UNIVERSITETET I STAVANGER

MASTERGRADSSTUDIUM I

SAMFUNNSSIKKERHET

MASTEROPPGAVE

SEMESTER:

Våren 2010

FORFATTER:

Stine Spørkel

VEILEDER:

Ole Andreas Engen

TITTEL PÅ MASTEROPPGAVE:

INTEGRERTE OPERASJONER
i et informasjonsperspektiv

EMNEORD/STIKKORD:

Ny teknologi, integrerte operasjoner, sikkerhetskultur, mentale modeller, målkonflikter, informasjon og kommunikasjons problematikk.

SIDETALL: 99

STAVANGER : ……15.6.2010……

DATO/ÅR

FORORD

Innledningsvis vil jeg takke min veileder Ole Andreas Engen for hans fantastiske veiledninger. Min bror for hans korrekturlesing. Vil takke min familie og venner for deres tålmodighet når jeg var stresset. Og til slutt vil jeg takke Øyvind Hebnes for hans enestående konstruktive innspill i prosessen.

SAMMENDAG

Denne masteroppgaven har som mål å avdekke hvilke sikkerhetsmessige utfordringer som oppstår ved implementering av ny teknologi. For så å vurdere hvordan utfordringene vil vise seg ved implementeringen av integrerte operasjoner på norsk sokkel.

For å kunne svare på problemstillingene ble det gjennomført en dokumentanalyse, for å avdekke hvilke faremomenter ny teknologi kunne introdusere, basert på antakelsen at implementering av ny teknologi er innføring av informasjon. Analysen avdekket at innføring av ny teknologi skaper en tilstand som preges av at organisasjonen har manglende tilgang på sikkerhetskritisk informasjon. Manglende informasjon gjør det vanskelig å kartlegge risikoen teknologien kan innføre (fase en). Og prosessen hvor teknologien tilpasses den lokale konteksten (fase to), kan representere en risiko dersom informasjonen i endringene ikke identifiseres og implementeres. Når et teknologisk element endrer seg, må også organisasjoner sørge for å endre andre elementer, for å unngå at disse kommer i konflikt og forårsaker ulykker.

For å få svar på hvordan utfordringene med ny teknologi vil vise seg når IO implementeres på norsk sokkel, ble det foretatt en dokumentanalyse. Analysen avdekket at IO systemet er preget av avstand og kompleksitet som kan forsterke risikoen som ny teknologi introduserer. Avstanden kan føre til en differensiert sikkerhetskultur. Sikkerhetskulturen som preger bransjen vil avgjøre hvor mye av informasjonen i endringene som identifiseres, deles og implementeres i systemet. Analysen avdekket at bransjen har hatt varierende fokus på sikkerhet. Ulikt fokus og ulike fortolkningsrammer kan resultere i at partene tar i bruk teknologien ulikt. Skjer dette kan de teknologiske elementene komme i konflikt og resultere i en uønsket hendelse.

Avstanden vil også gjøre det vanskelig for aktørene å ha gode mentale modeller, som er avgjørende for å unngå ulykker. At systemet er komplekst og preget av automatiseringer, utfordrer muligheten til å ha gode mentale modeller ytterligere. Dårlige mentale modeller har vært en medvirkende faktor i store kostbare ulykker.

IO teknologien muliggjør at mange parter involveres innen samme arbeidsområde, noe som skaper flere komplekse grenseområder. Uten gode prosedyrer og mentale modeller, vil komplekse grenseområder øke sjansene for målkonflikter. Avstanden kan forsterke

målkonflikter ved at aktørene offshore kan være villig til å foreta valg med høyere risiko enn aktører som arbeider fysisk onshore.

Analysen avdekket at IO i generasjon to er avhengig av å ha kommunikasjonsteknologi som er både robust og funksjonell. Robust fordi teknologien ikke må bryte sammen ved press i uvante situasjoner. Og funksjonell for å ivareta høy grad av meningsoverføring mellom avsender og mottaker. Skal IO systemet ha mulighet til å styre systemet sikkert, må meningsoverføringen være høy. Meningsoverføring er avhengig av tillit mellom partene som kommuniserer samt at systemet har gode uformelle kommunikasjonskanaler som stimulerer til informasjonsspredning.

Dokumentanalysen avdekket at det bør forskes mer på noen av temaer oppgaven fokuserer på, før IO teknologien som innfører avstand mellom enhetene og økt kompleksitet tas i bruk. Generelt konkluderer studien med at den er positiv til at risikoen den nye teknologien innfører kan kontrolleres. Men det krever at organisasjonene tar høyde for og jobber aktivt med problemstillingene studien avdekket.

FORKORTELSER

Ptil	Petroleumstilsynet
IO	Integrerte operasjoner
IKT	Informasjon og kommunikasjonsteknologi
HRO	High Reliability Organisations
NA	Normal Accident
IT	Informasjons teknologi
SINTEF	Stiftelsen for industriell og teknisk forskning ved Norges tekniske høgskole (NTH)
MTO	Forholdet mellom menneske teknologi og organisasjon
OLF	Oljeindustriens landsforening

FIGUR OG TABELL OVERSIKT

INNHOLDSFORTEGNELSE

1.0 NY TEKNOLOGI, NYE MULIGHETER?

Teknologi har løst flere problemer i ulike samfunn gjennom å forenkle og effektivisere vår hverdag, men teknologien har også sine skyggesider og kan føre til ulykker. *"Technology... is a queer thing. It brings you great gifts with one hand, and it stabs you in the back with the other".* (C.P. Snow, *New York Times*, 15 March 1971). Sitatet påpeker at man aldri kan vite de konsekvensene av den teknologien man tar i bruk, dette kan ses på som et resultat av at den teknologiske utviklingen går fortere enn eksperter klarer å bygge opp kunnskap:

> "*Throughout history, inventions and new technology have often gotten ahead of their scientific underpinnings and engineering knowledge, but the result have always been increased risk and accidents until science and engineering caught up*" (Leveson, 2004: 3).

Leveson viser her at utviklingen går fortere enn forskere og organisasjonene klarer å få en inngående forståelse for sammenhengene og potensialet i teknologien. Organisasjoner kan implementere ny teknologi der produksjonen i perioder innebærer høyere risiko, fordi organisasjonen mangler informasjon om teknologiens potensial til å fostre en ulykke. Gradvis vil teknologien tilpasse seg den nye konteksten gjennom reinovasjoner, hvor organisasjonen tilegner seg informasjon om teknologien og dens ulykkespotensial. Olsen og Lindøe (2008a) sier at denne prosessen kan ta opp til 20 år, fordi det eksisterer en organisatorisk treighet som følge av at læringsprosesser er tidkrevende. Denne reinovasjonsfasen er en tilstand som preges av endringer og manglende informasjon, der teknologien er uoversiktlig og risikofull.

I de kommende årene vil ny teknologi tas i bruk for å effektivisere og rasjonalisere driften av offshore installasjoner. Teknologien "Integrerte Operasjoner" er et driftskonsept som skal innføres på norsk kontinentalsokkel, der informasjonsteknologi brukes for å endre arbeidsprosesser, forbedre beslutningstakning, gjennomføre fjerndrift og flytte funksjoner fra offshore til land.

Ved implementering av ny teknologi som integrerte operasjoner, beror sikkerheten på i hvilken grad sikkerhetsledelsen håndterer kompleksiteten når de kartlegger risikomomentene som ligger i selve teknologien (fase en). Og hvordan endringene som skjer i reinovasjonsfasen når teknologien tilpasser seg den nye konteksten (fase to), fanges opp og implementeres i systemet gjennom oppdatering av regler og prosedyrer.

"Sikkerhet brukes ofte om forebyggende tiltak der hensikten er å redusere sannsynligheten for at noe uønsket skal skje eller redusere konsekvensene ved uønskede hendelser". (Aven et al.,

2008:17). De sier videre at sikkerhet kan relateres til det fysiske miljø, som teknologiske systemer, produkter og omgivelsene generelt. Men sikkerhet kan også relateres til menneskelige og sosiale faktorer som menneskelig atferd, organisasjonsstruktur eller samfunnets politikk. Her viser Aven at sikkerheten kan påvirkes gjennom handlinger og valgene vi gjør, sammen med omgivelse og tekniske verktøy.

Ulykker er *"uønskede hendelser som medfører tap av liv, personskade, store miljøskader eller stort økonomisk tap"* (Aven 2006: 7). I sikkerhetsteori er det ulikt syn på hvorvidt man kan forebygge ulykker eller ei. En retning som kalles "Normal Accidents" mener at ulykker i komplekse organisasjoner ikke kan forebygges. NA ser på ulykker som et forventet utfall når organisasjoner har komplekse interaksjoner[1] og tette koplinger[2]. I komplekse og tett koplede systemer, vil feil i en funksjon berøre andre funksjoner som kan resultere i ulykker. NA går så langt at de mener at teknologi som har disse egenskapene bør unngås, eksempelvis atomkraftverk (Perrow, 1984).

"High Reliability" er et teoretisk motstykke som har et mer positivt syn, de mener at organisasjoner kan designes slik at de blir pålitelige selv om teknologien er kompleks. At riktig design kan kompensere for menneskelige feil og svakheter. Sikkerhetstanken må gjennomsyre organisasjonen, hvor blant annet sikkerhetskultur og organisasjonslæring er grep som skal bidra til sikker produksjon (Arven et al., 2008). Det er vanskelig å påstå at den ene teorien er rett og andre feil.

Ved innføringen av ny teknologi går organisasjoner gjennom to sikkerhetskritiske faser. I fase èn, er det manglende informasjon om hvilke trusler systemet kan stå ovenfor og her vil det være viktig å jobbe aktivt med den tilgjengelige informasjonen, for å kartlegge risikoen den nye teknologien kan medføre. I fase to, vil systemet tilpasses driften (den nye konteksten). I denne fase vil det være viktig å fange opp informasjonen teknologien gir når den tilpasser seg den nye konteksten. Men hvilke endringer kan man forvente å se ved innføringen av den nye teknologien integrerte operasjoner?

[1] Komplekse interaksjoner eller samhandling, omfatter blant annet beslutningslinjer og informasjonsflyt som skjer etter ukjente, ikke planlagte og uventede sammenhenger eller sekvenser. Det kan oppfattes som påvirkninger mellom mennesker og maskin, mellom maskiner eller mellom mennesker (Arven et al., 2008).
[2] Når systemer er tett koplet, betyr det at feil i en del av systemet lett vil forplante seg til andre deler eller kanskje hele systemet. (Arven et al., 2008). For videre lesing se Perrow "Normal Accidents"

1.1 Hva er integrerte operasjoner?

”Integrerte operasjoner” kan for noen være et kjent begrep som opptrer i ny drakt, fordi ”integrerte operasjoner” opererer under ulike navn. For å nevne noen: ”e-felt”, ”e-drift”, ”smarte felt/smart fields”, ”field of the future”, ”digital oil fields” og ”integrerte operasjoner”(Johnsen og Lundteigen, 2008). I denne oppgaven vil begrepet ”integrerte operasjoner” heretter kalt IO bli benyttet.

Stortingsmelding nr 38 (2003/04) definerte IO til å være et driftskonsept der informasjonsteknologi brukes for å endre arbeidsprosesser, forbedre beslutningstakning, gjennomføre fjerndrift og flytte funksjoner fra offshore til land. Datateknologi gjør det mulig å overføre informasjon uten nevneverdig tidsforsinkelse over lange avstander (såkalt sanntidsdata). Landpersonell har tilgang på samme informasjon til samme tid som offshore personell, dette muliggjør å endre måten man arbeider på. I IO vil ulike teknologier og kunnskap kobles sammen til en helhet som omformer oppgavedeling mellom hav og land, operatør og leverandører. (www.regjeringen.no).

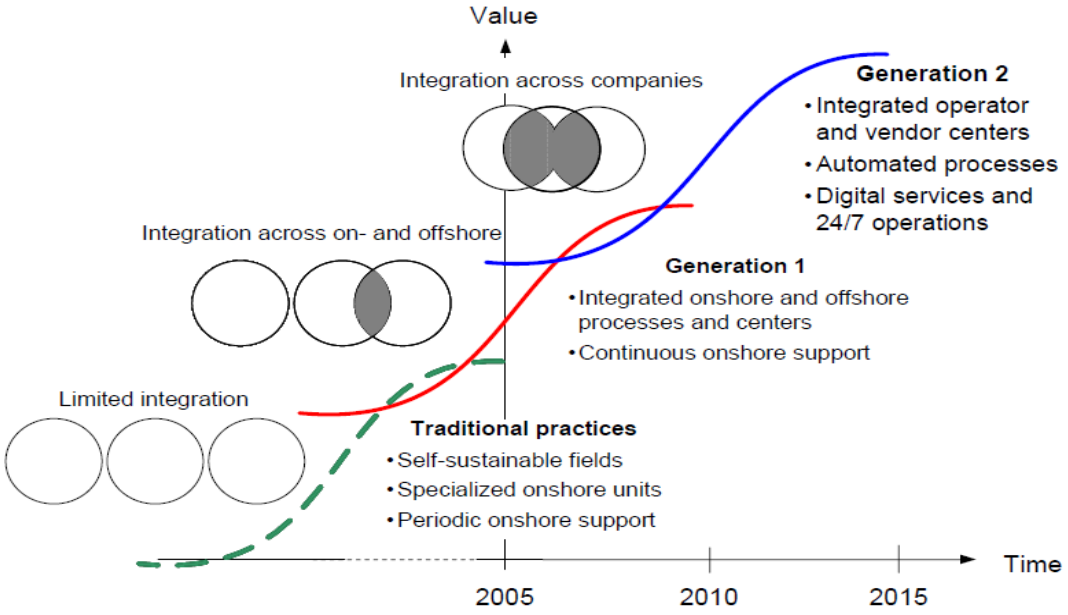
Videre er det verdt å merke seg at det mangler klarhet om begrepene, fjernstøtte, fjernovervåkning, fjernstyring og fjerndrift representerer ulike implementeringer av IO, som går på hvor mye styringsansvar som ligger offshore/onshore (Johnsen et al., 2008). Eksempelvis er fjerndrift når installasjoner er bemannede og driftsansvaret i sin helhet er flyttet fra installasjonen til en annen lokasjon. Mens man i fjernstyring har flyttet hele eller deler av driftsansvaret fra installasjonen til en annen lokasjon og installasjonen er normalt fjernstyrte og ubemannede (Ibid).

OLF anslår at potensialet knyttet til bruk av IO er opp mot 8–10 prosent økt produksjon, inntil 4–5 prosentpoeng økning i utvinningsgraden og inntil 30 prosent reduksjon av driftskostnadene i forhold til dagens nivå (Stortingsmelding 38 2003/04). I tall anslår OLF (2007a) verdien av Integrerte Operasjoner til å ha et potensial på 300 mrd norske kroner. Analysene fra årene 2005-2007 viser at det allerede er skapt 23 mrd norske kroner som et resultat av IO.

OLF (ibid) mener den største bidragsyteren til gevinstpotensialet er økt produksjon som følge av reserveøkning og produksjonsoptimalisering. IO kan gi tilgang til nye resursområder ved å bruke informasjons- og kommunikasjonsteknologi (IKT) til samhandling over avstand. Og gjøre det mulig å utøve oljevirksomhet i områder der det tidligere ikke var lønnsomt, eller har vært begrenset av klimatiske eller geologiske forhold (Tveiten et al., 2008). I tillegg til å

rasjonalisere allerede eksisterende oljefelt får man teknologi til å begynne å utvinne ressurser fra nye områder. Av dette ser man at IO er ny teknologi som skal motvirke den dårlige trenden med fallende produksjon, og sikre lønnsom drift for olje og gassnæringen i fremtiden.

OLF presenterte i 2005 en visjon om hvordan de ønsket IO utviklingen skulle se ut, hvor vi i dag befinner oss i generasjon èn, men strekker oss mot generasjon to, se figur:



Figur 1: Viser hvordan arbeidsprosesser vil bli implementert i 2 steg (OLF 2005:9)

Tradisjonell praksis: er situasjonen frem til ca 2005, hvor offshore og onshore er sett på som ulike enheter. Der daglige beslutninger i stor grad blir tatt offshore med begrenset støtte fra land. Det er en eller to operatører som utfører de daglige kontrollene fra et sentralt kontrollrom lokalisert offshore. Fra dette rommet optimaliseres brønnene basert på planer utarbeidet på land. Beslutningene er basert på offshore operatørenes egen dømmekraft og kunnskap om operasjonene. Støtte fra land er begrenset til fem dager i uken fra 08:00 til 16:00, og kommunikasjonen mellom enhetene går via audiokommunikasjon og e-post. Noe som innebærer at operatørene implementerer viktige beslutninger angående produksjon og sikkerhet tas uten støtte fra ingeniørene som har utviklet planene (OLF, 2005).

Generasjon 1: er situasjonen fra ca 2005 frem mot 2010. Det er betydelig mer samkjøring mellom hav og land. Personell integreres i onshore driftssentre og offshore kontrollrom, der begge parter kan overvåke produksjonen gjennom å sammenligne ”sanntidsdata” med

simulasjoner[3] . Sanntidsovervåkning blir mulig ved bruk av IKT løsninger, slik kan de identifisere operasjonelle så vel som sikkerhetsrelaterte problemer. Hovedkontrollen vil fortsatt være hos offshore operatørene, onshore vil være støttesenter som sammen med offshore ansatte finner ut hvordan de skal optimalisere produksjonen. Arbeidsteamene har fått delegert den nødvendige autoriteten til å ta beslutninger og implementere praksiser.

Her vil opplæring og trening rettes mot å utvikle nye tverrfaglige ferdigheter, som kan hjelpe operatørene til å ta informerte beslutninger. Onshoresentrene gir mulighet for økt involvering av eksterne aktører som kontraktører og servicearbeidere i problemløsningen og planlegningsarbeidet. Ved bruk av videokonferanser og "sanntidsdata" kan de ulike involverte aktørene onshore ha møter og ta hensyn til situasjonen offshore når de planlegger. Med denne arbeidsmåten vil spesialister kunne fremme proaktive råd om optimal produksjon, og gi aktiv støtte når problemer oppstår. (OLF, 2005)

Generasjon 2: er en fremtidig tenkt situasjon fra ca 2010 til 2015. Denne fasen preges av betydelig integrering av leverandører og operatører. Leverandørpersonell og operatørpersonell vil være lokalisert i geografisk uavhengige onshore driftsentre (både i Norge og utlandet). Samhandlingen mellom enhetene er "sanntidsdata" som alle har tilgang til. Sentrene vil være operasjonelle 24 timer i døgnet, og drives i henhold til "follow the sun" prinsippet. Det betyr at kontrollromsfunksjonen flyttes mellom senter i ulike tidssoner, slik at det alltid er dagskift som er på vakt. Nye software programmer vil gi oppdatert informasjon og 3D modeller kontinuerlig. Senarioer og estimater av mulig utfall vil bli presentert til teamene, som vil ta de avgjørende beslutningene om hvordan de skal optimalisere produksjon (OLF, 2005).

