemer. Egenskaper ved metodene blir kort beskrevet. Tabell 2 gir en oversikt over metodene. Ambisjonsnivået er ikke å gi en fullstendig beskrivelse av analysemetodene men kun kort å introdusere dem som basis for diskusjonene i oppgaven. Det henvises til det refererte kildemateriale for en mer fullstendig beskrivelse av hver enkelt metode.

2.6.1 Grovanalyse

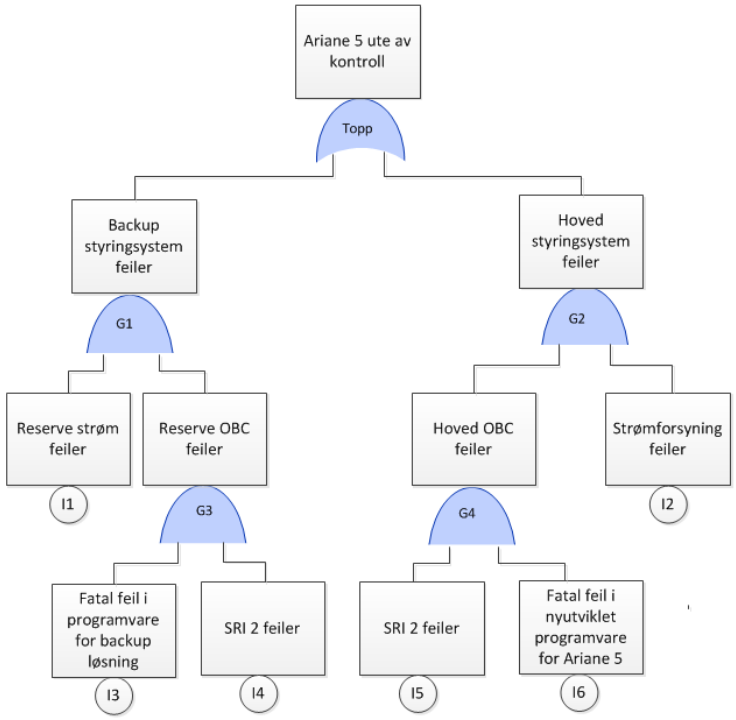
Mange system er ofte store, dårlig dokumenterte og uoversiktlige. Grovanalyse er en kvalitativ metode som kan anvendes for å få oversikt over risikobildet. Grovanalysen kan være et hjelpemiddel til å identifisere hvilke barrierer som er etablert og om disse er effektive eller ikke. Den kan også være en basis for planlegging av hvilke deler av systemet som bør analyseres nærmere og til å avgjøre hvilke metoder en skal bruke for en slik mer detaljert analyse. Grovanalysen er beregnet på å gjøre grove kartlegginger og anvendes derfor ofte i en tidlig fase i en analyse. Ved endringer, omlegging, nye anvendelsesområder, etc. kan metoden også være godt egnet. Grovanalyse av et system kan utføres stegvis som for eksempel (Aven 2008):

1. Velge ut hvilke deler av eller prosesser rundt systemet som skal analyseres
2. Identifisere mulige uønskede eller ønskede hendelser med systemet
3. Vurdere hver enkelt hendelse med hensyn til usikkerhet og konsekvens
4. Prioritere risikomomenter for videre analyse eller risikoreduserende tiltak

En sjekkliste forenkler arbeidet med analysen. Bruk av sjekkliste er en teknikk som kan inkluderes i en grovanalyse som den initielle tilnærmingen til risikoidentifisering i et system. Som del av grovanalysen kan sjekklister benyttes for å få et overblikk over det totale risikobildet. Eksempler på sjekklister for de fleste formål kan enkelt finnes på Internett, lastes ned og tilpasses spesifikke formål.

2.6.2 Feiltreanalyse

Feiltreanalyse er en metode som blir brukt til å analysere et system for å identifisere feil som kan lede til uønskede hendelser i et system. Et feiltre er en grafisk modell hvor den initierende (uønskede) hendelsen er i fokus (toppnode). Ved hjelp av boolsk logikk (f.eks. AND, OR gater) forbindes mulige årsaker som i kombinasjon kan lede til den initierende hendelsen. Feiltreet blir derfor en grafisk representasjon av hendelser (både menneskelige, teknologiske og organisasjonsmessige) som avhengig av tilstand, kan forårsake den initierende hendelsen (Aven 2008). Figur 4 viser et eksempel på et feiltre.

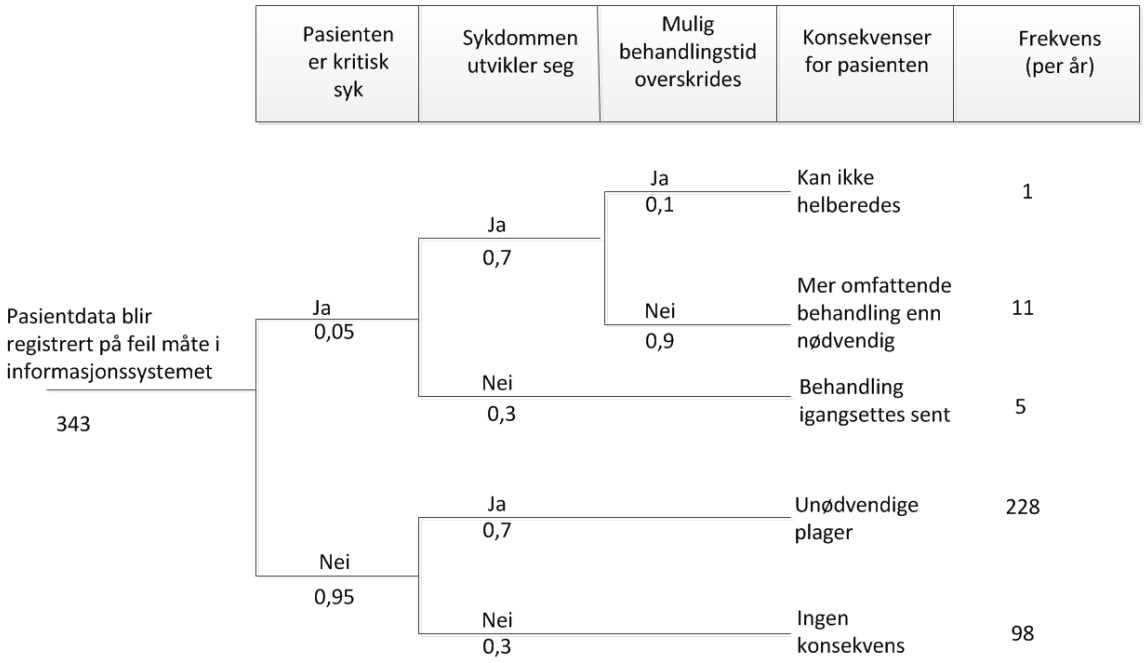


Figur 4: Eksempel på feiltre

2.6.3 Hendelsestreanalyse

Et hendelsestre brukes til å illustrere de forskjellige hendelsesforløp eller konsekvenser som en initierende hendelse kan medføre (figur 5). Ved å tegne opp et tre hvor hvert forgreiningspunkt inneholder de mulige konsekvensalternativer får en et totalbilde av mulige konsekvenser som kan oppstå. Hendelsestreanalyse kan brukes både til kvantitative og kvalitative analyser (Aven 2008). Dette er illustrert i figuren som viser en hendelsestreanalyse av tilfellet «David»[4] som er et av eksemplene som blir gjennomgått i empirikapittelet (Kapittel 4).

[4] I eksemplet er tallene 343 på antall feilregistreringer og 1 hvor konsekvens ble at sykdommen ikke kunne helberedes, virkelige tall hentet fra Vedleer og Eggesvik (2013). De andre tall er konstruerte for eksemplets formål.



Figur 5: Eksempel på hendelsestre

2.6.4 FMEA (*Failure Modes and Effect Analysis*)

FMEA er en enkel kvalitativ metode som innebærer en systematisk gjennomgang av hver enkelt systemkomponent og undersøkelse av hva som skjer dersom denne svikter. Systemet deles opp i komponenter som testes isolert og hvor alle mulig kombinasjoner av input testes for å vurdere all mulig respons fra komponenten. Gjennomgang av de relevante komponenter gir god forståelse for de enkeltfeil som kan inntreffe og effekten av disse (Aven 2008).

Selv om man som regel kan programmere og automatisere alle tester og feilmuligheter i et informasjonssystem, er dette ofte svært tidkrevende og blir i praksis ofte nedprioritert. FMEA kan danne grunnlag for kvantitative analyser med metoder som feiltre og hendelsestre.

FMEA er ikke spesielt godt velegnet for gjennomgang av redundante systemer siden man bare ser på en og en komponent (Aven 2008).

2.6.5 Sikker Jobb Analyse (SJA)

En SJA gjennomføres ved å dele arbeidet opp i deloppgaver og så foreta en risikoanalyse av hver enkelt av deloppgavene. SJA brukes mye blant annet i olje- og gassvirksomheten. Gjennom en SJA går en gjennom oppgaver eller aktiviteter som skal utføres før man starter arbeidet. Målet er å (Aven 2008):

1) Identifisere faremomenter og årsaker til mulige uønskede hendelser
2) Identifisere mulige konsekvenser for hver uønsket hendelse
3) Identifisere mulige tiltak for de konsekvenser en ønsker å unngå

Hjelpemidler er ofte sjekklister, skjema som fylles ut med resultater av analysen eller presentasjon i risikomatriser. Ofte er det knyttet formaliteter til vurderingen av om tiltak må iverksettes før jobben kan startes opp. SJA er en enkel metode som er lett å forstå, planlegge og gjennomføre og er derfor blitt populær.

2.6.6 HAZOP

HAZOP (*Hazard and Operability analysis*) er en kvalitativ risikoanalyseteknikk, som brukes til å påvise svakheter og farer i et prosessanlegg. Metoden brukes normalt i planleggingsfasen (design). Ved hjelp av ledeord som «ikke/ingen, mer/ mindre, deler av, mer enn, motsatt, andre/ annerledes» avklares hvordan ulike kombinasjoner av hendelser og prosessforhold som isolert sett er ufarlige, kan innebære en risiko. HAZOP brukes ofte i forbindelse med designgjennomganger av prosessanlegg etter at designet har kommet så langt at det finnes god dokumentasjon av det planlagte systemet (Aven 2008).

HAZOP analysen kan dokumenteres i en tabell med kolonner for identifikator, interessent, aktivt item, ledeord og mulige uønskede hendelser. Det er en omfattende og ressurskrevende prosess siden den krever et multidisiplint team for å kunne gjøre en bred gjennomgang. I forbindelse med forsøk på å bruke metoden på informasjonssystemer er det erfart at metoden kan være nyttig dersom den blir gjort på et tidlig stadium i utviklingen av systemet og dersom det benyttes tilstrekkelig med ressurser (McDermid 1995).

2.6.7 Bayesiansk nettverk

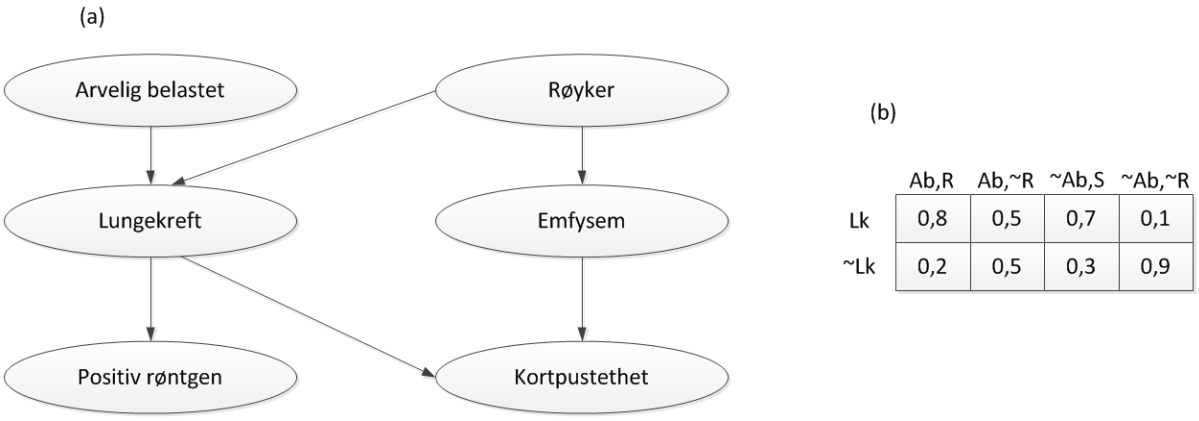
Bayesiansk nettverk er både en kvalitativ og en kvantitativ metode som er mer generell enn hendelsestrær og feiltrær, og har vist seg hensiktsmessig i forbindelse med analyse av komplekse årsaksforhold (Aven 2008). Et Bayesiansk nettverk består av to deler. En rettet asyklisk graf (merket (a) i figur 6) som består av noder der hver node representerer en tilfeldig variabel, kantene på nodene representerer betingete avhengigheter og piler som angir avhengighetene, det vil si årsakssammenhenger. I følge Bayes teori kan variablene være observerbare kvantiteter, latente variabler, ukjente parametere eller hypoteser. Nodene betegnes foreldre eller barn etter den vei pilene peker (Fra foreldre mot barn).

I tillegg inngår tabeller for hver variabel (*Conditional Probability Table (CPT)*). I eksemplet i figur 6 er CPT for variablen Lungekreft merket med (b). Slike betingede sannsynligheter angis med basis i erfaringsdata eller ved hjelp av ekspertvurderinger (Aven 2008).

Nettverket kan for eksempel, gitt ulike symptomer, kalkulere sannsynligheten for at en person har en sykdom. Dette er vist i det følgende forenklede eksemplet basert på detaljer fra figur 6 (Han 2012):

P(Lungekreft(Lk) | Arvelig belastet(Ab), Røyker(R)) =0.8

P(Ikke Lungekreft(Lk) |Ikke Arvelig belastet(Ab), Ikke Røyker(R))=0.9



Figur 6: Eksempel på Bayesiansk nettverk (Kilde Han(2012))

Ved hjelp av *Bayes formel* kan sannsynlighetene for ulike tilstander i nettverket beregnes gitt at vi har observert tilstandene i noen av nodene. Fra nettverket i figur 6 vil en for eksempel kunne beregne sannsynligheten for at en pasient har lungekreft gitt at han røyker og er arvelig belastet.

2.6.8 KITHs risikoanalysemetodikk for informasjonssystem

KITH (Kompetansesenter for IT i Helsevesenet AS) (Aksnes m.fl. 2000) beskriver risikoanalyse som et verktøy for å skape oversikt over verdier og trusler mot disse i en organisasjon eller i et informasjonssystem. Risikoanalyser sees i sammenheng med BS 7799 – en britisk standard for informasjonssikkerhet. Aksnes m.fl. sier at (2000 s.18):

> «*BS7799 beskriver risikoanalyse som en systematisk overveiing av a) sannsynlige skader som kan komme som et resultat av et sikkerhetsbrudd, når man vurderer potensielle konsekvenser av tap av konfidensialitet, integritet eller tilgjengelighet til informasjon og andre verdier, og b) den realistiske sannsynligheten for at en slik feil skal skje sett i lys av fremtredende trusler og svakheter og eksisterende mottiltak*».
>
> Metodikken fokuserer primært på sikkerhet. KITH presenterer sin metode som *«rimelig enkel»* og foreslår *«å starte med et enkelt oppsett som krever enkle hjelpemidler, og så bli mer sofistikert etter hvert»* (s. 19).

Ifølge KITHs metodikk bør følgende trinn inngå i en risikoanalyse:

- Identifisering av trusler med beskrivelse av teknikker og forslag til verktøy som kan benyttes

- Sannsynlighets-, konsekvens- og risikovurderinger (eksempler og forslag til hjelpemidler er beskrevet)
- Tiltak og oppfølging (eksempler på strategier og type tiltak for risikohåndtering er beskrevet)
- BS 7799 og risikoanalyse (Det refereres til standarden for en rekke anbefalinger for sikkerhetstiltak som KITH mener er et godt utgangspunkt for å utføre risikoanalyse)
- Kritisk vurdering – hypoteser og usikkerhet. En refleksjon av hvordan betrakte pålitelig-heten i resultatet fra en analyse og hvordan analysen kan brukes til beslutningsstøtte

BS 7799 gir en rekke anbefalinger for sikkerhetstiltak en organisasjon bør implementere. Inkludert i dette er blant annet anbefalinger knyttet til systemutvikling og vedlikehold, klassifisering av, og tilgang til informasjon samt sikkerhetspolicy.

KITHs risikoanalysemetodikk for informasjonssystem fremstår mer som en prosess/ prosedyre enn en metodikk. Den beskriver hvordan en risikoanalyse kan gjennomføres og samsvarer i store trekk med alle steg i risikoanalysens ulike trinn som beskrevet i delkapittel 2.5 (Se også figur 3).

2.6.9 RANDs VAM

VAM (*The Vulnerability Assessment & Mitigation methodology*) betegnes som en ovenfra og ned metode som består av seks definerte steg. VAM er utviklet av RAND som er en amerikansk forskningsinstitusjon knyttet til det amerikanske forsvar. Metoden spesifiserer at følgende steg utføres i en risikoanalyse (Anton m.fl. 2003 s. 9):

1. Identifikasjon av en organisasjons essensielle informasjonsfunksjoner
2. Identifikasjon av informasjonssystemer som er essensielle i forhold til å implementere de identifiserte informasjonsfunksjoner
3. Identifikasjon av sårbarheten i de identifiserte informasjonssystemene
4. Identifisering av aktuelle sikkerhetsteknikker for å minske sårbarheten identifisert i steg 3 Til dette tilbys et verktøy *the VAM matching matrix tool*
5. Valg og implementering av teknikker fra steg 4 ut fra begrensninger, kost- og nytte-vurderinger
6. Testing av de benyttede teknikker for robusthet og nytte når de utsettes for trusler

Steg 3-6 gjentas etter behov.

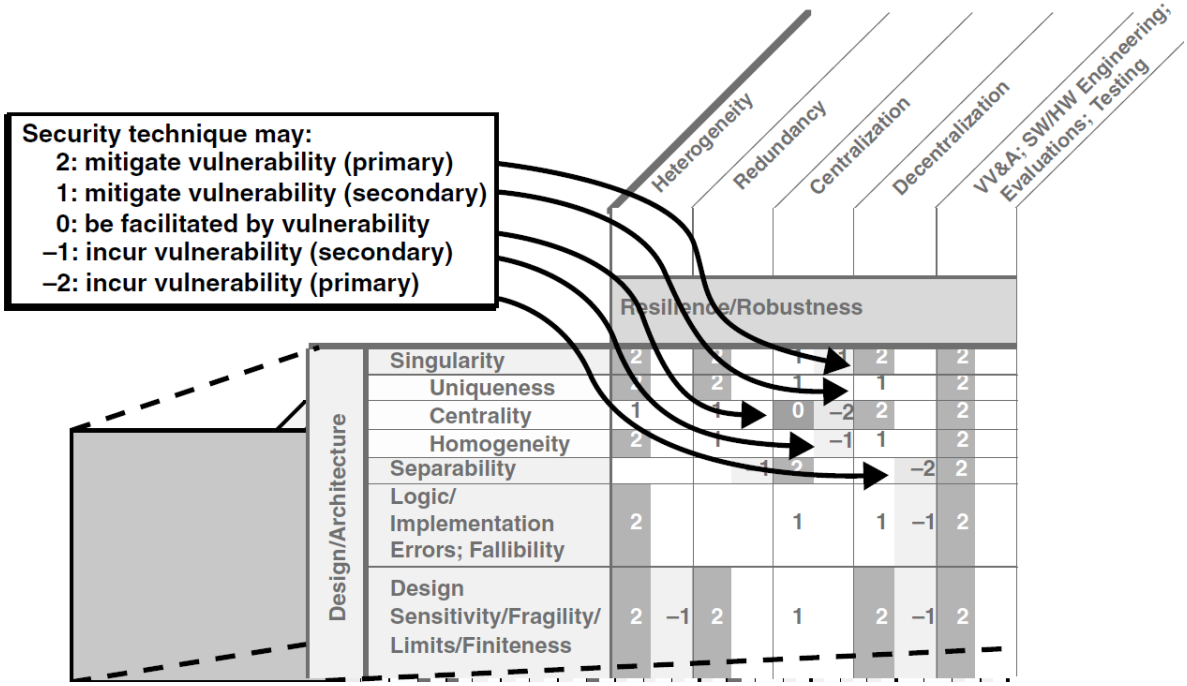
Resultatet av steg 3 er en sårbarhetsmatrise. For å etablere sårbarhetsmatrisen deles informasjons-systemene opp i objekter. Objektene kan være komponenter i informasjonssystemet, aktører som har en rolle i forhold til informasjonssystemet eller andre elementer som kan påvirke systemet. Deretter betrakter en egenskaper (attributter) ved objektene for å identifisere områder hvor systemet

er sårbart. Kolonnene i sårbarhetsmatrisen utgjør her de sårbare objekter mens radene utgjør attributtene. Feltene i matrisen vil inneholde en beskrivelse av den konkrete «sårbarheten» som er identifisert.

I steg 4 mappes mulige sikkerhetsteknikker til de identifiserte sårbarheter. Som et hjelpemiddel til å velge adekvat teknikk for risikoreduksjon foreslår metoden en rekke standardteknikker som kan vurderes. Hvor effektiv risikoreduksjonsteknikken anses å være, bedømmes. I matrisen graderer man så teknikken i henhold til følgende skala:

2: reduserer sårbarheten (primær)
1: reduserer sårbarheten (sekundær)
0: sårbarheten kan ha positive sideeffekter
-2: Sikkerhetsteknikken kan gjøre at en blir utsatt for ny sårbarhet (primær)
-1: Sikkerhetsteknikken kan gjøre at en blir utsatt for flere sårbarheter (sekundær)

Matrisene er å anse som et hjelpemiddel til å velge metode i det store utvalg med muligheter som kan foreligge. Figur 7 viser et eksempel på en resultatmatrise fra en VAM analyse.



Figur 7: Eksempel på utfylt VAM matrise (Anton m.fl. 2003))

2.6.10 CORAS

Metoden CORAS beskriver 8 steg som utføres i sekvens. Steg 1-4 er en beskrivelse av hvordan en planlegger og etablerer konteksten til analysen. Dette svarer til referansemodellens steg «Planlegging» (delkapittel 2.5 og figur 3). Mens referansemodellen er generell foreslås i CORAS helt konkret hvordan aktiviteten skal gjennomføres (som eksempelvis ved å arrangere møter, holde presentasjoner, etc.).

Steg 5-8 i CORAS beskriver hvordan selve analysen gjennomføres.

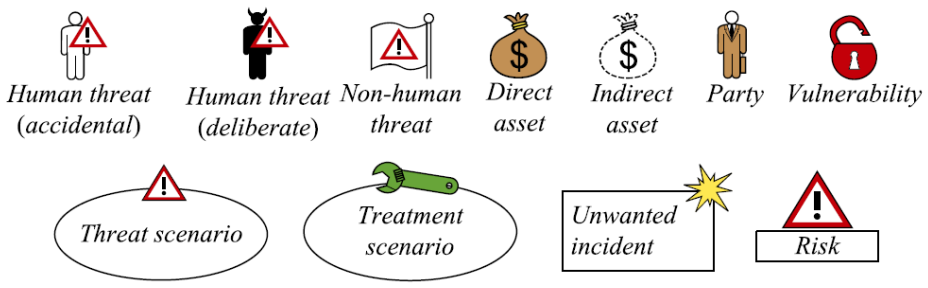
De 8 stegene er (Lund 2011):

Steg 1: Presentasjon av analysemetoden til kunde
Steg 2: Kunden presenterer sine mål og forventninger til analysen
Steg 3: Mål og kundens forventninger blir videre raffinert
Steg 4: Mål, planer, mandat etc. blir godkjent
Steg 5: Risiko identifisering
Steg 6. Risiko estimering
Steg 7. Risiko evaluering
Steg 8. Risiko håndtering

CORAS introduserer symboler (**Error! Reference source not found.**) som kan kombineres til å age illustrasjoner av risikobildet, tiltak og farer. Symbolene kombineres til diagrammer tilsvarende slik det gjøres i *UML*[5]. Symbolene kan også kombineres med *UML*-diagram, for eksempel aktivitetsdiagram, *use cases*, interaksjons diagrammer, for å synliggjøre risiko. Forskjellige diagramtyper som foreslås er:

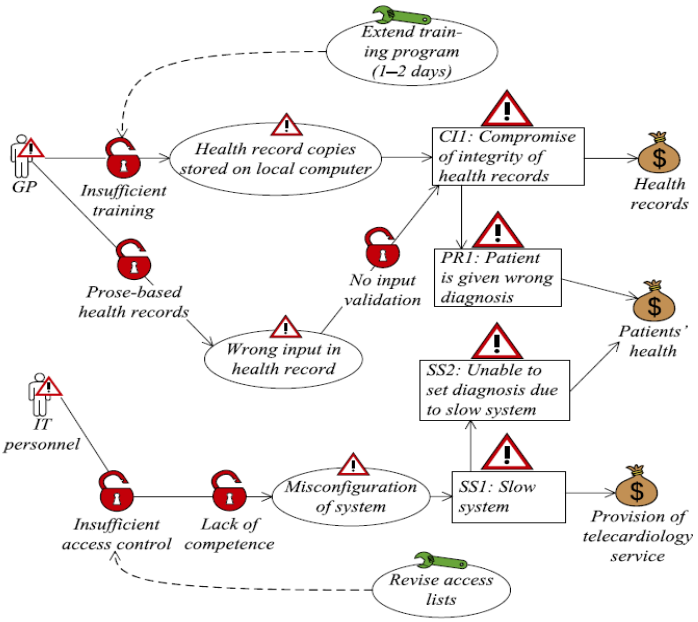
- Oversikt over eiendeler som blir utsatt for trussel (*Asset diagram*)
- Trusselbilder med estimater over sannsynligheter og konsekvenser (*Threat diagrams*)
- Risiko diagram
- Oversikt over mulige tiltak (*Treatment diagrams*)

I figur 9 er det tatt med et eksempel på et tiltaksdiagram som et eksempel på hvordan et CORAS diagram ser ut. Til bruk med CORAS finnes det også egenutviklet programvare (Lund 2011).



Figur 8: Symboler brukt i CORAS metoden (Lund 2011)

[5] Ref Fowler (2004) for en enkel introduksjon til de forskjellige diagramtyper som benyttes i Unified Modelling Language(UML)



Figur 9: Eksempel på tiltaksdiagram (Treatment diagram) i CORAS (Lund 2011)

2.6.11 Dataprofilering

Dataprofilering er en metode hvor man eksaminerer data i et informasjonssystem (ustrukturert, strukturert eller referansebasert) og genererer statistikk og informasjon om dataene. Disse genererte data utgjør metadata til informasjonssystemet. Typiske metadata kan være (Lindsey 2008):

- Verdier tilordnet bestemte felt eller variabler (f.eks. for å verifisere at verdiene er innenfor tillatte grenser)
- Data typer (karakterer, numeriske, dato)
- Mønster (telefonnummer, postnummer)
- Telling av forekomster (antall kunder i en bestem region)
- Statistikk (minimum, maksimum, gjennomsnitt)
- Avhengigheter (konsistente primær- og sekundærnøkler i en database)

Gjennomgangen vil kunne avdekke om det er feil eller mangler i informasjonen. Bakgrunnen for å lage en dataprofil er vanligvis (Lindesey 2008):

- For å finne ut om eksisterende data kan brukes til andre formål enn det opprinnelige
- Bedømme risiko forbundet med å integrere et sett data med et annet
- Følge opp kvalitet over tid
- Lage eksakte ETL (*Extract-Transfer-Load*) spesifikasjoner
- Bedømme om metadataene eksakt beskriver verdiene i en database
- Avklare utfordringer med data tidlig i et utviklingsprosjekt
- Dokumentere et informasjonssystem og lage korrekte metadata for fremtidige prosjekter
- Finne ut hvilke data som finnes i et gammelt eksisterende system

En rekke programvarer er tilgjengelig med innebygget funksjonalitet for denne type analyser.

2.6.12 ISO-8000 Data Quality

Det pågår et arbeid i ISO for å frembringe en standard for datakvalitet (ISO 2011). Utgangspunktet for denne standarden er et behov for å sikre kvalitet på data som blir overført mellom to organisasjoner. Man har bevisst bestemt seg for å bruke data som begrep i denne standarden (i stedet for informasjon). Argumentasjonen for dette er at en kan definere objektive målekriterier for datakvalitet. Målbare krav for informasjonskvalitet kan en ikke like enkelt definere (Benson 2009). Codd introduserte i 1970 det som i ettertid er betegnet som de tradisjonelle databaseintegritets-regler. Codds integritetsregler består av entitets-, referensiell-, domene-, kolonneintegritet og forretningsregler (Lee 2006). Integritetsreglene har generell anvendelse og man kan avlede generelle måleparametre (metrikker) for å kunne måle tilstanden på datakvaliteten i forhold til disse. Spesifikke forretningsregler krever kontekstavhengige metrikker og målerutiner. Disse reglene har alltid vært sentrale og former nå grunnlaget for det som i ISO-8000 sammenheng betegnes som syntaktisk datakvalitetssjekk (ISO 2011). Syntaktiske sjekker kan enkelt programmeres og automatiseres.

I tillegg introduserer også ISO-8000 begrepet semantisk datakvalitet (ISO 2011). I praksis opplever en at feltnavn i en tabell kan være helt ulikt feltnavnet i en annen tabell selv om feltene skal holde det samme dataelementet. En organisasjon har sine masterdata, det vil si informasjon som flere informasjonssystemer bruker. Eksempler her er ansattinformasjon, kundeinformasjon, produkt-informasjon, interne standarder og prosedyrer. ISO (2011) inkluderer masterdata og også annen informasjon som utveksles eller deles i det som betegnes for referansedata. Ved å etablere referanser eller pekere til definisjoner og metadata, eller klassifisere dataene, bygger en inn en definisjon av type dataelement. Dette tilsvarer det som i avsnitt 2.2.3 ble betegnet Referansebaserte (semantiske) strukturer. Formålet er å gjøre dataene kombinerbare. Basert på ISO-8000 er håpet at en vil få utviklet effektive metoder og verktøy for kvalitetssikring av informasjon. Det Norske Veritas er for eksempel i gang med å utvikle en verktøykasse basert på ISO-8000.

2.6.13 Datamining

Teksten i dette delkapittel er i sin helhet hentet fra Han (2012). Datamining er en metode for å analysere data i et informasjonssystem. Dette gjøres ved å søke etter forekomster av mønstre som er av interesse. Datamining gjøres tradisjonelt på voluminøse strukturerte informasjonssystemer med databaser eller datavarehus i bunn. Begreper kommer fra assosiasjonen med gruvedrift om at en ønsker å utvinne (mine) kunnskap fra en stor og uoversiktlig datamengde. Datamining kombinerer metoder fra statistikk, mønstergjenkjenning, database og datavarehus, maskinlæring (hvordan

datamaskiner kan forbedre sin effektivitet ved å lære av de data som behandles), visualisering og effektivitet i behandling av ustrukturerte data. Datamineringen skjer etter noen definerte prinsipper:

Klassifisering av data

Ved hjelp av beslutningsalgoritmer (definerte beslutningstre) kan gjenkjente dataelementer også klassifiseres. Klassifiseringsmodeller brukes eksempelvis av bankene når de skal bedømme identifisere og bedømme risiko knyttet til en lånesøknad. Eksempler på slike klassifiseringsregler kan være:

IF alder= «ungdom» THEN risikoprofil = «Høy risiko»

IF inntekt= «høy» THEN risikoprofil = «Lav risiko»

IF alder= «middelaldrende» AND inntekt = «lav» THEN risikoprofil= «Høy risiko»

Eller i markedsføring og salg:

IF alder= «ungdom» og student= «ja» THEN Sannsynlig_kjøper_av_datamaskin = «ja»

Informasjonssystemene kan også lære av erfaringsdata. Ved for eksempel å gjennomgå bankens lånehistorikk kan profilen som benyttes for å bedømme kunders risikoprofil etableres automatisk og endres etter hvert som en får mer læring. Ved å kople informasjon fra salgsoversikter til personopplysninger kan en lage modeller på hvem som er de mest sannsynlige kjøpere av et spesifikt produkt.

Det finnes en rekke teknikker for klassifisering av data, både enkle og avanserte, disse er ikke beskrevet her. Detaljert beskrivelse av disse er gjort av blant andre Han (2012).

Klustering

Klustering består i å gruppere dataobjekter i forskjellige grupper, eller klustere, slik at de objekter som har stor grad av likhet blir i en gruppe. Grupperingen skjer basert på analyser og forskjellige klusteringsteknikker. Resultatet av grupperingen kan bli forskjellig avhengig av hvilken teknikk som brukes. Det finnes en rekke forskjellige måter å gjøre klustering på som er avhengig av hva resultatet skal anvendes til.

Det forskes i dag på anvendelse av datamining på ustrukturerte store informasjonssystemer. Søkemotorer eller såkalte *Web crawlere* søker metodisk gjennom Internett for å klassifisere data og bygge opp indekser med begreper som er relatert. Dvs å etablere referansebaserte (semantiske) strukturer ut fra ustrukturerte data. For de store søkemotorene blir datamengdene som skal gjennomgås, enorme. Man benytter såkalte *computer clouds* hvor tusenvis av maskiner er programmert til kollektivt og koordinert å søke og indeksere data.

Identifisering av utliggere

En utligger er et objekt som skiller seg vesentlig ut fra andre som om det var generert av en annen mekanisme. Identifisering av utliggere og klustering er nært beslektede teknikker. Klustering finner de mønstre som gjentar seg og grupperer deretter, mens utligger identifikasjon forsøker å finne de objektene som skiller seg vesentlig ut fra alle andre. Han (2012 s.543) referer til kredittkort-selskapene som har benyttet denne metoden lenge for å identifisere korttransaksjoner som er unormale. Identifisering av utliggere kan også brukes til å overvåke sosiale media (s.545):

> *«Outlier detection is also related to novelty detection in evolving data sets. For example by monitoring a social media web site where new content is incoming, novelty detection may identify new topics and trends in a timely manner»*

Data mining for å oppdage og forhindre datainnbrudd

Hovedfunksjonen til et system som skal forhindre datainnbrudd er å identifisere ondsinnet aktivitet, logge informasjon om slik aktivitet, om mulig forhindre aktiviteten og rapportere om aktiviteten. Majoriteten av slike systemer er enten signaturbaserte systemer eller uregelmessighetsbaserte systemer. Innenfor begge disse områder kan datamining være nyttig:

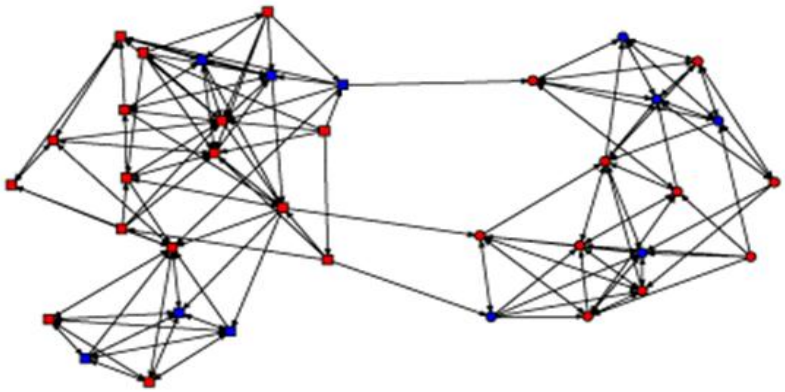
Signaturbaserte systemer er avhengig av at eksperter har definert gjenkjennbare signaturer på angrepsmønster. Systemet monitorer nettverkstrafikk for å se om signaturene gjenkjennes slik at de kan stoppes. Systemene må oppgraderes kontinuerlig etter hvert som nye signaturer blir kjent. Aktiviteter kan overvåkes og klassifiseres etter signatur som enten «normale» eller «innbruddsforsøk». Uregelmessighetsbaserte metoder bygger klustre (kalles også i sikkerhets-sammenheng «profiler») med normal «nettverksoppførsel». Datamining vil identifisere oppførsel som skiller seg ut fra profilene slik at disse kan analyseres nærmere. Datamining kan også bli brukt til å analysere mulighet for angrep fra mange forskjellige lokasjoner i et datanettverk, for eksempel i Internett.

Mønstergjenkjenning i ustrukturerte databaser er komplekst både på grunn av at det må bygges inn stor grad av tolkningsrom for mønster men også på grunn av forskjellige nasjonale reguleringer av personvern. Datamining skaper muligheter men også farer for personvernet og for datasikkerhet når metoden blir misbrukt.