For å unngå informasjonsoverbelastning, vil automatisk filtrering av informasjon og beslutningsprosesser tas i bruk. Leverandørene overtar deler av arbeidet som tidligere ble utført av operatører, eksempelvis overvåkning, analysering av informasjon samt å gi råd til operatørene når avvik og alarmer registreres. Operatørene vil fortsatt ha det generelle ansvaret for operasjonene offshore, og ta nødvendige beslutninger når alarmen går. Prosessovervåkning og kontroll funksjoner vil flyttes onshore, og ny teknologi erstatter operatørfunksjoner og oppgaver (OLF, 2005).

[3] Simulering i denne sammenheng er oppdaterte virtuelle modeller av de tekniske systemer.

Ved å implementere fjerndrift i generasjon to, innebærer det en betydelig endring i hvordan beslutninger, prosesser, samarbeid og kommunikasjon blir innen norsk petroleums næring. Endringene kan medføre at næringen står overfor nye og ukjente risikoer.

1.2 Problemstilling

Sikkerhetsdimensjonen er viktig ved innføringen av all ny teknologi, fordi ingen ønsker en lammende og kostbar ulykke. For å unngå ulykker er det viktig å kartlegge hvilke sikkerhetsmessige utfordringer innføringen av teknologien kan produsere og iverksette preventive tiltak som reduserer risikoen. Ved kartlegging av de sikkerhetsmessige utfordringene er det viktig å vurdere hvorfor innføring av ny teknologi representerer en risiko. For deretter å vurdere om særtrekk ved IO kan forsterke risikoen den nye teknologien representerer. Det vil være viktig for å bygge en sikker organisasjon å vurdere om IO forsterker negative elementer som innføring av ny teknologi tar med seg. Hovedmålet med oppgaven er å finne svar på hvilke risikoer innføring av IO i generasjon to innebærer, derav problemstillingen:

- **Å avdekke hvilke sikkerhetsmessige utfordringer som oppstår ved implementering av ny teknologi.**
- **For så å vurdere hvordan utfordringene vil vise seg ved implementeringen av integrerte operasjoner.**

Problemstillingen er aktuell for å unngå ulykker som medfører kostnader i form av tapt produksjon, skader på utstyr, tap av menneskeliv og svekke omdømmet slik at videre drift vil være vanskelig (Reason, 1997). Ved å avdekke sikkerhetsutfordringene kan man planlegge å forebygge for å unngå at svakhetene utvikler seg til en ulykke.

For å begrense oppgaven har jeg valgt å ta utgangspunkt i informasjonsbehandlingen under kartlegging av den nye teknologien (fase en) og når teknologien tilpasser seg den nye konteksten(fase to). Informasjonsperspektivet er viktig for å avdekke de sikkerhetsmessige utfordringene. Det er fordi innføring av ny teknologi kan forstås som implementering av ny informasjon, samt at endringene som skjer når teknologien tilpasser seg den nye konteksten (fase to) produserer informasjon. For å svare utfyllende på problemstillingen vurderes også særtrekk ved IO teknologien som påvirker risikoen ved å ta i bruk ny teknologi. IO vil utfordre informasjonsprosessene gjennom at fjerndrift introdusere en avstand mellom enhetene som gjør det vanskelig å dele informasjon. Og implementering av komplekse IKT

systemer gjør at det er vanskelig å ha en oversikt over informasjonen. Basert på dette vil fokuset til studien være på tematikk som berører informasjon.

Temaene som analyseres i studien er sikkerhetskultur, fordi den former aktørenes holdninger og deling av sikkerhetsrelevant informasjon. Dårlige mentale modeller kan forårsake en ulykke, og kvaliteten på modellene beror på kvaliteten til sikkerhetsinformasjonen. Målkonflikter, fordi ukoordinert sikkerhetsinformasjon kan føre til simultane handlinger og ulykker. Så vil studien runde av med å se på hvilke faktorer som kan påvirke forståelse og kommunikasjon av sikkerhetsinformasjon.

1.3 Hvorfor informasjonsperspektivet er viktig

Turner (1997) ser katastrofer og ulykker som et resultat av energi pluss missinformasjon. Ut fra dette perspektivet er det viktig å se på forhold som påvirker forståelse og bruk av informasjon i et system dersom man skal forebygge ulykker. Ved innføringen av ny teknologi vil organisasjoner mangle informasjon om de teknologiske risikoene. Videre er informasjonsperspektiver viktig i forhold til IO, fordi utvekslingen og bruken av informasjonen i IKT systemet er avgjørende for å unngå uønskede hendelser. Når enheter er separert i tid og rom vil informasjonen som strømmer mellom dem, gjennom ulike kommunikasjonskanaler (videokommunikasjon, tekst, lyd osv), påvirke situasjonsforståelsen til aktørene. Situasjonsforståelse handler om innsikt til å forstå sammenhengene i omgivelsene, og er viktig for å gjenkjenne og diagnostisere problemer (Rosenthal et al., 2001). Informasjon skal flyte mellom ulike avdelinger, organisasjoner og kanskje til og med land når den nye teknologien tas i bruk. Og i følge Turners definisjon vil kvaliteten på informasjonen og hvordan den utnyttes være avgjørende for å gjenkjenne og forstå problemer slik at man kan unngå ulykker.

Ved å avdekke og belyse informasjonsmessige utfordringer teknologien står overfor, kan man forebygge med å designe sikrere systemer. Design vil i denne oppgaven ikke være fokusert på de tekniske løsningene. I tråd med MTO tradisjonen, vil design være like mye design av organisatoriske og menneskelige tilrettelegging som tekniske løsninger. Samtidig ses design på som en prosess, der de er viktig å fange opp signaler og endre design etter hvert som man oppdager uforutsette faktorer ved den nye teknologien.

Organisasjonene er nå i en prosess for å bli kjent med eksisterende teknologi (IKT) innført i generasjon null og èn. Samtidig som de får tilført nye teknologiske elementer som skal klargjøre organisasjonene for generasjon to. Prosessen endrer måten enhetene samhandler,

gjennom økt grad av samarbeid ut over organisasjonsgrensene og hvor onshore sentrene blir viktigere og viktigere.

Dette viser at organisasjoner har gått fra tradisjonell praksis hvor onshore offshore har vært atskilt, der onshore har gitt støtte mellom 8- 16 via telefon og e-post. Til generasjon en, hvor onshore støtten blir mer fremtredende der både offshore og onshore har tilgang til "sanntidsdata", og samarbeider mer aktivt med problemløsingen. I generasjon to, er visjonen at flere parter skal inkluderes i samarbeidet. Da ser man for seg enheter rundt om på kloden som muliggjør et "follow the sun" prinsipp, der onshoresentre tilbyr støtte 24 timer i døgnet. Generasjon to muliggjør å kommunisere via 3D modellering, i tillegg til tradisjonell IKT for spre kommunikasjonen. Det er for å sikre at informasjonsdelingen mellom enhetene gir et så fullstendig bilde av virkeligheten som mulig.

Å kartlegge sikkerhetsmessige utfordringer innføringen av IO i generasjon er utfordrende fordi man mangler kunnskap om teknologien. Informasjonsperspektivet kan bidra til å synliggjøre problemer i implementeringen av IO, fordi bruk og forståelse av informasjon er viktig i fase en hvor man kartlegger teknologien og risikoen. Og i fase to i reinovasjonsprosessen for å fange opp informasjonen endringer gir. Klarer aktørene å behandle sikkerhetsinformasjonen i teknologien, kan man overkomme utfordringene IO introduserer.

1.4 Begrensninger av oppgave

Vi har tidligere sett at problemstillingen har begrenset oppgaven til å fokuserer på ny teknologi, informasjon og særtrekk ved IO. Og at oppgaven vil se på menneskelige og organisatoriske forhold, og ikke vurderer de tekniske løsningene som tas i bruk ved IO. De teknologiske løsningene blir interessante i oppgaven ettersom de gir innsikt om informasjonsbehandlingen som foregår i fase en eller to. Analysenivået er rettet mot organisasjon og ikke individ, derfor vil individnivå i likhet med teknologiske løsninger bli overfladisk behandlet. Individnivå vil bli drøftet dersom det påvirker informasjonsbehandlingen som foregår mellom enhetene.

Problemstillingen i oppgaven gjør seg gjeldende for en begrenset del av IO. Problematikken gjelder for de driftsformene i IO som har separerte enheter, med mennesker som må kommunisere og samarbeide over avstand. Problemstillingen vil ikke gjøre seg gjeldende for fjernstyrte ubemannede innretninger, men for fjerndriftede bemannende installasjoner som baserer seg på informasjonsutveksling mellom offshore og onshore. Det viktigste her er at

installasjonene er atskilt i tid og rom, slik at sikkerhetskulturen, målkonflikter, mentale modeller og informasjonsutvekslingen blir påvirket. Nå vil fokuset flyttes mot hvordan studien har hentet inn data til å besvare problemstillingene.

2.0 FORSKNINGSDESIGN OG FORSKNINGSSTRATEGI

Forskningsdesign er*"A logical plan for getting from here to there"* (Yin, 2009:26). Med andre ord er forskningsdesign en plan på hvordan man skal svare på problemstillingen, og den fremgangsmåten som passet for å svare på problemstillingen var case-studien. Jacobsen (2003) sier at en case-studie gjøres når ett eller noen få tilfeller gjøres til gjenstand for inngående studier. Case-studien setter fokuset på en spesiell enhet som kan være kollektive enheter som består av flere absolutte enheter eller en gruppe, organisasjon eller et lokalsamfunn. I dette tilfellet er case-studien partene som er involvert i IO systemet på norsk sokkel. Case-studien gir mulighet for å studere IO i dybden innenfor et avgrenset område i tid og rom (generasjon to), slik at man kan beskrive hva som er spesifikt med generasjon to og forklare hvordan ting henger sammen (Yin, 2009).

Jeg ønsker med denne oppgaven å se nærmere på IO i generasjon to, et fenomen som ligger i fremtiden. Målet er å avklare nærmere hva innføringen av ny teknologi og avstanden mellom enhetene i IO systemet vil innebære. Case-studien er en del av kvalitativ metode, en metode form som passer når man "*vet lite om temaet vi har bestemt oss for å undersøke*" (Jackobsen 2003: 118). Det eksisterer lite kunnskap om temaet fordi det er få forskningsrapporter som har beskrevet generasjon to. En kvantitativ studie ville vært problematisk å gjennomføre, fordi det finnes få informanter med tilfredsstillende kunnskap om fremtidens IO løsninger. Manglende kunnskap om et tema svekker den kvantitative metode, men den kvalitative metodens styrke.

2.1 Utvalg av kilder og enheter

Oppgavens mål er å benytte seg av dagens kunnskap til å si noe om fremtiden, generasjon to. Casen omfatter mange ulike parter, herunder organisasjoner og nivåer i organisasjoner som ville krevd mange intervjuer. Videre bygger problemstillingen på forhold som ligger i fremtiden, derfor var det nødvendig å utføre en kartlegging av "Status Quo" i generasjon èn. Dokumentstudie muliggjør en rask kartlegging av partenes kunnskap om sikkerhetsmessige utfordringer i generasjon en. Samtidig vil en dokumentstudie gi en oversikt over eksisterende forskning og avdekke områder hvor forskningen er mangelfull.

Videre sier Yin (2009) at dokumenter gir informasjon som sannsynligvis er relevant for enhver case-studie. Yin viser at denne typen informasjon kommer i ulike former: personlige dokumenter som brev, rapporter fra hendelser som referat og rapporter. Administrative

dokumenter som forslag, progresjons rapporter, formelle studier eller evalueringer av de samme "casene" som du studerer og nyhetssaker og andre artikler fra media osv (Ibid). Jacobsen (2003) påpeker at de viktigste valgene ved dokumentanalyse er knyttet til hvilke dokumenter vi velger ut, og hvor stor troverdighet de enkelte dokumentene har. For å sørge for at troverdige dokumenter ble benyttet baserer oppgaven seg på tidligere forskningsrapporter utgitt av SINTEF, Ptil og OLF.

Videre benyttes data fra boken til Tinmannsvik (2008), en artikkelsamling av forskere som analyserer og vurderer ulike problemstillinger ved IO. Tidligere masteroppgaver er brukt som støttelitteratur i analysen.

Problemstillingen har vært førende for hvilke dokumenter analysen baserer seg på. Her er en forenklet oversikt over dokumentene i studien, som viser dokumentenes tittel og deres relevans til temaene i oppgaven. Tabellen gir ingen komplett oversikt over alle dokumenter som berører samme tema. I de tilfeller dokumentene beskrev samme tema ble det mest utfyllende og relevant dokument benyttet som kilde. For en mer detaljert oversikt se tabell vedlegg 1.

Dokument	**Problemstilling/tittel**	Mål med dokumentet
Sintef 2005	*Trusler og muligheter knyttet til eDrift*	Ny teknologi Sikkerhetskultur Mentale modeller Målkonflikter Informasjonsprosesser
Sintef 2008 a	*Risikokartlegging og analyse av Integrerte Operasjoner (IO) med fokus på å avdekke viktige MTO aspekter*	Mentale modeller Informasjonsprosesser
Sintef 2008 b	*Kartlegging av bruken av integrerte operasjoner i vedlikeholdsstyring*	Ny teknologi Sikkerhetskultur
Sintef 2008c	*Hva innebærer egentlig Integrerte Operasjoner?* *Fenomenforståelse og generiske elementer med mulige konsekvenser for storulykkespotensialet.*	Ny teknologi Mentale modeller Målkonflikter Informasjonsprosesser

Sintef 2010	*Interdisciplinary risk assessment of Integrated Operations addressing human and organizational factors*	Mentale modeller
Ptil 2008	*Sikkerhet - status og signaler*	Målkonflikter
OLF 2003	*Edrift på norsk sokkel – det tredje effektiviseringsspranget*	Informasjonsprosesser
OLF 2005	*Integrated work process: Future workprocess on the Norwegiancontinental shelf*	Ny teknologi Mentale modeller Målkonflikter Informasjonsprosesser
OLF 2007 a	*Oppdatert verdipotensial for integrerte operasjoner på norsk sokkel*	Sikkerhetskultur Informasjonsprosesser
OLf 2007b	*HMS og integrerte operasjoner: forbedringsmuligheter og nødvendige tiltak*	Ny teknologi Mentale modeller
Olsen og Lindøe 2008	*Ny teknologi og organisasjoner i endring. Risiko på vandring*	Ny teknologi
Olsen og Engen 2010	*Small steps towards big accidents*	Ny teknologi
Tveiten et. al 2008	*Underveis mot integrerte operasjoner – en borekontraktør tilegner seg nye IKT- løsninger*	Ny teknologi Sikkerhetskultur Mentale modeller Målkonflikter Informasjonsprosesser
Johnsen og Lundteigen 2008	*Sikrere Fjerndrift med CRIOP*	Ny teknologi Mentale modeller Målkonflikter Informasjonsprosesser
Rosness et al	*Organisational Accident and Resillient Organisations*	Målkonflikter
Grøtan 2008	*IKT som bidrag til robusthet i integrerte operasjoner – et skråblikk*	Mentale modeller
Espen Olsen	*Kultur og atferd som tilnærming for å bedre sikkerheten: En evaluering av kollegaprogrammet*	Sikkerhetskultur

Høivik Dordi	*Helse, miljø og sikkerhetskultur i petroleumsindustrien i Norge*.	Sikkerhetskultur Målkonflikter
Haukelid Knut	*Oljekultur og sikkerhetskultur*	Sikkerhetskultur
Ryggvik, Helge	*Adferd, teknologi og system – en sikkerhetshistorie.*	Sikkerhetskultur
Nystøl Anders:	*Databehandling i komplekse og integrerte operasjoner, fra et MTO-perspektiv. (masteroppgave)*	Mentale modeller Informasjonsprosesser
Høyland Elisabeth	*Sikkerhetsbetraktninger ved implementeringen av integrerte operasjoner i norsk petroleumsvirksomhet.(Maste oppgave)*	Ny teknologi Sikkerhetskultur Informasjonsprosesser
Haaland Geir:	*Integrerte operasjoner i V&M kontrakter. (Master oppgave)*	Målkonflikter

Tabell 1: Viser dokumentenes fokus i forhold til studiens tematikk

2.2 Reliabilitet og validitet

For at en undersøkelse skal være pålitelig (reliable), må selve undersøkelsesprosessen være systematisk og åpen. Mens validitet dreier seg om i hvilken grad funnene i undersøkelsen kan generaliseres (Jacobsen, 2005).

En åpen undersøkelsesprosess er viktig for at andre forskere skal kunne etterprøve funnene, ved å følge samme prosess er målet å oppnå samme funn og konklusjon. Yin (2009) påpeker at forskeren bør utvikle en case-studie protokoll for å styrke påliteligheten til undersøkelsen. Derfor laget jeg en prosjektbeskrivelse tidlig i prosessen hvor jeg valgte tema og laget en foreløpig problemstilling og satte opp en tidsplan. For å styrke oppgavens reliabilitet systematiserte jeg de empiriske dokumentene i henhold til temaene.

Case-studie protokollen bidro til å holdefokus på problemstillingen under studien. I dokumentstadiet var den et godt redskap for å finne rapporter som omhandlet ønsket måling. Som Yin (2009) påpeker er det ofte et problem med at internett søk gir mange treff, slik at relevante rapporter kan forsvinne i mengden. Protokollen gjorde det enklere å analysere i de store forskningsmengdene som finnes om IO.

I følge John Scott (1990) bør dokumenter behandles vitenskaplig for å avdekke meningen de kommuniserer, derfor har dokumentene blitt vurdert i forhold til: authenticity, credibility, representativeness og meaning.

Authenticity: Her må forskeren spørre seg selv om bevisene (rapportene) og opphavet er genuine. Forskeren må vite om det er originalt opphav(originale studie), om det har vært kopiering av originalen (for eksempel masteroppgaver), eller kopi av kopi (3grads fortolkning). Nærheten til kilden, altså oppgaven, er viktig for å hindre at man gjengir en tolkning som kan være feilaktig. I oppgaven er det valgt data fra originalrapporter utført av offentlige instanser, og unngått masteroppgaver som ofte er kopi av originalen (tolkning av tolkning). Masteroppgavene har som tidligere vist vært brukt som støttelitteratur. Selv om originale studier og andregrads fortolkninger har vært hovedfokus i arbeidet, henviser disse rapportene tidvis til tidligere studier, slik at tredjegrads fortolkning kan forekomme.