2.6.14 Nettverksanalyse

Nettverksanalyse benyttes for fremstilling av alle interaksjoner mellom enheter i et avgrenset og definert sosialt felt. Punktene er enheter og linjene som forbinder enhetene, er relasjoner. Et kart kan tegnes basert på analyse av interaksjoner mellom enheter for å illustrere hvilke enheter som er de mest sentrale eller er involvert (figur 10). Enheter kan f.eks. være personer, organisasjoner og

grupper. Som del av politiets etterforskning og etterretning kan enheter like gjerne være telefonnumre, e-postadresser, bankkontoer etc. (Sætre 2007).



Figur 10: Eksempel på nettverksdiagram

Et eksempel på praktisk anvendelsen av denne metoden er Sentrum politistasjon i Oslo som har gjort gode erfaringer med dette i bekjempelsen av lommetyverier (Datatilsynet og Teknologirådet 2013 s.44):

> «*Ved å analysere mønstre som danner seg når historiske kriminalitetsdata blir lagt over på kart sammen med andre data, kunne politistasjonen raskt se nye sammenhenger mellom tid og sted for registrerte lommetyverianmeldelser og aktivitet ved bestemte utesteder. Gjennom relativt enkle grep kunne så politiet, i samarbeid med utestedene, iverksette tiltak som gjorde det vanskeligere for lommetyver å operere i området. Denne metodikken ga resultat i form av en kraftig reduksjon i anmeldte lommetyverier i Oslo sentrum*»

2.6.15 Ekspertintervju

I henhold til Sætre (2007) er en ekspert er en person som har særdeles god kunnskap innenfor et spesifikt emne eller område. Et ekspertintervju er et planlagt intervju med en slik person om emner som kan relateres til personens kunnskapsområde. Bedømming av en ekspert blir ofte gjort for å kunne angi sannsynligheter, ikke som en risikoanalysemetode i seg selv. Hvor stor vekt en legger på informasjonen en får fra en ekspert avhenger av den tillit en har til personen. For å få et inntrykk av hva en kan forvente av informasjon fra en ekspert i en analysesammenheng, er det interessant å se på hvordan politiet kvalitetsikrer og kategoriserer den informasjon som de får fra det som politiet betegner «informanter». Politiets 4x4 matrise for kvalitetssikring av informasjon er beskrevet i tabell 1. Systemet for kvalitetskontroll av informasjon fra en informant, brukes av politiet internasjonalt og er bygget opp på en slik måte at det setter karakter på kildens pålitelighet og graderer opplysningens troverdighet (Sætre 2007 s.36).

Tabell 1: Politiets 4x4 matrise for kvalitetssikring av informasjon (Sætre 2007)

Kildekode	**Definisjon**
A	Når det ikke er det minste tvil om kildens ekthet/ soliditet, pålitelighet og kvalifikasjon, eller hvis opplysningen kommer fra en person som før har bevist at han er pålitelig på alle måter.
B	En kilde som tidligere har gitt opplysninger som på de fleste måter har vist seg å være pålitelig.
C	En kilde som tidligere har gitt opplysninger som i de fleste tilfeller har vist seg å være pålitelige.
X	I tilfeller av tidligere uprøvde kilder der det er tvil om ekthet, pålitelighet eller kvalifikasjoner til kilden.
Opplysnings-kode	**Definisjon**
1	Når opplysningen kan sies å være korrekt uten noen som helst reservasjon.
2	Når kilden personlig har kommet til kunnskap om opplysningene, men hvor politiet ikke direkte har fått disse.
3	Når kilden ikke personlig har fått kunnskap om opplysningene, men der de understøttes av allerede registrerte opplysninger.
4	Når kilden ikke personlig har fått kunnskap om opplysningene, og de ikke kan understøttes på noen måte.

2.6.16 Valg av risikoanalysemetode

Wiencke m.fl. (2006) sier at forskjellige beslutningssituasjoner nødvendiggjør forskjellige analysemetoder for informasjonssystemer. Et helhetlig rammeverk som dekker både villede og ikke-villede hendelser, beskrives. Rammeverket gir veiledning til å velge passende metode for forskjellig typer beslutningssituasjoner og som reflekterer forskjellig nivå på mulige konsekvenser og assosiert usikkerhet. Valg av metode gjøres ut fra en fast prosedyre (Wiencke m.fl. 2006 s.2300):

1. Evaluering av forventet konsekvens relatert til feil i informasjonssystemet og sannsynligheten for at feilen vil inntreffe
2. Mapping av resultatet til en risikomatrise basert på et forhåndsdefinert sett med regler (Benevnes Matrise 1)
3. Vurdering av faktorer som kan forårsake store avvik mellom forventede verdier og de virkelige konsekvenser
4. Mapping av resultatene til en ny risikomatrise (Matrise 2). Denne matrisen gir en indikasjon på om en bør bruke en mer eller mindre detaljert tilnærming enn angitt i Matrise 1
5. Vurdere rammebetingelser (Eks. faktorer som tid, ressurser, tilgjengelig informasjon)

6. Diskutere den anbefalte metode ut fra de rammebetingelser som er identifisert
7. Konkludere på type metode
8. Velge spesifikk metode

2.6.17 Oppsummering av delkapitlet

Tabell 2 gir en kort oppsummering av de metoder som er gjennomgått.

Tabell 2: Oversikt over de metoder som er gjennomgått

Fra område	Navn på metode	Beskrivelse
«Klassiske» risikoanalyse-metoder	Grovanalyse	Begrepet grovanalyse relaterer seg til en analysemetode som kan gjennomføres med en relativt beskjeden arbeidsinnsats. På en systematisk måte gjennomgås enten hele eller deler av «*bow-tien*» (se figur 1) og en identifiserer mulige uønskede hendelser, mulige årsaker og konsekvenser. Sjekklister kan brukes til å planlegge og forberede gjennomganger, intervju eller tilsvarende. Sjekkliste, som teknikk, består i hovedsak i å forberede, tenke gjennom viktige momenter en ønsker å få klarlagt og kunne sjekke ut at en har fått svar på de spørsmål en har listet (Aven 2008).
	Feiltreanalyse (FTA)	I en feiltreanalyse er utgangspunktet en ikke ønsket feil-situasjon (hendelse). Mulige årsaker til denne modelleres med et feiltre. Grafiske symboler brukes for å vise sammenhenger (Aven 2008).
	Hendelsestreanalyse (ETA)	I en hendelsestreanalyse vurderes kvalitativt og også (om ønsket) kvantitativt, mulige konsekvenser som en initierende hendelse kan medføre. Det etableres ofte en konsekvensmatrise for å visualisere mulige hendelsesforløp (Aven 2008).
	FMEA (Failure Modes and Effekt Analysis)	En metode som innebærer en systematisk gjennomgang av hver enkelt systemkomponent og som analyserer hva som skjer dersom denne svikter (Aven 2008).
	Sikker Jobb Analyse (SJA)	En sikker jobb analyse gjennomføres ved å dele arbeidet opp i deloppgaver og så foreta en analyse av hver oppgave (Aven 2008).
	HAZOP (Hazard and Operability analysis)	Ved hjelp av ledeord som «ikke/ingen, mer mindre, deler av, mer enn, motsatt, andre/annerledes» avklares hvordan ulike kombinasjoner av hendelser og prosessforhold som isolert sett er ufarlige, kan innebære en risiko (Aven 2008).
	Bayesiansk nettverk	Et bayesiansk nettverk består av hendelser representert med noder og piler(avhengigheter). Det brukes både til kvantitative og kvalitative analyser. Bayesianske nettverk er mer generelle enn hendelsestrær og feiltrær, og har vist seg hensiktsmessige i forbindelse med analyse av komplekse årsaksforhold. (Aven 2008)
«Spesialiserte»	KITHs risikoanalyse-	Kompetansesenter for IT i helse- og sosialsektoren sin metode for risikoanalyse av i hovedsak sikkerhetsy aspekter

IT-metoder	metodikk	med informasjonssystemer (Aksnes mfl. 2000).
	RANDS VAM	RAND (en forskningsorganisasjon som leverer tjenester til det amerikanske forsvar). VAM (*Vulnarability Assessment and Mitigation*) beskriver sikkerhetsteknikker for å redusere sårbarhet i informasjonssystemer (Anton m.fl. 2003).
	CORAS[6]	CORAS er et eget rammeverk for modellbasert risiko-analyse av informasjonssystemer, og spesifiserer et eget modellspråk basert på UML (*Unified Modelling Language*) (Lund 2011).
Metoder fra informasjons-kvalitet	Data profilering	Data profilering er en metode for å analysere et strukturert eller et ustrukturert informasjonssystem og samle statistikk og informasjon om dataene. Statistikk og informasjon om struktur, innhold, relasjoner og regler i dataene kartlegges (Lindsey 2008).
	ISO-8000 Information Quality Management	Når klare regler er definert for strukturen eller innholdet i et informasjonssystem kan kvaliteten på dataene som er lagret, måles mot slike metadata (Benson 2009).
Metoder fra andre områder (økonomi, etterretning, politi, forsvaret)	Datamining	Datamining brukes for å lete etter struktur og mening i store informasjonsmengder. En typisk måte å lete etter data på er å søke etter forhåndsdefinerte mønstre i dataene. Et mønster kan være et navn, adresse, nummer, el. Datamining gjør det mulig å kombinere data fra flere kilder for rapportering og analyse (Han 2012).
	Nettverksanalyse	Nettverksanalyse er basert på en samling informasjon om forbindelser mellom personer eller andre enheter. Nettverket tegnes som et kart hvor man for eksempel kan illustrere hvem som kommuniserer med hvem, hvor ofte og på hvilken måte. Nettverksanalyse benyttes innen en rekke fag som antropologi, sosiologi, økonomi, og har en særstilling innen sosialt arbeid og psykologi i form av nettverksterapi (Sætre 2007).

[6] CORAS var et EU-finansiert forskningsprosjekt med SINTEF og Telenor i koordinerende roller. Programvare og metodikk blir nå vedlikeholdt av SINTEF (Sivertsen 2007)

2.7 ULYKKESPERSPEKTIVER

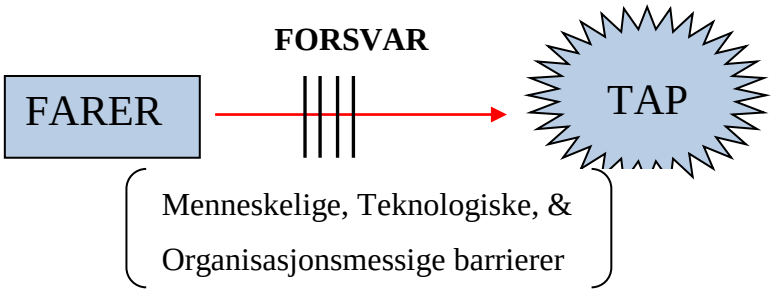
De teoretiske perspektivene på hvorfor ulykker skjer og som vil bli brukt som referansegrunnlag i oppgaven, er:

- Energi-/barriereperspektivet
- Informasjonsprosesseringsperspektivet
- Høypålitelige organisasjoner (*High Reliability Organizations (HRO)*)
- Normale ulykker (*Normal Accidents*)
- Beslutningsperspektivet (*Conflicting Objectives*)
- Menneskelige faktorer (*Human Factors*)

Perspektivene har vært gjennomgått og brukt som referansegrunnlag i flere fag ved studiet *Master i risikostyring og sikkerhetsledelse* ved UiS. Ikke minst i fagene *Granskningsmetodikk* og *Risiko, sikkerhet og sårbarhet*. Perspektivene er kort beskrevet i de følgende delkapitler.

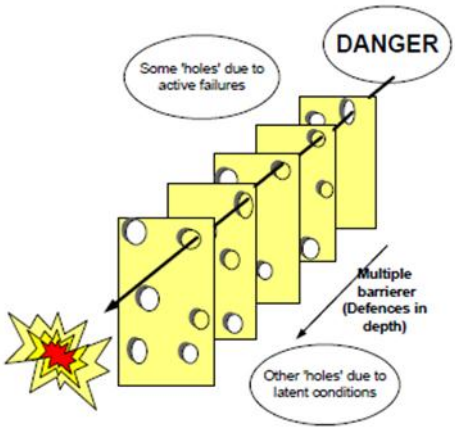
2.7.1 Energi-/barriereperspektivet

I Energi-/barriereperspektivet fokuseres det på at ulykker kan forhindres ved å fokusere på farlige energimengder (for eksempel vekt, trykk, varme, eksplosjoner) og tiltak (barrierer) for å skille disse fra sårbare elementer (mennesker, utstyr, miljø). Premissen er at systemet kan forstås som en fast struktur av definerte elementer, men med hendelser drevet fram av «energi på avveie» som den dynamiske komponenten i systemet. En feil som ligger latent og som en ikke er klar over, blir utløst ved en helt spesiell kombinasjon av årsaker. En annen mulighet er også at en er bevisst risikoen, og har akseptert å leve med den. Dersom en er bevisst på at ulykken kan skje, kan en strategi for å redusere risikoen enten være å redusere selve farekilden (energimengden) eller å etablere barrierer (f.eks. brannvegger, se figur 11) for å avskjære eller dempe hendelsesforløp (Haddon 1980 i Rosness 2004). Med barrierer forstås her tiltak og funksjoner som er planlagt for å bryte et spesifisert uønsket hendelsesforløp (Rosness 2004). En barrierefunksjon må forståes i et MTO-perspektiv (Menneske, Teknologi, Organisasjon). En enkelt barriere trenger ikke gi tilstrekkelig sikkerhet fordi hverken mennesker eller systemer er feilfrie. Noen ganger er det hensiktsmessig å etablere et forsvar i dybden, se figur 12 (Reason 1997). Svikter en barriere står neste klar til å ta over.



Figur 11: Energi-/barriereperspektivet

Gevinsten med å legge til flere barrierer avtar imidlertid dersom det er sterk avhengighet mellom barrieren (dvs to eller flere barrierefunksjoner settes ut som følge av et enkelt forhold). For at forsvar i dybden skal være mest mulig effektivt er derfor uavhengighet mellom barrierene et viktig prinsipp. Perspektivet er sentralt fordi det er grunnlag for etablering av de sentrale sikkerhets-systemer i for eksempel prosessindustrien og atomkraft (Rosness 2004). Perspektivet er mest relevant for systemer der den tekniske kjernen og farekildene er veldefinerte med hensyn til komponentegenskaper og sammenhenger, systemet er fysisk avgrenset og forholdsvis stabilt. I den senere tid er Energi-/barriereperspektivet blitt stadig utvidet til å omfatte ikke bare teknologi (T-en) i et MTO-forhold, men også menneskelige (M) og organisatoriske (O) faktorer. Menneskelige handlinger kan være både feilkilder og barriereelementer, mens organisatoriske faktorer gjerne er bakenforliggende (latente) betingelser for teknologiske og menneskelige elementer (Reason 1997).

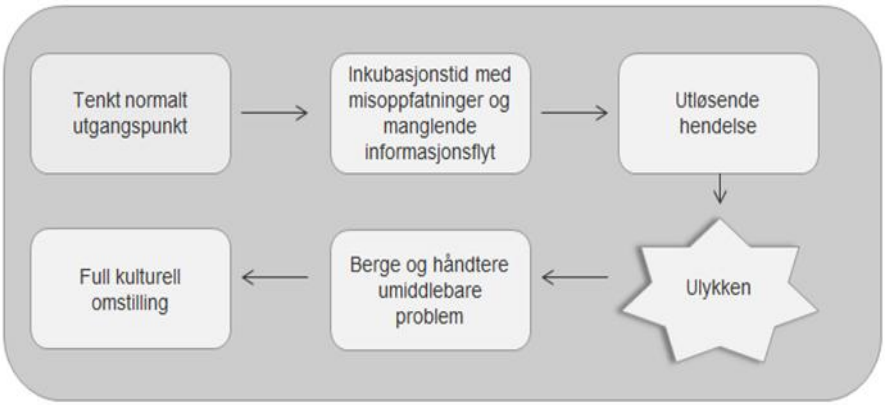


Figur 12: Reasons "sveitserost modell" illustrerer hvordan alle "åpninger" i flere barrierer kan være posisjonert slik at de er samtidig gjennomtrengbare (Reason 1997)

2.7.2 Informasjonsprosesseringsperspektivet

Dette perspektivet har Turners (1978) teori om menneskeskapte ulykker *(Man-Made Disasters*) som utgangspunkt. Turners poeng er at selv om ulykker fremstår som fundamentale overraskelser der og da, så finner granskinger i etterkant ofte både forstadier og advarsler som er blitt oversett. Disse fremstår som «åpenbare» i etterpåklokskapens klare lys. Ulykken er altså en kulminasjon av latente feil og hendelser som ikke blir oppfattet fordi kultur og sosiale normer hindrer oppfattelsen av dem. En ulykke kan i følge Turner, sees på som en prosess med seks faser som illustrert på figur 13. I henhold til dette perspektivet blir derfor årsakene nødvendigvis hverken at informasjons-systemet har feilet eller at noe har gått galt. Manglende informasjonsflyt og/eller feiltolkninger hindrer oppfattelsen av at avvik oppstår, utvikles og akkumuleres i det som betegnes hendelsens inkubasjonstid. For strenge tilgangsrestriksjoner og misoppfatninger av hva som er gjeldende regler

for informasjonsutveksling kan også forårsake at beslutningstagere ikke får tilgang til nødvendig informasjon til å foreta de beste beslutninger.



Figur 13: Faser i utviklingen av en ulykke iht. informasjonsbehandlingsperspektiv (Turner 1978)

Manglende opplæring, hindringer i å kombinere informasjon eller mangelfull trening i å bruke informasjonssystemene riktig, er også typiske karakteristikker på risiko i forhold til informasjonsprosesseringsperspektivet. I enkelte tilfeller kan det være et problem at det er for mye informasjon tilgjengelig slik at det vesentlige drukner i den store mengden (Rosness 2004).

Tabell 3: Typologi på hvordan forskjellige organisasjonskulturer behandler informasjon. Westrum (1993 i Rosness 2004)

Patologisk	Byråkratisk	Generativ
Vil ikke vite	Finner kanskje ikke ut	Søker aktivt etter informasjon
Budbringere blir skutt	Dersom de står frem blir de hørt på	Budbringere blir trent opp
Ansvar blir unngått	Ansvar er fordelt på områder	Ansvar er delt
Brubygging er ikke populært	Brubygging er tillatt men blir neglisjert	Brubygging blir belønnet
Feil medfører straff eller blir skjult	Organisasjonen er rettskaffen og barmhjertig	Undersøkelser og justeringer
Nye ideer blir motarbeidet	Nye ideer representerer problemer	Nye ideer ønskes velkommen

Dette er et økende problem med den eksponentielt økende informasjonsmengden vi erfarer i dag. I tillegg til at informasjon blir gjort tilgjengelig må også organisasjonen være i stand til å forstå hva informasjonen betyr og kunne handle deretter. Informasjonsflyt i en organisasjon bidrar derfor til å gjøre organisasjoner i stand til å nyttiggjøre seg informasjon, observasjoner og ideer uansett hvor de finnes i systemet, uten hensyn til plassering og status til person eller posisjon. Dette kan dreie seg

om alt fra å videresende mail, publisere informasjon på Internett, sørge for at informasjonssystemet er oppdatert med tidsriktig informasjon og at de som har behov for det har tilgang til informasjonssystemet når og hvor det er behov for det. Westrum (1993 i Rosness 2004) beskriver stereotyper på organisasjonsformer for å vise hvordan forskjellige organisasjonskulturer responderer på og behandler informasjon. Dette er oppsummert i tabell 3.

2.7.3 Teorien om Normale ulykker (*Normal Accidents*)

Charles Perrows teori om Normale ulykker (Perrow 1984) er grunnlaget for dette perspektivet. Perspektivet forklarer storulykker som et misforhold mellom egenskapene til teknologien og organisasjonen som er ansvarlig for å kontrollere den. Perrow definerer løse og tett koplede systemer, hvor et tett koplet system består av deler som er gjensidig avhengig av innbyrdes tilgjengelighet. Hele systemet kan bli inaktivt hvis en del feiler. Perrow (1984) definerer også interaksjonene i et system som enten lineære eller komplekse. Lineære interaksjoner består av deler, enheter og sub-system som er direkte avhengig av hverandre. Komplekse interaksjoner eksisterer når det er alternative forgreininger og løsninger i systemet. Hvis en del, enhet eller sub-system feiler er disse ikke gjensidig avhengig av hverandre og systemet vil kunne fungere likevel. Det kan eksistere avhengigheter i systemet som er lite synlige eller ikke planlagte. Perrow anbefaler forskjellige strategier med hensyn til optimal organiserings i en organisasjon, avhengig av hvilke teknologiske utfordringer en står ovenfor. Dette er vist i tabell 4. Rosness (2004) mener at i tilfeller hvor det både er en tett kopling og en kompleks interaksjon eksisterer det en konflikt, sentralisert organisering for å håndtere tett kopling og desentral for å håndtere uventede interaksjoner kan ikke eksistere samtidig.

Tabell 4: Organisering for kopling og kompleksitet (Perrow 1984)

Interaksjon / Kopling	Lineær	Kompleks
Tett	Sentraliser for å håndtere tett kopling	Sentraliser for å håndtere tett kopling og desentraliser for å håndtere uventede interaksjoner
Løs	Sentraliser eller desentraliser Begge vil virke	Desentraliser for å håndtere uforutsette interaksjoner

Systemet vil være kandidat for en «Normal ulykke». Denne teorien har provosert mange hovedsakelig fordi den konkluderer med at noen teknologier bør forlates i sin nåværende form fordi de ikke lar seg tilstrekkelig kontrollere av en organisasjon (Rosness 2004).

2.7.4 Høypålitelige organisasjoner (*High Reliability Organizations*)

Teorien om høypålitelige organisasjoner ble utviklet delvis som en reaksjon på utfordringen gitt i teorien om Normale ulykker (Rochlin m.fl. 1987 i Rosness 2004; LaPorte og Consolini 1991 i Rosness 2004). Teorien om høypålitelige organisasjoner er basert på studier av organisasjoner som har vist evne til å håndtere komplekse og krevende teknologier uten store ulykker. Sentrale elementer er kunnskapen om organisatorisk redundans og evne til spontan strukturendring som tilpasning til kriser og plutselige belastningstopper. Ingeniører bygger inn duplikate komponenter og utstyr i tekniske systemer for å forebygge fatale hendelser. Tilsvarende vil organisasjoner med innebygd duplisering av funksjoner, kunne oppnå en bedre toleranse for feil. Dette tilstrebes ofte i høypålitelige organisasjoner for eksempel ved at personell overlapper hverandre med hensyn til kompetanse og arbeidsoppgaver. Rosness (2004) betegner denne måten å forebygge feil på som organisatorisk redundans, og beskriver forholdet som samhandlingsmønstre som tillater organisasjonen som et hele å opptre mer pålitelig enn operatørene hver for seg. For å oppnå organisatorisk redundans må både de strukturelle (f.eks. bemanning, arbeidsoppgaver) og kulturelle forhold i organisasjonen ligge til rette. LaPorte og Consolini (1991 i Rosness 2004) mener at mange høypålitelige organisasjoner har evne til spontan omstrukturering i spesielle situasjoner. Kultivering av mangfoldighet er en karakteristikk som blir brukt. Det samme er beslutningsmigrasjon fra makt/ politikk til ekspertise som skifte av lederskap i krise- og problemsituasjoner i henhold til den grad av ekspertise, myndighet, fullmakter, hybridisering mellom hierarki og spesialisering som er best egnet til å håndtere den gitte situasjon.

Begrepet «*mindfulness*» [7] ble utviklet for å fange karakteristika ved samhandlingsmønstre i høypålitelige organisasjoner (Weick og Sutcliffe 1993 i Rosness 2004). Årvåkenhet innebærer at sikkerhet og pålitelighet betraktes som dynamiske ikke-hendelser der håndtering av det uventede blir vesentlig. Sikkerhet og pålitelighet er ikke en statisk størrelse som kan bygges inn i organisasjonen, men oppnås gjennom interaksjon, oppmerksomhet, kommunikasjon og kompetanse. I følge Weick og Sutcliffe (1993 i Rosness 2004) omfatter begrepet årvåkenhet følgende dimensjoner:

[7] Det engelske ordet «*Mindfullness*» kan oversettes til årvåkenhet, oppmerksomhet eller omhyggelighet. I denne rapporten er det valgt å bruke ordet årvåkenhet.

Fokus på feil. Betrakte feil som viktige symptomer. Fokus skal være på læring av feil og av nestenulykker. Hendelsesgjennomganger og -analyser, rapporteringskultur og åpenhet er viktig. Det samme er stor grad av trening for kontinuerlig oppdatering av kunnskap om systemet.

Motstand mot å forenkle. Fokus på et fullstendig og nyansert bilde for å håndtere det usikre og uventede. Kontekst, differensiering og konstant interaksjon gir et rikere og variert bilde av potensielle konsekvenser. Heterogene grupper gir ulike perspektiver. Troverdighet, tillit, mellommenneskelige relasjoner er viktige.

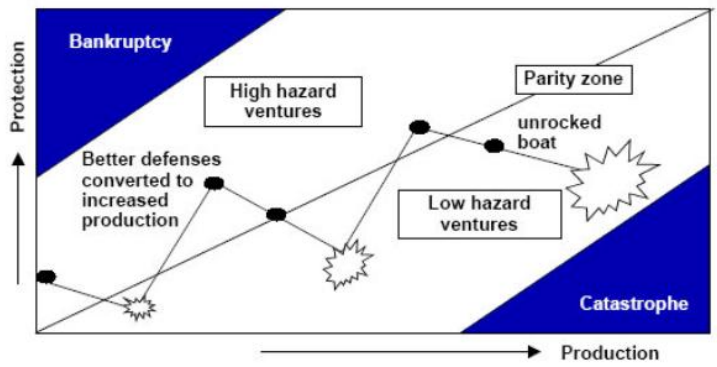
Fokus på drift. Stor grad av oppmerksomhet og åpenhet vedrørende symptomer og latente feil i systemer. Velutviklet situasjonsbilde. Redusert forskjell mellom operativt, taktisk og strategisk nivå med dreining mot operativt nivå. Hyppige driftsmøter, direkte kontakt/ interaksjon, spredning av operasjonelle ytelsesmål.

Satsing på robusthet. Unngå at feil i systemene blir lammende. Intelligente reaksjoner og improvisasjon er viktig. Kunnskap, erfaring, kombinasjon, trening, simulering av *worst case* scenarier. Det å kunne belyse og analysere en problemstilling fra flere synsvinkler inkludert å benytte uformelle nettverk for å få informasjon, er viktige for å oppnå et robust system.

Respekt for ekspertise. Kultivering av mangfoldighet. Se på systemer fra mange forskjellige synsvinkler som funksjonalitet i forhold til forskjellige brukergruppers behov, drifts- og sikkerhets-aspekter, ledelsens behov for innsyn og kontroll, etc.

2.7.5 Målkonfliktperspektivet (*Conflicting objectives*)

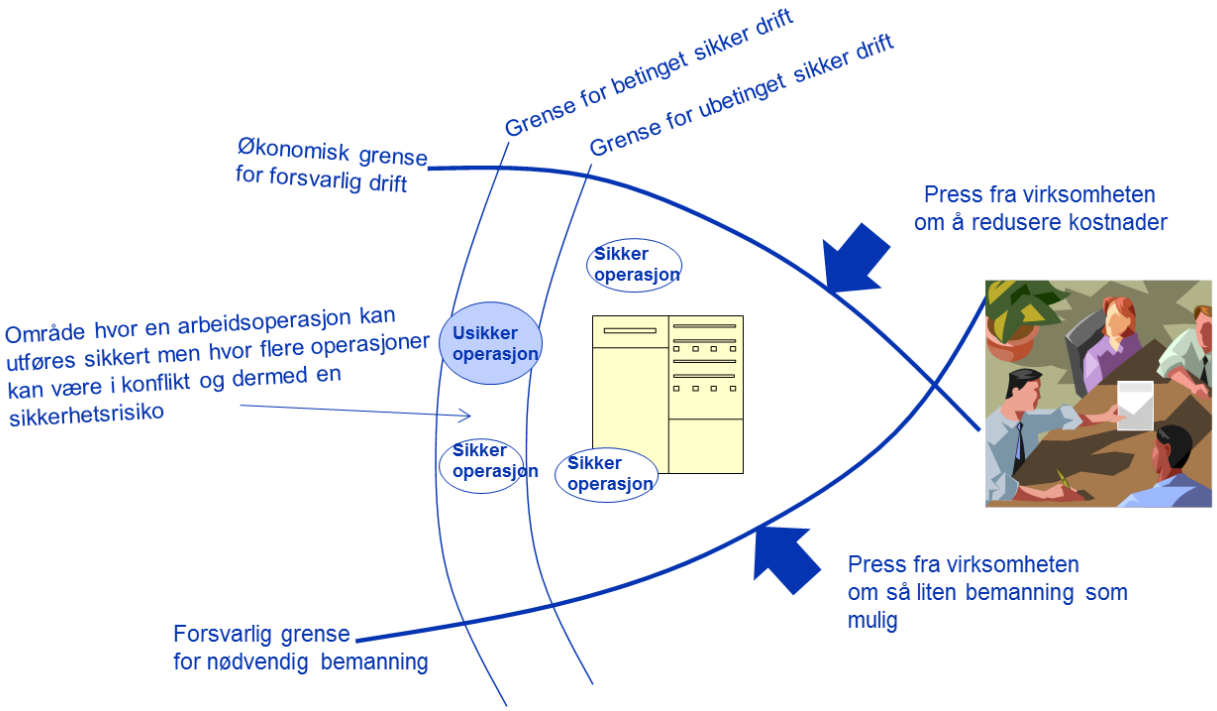
Sammenhengen mellom tid, kostnader og det å skape resultater er essensielle element i organisasjonsstyring og i prosjektstyring. Målkonfliktperspektivet fokuserer på disse målkonflikter og at dette er et essensielt element i risikostyring. Mangel på eller fravær av en sentral beslutningstaker med full oversikt som fatter beslutninger (Rasmussens 1997 i Rosness 2004) der aktiviteter drifter mot grensen for sikker drift er også et sentralt element.



Figur 14: Konflikten mellom beskyttelse og produksjon (Reason 1997)

Perspektivet viser hvordan mål for sikkerhet og profitt kan være i konflikt og derved kan bidra til at ulykker skjer, samt at god ledelse er essensielt for å oppnå høy grad av sikkerhet. En organisasjons ledelse påvirker i hovedsak sikkerhet med måten ressurser fordeles mellom produksjon og sikkerhet (beskyttelse). En riktig balanse mellom produksjon og beskyttelse er nødvendig. For mye beskyttelse er ikke alltid det beste som illustrert i figur 14.

Svært ofte dreier anskaffelse av et nytt informasjonssystem seg om utvikling av et system som skal være skreddersydd organisasjonen. Det betyr mye utvikling og press på budsjetter og tidsplaner for å bli ferdig. Ofte har man ikke full oversikt over all funksjonalitet som er ønsket når informasjonssystemet planlegges. Man lærer etter hvert som systemet materialiserer seg og budsjettene må økes. I en del tilfeller pålegges nye krav fra organisasjonen eller fra myndighetene som fører til endringer i spesifikasjoner og planer. Konflikter mellom individers, organisasjonens og myndighetenes krav kan oppstå og må håndteres i et utviklingsprosjekt. I noen tilfeller er det behov for og sterkt press på å få løsninger i drift uten at de er fullgodt testet og ikke klare for produksjonssetting. Feil kan oppstå med påfølgende kostbar brannslukking. Det har også vist seg vanskelig å styre IT utviklingsprosjekter innenfor planlagt gjennomføringstid og budsjett. Det finnes mange eksempler, ikke minst fra offentlig virksomhet (Statskonsult 1998). Figur 15 er en illustrasjon som viser hvordan forskjellige drivere kan påvirke grensene for sikker operasjon i en bedrift.



Figur 15: Mål som er i konflikt med hverandre i en organisasjon kan forårsake usikre operasjoner

Sivertsen (2007) sier at sikkerhetsarbeidet innenfor en organisasjon vil møte motstand fra flere miljøer. Eksempler på dette kan være:

- Ledere, siden ekstra sikkerhet kan gi dyrere løsninger uten synlige resultater i hverdagen.
- Ansatte, siden sikkerhetstenkningen kan ødelegge for funksjonelle løsninger.
- Drifts- og sikkerhetsansvarlige, siden ekstra sikkerhetskrav fører til merarbeid og legger beslag på allerede knappe ressurser

Ressursene til sikkerhetsarbeid vil normalt være begrenset, og det må argumenteres godt for at tiltak som innføres bidrar til økt sikkerhet. Da er det behov for metodikker som peker på de viktigste sikkerhetsutfordringene for organisasjonen, og som gjør det mulig å prioritere mellom tiltak. En risikoanalyse kan bidra til dette.

2.7.6 Menneskelige faktorer (*Human factors*)

Ifølge Sidney Dekker (2006) er det i hovedsak to måter å se menneskelige feilhandlinger på. Den første måten er kjent som *The Old View* eller *The Bad Apple Theory*. Dette innebærer at komplekse systemer hadde klart seg fint dersom det ikke hadde vært for upålitelige mennesker (B*ad Apples*). Menneskelige feil generer 2/3 av alle ulykker. Feil som skjer i en organisasjon, blir i henhold til dette perspektivet, introdusert gjennom handlinger fra de ansatte. *The New View* forkaster *The Bad Apple Theory* siden en menneskelig feil ikke nødvendigvis er ensbetydende med den bakenforliggende årsaken til en ulykke (Dekker 2006). Menneskelige feil er en følge av eller et symptom på alvorligere og dypere feil i systemet. Menneskelige feil er ikke tilfeldige, men er koblet til funksjoner i menneskers verktøy, oppgaver og operative miljø. Menneskelige feil er ikke årsaken til en hendelse, men et naturlig startpunkt for en eventuell gransking. Man må se på erfarte menneskelige feil som et problem som alle som opererer systemet kan bli utsatt for. Feilen blir en «markør» på mulige hendelser i informasjonssystemet og en mulighet til å lære mer om hvordan disse kan forebygges.

3 METODE

I dette kapittelet beskrives de metodene som er valgt for å besvare forskningsspørsmålene i oppgaven. I tillegg vil alternative fremgangsmåter og avgrensninger som er blitt gjort i oppgaven, bli diskutert.

3.1 METODER BENYTTET

En dokumentgjennomgang vil bli gjort for å etablere forståelse for definisjoner av de begrepene som er sentrale i oppgaven. Det blir primært forsøkt å bruke definisjoner anvendt i pensum-litteraturen i det erfaringsbaserte studie *Master i risikostyring og sikkerhetsledelse* ved UiS eller som er gitt i offentlige standarder. Det gjennomgås et utvalg vitenskapelige artikler for å kunne relatere til oppdatert og aktuell tolkning av noen av de brukte begrepene. Spesielt gjelder dette diskusjonen om risikobegrepet i avsnitt 2.2.3. Referansemodellen for risikoanalysens ulike trinn som er hentet fra Aven (2008), anses hensiktsmessig for de videre diskusjonene i oppgaven.

Ved å ta utgangspunkt i noen generelle perspektiver på hvorfor ulykker skjer, og relatere disse til mulige ulykker i eller med informasjonssystemer, blir det forsøkt å etablere en forståelse for typer risiko som kan forekomme og hva som karakteriserer risiko i informasjonssystemer.

Eksemplene som brukes i oppgaven er hentet fra noen utvalgte ulykker hvor informasjonssystemer har spilt en sentral rolle i hendelsen. Innledningsvis blir en rekke eksempler på slike hendelser kort gjengitt for å gi en introduksjon til hva som menes med risiko i informasjonssystemer. I empiridelen vil et utvalg av disse bli gjennomgått mer detaljert. Beskrivelsen av ulykkene er hentet fra forskjellige kilder. De fleste er fra offisielle granskningsrapporter. I noen av eksemplene er ulykkene beskrevet i tilgjengelig litteratur og artikler og i ett eksempel (tilfellet «David») er hendelsen hentet fra en avisartikkel. Eksemplene er valgt ut fra en motivasjon om å få belyst at ulykker hvor informasjonssystemer er sentrale, kan få svært store konsekvenser. For å få bredde i diskusjonene blir det inkludert eksempler fra flere bransjer. Det er valgt å benytte MTO-metodikken med tilhørende diagram for å analysere eksemplene og for å få en lettoversiktlig, strukturert og felles presentasjon av dem. I vedlegg A er det tatt med en kortfattet introduksjon til MTO-metodikken og de symbolene som er brukt i diagrammene.