Credibility: Her må forskeren tenke over om bevisene(rapportene) er uten feil og støy/forstyrrelser. Forskeren må vurdere om tidshorisonten kan ha endret innholdets relevans (for eksempel intervju fra 2002, er udatert i forhold til tankegang i 2010). I oppgaven har det konsekvent blitt fokusert på nyere rapporter, for at dataene skal være oppdaterte i forhold til nåværende situasjon. De gamle rapportene som brukes er relevant for å kartlegge historie og årsakene til hvorfor det ble besluttet å innføre IO på norsk sokkel.

Spørsmålet om ”Credibility” er også et spørsmål om forfatteren av dokumentet er partisk, og hvorvidt forfatteren hadde interesser i å produsere dokumentet. Yin (2009) sier at en fare med dokumenter er at de kan være partisk, slik at de kan være sensurerte eller editerte for å få frem et spesielt syn. Derfor må det utvises forsiktighet ved bruk av dokumentanalyser, og forsøke å avdekke om rapportene er partiske.

Dokumentanalysen avslørte ulikheter i rapportenes form på grunn av ulikt mål for utgivelse av rapportene. OLF rapportene var preget av å være utredninger av potensialet til IO og var preget av statistikker og verdiberegninger som skulle underbygge hvorfor IO er bra for norsk sokkel, mens utfordringene ved IO var mer tonet ned. Derfor virket det som om OLFs interesse for å utgi dokumentene var å underbygge myndighetenes vedtak om å innføre IO på norsk sokkel. Fokuset i OLF rapportene medførte at det var lite informasjon om utfordringene med implementeringen av ny IO teknologi.

Sintef rapportene og Tinmannsvik artiklene hadde ulik form enn OLF rapportene. Disse tok sikte på å avdekke problemer IO kan møte på. Rapportene/artiklene hadde fokus på å belyse MTO problemstillinger. Innfallsvinklene var mange og gav derfor et variert bilde på hvordan utfordringene med ny teknologi vil vise seg i generasjon to. Hovedinntrykket er at Sintef og Tinmannsvik forskning tok sikte på å avdekke så mange forhold som mulig for å bygge opp kunnskap om IO systemet.

Representativeness: Her må forskerne vurdere om bevisene er typiske av sitt slag, om dokumentene samsvarer i forhold til majoriteten av relevante studier? Rapportene benyttet i dette studiet var samstemte om hvilke sikkerhetsmessige problemstillinger som IO kunne møte i generasjon to. Det eneste som varierte var klassifiseringen av problemenes viktighetsgrad. Videre må forskeren vite noe om er metode i originalstudien, om metoden som er benyttet virker pålitelig. Rapportene i studien hadde gode metodebeskrivelser for innhenting av data.

Meaning: Her må forskeren reflektere over hva studien forteller oss, hva er det som blir studert og hvordan er ordbruken? Forsøke må forsøke å forstå skriften i dokumentene for å fange opp det forfatteren forsøker å fortelle, heller enn en overfladisk mening eller egen tolkning.

Yin (2009) påpeker i denne sammenheng at forskeren må være oppmerksom på at dokumentene kan være skrevet for andre årsaker enn undersøkelsene i den aktuelle case-studien. Svakheten med sekundære data er at man ofte ikke vet hvordan data er blitt samlet inn, hvilke måleapparater og innsamlingsmetoder som er brukt, og hvem som har registrert informasjonen. Dataene kan ha vært samlet inn og brukt i en helt annen hensikt, dermed kan det oppstå et misforhold mellom den informasjonen som kan benyttes i en sammenheng, og det man gjerne ønsker å benytte (Jacobsen, 2003).

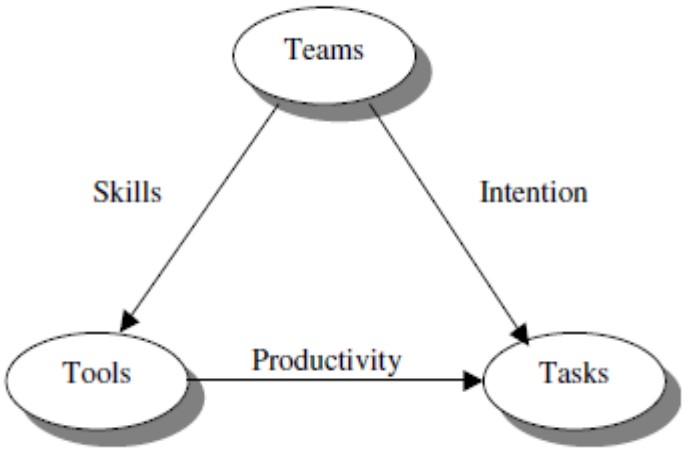
Det ble gjort forsøk på å begrense dette, ved å benytte forskningsrapporter fra troverdige forskningsinstanser som forklarer metodikken og målsetningene for rapporten. Rapportene er offentlige med hensikt om å opplyse om forhold rundt IO, som er avdekket gjennom kvalitative og kvantitative undersøkelser. Kompetansenivået til de som skriver disse rapportene kan antas å være høy, fordi de er ledende forskere innenfor sikkerhetsfaget. De har liten egeninteresse av å forvrenge informasjonen. Essensen i dokumentene er forsøkt ivaretatt selv om deler er omskrevet for å passe inn i oppgaveteksten.

Til tross for at dokumentene har blitt vurdert i forhold til de fire kriteriene finnes det ingen garanti for at bruken av dokumentene gjengir den opprinnelige meningen. . En ”svakhet” sosialvitenskapen har, er at forskere er en del av en hermenautisk fortolkning, der det som fortolkes blir farget av egne erfaringer og fortolkningsbriller. Ved å benytte en case-studie protokoll hvor fremgangen ble planlagt, viser oppgaven at faktisk måling samsvarer med ønsket måling (realibilitet). Samtidig som Scotts kriterier for vurdering av dokumentene, har sørget for at oppgaven er bygget på troverdige data og styrker konklusjonens validitet. Oppgaven måler IO systemet på norsk sokkel, og funnene vil være valide i forhold til situasjonen på norsk sokkel. Funnene kan benyttes til sammenligning i andre liknende tekniske systemer som tar i bruk ny teknologi og er preget av samarbeid over avstand.

I neste kapittel vil teori som behandler risiko ved implementeringen av ny teknologi i et system preget av avstand og kompleksitet bli presentert. Første del av teorien vil omhandle risiko ved implementeringen av ny teknologi. Videre vil kapittelet presentere teori som illustrerer ulike informasjonsmessige problemer som kan representere en risiko ved implementering av ny teknologi (ny informasjon), i et komplekst system preget av avstand.

3.0 NY TEKNOLOGI OG ULYKKER

Når man skal vurdere hvilke sikkerhetsmessige problemstillinger IO i generasjon to kan skape, er det viktig å forstå hvordan innføringen av ny teknologi kan representere en risiko. Tradisjonelt blir teknologi forstått som de fysiske verktøyene man benytter til å løse oppgaver. Forståelsen av teknologi har utviklet seg til også å inkludere konteksten verktøyene opererer innenfor. Olsen og Lindøe (2008 a) viser at teknologi er en integrasjon av en rekke faktorer. Se figur:



Figur 2: Viser samspillet mellom team, oppgaver og verktøy hentet fra Olsen og Lindøe (2008a)

Figuren viser at teknologi er et komplekst fenomen bestående av tre ulike elementer: aktører (team), instrumentelle innretninger/verktøy (tools) og oppgaver som skal løses (tasks). Med andre ord benytter individer/grupper verktøy til å løse gitte oppgaver(Olsen og Lindøe 2008b). Utfallet på oppgaveløsningene kommer an på faktorene: intensjonene gruppene har når de opererer verktøyene (intention), og hvilke kunnskaper aktørene har om hvordan de skal operere verktøyene (skills). Faktorene og elementene vil forme et sømløst nett som i et dynamisk forhold former teknologi. Definisjonen tilsier at teknologi ikke kan skilles fra konteksten den opererer innenfor. Som Engen og Olsen (2010) påpeker er teknologi et resultat av felles innsats, erfaringer og beslutninger gjort av folk i spesifikke situasjoner. Små endringer i et av de teknologiske elementene, vil sannsynlig skape et behov for å endre de andre elementene også, dersom dette ikke skjer kan resultatet bli en dårlig eller i verste fall risikofull teknologi (Engen og Olsen, 2010).

Teknologien utvikles hos en produsent og overføres, for så å integreres hos mottakerne. Olsen og Lindøe (2008 a) sier at teknologioverføring best forstås som en overføring mellom ulike kontekster og kulturer. De sier videre at det eksisterer ulik grad av kunnskap som skal

overføres. Det er kunnskap som er nedskreven i manualer og personlig erfaring som er vanskelig å overføre fra produsent til mottaker. Det vil si at selv om produsenten har utviklet prosedyrer og rutiner på hvordan teknologien skal benyttes, er det vanskelig å overføre kunnskapen til mottaker. Mottaker må selv jobbe aktivt for å omdanne den overførte informasjonen til kunnskap[4].

Alle de teknologiske elementene endres ved implementeringen av IO i generasjon to. IKT verktøyene blir utviklet hos en produsent og overføres til mottakerbedriftene. Arbeidsoppgavene vil også endres betraktelig fordi aktørene blir atskilt i tid og rom, og må forholde seg til ulike oppgaver enn før og aktører vil som følge av "follow the sun" prinsippet forholde seg til nye gruppesammensetninger. Når endringene blir så store og omfattende vil design av systemet ha stor betydning for sikkerheten, fordi designet bestemmer hvordan de teknologiske elementene forholder seg til hverandre, og hvordan de ulike aktørene samarbeider.

Turner (1997) sier at undersøkelser av prosessen med å designe systemer, og faktorene som har ført til designfeil i fortiden, avslører noen begrensninger som designere må jobbe under. Det er ofte antatt at all relevant og brukbar informasjon som designere trenger for å forstå en handling ligger tilgjengelig og er nedskrevet i skriftlig form. Sannheten er at designere ofte må jobbe med begrensede data om materialene de skal bruke, deres egenskaper og reliabilitet. Ofte mangler designerne informasjon om driftsforholdene som deler av utstyret skal arbeide under, slik at noen designløsninger må søkes gjennom prøving og feiling (Turner, 1997). Mangelen på informasjon er et kjennetegn på ny teknologi, fordi produsent av teknologien ikke klarer å overføre all kunnskap de besitter til mottaker organisasjonen, noe som vanskeliggjør designprosessen. Derfor kan IO designet og planleggingen i fase en være mangelfull, noe som medfører at endringer må bli gjort når man blir kjent med teknologien i fase to (se figur 4).

Olsen og Lindøe (2008 a) påpeker at den forventede ulykkesraten vil øke de første årene i den nye konteksten, helt til risikoledelsens kunnskap/kompetanse i forhold til den nye teknologien er tilfredsstillende. Ofte setter teknologi overføring i gang en prosess med reinnovasjoner for å tilpasse teknologi til den nye konteksten. Disse reinovasjonene bygger opp kompetansen og gjør mottakerne i stand til å bruke den overførte teknologien som byggeklosser i egen

[4] Kunnskap er en bevisst forståelse av noe, og med muligheten til å bruke denne for en bestemt hensikt. Kunnsskap er internalisering av informasjon; summen av et individs oppsamlede informasjon. (www.wikipedia.no)

utvikling av den nye teknologien. I følge Olsen og Lindøe (Ibid) kan denne prosessen vare i hele 20 år. Prosessen kjennetegnes av mange små og store endringer som genererer informasjon organisasjonen må fange opp og implementere i organisasjonen for å unngå ubalanse mellom de teknologiske elementene.

Engen og Olsen (2010) viser at endringer i ett av elementene i teknologien (se figur 3) krever at de andre elementene også tilpasser seg. I reinovasjonsprosessen tilpasser teknologien seg den nye konteksten, og det skjer endringer i de ulike teknologiske elementene. Å fange opp endringene/tilpasningene som skjer over tid er en del av designprosessen. Designerne må forbedre eksisterende prosedyrer ut fra erfaringer organisasjonen bygger opp ved å samhandle med den nye teknologien. Dersom man ikke fanger opp endringene kan man risikere en mismatch mellom elementene i den teknologiske modellen og økt risiko for at uønskede hendelser kan inntreffe. Se figur:

Figur 3: Illustrerer risiko ved teknologisk endring, hentet fra Engen og Olsen (2010)

Olsen og Engen poengterer at små endringer i ett teknologisk element, ikke nødvendigvis resulterer i at de andre teknologiske elementene endres, og det oppstår et gap mellom elementene som kan føre til en uønsket hendelse.

De inkrementelle endringer som skjer i reinovasjonsprosessen er ofte små og lette å overse (Olsen og Lindøe, 2009). Leveson (2004) sier at man må designe for endring, fordi enhver modell som inkluderer sosiale system og menneskelig feil, må ta høyde for endringer og tilpasning over tid. Hun påpeker at sikkerhetsledelse er å fange opp endringer som skjer i

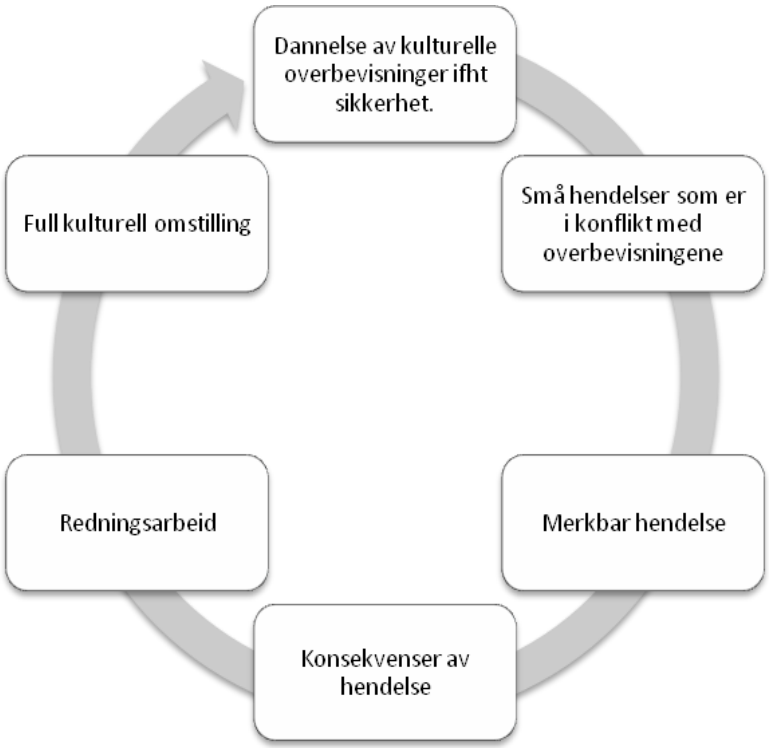
systemet. Ved innføringen av IO må organisasjonene være aktivt med i implementeringsprosessen, for å fange opp disse endringer som skjer når individene samhandler med den nye teknologien. Sikkerhetsledelsen må være oppmerksomme og sørge for at informasjonen blir fanget opp, slik at de andre teknologiske elementene kan tilpasses den aktuelle endringen, for å unngå økt risiko for uønsket hendelse.

Det vil være vanskelig å kartlegge risikoen den nye teknologien introduserer siden det eksistere en situasjon med manglende informasjon, og at reinovasjonsprosessen i seg selv kan tilføre nye risikoer. IO systemet er som vi ser avhengig av informasjon i kartleggingen av teknologien, men også av å fange opp informasjonen som reinovasjonsfasen produserer når teknologien endrer seg.

3.1.1 Informasjonens rolle i fremveksten av ulykker

Informasjonens rolle i forhold til fremveksten av ulykker er anerkjent. Turner (1997) hevder at to viktige element står sentralt ved alle endringer i verden, nemlig energi og informasjon. Han ser ulykker som et resultat av feilplassert eller manglende informasjon og energi som går i feil retning. Turner påpeker at alle ulykker er uventede eller overraskende, men noen er uventet bare fordi ingen vet nøyaktig når og hvor ulykken vil inntreffe. Andre ulykker er uventede i form av at hendelsen er ny og derfor mangler informasjon. Hendelsene provoserer en høyere grad av overraskelse enn en ulykke man har "forventet", fordi vi ikke har noe akutt tilgjengelig rammeverk for å håndtere dem. Slike hendelser definerer Turner som anomalier[5]. Det Turner argumenterer for er at det alltid er noen som besitter den relevante informasjonen om den kommende ulykken med mindre ulykken er en anomali. Turner sier at farer og trusler må tas alvorlig og ses på som biter av informasjon som må absorberes og gjennomgå en psykologisk eller sosial prosess hvor de settes i sammenheng. Informasjonen som kan forhindre en ulykke eksisterer i organisasjonen, men er ofte ikke implementert og derfor skjer ulykken. Turner ser for seg at ulykker er et resultat av en prosess som består av en rekke faktorer (se figur 4).

[5] Anomalier: betyr en avvikelse fra normen, det forventede eller lovmessige. En anomali er en irregularitet som er vanskelig å forklare ut fra eksisterende teorier, altså et faktum som strider mot et etablert paradigme.(www.wikipedia.com)



Figur 4: Viser prosessen som fører til ulykker, og hva som skjer i etterkant av ulykker

Fase en: kulturelle overbevisninger om verden og farer vokser frem, man kartlegger og planlegger for å kunne arbeide sikkert. Her dannes grunnlaget for hva organisasjonen anser som sikkert i form av formelle prosedyrer, men også uformelle prosedyrer vokser frem i denne fasen.

Fase to: Inkubasjonsperioden er en periode hvor umerkbare hendelser akkumulerer, som ikke stemmer overens med det man kartla i fase en. Her håndteres problemene ofte basert på det man kartla i fase en, man behandler problemene ut fra hva man vet om verden. Slik misforstås problemene og de dypere mer underliggende/kritiske problemer overses/ignoreres. De små hendelsene er informasjon som kan være et hint om hva som ligger i vente, en periode som kan vare i en måned eller i mange år.

Fase tre: En merkbar hendelse som avslutter inkubasjonsperioden, og som synliggjør de underliggende strukturene. Hendelsen anses som uventet, men kan ha vært varslet av noen grupper men ikke internalisert i organisasjonen. At hendelsen er uventet har en tydelig effekt på organisasjonen og fører til en anerkjennelse av at situasjonen trenger en ny kartlegging.

Fase fire: Umiddelbar reaksjon og kollaps av kulturelle overbevisninger. Verden viser seg annerledes enn antatt.