Beskrivelse av risikoanalysemetodene hentes fra diverse litteratur og i noen tilfeller fra artikler som er tilgjengelig på Internett.

Karakteristikker på typisk risiko i informasjonssystemer avledes med utgangspunkt i ulykkes-perspektivene. Det diskuteres hvilke metoder som vil være best egnet til å analysere risiko relatert til de forskjellige ulykkesperspektivene. Diskusjonen summeres opp i et anbefalt rammeverk og et

forslag til hvordan man velger riktig analysemetode ut fra den beslutningssituasjonen som eksisterer. Det anbefalte rammeverket blir så prøvd og drøftet mot eksemplene. Det blir diskutert om metodene, dersom de var blitt benyttet, ville kunne ha bidratt til å forhindre ulykkene. Rammeverket brukes også til å identifisere og diskutere områder hvor metodedekningen ikke ansees som god nok. Dette gir en basis for å kunne diskutere om det er behov for nytenkning og utvikling av nye metoder, og hvilke det i så fall er behov for. Karakterer er gitt for å forsøke å være konkret i forhold til det inntrykk av egnethet som sitter igjen etter gjennomgangen av analysemetodene og eksemplene. Bedømmingen kan selvfølgelig diskuteres, og det vil være synspunkter på diskusjonen bak denne karaktersettingen. Argumentasjonen bak karaktersettingen blir tatt med som Vedlegg B.

Det blir forsøkt å gi besvarelse på forskningsspørsmålene gjennom drøfting og det foreslås hvordan en kan komme videre med disse.

3.2 ALTERNATIVE FREMGANGSMÅTER

En alternativ fremgangsmåte for å vurdere risikoanalysemetodenes egnethet kunne baseres på praktisk utprøving av metodene relatert til forhåndsdefinerte «*cases*». Ved å gjøre dette ville en kunne sette opp kriterier for å sammenligne egenskaper i metodene mot hverandre og gjøre en vurdering ut fra disse.

Valg av analysemetoder er gjort med utgangspunkt i de etablerte generelle metoder for risikoanalyse som er beskrevet av Aven i læreboken i *Risikoanalyse* (2008). I BAS5[8]-prosjektet ble flere andre metoder identifisert som aktuelle. BAS5-prosjektet klassifiserte disse som (Sivertsen 2007):

- Egenutviklede organisasjonsinterne risikoanalysemetodikk. Eksempler er Telenors *TeleRisk* og British telecoms *Risk Analysis Method*.
- Åpen tilgjengelig risikoanalysemetodikk. To norske eksempler er Nasjonale sikkerhets-myndighets ROS 2004 og DSBs risikoveileder for kommunene.
- Åpen tilgjengelig metodikk, spesielt utviklet for IKT-sikkerhet og ofte koblet til standarder innenfor informasjonssikkerhet. Eksempler er KITHs Risikoanalyse. Metodegrunnlag og bakgrunnsinformasjon, den franske stats EBIOS, RANDS VAM og CORAS.
- Kommersielle metoder som kan kjøpes.

Fra BAS5-prosjektets liste er noen av de åpne metodene valgt ut for å bli diskutert i oppgaven. Metoder som er organisasjonsinterne eller ikke er åpent tilgjengelige blir ikke vurdert. Flere av

[8] BAS5 (Beskyttelse av samfunnet 5) var et forskningsprosjekt med fokus på metodikk for analyse av kritisk informasjonsinfrastruktur. Prosjektet var et sammarbeid mellom en rekke forskningsinstitusjoner, universiteter/ høgskoler, departementer og direktorater, og var også støttet av Norges forskningsråd gjennom IKT-SOS (Sikkerhet og sårbarhet) programmet.

metodene på listen fra BAS5 og også andre metoder som ikke er listet her, kunne det være interessant å vurdere for å komme videre med forskningsspørsmålene

De alternative metoder som diskuteres i oppgaven er valgt ut basert på tidligere personlig erfaring. Datamining spesielt, er et omfattende område som inneholder mange spesifikke teknikker. I oppgaven er bare tre av disse diskutert (klassifisering, klustering og utliggeridentifisering). Under hver av disse gruppene igjen finnes det en rekke spesialiserte metoder for mer avansert bruk. Han (2012) er et godt startsted for den som vil studere dette nærmere.

Sammenhengen mellom metoder for kvalitetssikring og metoder for risikoanalyse er interessant i et MTO-bilde. I denne oppgaven diskuteres denne sammenhengen ut fra et risikoanalyseperspektiv. En kunne valgt det motsatte utgangspunkt å ha sett det hele fra en kvalitetsstyringssynsvinkel og diskutert hvordan risikoanalysen passer inn og kan være et bidrag i en kvalitetsstyringsprosess. Risikobasert kvalitetsstyring er blitt et begrep i mange bransjer og bedrifter, blant annet hos Forsvaret og hos Det Norske Veritas.

4 EMPIRI

I dette kapittel gjennomgås noen storulykker fra forskjellige bransjer hvor informasjonssystemer har hatt en sentral rolle. Informasjonssystemenes rolle i hendelsene er analysert med MTO-metodikken (se vedlegg A). Et MTO-diagram er inkludert i hvert eksempel og viser resultatet av denne analysen.

4.1 ARIANE 5

Dette eksempel er hentet fra *European Space Agency (ESA*) sin granskningsrapport etter ulykken med Ariane 5 bærerakett (ESA 1996).

Den 4.6.1996, 39 sekund etter oppskyting fra Kourou i Fransk Guinea, eksploderte den Europeiske Ariane 5 bæreraketten på sin jomfrutur. Ariane 5 var skreddersydd for å transportere satellitter og til å plassere dem i bane rundt jorden. Ariane programmet er et europeisk samarbeidsprosjekt under ESA. Firmaet Astrium var hovedkontraktør og benyttet seg av en rekke underleverandører. Oppskytingen var en testoppskyting, men tapet ble allikevel beregnet til 500 millioner USD.

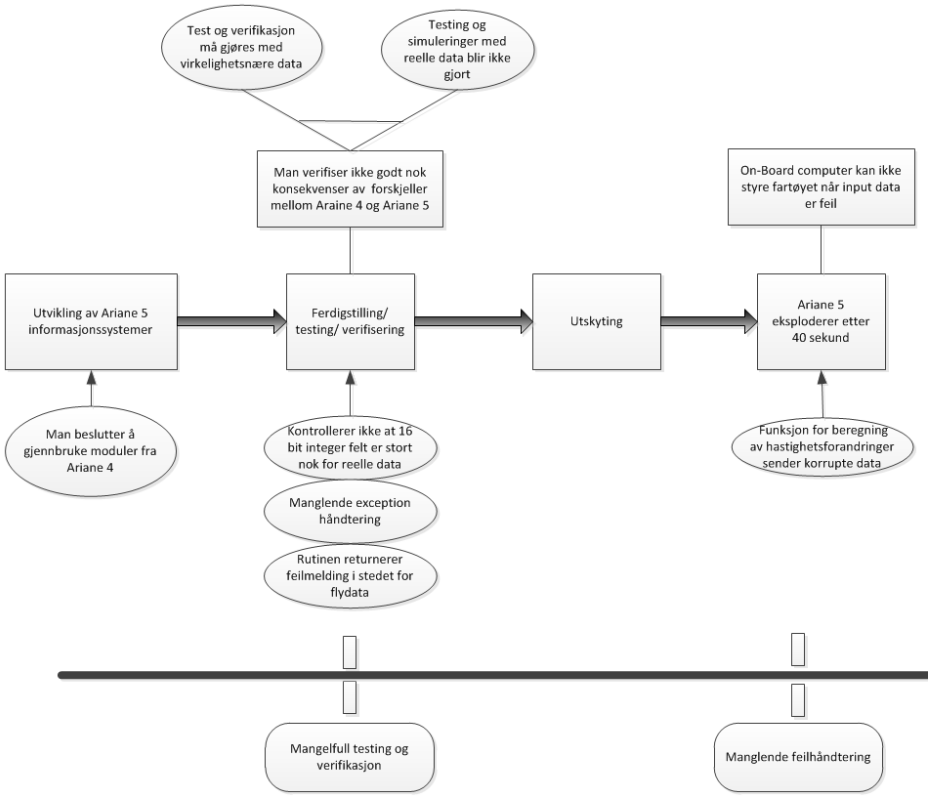
Styringen av raketten ble gjort av informasjonssystemer om bord som feilaktig beregnet at det måtte gjøres en kursendring på grunnlag av informasjon som kom fra skipets «*Inertial Reference System*» (SRI 2). Dette systemet mottar data fra gyroskop og akselerometer for å holde rede på rakettens bevegelse. Hoved-datamaskinen beregnet feilaktig at en større korreksjon av et høydeavvik måtte gjøres. Styresignaler ble sendt til ventilene på startraketten og litt senere til ventilen på hovedmotoren. En rask høydeforandring skjedde, noe som fikk fartøyet til å begynne å gå i oppløsning på grunn av de aerodynamiske krefter som det ble utsatt for. Det var også installert et redundant styringssystem som skulle ta over dersom primærsystemet feilet. Dette fungerte heller ikke på grunn av den samme feilen. SRI 2 var tidligere brukt med vellykket resultat på Ariane 4 raketter. Her opererte man med lavere hastigheter enn det som var tilfelle for Ariane 5. På grunn av at raketten kom ut av kurs ble det innebygde selvdestruksjonssystemet aktivert. Granskningsrapporten gir følgende oppsummering av informasjonssystemene sine bidrag til ulykken:

- Raketten begynte å gå i oppløsning etter 39 sekunder på grunn av 20 graders avvik på kursen.
- Kursavviket skyldes kursendring styrt av *On-Board Computer* (OBC) software på basis av data overført fra det aktive SRI 2 systemet. Deler av datastrømmen inneholdt ikke virkelige flydata men var en feilmelding fra SRI 2 som ble tolket som flydata av OBC.
- Grunnen til at feilmeldingen ble sendt var en *software exception* i SRI 2 som oppsto under konvertering fra *64-bit floating point til 16-bit signed integer variabler*. *Floating point* nummeret hadde en høyere verdi enn det som kunne representeres i en 16 *bit integer*. Denne

exception ble ikke tilstrekkelig håndtert i programkoden. Spesifikasjonen som lå til grunn for utvikling av SRI 2 var fra Ariane 4, ikke Ariane 5.

- Verdiene var mye større enn forventet siden Ariane 5 har betydelig høyere sideveis hastighet enn Ariane 4.

Granskningen viste også flere andre latente feil og konkluderte med at testing av SRI 2 hadde vært for dårlig. Feilen ble rettet og det har senere vært en rekke vellykkede utskytninger av Ariane 5 raketter. Figur 16 viser et MTO-diagram som illustrer en analyse av hendelsesforløpet når informasjonssystemenes rolle er satt i fokus. I vedlegg A er det tatt med en kort introduksjon til MTO-metodikken og forklaring på de symboler som er vist.



Figur 16: MTO-diagram av Ariane 5 ulykken

Ingen organisasjoner eller personer ble kritisert i granskningsrapporten. Men det anbefales å (ESA 1996):

- «*Give the justification documents the same attention as code. Improve the technique for keeping code and its justifications consistent*»
- *«Set up a team that will prepare the procedure for qualifying software, propose stringent rules for confirming such qualification, and ascertain that specification, verification and*

testing of software are of a consistently high quality in the Ariane 5 programme. Including external RAMS[9] experts is to be considered.»

- *«A more transparent organisation of the cooperation among the partners in the Ariane 5 programme must be considered. Close engineering cooperation, with clear cut authority and responsibility, is needed to achieve system coherence, with simple and clear interfaces between partners. »*

Kommentarene tyder på at man ikke helt har latt seg overbevise om en velfungerende organisasjon eller et prosjekt som har gjennomført de aktiviteter som en kunne forvente.

4.2 THE NASA MARS CLIMATE ORBITER

Innholdet i dette delkapittelet er i sin helhet gjengitt fra NASAs granskningsrapport etter ulykken med NASAs Mars Climate Orbiter 23.9.1999 (NASA 1999).

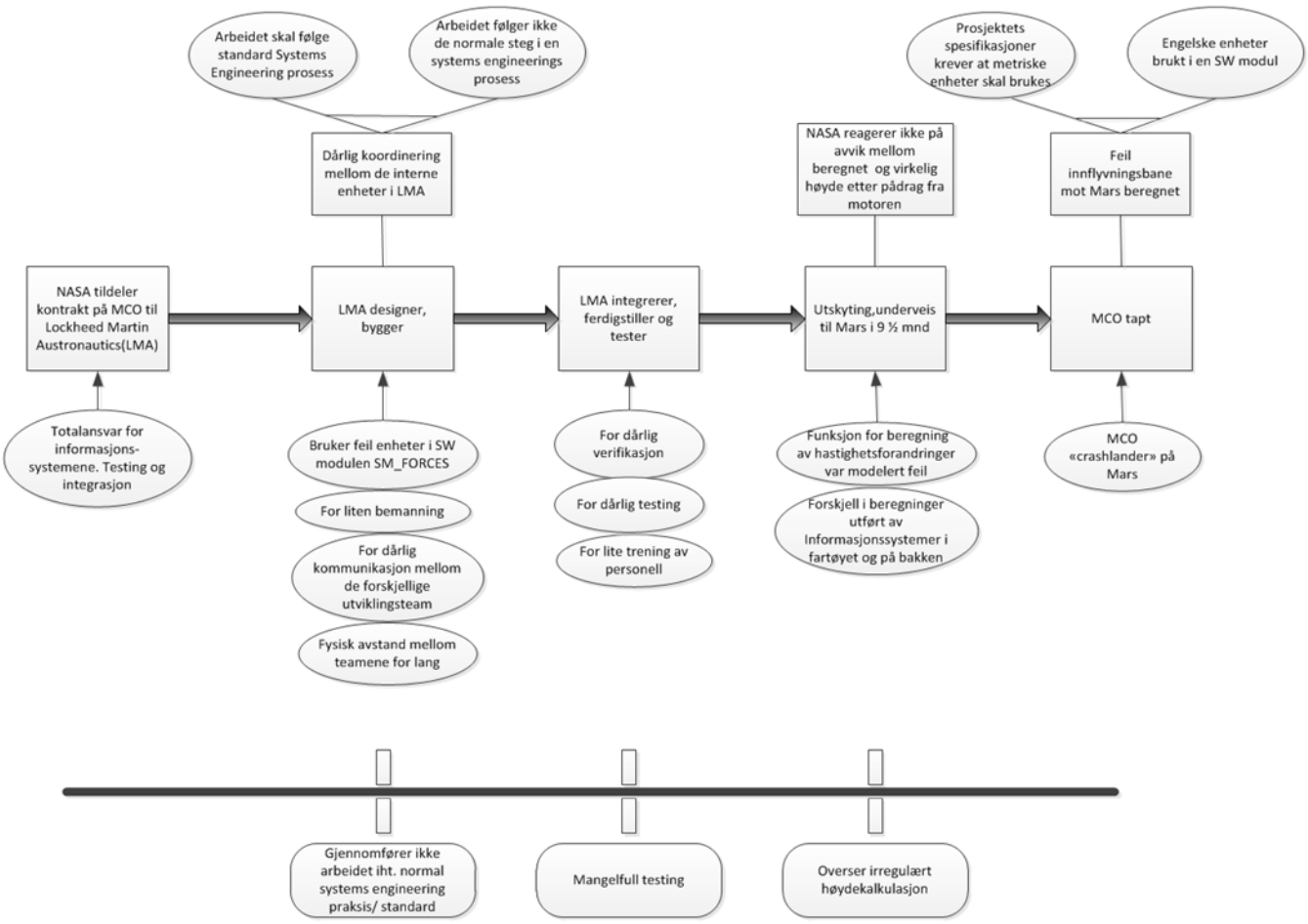
Mars Climate Orbiter var laget for å studere vær og klima på planeten Mars. Sentralt er leting etter forekomster av vann og is på overflaten til Mars. Den ble skutt opp fra Cape Canaveral Air Station i Florida, *USA* 11.12.1998. Etter å ha vært underveis i 9 ½ måned ankom den Mars. For å komme inn i bane rundt planeten før landing, ble hovedmotoren startet for å brenne i 16 minutter. Det var indikasjoner på at virkelig og beregnet høyde var forskjellig etter pådrag fra motoren, men NASAs personell reagerte ikke på denne hendelsen. Etter 5 minutter forsvant Mars Climate Orbiter bak Mars slik at NASA ikke hadde kontakt med den fra jorden. Beregnet tid til man ville oppnå kontakt igjen var 21 minutter. Men man fikk aldri mer kontakt med fartøyet og NASA erklærte det tapt 24.9.1999. Et annet fartøy Mars Polar Lander (MPL), var samtidig på vei til Mars med planlagt landing 3.12.1999. Det hastet med å finne ut om det var feil som kunne sette også dette fartøyet i fare.

Granskningsteamet konkluderte med at det var en rotårsak til ulykken. Det var brukt engelske enheter i stedet for metriske enheter i en programvaremodul *«SM_FORCES»*. SM_FORCES ble brukt til å beregne romskipets bane, og output fra denne modulen var spesifisert i prosjektets *Software Interface Specification (SIS)* til å skulle være i den metriske enheten *Newtonseconds (N-s)*. I stedet ble dataene rapportert i den engelske enheten *pound-seconds (lbf-s)*. Filen *Angular Momentum Desaturation (AMD)* inneholdt resultatdata fra SM_FORCES. SIS definerer både formatet og enhetene for AMD-filen som blir generert av bakkebaserte informasjonssystemer, men de ble ikke fulgt opp. Påfølgende prosessering av AMD filen i navigasjonsprogrammet,

[9] RAMS = Reliability, Availability, Maintaianbility and Safety

underestimerte derfor effekten av fartøyets bane med en faktor på 4.45, som er konverteringsfaktoren for kraft mellom pound og Newton. Feil bane for fartøyet ble beregnet på grunn av denne feilen i informasjonssystemet.

Utviklingen av Mars Climate Orbiter ble ledet av NASAs *Jet Propulsion Laboratory (JPL)*. JPL inngikk avtale med Lockheed Martin Astronautics (LMA) som hovedkontraktør med ansvar for design og utvikling av blant annet selve fartøyet, flysystemene, testingen og integrasjonene.



Figur 17: MTO diagram av ulykken med Mars Climate Orbiter

Granskningsteamet konkluderte også med at det var flere medvirkende årsaker til ulykken (listen under er ikke komplett):

- Hastighetsforandringer var modellert feil. De bakkebaserte informasjonssystemene brukte resultater fra SM_FORCES (pounds-seconds), mens informasjonssystemene om bord i fartøyet brukte newton-sekund for å beregne kraftpåvirkning (impuls) for hastighets-forandring. Dette var også en latent feil som man ikke var klar over.

- Det ble også stilt spørsmål til *systems engineering*-prosessen[10] som var gjennomført. Det var mange muligheter til å identifisere problemene med feil bruk av enheter i blant annet overføringen fra utvikling til drift.
- Utilstrekkelig kommunikasjon mellom teamet som jobbet med Mars Climate Orbiter utvikling og teamet som forberedte navigasjonssystemene. Teamene var isolert fra hverandre. Antagelser var gjort uten at disse var blitt bekreftet.
- Utilstrekkelig bemanning av teamet som forbereder navigasjonssystemene og for dårlig trening av personell.
- Utilstrekkelig eller ingen testing av programvaremoduler.

I figur 17 er det tatt med et MTO-diagram som illustrerer hendelsesforløpet i eksemplet for Mars Climate Orbiter etter en analyse hvor informasjonssystemenes rolle er satt i fokus.

4.3 SLEIPNER-A-ULYKKEN

Kildematerialet til dette delkapittel er hentet fra Jacobsen og Rosendahls artikkel «*The Sleipner Accident*» (Jakobsen 1994).

Sleipner-A-Platformen var en typisk betongplatform som ikke var vesentlig forskjellig fra andre platformer av «*Condeep*» typen. Den var den 12. i en serie *GBS (Ground Based Structure*) plattformer, designet og bygd av firmaet *Norwegian Contractors*. Dybden som plattformen var designet for å operere på var 82 m. Leveranser fra Sleipnerfeltet inngår i Troll gass-kontrakten som skal dekke 10 % av Vest-Europas gassbehov i 30 år. Sleipnerfeltet alene skulle dekke leveransene de første tre årene etter oppstarten som var planlagt 1.10.1993.

Under en kontrollert test av ballast i Gansfjorden 23.8.1991, oppstod en kraftig lekkasje og plattformen sank. Formålet med testingen var å sjekke for mindre lekkasjer, teste mekanisk utstyr under operative forhold og gjøre personellet kjent med driftssystemene. Ulykken skjedde mens plattformen var senket ned til 97,5 meter. 14 personer var ombord da ulykken skjedde men ingen menneskeliv gikk tapt. Ingen observasjoner av uvanlige hendelser hadde blitt rapportert før ulykken. Det ble ganske fort klart at plattformen hadde blitt så ødelagt at ingen fysisk inspeksjon ville kunne gjennomføres. Da ikke noe fysisk produkt var tilgjengelig for undersøkelse, måtte

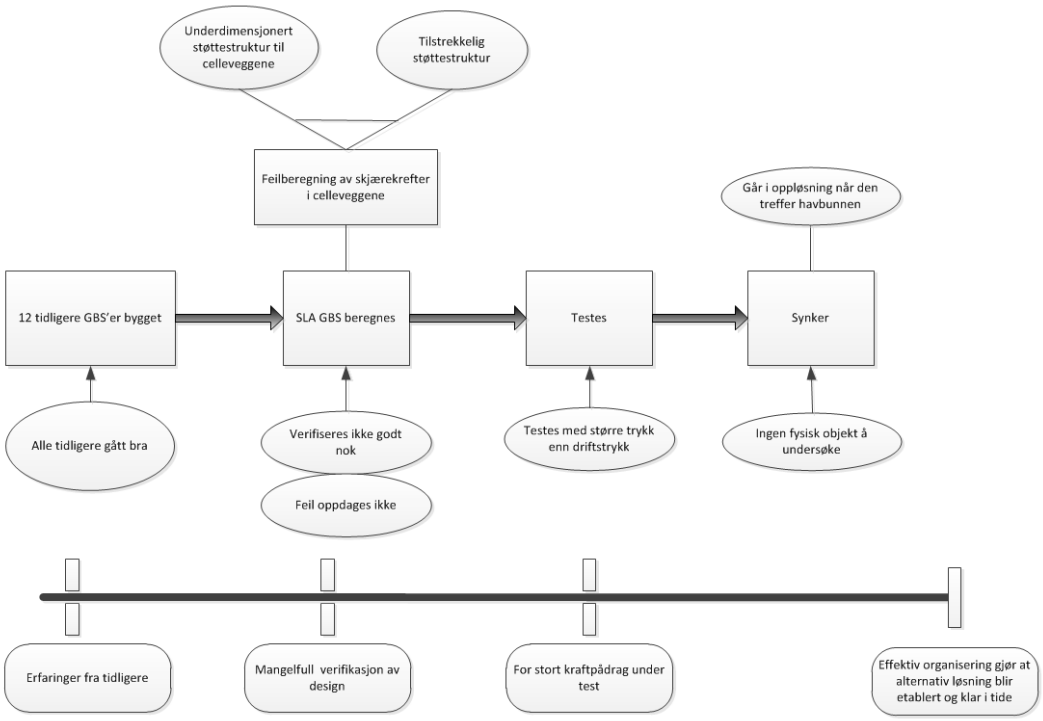
[10] *Systems Engineering* er et fagområde for å styre utviklingen av komplekse systemer. NASA's egen definisjon er (kilde: NASA NPR 7/23):

«The application of a systematic, disciplined engineering approach that is quantifiable, recursive, iterative, and repeatable for the development, operation and maintenance of systems integrated into a whole throughout the lifecycle of a project or a program»

andre arbeidsmetoder anvendes. Alle teoretisk mulige hendelser ble knyttet til vitneobservasjoner og de usannsynlige ble fortløpende eliminert. Til slutt satt en igjen med en sannsynlig hypotese som en kunne vurdere med analytiske beregninger. Det viste seg at mest sannsynlig var årsaken (Jacobsen 1994 s.191):

> *«Unfavourable geometrical shaping of some finite elements in the global analysis. In conjunction with the subsequent post-processing of the analysis result, this led to underestimation of the shear forces at the wall support by some 45 %. Inadequate design of the haunches at the cell joints, which support the tricell walls. This led to T-headed bars that were to short and the absence of stirrups in the joints.»*

Det var altså en designfeil under utformingen av støttestrukturen til veggen i en av cellene som GBSen er bygget opp av. Designfeilen førte til at det ble beregnet for lave skjærekrefter og for svak støttestruktur. *Failure Mode* tester ble utført på fullskala modeller av seksjoner av cellene og en fikk bekreftet at hypotesen som en kom frem til, var den sannsynlige årsaken.



Figur 18: MTO-diagram av Sleipner-A ulykken

Umiddelbart etter ulykken satte operatørselskapet Statoil og leverandøren i gang granskninger av ulykken. Dagen etter ulykken ble en plan for en ny plattform presentert. For å kunne overholde leveranseforpliktelsene ble den nye plattformen designet samtidig som man utførte granskningene. Det var derfor nødvendig med en rask avklaring. Det var enighet om årsaken til hendelsen. En ny GBS ble laget og var klar til å få påmontert dekkstrukturen 1.5.1993. Gass ble levert til Europa som planlagt 1.10.1993. En alvorlig ulykke ble snudd til en demonstrasjon av effektivitet og pålitelighet som olje- og gassbransjen kan hente mye erfaring og kunnskap fra.

I figur 18 er det tatt med et MTO-diagram som illustrerer hendelsesforløpet i Sleipner-A-eksemplet når informasjonssystemenes rolle er satt i fokus.

4.4 DEEPWATER HORIZON

Beskrivelsen av dette eksempel er i hovedsak hentet fra BPs «*Deepwater Horizon Accident Investigation Report*» datert 8.9.2010. Tilleggsinformasjon er hentet fra Vinnem (2011).

20.4.2010 skjedde en ukontrollert utblåsning fra *Macando*-brønnen *på* Mississipi Canyon Block 252, 66 km utenfor kysten av Louisiana, USA. Riggen Deepwater Horizon var leid av BP fra firmaet Transocean. Riggen var i ferd med å bore en letebrønn på omtrent 1500 meters dyp da ulykken skjedde. Utblåsningen resulterte i en eksplosjon og brann på riggen. Hydrokarboner strømmet til riggen i 36 timer før riggen sank. Hydrokarboner fortsatte å strømme fra brønnen i 87 dager. 11 personer mistet livet og 17 ble skadet. Forurensningene som fulgte var svært store (BP 2010).

Deepwater Horizon var utstyrt med de mest moderne, databaserte sikkerhetssystemer relatert til overvåkning av brønn, avstengning av brønn, frakopling av rigg, kraftforsyning, deteksjon og varsling av mannskap. Under ulykken sviktet alle disse informasjonssystemene helt eller delvis. Det ble i den påfølgende granskning påvist at det var kjent at flere av informasjonssystemene hadde feil og mangler og at dette var blitt ignorert og akseptert.

Granskningsteamet summerer sin hovedkonklusjon som (BP 2012 s.5):

> *«The team did not identify any single action or inaction that caused this accident. Rather, a complex and interlinked series of mechanical failures, human judgements, engineering design, operational implementation and team interfaces came together to allow the initiation and escalation of the accident»*

I tillegg blir åtte mulige hovedårsaker til ulykken oppgitt:

1. Det var svakheter i designet av den sementbarrieren som var støpt i borehullet. Denne var ikke testet og kvalitetssikret godt nok.
2. Den påmonterte bunnplaten «*Shoe track barrier*» på foringsrøret, forhindret ikke utstrømning av hydrokarboner slik den skulle.
3. Feil bedømming fra mannskapet om bord angående resultat fra negativ trykktest.
4. Innstrømning av hydrokarboner ble ikke oppdaget før disse hadde passert «*Blow Out Preventer*» (BOP) og var i stigerøret.

5. Veskestrømmen kunne ha blitt ledet overbord i stedet for til slam-gasseparatoren. Dette ville ha gitt mer tid til å stoppe utblåsningen slik at konsekvensene kunne ha blitt redusert.
6. Ved å lede veskestrømmen til «*Mud Gas*»-separatoren ble det frigitt gass som strømmet inn i plattformen
7. Brann- og gass-systemene forhindret ikke antennelse av hydrokarbonene
8. BOP fungerte ikke som forventet og var ute av stand til å tette brønnen. Teamet påviste indikasjoner på feil i testregimet og vedlikeholdssystemet for BOP.

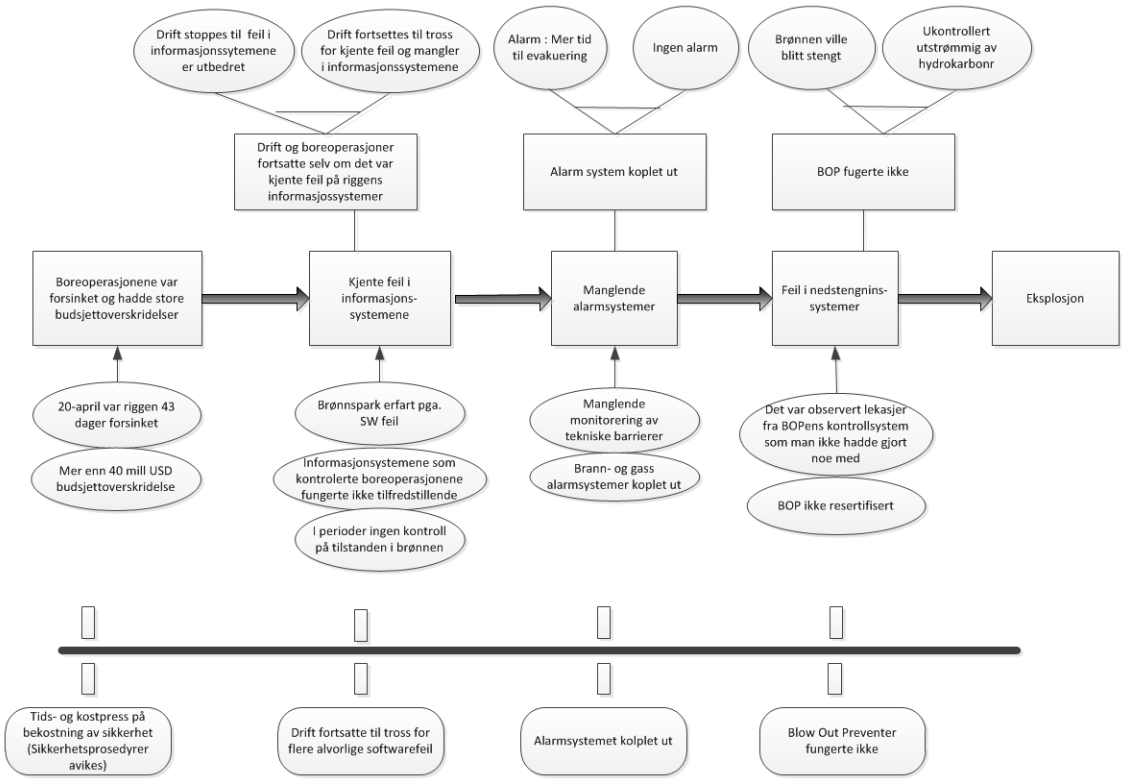
Vinnem (2011) refererer til at disse mulige hovedårsakene er blitt debatterte og at de ikke representerer det hele bildet i forhold til menneskelige og organisasjonsmessige årsaker som er kommet frem gjennom andre høringer og kommentarer. Inkludert i dette er følgende som angår informasjonssystemene ombord:

20.4.2010 var Deepwater Horizon riggen 43 dager forsinket og hadde en budsjettoverskridelse på mer enn 40 millioner USD. Det var flere kjente programvarefeil på riggen. Et brønnspark[11] var tidligere erfart på grunn av en slik feil. Datamaskinene som kontrollerte boreoperasjonene fungerte dårlig, i perioder hadde man ikke oversikt over tilstanden i brønnen.

Et nytt system var bestilt, men feil i nytt operativsystem gjorde at gammel programvare ikke lot seg kjøre på det nye operativsystemet. Noen av riggens alarmsystemer, inkludert riggens generelle alarmsystemer, var sperret. Dette medførte at selv om sensorer på riggen registrerte høye gassnivåer, giftig gass eller brann, og overførte disse signaler til brann- og gassvarslingssystemet, så ble ingen alarm aktivert. BOP stengte ikke av brønnen slik den skulle gjøre. Det er uklart om den ble skadet under ulykken eller om den allerede var i ustand. Det var gjort observasjoner om lekkasjer fra BOPens hydrauliske kontrollsystem uten at man hadde gjort noe med det. På grunn av at en resertifisering av BOPen, slik de var myndighetspålagt å gjøre, ville nødvendiggjøre en nedstengning i 90 dager, var ikke dette blitt utført.

I figur 19 er det tatt med et MTO-diagram som illustrerer hendelsesforløpet i Deepwater Horizon-eksemplet etter en analyse hvor informasjonssystemenes rolle er satt i fokus.

[11] Brønnspark, situasjon som oppstår når formasjonstrykket i en petroleumsbrønn overskrider det hydrostatiske trykket og brønnvæske strømmer ut. Brønnspark kontrolleres ved at man stenger ventiler og sirkulerer inn tyngre boreslam. (Kilde: Store norske leksikon. Hentet fra: http://snl.no/br%C3%B8nnspark/petroleumsvirksomhet 27.02.13)



Figur 19: MTO-diagram av Deepwater Horizon ulykken

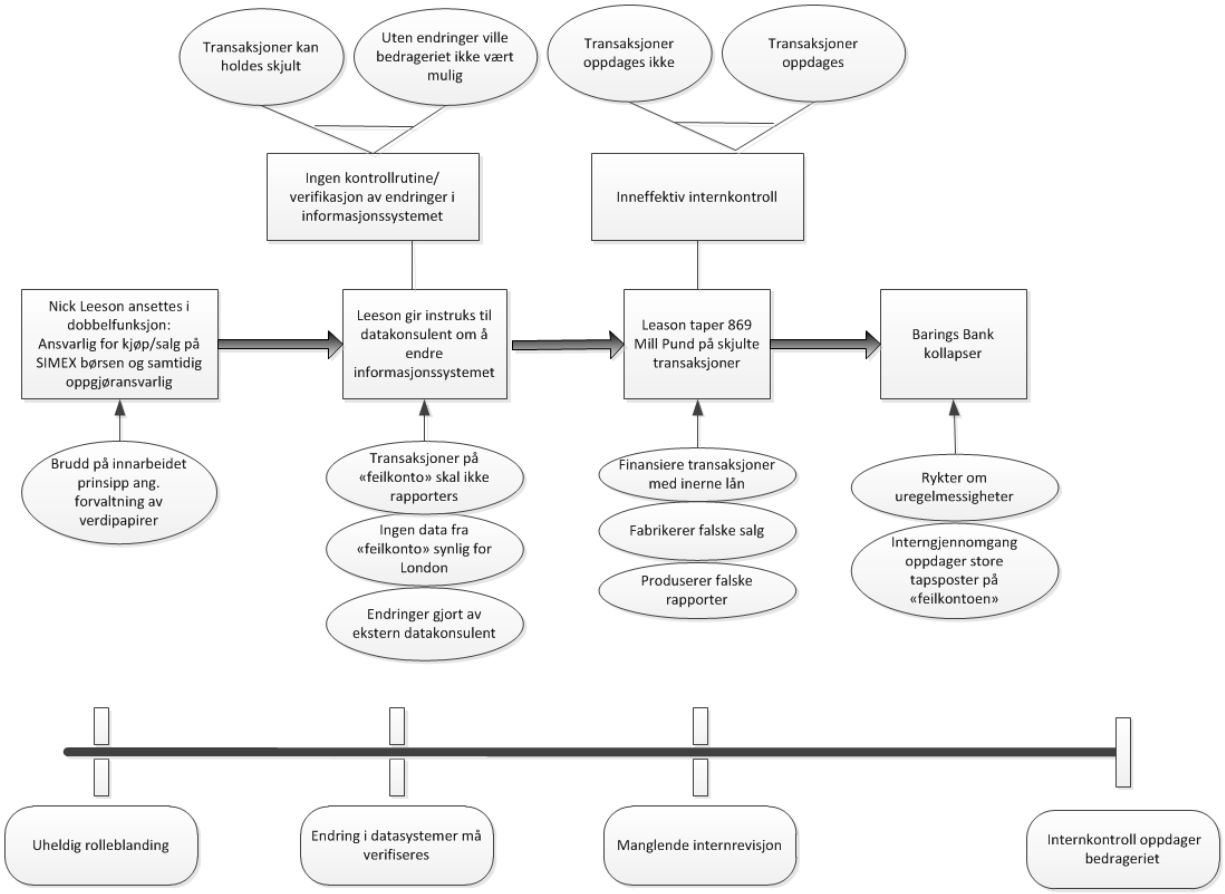
4.5 BARINGS BANK

Dette eksempelet er hentet fra James Reasons bok «*Managing the Risks of Organizational Accidents*» (1997) kapittel 2 under overskriften «*The Millions that Gushed Away: the Barings Collapse*». Reason beskriver hendelsen for å vise hva som kan skje dersom «*defences in depth*» ikke er tilstede. Det er ikke bare hvis fysisk energi blir frigjort ved en ulykke at noe kan skje - det samme gjelder når illojale medarbeidere får operere fritt og når ikke nødvendige barrierer er etablert.