Fase fem: Organisasjonen jobber for å redde og minimalisere konsekvensene av hendelsen. Eksempelvis evakueringer og brannslokking.

Fase seks: Når de umiddelbare konsekvensene er håndtert, kommer en periode hvor organisasjonen revurderer de eksisterende antakelsene om verden og farer. Her jobbes det for å kartlegge hva som skjedde, for å forebygge liknende hendelser i fremtiden. Etter dette arbeidet er gjort, utarbeides nye regler og prosedyrer basert på erfaringene organisasjonen har opparbeidet i de seks fasene, og da er organisasjonen tilbake til fase en.

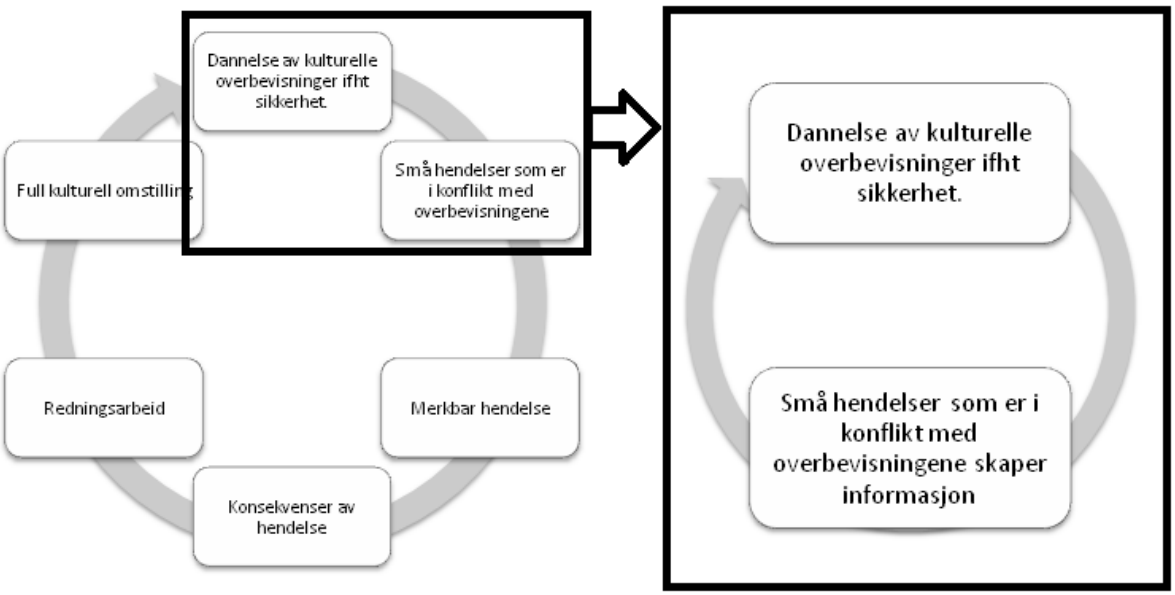
3.1.2 Dannelse av kulturelle overbevisninger og inkubasjonsperioden

Figur 4 viser at faktorene som skaper en ulykker starter i fase en, der man kartlegger verden for å få kunnskap nok til å designe et sikkert system. Kartleggingen skjer basert på erfaring gjort med samme eller liknende system. I fase en vil IO designerne ha tilgang til begrenset informasjon fordi IO teknologien er ny, og kunnskapen som er tilgjengelig fra utviklerne vil bare delvis blir overført i overføringsprosessen. Designerne av IO systemet vil også ha begrensede muligheter til å forestille seg alle mulige risikoer, fordi designprosessen er i likhet med all menneskelig aktivitet underlagt begrenset rasjonalitet[6]. Begrenset rasjonalitet betyr at man aldri kan forutse alt som kan føre til ulykker uavhengig av hvor mye man reflekterer, prøver og feiler, for problemene er ofte så komplekse at vi ikke forstår dem. Alternativt kan man ha misforstått signaler, og derfor ha feilaktige antakelser av verden. Alle disse faktorene bidrar til å forme de kulturelle overbevisningene og deres begrensninger.

Feilaktige antakelser og misforståelser vil bli utfordret i inkubasjonsfasen (fase to), for her kan man se hint om at noe er galt. Man får en mismatch mellom hvordan verden antas å fungere (kartlagt i fase en) og hvordan den virkelig fungerer (hendelser som skjer i fase to). Dersom de endringene som skjer i fase to ikke fanges opp, vil organisasjonen bevege seg videre til fase 3 - 6 og bli fanget opp gjennom at en ulykke presser organisasjonen til å implementere endringene. Med riktig organisering og villighet, kan organisasjoner fange opp signalene i inkubasjonsfasen (fase to) og gjøre en revurdering av prosedyrer og rutiner, uten at en merkbar hendelse inntreffer. Dette vil være mulig gjennom å tolke signalene i organisasjonen og fra omgivelsene, fange opp endringene som skjer i fase to, og til slutt endre de kulturelle overbevisningene (rutiner og praksis). Med andre ord må organisasjonen aktivt

[6] Begrenset rasjonalitet: En forenkling som skjer i selve fortolkningen av et problem. Vi fester oss ved spesielle utsnitt av problemet, og utvikler en forenklet mental modell av det. Det kan være både ønskverdig og nødvendig, men bærer også i seg en risiko for at vi forstår problemet på en for enkel eller forvrengt måte. (Kaufmann og Kaufmann:157)

søke etter informasjon, som analyseres og benyttes aktivt, slik at organisasjonen befinner seg i en ”loop” mellom fase en to. Dersom de ikke mestrer dette vil organisasjonen få en merkbar hendelse, som vil føre til en tilsvarende kulturell rejustering.



Figur 5: Viser hvordan man kan fange opp endringer i fase to og endre de kulturelle overbevisningene slik at man unngår en uønsket hendelse.

Fase en og to bør være hovedfokuset ved implementeringen av IO, fordi det ikke bør være nødvendig med en merkbar hendelse før man fanger opp informasjonen og endrer prosedyrer og rutiner. Det er også i denne fasen endringene blir synlige, slik at inkubasjonsperioden kan forstås som reinovasjonsfasen. Fokuset bør være på fase en og to fordi det er i disse fasene informasjonen spiller en stor rolle for de sikkerhetsmessige utfordringene innføringen av ny teknologi skaper. Jobber man aktivt og kreativ i fase en gjennom ”workshops”, ”brainstorming” og konstruerer scenarioer kan organisasjonen oppdrive informasjon som hjelper designerne til å ta høyde for flere av de sikkerhetsmessige utfordringene IO introduserer. Videre må organisasjonen være oppmerksom i den daglige driften (fase to) og fange opp informasjonen som produseres når teknologien tilpasser seg den nye konteksten. Og implementerer endringene i organisasjonen slik at man ikke får ubalanse mellom teknologielementene.

Målet til IO systemet bør være å jobbe proaktivt[7]: å fange opp informasjonen i fase en og to for å unngå en merkbar hendelse som tvinger organisasjonene til å lære. Merkbare hendelser kan være kostbare for organisasjonen avhengig av deres størrelse og omfang, både i form av kostbare skader men også organisasjonens omdømme[8] kan skades som følge av personskader/dødsfall. Ikke alle merkbare hendelser har store negative konsekvenser, små merkbare hendelser som en nestenulykke gir en mulighet til å lære reaktivt[9], for da tvinges organisasjonen til å utarbeide løsninger som kan forebygge liknende hendelser. Problemet er at man ikke vet om den merkbare hendelsen er stor eller liten og bør derfor fokusere på å unngå at organisasjonen havner i fase tre.

3.1.3 Avsluttende på ny teknologi og ulykker

Det vi har sett her er at de sikkerhetsmessige utfordringene ny teknologi innfører kan knyttes opp imot bruk og forståelse av informasjon. Fordi innføring av ny teknologi preges av en periode med lite informasjon. Der det er vanskelig for designerne å avdekke alle sikkerhetsmessige utfordringer i fase en. Ny teknologi vil ha en etterfølgende reinovasjonsprosess hvor informasjonen gradvis bygges opp gjennom interaksjon med teknologien hvor de kulturelle overbevisningene blir utfordret. Reinovasjonsprosess produserer informasjon om teknologien som må fanges opp og føre til rejusteringer av de kulturelle overbevisningene (prosedyrer rutiner) for å forhindre en merkbar uønsket hendelse.

Implementering av ny teknologi representerer en risiko dersom sikkerhetskritisk informasjon ikke fanges opp og håndteres riktig. Ut fra dette blir det viktig å se nærmere på hvilke faktorer som kan påvirke bruken og forståelsen av informasjon ved innføringen av ny teknologi og vurdere hvordan særtrekk ved IO påvirker bruken og forståelsen. IO systemet preges av en kompleksitet og fysisk avstand mellom aktørene, som kan vanskeliggjøre utnyttelsen og forståelsen av den begrensede informasjon i den nye teknologien.

For å få en bedre forståelse av hva som påvirker informasjonsprosesser, skal studien først se på hvordan sikkerhetskulturen kan påvirke dannelsen av kulturelle overbevisninger som former hvilken informasjon designerne benytter i kartleggingen av fase en. Sikkerhetskulturen påvirker også hvordan informasjonen (endringer) i fase to fanges opp og behandles. Ulike

[7] Reason (1997) definerer proaktivt som tiltak man bruker før en hendelse for å sikre sikkerheten i systemet, det handler om å identifiserer svakheter (latente forhold) i systemet før de fører til en ulykke.
[8] Omdømmet bidrar til interessenter som ansatte, kunder, investorer, leverandører, partnere, myndigheter osv syn på organisasjonen (Hatch & Schultz 2003)
[9] Reason (1997) definerer reaktivt som tiltak man iverksetter etter en ulykke som tar høyde for å forhindre en liknende hendelse i å inntreffe igjen. Man lærer av tidligere hendelser slik at man kan jobbe proaktivt, derfor er både reaktiv arbeid en kilde til viktig informasjon.

subkulturer kan ha forskjellige overbevisninger som kan føre til at de tar til seg teknologien ulikt. Subkulturene kan bli forsterket når fjerndrift gjør at enhetene blir atskilt i tid og rom.

Avstanden mellom enhetene vil videre påvirke de ansattes mentale modeller, hvordan informasjon benyttes til å utvikle et bilde av den totale situasjon. Når IO systemet er komplekst og enhetene er atskilt, blir informasjonsmengden stor og det vanskeliggjør muligheten til å se sammenhengen mellom informasjonsbitene i teknologien. Manglende situasjonsforståelse kan føre til målkonflikter, fordi aktørene handler på bakgrunn av begrenset informasjon der handlingen fremstår som sikker. Selve handlingen kombinert med andre aktørers handlinger kan føre til en uønsket hendelse. Informasjonsbehandlingen blir viktig for å unngå ulykker når den nye IO teknologien skal implementeres. Derfor vil studien avslutningsvis se hva som påvirker om informasjon blir avdekket og implementert i systemer.

3.2 Fremveksten av sikkerhetskultur

Begrepet sikkerhetskultur fikk fotfeste i sikkerhetsstudiene etter Chernobyl ulykken i 1986, hvor sikkerhetskulturen var ansett som et viktig bidrag til ulykken. I nyere historie har man eksplosjonen ved BP raffineriet i Texas 2005 hvor et utvalg av Amerikas fremste ulykkeseksperter konkluderte med at manglende sikkerhetskultur var årsaken til ulykken som kostet 15 mennesker livet. Flin (2007) definisjon av sikkerhetskultur er sammenfallende med Reasons, når de anser sikkerhetskultur til å være følgende:

> ”[…] the product of individual and group values, attitudes, perceptions, competencies and patterns of behavior that determine the commitment to, and the style and proficiency of, an organisations health and safety management […] (Reason, 1997: 194)

Sikkerhetskultur blir et produkt av delte verdier, holdninger og handlingsmønster som avgjør hvor mye sikkerheten prioriteres i organisasjonen. Richter og Koch (2004) ser sikkerhetskulturen som et aspekt av organisasjonskulturen. Det er ikke bare lokale faktorer innenfor organisasjonen som bestemmer medlemmenes kultur, men kulturen vil også bli påvirket av eksterne (nasjonale og regionale) faktorer og bakgrunnen til arbeiderne (utdannelse, sosiale økonomi og religion) (Guldemund, 2007). Sikkerhetskulturen former aktørenes overbevisninger om fare og vil derfor være viktig for IO systemet. Der er fordi feil fokus kan representere en risiko når sikkerhetskritisk informasjon blir ansett som irrelevant.

De kulturelle overbevisninger til sikkerhet som dannes i fase en, er påvirket av deres historiske bakgrunn, erfaringer som organisasjonen og dens individer har i forhold til tidligere ulykker og hendelser samt ekstern påvirkning.

3.2.1 Informasjonssøkende kultur

Ulykker og katastrofer kommer alltid som et resultat av en form for avvik/gap mellom hvordan man tror verden fungerer (fase en) og hvordan verden faktisk er (fase to) (Turner, 1997). Sikkerhetskulturen vil påvirke både dannelsen av overbevisningene i fase en og hvilke endringer som fanges opp i fase to ved implementeringen av IO, derfor blir det viktig å ha en kultur som fokuserer på å fange opp og bruke informasjon.

I fase en former kulturen antakelsene om hva som representerer en risiko ved implementeringen av IO teknologien, hvilke ulykker man kan stå ovenfor, og hvordan man forebygger dem. Mer konkret vil organisasjonens kreativ visualisering, historie og verdier påvirke hva som anses som sikkerhetsutfordringer. Etter at risikoen er kartlagt vil overbevisningene internaliseres i organisasjonen gjennom prosedyrer og rutiner som etter hvert tas for gitt. Turner (1997) sier at kultur har en viktig rolle for å fremme blindhet overfor visse typer farer som ikke er kartlagt i fase en.

Gruppetekning og konsensussøking fører i fase to til falske hypoteser og antakelser om den eksterne verden, samt til forsømmelse og misforståelse av advarsler (Turner 1997). I fase to vil antagelsene om hvordan verden fungerer bli utfordret gjennom den daglige driften, dette er aktuelt når man tar i bruk ny teknologi da driften vil skape informasjon når teknologien tilpasser seg den nye konteksten. Sikkerhetskulturens rolle blir viktig for hvordan denne informasjonen fanges opp og brukes i organisasjonen. En god sikkerhetskultur må i følge Reason (1997) være informert. Det betyr at organisasjoner må aktivt lete etter og bruke informasjonen som er tilgjengelig i organisasjonen. Westrum (1993) har kategorisert organisasjonskulturers informasjonsbehandling opp i patologisk, byråkratisk og generativ kulturer.

Pathological	Bureaucratic	Generative
Don't want to know	May not find out	Actively seek information
Messengers are shot	Listened to if they arrive	Messengers are trained
Responsibility is shirked	Responsibility is compartmentalized	Responsibility is shared
Bridging is discouraged	Bridging is allowed but neglected	Bridging is rewarded
Failure is punished or covered up	Organization is just and merciful	Inquiry and redirection
New ideas are actively crushed	New ideas present problems	New ideas are welcome

Tabell 2: Westrums (1993) typologi om hvordan organisasjoner behandler informasjon

Typologien viser at patologiske kulturer har dårlig informasjonskultur hvor "man ikke vil vite" om uheldige forhold, og man søker heller ikke etter informasjon. I en slik organisasjon vil det være vanskelig å fange opp informasjonen som dannes i reinovasjonsfasen. På motsatt side har man den generative kulturen, som aktivt søker etter ny informasjon gjennom å oppfordre til leting og deling av informasjon. Westrum viser at flere ulykker er en konsekvens av undertrykking av informasjon. Dette kan ses i sammenheng med Turners definisjon som sier at ulykker er resultat av informasjon og energi. I forhold til IO som introduserer en ny teknologi med mangelfull informasjon, bør organisasjonene etterstrebe en generativ kultur som fanger opp informasjonen lokalt og deler med systemet som helhet. Derimot er en patologisk kultur en sikkerhetsrisiko for IO systemet, fordi patologiske kulturer ikke er i stand til å fange opp endringene som skjer i reinovasjonsfasen, og vil føre til en ubalanse i teknologi elementene og derfor en ulykke.

Det er flere ulike faktorer som påvirker om kulturen er patologisk eller generativ, men ledelsens rolle i å fremdyrke en generativ kultur er avgjørende. Turner (1997) mener at en god sikkerhetskultur må ha en ledelse som prioriterer sikkerhet, fremmer en kontinuerlig refleksjon rundt egen virksomhet gjennom analyser og systemer for tilbakemelding. Ledelsen må aktivt være med på å spre det gode budskap, og opptre som rollemodeller for resten av organisasjonen. Man kan ikke forvente at ansatte tenker sikkerhet dersom ledelsen oppfordrer til snarveier og brudd på reglement. DeJoy (2005) mener en god sikkerhetskultur er preget av tillit. En nøkkelkomponent for å oppnå tillit er at ansatte har tro på egenskapene til ledelsen, at

ledelsen handler til det beste på vegne av ansatte med hensyn til sikkerhet. Også Richter og Koch (2004) erkjenner viktigheten av tillit, fordi det ofte er sprik mellom hvordan ledelsen og ansatte tolker sikkerhet, som videre påvirker delingen av informasjon mellom nivåene. En ledelse som slår ned på og dekker over feil de anser som urelevante vil ikke oppnå tillit fra de ansatte, og vil derfor ikke stimulere til generering og deling av informasjon. Dersom IO systemet ønsker å oppnå en generativ kultur som er best egnet for å unngå ulykker, må ledelsen fungere som rollemodeller og fokusere på å skape et system som fremmer og oppfordrer til informasjonsdeling. En generativ kultur vil også se viktigheten av å ha en velfungerende sikkerhetsledelse som fokuserer på å fange opp endringer. En generativ kultur kan være vanskelig å oppnå i IO systemet fordi det består av så mange ulike parter, med ulike verdier og holdninger.

3.2.2 Differensiert kultur

Kulturstudier har gått fra å se kultur som integrert og deles av alle, til å se kultur også som differensiert. En differensiert kultur betyr at det eksisterer variasjoner innenfor en og samme organisasjon, selv om organisasjonen har en felles kulturell overbygning (Richter og Koch, 2004). De ulike grupperingene innenfor en og samme organisasjon kan tolke de kulturelle konstruksjonene ulikt, fordi deres fortolkningsrammer blir påvirket av ulike verdier. Skolebakgrunn, eller hvilken avdeling man jobber i organisasjonen kan forme verdiene, og føre til ulikheter. For eksempel kan man på en flyplass ha flymannskap og vedlikehold på bakken, ledere og arbeidere, fast ansatte og kontraktører, og alle kan ha sine egne sikkerhets subkulturer (Turner, 1997). Olson og Olson (2000) påpeker at ulikheter i lokal fysisk kontekst, tidssoner, kulturer og språk eksisterer til tross for bruk av moderne teknologi. Selv om ny teknologi muliggjør noen former for langdistanse arbeid, vil flere aspekt alltid være vanskelige om ikke umulige å overkomme i fremtiden. Dette har konsekvenser for implementeringen av IO, fordi subkulturene kan resultere i ulik implementering av den nye teknologien. Subkulturer kan forsterkes av at enhetene er separert i tid og rom.