Baring Brothers & Co., Limited (Barings Bank) var den eldste forretningsbanken i London. Siden 1792 hadde den vært uavhengig og privat eid. Et datterselskap *Barings Securities*, hadde fra 1992 vært en etablert aktør på børsen i Singapore (SIMEX) med det formål å operere på det raskt voksende opsjonsmarkedet. Et nytt firma *Barings Futures (Singapore) Pte Limited* (BFS) skulle utføre handlene på børsene i Japan og i Singapore.

Nick Leeson ble ansatt som oppgjørsansvarlig for inngåtte avtaler i BFS. Han ble samtidig også spurt om å være firmaets «*floor manager*» for SIMEX. Dette var et brudd på et innarbeidet prinsipp angående forvaltning av verdipapirer. Aktiviteter med oppgjør og handel skal holdes strengt adskilt. De som er ansvarlige for handel har som oppgave å tjene penger. Oppgjørsansvarlig skal sikre at det

ikke gjøres feil i regnskapet, og rette opp slike feil hvis de oppstår. At disse to funksjonene ble kombinert var det Leeson utnyttet til egen vinning. I juli 1992 åpnet BFS en *«feilkonto»* i henhold til standard prosedyre. Denne «feilkonto» skulle holde alle transaksjoner for handler som det var uenighet om. Slike uenigheter ble normalt avgjort i løpet av 24 timer. Leeson instruerte en datakonsulent til å forandre informasjonssystemet hos BSF slik at beløp på «feilkontoen» ikke var med i de daglige rapporter til London.



Figur 20: MTO-diagram av Barings Bank kollapsen

Resultatet var at ingen informasjon fra «feilkontoen» ble overført til de sentrale rapporteringssystemer. Han satte deretter i gang å kjøpe opsjoner, finansiert fra «feilkontoen», men pådro etter hvert store tap. I løpet av tre år utgjorde tapet 869 millioner pund. Tapene ble finansiert gjennom interne lån i *Baring Securities*, lån hos BSL i London og gjennom å fabrikkere falske salg i SIMEX-systemet. Han fabrikkerte også falske handels- og regnskapstransaksjoner for å skjule tapene. Rykter begynte etter hvert å gå om uregelmessige transaksjoner, og til slutt oppdaget en intern gjennomgang, «feilkontoen» med de enorme tapspostene. Barings Bank var ikke i stand til å ta disse tapene og selskapet kollapset. Leeson ble stilt for retten og idømt seks og et halvt års fengselsstraff for bedrageri.

I figur 20 er det tatt med et MTO-diagram som illustrerer hendelsesforløpet i eksemplet fra Barings Bank etter analysen hvor informasjonssystemenes rolle er satt i fokus.

4.6 9/11 I USA.

Flyangrepet mot de to tårnene i *World Trade Center* 11.9.2001 betegnes som et av historiens mest omfattende terrorangrep. Symbolkraften i å tilintetgjøre de to tårnene var enorm. Hendelsen var startskuddet for «Den globale kampen mot terrorisme» slik den ble definert av amerikanerne. En hel bydel ble jevnet med jorden. 2763 personer mistet livet, og over 6000 ble skadet (NOU 2012).
Hvilken informasjon hadde man på forhånd om et mulig terrorangrep, og hvordan ble denne informasjonen brukt, ble et sentralt spørsmål i granskningen som fulgte. Kilde til teksten i dette delkapittel er fra de amerikanske myndigheters granskningsrapport. «*The 9/11 Commission report*» (The 9/11 report 2004 s.265):

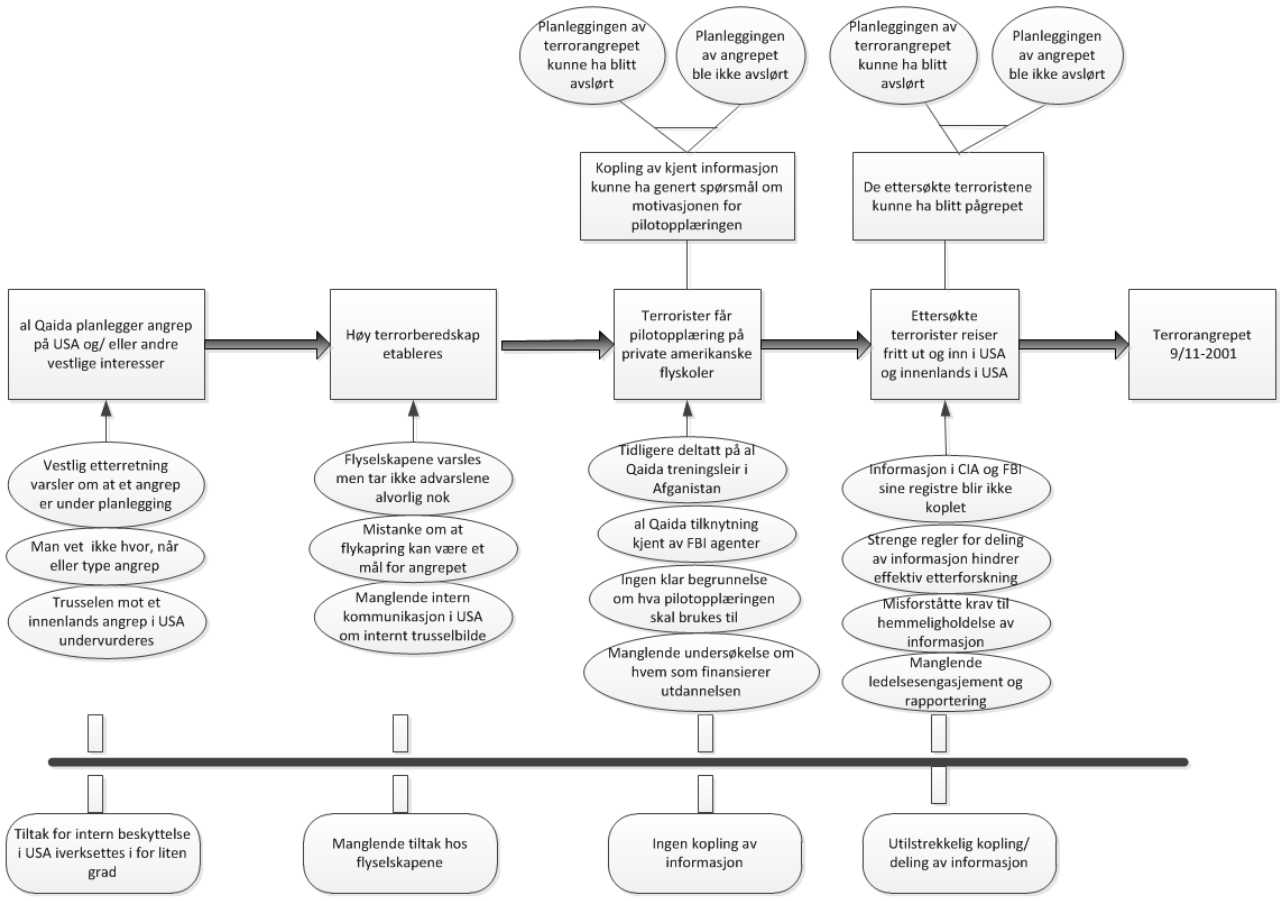
> *«The terrorists exploited deep institutional failings within our government. The question is whether extra vigilance might have turned up an opportunity to disrupt the plot……Al Qaeda's operatives made mistakes. At least two such mistakes created opportunities during 2001, especially in late August.»*

De to hendelsene det refereres til er at informasjon om flere av terroristene som deltok i angrepet, var kjent i myndighetenes informasjonssystemer, men ble ikke brukt. Manglende tilgjengeliggjøring og kommunikasjon av denne informasjon mellom de forskjellige amerikanske etterretnings-organisasjoner, som *FBI* og *CIA*, samt strenge regler for hvem som kunne få tilgang til gradert informasjon, gjorde at informasjon som ville kunne ha avdekket hva som var under planlegging, ikke ble kombinert og brukt på en hensiktsmessig måte.
En av terroristene Zacarias Moussaoui, deltok i et flyopplæringsprogram ved bl.a. *Pan Am International Flight Academy,* Eagan, Minnesota. Moussaoui utmerket seg med lite kunnskap om flyvning og et uttrykt ønske om å lære hvordan man tok av og landet en Boing 747. Han var også klassifisert av FBI-analytikere som en mulig fremtidig flykaprer. Moussaoui var fransk statsborger og hadde vært lengre i USA enn han hadde visum til. Amerikanske myndigheter vurderte den tilgjengelige informasjonen til ikke å være tilstrekkelig til å gjøre videre etterforskning. Undersøkelser som ble gjort etter angrepet «9/11» viste at britisk etterretning hadde informasjon om at Moussaoui tidligere hadde deltatt på al-Qaida treningsleir i Afghanistan. Det kom også frem at dette var kjent av amerikanske FBI agenter. Dersom denne informasjonen hadde vært kombinert tidligere ville det muligens kunne ha bidratt til at flere spørsmål om målet med flyopplæringen var blitt stilt. Flere av terroristene hadde tidligere deltatt i aksjoner og var internasjonalt ettersøkte. CIA satt på omfattende informasjon om flere av dem. Deler av informasjonen var gradert og det eksisterte restriksjoner på hvem som skulle få tilgang. Dette gjorde at selv om flere CIA- og FBI-

agenter fulgte spor som kunne ha ført til pågripelse av disse personene, så hadde de ikke tilstrekkelig tilgang til informasjonssystemer eller informasjon. Flere av terroristene reiste ut og inn av USA og rundt i USA flere ganger med fly, uten at etterretningsorganisasjonene oppfattet denne informasjonen. En av anbefalingene fra 9/11-kommisjonen er at (s.418):

> *«The president should lead the government-wide effort to bring the major national security institutions into the information revolution. He should coordinate the resolution of the legal, policy, and technical issues across agencies to create a «trusted information network».»*

I figur 21 er det tatt med et MTO-diagram som illustrerer resultat av analyse av hendelsesforløpet slik det fremgår i 9/11-kommisjonens rapport, når informasjonssystemenes rolle er satt i fokus.



Figur 21: MTO-diagram av 9/11-hendelsen

Det er velkjent fra den siste tids medieoppslag fra lekkasjer som den tidligere CIA-ansatte Edward Snowden gjorde til amerikanske medier, hvor omfattende den amerikanske etterretning nå er blitt som en følge av erfaringer fra det som skjedde før 9/11-hendelsene (France24 2013):

> *«Both the "Guardian" and the "Washington Post" reported last week that US security services had monitored data about phone calls from US telecoms firm Verizon and Internet usage data from large companies such as Google and Facebook».*

Og *Snowden* selv sier at *(France24 2013):*

«The NSA has built an infrastructure that allows it to intercept almost everything»

Også for Europa har 9/11-hendelsene fått ringvirkninger. I mars 2006 vedtok EU et direktiv (2006/24/EF) som pålegger eierne av telekommunikasjonstjenester å lagre trafikkdata i en periode på ikke mindre enn 6 måneder og ikke mer enn to år (*Datalagringsdirektivet*). Formålet med direktivet er å bekjempe alvorlig kriminalitet. Det dreier seg om lagringsplikt for data som er nødvendige for å identifisere avsender og mottager og tid og sted for kommunikasjonen, men plikten omfatter ikke selve innholdet i kommunikasjonen (FAD 2007 s. 135). Datalagringsdirektivet er nå også vedtatt innført i Norge, men er enda ikke trådt i kraft.

4.7 22/7 I OSLO OG PÅ UTØYA

Etter angrepene på regjeringskvartalet i Oslo og Utøya 22.7.2011 ble det oppnevnt en uavhengig kommisjon for å gjennomgå og trekke lærdom fra hendelsene. I kommisjonens rapport (NOU 2012), som er kilde til dette delkapittel, står det som et punkt i oppsummeringen (s.16):

«Potensialet i informasjons- og kommunikasjonsteknologi har ikke vært godt nok utnyttet».

Den 22.7.2011 eksploderte en 950 kilos gjødselbombe i regjeringskvartalet i Oslo. Åtte mennesker ble drept momentant og ti innlagt på sykehus. Gjerningsmannen Anders Behring Breivik, hadde noen timer tidligere sendt en e-post med vedlegg til flere tusen mottakere i inn- og utland. Vedlegget, et kompendium på om lag 1500 sider med tittelen 2083 – *A European Declaration of Independence* ble distribuert til en rekke mottagere. Etter å ha antent bomben dro han til *Utøya* i Hole Kommune, Buskerud hvor Arbeidernes Ungdomsfylking (AUF) hadde sin årlige sommerleir. Her drepte han 69 personer, de fleste ungdommer som deltok på sommerleiren.

Kommisjonen slår fast at Norsk politi ikke var tilstrekkelig forberedt på å håndtere en nasjonal beredskapssituasjon (s.147). Store mangler i den operative og taktiske ledelsen, manglende systemer for informasjonsdeling og manglende kommunikasjonsutstyr, blir beskrevet. Mangelfull læring fra tidligere hendelser er også påpekt. Et felles og raskt varslingssystem av hendelser i politietaten etterlyses. Kommisjonen sier (s.163):

> *«Det er vanskelig å se hvordan POD på en selvstendig måte med dagens IT-systemer og kapabiliteter kan bidra til å oppfylle den rollen direktoratet er gitt, med å sikre at nødvendige personell- og materiellressurser er disponible for politidistrikter i en krisesituasjon. Den viktigste informasjon for å støtte sitt arbeid finnes i PODs ansattes egen kjennskap, kunnskap og erfaring med de nasjonale beredskapsressursene og kapasiteten i de enkelte distrikter eller samvirkeaktører. Gjennom øvelser, tilsyn og tildelinger har POD en betydelig oversikt, men ikke i form av databaser eller andre informasjonssystemer ».*

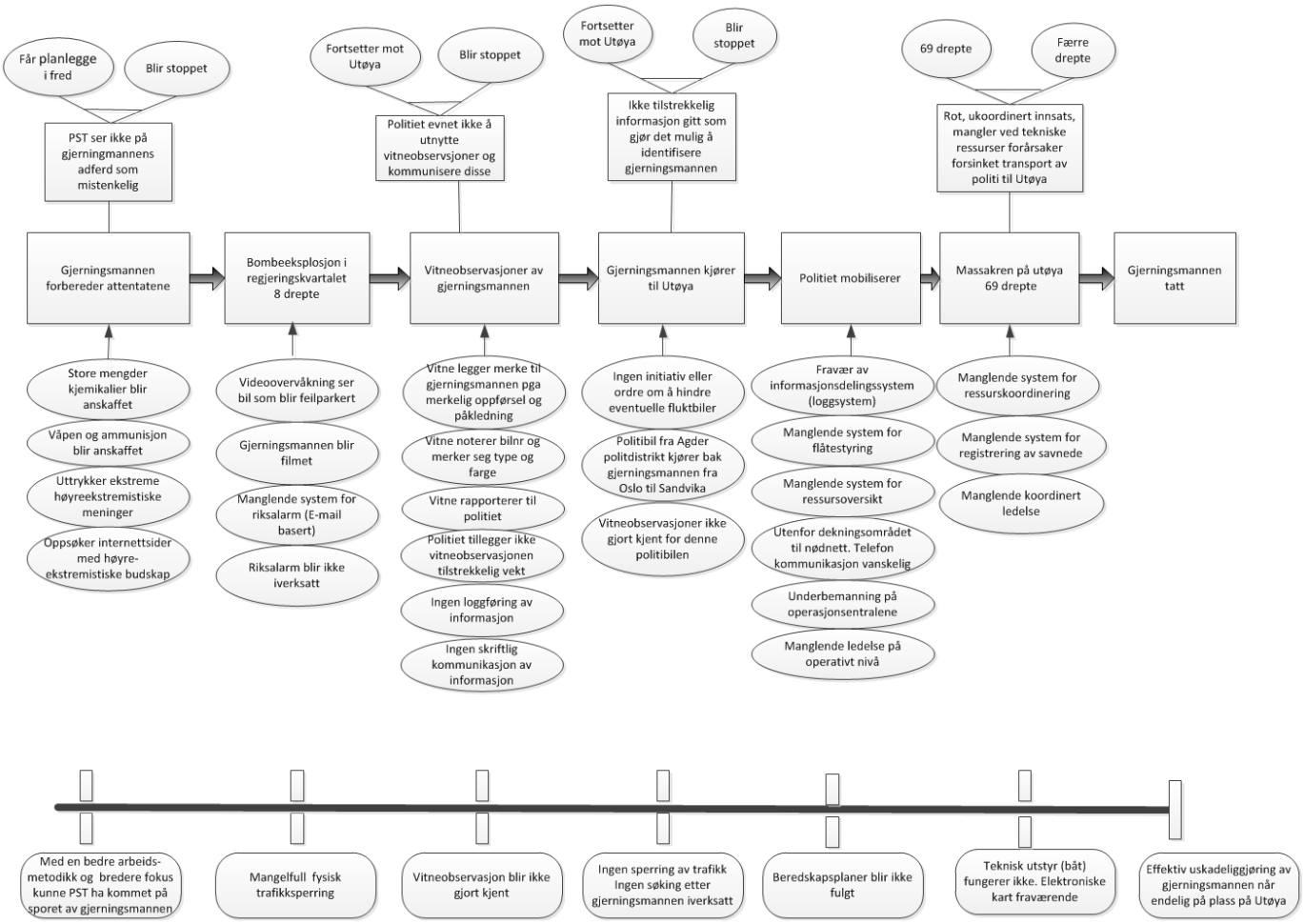
Det konkluderes også med at (NOU 2012 s.65):

> *«Internett har medført massiv spredning, ikke bare av ideologi og inspirasjon, men også praktisk veiledning i ulike former for terrorvirksomhet.»*

I MTO-diagrammet under gjengis hendelsesforløpet med fokus på informasjon som var tilgjengelig og ble eller kunne ha blitt brukt, samt en analyse av hvilke barrierer som sviktet eller manglet. I en rapport fra konsulentselskapet *Accenture* i 2010 som tok for seg IKT-situasjonen i politi-Norge heter det (Accenture 2010 i NOU 2012 s.333):

> *«Politiets IT funksjon har høy risiko og har utfordringer med å iverksette nødvendige forbedringer. IT funksjon har ikke felles mål og retning. Ikke helhetlig styring. POD har og begrenset kapasitet og kompetanse til å utøve premissgiverrollen.[…]Politiet har fulgt strategien om lavkost/ høy risk.»*

«En rapport fra *Gartnergruppen* pekte på de samme fundamentale svakhetene i 2005» (NOU 2012 s.333).



Figur 22: MTO-diagram av 22/7 hendelsene i Oslo og på Utøya

22. juli-kommisjonen er knusende i sin dom over politiets manglende bruk av informasjons-systemer. Politiet hadde for eksempel begrensede muligheter til å søke i egne data, viktig informasjon som gjerningsmannens bilnummer nådde ikke ut i tide, riksalarmen kom for sent og

patruljene kunne ikke motta tekst, bilder eller kartopplysninger. Listen er lang, men kort fortalt må norsk politi, i følge kommisjonen, begynne å utnytte potensialet i informasjons- og kommunikasjonsteknologien bedre. For å bruke 22.juli kommisjonens egne ord (NOU 2012 s 170):

> *«Omfanget av svakheter og feil er så omfattende at det samlet utgjør en foruroligende indikasjon på ledelsens manglende oppmerksomhet på utviklingen av Politi-Norge på beredskapsområdet, ledelsens evne og vilje til raskt å korrigere feil og ikke minst sørge for at det investeres tilstrekkelig i å etablerer robuste systemer for å kunne løse politiets primære oppgave»*

og (NOU 2012 s.335):

> *«Norge har et kompetent og mangfoldig politikorps, men ledelsen og verktøyene de har for å styre denne store sektoren er ikke tilstrekkelig. Det er behov for endringer på flere områder.»*

I figur 22 illustreres hendelsesforløpet i i 22/7 i Oslo og på Utøya eksemplet, og resultat av analysen av informasjonssystemets rolle som er gjort, i et MTO-diagram.

4.8 TILFELLET «DAVID»

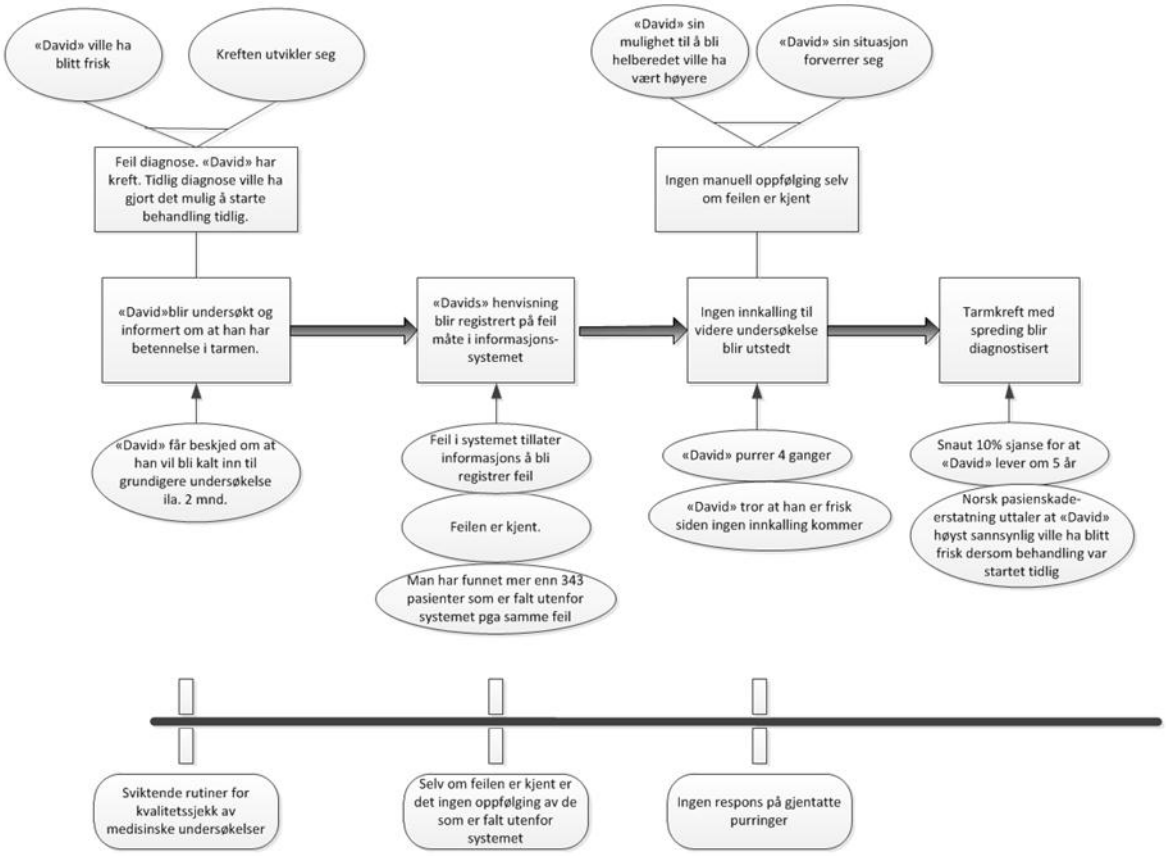
Teksten under er hentet fra en artikkel i Aftenposten mandag 11.3.2013 under overskriften *«David» dør av kreft etter datafeil*. I artikkelen summeres opp en rekke problemer som er erfart med informasjonssystemer i helsevesenet. Forfattere av artikkelen er Mathias Vedeler og Olav Eggesvik (Vedeler og Eggesvik 2013). Hendelsen med «David» er et eksempel på en av mange hendelser som er erfart i helsevesenet i Norge i de senere år.

«David» fikk høre fra Drammen sykehus i slutten av mai-2011 at han hadde betennelse i tarmen. Han fikk behandling med antibiotika og ble henvist til en grundigere undersøkelse om ca. to måneder. Det kom aldri noen innkalling selv ikke etter gjentatte purringer. «David» trodde at siden han ikke hørte noe var det ikke oppdaget noe alvorlig med hans helse. Han fikk smerter i magen og i juni-2012 fikk han konstatert tarmkreft med spredning til lever og bukhinne. Sykehuset fant da ut at det var en «datafeil» som var grunnen til at han ikke hadde blitt kalt inn et år tidligere. En feil i informasjonssystemet gjorde at «Davids» henvisning var blitt feilregistrert. Dette gjorde at han «forsvant» i systemet. Norsk pasientskadeerstatning kom frem til at «David» ville ha blitt frisk etter behandling hvis den hadde blitt igangsatt tidlig nok. Feilen i informasjonssystemet var kjent og var meldt inn til leverandøren i desember-2010. Feilen ble klassifisert som mindre alvorlig. I etterhånd har det vist seg at minst 343 pasienter på landsbasis var falt ut av systemet på grunn av den samme feilen. Det er ikke konstatert at noen av disse feilregistreringene har fått tilsvarende alvorlig konsekvens. Legene som behandler David har konkludert med at han aldri vil bli frisk. I avisartikkelen refereres det også til andre tilsvarende «dataulykker» i helsevesenet (Vedeler og Eggesvik 2013):

«Røntgenbildene til en kreftpasient ved Helgelandssykehuset ble i 2007 borte på grunn av en datasvakhet. Prøvesvaret kom ikke før dagen før pasienten ble innlagt med uhelbredelig kreft».

I 2011 ble *Helsetilsynet* gjort kjent med at svikt i informasjonssystemet førte til at sykehusene mistet kontrollen på mange tusen dokumenter, inkludert prøvesvar. Bare hos *Akershus universitets-sykehus* fant man nesten 40 000 dokumenter som ikke ble fulgt opp.

I figur 23 illustreres hendelsesforløpet i tilfellet «David» og resultat av analysen av informasjons-systemets rolle som er gjort, i et MTO-diagram.



Figur 23: MTO-diagram av eksemplet tilfellet «David»

5 DRØFTING

I dette kapittelet diskuteres forskningsspørsmålene ut fra den gjennomgåtte teori og empiri. Forskningsspørsmålene diskuteres i følgende sekvens:

1) Hva karakteriserer risiko i informasjonssystemer
2) Kan de vanlige risikoanalysemetoder også anvendes for risiko i informasjonssystemer
3) Hvordan kan slik risiko styres
4) Hvilke typer nye metoder vil det eventuelt være behov for

5.1 KARAKTERISTIKKER PÅ RISIKO I INFORMASJONSSYSTEMER

ISO (2009b s.2) sier at risiko ofte er karakterisert med referanse til mulige hendelser og konsekvenser eller en kombinasjon av disse. ISOs definisjon mangler usikkerhetsdimensjonen i forhold til den definisjonen som er brukt på risiko i denne oppgaven, og denne må også med i diskusjonen. Det argumenteres i denne oppgaven for at karakteristikker som er typiske for ulykkesperspektivene også gjelder for informasjonssystemer. Ulykkesperspektivene sier hvorfor ulykker skjer og hva som skal til for å forhindre disse. Eksemplene som er gjennomgått og analysert i kapittel 4, beskriver ulykker som har skjedd og hva konsekvensen av disse ble. Ved å relatere de inntrufne hendelsene, konsekvensene og den tilhørende usikkerhet som eksisterte i hvert eksempel, til ulykkesperspektivene, forsøkes det å etablere en forståelse for hva som er de typiske karakteristikker på risiko i informasjonssystemer. Karakteristikker på risiko blir derfor i denne sammenheng: typiske hendelser som kan skje i et informasjonssystem, mulige konsekvenser av disse og den tilhørende usikkerhet.

5.1.1 Karakteristikker relatert til Energi-barriere perspektivet

Latente feil i informasjonssystemer kan utløse oppsamlet «energi på avveie» når de rette forutsetninger er tilstede. Det samme gjelder feil i informasjonsinnholdet som kan forårsake feil eller mangelfulle avgjørelser. Energi-/barriereperspektivet er i høyeste grad relevant for informasjonssystemer. Som eksemplene viser, skjer store ulykker ofte plutselig og overraskende. Dersom informasjonssystemet kontrollerer fysiske prosesser kan slike ulykker forårsake fysisk ødeleggelse og skade slik som i Ariane 5 og Mars Climate Orbiter eksemplene. Er informasjonssystemet brukt til å håndtere personinformasjon kan systemfeil føre til at mennesker ikke får den oppfølging de trenger, som i tilfellet «David».

Begrepet «teknisk gjeld» er en metafor som brukes for å si at det du ikke har gjort eller det du burde ha gjort, har en kostnad. En «teknisk gjeld» kan være en latent feil som en har akseptert å leve med eller en feil som en ikke er bevisst. «Teknisk gjeld» kan derfor føre til «energi på avveie» og

representerer derfor en latent trussel i et informasjonssystem. Eksempler på bidrag til den «tekniske gjelden» for et informasjonssystem kan være (Hartvigsen mfl. 2011 s.37):

- Kode som er uferdig uten komplett håndtering av alle eventualiteter. Uferdige «*try – catch*»[12] -sekvenser i et dataprogram er eksempel på dette. Ofte erfares at ikke alle feilutganger og eventualiteter i programlogikk er spesifisert eller blir kodet ferdig. Gjennomtenkte og velfungerende «*Catch*»-sekvenser i programlogikk kan være gode barrierer. Er ikke disse tilfredsstillende på plass vil ulykker kunne skje slik som det gjorde i eksemplene fra Ariane 5 og Mars Climate Orbiter.
- Alle "*TODO*"[13] statement i koden som er utsatt, eksempelvis dokumentasjon, effektivisering av kode, all kode som var planlagt å skrive, men som ikke ble gjort.
- Kodesekvenser og programlogikk som ikke er dokumentert.
- De tester som det burde ha vært tenkt på, som har blitt glemt, som ikke ble skrevet eller som aldri ble utført.
- Overlapp og kompatibilitetsutfordringer mellom "denne kodebiten" og annen kode.
- Alle de ting som er utsatt fordi en ble presset til å levere på tid.
- Refakturering av kode[14] og eventuelt redesign av arkitektur som burde vært gjort.

Slike feil eller mangler kan eksistere i programkoden i et informasjonssystem.

I henhold til Energi-/barriereperspektivet var det «energi på avveie» som ble utløst da Mars Climate Orbiter kom inn i Mars gravitasjonsfelt og skulle inn i en geostasjonær bane før initiering av selve landingsprosessen. NASA (1999) fant at den bakenforliggende feilen var at det var benyttet ulike måleenheter for å angi hastighetsforandringer i to forskjellige programmoduler. Spesifikasjonen var klar på hvilken enhet som skulle benyttes, men ble ikke fulgt. Feilen ble ikke oppdaget under utvikling, test og verifikasjon. Tilstrekkelige barrierer for å forhindre hendelsen var ikke på plass. Mars Climate Orbiter-ulykken er svært lik Ariane 5 ulykken og skjer bare 3 år senere. I Ariane 5-ulykken var det konvertering mellom to variabler som genererte en feilsituasjon som ikke ble håndtert i programkoden (ESA 1996). Dette var selvfølgelig noe som kunne og burde ha vært oppdaget under utvikling og test. Eksisterende kode kunne lett inspiseres og utvikling av ny programvare justeres i forhold til den gamle. Mars Climate Orbiter- og Ariane 5-ulykkene var utilsiktete, og skjedde fullstendig uventet. Latente feil i informasjonssystemene ble utløst ved at

[12] «*Try*»-«*Catch*» sekvenser finnes i de fleste moderne programmeringsspråk. «*Try*» medfører at en funksjon kan ha forskjellige utganger (resultater). «*Catch*» beskriver de forskjellige alternative utganger og må kodes fullstendig slik at alle mulige resultater håndteres. Slurves det med dette vil programmet kunne feile.

[13] «*TODO*» er et eksempel på en vanlig måte blant programmerere å merke områder i programkoden som ansees som uferdig. «*TODO*» og en beskrivelse på hva som planlegges gjort, legges ofte som kommentar der hvor en mener at mer arbeid må gjøres.

[14] Refakturering av kode betyr at en skriver om (koder om) en programrutine uten at den funksjonelt sett endres. Motivasjonen kan være å effektivisere kode, forenkle, integrere eksisterende funksjoner etc.

fartøyene blir utsatt for de påvirkninger som de var designet for, men hvor tilstrekkelig validering og testing av informasjonssystemene ikke var utført på forhånd.

Før Deepwater Horizon-ulykken var det kjent at flere av de kritiske informasjonssystemene ikke fungerte som de skulle (Vinnem 2011). Et tidligere brønnspark var forklart med en feil i et informasjonssystem. Det var kjent at informasjonssystemene som kontrollerte boreoperasjonene, fungerte dårlig og var under utskifting. Alarmsystemene fungerte ikke tilfredsstillende. Dette er eksempler på «energi på avveie». Til tross for at den mangelfulle tilstanden til informasjons-systemene var kjent, fortsatte man boreprogrammet.

I Barings Bank kunne Nick Leeson uhindret gi instruks om endringer i bankens informasjons-systemer. På grunn av manglende kontroll kunne han benytte bankens midler til å oppnå personlig vinning (Reason 1997). Barrierer var fullstendig mangelvare og et voksende skjult underskudd ble til slutt så stor «energi på avveie» at banken gikk konkurs. Her burde organisasjonsmessige barrierer som internkontroll, gjennomganger og kryss-sjekker, samt verifisering av oppdrag om å utføre endringer i informasjonssystemene, være en del av bankens faste rutiner.

Tilfellet «David» viser at feil eller manglende informasjon i informasjonssystemene kan få katastrofale følger. Ingen manuell oppfølging ble igangsatt selv om det var kjent at mange personer var falt utenfor systemet på grunn av en kjent feil (Vedeler og Eggesvik 2013). «Energi på avveie» rammer i dette eksemplet en person med fatale følger. Det kunne ha rammet flere av de som var feilregistrert. Barrierer som burde vært på plass her er ikke minst manuell oppfølging av feilregistreringer og varslingsrutiner når en slik feil blir kjent. At man aksepterer å fortsette og benytte et informasjonssystem som man vet har slike kjente feil og som kan få så alvorlige konsekvenser for pasientene, er tegn på en holdning man ikke burde forvente i helsevesenet i Norge.

I eksemplet 9/11 i USA og også 20/7 i Oslo og på Utøya er «energien på avveie» representert ved planer om terroraksjoner og de forberedelser som gjøres av terroristene før aksjonene. Barrierene som kunne hindret disse aksjonene, er først og fremst informasjon og kunnskap fra myndighetenes etterretning, som ved analyse kan gi den visdom myndighetene trenger til å forhindre slike ugjerninger. Som vist i eksemplene var disse barrierene ikke tilstrekkelig på plass. Informasjons-systemene fungerte ikke etter intensjonen og vital informasjon ble derfor ikke gjort tilgjengelig for de som kunne ha mulighet til å forhindre hendelsene.

I Sleipner-A-eksemplet er «energi på avveie» representert ved en uoppdaget designfeil som førte til at støttestrukturen i veggene i GBSen var for svake. Energien ble utløst under trykktesting. I dette tilfelle kan ikke feilen relateres til tekniske feil i et informasjonssystem, men til den informasjonen som er skapt. Sleipner-A-eksemplet skiller seg i så måte ut fra de andre eksemplene.

5.1.2 Karakteristikker relatert til Informasjonsprosesseringsperspektivet

Det anbefales i høringsrapporten i Ariane 5 eksemplet at det etableres en mer transparent organisasjon med enkle og klare grensesnitt mellom partnerne (ESA 1996). Dette er et tiltak som vil gjøre at informasjonsutvekslingen kan skje enklere. I Mars Climate Orbiter eksemplet konkluderer granskningsrapporten med at det har vært utilstrekkelig kommunikasjon mellom teamet som jobbet med Mars Climate Orbiter utviklingen og teamet som forberedte navigasjonssystemene. Teamene var isolert fra hverandre og antagelser var gjort uten at disse var bekreftet (NASA 1999). Dette er eksempler på mangel på informasjonsutveksling som fører til misforståelser og i disse tilfeller feil som får fatale konsekvenser.

I Barings Bank kunne Leeson manipulere informasjonssystemene slik at han kunne operere fritt. Ingen datatransaksjoner inn og ut av feilkontoen var synlig for hovedkontoret i London og ingen etterspurte slik informasjon (Reason 1997).

I tilfellet «David» fører mangel på kommunikasjon av en kjent feil i informasjonssystemet til at «David» blir glemt og hans kreftsykdom utvikler seg til å bli uhelbredelig (Vedeler og Eggesvik 2013). Budskapet her, i forhold til risiko i informasjonssystemer, er at i en del bedrifter vil det finnes en kultur hvor det er akseptert at informasjon ikke gjøres tilgjengelig, deles eller utveksles på en hensiktsmessig måte. I tillegg til at dette kan være den direkte årsak til ulykker kan det også bidra til å hindre at potensialet som ligger i informasjonssystemene til å forebygge ulykker, blir utnyttet. Det samme kan sies om 9/11 i USA, hvor informasjon mellom de forskjellige amerikanske etterretningsorganisasjoner ikke blir delt. Flere grunner oppgis til at dette skjer som blant annet forskjellig fokus og manglende forståelse for andres informasjonsbehov, samt misforståtte krav til hemmeligholdelse av informasjon (The 9/11 report 2004). I eksemplet 22/7 i Oslo og på Utøya blir gjerningsmannen tidlig filmet av overvåkningskameraer. Et vitne legger merke til en person som oppfører seg merkelig og har en merkelig påkledning. Vitnet melder dette og også bilnummer, biltype og farge til politiet. Hadde denne informasjonen nådd frem til politibilen fra Agder politidistrikt som i en periode kjørte rett bak gjerningsmannen, ville dette kunne ha ført til at han ble stoppet. Manglende system for riksalarm og mangelfullt utbygd nødnett bidrar også til at deling av informasjon blir for dårlig (NOU 2012).

I forkant av Deepwater Horizon-ulykken er det kjent at informasjonssystemene ikke fungerer (Vinnem 2011). I granskningsrapporten til BP (2010) er dette faktum lagt lite vekt på som mulig medvirkende årsak. Det er heller ikke beskrevet i hvor stor grad denne informasjonen var meldt videre i organisasjonen. I forhold til informasjonsbehandlingsperspektivet representerer dette et eksempel på en inkubasjonstid med misoppfatninger og manglende informasjonsflyt. Det var kjent at mange av de kritiske informasjonssystemer hadde feil og mangler og det var akseptert at man fortsatte operasjonene på riggen til tross for disse feilene.

Sleipner-A skiller seg igjen ut siden informasjonen og beregningene var et sentralt designgrunnlag og dermed godt kjent og tilgjengelig informasjon i prosjektorganisasjonen. Her er utfordringen kompetanse og kunnskap og tilstrekkelig visdom til å forstå og etterprøve den informasjon som var skapt i prosjektet.

5.1.3 Karakteristikker relatert til Høypålitelige organisasjoner

Høy grad av årvåkenhet vil bidra til at komplekse informasjonssystemer blir høypålitelige, og dermed i stand til å fungere med minimal sannsynlighet for uønskede hendelser. Årvåkenhet under systemutvikling eller anskaffelse vil bidra til at informasjonssystemer ivaretar forskjellige brukergruppers behov. Under drift vil sikkerhet, stabilitet, og tilgjengelighet være sentralt. Avhengig av kritikalitet vil grad av nødvendig redundans avgjøres og etableres. I Høypålitelige organisasjoner-perspektivet er opplæring og trening i å også håndtere det uventede sentralt. Det må også prioriteres å bruke ressurser og å ha tilstrekkelig fokus på utvikling av kompetanse til vedlikehold, overvåkning og til å gi tilstrekkelig brukerstøtte.

Aven(2013c s.4) diskuterer årvåkenhet i forhold til nye måter å betrakte risikokonseptet på og sier:

> *«The new ways of thinking about risk are focusing on the risk sources: the signals and warnings, the failures and deviations, uncertainties, probabilities, knowledge and surprises, and the concept of mindfulness help us to see these attributes and take adequate actions.»*

Alle de åtte eksemplene som er gjennomgått i kapittel 4, avslører mangel på årvåkenhet. Mangel på tilstrekkelig interaksjon, oppmerksomhet og kommunikasjon mellom aktørene bidrar i stor grad til at ulykkene skjer. Ulykkene kunne ha vært avverget dersom tilstrekkelig kompetanse og ressurser på forhånd hadde vært anvendt til å gjennomgå informasjonssystemene med tanke på mulige hendelser, samt at det var blitt øvd på håndtering av slike hendelser på forhånd.

<u>Motstand mot å forenkle</u>

Motstand mot å forenkle innebærer fokus på et fullstendig og nyansert bilde for å håndtere det usikre og uventede. Dette er ikke tilfelle i Ariane 5- og i Mars Climate Orbiter-eksemplene. Informasjonssystemene var integrerte og vitale deler i totalsystemet som utgjorde romfartøyene. Man hadde ikke forutsett og forberedt seg på det usikre og uventede som at en kritisk programvaremodul skulle svikte. Gjennomganger med heterogent sammensatte ekspertgrupper gir mulighet til å se på løsninger fra forskjellige synsvinkler. Kanskje mange er redde for å stille de «dumme» spørsmålene og kanskje bedriftskulturen er slik at det ikke blir oppmuntret til det. Ikke minst kunne kanskje slike spørsmål ha sørget for fokus i diskusjonene på både beredskapen rundt etterretningsorganisasjonenes informasjonssystemer og informasjonsdelingen i forkant av 9/11 i USA. Fokus på totalbilde og beredskap til å håndtere det uventede, manglet både i 9/11 i USA og 22/7 i Oslo og på Utøya-hendelsene. Det samme også i virksomheten til Leeson hvor totalbildet

med lånopptak fra noen kilder i banken, store tapsposter bokført på feilkontoen, burde det ha vært satt spørsmålstegn ved dersom noen hadde prøvd å danne seg et totalbilde av virksomheten. I eksemplet «David» er det klart at de som har oversikt over feilen i informasjonssystemet ikke vurderer hva mulige hendelser og konsekvenser av disse kan være og hvilke barrierer som kan hindre uønskede konsekvenser.

Fokus på drift

Fokus her er på å avdekke latente feil i informasjonssystemene. Oversikt over og åpenhet rundt den «tekniske gjelden» i systemet og hva denne representerer av akseptert risiko, er sentralt. I flere av eksemplene er det en rekke feil i forkant av ulykkene som burde ha vært fulgt opp. I eksemplet med «David» er det en kjent feil i innleggingsrutinene som gjør at informasjon blir borte. Dette blir ikke godt nok fulgt opp (Vedeler og Eggesvik 2013). Under boreoperasjonene på Deepwater Horizon vet man at informasjonssystemene som kontrollerer boreoperasjonene ikke fungerer tilfredsstillende og at brann- og gassalarmsystemene er koplet ut. Drift av riggen fortsetter til tross for disse kjente feil (Vinnem 2011). I Ariane 5-eksemplet rapporteres det heller ikke noe om observasjoner som kunne gi et signal om at noe var galt. I Mars Climate Orbiter-eksemplet rapporteres det at NASA ikke reagerte på feil i beregnet og virkelig høyde etter pådrag fra motoren som skjedde før landingsprosedyren ble initiert (NASA 1999). I Barings Bank-eksemplet var det en prosedyrefeil å utnevne Leeson i en dobbeltfunksjon (Reason 1997). Endringer i informasjonssystemer burde ikke kunne instrueres av enkeltpersoner uten at dette ble verifisert. Det var en feil i bankens internkontroll at ikke Leesons aktiviteter ble fulgt opp bedre. I forkant av 9/11 i USA var det feil at informasjon ikke ble gitt til de som kunne ha kombinert dette med egen informasjon, noe som kunne ha gitt nye spor i etterforskningen (The 9/11 report 2004). 22/7 i Oslo og på Utøya ulykkene avslørte at nasjonen mangler et fungerende system for riksalarm, det er ingen loggføring av informasjon på grunn av fravær av et felles logg- og informasjonssystem. Nødnettet er enda ikke på plass og alternative kommunikasjonsmidler fungerer dårlig (NOU 2012).

Sleipner-A eksemplet skiller seg ut her siden det ikke dreier som om et informasjonssystem som ble satt i drift, men bruk av informasjon som viste seg å være feilaktig. Det sies ingenting om forhåndsobservasjoner eller signaler som kunne gitt en indikasjon på at noe var galt.

Satsing på robusthet

En organisasjon må unngå at store feil blir «lammende». Informasjonssystemene må være robuste nok til å møte uforutsette situasjoner og bruk. Robusthet er et velkjent prinsipp i risikostyringen for å møte trusler og usikkerheter (Aven 2013c). Det samsvarer med forsiktighetsprinsippet som sier at forsiktighet skal være det rådende prinsipp når det er usikkerhet knyttet til hva som blir konsekvensene (utfallene) (Aven 2007).

I eksemplet fra Mars Climate Orbiter får man indikasjoner på at en feil eksisterer ved at virkelig og beregnet høyde registreres å være forskjellig etter pådrag fra motorene. NASAs personell følger ikke dette opp (NASA 1999). I Ariane 5-eksemplet fikk en enkeltfeil katastrofale følger. Informasjonssystemene var ikke robuste nok til å håndtere de påvirkninger de var spesifisert for å skulle operere med. Det samme er tilfelle i eksemplene med Deepwater Horizon og tilfellet «David». I tilfellet «David» fortsetter man å registrere pasientinformasjon selv om det er kjent at det er en feil i informasjonssystemet. Det er ingen oppfølging av de pasienter som blir feilregistrert (Vedeler og Eggesvik 2013). I eksemplet med Deepwater Horizon er det en rekke feil som er kjent. Boreoperasjonene fortsetter til tross for dette. Både i tilfellet «David»- og i Deepwater Horizon-eksemplene kan man argumentere for at forsiktighetsprinsippet ikke ble overholdt. I Barings Bank kunne Leeson operere fritt i bankens informasjonssystemer. Ingen andre hadde et fullstendig og nyansert bilde og forsto hva som var i ferd med å skje før det var for sent (Reason 1997). Eksemplene fra 9/11 i USA og 22/7 Oslo og på Utøya viser at organisasjonene ikke var forberedt og trenet i å operere systemene i den situasjonen som oppstod. Systemene var funksjonelt sett ikke forberedt til å bli brukt på en formålstjenlig måte. I forbindelse med 22/7 i Oslo og på Utøya var det også kjent både av politikere og politiet at informasjonssystemene var mangelfulle (NOU 2012). I forkant av 9/11 i USA var det også kjent at amerikanske etterretningsorganisasjoner satt på egen informasjon som ikke ble delt og som gjorde at etterforskerne ikke fikk et fullstendig bilde av de forberedelser til terroraksjoner som var under planlegging (The 9/11 report 2004).

I Sleipner-A-eksemplet er det også et spørsmål om grad av respekt i forhold til ekspertise. Kanskje hadde ulykken kunne vært unngått hvis de rette eksperter, med tilstrekkelig kunnskap og den rette visdom, hadde vært involvert tidlig.

Respekt for ekspertise

I granskningsrapporten etter Ariane 5-ulykken anbefales det at det etableres en mer transparent organisering av samarbeidet mellom aktørene, spesielt innenfor ingeniøraktivitetene, samt økt fokus på myndighet og organisasjon (ESA 1996). Utilstrekkelig bemanning av teamet som forbereder navigasjonssystemene på Mars Climate Orbiter blir påpekt av NASA (1999) sammen med for dårlig trening av personell. Grensesnittet mellom aktørene var ikke klart definert og var ikke enkelt å forholde seg til. Innen samme bransje skulle en forvente at erfaringer ble utvekslet og at man lærte av tidligere store ulykker. Mars Climate Orbiter ulykken som skjedde tre år etter Ariane 5, tyder ikke på at dette er tilfelle. Gjennom kommentarer i granskningsrapporten til Mars Climate Orbiter og Ariane 5 ser en at det anbefales å etablere et team for å sørge for prosedyrer for bl.a. å kvalifisere programvare som skal benyttes. I forhold til det høypålitelige organisasjonsperspektivet må en kunne slutte at tilstrekkelig årvåkenhet ikke fantes. Tilstrekkelig fokus ble ikke gitt til å sikre den nødvendige robusthet. For å forenkle produktutviklingen ble programvaremoduler som var brukt i

en annen kontekst (med et annet fartøy med andre karakteristikker) benyttet uten tilstrekkelig refleksjon over hva forskjellene besto i. I granskningsrapporten anbefales det å etablere en mer transparent organisasjon med tettere koplinger på ingeniøraktivitetene. I Sleipner-A-eksemplet burde en ha involvert ekspertise til å gjøre verifikasjoner av de beregninger som var foretatt. Det er mye som tyder på at dette hadde vært den eneste måten å avverge denne ulykken på. Å være ydmyk i forhold til egen ekspertise, åpenhet og involvering av andre er stikkord her.

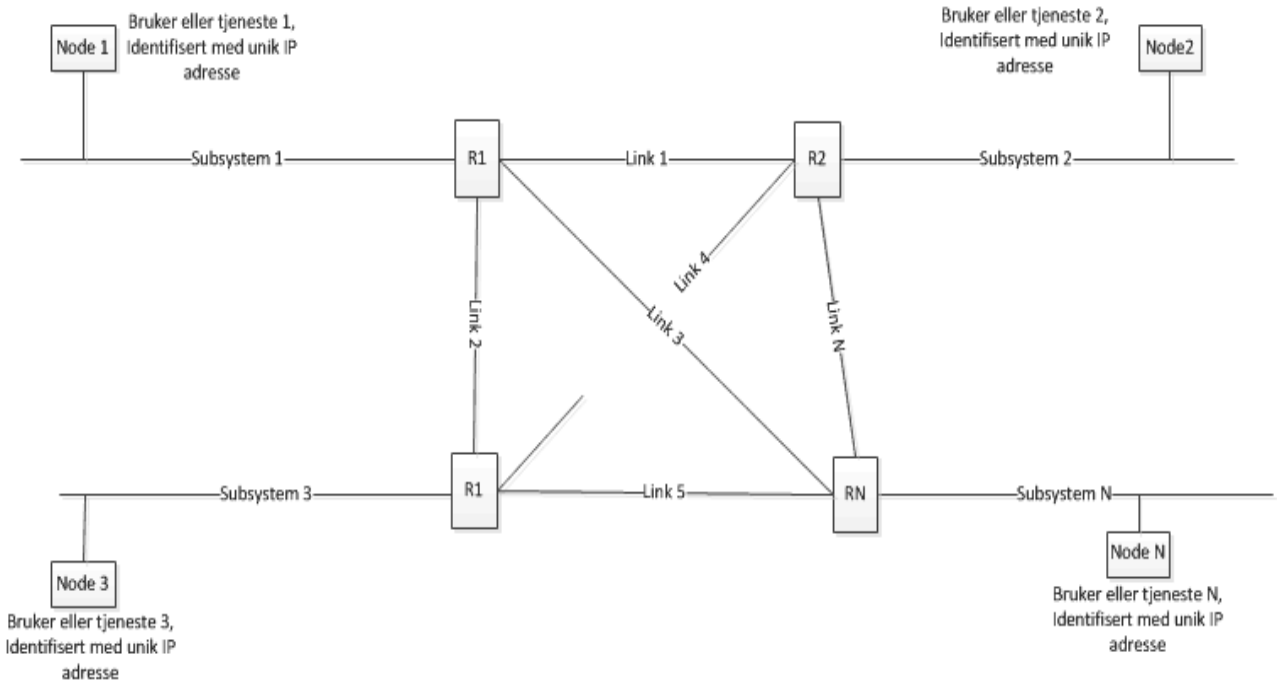
Høypålitelige organisasjoner som praktiserer høy grad av årvåkenhet vil være mindre utsatt for uønskede hendelser, inkludert storulykker, enn de som ikke gjør det. Å etablere en høy grad av årvåkenhet i en organisasjon vil derfor være et risikoreduserende tiltak. Grensesnittet mellom styring av kvalitet og styring av risiko blir flytende i dette tilfellet. Høy kvalitet i, og god styring av produksjon og prosesser krever kontinuerlige målinger, bedømminger og tilbakemeldinger samt kontroll med endringer.

Mest sannsynligvis var ikke informasjonssystemene gjenstand for egne risikogjennomganger i de ulykkene som er gjennomgått. Det er ikke funnet noen omtale av utførte risikogjennomganger verken i rapportene fra de bransjer hvor dette tradisjonelt gjøres, eller i noen av de andre rapportene som er gjennomgått.

5.1.4 Karakteristikker relatert til Normale ulykker (Normal Accidents)

Informasjonssystemer skiller seg ikke ut fra andre systemer i forhold til Perrows (1984) beskrivelse. Informasjonssystemer kan være tett eller løst koplede. De kan samtidig også være enten lineære eller komplekse. Perrows teori om Normale ulykker er derfor like relevant for informasjons-systemer som for andre system. Ansvar og myndighet for å styre slike systemer, bør i henhold til Perrow, organiseres som angitt i tabell 3. Storulykker hvor informasjonssystemer er involvert, skyldes ofte et misforhold mellom egenskapene til teknologien og organisasjonen som er ansvarlig for å kontrollere systemene. Storulykker er derfor noe man må forvente vil kunne skje. En må organisere seg for best mulig å forebygge disse, og også for å håndtere konsekvenser av slike ulykker etter at de har skjedd.

Siden Internett er så sentralt i det moderne informasjonssamfunn relateres det i det følgende til Perrows systemnedbrytning, og det brukes som basis for å diskutere karakteristikker med det Normale ulykker-perspektivet. Internett er i henhold til Perrows definisjon, *et løst koplet system* siden systemet vil kunne fungere så lenge det finnes alternative trafikkveier. Trafikkveiene i Internett er ikke forutbestemte og de som er tilgjengelige er alle kandidater til å bli brukt. Dette er med på å bidra til at Internett som system, blir feiltolerant.



Figur 24: Internett modellert iht. Perrows systeminndeling

Figur 24 viser en skjematisk oversikt over Internett hvor hver tjenesteleverandørs nett eller hierarki av nett, er betegnet sub-system (ENISA 2011). I noen tilfeller betegnes dette som Autonome Systemer. Noder som Perrow omtaler som enheter, kan for eksempel være PCer som er tilkoplet nettet (smarte mobiltelefoner, datamaskiner, iPad, iPhone, eller lignende). En del blir, i henhold til Perrows systeminndeling, en bruker som betjener en maskin eller en applikasjon som kjøres på en Web server eller på en av enhetene som er koplet til Internett. Komplekse interaksjoner mellom tjenester og deler er en av egenskapene til Internett og Internett må derfor kunne betraktes som et komplekst system.

Ved å assosiere hele Internettet til Perrows systeminndeling blir:

- Lag 4: Systemet: Hele Internettet
- Lag 3: Sub-system: Et Internett segment slik det blir levert og drevet av en sub-system eier (også kalt ISP = *Internett Service Provider*)
- Lag 2: Enhet: Ruter, linjeforbindelser, noder som kan være Multiplexere, servere, brannvegger
- Lag 1: Del: Internett-brukere, tjenester på Internett som applikasjoner, E-post-tjenester, sosiale medier.

Perrow (1984) mener at løst koplede systemer gir økt sikkerhet også i komplekse systemer. En desentral organisasjon er best egnet til å håndtere uforutsette interaksjoner. Det ser ut som denne teorien passer bra for Internett slik det eksisterer i dag. Kanskje den høye grad av erfart feiltoleranse i Internettet skyldes de løse koplinger og at hver enkelt aktør har et selvstendig ansvar for å holde sitt sub-system operativt. Mye nedetid i et sub-system vil føre til misfornøyde kunder som betaler

for nett-tilgang eller for drift av informasjonssystemer. For den globale Internett-trafikken vil ikke nedetid hos en sub-system-leverandør bety så mye så lenge det finnes alternative transportruter i nettet.

Til tross for sin kompleksitet har Internett så langt vært stabilt. Hendelser som har påvirket nettet har raskt vært utbedret. Ifølge Normale ulykker-perspektivet må vi forvente og være forberedt på at det kommer til å skje ulykker enten med lokale eller globale konsekvenser. I henhold til ENISA[15] (2011) vil slike ulykker typisk kunne være:

- Regionale feil på den fysiske infrastrukturen eller svikt i den menneskelige infrastrukturen som er etablert for å vedlikeholde den.
- En kaskade av tekniske feil hvor den nærliggende oppgradering fra Internett Protokoll versjon 4 (IPv4) til versjon 6 er den største utfordring på kort sikt. Dette er en nødvendig oppgradering for blant annet å øke lengden på adressefeltet (Nødvendig for å kunne ha flere unike adresser på enheter og deler i Internett). En rekke nettverkskomponenter og programvare i tilkoplede enheter må oppgraderes samtidig.
- Sabotasje ved at BGP (*Border Gateway protocol)*, som holder rede på «routingen» mellom de forskjellige sub-system blir gjort korrupt.

Mange informasjonssystemer er i dag avhengig av et kontinuerlig tilgjengelig Internett. Blir Internett utilgjengelig vil også informasjonssystemene bli utilgjengelig eller informasjonen i systemene bli upålitelig.

I eksemplene Barings Bank og tilfellet «David» dreier det seg om løst koplede systemer med komplekse interaksjoner. Det finnes alternativer hvis en del svikter. I tilfellet «David» burde man sende manuelle innkallinger til pasientene når de automatiske sviktet (løst koplet), men mange funksjoner var sannsynligvis avhengig av informasjon (leger, administratorer, pasienter). I Barings Bank kunne man også benytte manuelle rutiner, gjennomganger og rapporteringer som alternativ til de automatiske, men mange var avhengig av denne informasjon. Perrow (1984) sier at slike systemer håndteres best av en desentral organisasjon. Dette virker riktig i disse to eksemplene.

Hendelsene 22/7 i Oslo og på Utøya, og også beredskapen før 9/11 i USA, må kunne sies å være håndtert av desentrale organisasjoner. Informasjonssystemene ble ikke brukt til, eller var ikke forbered på, effektiv kommunikasjon. Mange enheter jobbet hver for seg uten at vital informasjon ble delt. Enhetene hadde forskjellige fokusområder og opererte uten sentral styring. Systemene var komplekse men burde vært lineære. De var løst koplet, men burde vært tett koplet. Med lineære menes at informasjon som ble samlet inn, burde distribueres etter faste forutbestemte rutiner og i

[15] ENISA = *The European Network and Information Security Agency is an EU agency created to advance the functioning of the internal market*.(ENISA 2011)

felles informasjonssystemer. Håndtering av denne type situasjoner krever øyeblikkelig handling og aktivitetene må være planlagte og koplet til hverandre. Med tett koplet menes at informasjonsutvekslingen vil følge faste forhåndsdefinerte veier og være avhengig av at alle delsystemer fungerer som forutsatt. Perrow (1984) mener at en sentral organisering er nødvendig for å håndtere tette koplinger. For politiets beredskaps- og alarmsystemer oppfattes dette som riktig. Utviklingen, drift og operering av slike informasjonssystemer må styre sentralt. Det må ikke være den minste tvil om hvordan de skal fungere i en nødsituasjon.

I alle eksemplene må informasjonssystemene betraktes som en integrert del av totalsystemet. De er med på å bidra til totalsystemets kompleksitet. Samspillet mellom de delsystemer som inngår blir ytterst komplekst og ingen er i stand til å ha en total detaljert oversikt over alle detaljer som bidrar i samspillet. I tillegg til at man må ha eksperter som kjenner delsystemene må disse også kunne koordinere og verifisere sine systemer i forhold til totaliteten. Man må etablere samhandlings-mønstre som håndterer totaliteten på en tilfredsstillende måte. Dette var ikke tilfelle i eksemplene.

5.1.5 Karakteristikker relatert til Målkonfliktperspektivet

Prioriteringen av bruken av midler i en organisasjon er en lederutfordring. En organisasjons ledere må etablere hensiktsmessige mål og avgjøre risikovilligheten til organisasjonen. For mye eller for liten risikovillighet kan avgjøre en organisasjons skjebne (Reason 1997) (se figur 8). Gjennom en risikoanalyse avdekkes både muligheter og trusler. Teorier og metoder fra økonomi og beslutningsanalyse vil kunne være til hjelp her (Aven 2007).

Utviklingen av et informasjonssystem er en dynamisk prosess og forståelsen for nødvendige risikogjennomganger underveis i utviklingsprosjekter mangler ofte. Moderne «*smidige*» systemutviklingsmetodikker som *SCRUM*, legger opp til rask produksjon, hurtige endringer og mye dynamikk i utviklingen. Verifikasjoner, testing og risikoanalyser forsinker produksjonshastigheten av programkode og blir derfor ofte noe som gjøres etter at kode er produsert. Det er en fare for at risikogjennomganger blir en kandidat som salderingspost når prosjektmidlene blir mindre i slutten av et utviklingsprosjekt. Det er derfor viktige at kriterier for risikogjennomganger med fokus på MTO, er et krav i utviklingsplaner og at tilstrekkelig med ressurser blir avsatte til dette.

Målkonfliktperspektivet kommer til uttrykk i eksemplene gjennom for lite ressurser anvendt til testing og verifikasjon i forhold til å prioritere ferdigstillelse på tid og for å holde kostnadene nede. I Ariane 5 ble SRI 2 systemet gjenbrukt fra Ariane 4 programmet (ESA 1996). Vanlig argument for å gjenbruke programvarekode er ofte for å spare tid og penger. I Mars Climate Orbiter eksemplet ble en alvorlig misforståelse i bruk av forskjellige enheter for hastighetsforandring ikke oppdaget, noe som er tegn på at det var brukt for lite ressurser til verifikasjon og test. Det ble av granskings-kommisjonen anbefalt at man etablerte bedre rutiner for å kvalifisere informasjonssystemer (NASA

1999). Deepwater Horizon boreprogram var 43 dager forsinket og hadde en budsjettoverskridelse på mer enn 40 millioner USD. Dette la nok et press på organisasjonen til å akseptere risikoen forbundet med å fortsette boreprogrammet til tross for kjente feil og mangler. Resertifisering av *Blow Out Preventor* (BOP) var ikke utført selv om dette var myndighetspålagt. Utbedring av kjente feil i informasjonssystemene ble utsatt. Man aksepterte høy risiko for å kunne avslutte boreprogrammet så raskt som mulig. I eksemplet fra Barings Bank fikk Leeson operere fritt siden han hadde en høy stjerne i organisasjonen og tilsynelatende bidro med gode resultater for banken. Det var en utbredt oppfatning at Leeson tjente masse penger for banken (Reason 1997). I 9/11 i USA eksemplet hadde de involverte organisasjoner forskjellig fokus og manglet tillit til hverandre. Etter hendelsen har amerikanske myndigheter økt sine investeringer til etterretning- og informasjonssystemer, slik det ble anbefalt av 9/11 kommisjonen. Eksempler fra 22/7 i Oslo og på Utøya hendelsen viser manglende bevilgninger til nødnett som enda ikke på plass. Prioriteringer for å etablere et felles fungerende riksalarmsystem mangler. 22/7 i Oslo og på Utøya eksemplet viser at de informasjonssystemer man hadde hatt bruk for i en slik situasjon ikke fantes. Politiets midler var ikke prioriter brukt til anskaffelser av tilstrekkelige informasjonssystemer. Det samme gjelder et felles logg- og informasjonssystem. I Sleipner-A-eksemplet var det viktig å få startet gassleveranser i tide for å møte forpliktelsene i Troll-gasskontrakten. I tilfellet «David» ser vi at man ikke prioriterer å bruke midler til umiddelbart å rette en feil i systemet. Heller ikke prioriteres det å sette inn tiltak og ressurser til å følge opp feilen manuelt.

5.1.6 Karakteristikker relatert til Menneskelige faktorer perspektivet

Store profesjonelle organisasjoner som eksemplene er hentet fra, legger ikke skylden for store ulykker på enkeltpersoner. Selv om det er lett å si at en systemutvikler, en ingeniør eller en operatør var den som forårsaket feilen, er det de bakenforliggende organisasjonsmessige eller tekniske grunner som er i fokus gjennom granskningene av ulykkene. Ingen «*Bad Apples*» nevnes i gransknings-rapportene.

En person som legger ut informasjon for å mobbe eller henge ut andre, må vel kunne karakteriseres som «*Bad Apple*» slik som nevnt innledningsvis i eksemplet med jenta i Gøteborg som la ut kompromitterende bilder av andre på Instagram, men samtidig er dette symptomer på manglende reguleringer og barrierer i samfunnet. Det samme gjelder Nick Leeson i Barings Bank eksemplet som manipulerte bedriftens datasystemer og produserte falske rapporter slik at han kunne bruke bedriftens penger til egen vinning. Han må vel også kunne betegnes et «*Bad Apple*» i organisasjonen når han utnyttet svakheter i systemene til egen vinning. Terrorangrepene 9/11 i USA og 22/7 i Oslo og på Utøya ville ikke ha skjedd dersom de offentlige kontrollmekanismer og barrierer hadde fungert hensiktsmessig.

Grensen mellom når et bevisst innbruddsforsøk i informasjonssystemer (eller «*hacking*») går over fra å være en uskyldig hobby til å være en bevisst forbrytelse er uklar. Hva som er motivasjonen bak å plante eller spre datavirus til andre sine informasjonssystemer er også vanskelig å forstå når dette gjøres av enkeltpersoner kun for å demonstrere egne ferdigheter.

Slurv med å oppdatere viktig statusinformasjon i informasjonssystemer kan også skyldes en menneskelig uteglemmelse eller dårlige rutiner, slik som i tilfellet «David». Det samme gjelder når det gjøres en dårlig jobb eller slurves under systemutviklingen. Det er ikke systemutvikleren som er syndebukken når programkoden ikke er skrevet for å håndtere alle tenkelige feilsituasjoner og når informasjonssystemet feiler, men organisasjonen som ikke har sørget for at nødvendige kontrollfunksjoner er på plass og at nødvendige verifikasjoner blir utført.

5.1.7 Oppsummering av delkapitlet

I organisasjonsteori understreker Morgan (1984 i Rosness 2004) og Bolman og Deal (1986 i Rosness 2004) viktigheten av å kombinere perspektiver for å forstå organisasjoner. En lignende holdning er implisitt i måten Reason (1997) og Hopkins (2000b i Rosness 2004) kombinerer ulike perspektiver i sine diskusjoner om organisatoriske ulykker. Det er viktig å ha en forståelse av alle perspektivene for å kunne gjøre bedre analyser og gi det beste beslutningsgrunnlag. Perspektivene representerer ulike sett av forutsetninger og metaforer for å forstå hvorfor ulykker skjer. Noen perspektiver overlapper hverandre delvis, som for eksempel Informasjonsprosesserings- og Høypålitelige organisasjoner-perspektivene. Det gir ingen mening å påstå at et perspektiv er bedre enn et annet. Det er viktig å fokusere på hva som kan læres av de ulike perspektiv.

I tabell 5 på neste side, summeres opp de vesentligste karakteristikker i forhold til risiko i informasjonssystemer slik de har blitt gjennomgått i dette delkapittel.

Tabell 5: Oppsummering av karakteristikker for forskjellige ulykkesperspektiv og hvordan dette kan relateres til informasjonssystemer

Perspektiv	Karakteristikker	Konsekvenser
Energi-/ barriere	• Latent feil i informasjonsinnholdet • Latent feil i programlogikk og kode • «Teknisk gjeld»	Objekter blir utsatt for «energi på avveie» pga. fravær av effektive barrierer
Informasjons-prosessering	• Manglende informasjonsflyt • Manglende tilgang til relevant informasjon • Feiltolkninger • Ikke oppdatert informasjon	Sammenbrudd i informasjonsflyt og manglende informasjonsutveksling
Normal ulykke	• Komplekse og tett koblede system gir fare for ulykker • Redundans gir økt risiko siden kompleksiteten øker • Uhensiktsmessig organisering i forhold til å håndtere hendelser	Store ulykker som skjer uventet og som får store konsekvenser fordi organisasjonen ikke er forberedt på å takle dem.
Høypålitelige organisasjoner	• Ulykker unngås ved god organisasjons-design • Redundans forsterker sikkerhet • Desentralisert styring viktig • Pålitelighetskultur • Kontinuerlig fokus på trening og simulering • Evne til å lære av feil	På grunn av manglende organisatorisk redundans, årvåkenhet og omstillingsevne mangler organisasjonen evne til å håndtere det uforutsette
Målkonflikter	• Makt og motstridende mål som profitt-krav • Mangelfull systemanskaffelse • Dårlig kvalitet på systemutvikling • For lite tid til testing • For lite tid til å legge inn og vedlikeholde informasjon • Dårlig systemvedlikehold • Manglende dokumentasjon • For lite opplæring • Dårlig sikkerhet • Manglende eierskap til informasjon	Robusthet i informasjonssystemer og sikkerhet nedprioriteres i forhold til andre mål
Menneskelige faktorer	• Svakheter i systemene utnyttes til egen vinning • Informasjon blir ikke oppdatert • Informasjon som har til hensikt å skade andre blir publisert • «Hacking» og planting av datavirus • Informasjon som ikke er ment å bli publisert blir gjort tilgjengelig i informasjonssystemer	Villede eller ikke-villede hendelser skjer i et informasjonssystem på grunn av bevisste eller ubevisste menneskelige handlinger. Old view: Mennesker gjør feil og har skylden. New view: Mennesker gjør feil, men slike feil er koblet til funksjoner i menneskers verktøy, oppgaver og operative miljø

5.2 RISIKOANALYSEMETODER OG RISIKO I INFORMASJONS-SYSTEMER

I dette delkapittel vurderes eksemplene i forhold til risikoanalysemetodene. Det diskuteres om metodene er egnet for analyse av risiko i informasjonssystemer. For hver metode vurderes det hvilken nytte den kunne ha hatt, dersom den var blitt anvendt i hvert enkelt av eksemplene.

5.2.1 Grovanalyse

Som beskrevet i delkapittel 2.7.1 er grovanalyse en metode som tar for seg alle stegene i risiko-analysen for å gjøre en grov kartlegging av risikobildet. Sjekklister kan være gode hjelpemidler i en slik analyse (Aven 2008).

I alle eksemplene som er gjennomgått ville en grovanalyse, dersom den var tilstrekkelig fokusert på det som viste seg å være problemområdet og dersom tilstrekkelig ekspertise var involvert, kunne ha bidratt til å avdekke årsakene til feilen. En grovanalyse kan være relativt overfladisk når det gjelder identifisering av mulige årsaker men kan være tilstrekkelig til å identifisere problemområder som bør analyseres nærmere. En grovanalyse trenger nødvendigvis ikke å være så detaljert at den etterprøver regler, databaseskjema, spesifikasjoner, etc. som definerer strukturen i et informasjons-system. Grovanalysen kan godt være basert på ustrukturert informasjon, samtaler, intervju, eller annet. Involvering av tilstrekkelig ekspertise blir fort en nøkkel for at metoden skal gi resultat. Ifølge politiets 4x4 matrise for kvalitetssikring av informasjon i tabell 4, vil enhver informasjon fra en pålitelig kilde (kategori C3 eller høyere i matrisen) være tilstrekkelig til at mer detaljert undersøkelse burde igangsettes.