I en kompleks situasjon der flere parter håndterer et problem, er de ikke i stand til å ha samme forståelse av informasjonen. Dette medfører at det eksisterer mange ulike tolkninger av situasjonen. Kunnskap om farer, forhåndsregler, om sikkerhets nivåer og sannsynligheten for ulike typer av ulykker er ikke jevnt fordelt i samfunnet. Å kunne ta rasjonelle velinformerte beslutninger, er ujevnt fordelt mellom grupper og individer (Turner, 1997). Dette kan bety at ulike grupper/subkulturer vil foreta ulike valg i samme situasjon fordi de har ulik bakgrunn og begrenset informasjon om problemet. Olsen og Lindøe (2008a) sier at i reinovasjonsfasen kan

risiko endre form gjennom tilpasningsprosessen. Reinovasjonsprosessen kan utarte seg ulikt for aktørene i IO systemet og medføre ulik praksis. Dersom disse endringene ikke fanges opp og deles på tvers av organisasjonene, kan de teknologiske elementene komme i utakt og skape en uønsket hendelse.

3.2.3 Ulike fortolkninger

Prosessen med å spre informasjonen vil i IO være vanskelig fordi man har kulturelle og sosiale ulikheter som påvirker risikopersepsjonen, og gjør det vanskelig å forstå risiko og farer likt. Det eksisterer ulike fortolkninger fordi man innehar ulik fortolkningsrammer og informasjonen er ikke jevnt fordelt mellom partene. Turner (1997) mener denne problemstillingen også gjør seg gjeldende i preulykke situasjoner. Når flere grupper står ovenfor en informasjonsbehandlings situasjon, feiler de ofte i å bli enige om en overordnet beskrivelse, fordi den enkelte har tilgang til ulik informasjon. Hver gruppe har en tendens til å konstruere ulike teorier, om hvilke problemer man står ovenfor og hva som må gjøres. Derfor kan organisasjonene komme frem til ulike løsninger på problemer i fase to, og resultatet bli ulike rutiner og praksis hos aktørene. Turner poengterer at det er mulig å finne en overordnet teori, men ofte er tid, penger og energi begrenset. Vanligvis kan informasjonen genereres, men de tilgjengelige ressursene er ofte mindre enn det som trengs for å beskrive eller kartlegge situasjonen tilfredsstillende. Relevant informasjon blir en begrenset ressurs i slike situasjoner, da ender man opp med et system som har teknologiske elementer som ikke er samkjørte (Turner, 1997).

3.2.4 Avsluttende på kultur

Vi har i dette avsnittet sett at sikkerhetskulturen påvirker hvor mye sikkerheten prioriteres i organisasjonen. At sikkerhetskulturen former overbevisningene som skapes i fase en og fører til en blindhet for noen typer farer, fordi overbevisningene skaper falske antakelser om hva som representerer en risiko. En dårlig sikkerhetskultur som ikke stiller spørsmålstegn ved de eksisterende reglene og rutinene, vil utgjøre en sikkerhetsrisiko ved implementeringen av ny teknologi. En patologisk kultur vil være en sikkerhetsrisiko for IO, fordi informasjonen som er nødvendig for å bli kjent med teknologien ikke blir fanget opp og de teknologiske elementene havner i utakt. Innføringen av ny teknologi preges av lite informasjon og den informasjonen som eksisterer kan tolkes ulikt av gruppene.

IO kan ha en utfordring når problemer skal håndteres av flere grupper. Det er fordi gruppene foretar beslutninger basert på begrenset informasjon om problemet, som kan føre til uønsket

hendelse. IO systemet må arbeide for å oppnå en viss grad av samkjøring av de ulike subkulturene, for å unngå at ulik tolkning av informasjonen fører til ulik praksis hos aktørene og resulterer i målkonflikter. En generativ kultur er essensiell for å produsere informasjon til kartlegging av problemer i den nye teknologien, og å fange opp endringene i reinovasjonsfasen. Å bygge en generativ kultur kan bli utfordrende i IO systemet fordi det eksisterer så mange parter med ulike verdier og bakgrunner. Da kan man ende opp med en teknologi som er lite samkjørt, og hvor de teknologiske elementene kan komme ut av balanse og skape en uønsket hendelse. IO systemet må arbeide for å bygge en kulturell overbygning som prioriterer sikkerhet, for å bedre fange opp sikkerhetsrisikoer den nye teknologien innfører.

3.3 Mentale modeller er viktig for å kartlegge risiko

Gode mentale modeller blir viktig for å minimere antall usikre handlinger, fordi aktørene kan gjennom en god forståelse avdekke om handlingene får negative konsekvenser. En mental modell er en forenklet måte å forstå et problem på. Vi fester oss ved spesielle utsnitt av problemet, og utvikler en forenklet mental modell av det (Kaufmann og Kaufmann, 1997). Mentale modeller er en forenklet virkelighet som benyttes både av designerne som kartlegger og planlegger IO systemet, og av aktørene som jobber i systemet. Det vil være vanskelig å sørge for at aktørene har gode mentale modeller når aktørene er atskilt i tid og rom og samtidig er bunnet sammen av komplekse IKT systemer. Avstanden og kompleksiteten gjør at aktørene kan miste oversikten og mangelfulle mentale modeller kan utgjøre en sikkerhetsrisiko både i fase en og to. I fase en kan designerne lage farlige løsninger fordi de besitter modeller som ikke griper virkeligheten godt nok, og i fase to er mentale modeller avgjørende for å fange opp endringene i teknologien.

Leveson (2004) påpeker at det kan skje en ulykke selv om softwaren utføre sin intenderte funksjon, fordi designerne av systemet feilet i å forutse at i noen situasjoner ligger forholdene til rette for at ”normal drift” kan føre til en uønsket hendelse. Forståelsen av sammenhengene mellom systemets komponenter er viktig i fase en hvor man forsøker å kartlegge hva som kan gå galt. Pidgeon og Leary (2000) sier at man må arbeide med å fremme ”sikkerhetsfantasien” gjennom å frykte det verste og bruke teknikker som å visualisere ”worst case” situasjoner, hvilke potensielle farer man kan stå ovenfor og hvordan nestenulykker kan utvikle seg til ulykker.

Ofte konstruerer vi software som overgår menneskelig fatteevne, og automatisering av teknologien gjør systemene mer komplekse og man mister oversikten (Leveson, 2004). Mentale modeller er påvirket av begrenset rasjonalitet, som setter grenser for hva vi klarer å forstå når prosesser blir automatiserte. Software (IKT) har åpnet for muligheter som er mer omfattende enn det vi klarer å styre på en suksessfull og sikker måte. Leveson sier videre at det er problematisk at vi forsøker å bygge systemer som sprenger vår intellektuelle evne: Økt interaktiv kompleksitet og koplinger gjør det vanskelig for designerne å forutse alle de potensielle utfordringene den nye teknologien kan møte. IO systemet er et slikt system med økt interaktiv kompleksitet og koplinger. Det er fordi mange aktører er involvert, prosessene er automatiserte og operatører på land kan utføre operasjoner som gir direkte utslag offshore.

3.3.1 Mentale modeller viktig for å fange opp endringene i den daglige drift

Når man i fase to tar i bruk fjerndrift i IO systemet blir det viktig at de involverte partene har gode mentale modeller, for å fange opp eventuelle design svakheter. Weick et al. (1999) påpeker at det er viktig at individene i en kompleks organisasjon har et fullstendig bilde av systemet de jobber i, for å bedre håndtere det usikre og uventede (det man ikke kartla i fase en). Weick fokuserer på det kognitive aspekt hos individende, og hvilken betydning situasjonsforståelsen og mentale modeller har for å oppdage og utbedre feil i en organisasjon. Men det er ikke alltid den menneskelige kontrollør er i stand til å forstå mentalt hva den komplekse automatikk sier. Systemulykker[10] har ofte sitt utspring i ulikheter mellom den mentale modellen kontrolløren besitter (kulturelle overbevisninger), og den aktuelle prosess (Leveson, 2004). I likhet med Turner (1997) ser Leveson viktigheten av å fange opp og implementere informasjonen som genereres i fase to, for å unngå at man får et sprik mellom de mentale modellene og den aktuelle prosessen. Et viktig spørsmål som alltid bør reises er om kontrollørene og beslutningstakerne har den nødvendige informasjonen. Leveson sier at informasjon styres i deres prosessmodeller, og oppdatering av disse mentale modellene er vitalt for å unngå ulykker.

For å kunne kontrollere IO systemet må operatøren ha en modell av systemet og kontrolløren må være i stand til konstatere systemets status. Modellen kan være fysisk for en automatisk kontrollør, men kan også være en mental modell for en menneskelig kontrollør. Den må bare inneholde samme type informasjon (Leveson, 2004). Mentale modeller utvikles gjennom trening og at fysisk modeller av systemet er tilgjengelig for operatørene. Målet er å gjøre

[10] . En systemulykke er i følge Reason (1997) sjeldne men ofte katastrofale. De kan ha flere årsaker og involvere mange ansatte som arbeider på ulike nivåer i organisasjonen.

prosessmodellene så konsistente som mulig slik at de ikke utgjør en risiko når de er i bruk, noe som er vanskelig når IO systemet er komplekst og består av automatiserte og menneskelige prosesser (Leveson, 2004).

3.3.2 Feilaktige mentale modeller kan lede til ulykker

Prosessmodellene kan være feil fra starten av på grunn av utilfredsstillende kartlegging i fase en, eller de kan bli feil på grunn av manglende feedback i fase to. Manglende feedback kan redusere evnen til å fange opp endringene eller formidle informasjonen til de rette instansene. Modellene kan også være unøyaktig for en periode, på grunn av tidsforsinkelse på feedbacken. Det fører til at de mentale modellene kan ligge bak systemets endring og derfor bli utdaterte og feilaktige. For Leveson (2004) er informasjonsdeling(feedback) nødvendig i alle avdelinger og mellom alle nivåer, for å fange opp endringer og unngå uønskede hendelser.

Mentale modeller blir viktig i IO systemet siden de kan hjelpe aktørene å se sammenhengene mellom de ulike komponentene og forstå dersom det forekommer et avvik (endring). Avviket kan vise seg i form av en unaturlig tallverdi i en annen del av systemet enn hvor handlingen ble utført. Avviket kan fanges opp dersom aktørene har en forståelse som går ut over sin egen situasjon. Mindre avvik anses ofte som små og ubetydelige slik at de ignoreres og får rom til å utvikle seg til å bli store og i verste fall en ulykke, derfor må også små endringer fanges opp.

Turner viser at en viktig årsak til ulykker er systemer som er store eller komplekse, der flere ansatte og organisasjoner har tilgang. Dette er fordi det blir så vanskelig å holde oversikt over hvem som gjør hva til hvilken tid. Sammenhengene mellom elementene blir så omfattende og komplekse at man har problemer med å bygge opp tilfredsstillende mentale modeller. IO er et stort og komplekst system hvor flere organisasjoner har adgang, og systemet blir enda mer komplekst fordi det benytter seg av ny teknologi som kontinuerlig endrer seg. Det blir viktig for IO systemet å fange opp endringene i teknologien dersom de skal sørge for at aktørene har tilfredsstillende mentale modeller.

3.3.3 Avsluttende på mentale modeller

Vi har sett at mentale modeller er en forenklet virkelighets modell som er viktig for at designerne skal kartlegge sikkerhetsmessige problemstillinger i den nye teknologien på en tilfredsstillende måte. Men at teknologi som preges av automatiseringer vil øke kompleksiteten og koplingene og gjøre det vanskelig for både designere og aktører å få en

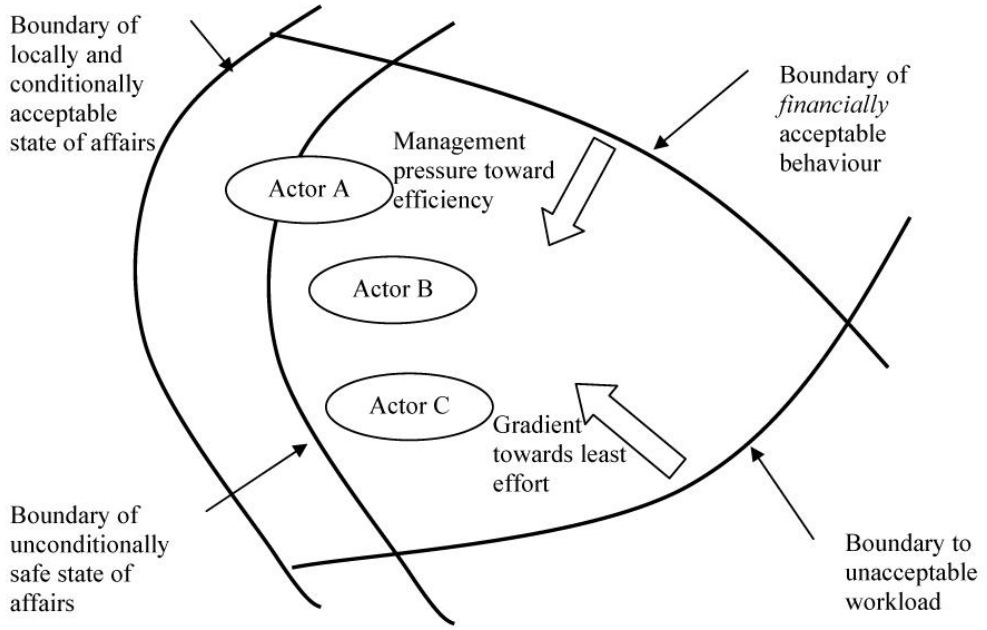
tilfredsstillende forståelse. Gode mentale modeller er avgjørende for å oppdage endringer i den daglige driften (reinovasjonsfasen), fordi operatører må være i stand til å konstantere systemet status og oppdage avvik. Skal IO teknologien være sikker må systemet sørge for å fange opp informasjonen lokalt, og spre den til designerne som kan oppdatere prosedyrer og rutiner. Dersom endringene fanges opp og implementeres i prosedyrer, vil aktørene besitte like og oppdatere mentale modeller.

Målet for IO systemet må være å sikre at alle de involverte aktørene besitter så gode og oppdaterte mentale modeller som mulig. Det for å minimere risikoen for målkonflikter som avstanden i IO systemet kan forsterke. IO systemet innfører ulike utfordringer i forbindelse med mentale modeller, for det første er systemet så stort og komplekst at aktørene sliter med å forstå det, og derfor feiler med å se sin egen rolle i forhold til helheten. Eller fordi systemet er så fragmentert ved at aktørene er separert i tid og rom at det vil være en treighet i systemet, som gjør at informasjonen ikke fanges opp like fort som teknologien utvikler seg, og fører til at de mentale modellene ikke er oppdaterte.

3.4 Målkonflikter kan føre til ulykker

Målkonflikter vil være en sikkerhetsmessig utfordring som IO systemet må jobbe aktivt for å bekjempe. Når teknologien er ny betyr det at aktørene i systemet har begrenset informasjon om arbeidsprosessene og sammenhengene i systemet. Avstand i tid og rom forsterker at målkonflikter kan inntreffe, fordi aktørene ikke forstår egen rolle i forhold til helheten. Videre kan systemet bli så stort og komplekst at aktørene innehar mangelfulle mentale modeller som fører til målkonflikter.

Rosness (2004; 2001) viser at i komplekse systemer hvor mange aktiviteter utføres parallelt, kan hver aktør ha ufullstendig eller upresis kunnskap om statusen til systemet og de pågående aktivitetene. De pågående aktivitetene kan komme i konflikt med hverandre uten at det virker logisk for aktørene. Dette er relevant dersom systemet har høy grad av interaksjon og kompleksitet, hvor beslutningstakningen er distribuert. Det er fordi hver beslutningstaker kan ha en modell og informasjon av en begrenset del av problemet, Rasmussens (1994) modell visualiserer problematikken:



Figur 6: Rasmussens modell som visualiserer tilpasning i en kompleks organisasjon, der flere aktører handler individuelt innenfor området som er akseptabelt.

Rasmussen viser med sin modell at det eksisterer en ytre og en indre grense for sikker atferd. Den ytre grensen kan krysses med forbehold mens den indre grensen ikke kan krysses uten at det innebærer for høy risiko. Dette vil si at en aktør kan krysse den ytre grensen for sikker atferd uten at dette gir negative konsekvenser for sikkerheten. Men krysser flere aktøren den ytre grensen kan summen av handlingene føre til at de samlet sett krysser den indre grensen. Det vil resultere i en uakseptabel høy risiko for at en ulykke kan inntreffe. Atferd som isolert sett er rasjonell kan sammen med liknende atferd føre til en ulykke. Og sikker atferd som utføres innen ett arbeidsområde kan endre grensene for hvilke atferd som kan utføres i andre arbeidsområder. Finansielt press og tidspress er medvirkende faktorer som kan forsterke at aktører gjør individuelle nyttemaksimerende valg og krysser den ytre grense (Rasmussen, 1994).

IO systemet er preget av tette koplinger og komplekse interaksjoner vil gjøre det mer utsatt for målkonflikter. Når aktørene har begrenset informasjon om den totale situasjonen og risikoen, forstår de ikke konsekvensene av egne handlinger. IO som er ny teknologi vil være preget av en tilstand med manglende informasjon i reinovasjonsfasen, og derfor være mer utsatt for målkonflikter. Operasjoner utført på land kan være i konflikt med det som gjøres offshore. Avstanden i systemet gjør det vanskeligere for aktørene å forstå resultatene av egne handlinger, fordi resultatet ikke er synlig og rammer mennesker som er langt borte.

3.4.1 Avstand til risikokilden kan påvirke sannsynligheten for målkonflikter

Videre kan avstand til risikokilden være avgjørende for hvor stor risiko aktørene er villige til å ta. Personell ved ”sharp end” som jobber tett på risikokildene vil unngå å ta valg som medfører risiko fordi de rammes først dersom en ulykke skulle oppstå. ”Sharp end” personell blir ofte ansett som syndebukk når det smeller, siden deres handling kan lett relateres til de utløsende faktorer til ulykken. Personell ved ”blunt end” slik som ledere, er ofte i større grad villig til å ta risiko på bakgrunn av deres orientering mot produksjon og distanse fra de daglige opperasjonene som innebærer risiko (Rasmussen, 1994). Mennesker handler stort sett ikke risikofullt, og Rosness (2001) viser til en studie av 57 ulykker på sjøen, hvorav 21 % av ulykkene ikke hadde tilgjengelig informasjon, og i 27 % av tilfellene ble ikke situasjonen ansett som problematisk. Han viser at aktører tar risikofylte valg når de har manglende informasjon, eller undervurderer situasjonen.