NASAs undersøkelses-kommisjon påpekte utilstrekkelig kommunikasjon mellom teamet som jobbet med Mars Climate Orbiter utviklingen og teamet som forberedte navigasjonssystemene (NASA 1999). Dette forholdet burde kunne vært avdekket i en grovanalyse. Det samme i Ariane 5 hendelsen hvor det etterlyses en mer transparent organisasjon (ESA 1996). De tekniske feil som eksisterte ville nok ikke grovanalysen kunne identifisere men muligens at grensesnitt mellom komponenter var et område hvor det ikke var gjort tilstrekkelig kvalitetssikring. Dette kunne gi tilstrekkelig fokus på dette som et område hvor mer detaljerte analyser burde gjennomføres. I Barings Bank eksemplet forfalsket Leeson rapporter, rapporterte fiktive salg og fikk endret informasjonssystemet slik at transaksjoner på feilkontoen ikke var synlig for hovedkontoret. En gjennomgang av Leesons virksomhet ble igangsatt, men for sent til å hindre ulykken (Reason 2007). En grovanalyse hvor aktivitetene rundt feilkontoen var et tema, ville kunne ha gitt oppmerksomhet til Leesons aktivitet. I 9/11 i USA hendelsen er det flere eksempler på at informasjon ikke ble utvekslet og kombinert på en hensiktsmessig måte. Opplysninger om terroristenes inn- og utreiser til og fra USA, innenriks i USA, opplysninger om tidligere forbindelser til al-Qaida, ble ikke koplet sammen (The 9/11 report 2004). En grovanalyse som hadde påpekt dette som et problemområde,

kunne ha vært tilstrekkelig til at myndighetene, ut fra at man visste at en terrorangrep mot amerikanske interesser var under forberedelse, hadde satt i gang aktiviteter hvor informasjon fra de forskjellige informasjonssystemer ble sammenstilt. For etterforskere som jobbet med forebygging av terrorisme kunne dette ha gitt nye spor å følge. 22/7 hendelsen i Oslo og på Utøya er også eksempel på at informasjon ikke ble kombinert og delt hensiktsmessig (NOU 2012 s 109):

> *«Kommisjonen mener at systemer for skriftlig informasjonsdeling, på og mellom de ulike nivåene, ville økt politiets prestasjonsevne 22/7 og bidratt til bedre oversikt, bedre koordinering og bedret kunnskapsgrunnlag for de beslutninger som ble truffet.»*

Dette er eksempler på dårlig informasjonsflyt eller deling som kunne og burde vært identifisert gjennom en grovanalyse av politiets informasjonssystemer.

I tilfellet «David» var feilen i informasjonssystemet som gjorde at informasjon om pasienter kunne bli feilregistrert, meldt til leverandøren (Vedeler og Eggesvik 2013). Det betyr at den var kjent både av personer i helsevesenet som opererte systemet og hos leverandøren. En grovanalyse burde kunne identifisere det som en mulig årsak til uønskede hendelser som kunne få alvorlige konsekvenser. Det burde heller ikke være vanskelig å frembringe oversikt over antall feil som var blitt registrert feil over tid og ut fra dette gjøre en risikovurdering.

Sleipner-A-eksemplet viser at det er en forskjell mellom designfeil og det som kan betraktes som mer typiske feil i informasjonssystemer. I Sleipner-A-eksempelet er det vanskelig å tenke seg andre måter å avdekke den latente feilen på enn at eksperter som kunne verifisere designet, på forhånd ble involvert. Her er den latente feilen skjult i designet, informasjonen burde ha vært bedre gjennomgått og kvalitetssikret av eksperter med tilstrekkelig kunnskap. Dette ble ikke gjort i tilstrekkelig grad slik at ulykken skjedde plutselig og var en stor overraskelse for alle.

5.2.2 Feiltre- og hendelsestreanalyse

I eksemplene fra både fra Deepwater Horizon og fra tilfellet «David» eksisterer det kjente feil som organisasjonen ikke hindrer i å la utvikle seg til en ulykke. Hendelsestreanalyser vil med fordel kunnet ha blitt anvendt her for å lage et beslutningsgrunnlag for om man skulle akseptere risikoen eller igangsette forbyggende tiltak. Risikobildet er kjent og burde ha vært beskrevet i for eksempel «*Bow-tie*» diagram for effektiv kommunikasjon og videre analyse. «*Bow-tie*» diagram er ofte ikke så detaljert som feiltre og hendelsestre på den måten at de ikke fanger opp komplekse hendelseskjeder. De er fokusert på mulige årsaker – initierende hendelser – mulige konsekvenser, mens feiltre og hendelsestre gir en detaljert analyse av potensielle komplekse hendelseskjeder på henholdsvis årsaker og konsekvenser.

I en risikoanalyse av Deepwater Horizon før ulykken, kunne man med fordel også ha gjort en feiltreanalyse. Her ville man kunne ha illustrert og analysert de mulige initierende hendelser som de

kjente feil ville kunne resultere i hvis de fikk utvikle seg. I dette tilfellet var det ikke nødvendig med ytterligere tekniske gjennomganger for å slå fast at det var betydelige problem med informasjons-systemene om bord og at det burde vært menneskelige og organisasjonsmessige barrierer tilstede som hindret de latente farene i få utvikle seg. En hendelsestreanalyse ville kunne ha gitt et godt beslutningsgrunnlag i tilfellet «David» (se figur 5). Her er det en risiko som aksepteres av leverandøren og av de som vet om feilen og melder denne til leverandøren. De burde også sørge for at en risikoanalyse ble utført, for eksempel ved en feiltreanalyse.

Forsiktighetsprinsippet burde ha kommet til anvendelse både i tilfellet «David» og i forkant av Deepwater Horizon ulykken.

Feiltreanalyser hadde også kunnet avsløre feilen i Ariane 5- og Mars Climate Orbiter-eksemplene (se figur 4).

5.2.3 FMEA

I en FMEA gjennomgang ville fokus være på hver enkelt systemkomponent og en undersøkelse av hva som skjer dersom denne svikter. Som ved HAZOP ville en FMEA analyse med fokus på de modulene som det var feil i, kunne ha avslørt «energi på avveie» i eksemplene i Ariane 5 og i Mars Climate Orbiter. Dersom fokus hadde vært på SRI 2 modulen i Ariane 5 og SM_FORCES i Mars Climate Orbiter i en FMEA gjennomgang og analysen hadde vurdert hva som kunne skje dersom disse modulene sviktet, så ville sannsynligvis dette lede til en erkjennelse av hvor kritisk disse komponentene var. Noe som kunne ha ledet til at kvalitetssjekker ble grundigere gjennomført.

En FMEA av et informasjonssystem eller en modul i et informasjonssystem, burde kunne automatiseres. Tester som kunne utføres automatisk ville det ha vært hensiktsmessige å benytte. Muligens hadde det vært hensiktsmessig å utvikle egen programvare for å gjøre disse verifikasjonene. Her ville man kunne simulere inndata, måle resulterende respons og ut fra dette gjøre en vurdering ved å sammenligne med eksisterende og analysere resultatet hvis modulen ikke responderte som forventet.

En FMEA i de andre eksemplene er det vanskelig å se ville ha noen større nytteverdi. I eksemplene fra Deepwater Horizon, tilfellet «David», Barings Bank, 9/11 i USA og 22/7 i Oslo og på Utøya er hendelsene ikke direkte knyttet til noen integrerte moduler i informasjonssystemet som man kunne analysere. I overført betydning kunne man sett på hvert informasjonssystem i samspill med andre og brukt fremgangsmåten i en FMEA. Dette ville kunne gi resultater men i disse bransjer er det ingen tradisjon å benytte denne type metode, så andre analysemetoder ville mest sannsynlig kunne ha vært mer naturlig å bruke.

I i Sleipner-A er det vanskelig å tenke seg hvordan en gjennomgang av informasjonssystemene eller av informasjonen ville kunne ha bidratt til identifisering av feilen som eksisterte i designgrunnlaget.

5.2.4 Sikker Jobb Analyse (SJA)

En SJA utføres vanligvis i forkant av fysiske arbeidsoperasjoner før en starter med slike oppgaver. En SJA kunne, i tilfellet «David», ha blitt utført hver gang pasientinformasjon ble lagt inn. Siden man vet at det eksisterer en kjent feil i informasjonssystemet eksisterer bør en være ekstra påpasselig med å gjøre dette riktig. De som legger inn data bør bli gjort klar over at det kan få konsekvenser hvis det gjøres feil siden tilstrekkelige barrierer mangler. Enkle barrierer som for eksempel sidemannskontroll, kunne ha vært etablert i dette tilfelle. Det samme burde vært gjort i Deepwater Horizon eksemplet. Når det er bestemt at man skal akseptere risikoen med å operere informasjonssystem med kjente feil bør man være bevisst hva konsekvensene av dette kan bli, og ha planlagt konsekvensreduserende tiltak som iverksettes når feilen oppstår. I de andre eksemplene er det vanskelig å tenke seg hvordan en SJA kunne anvendes med et positivt resultat.

5.2.5 HAZOP

I en HAZOP-analyse ville man kunne fokusere på hver enkelt komponent informasjonssystemet er bygget opp av og, ved hjelp av ledeord, analysert farepotensialet dersom komponenten ikke responderte som forventet på inndata. McDermid (1995) har gjennomført HAZOP av flere informasjonssystemer og anbefaler å ikke begrense frihetsgraden til faste ledeord. Han sier (Avsnitt F):

> *«Whatever guide words are used their most important function is as discussion starters, and it is important not to unnecessarily restrict the freedom of the team to interpret them in novel ways»*.

I eksemplet med Ariane 5 ville en kunne ta for seg SRI 2-modulen og bruke ledeord som maks/ min for de forskjellige inn- og utparametre til og fra modulen. Alternativt ledeord som «ingen respons fra modulen» ville kunne ha gitt samme indikasjon som med en FMEA. Kombinert med en forståelse for hva som er de reelle verdier kunne dette ha ledet til at problemet ble identifisert. Tilsvarende gjelder for Mars Climate Orbiter, her ville en gjennomgang av modulen SM_FORCES og ved å bruke tilsvarende ledeord, eventuelt ledeordene «mer/ mindre», ha gitt indikasjoner på uoverensstemmelser i bruk av enhet for kraftpådrag. En HAZOP for DeepWater Horizon ville også kunnet ha sørget for fokus på farene som eksisterte.

En HAZOP i Sleipner-A eksemplet ville kreve grundig ingeniørkompetanse hos de som gjennomførte analysen men ville kunne ha vært et hjelpemiddel til en forståelse for at et problem eksisterte. Her ville ledeord som «høyt kraftpådrag», «maks kraftpådrag» muligens kunne ha gitt resultater som ledet til grundigere undersøkelser. Sleipner-A-eksemplet er interessant for å vise forskjellen mellom det som kan karakteriseres som en klassisk bruker/ingeniør feil og det som i denne oppgaven er beskrevet som feil i informasjons-systemer. Her er det også «energi på avveie» og manglende barrierer. Feilen kan sannsynligvis ikke oppdages gjennom metoder hvor ikke ekspertkompetanse er involvert. En HAZOP hvor fag-eksperter deltar i teamet, ville kunne ha

avdekket feilen. En fellesnevner for de to eksemplene fra romfartsindustrien og ulykken med Sleipner-A er at siden det var gått bra tidligere, undervurderer eller overser man forskjellene fra tidligere lignende vellykkede prosjekter og utfører derfor ikke tilstrekkelig med verifikasjoner. Tidligere positive erfaringer medførte at en ikke var observant nok. Barrierene ble ikke tilstrekkelig opprettholdt.

I resten av eksemplene ville ikke en HAZOP være en naturlig analysemetode å benytte. Dette delvis fordi det ikke er noen tradisjon for HAZOP i disse miljø og delvis for at det ikke er noen klart identifiserbare og avgrensbare komponenter som kan betraktes. I disse eksempler dreier det seg om strukturert informasjon, det er spesifikasjoner på hva som forventes av inngangsdata til og utgangsdata fra de forskjellige informasjonssystem.

I romfartsindustrien og i olje- og gass virksomheten er det tradisjon for å gjøre metodisk gjennomgang med kjente metoder som HAZOP, FMEA, feiltreanalyse eller hendelsestre-analyse. Bayesiansk nettverk har i lang tid vært vanlig å bruke i bransjer som luftfart og romfart, men som til nå ikke har vært særlig vanlig i offshoreindustrien (Aven 2008 s.109).

5.2.6 Bayesiansk nettverk

Bayesianske nettverk er meget anvendelige i situasjoner der vi kan sette opp årsakssammenhenger, og der vi deretter kan «sjekke» hvilken tilstand enkelte av nodene er i (Aven 2008).

Bayesiansk nettverk kunne derfor vært brukt i alle eksemplene med positivt resultat. I en analyse av Ariane 5 og Mars Climate Orbiter ville en kunne lage Bayesianske nettverk som illustrerte sammenhenger mellom de involverte systemmoduler. En systemmodul ville utgjøre en node (variabel) i nettverket. Ved å analysere sammenhenger og konsekvenser ved tilstander på de forskjellige noder, ville en kunne få frem risikobildet knyttet til utfall av enkeltkomponenter. Et romfartøy er et tett koplet og komplekst system som burde være godt egnet til analyse med Bayesianske nettverk. Et Bayesiansk nettverk kan inneholde alle de variabler som påvirker hverandre. Samspillet og gjensidig påvirkning mellom menneskelige, teknologiske og organisasjonsmessige variabler kan modelleres og analyseres. Metoden er derfor godt egnet til å analysere komplekse forhold som de som er beskrevet i eksemplene.

Samspillet mellom informasjonssystemene, andre tekniske og administrative systemer på Deepwater Horizon ville vært godt egnet til å bli modellert og analysert med et Bayesiansk nettverk. Her ville man ved å analysere mulige konsekvenser og usikkerheten forbundet med å fortsette boreoperasjonene, kunnet gitt ledelsen et beslutningsgrunnlag for å avgjøre om gevinsten ved å fortsette boringen opp mot den risikoen som man aksepterte ved å fortsette.

I Barings Bank ville Leesons aktiviteter fort bli synlige dersom det ble satt fokus på de operasjonene han var involvert i. I 9/11 i USA og 22/7 i Oslo og på Utøya eksemplene, ville

Bayesianske nettverk av hele organisasjonens virksomhet kunnet vise avhengigheter til, samspill og konsekvenser av manglende integrasjon mellom informasjonssystemene. I tilfellet «David» ville konsekvensene av ikke å følge opp feilregistreringer kunne bli analysert og beskrevet. Noe som sannsynligvis hadde ført til oppmerksomhet rundt dette og etablering av konsekvensreduserende barrier som eksempelvis manuell oppfølging av de pasienter hvor det forelå feilregistreringer.

Det er vanskelig å tenke seg hvordan Bayesiansk nettverk metoden ville kunne ha bidratt til å avverge Sleipner-A-ulykken. Et nettverk hvor de beregninger som var gjort var en av variablene ville kanskje ha gitt grunnlag for at kritiske spørsmål ble stilt. I utgangspunktet er «energien på avveie» så «godt gjemt» i designet at den, uansett metode, er lite sannsynlig vil bli oppdaget.

5.2.7 KITHs metodegrunnlag og bakgrunnsinformasjon for risikoanalyse

KITHs rapport sier i innledningen at den gir råd om hvordan arbeidet med risikoanalysen kan gjennomføres (Aksnes 2000). Den lener seg mye på den britiske standarden BS 7799. Rapporten spesifiserer i hovedsak eksempler på hvordan noen av stegene i referansemodellen, som er spesifisert i delkapittel 2.5 (se også figur 3), kan gjennomføres. KITHs rapport fremstår derfor mer som en beskrivelse av en analyseprosess eller prosedyre enn en metode. I så måte kunne KITHs råd vært anvendt i alle eksemplene og ville kunne ha gitt resultater der. En grovanalyse hvor man inkluderer elementer fra KITS metodikk, kanskje spesielt elementer fra BS 7799, ville kunne være nyttig når fokusområdet er villede handlinger. I tilfellet «David», som nettopp er fra helsevesenet i Norge, burde KITHs metode vært benyttet. KITH beskriver trusler mot en informasjonsressurs (Aksnes mfl. 2000 s.5) som et fokusområde under risikoidentifikasjon. I tillegg til et rent sikkerhetsaspekt burde man inkludere en verifikasjon av integritetsreglene som spesifisert under ISO-8000 metoden (beskrives i delkapittel 5.2.11). I tilfellet «David» burde en gjennomgang i henhold til KITHs metode ha ført til at feilen som eksisterte i systemet ble avdekket og usikkerheten knyttet til både hva som kunne skje og hva konsekvensene kunne bli, blitt analysert. Nødvendige barrierer for å hindre de konsekvensene feilen fikk for «David», burde blitt etablert. Dersom en hadde gjennomført en analyse i henhold til KITHs risikoanalysemetodikk for informasjonssystemer, ville mest sannsynlig feilen i pasientadministrasjonssystemet blitt avdekket og risikoen forbundet med å fortsette å operere systemet kunne fått oppmerksomhet og bli analysert.

5.2.8 RANDs VAM

RANDs VAM metode skiller seg ut med sin ovenfra og ned vinkling. Her er i første omgang ikke informasjonssystemene i fokus, men en organisasjons essensielle funksjoner. Deretter identifiseres de informasjonssystemer som er implementert for å utøve funksjonene. I alle eksemplene som er gjennomgått ville en VAM-analyse vært en nyttig øvelse for å få bevissthet i organisasjonen rundt hvor sentrale informasjonssystemene er for sikker drift. I Ariane 5 eksemplet ville fokus fort blitt på

SRI 2-systemet og i Mars Climate Orbiter-eksemplet på SM_FORCES. For Deepwater Horizon ville fokus raskt bli på overvåkningssystemet for boreoperasjoner, *Blow Out Preventeren*, riggens alarmsystemer osv. Alle de systemene som er vitale for sikker drift. I 9/11 i USA og 22/7 i Oslo og på Utøya ville de sentrale systemer komme i fokus og svakheter ved disse kommer frem i en slik analyse. Tilsvarende i Barings Bank og tilfellet «David». Fokus ville bli på de sentrale informasjonssystemer og en videre analyse ville avdekke svakheter i dem.

VAM fremstår som en omfattende metode og skiller seg ut fra de andre metodene med sin ovenfra og ned tilnærming. I forhold til risikoanalysens ulike trinn som er spesifisert i delkapittel 2.5 dekker metoden risikovurdering og delvis risikohåndtering.

Sleipner-A-eksemplet er igjen interessant siden det sannsynligvis ville falle utenfor VAM-analysen siden det her dreier seg om informasjon som er feil og som ikke kan relateres direkte til et konkret informasjonssystem. Feilen kan heller ikke relateres til det som ville komme frem av en gjennomgang av funksjoner.

5.2.9 CORAS

En gjennomgang med CORAS ville ha frembrakt diagrammer hvor en ved analyse kunne ha identifisert kritiske kommunikasjonslinjer som hjelp for grundigere undersøkelser av hvordan disse fungerte. Hvor godt informasjonsflyten fungerer i en organisasjon og analyse av hvor mye informasjon som er «lagret» opp i en organisasjon i inkubasjonstiden før en ulykke, er ikke et hovedtema i noen av de risikoanalysemetodene som er gjennomgått, her dekker CORAS et behov som ikke de andre metodene gjør. UML har i IT-bransjen blitt det mest anvendte verktøy for for å modellere informasjonsflyt i forbindelse med analyse og planlegging av informasjonssystemer. CORAS er en nyttig påbygning på UML og fokuserer spesielt på sikkerhetsproblemstillinger. Det virker som kombinasjonen UML og CORAS vil være nyttige hjelpemidler til å analysere og visualisere hvordan informasjonsutvekslingen i en organisasjon fungerer. I forhold til rammeverket er CORAS og nettverksanalyse særdeles godt egnet for å analysere risiko relatert til Informasjonsprosesseringsperspektivet. Feiltre, hendelsestre og datamining vil også være meget godt egnet. Visuelle metoder som CORAS gir gode oversikter over aktører og relasjoner mellom dem. Nettverksdiagrammer som viser hvilke kommunikasjonskanaler som er aktive vil også gi oversikt over hvem som kommunisere med hvem, men også hvem som ikke eller i mindre grad, er involvert i slik kommunikasjon.

I eksemplene hvor informasjonsprosesseringsperspektivet var sentralt vill CORAS ha kunnet blitt utnyttet med stort hell. Både i 9/11 i USA og i 22/7 i Oslo og på Utøya eksemplene var det manglende informasjonsutveksling mellom informasjonssystemer. Dette kunne vært analysert og visualisert med en kombinasjon av UML og CORAS. Også i de fleste andre eksemplene antas det at

CORAS ville kunne ha blitt benyttet med positiv effekt for å visualisere trusselbilder med estimater over sannsynligheter og konsekvenser. Ikke minst gjelder dette i tilfellet «David» og i Deepwater Horizon eksemplene hvor kommunikasjon av og forståelse for risikobildet var mangelfull. Hadde man gjennomført en analyse etter CORAS metoden i Barings Bank med fokus på Leesons aktivitet, ville det fort bli satt spørsmålstegn ved hans aktiviteter. I eksemplene fra romfartsvirksomheten og i Sleipner-A-eksemplet, er det vanskelig å se hvilken effekt CORAS analysen ville kunne gitt. Metoden har et fokus på sikkerhet som gjør at identifisering av tekniske feil muligens faller utenfor metodens fokusområder.

5.2.10 Dataprofilering

Bidraget som metodene fra kvalitetssikringsdomenet vil kunne gi til risikoanalysen, er først og fremst til risikoidentifisering men også som barrierer ved at etablerte profiler overvåkes over tid for å følge med i om det er positiv eller negativ utvikling i forhold til en mulig uønsket hendelse. Ved å sammenligne inndata med utdata enten ved å etablere profiler som sammenlignes, eller ved at spesifiserte algoritmer som er implementert i programkode testes med relevante data, isolert eller i den sammenheng det skal inngå i, kan feil bli oppdaget. Å spesifisere og gjennomføre slike kvalitetstester vil være et bidrag til risikoidentifisering.

Både i Mars Climate Orbiter- og i Ariane 5-eksemplet kunne et alternativ være å etablere en dataprofil forutsatt at en hadde tilgang til relevante og tilstrekkelig med testdata i systemet. En profil hvor inndata og utdata, som korresponderer med hverandre, ble etablert og sammenlignet, ville ha avslørt at det var uoverensstemmelser. Ved å etablere en profil på inndata og på tilsvarende utdata for Ariane 5 og for Mars Climate Orbiter kunne en sammenligne og avdekke uoverensstemmelser. Det er svært overraskende å observere at en kvalitetsgjennomgang med relevante testdata og inspeksjon av testresultatene i forhold til eksisterende spesifikasjoner, sannsynligvis ikke har blitt gjennomført i disse to eksemplene. En burde forvente at grundige verifikasjoner og tester ble gjennomført av slike kritiske komponenter. Det burde ikke være nødvendig med en forutgående risikoanalyse for å påpeke at slike kvalitetstester bør gjennomføres. Det bør være en selvfølge for alle kritiske komponenter som inngår i en tett kopling i et komplekst system.

For Deepwater Horizon var problemene at systemene teknisk sett ikke fungerte. En Dataprofilering ville være lite hensiktsmessig i dette eksemplet. Det samme for 22/7 i Oslo og på Utøya og i 9/11 i USA. Her er det så store mangler på de tekniske løsninger og på datautvekslingen mellom dem at andre analysemetoder hadde vært bedre egnet.

I Barings Bank ville en profil på på de transaksjoner i bankens systemer som hadde med Leesons virksomhet å gjøre, sannsynligvis sørget for nok oppmerksomhet til at det ble satt spørsmålstegn

ved hans virksomhet. Spesielt ville en synlig oversikt over de enorme beløpene som var i ubalanse på feilkontoen gitt bankens ledere informasjon om at noe var galt.

En profil som viser avhengigheter mellom tabeller i databasen og spesielt relasjoner og kompletthet mellom primærnøkler og sekundærnøkler kan være nyttig. Duplikater i data er også noe som bør vurderes. I tilfellet «David» er det mulig at dette ville ha identifisert uoverensstemmelsene som førte til feil-registreringer av data.

En dataprofil i Sleipner-A-eksemplet er det vanskelig å tenke seg ville ha noen effekt.

5.2.11 ISO-8000

Metoder basert på ISO-8000 vil kunne også ha vært anvendt i flere av eksemplene som en alternativ måte å identifisere «energi på avveie» på samme måte som ved dataprofilering beskrevet over. Som beskrevet i delkapittel 2.6.12 er det to typer kvalitetsgjennomganger som blir spesifisert i ISO-8000. Ved de syntaktiske sjekker blir grad av overenstemmelse med integritetsregler i et informasjons-system målt og elementer som avvik fra reglene, identifisert. Sjekkene skjer mot informasjons-systemets metadata. I forhold til eksemplet med «David» er det mulig at feilen er en syntaktisk uoverensstemmelse i informasjonssystemet. Når data «blir borte» kan det tyde på at dataene ikke blir knyttet til en eksisterende identifikator (for eksempel personnummer, pasient id) eller med andre ord, den refererte primærnøkkelen finnes ikke i systemet eller at peker til feil primærnøkkel blir etablert. Det er sannsynlig at en syntaktisk kvalitetssjekk (referensiell integritetssjekk) ville kunne ha avdekket en slik uoverensstemmelse.

De semantiske sjekker verifiserer at informasjonselementenes referansedata (i noen sammenhenger er dette en organisasjons masterdata) er i overenstemmelse når data overføres mellom to elementer, eller når to elementer sammenlignes. Metoder basert på ISO-8000 ville kunne ha avslørt manglende semantisk interoperabilitet i Mars Climate Orbiter-eksemplet. Spesifikasjonen var klare og utgjorde referansegrunnlaget. En gjennomgang med fokus på hvilke referanser som lå knyttet til hvert enkelt felt, kunne ha påvist feilen. I Ariane 5 var problemet uoverensstemmelse mellom to variabler som skulle holde de samme data. Dette kunne også ha vært avdekket med kvalitetssjekker. For eksempel med det som i ISO-8000-sammenheng betegnes som «kolonneintegritet» hvor maks verdier i felt blir verifisert. Både i Ariane-5 eksemplet og i Mars Climate Orbiter er det uoverensstemmelser i henholdsvis metadata (64-bit floating point og 16-bit signed integer) og referansedata (forskjellige enheter brukt for kraftpådrag).

Rent praktisk ville sjekker basert på ISO-8000 bli utført ved å benytte relevante testdata og være avhengig av ekspertvurdering både når det gjelder spesifikasjon av inndata og resultatdata. Sett i risikoanalysesammenheng vil datakvalitetsmetodene kunne brukes til risikoidentifikasjon og ikke tilføre noen nye muligheter i forhold til andre aktiviteter i analysen. Bidraget til risikoidentifikasjon

ville være gjennom å avdekke feil og mangler i informasjonssystemet ved å analysere de data som inngår som en del av eller er et resultat fra informasjonssystemet. Ved å bidra til å avdekke feil og mangler for videre risikoanalyse, er det en sammenheng hvor kvalitetssikringsmetoden både kan bidra til identifisering av feil og mangler som kan være en årsak til uønskede hendelser men også være barrierer ved at informasjon blir monitorert og verifisert i forhold til definerte kriterier.

5.2.12 Datamining

Datamining kan anvendes som barrierer som vist i eksemplet fra kortselskapene hvor «unormale» transaksjoner blir identifisert og fulgt opp. I forkant er det gjort analyser hvor hva som menes med «unormale» oppførsel er definert og, som i eksemplet fra kortselskapene, spesifisert hvor stort transaksjonsbeløpet må være for at dette skal betraktes som en sak som må følges opp.

Datamining kan også være et hjelpemiddel til risikobedømming. Ved å mine på historikk kan en se hvor ofte slike «unormale» transaksjoner har skjedd og se på hva konsekvensene har vært. Ut fra dette kan en avlede sannsynligheten for at det skal skje igjen og hvor store konsekvenser en slik hendelse har fått for selskapet. Dette vil gi bedre beslutningsstøtte for å kunne vurdere hvordan risikoen skal håndteres og hvor tiltak bør settes inn.

Datamining kunne ha vært et hjelpemiddel for etterretning i forkant av 9/11 i USA og 22/7 i Oslo og på Utøya-hendelsene. Kombinering av informasjon om terroristene fra forskjellige kilder, kunne ha ført til at informasjon om terroristenes forberedende aktiviteter kunne ha gitt spor i etterforskningen. I eksemplet fra 22/7 i Oslo og på Utøya er gjerningsmannen aktiv på sosiale media hvor han uttrykker ekstreme høyreekstremistiske meninger og oppsøker sider med høyreekstremistiske budskap. Han anskaffer våpen og store mengder kjemikalier, i tillegg er han en kjent person i politiets registre fra tidligere forhold. Hadde man hatt mistanke om at en terroraksjon var under planlegging kunne kombinasjonen av all denne informasjonen fra forskjellige registre, til sammen ha gitt politiet grunn til å etterforske gjerningsmannen før ulykken. Ved datamining søker man etter forekomster av «mønstre» som er av interesse. En må derfor vite på forhånd hva som skal søkes etter. «Mønsteret» i dette tilfelle er navnet på terroristen som man kunne «mine» etter i forskjellige kilder. Her hadde det også vært særdeles nyttig å kunne «mine» etter informasjon også i ustrukturerte databaser som elektronisk post, sosiale medier, tekstfiler, etc. For videre analyse kunne kunne slik informasjon samles og presenteres i et nettverk, som beskrevet i neste delkapittel.

I eksemplet 9/11 i USA kunne en, ved å kunne «mine» på den kollektive informasjon i FBI og CIA sine registre, sammen med flyselskapenes logger av transporterte personer, immigrasjons-myndighetenes logger over personer som krysser landegrenser kombinert etterretningsagenters personlige kjennskap til terroristene og at det var mottatt signaler om at et terrorangrep var

forestående, burde ha vært nok informasjon til at etterretningsorganisasjonene mer aktivt fulgte opp de personer som planla terroraksjonene.

Anvendt i Barings Bank-eksemplet kan man forestille seg at store unormale transaksjoner ble identifisert gjennom utligger analyser, slik at disse kom i fokus og ble fulgt opp. I tilfellet «David» ville man for eksempel kunne identifisere pasienter med diagnose men som ikke hadde noen oppfølging registrert. For eksemplene fra romfart ville neppe datamining ha hatt noen effekt. Her ville andre metoder ha vært mer til nytte. I Deepwater Horizon-eksemplet ville også fokus ha kunnet komme på den «energi på avveie» som eksisterte her. Men det samme ville kunne oppdages med langt enklere metoder. I Sleipner-A-eksemplet er det vanskelig å se at datamining ville ha hatt noen effekt.

Så lenge informasjonssystemene er strukturerte og regelbaserte kan de vanlige risikoanalysemetoder anvendes. Her finnes regler som er etterprøvbare. Når det gjelder ustrukturerte informasjons-systemer er situasjonen en annen. Her finnes ikke regler som kan etterprøves. Ustrukturert informasjon blir skapt og lagret i henhold til et verktøys funksjonalitet og behov. Store nettaktører samler i dag inn og krever eierskap til den enorme informasjonsmengden som legges ut på sosiale media. Det er stor usikkerhet forbundet med hvilke hendelser bruk av denne informasjonen kan føre til i fremtiden og til hva konsekvensene vil kunne være, både for mennesker og organisasjoner. Metadata som viser definisjoner og sammenhenger, må skapes og assosieres med informasjons-elementene for at slik informasjon skal bli meningsfull for andre verktøy enn det de er laget for. Til dette kan datamining ha stor nytte. Klassifisering av ustrukturerte data skjer ved hjelp av datamining-teknikker og gjør ustrukturert informasjon om til referansebaserte (semantiske) strukturer. «Utliggere» er et begrep som brukes i datamining-sammenheng. I risikoidentifisering kan en «utligger» være noe eller noen som ikke følger forventede regler eller har forventet adferd, noe som kan være grunnlag for videre analyse. I dataanalysen kan en utligger representere noe nytt som ikke er klassifisert tidligere og som kan være et mønster man benytter i den videre «miningen». På denne måten kan læring være en effekt.

Datamining kan bli misbrukt. Det er viktig at man er bevisst de nye trusler som oppstår når man kan kombinere informasjon fra mange kilder og gir en annen kontekst til informasjon enn den er ment for. Mange er uforsiktige med hva de publiserer på sosiale media. De er ikke bevisste at det som kommuniseres på offentlige media, enkelt kan fanges opp og benyttes av andre, og settes inn i en sammenheng som ikke var tiltenkt. Ikke bare offentlige instanser overvåker og gjenbruker informasjon fra offentlige kanaler men også private aktører som har kommersielle eller politiske interesser av slik informasjon. Det at vårt nasjonale lovverk nå omsider er endret til at informasjon som publiseres elektronisk skal betraktes på samme måte som informasjon publisert på papir, er en viktig barriere mot mobbing og personsjikane på nett.

Dersom Edward Snowdens påstand om at amerikanske myndigheter nå er i stand til å «avlytte» nesten alt (France24 2013) betyr dette at man kan gjøre massive innsamlinger av data. Dette innbefatter e-post, sosiale medier og filoverføringer. Store «eiere» av data som Google og Microsoft blir pålagt å levere data til myndighetene til etterretningsformål. Hva som er etterretningsformål er det da opp til myndighetene å definere. Mange mener at utviklingen nå er gått for langt.

5.2.13 Nettverksanalyse

I etterretningssammenheng vil metoder som nettverksanalyse brukes for å avdekke nettverk via for eksempel overvåkning av kommunikasjonskanaler og innsamling av informasjon om hvem som kontakter hvem, hvor ofte, når og på hvilken måte. Datamining vil kunne brukes til å søke etter og kombinere informasjon om personer i offentlige registre eller i andre informasjonssystem slik som beskrevet over, mens nettverksanalyse kan være et hjelpemiddel til å visualisere og analysere informasjon som er fremskaffet ved datamining.

5.2.14 Oppsummering av delkapitlet

«Energi på avveie» finnes i alle eksemplene som er gjennomgått. Det er snakk om å anvende kjente metoder for å identifisere den. I komplekse sammensatte systemer som de som er gjennomgått i eksemplene, blir oppgavene ofte svært vanskelig når man ikke har indikasjoner på hva som kan være feil. Å søke etter alle mulige eventualiteter av «energi på avveie» blir ofte i praksis en umulig oppgave. Her kan en fremgangsmåte som beskrevet i rammeverket i neste delkapittel være til hjelp.

HAZOP, FMEA, feiltre, hendelsestre og Bayesiansk nettverk ansett som særdeles god egnet for å kunne analysere risiko som kan relateres til Energi-/barriere-perspektivet. Det samme gjelder dataprofilering og metoder basert på ISO-8000. Siden det tidligere i oppgaven er konkludert med at «energi på avveie» er tilstede i alle eksemplene som er gjennomgått, kan en også slutte at disse analysemetodene ville kunne ha gitt resultater dersom benyttet i alle eksemplene.

Bayesiansk nettverk er sannsynligvis den metoden som er mest generell anvendbar. I alle eksemplene er det gjennom analysen av informasjonssystemenes rolle, påvist årsakssammenhenger som er velegnet til å bli analysert med denne metoden. I et Bayesiansk nettverk identifiseres variabler uavhengig av MTO-klassifisering, noe som gjør metoden anvendelig met komplekse og tett koplede systemer.

Sleipner-A-eksemplet skiller seg ut siden ingen av de gjennomgåtte metodene ville ha vært en innlysende kandidat til å avsløre «energien på avveie» i dette eksemplet. Konklusjonen er at involvering av tilstrekkelig ekspertise til å vurdere det designet og de beregninger som var gjort, er den eneste måten som dette ville kunnet ha blitt oppdaget på. I stor grad er dette et

kvalitetssikringsspørsmål og det er uvisst hvordan en med de gjennomgåtte risikoanalysemetoder ville kunne ha hatt noe effekt her.

De gjennomgåtte eksempler er hentet fra bransjer hvor det er en tradisjon for å gjennomføre risikoanalyser (Aven 2008). Sannsynligvis er det gjennomført en rekke analyser av de komplekse systemene som er beskrevet i eksemplene uten at disse står omtalt i den gjennomgåtte dokumentasjon. Det er mulig at informasjonssystemene ikke har blitt identifisert som problemområder og ikke har blitt inkludert i slike analyser.

5.3 ET RAMMEVERK FOR ANALYSE AV RISIKO I INFORMASJONS-SYSTEMER

I dette delkapittel diskuteres hvordan risiko i informasjonssystemer kan styres og analyseres. Det foreslås et rammeverk for hvordan dette kan gjøres.

5.3.1 Forslag til et rammeverk

Risikostyringsprosessen som definert av ISO (2009) er generell og gjelder også for informasjonssystemer. VAM beskriver en alternativ prosess hvor man systematisk starter med en organisasjons vitale funksjoner (steg 1) og ut fra disse identifiserer relevante informasjonssystemer (steg 2) og videre sårbarheten i disse informasjonssystemene (steg 3).

Risikoanalysen skal gi beslutningsstøtte. Metodene som brukes, må være tilpasset analysens formål (Aven 2008). Et uttrykt ønske fra beslutningstagere eller en etablert praksis i en organisasjon kan også være styrende i valg av analysemetode. Det samme gjelder kompetanse og erfaringer til den eller de som skal utføre analysen. I planleggingsfasen, hvor konteksten til analysen er i fokus (ISO 2009) (se figur 2 og 3), bestemmes hvilken metode eller hvilke metoder som skal benyttes. Risiko i informasjonssystemer har mange fasetter. Mange forskjellige spesialiserte metoder med forskjellige detaljeringsgrad er derfor nødvendige for å kunne ta de riktige beslutninger (Wiencke 2006). Eksemplene har vist at det på vesentlige områder kunne ha vært gjort analyser som ville ha gitt beslutningsstøtte i forhold til den risikoen som forelå.

Som hjelp til å finne best egnet analysemetode kan flere fremgangsmåter velges. Blant disse er:

1) Gjøre en grovanalyse som beskrevet i delkapittel 2.6.1.
2) Benytte fremgangsmåten beskrevet av Wiencke m.fl. (2006) som er omtalt i delkapittel 2.6.15
3) RANDs VAM ovenfra-og-ned *(«Top-down»)* metode som består av seks steg (Beskrevet i delkapittel 2.6.8). Steg 1-3 i denne metoden vil kunne benyttes som et grunnlag for å velge analysemetoder.

4) KITHs metode. Ifølge denne skal man starte enkelt og bli mer sofistikert etter hvert (Aksnes 2000).

Igjen er det konteksten rundt analysesituasjonen og beslutningssituasjonen som vil være det avgjørende for hvilken tilnærming en velger. Alle metodene vil kunne gi indikasjoner på hva en bør fokusere på i analysen og ut fra dette gi hjelp til å velge best egnet analysemetode. Ved å vurdere slike indikasjoner i forhold til ulykkesperspektivene vil en kunne få hjelp til bestemme fremgangsmåte og velge metode. I tabell 6 summeres opp en subjektiv bedømming av hvor godt egnet hver enkelt metode anses å være relatert til ulykkesperspektivene. Karaktersetting og egnethet er basert på diskusjonene i de to forrige delkapitler og er basert på eksemplene som er gjennomgått i oppgaven. Tabeller som summerer opp disse diskusjonene er tatt med i Vedlegg B.

	Grovanalyse	Feilte	Hendelsestre	FMEA	Sikker jobb Analyse (SJA)	HAZOP	KITHs risikoanalysemetodikk	RANDs VAM	CORAS	Datamining	Dataprofiling	ISO-8000	Bayesiansk nettverk	Nettverksanalyse
Energi-/barriere-perspektivet	G	S	S	S	M	S	N	G	N	M	S	S	S	N
Informasjons-prosessering-perspektivet	G	M	M	L	G	L	N	N	S	M	L	G	M	S
Normal ulykke-perspektivet	G	M	M	L	N	L	N	N	G	G	L	G	M	G
Høypålitelige organisasjoner	G	G	G	L	G	G	N	N	G	G	L	G	M	N
Målkonflikter	G	L	L	L	N	L	N	N	N	G	L	G	G	N
Menneskelig faktorer	G	L	L	L	G	L	M	S	S	M	L	G	M	G

Tabell 6: Subjektiv vurdering av metodenes egnethet i forhold til ulykkesperspektivene

Karakterskala som er benyttet i tabell 6:
S = Særdeles godt egnet, M= Meget godt egnet, G=Godt egnet, N= Noe egnet, L=Lite egnet

5.4 HVA SLAGS NYE METODER ER DET BEHOV FOR?

I dette delkapitlet diskuteres områder som ikke ville ha blitt avdekket med de gjeldende analysemetodene og hvor det er behov for nytenkning. Videre diskuteres hvilke metoder det i så fall er behov for.

5.4.1 Energi-/barriereperspektivet og behov for nye risikoanalysemetoder

Fra tabell 6 utledes det at metodestøtten er god når fokus for analysen er på kategori uønskede hendelser som i oppgaven er blitt relatert til Energi-/barriereperspektivet. «Energi på avveie» er noe som finnes og som kan identifiseres, analyseres og håndteres i en risikoanalyse. Gjennom planleggingen av risikoanalysen skal problemet en søker å løse defineres og en skal velge analysemetode. Ved analyse av et informasjonssystem støter en på mange utfordringer i forhold til hva en skal lete etter, hvor en skal lete og hvordan en skal lete. Riktig tilnærming til valg av

analysemetode vil være avgjørende for resultatet av analysen. En mulig fremgangsmåte for å avgjøre hvilken metode som er best egnet er beskrevet i kapittel 5.3. I tilfeller som Deepwater Horizon og eksemplet tilfellet «David» er det indikasjoner på at feil finnes, noe som vil være naturlig utgangspunkt når analysen skal planlegges. I de andre eksemplene er det ikke slike indikasjoner så her er må det velges en mer åpen tilnærming. I eksemplene fra romfart- og fra Sleipner-A burde feilene ha vært oppdaget dersom tilstrekkelig kvalitetssikringsaktiviteter var blitt gjennomført. Som beskrevet tidligere i oppgaven kunne dataprofilering og ISO-8000 baserte metoder vært anvendt til dette i romfartseksemplene. Sleipner-A designet og de beregninger som var gjort, burde ha blitt bedre verifisert av eksperter. Å oppdage «Energi på avveie» dreier seg derfor i mange tilfeller om å gjennomføre systematiske kvalitetssikringsaktiviteter. Gjennom kvalitetssikringsaktivitetene gjøres observasjoner som enten gjelder avvik fra direkte krav eller standarder og som må håndteres deretter, eller gir nyttig informasjon til bruk i planleggingen av en risikoanalyse. Dersom det blir besluttet å akseptere risikoen kan kvalitetssikringsmetoder anvendes som barrierer ved at kvalitet og innhold i en datastruktur analyseres og overvåkes i forhold til de risikoakseptkriterier som er definert.

Den subjektive bedømmingen som ligger bak karaktersettingen i tabell 6 er i hovedsak basert på gjennomganger av informasjonssystemer som håndterer strukturert informasjon. Her finnes det regler som er etterprøvbare og metadata som gir definisjoner og kontekst til informasjonen. For strukturerte regelbaserte informasjonssystemer er ikke utfordringen mangel på risikoanalysemetoder men som oftest at risikoanalyser ikke blir utført i tilstrekkelig grad. I dag er det volummessig mest ustrukturert informasjon som samles inn og lagres i informasjonssystemene. Dette gjør identifikasjon, klassifisering og kombinasjon av informasjon til en utfordring. Da det antas å ligge enorme fremtidige forretningsmuligheter i å kunne utnytte den ustrukturerte informasjonsmengden, investerer de store nettaktørene store midler på forskning for å finne nye måter å bruke denne på. Slagord som *big data is big business* brukes av enkelte store aktører når de beskriver motivasjonen for sin satsning. Ikke bare forretningsmuligheter vil oppstå, men også nye trusler mot personvernet og nasjonale reguleringer. I det moderne informasjonssamfunnet er nasjonale grenser ikke alltid like synlige. På godt og vondt.

«Energi på avveie» i ustrukturert informasjon kan være manglende intern integritet eller semantiske uoverensstemmelser slik som beskrevet i delkapittel 2.2.2. Å gjøre ustrukturerte data om til meningsfull informasjon er en utfordring. Den ustrukturerte informasjonen må klassifiseres og gjøres referansebasert før den kan kan kombineres med annen informasjon i et informasjons-system. Her vil de forskjellig teknikkene som inngår i metoden dataprofilering kunne anvendes. Når data er klassifisert og strukturert vil de tradisjonelle risikoanalysemetoder kunne anvendes.

Gjennomganger av ustrukturert informasjon vil selvfølgelig også kunne gjøres av eksperter ved tradisjonelle dokumentgjennomganger og ved å benytte risikoanalysemetodene på tradisjonell måte. Kunnskap og visdom til å forstå sammenhenger, forutse mulige uønskede hendelser, konsekvenser og bedømme den tilhørende usikkerhet vil uansett være den avgjørende faktor. I Sleipner-A-eksemplet ville dette sannsynligvis vært den mest hensiktsmessige måten å identifisere «energien på avveie». I dette ligger også en advarsel i at for mye fokus på informasjonssystemene kan være en fare. «Energi på avveie» kan være skjult i informasjonen og være uavhengig av de regler og strukturer som finnes i informasjonssystemene.

5.4.2 Informasjonsprosesseringsperspektivet og behov for nye risikoanalysemetoder

CORAS og nettverksanalyse anses å være de metodene som best støtter risikoanalyse av mulige hendelser som er relatert til Informasjonsprosesseringsperspektivet. Feiltre, hendelsestre, Bayesiansk nettverk og datamining vil også være metoder som anses å kunne gi gode resultater. UML er tradisjonelt brukt til å beskrive og analysere informasjonssystemer. UML beskriver forskjellige synsvinkler (*views)* som en kan betrakte et informasjonssystem fra. I forbindelse med informasjonsflyt er *Use case* synsvinkelen spesielt interessant. Her identifiseres de forskjellige roller (*actors*) i forhold til systemet og deres interaksjoner med systemet. UML vil også uten CORAS påbygningen, kunne brukes i risikoanalysen. Ved å lage *Use case* modeller vil en kunne visualisere funksjonalitet i systemet og også de forskjellige aktørene som har en rolle i forhold til systemet, enten som organisasjoner eller personer. UML modellene kan være grunnlag for en risikoanalyse på samme måte som den CORAS beskriver.

Informasjonsprosesseringsperspektivet er nært knyttet til Høypålitelige organisasjoner-perspektivet ved at effektiv informasjonsflyt er en forutsetning for at en organisasjon skal fungere optimalt. Det er et sykdomstegn i en organisasjon at mennesker ikke gir informasjon om observasjoner og erfarte problemer, at det ikke finnes et mottaksapparat for slikt eller at dette ikke blir tatt alvorlig. I enkelte organisasjoner blir mennesker som varsler om sine synspunkter stemplet som syndebukker og oppfattet som et problem. Dette et ledelsesproblem og et spørsmål om bedriftskultur. Det er en utfordring å endre holdninger i mange bedrifter med inngrodde tradisjoner. Datatilsynet og Teknologirådet (2012 s.43) beskriver et eksempel hvor man har fått positive resultater ved forbedret informasjonsflyt og ved å kombinere informasjon fra flere kilder:

> *«I kjølvannet av 11. september tok New York politiet nye grep for å gi politimannen i gata raskest mulig tilgang til all relevant informasjon om en hendelse. New York Police Department (NYPD)'s "Real Time Crime Center (RTCC)" samler, behandler og videreformidler informasjon mellom politifolkene på operasjonssentralen og de som er i felten. Med tilgang til registre om involverte personer og steder, som nødtelefonlogg, tidligere arrestasjoner, parkeringsbøter, bygningstegninger, veinett, osv. kan RTCC gi fortløpende informasjon til patruljene og supplere*

med nye ledetråder i etterforskningen. Systemet kobler sammen ulike datakilder som data fra et åsted, politiinterne data, samt offentlige datakilder. Resultatet er i følge New York-politiet høyere oppklaringsrate og bedre ressursbruk.»

RTCC kombinerer eksisterende informasjon i flere informasjonssystemer til hjelp i etterforskningen av forbrytelser men det gir også fortløpende informasjon til patruljene slik at de får en mulighet til å avverge uønskede hendelser. I en risikoanalysesammenheng kan dette sees på et mulig hjelpemiddel til å identifiserer mulige trusler og farer og komme disse i forkjøpet med hensiktsmessige tiltak. Samtidig kan slik informasjonsbruk også anses som en barriere ved at det blir enklere for politiet å overvåke personer som man mistenker for å kunne begå straffbare handlinger.

Datamining er også en måte å sammenstille informasjon om en eller flere persons aktiviteter på. Sætre (2007) beskriver den strategiske analysens plass i det kunnskapsbaserte politi og hvordan nettverksanalyse kan brukes til å kartlegge nettverk med personer man ønsker å etterforske. Datamining og nettverksanalyse er to metoder som kan kombineres for bruk i slike sammenhenger. Politiet må bli smartere. Men hvor smart vil vi at politiet skal bli? Datatilsynet og Teknologirådet (2013) er bekymret for hvordan ny teknologi bidrar til innsamling og kopling av personlig informasjon i stor skala. Ansiktsgjenkjenningsteknologi er allerede i bruk på sosiale nettsamfunn og søketjenester i USA men er blitt forbudt i Norge. Personers posisjonsdata logges av informasjonssystemer som Google maps, yr.no, apper i mobiltelefoner, osv. Motivasjonen for å gjøre dette er uklar men selskapene som gjør dette krever eierskap og disposisjonsrett til slik informasjon, mest sannsynlig for å skape grobunn for fremtidige forretningsmuligheter. Tradisjonelt har offentlige og organisasjoners informasjonssystemer vært ansett som den største trussel mot personvernet. Nå ser man for seg muligheten til å kople informasjon om enkeltpersoner med organisasjoners informasjonssystemer på nye måter for å skape nye forretningsmuligheter (Datatilsynet og Teknologirådet 2013 s. 44):

«Lignende verktøy kan politiet benytte for å avdekke tidligere ukjente sammenhenger i kriminalitetsdata og andre tilgjengelige datakilder. Trender og mønstre kan brukes til å sannsynliggjøre en fremtidig utvikling. Dette kan hjelpe politiet i å forutsi hendelser, fordele ressurser og kanskje til og med komme noen hendelser i forkjøpet.»

Det er viktig med et risikofokus i parallell med forskningen som pågår om utnyttelsesmuligheter for den enorme datamengden som skapes for sosiale formål. Metoder for analyse og styring av risiko må utvikles og tilpasses de nye teknologiske muligheter og løsninger.

5.4.3 Høypålitelige organisasjoner og behov for nye risikoanalysemetoder

I følge tabell 6 er det kun Bayesiansk nettverksanalyse som gir god metodestøtte for dette perspektivet. Bayesiansk nettverk får høy score fordi metoden kan kombinere teknologiske, organisasjonsmessige og menneskelige forhold når et komplekst system skal analyseres. Gjennom ekspertintervjuer vil en også kunne danne seg et bilde av om det er erfart problemer som kan være indikasjon på om MTO i samspill fungerer eller ikke.

Et kjennetegn ved Høypålitelige organisasjoner er evnen til spontan omstrukturering i spesielle situasjoner. Som en sannsynlighetsreduserende barriere mot uønskede hendelser i en organisasjons informasjonssystem, vil etablering av en stor grad av årvåkenhet ha effekt. Aven (2013c s7) sier:

> *«The new ways of thinking about risks are focusing on the risk sources: the signals and warnings, the failure and deviations, uncertainties, probabilities, knowledge and surprises, and the concept of mindfulness help us see these attributes and take adequate actions»*.

Høy grad av årvåkenhet vil også være en muliggjører for å bringe frem og utvikle gode ideer og muligheter. Grad av årvåkenhet gjenspeiler organisasjonskulturen og vil være styrt av hvordan organisasjonen ledes og hvordan de menneskelige samspill fungerer. Vurdering av grad av årvåkenhet i en organisasjon er noe som en relaterer til kvalitetsstyringsfaget. ISO-9000 er en serie standarder som er relatert til kvalitetsstyringssystemer i en organisasjon. Standardene kan være et godt utgangspunkt for å identifisere de områder en må stille krav og mål til for at ønsket grad av årvåkenhet skal oppnås. Høy grad av årvåkenhet er et risikoreduserende tiltak også for de risikoer man ikke vet eksisterer. Det er et lederansvar å sørge for styring, tiltak og stimuli til at årvåkenhet får utvikle seg. I organisasjoner som er preget av sterke tradisjoner, mange meninger, sterke personligheter og motvilje mot forandring er dette ikke enkelt. Eksemplene 22/7 i Oslo og på Utøya og tilfellet «David» viser at politiet og helsevesenet i Norge er eksempler på organisasjoner som har en vanskelig prosess foran seg før tilstrekkelig grad av årvåkenhet er på plass slik at organisasjonene kan klassifiseres som høypålitelige.

Et feilrapporteringssystem hvor en ikke bare fokuserer på feil i informasjonssystemet men også loggfører og systematiserer nesten-hendelser, erfarte brukerproblemer, synspunkter og ønsker, vil være et godt utgangspunkt når risikoanalyser planlegges og for å vurdere etablering av barrierer eller tilstandsovervåkning av barrierer. Oppfølging av feillogger, rapportering og fokus på feil må skje på et beslutningsdyktig nivå i organisasjonen. Regelmessige gjennomganger med forskjellige ekspertgrupper involvert og med forskjellige fokusområder, vil kunne gi et mer fullstendig og nyansert bilde som kan være til hjelp for å identifisere risiko samt forebygge barrierer. Identifisering av mulige hendelser med anvendelse av de tradisjonelle risikoanalysemetodene, definering av barrierer og ikke minst beredskap og trening i å håndtere identifiserte uønskede hendelser kan også være et hjelpemiddel til å håndtere uventede hendelser. Backup løsninger og

redundans, både i M, T og O sammenheng og ikke minst øvelser i å bruke disse, bør prioriteres. Trening og opplæring av personellet og ydmykhet i forhold til egen kompetanse slik at den ekspertise som er nødvendig for å løse problemer blir involvert, er også viktig. Problemer som ser enkle ut på overflaten kan ha en dypere årsak som krever dyptgående kunnskap og erfaring for å kunne forstå. Overfladiske *Quick fixes* har erfaringsmessig vist seg å bli en utløsende årsak til en uønsket hendelse.

Verktøy og metoder for å måle effektivitet og forbedring av organisasjoners yteevne og effektivitet er noe som tradisjonelt er gjort gjennom kvalitetssikring-, organisasjonsutvikling- og andre ledelsesutviklingsprosesser. Ofte defineres KPIer (*Key Performance Indicators*) for å kunne måle og sammenligne både endringer over tid og egenskaper i organisasjoner mot hverandre. KPIer for en organisasjons årvåkenhet med informasjonssystemer burde kunne defineres på samme måte, og bli brukt til å måle effekt som endringer og forbedringer fører til over tid. Spørsmålet som dukker opp er hvor skillet mellom kvalitetssikringsprosesser, risikostyringsprosesser og andre ledelsesprosesser går. Akademisk sett er dette en interessant diskusjon, i det daglige liv i en organisasjon eller et prosjekt, er dette ikke så viktig. Det viktige er å få frem et godt beslutningsgrunnlag for de avgjørelser og prioriteringer som lederne må ta.

5.4.4 Normale ulykker perspektivet og behov for nye risikoanalysemetoder

Perrows (1984) teori har som utgangspunkt store komplekse systemer. Når en skal gjøre en risikoanalyse av slike systemer er oversikt over totalsystemet og en forståelse for hvordan de ulike delene samvirker og påvirker hverandre nødvendig når analysen skal planlegges. Eksemplene har vist at grensesnitt mellom informasjonssystemer, andre teknologiske systemer, organisasjonsmessige systemer og menneskelig informasjonsutveksling ikke er lett å trekke. Informasjonssystemene er så integrert i det meste vi foretar oss at det er lite hensiktsmessig å betrakte disse isolert sett. Informasjons-systemene må sees i sammenheng med de funksjoner de er ment å betjene og understøtte og det totalsystemet det skal inngå i. En hensiktsmessig organisering av ansvar for informasjonssystemer, slik som Perrow (1984) anbefaler i forhold til Normal ulykkesperspektivet, vil derfor være et hensiktsmessig risikoreduserende tiltak.

I delkapittel 5.1.4 ble Internett analysert i forhold til Perrows organisering og inndeling av et system og i forhold til Normal ulykkeperspektivet. ENISA (2011) sier at Internett ikke garanterer minimum responstider eller et minimum av servicenivå. Til tross for dette virker Internett greit for de fleste mesteparten av tiden. Internett er billig å bruke og tjenester på nettet markedsføres også for sentrale organisasjonssystemer. Et eksempel her er såkalt *Cloud computing* hvor organisasjonens informasjonssystemer skal være tilgjengelig overalt og alltid basert på Internett tilgang. ENISA

(2011 s.165) stiller spørsmål om i hvor stor grad risikoanalyser blir gjort før man gjør seg avhengig av Internett:

> *«How resilient do we actually expect services that depend on the Internet to be? If constant, high quality access to 'the Cloud' is accepted as essential to how we run our lives and our business, have we fallen into a trap or false expectation?»*

Og (s.164)

«

1. *are the risks properly explained?*
2. *are they properly appreciated?*
3. *do the cost savings blind users to the risks?*
4. *what about the social costs?»*

Slike risikoanalyser er, som eksemplet viser, ikke kun av teknisk art. Her må organisasjoner og enkeltmennesker ut fra sin situasjon vurdere hvor stor feiltoleranse som kan aksepteres. For store organisasjoner hvor kontinuerlig tilgang til Internett er viktig, vil det være behov for løpende å ha risikoanalyser som gir grunnlag for beslutninger i forhold til de planer og forpliktelser som organisasjon inngår. Til denne type risikoanalyser vil i henhold til tabell 6, feiltre, hendelsestre og Bayesiansk nettverk kunne gi meget god metodestøtte. I tillegg vil også metoder fra økonomi og beslutningsanalyse kunne benyttes til dette.

5.4.5 Målkonfliktperspektivet og behov for nye risikoanalysemetoder

Det moderne informasjonssamfunn vil skape nye muligheter og nye trusler. Bill Gates (1999, s.98-99) sier at:

> *«The digital world certainly makes it tough and uncertain for business, but we will all benefit. We're going to get improved products and services, better responses to complaints, lower costs, and more choices. We're going to get better government and social services that cost a lot less. This world is coming»*

Verden er i endring, utvikling av informasjonssystemer og utbredelsen i bruk av informasjons-systemer bidrar til dette, som Bill Gates sier. Avhengigheten til informasjonssystemer og nødvendigheten av at disse er kontinuerlig attraktive og tilgjengelige øker. Dette gir ledelses- og prioriteringsutfordringer. Hvor mye ressurser skal organisasjonen bruke til å sikre informasjonssystemene, hvor mye anskaffe eller utvikle og hvor stor «teknisk gjeld» skal organisasjonen tørre å leve med, veid opp mot andre mål, er sentrale spørsmål.

Det er ikke funnet noen risikoanalysemetoder som skiller seg ut som meget godt egnet til å analysere risiko som kan assosieres med dette perspektivet. Et viktig beslutningsunderlag vil være en analyse av hvor stor den tekniske gjelden er for et informasjonssystem. Analysen må inkludere

en vurdering av mulig uønskede hendelser, konsekvenser og usikkerheten organisasjonen må leve med ved å akseptere denne gjelden. En slik analyse vil kunne kombineres med feiltre- eller hendelsestre-analyser, men estimat på «teknisk gjeld» vil være basert på ekspertgjennomganger og antagelser.

Tilstrekkelig med midler og kompetente ressurser til nødvendig verifikasjon og test i et systemutviklingsprosjekt, er nødvendig for å sikre at systemet virker som tiltenkt og er tilstrekkelig robust. Dette er ledelsesbeslutninger som må tas og hvor en slik vurdering vil være en del av beslutningsgrunnlaget. Teorier og metoder fra økonomi og beslutningsanalyse kan benyttes til dette.

5.4.6 Menneskelige faktorer og behov for nye risikoanalysemetoder

VAM og CORAS ansees å gi svært god metodestøtte for villede handlinger. Fokus i disse metodene er risikoanalyse med fokus på sikkerhet som også er det sentrale i Menneskelige faktor-perspektivet. I tabell 6 er også Bayesiansk nettverk, KITHs og datamining bedømt til å gi meget god metodestøtte.

Det amerikanske forsvar som alle andre moderne lands forsvar, er bekymret for konsekvensene av et villet angrep på landets kritiske informasjonssystemer. Den amerikanske forsvarets forskningsinstitusjon RAND har gjort en studie av det de betegner som MEII (*Minimum Essential Information Infrastructure*) og hvordan denne kan beskyttes i tilfelle et lammende angrep. I en omfattende rapport (RAND 1999 s.xiv) konkluderes det med at:

> *«We suggest it is more useful to think of the MEII as a process rather than a hardened stand-alone structure».*

Det RAND foreslår som en prosess er VAM-metoden som er gjennomgått tidligere i oppgaven. RAND mener at gjennom steg 1 i metoden, i tillegg til kartlegging av funksjoner, også inkluderes identifikasjon av hvilke funksjoner som nødvendige for å opprettholde de absolutt mest vitale funksjoner i det amerikanske samfunn etter et angrep. VAM-metoden kan benyttes til å identifisere hvilke systemer som støtter disse funksjoner, identifisere sårbarhet og adekvate sikkerhetsteknikker. Det understrekes at øving på krisehåndtering er viktig for å være sikker på at beredskapen virker.

Kanskje er RAND sin tilnærming verdt å se nærmere på også for organisasjoner utenfor forsvarssektoren. Et fullstendig sikkert system er ikke mulig å oppnå. Den etablerte måten å tenke IT-sikkerhet på er et kontinuerlig kappløp mellom nye tiltak og nye angrepsformer. Ikke bare enkeltpersoner men militære forskningsinstitusjoner deltar i dette «kappløpet». Cyberforsvar har blitt den fjerde gren i mange lands forsvar. Sikkerhetssystemene er blitt så store og uoversiktlige at de i seg selv blir en trussel. For mye sikkerhet og for mange begrensninger blir i seg selv et hinder for den kreativitet og dynamikk som er så viktig for å sørge for robuste informasjonssystemer. Fokus på kjernefunksjonalitet som må være tilstede for at organisasjonen skal fungere, etablering av

barrierer som må fungere for at slike funksjoner skal kunne opprettholdes og ikke minst øvelse i å håndtere kriser, vil kunne forhindre at uønskede hendelser blir lammende og at organisasjoner går til grunne som resultat av dette.

Datamining brukes også i sikkerhetssammenheng som beskrevet i delkapittel 2.6.13, til signaturbaserte systemer eller uregelmessighetsbaserte systemer. Systemene kan også utvikles til å lære – uregelmessigheter som gjentar seg blir akseptabelt mens noe som forekommer en gang, sjeldent eller i en uvanlig kombinasjon, er noe som er unormalt og må få oppmerksomhet.

6 KONKLUSJONER OG ANBEFALINGER

I oppgaven er risiko definert som mulige hendelser, hva konsekvensene kan bli og tilhørende usikkerhet. Risikoanalysen skal gi et grunnlag for de vurderingene og beslutningene som må tas for hvordan en skal forholde seg til de farer, trusler og muligheter som eksisterer. Som i andre vitale systemer i en organisasjon, skjer det sjeldent storulykker med informasjonssystemer. Eksemplene som er diskutert i oppgaven har vist at ulykkesperspektivene er svært relevante også for ulykker med informasjonssystemer.

Sleipner-A-ulykken skiller seg ut fra de andre eksemplene ved at det her er snakk om feil i informasjonsinnhold som ikke kan relateres til feil i informasjonssystemene eller til bruken av disse, og som det derfor er lite sannsynlig at noen av de analysemetodene som er sett på, ville kunne ha identifisert. Feil i informasjonsinnhold er vanskelig å identifisere når en ikke har et referansegrunnlag å sammenligne med. Det eksisterer i utgangspunktet ikke noe problemsituasjon som man er bevisst, og som kan gi hjelp til problemdefinisjonen. Tilstrekkelig med erfaringstall mangler for å kunne angi usikkerheten for storulykker på en meningsfull måte ved hjelp av frekvensbasert sannsynlighet. Det er derfor nødvendig å gjøre mange antagelser ved en slik vurdering. Antagelsene er det viktig å få formidlet til beslutningstagerne, slik at dette også blir en vesentlig del av beslutningsgrunnlaget. En drøfting av usikkerheten ut fra den kunnskapen og den subjektive sannsynligheten som eksisterer, kan ofte være mer hensiktsmessig. For styring av risiko i et informasjonssystem vil ISO-standard ISO-31000:2009 (ISO 2009) kunne anvendes da denne er utviklet som en generell standard og uavhengig av type anvendelse.

Det konkluderes med at det finnes gode og alternative metoder som kan brukes til å analysere risiko i forhold til Energi-/barriereperspektivet, Menneskelige faktorer-perspektivet og Informasjons-prosesseringsperspektivet. De tradisjonelle risikoanalysemetodene kan anvendes, i tillegg kan metoder fra datakvalitetsområdet være et godt supplement. Nytten av metodene fra datakvalitets-området vil være begrenset til hjelpemidler for risikoidentifikasjon når det finnes representative data som kan analyseres, og som barrierer ved at kvalitet blir kontinuerlig målt og rapportert i forhold til definerte kriterier. Datamining brukes i dag til å identifisere data som enten har felles egenskaper ved klassifiserings- og klusteringsteknikker, eller data som skiller seg ut ved utliggeranalyser. Datamining brukes i dag som barrierer. Et eksempel kan være at bank-transaksjoner som ikke er forventet ut fra en kundes normale praksis, overvåkes og følges opp. Innen datasikkerhet brukes datamining til å overvåke unormal oppførsel i nettaktiviteter. Datamining kan også brukes i risikoevalueringen ved mining i historiske data for å generere statistikk som grunnlag for sannsynlighetsvurderinger og risikobedømming. Datamining kan for eksempel brukes til å besvare spørsmål som hvor mye penger er det sannsynlig at banken vil tape på illegale banktransaksjoner og om det vil være lønnsomt å etablere og drive de nødvendige barrierene for å forhindre dette,

Metodestøtten er dårlig for perspektiver hvor M og O i MTO-forholdet, er mest i fokus som i Normal ulykkes-, Høypålitelige organisasjoner- og Målkonfliktperspektivet. Generelt sett handler disse tre perspektivene om hvordan en organisasjon fungerer. Dette er et område som er i fokus i blant annet organisasjonsteori og kvalitetsstyring. Vurdering av grad av årvåkenhet, beredskap og organisering i forhold til å håndtere uønskede situasjoner, samt de økonomiske prioriteringer som bestemmer sikkerhet og robusthet i en organisasjons informasjonssystem, er viktige faktorer både når usikkerheten rundt mulige hendelser og resulterende konsekvenser skal analyseres og barrierer planlegges. Bayesiansk nettverk skiller seg ut ved at en ved hjelp av metoden kan fokuserer på både M, T og O relaterte variabler, deres tilstand og innebygde avhengigheter.

I videre arbeid med forskningsspørsmålene bør det fokuseres på hvordan risikoanalysemetoder kan utvikles i takt med utviklingen innen informasjonsteknologi. CORAS er et eksempel på en modellbasert analysemetode som er videreutviklet fra UML, og som kan få stor nytte fordi UML er godt etablert i IT-bransjen. Risikoanalysemetoder som kan brukes i forhold til sosiale media og Internett er noe som det bør satses på fremover. Datamining er et godt utgangspunkt for dette.

Pressens faglige utvalg har sine etiske regler for hva som kan publiseres i media og overvåker at disse reglene blir overholdt. Ved å bruke Internett og sosiale media er vi nå «alle» blitt journalister uten at vi har fått den nødvendige skolering og oppdragelse som gis gjennom journalistutdanningen. Dette gjør at begrepet «nettvett» nå er blitt viktig for oss alle. Hva dette innebærer og hvordan det best kan praktiseres fremover, er et forskningsspørsmål det bør satses på. Opplæring og øving i «nettvett» er en oppgave både på alle nivåer i skolevesenet og også i jobbsammenheng og privat.

Hvordan en kan forebygge storulykker hvor informasjonssystemer er involvert, blir en utfordring i fremtiden. Den store erfaringsbasen og den avledede kunnskapen som ligger i ulykkes-perspektivene, kan være til god hjelp når en skal analysere risikoen og forebygge ulykker i informasjonssystemer.

7 REFERANSER

Al-Hakim, L. (2007): Information Quality Management:Theory and application. University of Southern Queensland, Australia

Anderson, R.H., Feldman, P.M., Gerwehr, S., Houghton, B., Mesic, R., Pinder, J.D., Rothenberg, J., Chiesa, J. (1999): Securing the U.S. Defense Information Infrastructure: A proposed Approach. RAND (National Defense Research Institute), USA.
http://www.rand.org/content/dam/rand/pubs/monograph_reports/1999/MR993.pdf
(siste nedlast 6.6.2013)

Anton, P.S., Anderson, R.H., Mesic, R., Scheiern, M. (2003): The Vulnerability Assessment & Mitigation methodology. RAND (National Defense Research Institute), USA.
http://www.rand.org/pubs/monograph_reports/MR1601.html
(siste nedlast 6.6.2013)

Aksnes, B., Vestad, A., Grøtan, T.O. (2000): Risikoanalyse. Metodegrunnlag og bakgrunnsinformasjon. KITH rapport nr. 13/00.
http://www.kith.no/templates/kith_WebPage____637.aspx (siste nedlast 8.9.2013)

Aven, T. (2013a). A conceptual framework for linking risk and the elements of the data-information-knowledge-wisdom (DIKW) hierarchy. Elsevier. Reliability Engineering and System Safety 111 (2013) s30-36.

Aven, T., Reniers, G. (2013b): How to define and interpret a probability in a risk and safety setting. Elsevier. Safety Science 51 (2013) s223-231

Aven, T., Krohn, B.S. (2013c): A new perspective on how to understand, assess and manage risk and the unforseen. Reliability Engineering and System Safety.
http://dx.doi.org/10.1016/j.ress.2013.07.005 (Siste nedlast 20.8.2013).

Aven, T. (2012): The risk concept-historical and recent development trends. Elsevier. Reliability Engineering and System Safety 99 (2012) s33-44.

Aven, T., Røed, W. og Wiencke, H.S. (2008): Risikoanalyse. Universitetsforlaget

Aven, T. (2007): Risikostyring. Universitetsforlaget

Bentos, J-P. (2001): Menneske – Teknologi – Organisasjon. Veiledning for gjennomføring av MTO-analyser. Pensum i UiS kurs FXMTS 110 Granskningsmetodikk høst 20012 (inkludert i kurskompendium), (UiS INVIVO).

Benson, P.R. (2009): ISO 8000 Data Quality – The fundamentals part 1. Real-World Decision Support (RWDS) Journal, Volumn 3. http://www.ewsolutions.com/resource-center/rwds_folder/rwds-archives/issue.2009-10-12.0790666855/document.2009-10-12.3367922336/view?searchterm=ISO%208000 (siste nedlast 26.8.2013).

Daconta, M.C., Obrst, L.J., Smith, K.T. (2003): The Semantic Web, A guide to the Future of XML, Web Services, and Knowledge Management. Wiley, USA.

Datatilsynet og Teknologirådet (2013): Personvern tilstand og trender 2013. Publisert på www.datatilsynet.no og www.teknologiradet.no

Dekker, S. (2006): The Field Guide to Understanding Human Error. Ashgate, Lund University, Sverige.

DoD (2007): US Department of Defence: Systems Engineering for Mission Success. Preliminary Design Review. Program Risk Assessment Checklist.
https://acc.dau.mil/CommunityBrowser.aspx?id=384096 (Siste nedlast 5.3.2013).

English, L (1999): Improving Data Warehouse and Business Information Quality, Wiley, USA.

ENISA (2011). Inter-X: Resilience of the Internet Interconnection Ecosystem, Full Report-April 2011. The European Network and Information Agency. http://www.internetsociety.org/deploy360/resources/enisa-report-resilience-of-the-internet-interconnection-ecosystem/ (siste nedlast 6.6.2013).

ESA (European Space Agency) (1996): Ariane 5 Flight 501 Failure, report by the Inquiry Board, 19.7.1996, Paris, Frankrike. http://esamultimedia.esa.int/docs/esa-x-1819eng.pdf (siste nedlast 6.6.2013).

Fowler, M (2004): UML distilled. Addison-Wesley.

France24 (2013): International news: Ex-CIA employee source of leak on PRISM program http://www.france24.com/en/20130609-former-cia-employee-source-us-intelligence-leaks-snowden-nsa (siste nedlast 27.9.2013).

FRISCO (1998): A Framework of Information System Concepts, Web Edition, International Federation for Information Processing (IFIP). http://cs-exhibitions.uni-klu.ac.at/index.php?id=445 (Siste nedlast 28.5.2013)

Gates, W (1999): Business @ the Speed of Thought. Pearson Education Limited, England.

Han, J., Kamber, M., Pei, J (2012): Data Mining. Concepts and Techniques. Morgan Kaufmann Publishers, USA

Hartvigsen, T., Feiring, A., Sand Haarberg, A.M., Korsveien, S., Skogan, D. (2011): Vurdering av Altinn II-plattformen for Nærings- og handelsdepartementet, DNV rapport 2011-1239. http://www.regjeringen.no/upload/NHD/Vedlegg/Rapporter_2012/altinn_sluttrapport_20120321.pdf (siste nedlast 26.8.2013)

ISO (2009): Risk management – Principles and guidelines, ISO-31000:2009

ISO (2009b): Risk management - Vocabulary, ISO GUIDE 73:2009

ISO (2011): Data quality – Part 1: Overview, ISO/TS 8000-1:2011

Jakobsen, B., Rosendahl, F. (1994): The Sleipner Plaftorm Accident. Structural Engineering International 3/94. http://www5.in.tum.de/~huckle/sleipner_Jakobsen.pdf (Siste nedlast 6.6.2013).