Dersom dette er tilfellet kan operatører som er fjernt fra risikokilden være mer tilbøyelig til å ta risiko på bekostning av de som jobber offshore. Det er fordi de ikke anser situasjonen som problematisk ut fra en vurdering av tilgjengelig begrenset informasjon. Avstanden i IO systemet kan innføre en sikkerhetsrisiko fordi operatørene mangler en ”frykt” for å trå feil, og ved å handle på informasjon som er manglende kan skyve organisasjonene innenfor den ytre grensen for sikker atferd. Dersom personell offshore gjør lignende handlinger basert på begrenset informasjon, kan summen av dette bringe organisasjonen til den indre grensen og ulykken er et faktum.

3.4.2 Målkonflikter i grenseområdene

IO systemet innfører med sin fjerndrift i generasjon to flere grenseområder[11]. Det er fordi mange operatører og offshore skift vil være involvert gjennom ”follow the sun” prinsippet. Turner (1997) påpeker at en inter organisatorisk gruppering med en eller to store organisasjoner, samt noen små involvert, kan være en faktor som leder til ulykker. Leplat (1987) viser at ulykker ofte finner sted i grenseområder eller i overlappingen til to eller flere kontrollørers ansvarsområder. Siden det eksisterer en usikkerhet om hvem som er ansvarlig kontrollør, og det er vanskelig å koordinere i grenseområdende. Ulykker som har funnet sted på grunn av feil i grenseområder, har gjennom utredninger avdekket at involverte aktører trodde andre var ansvarlig for kontrollen.

[11] Grenseområde vil i studien bety områder der flere aktører er involvert og ansvar kan fremstå som uklart.

3.4.3 Avsluttende på målkonflikter

Vi har sett at målkonflikter stammer fra atferd som isolert sett er rasjonell, kan sammen med tilsvarende atferd føre til en ulykke. Målkonflikter kan inntreffe når mange aktiviteter utføres parallelt, og systemer har en høy grad av interaksjoner og kompleksitet. IO systemet er komplekst og tett koplet med aktiviteter som pågår parallelt. Samtidig er det mange både store og små organisasjoner involvert, som gjør at grenseflatene er mange og komplekse. Hovedårsaken til at målkonflikter forekommer er at beslutningstakerne mangler informasjon og undervurderer situasjonen. Ny teknologi forsterker muligheten for målkonflikter siden teknologien introduserer en tilstand med manglende informasjon. IO systemet vil ha mange grenseområder som må koordineres, og sørge for at informasjonen når de rette personene til rett tid, for å unngå at valg blir tatt på et begrenset informasjonsgrunnlag. En faktor som kan bidra til målkonflikter ved implementeringen av IO i generasjon to, er at beslutningstakere blir flyttet bort fra risikokilden og kan derfor være mer villige til å utføre risikofulle handlinger.

Det vil bli viktig å ha en felles forståelse for hovedmål og deres oppgaver/prosedyrer, og forstå ens egen rolle i forhold til andre (mentale modeller). Siden teknologien er ny og derfor utvikler seg kan målene og oppgavene skifte ettersom de teknologiske elementene endrer seg. IO systemet må avdekke endringene og implementere informasjonen i systemet fortløpende ettersom teknologien endrer seg. Slik at prosedyrer og de mentale modellene er oppdaterte og situasjonsforståelsen tilfredsstillende.

3.5 Det er viktig å fange opp informasjonen teknologien gir

Informasjon er viktig for sikkerheten i IO systemet, fordi informasjonen som ligger i den nye teknologien påvirker utviklingen av subkulturer, de mentale modellene og er viktig for å unngå målkonflikter. Endringene vil produsere informasjon som er viktig å fange opp, for å sørge for at de teknologiske elementene står i forhold til hverandre. På grunn av informasjonens rolle for sikkerheten i innføringen av ny teknologi vil vi se grundigere på hva som gjør informasjon så vanskelig å fange opp og dele i organisasjoner.

Turner(1997) viser at problemer med informasjon er ofte i tilknytning til ”ill structured problems[12]”, dette er problemer som er komplekse og vage, som det er vanskelig å systematisere eller skaffe informasjon om. Turner påpeker at det alltid er noen som innehar informasjon som kan forebygge uønskede hendelser. Informasjonen er kjent for noen men ikke integrert i organisasjonen til rett tid, alternativt blir ikke informasjonen verdsatt som relevant. Hendelser som ikke verdsettes/misforstås er ofte et resultat av problemer med å håndtere informasjon i komplekse situasjoner. Det vil si at man misforstår informasjonen som endringene gir oss, og dermed klarer vi ikke å fange dem opp. Hva som anses som relevant påvirkes av hvilken sikkerhetskultur organisasjonen innehar.

Man kan også ha problemer med å fange opp informasjonen endringene gir på grunn av ”decoy fenomenet”, som er når synlige problemer tar bort oppmerksomheten fra bakenforliggende problem (Turner, 1997). Det vil medføre at organisasjonen ikke forstår informasjonen, og Turner viser her til empiriske studier som sier at relevant informasjon forsvant i irrelevant informasjon i flere store ulykker. Reason (1997) viser en liknende problemstilling, og han poengterer at man ikke tar fatt i problemene, fordi det er noe annet som virker viktigere/mer kritisk.

Uavhengig av om informasjonen tas for gitt, misforstås eller overses vil resultatet bli at endringene ikke fanges opp og organisasjonen beveger seg til fase tre. Dersom riktig informasjon ikke er tilgjengelig er det lite sannsynlig å få en tilfredsstillende respons på den uønskede hendelsen. Sikkerhetsledelsen må jobbe aktivt og benytte tilstrekkelig med ressurser for å kartlegge problemene, og unngå ”decoy fenomenet”. Gjøres dette vil muligheten for å fange opp de riktige endringene øke.

For å fange opp informasjonen som skapes i reinovasjonsprosessen sier Weick et al. (1994) at organisasjonen må ha et fokus på drift. Med det mener han at oppmerksomheten må være rettet mot å avdekke symptomer som viser seg i den daglige driften (fase to). Weick benytter begrepet ”mindfullness” som kan forstås som at organisasjoner må ha en årvåkenhet, for å fange opp signaler fra omgivelsene som kan forebygge forekomsten av uønskede hendelser. Mindfullness er viktig for å redusere overraskelses momentet (anomalier) og redusere tiden før en reagerer på en hendelse. Weick sier videre at en bør utvikle uformelle nettverk til å

[12] Ill structured problems, er forstått som uoversiktelige problemer, hvor mange faktorer som gjør det vanskelig å få innsikt i problemets sanne natur.

supplere den formelle organisasjonen med kunnskap og erfaringer, for at den skal bli bedre rustet til å håndtere informasjonen og hendelser i reinnovasjonsfasen.

3.5.1 Kommunikasjon av informasjon

Informasjon kan være tilgjengelig i organisasjonen, men kommunikasjonen mellom enhetene er ikke tilfredsstillende. Når man i IO frem mot generasjon to innfører fjerndrifting av anlegg, vil den daglige driften basere seg på IT kommunikasjon mellom enhetene. Det vil si at sikkerheten i systemet er avhengig av kvaliteten på kommunikasjonen er mellom enhetene.

Feil- og kommunikasjonsproblemer er et sentralt moment i inkubasjonsfasen (fase to), og kan forsterke målkonflikter. Det er fordi misforståelser, forbigåelser og feil antakelser mellom parter vil bidra til at uønskede hendelser akkumulerer i en organisasjon (Turner, 1997). Kommunikasjon er:

> "[…] den prosessen der en person eller gruppe eller organisasjon (sender) overfører en type informasjon (budskap) til en annen person, gruppe eller organisasjon (mottaker), og der mottaker(ne) får en viss forståelse av budskapet" (Kaufmann og Kaufmann, 1997: 286).

Kaufmann og Kaufmann skiller informasjon og mening, da overføring av informasjon ikke nødvendigvis garanterer effektiv kommunikasjon, fordi meningsinnholdet er forskjellig for sender og mottaker. I en sikkerhetskontekst er dette skillet viktig for å unngå ulykker, man må sørge for en overføring av mening slik at mottaker får en forståelse for sitasjonen man står ovenfor, og kan ta rette valg. Det er verdt å merke seg at perfekt kommunikasjon aldri vil være mulig i komplekse systemer (Turner, 1997).

Dårlig kommunikasjon mellom to individer kan forekomme på grunn av personlighet eller andre ulikheter (Ibid). Noe så enkelt som valg av språk, dialekt og faguttrykk kan også representere hindringer i formidlingen mellom mennesker (Kaufmann og Kaufmann, 1997). Det man ser er at kommunikasjon over avstand kan føre til problemer i generasjon to fordi man er avhengig av å overføre meningsbærende informasjon mellom ulike disipliner og til og med land, som kan ha ulik forståelsesrammer og begrepsbruk.

Oppgaver som håndteres av store organisasjoner vil generere mange meldinger og øke sannsynligheten for feilkommunikasjon. Det er fordi relevant informasjon drukner i irrelevant informasjon. Sammenhengen mellom vanskeligheter med å håndtere informasjon og feilkommunikasjon fører til en akkumulering av hendelser og øker sjansen for en uønsket hendelse (fase tre) (Turner, 1997).

Etter at informasjonen blir fanget opp og overført, må den transporteres til de rette personene, som kan implementere informasjonen i organisasjonen. Leveson (2004) påpeker at sikkerhetsinformasjonen kommuniseres ofte på en dårlig måte til systemets designere og testere. Dersom man ikke får kommunisert den rette informasjonen til beslutningstakere og designerne får man utdaterte prosedyrer og rutiner, som videre gir dårlige mentale modeller og gjør det vanskelig å fange opp de teknologiske endringene.

Kommunikasjonsproblemene vil væres størst i forhold til de ulykkene Turner (1997) definerer som anomalier, fordi de er uventa og derfor vanskelige å klassifisere. Klassene er oftest definert på forhånd i fase en (kulturelle antagelser), basert på erfaringer og analyser av hvilke farer man forventer å stå ovenfor. Avsendere vil ha problemer med å plassere informasjonen i de riktige klassene, for å overføre dem på best mulig vis til mottaker.

Ulykkene Turner definerer som anomalier er en uventet situasjon, og havner derfor i kategorien ”null sannsynlighet”. Organisasjonene vet ikke hva de skal gjøre når eksisterende kommunikasjonsklasser er utilfredsstillende. Det vil nærmest være umulig å overføre informasjonen med de eksisterende kommunikasjonskanalene. La oss ta et eksempel: En hendelse inntreffer og en spesiell lukt kan gi informasjon om problemet til noen med erfaring. Problemet er at de med erfaring sitter på land, og hvordan skal de offshore klare å beskrive lukten, når kommunikasjonskanalene er video overvåkning og telekommunikasjon? Hvis lukten ikke fanges opp, vil man da få en tilfredsstillende respons på problemet, eller vil man bare behandle de synlige problemene?

IO systemet preges av avstand hvor de benytter standardiserte kommunikasjonskanaler for å overføre informasjon. Systemet kan møte en ekstra stor utfordring dersom en anomali inntreffer. Siden det er vanskelig å kommunisere over avstand, informasjon som ikke kan fanges opp av tall eller video overvåkning, slik som lukt, visse typer lyd eller følelser. Da kan man ende opp med en situasjon hvor operatørene på land bare får overført informasjon men ikke mening.

3.5.2 Avsluttende på informasjon og kommunikasjon

I dette kapittelet har vi sett at utfordringer med å fange opp informasjon i ny teknologi er et resultat av at problemer ikke er tydelige og lette å forstå men er komplekse og vage (”ill structured”). Selv om organisasjoner lykkes med å fange opp informasjon kan den misforstås. Misforståelsene kan være resultat av menneskelig begrensning og gjeldende sikkerhetskultur. En patologisk kultur vil i begrenset grad se verdien av sikkerhetskritisk informasjon. Skal

implementeringen av IO i generasjon to være vellykket må vage problemer fanges opp og forstås, samt å dyrke en kultur som er opptatt av sikkerhet og endringer.

”Decoy fenomenet” kan hindre at endringene fanges opp, når synlig problem tar bort oppmerksomheten fra bakenforliggende årsaker. Også her blir det viktig å bygge opp en generativ kultur som samtidig er skeptisk, som ikke tror løsningen ligger i den første som byr seg. Organisasjoner må ha fokus på drift og omgivelsene for å fange opp den mindre synlige informasjon.

Når informasjonen er fanget opp, er feil og kommunikasjonsproblemer et sentralt moment i inkubasjonsfasen. Sikkerhetskritisk informasjon blir ikke overført tilfredsstillende på grunn av språk, dialekt, feilrapportering eller fordi systemet har mange aktører som skaper for mye informasjon. Størst fare for dårlig kommunikasjon skjer i pressede situasjoner når organisasjonen står ovenfor anomalier, fordi eksisterende kommunikasjonskanalene feiler. De klarer ikke å overføre tilstrekkelig mening til mottakerne gjennom de etablerte kanalene. IO kan få problemer dersom de står ovenfor en endring de ikke har planlagt for, fordi avstanden i seg selv kan vanskeliggjøre overføringen av informasjon til operatørene på land.

Hittil er teori som omhandler de utfordringer ny teknologi representerer og hvordan avstand og kompleksitet i systemer påvirker informasjonsbehandlingen presentert. I neste kapittel vil resultatene fra dokumentanalysen bli presentert og drøftet fortløpende i forhold til oppgavens teoretiske ramme. Sentralt i diskusjonen er å vise hva forskningsdokumenter sier om problemstillingene vi har presentert i dette kapittelet. Henholdsvis sikkerhetskultur, mentale modeller, målkonflikter og informasjonsbehandling.

Diskusjonen vil starte med en vurdering av hvor langt man har kommet med implementeringen av IO på norsk sokkel og om IO kan kalles for ny teknologi. Deretter blir det viktig å vurdere om sårbare elementer ny teknologi innfører, kan bli forsterket av særtrekk ved IO teknologien. Vi har tidligere sett at ny teknologi introduserer en tilstand med manglende informasjon som øker sjansene for en ulykke. IO introduserer en avstand mellom enhetene og en kompleksitet som kan påvirke bruk og forståelse av informasjonen i den nye teknologien.

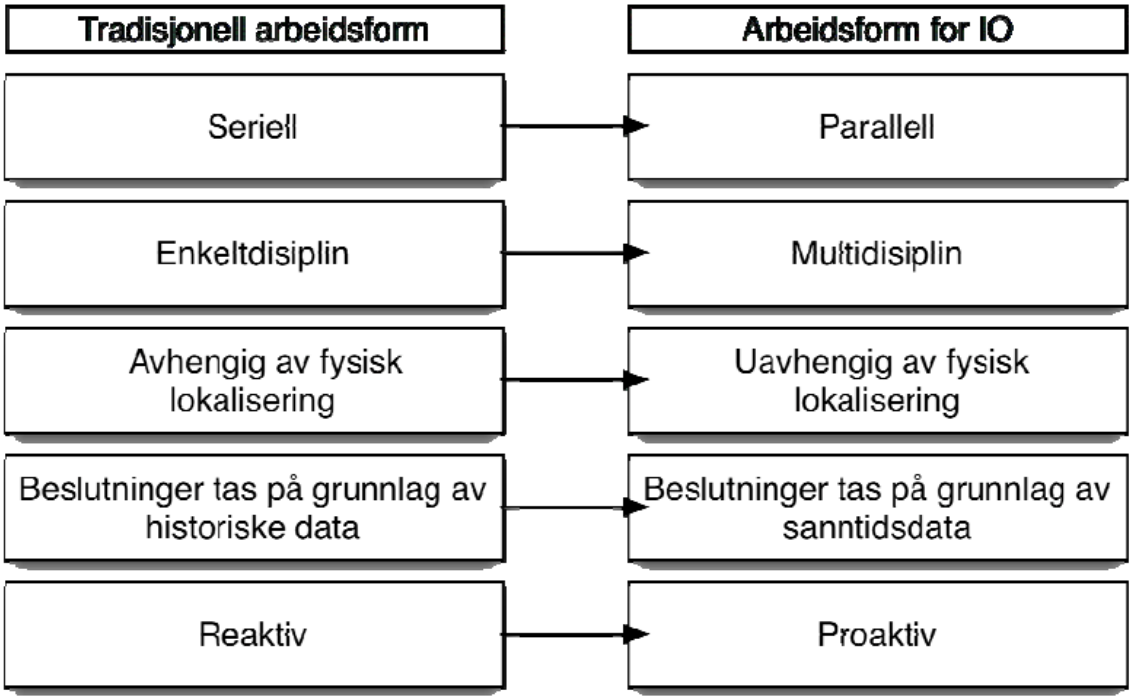
4.0 IMPLEMENTERING AV INTEGRERTE OPERASJONER

Ptil skriver at innføring av IO har ikke skjedd i det tempo som oljeindustrien forventet for få år siden. Årsaken kan være høy oljepris og stor aktivitet på sokkelen. Operatørene har som følge av IO bare flyttet noen av sine administrative oppgaver fra hav til land. Entreprenørene har enda ikke endret på arbeidsdelingen mellom hav og land som følge av IO (Sintef, 2008 b). Ptil påpeker videre at operatørselskapene er mer positive til IO-prosessen enn entreprenørene. Mens operatørselskapene mener at mange av målsettingene er innfridd, etterlyser entreprenørene en bedre deling av gevinst og risiko. Entreprenørene er misfornøyd med informasjon og tilgang på data. Det kan skyldes forhold rundt kontrakter eller IT-sikkerhet (www.ptil.no). Sintef påpekte at i 2008 var mangel på tilgjengelige data et problem i IO, men at man var i ferd med å gå inn i et prosjekt for bedre innsamling av data og overvåking av operasjoner fra land. Rapporten viser også at bransjen ønsket en større grad av styring av operasjoner fra land i fremtiden (Sintef, 2008b). Implementeringen av IO har ikke hatt den fremdrift som forventet. Det kan bety at de teknologiske endringene i generasjon to vil inntreffe på et senere tidspunkt enn 2015.

4.1.1 Er integrerte operasjoner ny teknologi?

Olsen og Lindøe påpekte at den forventede ulykkesraten vil øke de første årene i den nye konteksten, helt til risikoledelsens kunnskap/kompetanse i forhold til den nye teknologien er tilfredsstillende. For å si noe om sikkerhetsutfordringene ved implementeringen av IO er det viktig å vurdere om IO teknologien er ny teknologi.

Tveiten et al. (2008) sier at integrerte operasjoner ikke nødvendigvis er ny teknologi, men å bruke data på nye måter. En snever forståelse av begrepet teknologi omfatter kun verktøyene. I en slik forståelse vil ikke IO være ny teknologi fordi de benytter allerede eksisterende IKT teknologi. Spørsmålet er hvor grensen er for å kalle en teknologi for ny? IO vil basere seg på eksisterende IKT, men må omorganisere og jobbe på en ny måte. Det innebærer endringer i de teknologiske elementene team og oppgaveutførelsen (se figur 2/3), og kvalifiserer dermed IO som ny teknologi. Implementeringen av IO innfører nye teknologiske elementer som man ikke har full kunnskap om, og som må tilpasse seg den nye konteksten gjennom reinovasjoner. Endring i samarbeidsformene blir visualisert av OLF:



Figur 7: Illustrerer endringene i arbeidsformene fra generasjon null til generasjon to. Hentet fra OLF (2007 b)

Figuren viser at IO vil innføre endringer: at arbeidsformene blir mer komplekse da arbeid utføres samtidig uavhengig av fysisk lokalisering, og basert på sanntidsdata hentet ut fra en database. Den nye teknologien som innføres vil hovedsakelig endre ”teams” og ”tasks” i teknologimodellen (se figur 2). Dette er mulig som følge av en utvikling av de verktøyene man i dag benytter ”tools”.

Det at IO blir definert som ny teknologi betyr at implementeringen vil ha de samme trekkene som innføringen av ny teknologi beskrevet av Engen, Olsen og Lindøe. Ny teknologi skaper en tilstand med manglende informasjon som gjør det vanskelig å planlegge og kartlegge sikkerhetsrisikoen IO kan introdusere. IO vil samtidig være utsatt for kontinuerlige endringer når teknologien tilpasser seg den nye konteksten, og kan føre til en ulykke. Derfor vil det være viktig for IO systemets sikkerhet å jobbe aktivt med informasjonsbehandlingen både i fase en og to.

4.1.2 Kartlegging av ny teknologi og endringer av teknologien.

Planleggingen av IO mot generasjon to vil være en omfattende design prosess, fordi man skal implementere noe nytt der designerne mangler informasjon om sikkerhetsutfordringene. Turner påpekte at designerne jobber under en tilstand med begrensede data. Dette sammen

med at teknologien er ny, vil vanskeliggjøre planleggingen og designet av IO. Kunnskap designerne besitter er ofte overlevert i teknologioverføringen (fra for eksempel produsent gjennom trening), eller kunnskap man produserer i planlegningsfasen (gjennom "worst case" scenarioer). Men som vi har sett er det vanskelig å overføre kulturelle og sosiale forhold fra de organisasjonene som har utviklet IO systemet, til de som skal ta i bruk IO. Samtidig er menneskets evne til å forutse alle utfordringer underlagt begrenset rasjonalitet. Derfor er det riktig å anta at risikoene som kartlegges i fase en ikke vil være fullstendig på grunn av manglende informasjon. Og at man derfor må jobbe aktivt for å fange opp informasjonen som skjer i reinnovasjonsfasen. I følge Engen, Olsen og Lindøes teori må både små og store endringene fanges opp for å unngå en uønsket hendelse.

Ved implementering av IO kan risikovurderinger og risikoidentifikasjoner, som er gjort i tidligere faser ha mistet sin relevans underveis og blitt erstattet av nye. Det er fordi de opprinnelige forutsetningene som har vært lagt til grunn ikke er relevant eller riktige lenger (Sintef, 2005). Skal IO systemet være sikkert må organisasjonene fange opp informasjonen og implementere den inn i organisasjonen etter hvert som teknologien endres, for å unngå at det eksisterer områder som ikke har bra nok sikkerhetsprosedyrer. Arbeidet med å fange opp endringene er vanskelig når teknologien er ny, fordi forutsetningene endres så fort og gjør det vanskelig å fange opp og implementere endringene fortløpende. Og resultatet blir utdaterte sikkerhetsprosedyrer.

Teknologisk utvikling var en faktor som førte til Challenger ulykken[13]. Ingeniørene måtte konstant jobbe med den teknologiske utviklingen hvor de ikke hadde full kunnskap om teknologien. De utviklet teknologien mens de jobbet med den. I slike omstendigheter kan ikke design og operasjoner fullt ut kartlegges og implementeres i prosedyrer på forhånd. Selv om NASA hadde regler for å designe sikkerhet, var det også et system som aksepterte avvik når det var nødvendig som et direkte resultat av teknologien. Hva som ble ansett som akseptabel risiko var et spørsmål underlagt sosial forhandling, heller enn en objektiv egenskap i et teknologisk system (Turner, 1997).

Johnsen og Lundteigen (2008) påpeker at det å innføre IO er en læringsprosess for alle som utfører drift og vedlikehold, enten i et oljeselskap eller hos leverandører, fordi det er en ny teknologi som stadig utvikler seg. Høyland (2007) avdekket i et intervju av en representant fra OLF at utfordringene i forbindelse med IO er at teknologien endrer seg så rask. Det vil si at

[13] Challenger:: romferje som eksploderte ved oppskytning 28.Januar 1986 (Turner 1997)

ansvar, roller og arbeidsprosesser i den styrende dokumentasjonen ligger alltid langt bak teknologiutviklingen. Dette synliggjør viktigheten med å ha en sikkerhetsledelse i IO som jobber aktivt med å fange opp og implementere endringene fortløpende i generasjon to. Dersom dette ikke gjøres kan reinovasjonsprosessen i seg selv representere en risiko fordi endringene gjør at de teknologiske elementene ikke står i forhold til hverandre (Engen og Olsen, 2010).

4.1.3 Integrerte operasjoner og ulykker

Avstand sammen med kompleksiteten i IO systemet er særtrekk som kan forsterke de sikkerhetsmessige utfordringene ny teknologi innfører. Som vi har sett tidligere vil generasjon to innebære innføring av ny teknologi som gjør det mulig å knytte hav og land tettere sammen. Flere aktører involveres i arbeid som tradisjonelt har vært utført separat enten på land eller sjø. Landapparatet vil i den forbindelse bli mer involvert i det operative arbeidet som skjer på plattformen (OLF, 2007b). Utviklingen innenfor IKT-området har gjort det teknisk mulig å overføre sanntidsinformasjon til land og å optimalisere og styre de fleste av operasjonene derifra. Løsninger for automatisk innsamling av data, identifisering av avvik og optimalisering av driften, vil bedre muligheten for fjerndrift (OLF 2005). Det er innføring av nye IKT verktøy som skaper muligheter for endringer av den eksisterende organiseringen. Som innebærer å flytte flere funksjoner til land og at flere aktører samarbeider over avstand. Samtidig fører disse endringene til at IO systemet blir tettere koplet og interaksjonen mer komplekse. Siden flere aktører involveres, og operatører på land kan gjøre valg som påvirker offshore plattformene.

Storulykker i petroleumsvirksomheten er oftest systemulykker som skjer i komplekse og tidvis tett koblede systemer (Sintef, 2008c). På grunn av kompleksiteten og koplingene kan storulykker sjeldent forklares med enkle årsaksforhold, ofte er det vekselvirkninger mellom menneskelige, teknologiske og organisatoriske faktorer som fører til ulykker (ibid). Både NA og HRO teknologi påpeker at tettere koplinger og mer komplekse interaksjoner utgjør en sikkerhetsrisiko i et system. Men som vi har sett mener HRO at organisasjoner blant annet gjennom en god sikkerhetskultur kan drifte slike systemer sikkert.

4.1.4 Avsluttende på ny teknologi og ulykker

Vi har sett at IO vil basere seg på eksisterende IKT, men omfattende omorganiseringer og nye arbeidsmåter endrer de teknologiske elementene slik at IO kan kalles ny teknologi. IO står derfor ovenfor samme sikkerhetsproblemer som innføring av all ny teknologi, altså en tilstand

med manglende informasjon som gjør det vanskelig å kartlegge sikkerhetsrisikoen og kontinuerlige endringer.

Manglende informasjon gjør designprosessen vanskelig, slik at sikkerhetsrisikoer kan bli oversett. Videre kan endringer som skjer i reinovasjonsfasen føre til ubalanse i de teknologiske elementene og føre til en ulykke. I tillegg til at trekk ved innføringen av ny teknologi kan føre til ulykker, har IO særtrekk som kan forsterke risikoen den nye teknologien innfører. IO er en teknologi som gir tettere koplinger og mer komplekse interaksjoner, som kan øke sannsynligheten for en systemulykke fordi informasjonen i systemet er vanskelig å forstå. Et tettere og mer komplekst system gjør det vanskelig for designerne å kartlegge systemet og vanskeligere å fange opp informasjonen i endringene. Avstanden som implementeres i generasjon to, vanskeliggjør arbeidet med å fange opp endringene og overføre informasjonen slik at den blir implementert i systemet som helhet.

Dette sammen med at systemet blir tettere koplet og mer komplekst (som følge av avstanden og introdusering av IKT systemer) er særtrekk ved IO, som sammen med trekk ved ny teknologi kan skape sikkerhetsmessige problemstillinger. På bakgrunn av denne kunnskapen vil oppgaven analysere hvordan manglende informasjon og avstand påvirker de fire temaene sikkerhetskultur, mentale modeller, målkonflikter og informasjonsbehandling.

Analysen vil vise hvordan avstanden kan påvirke at sikkerhetskulturene tar til seg teknologien ulikt, fordi subkulturene tolker den informasjonen i teknologien ulikt. At systemet er komplekst og preget av avstand og manglende informasjon, gjør det vanskelig for aktørene å ha komplette mentale modeller. Hvordan avstand og manglende kunnskap om teknologien gjør aktørene mer utsatt for målkonflikter. For så å avrunde med å se på hvilke informasjons og kommunikasjonsproblemer IO teknologien introduserer i generasjon to, som kan forsterke de sikkerhetsmessige utfordringene ny teknologi introduserer.

4.2 Sikkerhetskulturen i norsk petroleumsbransje

Sikkerhetskulturen vil være viktig for sikkerheten ved innføringen av IO, fordi sikkerhetskulturen påvirker hvordan man tenker sikkerhet, hvilke verdier og prioriteringer som tas i forhold til sikkerhet. Vi så i teorikapittelet at verdiene vil påvirke hvordan organisasjonen tar til seg den nye teknologien, og at et for stort sprik her vil føre til ulik praksis som kan representere en sikkerhetsrisiko. I dette kapittelet vil vi se på hvordan

dokumentene klassifiserer sikkerhetskulturen på norsk sokkel og hvor stor grad av differensiering man kan finne.

En dårlig sikkerhetskultur vil innføre sikkerhetsmessige problemstillinger i generasjon to. Når man innfører ny IO teknologi vil i følge Reason (1997) verdiene til organisasjonene være avgjørende for hvor mye sikkerhet blir prioritert. Og hvor mye midler som settes av for å kartlegge og planlegge utfordringer man kan møte ved implementeringen av IO. Dokumentstudien avdekket et heller manglende fokus på sikkerhetskulturens rolle ved implementeringen av IO i generasjon to. Utvalget av forskningsrapporter hadde ikke et fokus på at bransjen må bygge opp en felles sterk sikkerhetskultur som styrker beste praksis for sikkerhet. Det virker som lite forskning er gjort på sikkerhetskulturen på norsk sokkel, og betydningen av sikkerhetskulturen i generasjon to når enhetene er separert i tid og rom er ikke vurdert i noen av dokumentene som ble gjennomgått i arbeidet med denne oppgaven/rapporten. Derfor var det nødvendig å kartlegge den generelle sikkerhetskultur og grad av differensiering som har vært rådende på Norsk sokkel. Det er utført noen studier om kulturen på sokkelen, som viste stor variasjon i sikkerhetsfokuset, og stor grad av differensiering.

Fokus på sikkerhet er i dag en sentral del av norsk petroleumssektor, men sikkerheten har ikke alltid stått i høysetet. Ryggvik (2008) forteller om forholdene i Nordsjøen både på 70 og 80 tallet var preget av en fremmed arbeidskultur hvor selskapene ikke tok sikkerhet på alvor. Haukelid (2004) forteller at den første tiden (fra 1966) var preget av litt ”ville” tilstander, dette var særlig innen oljeboring, som fikk kallenavnet Texas kultur. Man sto ovenfor selskaper med en fiendtlig holdning til alle typer kollektive krav fra de ansatte, hvor den enkelte som sa ifra risikerte trakassering eller å miste jobben. Samme kunne folk som nektet visse typer arbeid (Ryggvik, 2008).

Fra begynnelsen av 80 tallet fikk vi et systemskifte med fornorskning av kulturen, hvor internkontrollen innførte ”safety management ”systemer. Systemene besto av en rekke forskjellige tiltak, både menneskelige, organisatoriske og tekniske (Haukelid, 2004). Ryggvik (2008) skriver at det var ingen tilfeldighet at internkontroll først ble utviklet i oljevirksomheten. Den teknologiske utviklingen offshore på 1970 tallet gjorde det nesten umulig for myndighetene å følge opp med egnede reguleringer. Samtidig hadde oljevirksomheten en komplisert selskapsstruktur som skapte diffuse ansvarsforhold. Innføringen av internkontrollen førte til at Oljebransjen ble ”presset” til å ta til seg

sikkerhetstanken. Verdier om sikkerhet ble "påtvunget" fra utsiden, men gradvis tatt opp i bransjen til å i dag være en bransje som setter sikkerhet svært høyt. I følge Ryggvik (2008) var det en kulturendring som på en og samme tid både forandret adferd og progresjon i utviklingen og introduksjon av mer robust teknologi. De vesentlige bakenforliggende forhold var en grunnleggende endring av styrkeforholdet mellom partene i arbeidslivet. Selskapene sto både ovenfor et langt sterkere tillitsapparat og et mer selvbevisst handlekraftig oljedirektorat. Samtidig gav Kiellandulykken[14] en moralsk autoritet til alle som ønsket å ta et krafttak for sikkerhet.

4.2.1 Sikkerhetskulturen mot slutten av generasjon en

På midten av 90 tallet hadde man en rimelig god sikkerhetskultur i hele bransjen. I tillegg til systemene ble sikkerhet en del av vanlig arbeidspraksis. Så fikk oljeprisen et kraftig fall i 1998, med påfølgende innstramminger, omorganiseringer og nedbemanninger, og i dag mener flere at vi er kommet inn i en ny periode (Haukelid, 2004). Han sier videre at det har de siste par årene vært en hard og bitter strid mellom partene om sikkerheten, og oljedirektoratet iverksatte derfor et eget prosjekt for å overvåke risikoen. Konklusjonen fra dette prosjektet er at på de fleste hms områder har vi fått en stagnasjon eller en forverring. Haukelid (ibid) har gjennom ulike intervjuer støttet seg til oljedirektoratets konklusjon. Dette fordi det eksisterer konflikter i form av enighet om hvilke konkrete tiltak som er viktige når man skal skape en god sikkerhetskultur. Haukelid (ibid) sier videre at generelt synes tilliten mellom partene å være på et lavmål. Hvis målet er å skape en felles sikkerhetskultur er det nødvendig med mer samarbeid forståelse og tillit. Haukelid (ibid) viser til en økning i antall olje og gasslekkasjer og kollisjoner og frekvensen av alvorlige personskader, og han ser på dette som en indikasjon på at det ved slutten av 90 tallet rådet en dårlig sikkerhetskultur.

Ptil (2008) viser at i 2008 hadde flere hendelser med storulykkespotensial i norsk petroleumsvirksomhet – som lekkasjen på Statfjord A i mai og hendelsen med krakkeren på Mongstad-raffineriet i august. I begge tilfeller kunne læring etter tidligere hendelser forhindret det som skjedde (ibid). Dette kan tyde på at det er en dårlig trend i norsk offshore næring hvor andre verdier enn sikkerhet er i høysetet.

Man ser av dette at fokuset på sikkerhet kan svinge, at sikkerhetskulturen kan lide under lave oljepriser og lite tillit mellom de ulike partene. Dette er forhold som kan ha endret seg til det

[14] Alexander L. Kielland var en boligplattform, som var stasjonert på Ekofisk-feltet i Nordsjøen. Plattformen kantret 27. mars 1980, da ett av dens fem ben ble revet av i høy sjø. 123 mennesker omkom, 89 ble reddet (www.snl.no)

bedre mot generasjon to, men hovedpoenget er at fokuset på sikkerhet vil være under stadig press fordi aktørene kan ha skiftende og ulike verdier.

Ved implementeringen av IO er det viktig at bransjen blir enig om felles verdier, som understøtter en sikkerhetskultur. Fordi sikkerhetskulturen påvirker både fase en og to av IO implementeringen er det avgjørende at bransjen er enig om sikkerhetsfokuset uavhengig av svingninger i markedet. På grunn av sikkerhetskulturens rolle i å forme sikkerhetstankegangen bør det frem mot generasjon to settes inn midler til å kartlegge og vurdere felles verdier, holdninger, atferd osv som bransjen kan dele. Tilliten må opparbeides, slik at de ulike partene føler at aktørene som besitter beslutningsmakt tar valg og handler til det beste på vegne av alle partene som er involvert i IO. Utfordringen med IO vil nok være å finne de best egnede representantene til å forhandle frem forhold som alle partene i IO kan enes om. Dette fordi IO i generasjon to vil ha mange atskilte parter som er involvert i driftingen av installasjonene. Hvordan skal man klare å ivareta alle partenes interesser på best mulig vis? Fase en av IO implementeringen vil kun bli vellykket dersom alle partene samarbeider om å frembringe informasjon som kan avdekke og kartlegge risiko. I fase to må det være i alles interesse å avdekke lokale endringer som kan ha konsekvenser for resten av systemet. Verdier som bygger opp under rapportering og deling av sikkerhetskritisk informasjon må dyrkes frem og deles av alle organisasjonene. Dersom dette ikke skjer kan man risikere en sikkerhetsrisiko i form av at de ulike aktørene prioriterer sikkerhet ulik, fordi kulturen er veldig differensiert.