Lang, P. (2013): Digital dømmekraft. Kronikk i Dagsavisen 5.2.2013

Lee,Y.W., Pipino, L.L., Funk, J.D., Wang, R.Y., (2006): Journey to Data Quality. The MIT press, USA.

Lindsey, Ed (2008): Three-Dimensional Analysis. Data Profiling Techniques. Data Profiling LLC

Lund, M.S., Solhaug, B., Stølen, K. (2011): Risk Analysis of Changing and Evolving Systems Using CORAS. Springer, Heidelberg.

Løvås, G. (2004): Statistikk for universiteter og høgskoler. Universitetsforlaget, Oslo.

McDermid, J.A., Nicholson, M., Pumfrey, D.J., Fenelon, P. (1995): Experience with the application of HAZOP to computer-based systems. British Aerospace Dependable Computing Systems Centre and High Integrity Systems Engineering Group, Departement of Computer Science, University of York, UK. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.38.1568 (Siste nedlast 18.8.2013).

NASA (1999): Mars Climate Orbiter – Mishap Investigation Board, Phase 1 report. USA http://sunnyday.mit.edu/accidents/MCO_report.pdf (siste nedlast 6.6.2013).

NOU (Norges offentlige utredninger) 2012:14 (2012). Rapport fra 22-juli-kommisjonen. Departementenes sevicesenter. http://www.regjeringen.no/pages/37994796/PDFS/NOU201220120014000DDDPDFS.pdf (Siste nedlast 6.6.2013)

Perrow, C. (1984): Normal Accidents: Living with high-risk technologies. New York: Basic Books

Rosness, R., Guttormsen, G., Steiro, T., Tinmannsvik, R.K., Herrera, I.A. (2004): Organisational Accidents and Resilient Organisations: Five Perspectives. SINTEF Report

Reason, J. (1997): Managing the Risks of Organizational Accidents. Ashgate, USA.

Sivertsen, T.K. (2007): Risikoanalyse av samfunnskritiske IKT-Systemer. Teknologiske erfaringer. FFI/Rapport-2007/00910 http://rapporter.ffi.no/rapporter/2007/00910.pdf (siste nedlast 6.6.2013).

FAD (2007): Stortingsmelding nr. 17 (2006-2007): Eit informasjonssamfunn for alle. Det kongelege Fornyings- og administrasjonsdepartement. http://www.regjeringen.no/Rpub/STM/20062007/017/PDFS/STM200620070017000DDDPDFS.pdf (Siste nedlast 6.6.2013)

Statskonsult (1998): Erfaringer fra store statlige IT-prosjekt. Vurderinger og mulige tiltak. http://www.difi.no/statskonsult/publik/rapporter/fulltekst/R-1998-6.PDF (siste nedlast 6.6.2013)

Sætre, M. (2007): Analyser av kriminalitet. En innføring i data og metoder i samfunns-vitenskapelige og strategiske kriminalanalyser. Høyskoleforlaget.

The 9/11 report(2004): Final Report of the National Commission on Terrorist Attacks Upon the United States (2004). US Government Publications. http://www.gpo.gov/fdsys/search/pagedetails.action?granuleId=&packageId=GPO-911REPORT&fromBrowse=true (siste nedlast 7.8.2013)

Tjønn, H (2013): Verdens redningsmann hylles. Artikkel i Aftenposten 23.2.2013

Turner, B., Pidgeon, N.F. (1978): Man-made Disasters. Butterworth/Heinemann.

Vedeler, M., Eggesvik, O. (2013): «David» (60) dør av kreft etter datafeil. Artikkel i Aftenposten 11.3.2013.

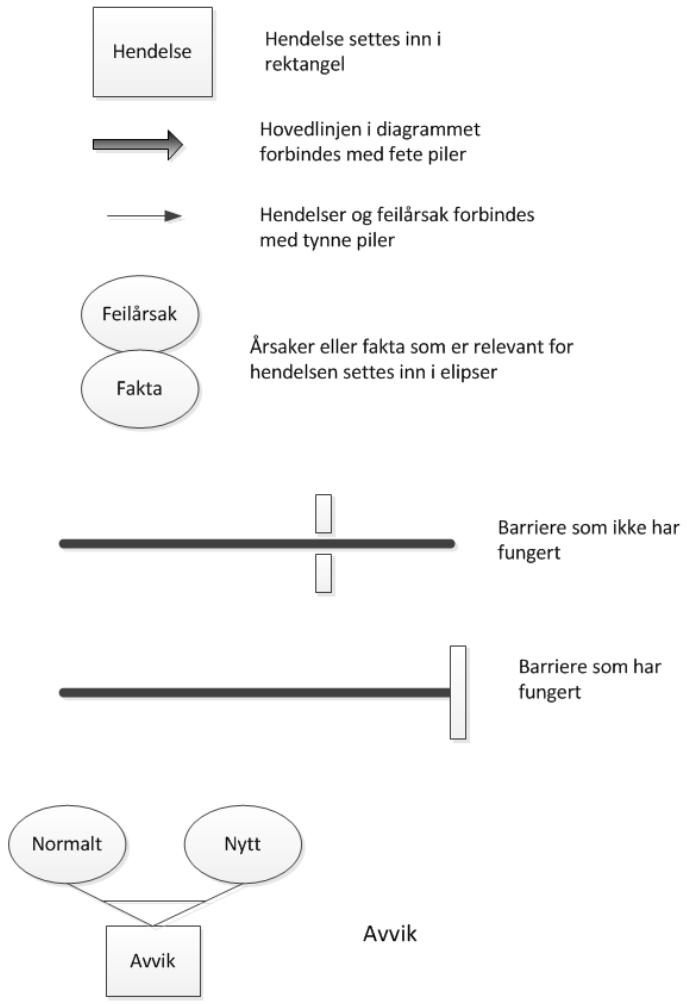
Vinnem, J.E., Utne, I.B., Skogdalen, J.E. (2011):Looking Back and Forward: Could Safety Indicators Have Given Early Warnings about the Deepwater Horizon Accident? Deepwater Horizon Sudy Group. Working Paper – Jan-2011. http://ccrm.berkeley.edu/pdfs_papers/DHSGWorkingPapersFeb16-2011/CouldSafetyIndicatorsHaveGivenEarlyWarningsAboutDeepwaterHorizonAccident-JES_IBU_JEV_DHSG-Jan2011.pdf (Siste nedlast 4.7.2013)

Wiencke, H.S., Aven, T., Hagen, J. (2006): A framework for selection of methodology for risk and vulnerability assesments of infrastructures depending on information and communication technology, Safety and Reliability for Managing Risks, Taylor & Francis Group, London

VEDLEGG A: Kort beskrivelse av MTO-(Menneske-Teknologi-Organisasjon) metodikken

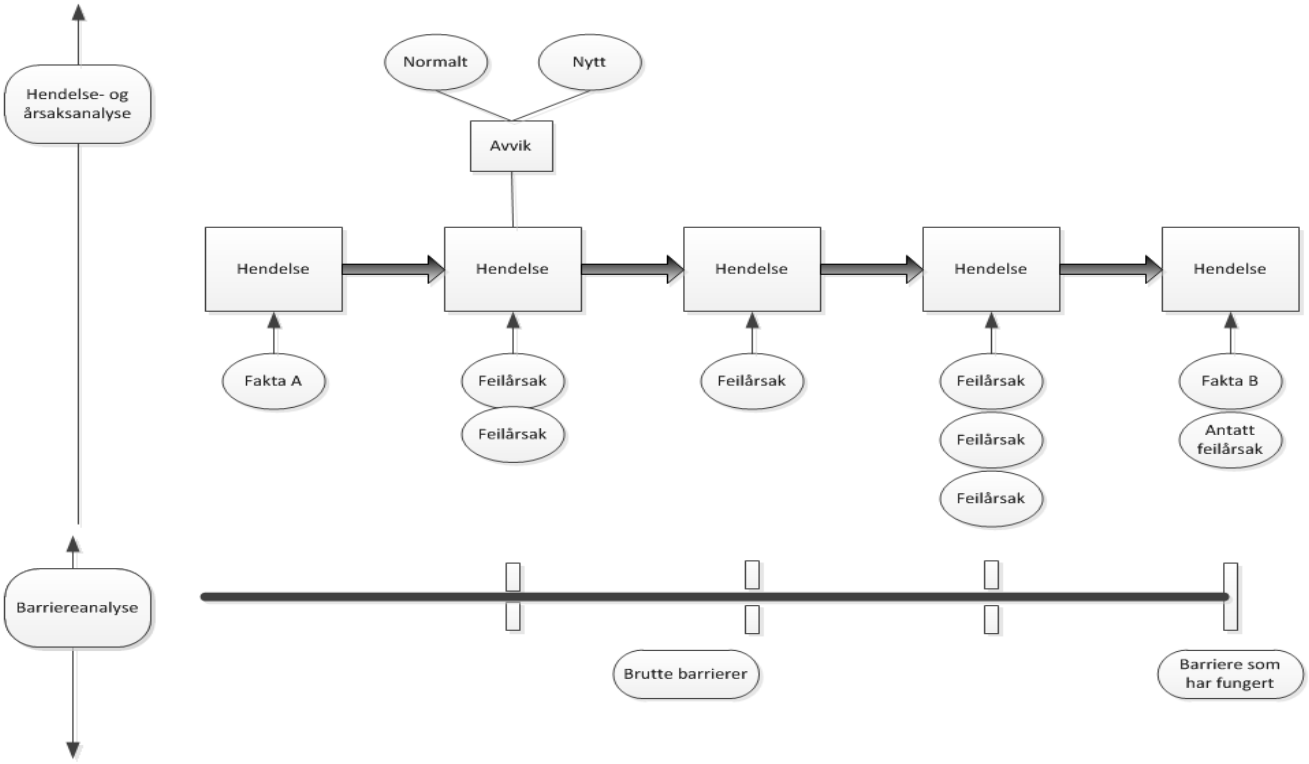
Det er funnet hensiktsmessig å gjøre en hendelse- og årsaksanalyse (som er en del av MTO metodikken) siden fokus i eksemplene i oppgaven er både M(Menneskelige), T(Teknologi) og O(organisasjonsmessige) forhold knyttet til informasjonssystemer. I henhold til MTO-metodikken (Bentos 2001) bør aktiviteter utføres i sekvensen som angitt i figur A3.

Figur A1 forklarer de symboler som er brukt i diagrammene:



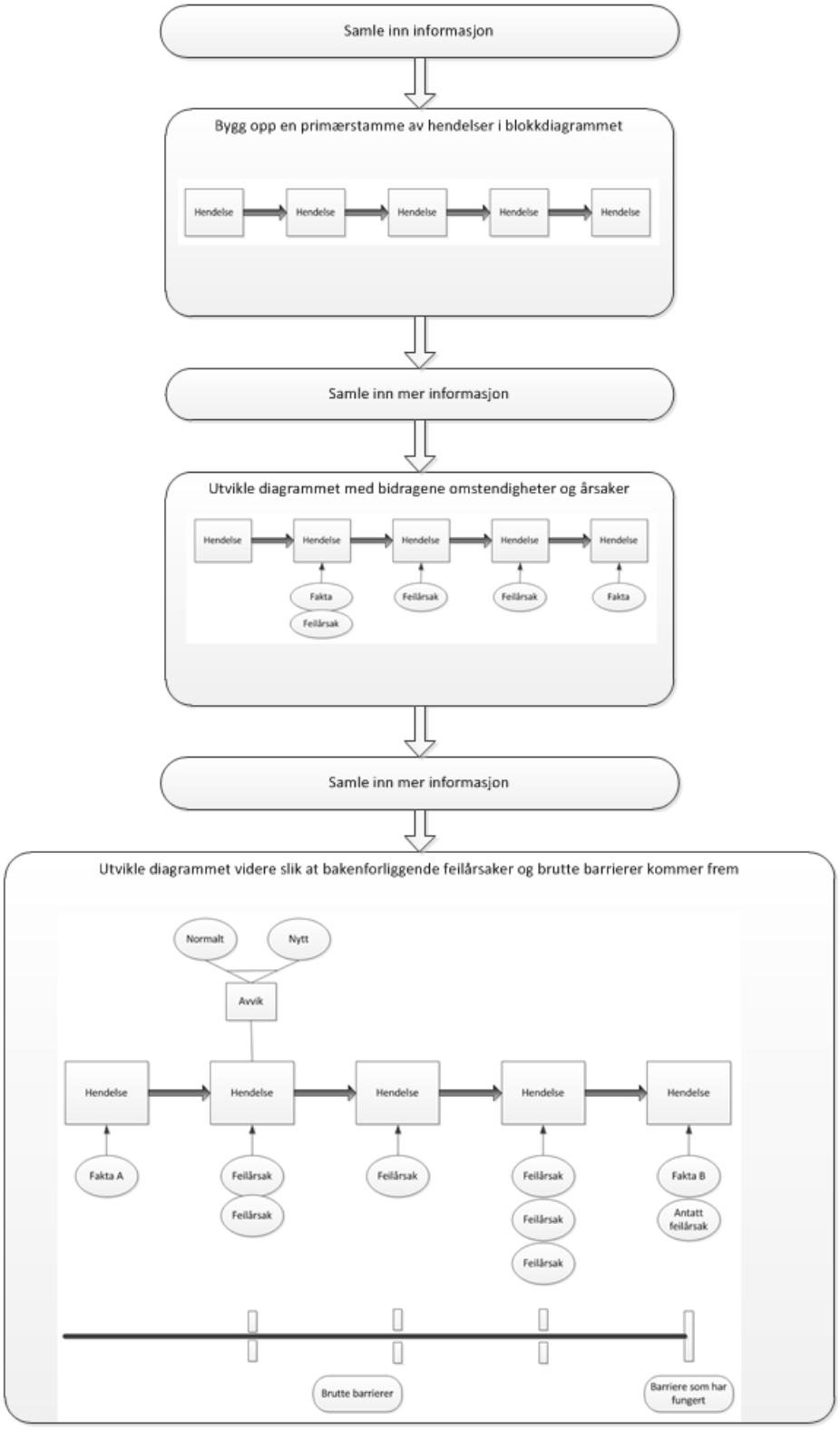
Figur A1: Forklaring på symboler brukt i illustrasjon av eksemplene

Figur A2 viser et komplett hendelses- og årsaksdiagram som er resultatet av en MTO analyse.



Figur A2: Hendelses- og årsaksdiagram

Figur A3 viser skjematisk fremgangsmåten i gjennomføringen av en hendelse- og årsaksanalyse i henhold til MTO metodikken.



Figur A3 viser fremgangangsmåten i henhold til MTO analysemetodikk.

VEDLEGG B: Gjennomgang av analysemetodene sett i relasjon til ulykkesperspektivene

I dette vedlegget er argumentasjonene som ligger bak etableringen av rammeverket som er foreslått i oppgavens delkapittel 5.3 tatt med tatt med. I tabellene under summeres diskusjonen som ligger bak den «score» som er gitt for hver enkelt analysemetode når disse er sett i forhold til ulykkes-perspektivene.

Grovanalyse og ulykkesperspektiv

Tabell C1: Grovanalyse og ulykkesperspektiv

Ulykkesperspektiv	**Hvordan kan grovanalyse benyttes til å analysere risiko relatert til angitt perspektiv i et informasjonssystem?**
Relevant for alle perspektiv	En grovanalyse vil kunne avdekke problemområder som relaterer seg til alle ulykkesperspektiv. Vanligvis vil ikke analysen være grundig nok til at problemet blir grundig analysert men kan være et hjelpemiddel til å planlegge mer detaljerte analyser og best egnede metoder for å gjøre dette. En grovanalyse kan være et godt startsted når man begynner en analyse av et informasjonssystem for å få en første oversikt over risikobildet for systemet.

Feiltre og ulykkesperspektiv

Tabell C2: Feiltre og risikoanalyse av informasjonssystemer

Perspektiv	**Hvordan kan Feiltre benyttes til å analysere risiko relatert til angitt perspektiv i et informasjonssystem?**
Energi-/barriere	Et feiltre er en visualisering av årsaker som i kombinasjon kan føre til en initierende hendelse. Metoden kan brukes både kvalitativt og kvantitativt.
Informasjonsprosessering	Dersom informasjon om organisasjonsmessige eller menneskelige forhold inkluderes i treet vil forhold som manglende kommunikasjon eller uønsket kommunikasjon kunne være medvirkenden årsak til en hendelse og komme frem av diagrammet.
Normal ulykke	Kan bidra til å visualisere komplekse interaksjoner.
Høypålitelige organisasjoner	Som et hjelpemiddel til barriereplanlegging.
Målkonflikter	Illustrasjoner som viser mulige årsaker kan være et nyttig beslutningsgrunnlag. Tilsvarende også kvantitative analyser.
Menneskelig faktorer	Menneskelige faktorer kan være en av flere årsaker som bidrar til en initierende hendelse og kan illustreres på feiltreet.

Hendelsestre og ulykkesperspektiv

Tabell C3: Hendelsestre og ulykkesperspektiv

Perspektiv	**Hvordan kan Hendelsestre benyttes til å analysere risiko relatert til angitt perspektiv i et informasjonssystem?**
Energi-/barriere	Et hendelsestre er en visualisering av konsekvenser av en initierende hendelse. Metoden kan brukes både kvalitativt og kvantitativt.
Informasjonsprosessering	Brudd på kommunikasjonskanaler eller uønsket spredning av informasjon kan være et resultat av en hendelse. Konsekvenser hvis dette opptrer vil kunne illustreres.
Normal ulykke	Konsekvenser av hendelser i både lineære og komplekse systemer kan analyseres.
Høypålitelige organisasjoner	Til analyse av nødvendighet for barrierer for å oppnå bedre robusthet i et informasjonssystem vil et feiltre kunne være et godt bidrag.
Målkonflikter	Til å lage et beslutningsgrunnlag kan illustrasjoner som viser mulige konsekvenser etter en hendelse være nyttig. En kvantitativ analyse vil vise antatt tap (eller gevinst) hvis hendelsen opptrer.
Menneskelig faktorer	Konsekvenser av menneskelige handlinger kan illustreres.

FMEA og ulykkesperspektiv

Tabell C4: FMEA og ulykkesperspektiv

Perspektiv	**Hvordan kan FMEA benyttes til å analysere risiko relatert til angitt perspektiv i et informasjonssystem?**
Energi-/ barriere	Dersom utført tilstrekkelig detaljert vil FMEA kunne avdekke latente feil og mangler i programlogikk. Anvendt riktig vil den kunne være svært nyttig i en software utviklingssammenheng hvor automatiserte tester kan gjennomføres fortløpende.
Informasjons-prosessering	FMEA fokuserer ikke på informasjonsbehandlingsaspekter som hvordan eller til hvem informasjon skal fordeles til. Fokus er på hva som er responsen i en teknisk komponent ved forskjellig input til komponenten.
Normale ulykker	Kompliserte systemer hvor det er bygget inn mye redundans er ofte dårlig egnet for FMEA.
Høypålitelige organisasjoner	FMEA er en ren teknisk orientert metode. Organisasjonsmessige forhold blir ikke vurdert.
Målkonflikter	Testing er omstendig og ressurskrevende og blir ofte en venstre-håndsjobb som blir nedprioritert.
Menneskelig faktorer	FMEA fokuserer på det tekniske system. Menneskelige feil kan oversees.

Sikker Jobb Analyse og ulykkesperspektiv

Tabell C5: SJA og ulykkesperspektiv

Ulykkesperspektiv	**Hvordan kan SJA benyttes til å analysere risiko relatert til angitt perspektiv i et informasjonssystem?**
Menneskelige faktorer	I utgangspunktet skulle en ikke tro at en metode som forbindes med å sikre fysiske arbeidsoperasjoner vil ha noen relevans for «myke» informasjonssystemer. Dersom man gjennom skole, foresatte, klubber etablerte en forståelse for at en må tenke gjennom de tre punktene som er målet for en SJA før en legger data om seg eller andre ut på Internett, ville muligens flere uønskede hendelser kunne bli avverget.
Målkonflikter	Gode og relevante testdata for tidlig testing av et informasjons-system er viktige for å verifisere at systemet virker som forventet. Sikkerhetsmekanismer for å beskytte slike data er ofte mangelfulle siden alle slike mekanismer ikke er på plass når tidlig test og verifikasjon startes. Det samme gjelder gjennomgang av nødvendige permanente sikkerhetsmekanismer. Her kan SJA med fordel benyttes for å få identifisert de trusler som en ønsker beskyttelse mot.

HAZOP og ulykkesperspektiv

Tabell C6: HAZOP og ulykkesperspektiv

Perspektiv	**Hvordan kan HAZOP benyttes til å analysere risiko relatert til angitt perspektiv i et informasjonssystem?**
Energi-/barriere	En strukturert gjennomgang, komponent for komponet, med betraktning av hva som er input og hva som er output fra hver komponent, vil kunne avdekke feil både i formater og i mulige verdier. I tillegg vil en slik analyse kunne være nyttig for å analysere om grensesnitt er optimalt konstruert. Vil eksport/ import til en komponent kunne nyttiggjøres av andre dersom spesifikasjonen ble endret.
Informasjonsprosessering	Dersom en inkluderer et menneske-maskin grensesnitt i analysen vil HAZOP kunne ha stor betydning i en risikoanalyse. Kan den informasjon som gis en operatør misforstås? Er den klar og entydig? Kan det oppstå misforståelser i gitte situasjoner? Er symbolbruk (F.eks. bruk av fargekoder) konsekvent og utvetydig?
Normal ulykke	En systematisk gjennomgang av for eksempel et UML sekvensdiagram, som beskriver logikken i et informasjonssystem, kan være en måte å utføre en HAZOP på.
Høypålitelige organisasjoner	HAZOP analyser er nyttige for å kunne bygge robuste systemer.
Målkonflikter	HAZOP er en tid og ressurskrevende metode.
Menneskelig faktorer	HAZOP kan brukes til å analysere brukergrensesnitt og være et hjelpemiddel til å avdekke hvor operatørfeil vil kunne skje og hvilke barrierer som derfor bør etableres.

Bayesiansk nettverk

Tabell C7: Bayesiansk nettverk

Perspektiv	**Hvordan kan Bayesiansk nettverk benyttes til å analysere risiko relatert til angitt perspektiv i et informasjonssystem?**
Energi-/barriere	Et Bayesiansk nettverk er meget anvendelig i situasjoner der vi kan sette opp årsakssammenhenger og forhold som påvirker hverandre. Komplekse mulige årsaksforhold kan derfor modelleres og analyseres, noe som kan avsløre konsekvenser dersom «energi på avveie» får utvikle seg. Dette kan igjen være basis for mer detaljerte gjennomganger og analyser med andre metoder.
Informasjonsprosessering	Metoden fokuserer ikke spesielt på de tekniske egenskaper men også på andre forhold (variabler) som påviker systemet.
Normal ulykke	Bayesianske nettverk er godt egnet til å analysere tett koplede og komplekse systemer.
Høypålitelige organisasjoner	Metoden fokuserer på organisasjonsmessige og menneskelige påvirkninger som variabler på lik linje med de tekniske. Sammenstillingen av dette vil være et grunnlag for å analysere og identifisere områder hvor stor grad av årvåkenhet er påkrevd.
Målkonflikter	Til å lage et beslutningsgrunnlag kan illustrasjoner som viser mulige konsekvenser etter en hendelse være nyttig. En kvantitativ analyse vil vise antatt tap (eller gevinst) hvis hendelsen opptrer.
Menneskelig faktorer	Konsekvenser av menneskelige handlinger kan illustreres.

KITHs metodikkog ulykkesperspektiv

Tabell C8: KITHs metodikk og ulykkesperspektiv

Perspektiv	**Hvordan kan KITHs risikoanalysemetodikk benyttes til å analysere risiko relatert til angitt perspektiv i et informasjonssystem?**
Energi-/barriere	Noe relevant siden en generell risikoanalyse vil kunne avdekke farer i form av latente feil i organisasjon eller tilgangssystemer. Tilsvarende vil metoden også kunne avdekke mangler i barrierer.
Informasjonsprosessering	Metoden fokuserer ikke på manglende informasjonsflyt i en organisasjon men er opptatt av hvordan autorisasjonsbarrierer kan hindre uønsket tilgang til informasjon. Klassifisering av og tilgang til informasjon er også et fokusområde.
Normal ulykke	Sterkt fokus på tilgangssystemet og oppbyggingen av dette.
Høypålitelige organisasjoner	Fokus på en beredskapsplanlegging, sikkerhetsorganisasjon, oppfølging av systemdrift. Aspekter rundt «mindfulness» som fokus på feil, drift, robusthet, ekspertise, autoritet, etc. vil være sentrale tema med denne metoden.
Målkonflikter	Ikke et tema direkte men etablering av sikkerhetstiltak vil koste penger og nødvendiggjøre prioriteringer slik at dette indirekte blir berørt.
Menneskelig faktorer	Hovedfokus er på sikkerhet. Sikkerhetspolitikk, adgangskontroll, fysisk sikkerhet for å hindre at villede uønskede handlinger kan bli utført, er sentralt i denne metoden

RANDS VAM og ulykkesperspektiv

Tabell C9: RANDs VAM og ulykkesperspektiv

Perspektiv	**Hvordan kan VAM benyttes til å analysere risiko relatert til angitt perspektiv i et informasjonssystem?**
Energi-/barriere	En systematisk gjennomgang iht. VAM metoden vil kunne avdekke om det er områder man bør gjennomgå for å avdekke sikkerhetsutfordringer. Mer detaljerte gjennomganger av utvalge områder kan gjøres basert på resultatet etter en VAM analyse
Informasjonsprosessering	Avhengig av hvilke aspekter og kontroller en legger inn i matrisen vil en kunne avdekke risiko relatert til dette perspektivet
Normal ulykke	Avhengig av hvilke aspekter og kontroller en legger inn i matrisen vil en kunne avdekke risiko relatert til dette perspektivet
Høypålitelige organisasjoner	Avhengig av hvilke aspekter og kontroller en legger inn i matrisen vil en kunne avdekke risiko relatert til dette perspektivet
Målkonflikter	Sikkerhetsutfordringer kan ofte medføre en avveining om hvor mye beskyttelse en skal velge (ref. konflikten mellom produksjon og beskyttelse illustrert i figur 14)
Menneskelig faktorer	Siden menneskelige faktorer assosieres med sikkerhet og metodens hovedformål er å avdekke sikkerhetsrisiko så vil den ha stor anvendelighet innenfor dette område.

CORAS og ulykkesperspektiv

Tabell C10: CORAS og ulykkesperspektiver

Perspektiv	**Hvordan kan CORAS benyttes til å analysere risiko relatert til angitt perspektiv i et informasjonssystem?**
Energi-/barriere	Metoden fokuserer ikke på spesifikt på innhold eller tekniske egenskaper i et informasjonssystem. Fokus er aktører og deres relasjoner til informasjonssystemet. Analysen gir gode oversikter og kan være et hjelpemiddel til å identifisere områder som må detaljeres grundigere med andre metoder.
Informasjonsprosessering	Diagrammene gir gode oversikter over aktører og relasjoner mellom dem. Dette kan være med på å avdekke manglende kommunikasjonslinjer eller ikke optimal organisering av informasjonsflyt. Samtidig vil analysen identifisere sikkerhetsaspekter med informasjonsflyten og være et godt hjelpemiddel til å planlegge og gi oversikt over barrierer.
Normal ulykke	Til planlegging av feiltoleranse (redundans) vil metoden være godt egnet. Konsekvensen av feil eller sikkerhetsbrudd vil kunne illustreres og også hvor tiltak for å forbedre systemets robusthet bør iverksettes. Aktørenes roller (f.eks. i form av sentral-, desentral styring) vil også kunne illustreres og analyseres.
Høypålitelige organisasjoner	Metoden fokuserer på roller, aktører og samhandlingsmønstre. Som basis for å analysere hvor dynamisk organisasjonen er til å tilpasse seg endringer eller uventede hendelser, vil CORAS diagrammer gi et godt grunnlag.
Målkonflikter	Sikkerhet koster penger og nødvendiggjør prioriteringer. Gode oversikter og analyser vil være et hjelpemiddel i de ledelses-beslutninger som skal tas.
Menneskelig faktorer	Fokusområdet for CORAS er sikkerhet og er derfor svært godt egnet til å illustrere mulige menneskelige trusler mot informasjonssystemene. Illustrasjonene formidler trusselbilder på en enkel og lettfattelig måte.

Dataprofilering og ulykkesperspektiv

Tabell C11: Dataprofilering og ulykkesperspektiv

Perspektiv	**Hvordan kan Dataprofilering benyttes til å analysere risiko relatert til angitt perspektiv i et informasjonssystem?**
Energi-/barriere	Vil være et effektivt hjelpemiddel til å identifisere latente feil og mangler i strukturerte informasjonssystemer. Ved hjelp av regler, statistikk, metadata og subjektiv vurdering av enkeltdataelementer eller kluster av informasjonen kan enkeltforekomster av data som skiller seg ut identifiseres for nærmere inspeksjon.

ISO-8000 – Information Quality Management og ulykkesperspektiv

Tabell C12: ISO-8000 og ulykkesperspektiv

Perspektiv	**Hvordan kan integritetsregler benyttes til å analysere risiko relatert til angitt perspektiv i et informasjonssystem?**
Energi-/barriere	Anvendelse av integritetssjekker vil kunne avdekke inkonsistenser i datastrukturer og referanser og i den forbindelse kunne være til hjelp for å identifisere risiko i forhold til ukomplett eller feilaktig datainnhold i et informasjonssystem. Integritetssjekker er regelsjekker basert på metadata og trenger faste definerte regler som etterprøves. Anvendelsen vil derfor være for strukturerte eller semantiske strukturer hvor slike regler finnes.
Informasjonsprosessering	Inkonsistenser mellom informasjonssystemer som bruker data fra samme kilde, vil kunne være årsak til en uønsket hendelse. Verifikasjoner vil kunne avdekke om brukeren er tilfreds med informasjonen som blir gjort tilgjengelig for han, om sikkerhet er ivaretatt og om informasjonene presenteres for brukeren på en optimal måte.
Normal ulykke	Gjennom sjekker vil en kunne avdekke om det er sider ved informasjonssystemet som oppleves som spesielt sårbart, hvor redundans bør bygges inn eller manuelle rutiner etableres som en backupløsning i tilfelle feil.
Høypålitelige organisasjoner	En vil kunne måle i hvor stor grad data er konsistente og korrekte. Effekten av kontinuerlige forbedringsprosesser vil kunne måles i forbedret datakvalitet.
Målkonflikter	Metoden kan, ved kartlegging av årsaker til feil i informasjons-systemer, bidra i et beslutningsgrunnlag om nødvendige forbedringer eller nyanskaffelser.
Menneskelig faktorer	Metoden fokuserer ikke på utvikling eller forvaltning av informasjonssystemer. Kun på tekniske egenskaper og vil derfor ikke være egnet for å analysere risiko knyttet til dette perspektiv.

Datamining og ulykkesperspektiv

Tabell C13: Datamining og ulykkesperspektiv

Perspektiv	**Hvordan kan Data mining benyttes til å analysere risiko relatert til angitt perspektiv i et informasjonssystem?**
Energi-/barriere	Data mining kan brukes til å avdekke såkalte «utliggere» i informasjonen. Dette er informasjon som skiller seg vesentlig ut fra annen tilsvarende informasjon i en mengde. En «utligger» kan være en feil eller det kan være noe som representerer noe som er annerledes og som kan være en mulighet til forandring. Identifiserte «utliggere» analyseres ofte videre med manuell inspeksjon og oppfølging.
Informasjonsprosessering	Datamining kan også brukes til å lage oversikter, statistikk etc. på hvem som kommuniserer med hvem, hvor mye, på hvilken måte, når. Eksempelvis kan informasjon om en person fra forskjellige informasjonssystemer, kombineres for å få et mer komplett bilde av personens kontaktnettverk. I etterretnings-sammenheng kan opplysninger om kontaktnettverk etableres fra sosiale media, E-mail, telefon. Analyse av slik informasjon kan brukes til å identifisere risiko og til å etablere sannsynlighets-reduserende barrierer.
Normal ulykke	Datamining kan brukes til å skape oversikter over avhengigheter og både lineære og komplekse interaksjoner i et system. Kombinert med statistikk på bruk, kan kritiske komponenter identifiseres og grunnlag for analyser av tekniske forhold som vil kunne være årsak til initierende hendelser.
Høypålitelige organisasjoner	Statistikk over bruk, feilmeldinger, henvendelser til «helpdesk», nesten hendelser og virkelige hendelser, endringsønsker, driftsproblemer, sikkerhetsbrudd er eksempler på informasjon som det kan mines i for å lage grunnlag for analyser for å kunne gjøre et informasjonssystem mer robust.
Målkonflikter	Data mining benyttes ofte som en muliggjører i organisasjon for salg og markedsføring (hva er typiske karakteristikker(alder, sosial status, inntekt, utdanning, etc.) for de som kjøper vårt produkt). Ofte kombineres data mining med en organisasjons datavarehus som er etablerert for å holde oversikt over salg, produkter, kunder og muligheter.
Menneskelig faktorer	«Utliggere» kan også være informasjon om personer med annerledes eller uforutsett adferd og kan være en indikasjon på en forbrytelse. Store pengeuttak fra en konto kombinert med en geografisk plassering som vanligvis ikke benyttes for denne kontoen, kan eksempelvis være en indikasjon på en slik forbrytelse. Data mining kan også være søk på tvers av flere informasjonssystemer for å kombinere informasjon om en bestemt person i en etterforskning eller overvåkningssammenheng.

Nettverksanalyse og ulykkesperspektiv

Tabell C14: Nettverksanalyse og ulykkesperspektiv

Perspektiv	**Hvordan kan Nettverksanalyse benyttes til å analysere risiko relatert til angitt perspektiv i et informasjonssystem**
Energi-/barriere	Som vist i eksemplet over kan mønster i organisert virksomhet avdekkes gjennom å se på relasjoner og hendelser over en tidsperiode.
Informasjonsprosessering	Nettverksanalyse kan være spesielt interessant i forbindelse med å kartlegge hvem som kommuniserer med hvem i en organisasjon som basis for å diskutere om denne kombinasjonen er optimal eller om tiltak bør iverksettes for å sikre at personer får den informasjonen de trenger for å kunne utføre sine arbeids-oppgaver på en sikker og funksjonell måte.
Normal ulykke	Nettverkstrafikk, visualisering og analyse av hvilke noder i et nettverk som kommuniserer med hverandre, hvor mye, når, belastningstopper kan være nyttig informasjon for identifisering av kritiske komponenter og planlegging av redundans.
Høypålitelige organisasjoner	Positive relasjoner mellom mennesker i en bedrift er viktig for å sikre høypålitelighet. Gjennomganger av prosjekter kan være et eksempel hvor man ser på om personer med den riktige ekspertise har blitt involvert.
Målkonflikter	For å planlegge organisasjonsendringer, kartlegge effektivitet hos medarbeidere og avdekke personlige nettverk i en organisasjon kan denne metodikken anvendes. Kjøreruten til en sjåfør i en bedrift over tid kan logges for å se om denne er hensiktsmessig og effektiv. Utfordringen her er ivaretagelse av personvernet.
Menneskelig faktorer	I etterforskning og i kartlegging av relasjoner mellom personer man mistenker for forbrytersk organisasjon, benyttes denne metoden aktivt. Hvem som kommuniserer med hvem (telefon, e-mail, sosiale nettverk) hvor mye, på hvilken måte og når, kan kartlegges. Det hender at noen av forskjellige grunner blir holdt utenfor på en arbeidsplass, anvendelse av uakseptable hersketeknikker, mobbing og trakassering skjer dessverre også. Ved undersøkelse av slike forhold vil også nettverkskartlegging og analyse kunne være et hjelpemiddel.

Ekspertintervju og ulykkesperspektiv

Tabell C15: Hvordan kan ekspertintervju benyttes i risikoanalyse av informasjonssystem

Perspektiv	**Hvordan kan ekspertintervju benyttes til å analysere risiko relatert til angitt perspektiv i et informasjonssystem?**
Alle	Identifisere mulige initierende hendelser knyttet til alle ulykkesperspektiv ut fra en inngående kjennskap til det informasjonssystemet som er aktuelt. For å vurdere mulige konsekvenser dersom den initierende hendelsen inntreffer. Til å vurdere hvilke barrierer som vil være de best egnede. I tilfeller hvor en mangler grunnlag for å anslå sannsynligheten for om en hendelse vil inntreffe, kan en eksperts vurdering være nyttig i beslutningsprosessen.