4.2.2 Differensiert kultur

En differensiert kultur betyr at man kan finne kulturelle variasjoner, eller subkulturer innenfor en kulturell overbygning. Dersom subkulturene blir for markante og delte i meningene i IO systemet kan dette representere en sikkerhetsrisiko, fordi det påvirker hvordan organisasjonene tar til seg teknologien gjennom at det er ulik praksis og fokus i organisasjonene. Den kulturelle overbygningen kan være at organisasjonene i IO systemet har verdier som fokuserer på at sikkerhet må være i fokus, men at man får subkulturer som har ulike tolkninger på hva som er sikkert arbeid. Som vi tidligere har sett er det delte meninger om hvilke tiltak man bør iverksette for å skape en god sikkerhetskultur.

Ulike sikkerhetskulturer innenfor en kultur forekommer fordi ulike grupper vil ha ulike verdier som påvirker deres syn på hvilke tiltak som kan skape en god sikkerhetskultur. Verdiene påvirkes som Turner (1997) viste av ulik skolebakgrunn, historisk tilknytning og

posisjon i organisasjonen osv. Mange forskjellige begreper og faglige ståsteder benyttes for IO, noe som kan lede til kommunikasjonsproblemer, misforståelser og dårligere HMS (Sintef 2005). Stortingsmelding 38 viser at med IO er "en av de store utfordringene er å få til utstrakt samarbeid mellom aktørene" (2003-2004: 36). Ulikhetene som preger fortolkningsrammene til aktørene kan medføre problemer med å samkjøre de ulike aktørene som er atskilt i tid og rom. Problemet med at kulturen blir for differensiert er at de ulike enhetene kan ta til seg teknologien ulikt. Derfor må man jobbe med å skape felles verdier som underbygger en sikkerhetskultur alle partene kan identifisere seg med.

4.2.2.1 Ulike kulturer på norsk sokkel

En differensiert kultur har variasjoner i hvordan individer fortolker verdier og sikkerhet, som er påvirket av individenes historiske bakgrunn (Richter og Koch, 2004). At det i dag eksisterer ulike kulturer på norsk sokkel er det liten tvil om. Haukelid (2004) presiserer at det eksisterer flere forskjellige virkelighetsforståelser eller kulturer i næringen. Det fremkommer av Dordi Høivik (2009) studie at det er ulikheter i kulturen mellom offshore og onshore. Dordi foretok en undersøkelse av offshore vs onshore forholdene slik de fremstår i generasjon 0 og 1. Hvor hun fant ulikheter mellom offshore og onshore ansatte oppfatninger av arbeidsmiljøet i et norsk olje og gass selskap. Videre hadde de ulike holdninger til den nærmeste leder og så ulikt på mulighetene til å finne elektronisk informasjon. Offshore ansatte var generelt sett mindre fornøyde med alle organisatoriske og arbeids miljø faktorer. Dordi henviser også til en studie fra UK som viser at offshore installasjonsledere rapporterte om problemer med å motivere og kontrollere viktige sikkerhetsaspekter og arbeidskraftens oppførsel, selv om de var klar over viktigheten av slikt lederskap. Oppfatningen om den nærmeste leder varierte stort mellom offshore og onshore ansatte i utvalg fra 2003,2004, og 2005 (Høivik, 2009).

Det er ikke bare onshore offshore som kan ha ulike verdier. En og samme organisasjon utvikler subkulturer i større eller mindre grad. Eksempel på at en organisasjon har subkulturer kan man lese ut av Nævestad og Olsens (2006) studie av kollegaprogrammet i Statoil. Kollegaprogrammet var et kulturprogram som tok høyde for å forbedre sikkerhetskulturen i Statoil over en fastsatt periode. Etter endt periode ble implementeringen evaluert, og det viste seg at ulike avdelingen hadde ulik suksess med programmet. Ulikhetene kan være et resultat av at subkulturer tok til seg verdiene i kulturprogrammet ulikt, alternativt kan det være et resultat av at ulike ledere er flinkere til å videreformidle verdiene i programmet. Uavhengig av hva som førte til ulik implementering ble resultatet at kollegaprogrammet var mer

vellykket på noen avdelinger/plattformer og tyder på ulikheter mellom avdelingene. Studien kan peke på at subkulturene er mer avanserte enn bare onshore vs offshore kultur, det kan også eksistere ulik kultur på de ulike plattformene.

Resultatene av implementeringen av kollegaprogrammet og Dordis studier kan kaste lys over Preben og Olsens utsagn, at kulturelle og sosiale ulikheter kan påvirke risikopersepsjonen og gjør det vanskelig å kommuniserer og forstå risiko og farer likt. Det er sannsynlig at kulturelle ulikheter internt i Statoil førte til ulik implementering, og det er sannsynlig at kulturelle ulikheter mellom aktørene vil eksistere også i generasjon to. Det eksisterer i dag lite forskning om hvordan ulikhetene mellom organisasjoner og interne sub kulturer kan påvirke sikkerheten i forhold til IO. Men det er viktig å reflektere over spørsmålet om de ulike subkulturene tar til seg teknologien ulikt i generasjon to, fordi de har ulik bakgrunn som gjør at de har ulike verdier som ikke blir samkjørte på grunn av avstanden.

Tveiten et al. (2008) sier to kulturer møtes offshore: De gamle ”med hår på brøstet”, med praktisk bakgrunn og lang fartstid i bransjen og ”teoretikerne”, de nye med skolebakgrunn. Motstand mot forandring, også når det gjelder integrerte operasjoner, er størst hos de som har vært der lengst. Men nå står man ovenfor et generasjonsskifte offshore, der de nye vil tilegne seg den moderne teknologien mye raskere. Her sier han at implementeringen av IO kan gå mer smertefritt, men dette sier lite om hvordan samarbeidet vil fungere mellom de ulike aktørene ved fjerndrift i generasjon to. Turner påpeker at det å ta rasjonelle veloverveide valg ulikt fordelt mellom partene, slik at partene kan ta ulike valg i samme situasjon. Ulik skolebakgrunn vil fortsatt fremme ulikheter, og den nye teknologien vil neppe overkomme problemene som ligger i den fysiske konteksten, språk osv (Olsen og Olsen, 2000). Fordi det i IO systemet vil eksistere så mange parter med ulik bakgrunn og fortolkningsramme som besitter ulik informasjon kan IO teknologien bidra til å forsterke at risiko kan endre seg i reinovasjonsfasen gjennom tilpasninger (Olsen og Lindøe, 2008a). Dette betyr at IO kan ha problemer med at partene tar til seg teknologien ulikt på grunn av ulike verdier. Og at reinovasjonsfasen i seg selv kan representere en sikkerhetsrisiko fordi risikoen vil kontinuerlig endre seg hos de ulike partene. Noe som gjør det vanskelig å holde oversikten over de ulike praksisene og samkjøre disse. En samkjøring er nødvendig for at de teknologiske elementene skal være i overensstemmelse.

4.2.2.2 Tillit mellom partene

En god sikkerhetskultur må som vi tidligere vist ha en stor grad av tillit mellom partene (Dejoy, 2005). Ulike aktører deriblant fagforeningene har uttrykket sin skepsis ovenfor å flytte kompetanse til land og jobbe på fjerndriftede plattformer (www.aftenbladet.no). Dersom fremtiden også preges av svekket tillit mellom ulike parter i petroleumsbransjen kan man forsterke subkulturene og skepsisen som eksisterer i bransjen. Fagforeningene ønsker minst mulig fjernstyring av virksomhet på sokkelen, og frykter nedbemanning av innretninger i havet (Ptil, 2008). I dag er det en bekymring for fjernstyring som gjør at tilliten mellom partene er redusert. Høyland (2007) sin informant kalte fjernstyring big brother i praksis, med kamra skjermer og mikrofoner over alt. Et kamera på hjelmen og en stemme i øret som forteller hva ansatte skal gjøre og hvor de skal gå. Industriens holdninger til egne ansatte, respekt for integritet og det å bryte slike grenser ser ut til å være ganske lav. Høyland (2007) avdekket at også fagforeningen var positive til fjernstøtte men negative til fjernstyring av bemannede plattformer. Fjernstyring av bemannet plattform vil føre til en utrygghet blant de offshoreansatte. De sammenligner det med å være passasjer på ett fly uten pilot som styres fra India. Tilliten til IO systemet som innføres i generasjon 2 er heller lav, fordi ledelsen mangler tillit fra sine ansatte med at de handler til det beste for sine ansatte, og ikke for å maksimere profitt.

OLF (2007 a)har sett på tillitsforholdet i bransjen, og kommet med noen forslag om hvordan tilliten mellom land og offshore kan forbedres. De som jobber på land har ulike roller og ulik forståelse av jobbhverdagen enn de som jobber offshore, derfor foreslår OLF rotasjon og besøk offshore eller på land for heving av kompetanse, og man må sørge for klare avtaler og roller mellom land og hav. Slik at de offshore og vice versa får en forståelse for arbeidshverdagen til de aktørene man skal samarbeide med. En slik kompetanseheving vil bygge opp de mentale modellene slik at de kan skape en forståelse og respekt for egne handlinger i forhold til aktører som er atskilt i tid og rom. En effekt av dette kan være økt tillit mellom partene, fordi man får forståelse for hverandres roller

Det vi ser her er at bransjen men også organisasjonene preges av ulike verdier, som gjør at det eksisterer subkulturer, og at svekket tillit mellom partene er med på å øke avstanden mellom gruppene. Subkulturer kan være en trussel for sikkerheten, fordi man risikerer at det kan vokse frem lokal praksis som er i konflikt med de andre teknologiske elementene, eller som kan skape en ulykke som følge av målkonflikter. Subkulturene kan ta til seg teknologien ulikt, noe som vil kompliserer samkjøringen av aktørene som er involvert i IO. Og som OLF

(2007a) påpeker, er det store variasjoner i folks forståelse av IO. Når enhetene er atskilt i tid og rom, kan man anta at de utvikler mer distinkte subkulturer enn dersom de var lokalisert på samme plattform

Ulik grad av subkulturer er ikke mulig å unngå, fordi det er mange faktorer som påvirker forståelsesrammen og verdiene til de ulike aktørene. Ulike verdier kan være hjelpsomt når de kartlegger fareområdene i fase en, da man har mange ulike grupper med ulike verdier og erfaring, som kan se utfordringene til IO i ulikt lys. Men man må ta alle partenes bidrag like seriøst, dersom man klarer dette kan man kartlegge flere farer i forhold til IO. Hovedutfordringene i forhold til subkulturenes ulike virkelighetsforståelse og verdier vil ligge i fase to. Fordi man kan oppleve mange ulike meninger og tolkninger om en og samme endring, som kan skape et hav av informasjon hvor det kan være vanskelig å luke ut hvilken informasjon er relevant eller ikke. Endringer som noen ser som betydningsfulle vil andre overse, derfor er det viktig med en generativ kultur som preges av tilliten mellom subkulturene. Da det vil være viktig å stole på gruppenes/individenes bekymringer, selv om for eksempel operatøren ikke ser den store faren, og ta informasjonen på alvor og følge opp slik at man kan avdekke eventuelle problemer.

4.2.3 Viktig med en generativ sikkerhetskultur

Rapportene hadde lite fokus på at man må skape en kultur som fremmer informasjonsbehandling i IO systemet. Men rapportene hadde fokus på informasjons og kommunikasjonsproblematikk når de vurderte risiko (se kapittel som behandler informasjon og kommunikasjon). Dette kan tyde på at også rapportene støtter viktigheten av å ha en generisk kultur, bare de ikke benytter begrepet generisk kultur eller ser på kulturens rolle til å fremme eller hemme informasjonsbehandlingen. På grunn av manglende fokus på kultur i rapportene, vil kapittelet basere seg på generelle trekk ved IO/norsk sokkel sett i forhold til Westrums teori.

En god sikkerhetskultur er avgjørende for hvordan organisasjonen behandler sikkerhetskritisk informasjon i fase en og to. Av Sintef (2008 b) undersøkelser framgår det at operatørselskapene er mer positive til IO prosessen enn entreprenørene. Entreprenørene er blant annet misfornøyd med informasjon og tilgang på data. Om manglende informasjon kan skyldes forhold rundt kontrakter, eller IT-sikkerhet er ikke relevant, da man frem mot generasjon to er avhengig av en generativ informasjonsdeling mellom enhetene. Når enhetene befinner seg separert i tid og rom vil det representere en stor utfordring å fange opp

informasjonen noen har ignorert. Dersom en patologisk kultur vokser frem vil man forsterke sårbare elementer i IO, ved at endringene i reinovasjonsprosessen ikke fanges opp og skaper ubalanse i de teknologiske elementene.

Når man har kartlagt farene IO kan introdusere, har Westrum vist at det vil være viktig å jobbe aktivt mot å dyrke en generativ kultur som fanger opp endringene i reinovasjonsprosessen for å sikre at informasjonen flyter og verdsettes i IO systemet. En sikkerhetskultur som fokuserer på sikkerhet og som er generativ (leter aktivt etter informasjon) er viktig for å unngå ulykker i IO systemet. Selv om ingen av dokumentene har vektlagt viktigheten av å bygge opp en generisk kultur som fremmer bruk og deling av informasjon, vedkjenner dokumentene viktigheten av å dele og benytte seg av informasjonen i systemet.

Turner poengterer sikkerhetskulturens rolle i å forme blindhet ovenfor feil, en kollektiv blindhet hvor gruppetenkning og konsensussøking gjør at gruppene jobber mot å forebygge de feilene som ble kartlagt i fase en. Slik at nye og ukjente farer som vokser frem i reinovasjonsfasen blir avvist fordi de ikke passer inn i kategoriene som ble laget i fase en. Har kulturen også patologiske trekk, vil ikke ansatte melde fra om potensielt farlige situasjoner, fordi de frykter konsekvensene da budbringere ved tidligere anledninger har fått dårlig behandling, fordi slike beskjeder er upopulære hos ledelsen. Det at kultur kan medføre kollektiv blindhet, sammen med en patologisk kultur kan representere en sikkerhetsmessig risiko når man i generasjon to involverer aktører som er separert i tid og rom. Fordi sikkerhetsmessige problemer vil for det første ikke bli oppdaget så lett, på grunn av den kollektive blindheten, men de få personene som ser at problemet er en fare, vil ikke melde ifra om dette fordi det kan få negative følger.

Dersom en av aktørene i IO systemet har en patologisk kultur, eller dersom en slik kultur over tid vokser frem i noen av organisasjonene vil dette forplante seg til de andre organisasjonene i form av at fellesskapet vil mangle informasjon. Ikke all informasjon kan fanges opp av operatørene som sitter på land fordi de er underlagt begrenset rasjonalitet, og klarer man ikke i fellesskap å fange opp informasjonen den patologiske kulturen undergraver, kan det innebære en stor risiko.

4.2.3.1 Ledelsens rolle til å skape en integrert generativ kultur

Som vi har sett er en ledelse som fokuserer på sikkerhet viktig for å dyrke frem en generativ kultur. En ledelse som oppfordrer ansatte til å si ifra om endringer og ikke straffer slike meldinger, som sørger for at ansatte får tilbakemelding når de har meldt fra om en potensiell fare og som til slutt sørger for at endringene blir implementert er viktig for å oppnå en generativ kultur. Ledelsen i de ulike organisasjonene i IO systemet må samarbeide om å definere verdier som setter sikkerhet høyt og fremmer generering og spredning av informasjon. Dersom ledelsen jobber med alle disse områdene, kan en god sikkerhetskultur preget av tillitt mellom partene vokser frem.

Det vi har sett her er at fokuset til IO bør være å unngå for stort gap mellom subkulturene og sørge for at man får en så integrert generativ kultur som mulig. Målet bør være å sørge for å skape verdier som fokuserer på sikkerhet og gjør at enhetene drar i samme retning, slik at man oppnår maks utbytte av å jobbe sammen. Patologiske kulturer der man forsøker å kamuflere for operatørene feil som er begått på plattformer og liknende, vil utgjøre en stor sikkerhetsrisiko i IO. Fordi systemet er avhengig av at de ulike aktørene samarbeider om å kartlegge og benytte seg av informasjonen endringene skaper. Selv om det i dag mangler forskning på sikkerhetskulturen betydning for sikkerheten i forhold til IO, betyr det ikke at dette er et område som bør ignoreres.

4.2.4 Avsluttende på kultur

Vi har sett at sikkerhetskulturen er viktig ved implementeringen av IO fordi sikkerhetskulturen påviker verdier og prioriteringer som tas i forhold til sikkerhet. Ulike teorier poengterer viktigheten av sikkerhetskulturen for å ha sikre systemer, og unngå ulykker som BP ulykken. Sikkerhetskultur er en av grunnsteinene i HRO tankegangen for å kunne drifte avansert teknologi slik som olje og gassutvinning sikkert. En dårlig sikkerhetskultur vil innføre økt risiko for ulykker i generasjon to. Sikkerhetskulturen kan påvirkes av oljepriser og tillit mellom partene.

Studien avdekket i kapittel tre at IO bør fokusere på å bygge en integrert kultur som prioriterer sikkerhet, for å bedre fange opp sikkerhetsrisikoer den nye teknologien innfører. Ved innføringen av IO i generasjon to bør det derfor brukes midler til å kartlegge verdier som understøtter en sikkerhetsverdier som partene enes om. Gjennomføres dette sikres en grad av integrering i kulturen, og man unngår for stort sprik i sikkerhetsarbeidet mellom partene, og at partene tar til seg teknologien ulikt. For stort sprik i fortolkningsrammene kan medføre

problemer med å samkjøre de ulike aktørene som er atskilt i tid og rom, og som vi har sett eksisterer det i dag flere forskjellige virkelighetsforståelser og kulturer i næringen: mellom organisasjonene, offshore vs onshore, i en og samme organisasjon og mellom unge og gamle offshore.

Manglende tillit mellom partene kan føre til økt grad av differensiering, som vil være en trussel for sikkerheten. Tillit er viktig for av to grunner. Først ved at gruppen som avdekker en sikkerhetsrisiko skal dele informasjonen, deretter ved at mottakeren tror på rapporteringen selv om de ikke ser faren.

Ved implementeringen er det viktig å unngå en patologisk kultur som hindrer de ansatte fra å melde fra om endringer, og har en gruppementalitet som skaper blindhet ovenfor feil. En patologisk kultur vil være en sikkerhetsrisiko ved implementeringen av IO, fordi organisasjonen ikke vil kunne fange opp informasjonen i den nye teknologien tilfredsstillende. En for stor grad av differensiering vil også skape en sikkerhetsrisiko fordi de ulike subkulturene kan ta til seg teknologien ulikt, og skape en ubalanse mellom de teknologiske elementene.

Målet til IO bør derfor være å ha en ledelse som kultivere en generativ kultur gjennom tydelige verdier, som fokuserer på sikkerhet. Der informasjon fanges opp og blir tilgjengelig for alle partene i systemet, for å unngå hull i kunnskapen som kan føre til usikre handlinger. Sterke verdier vil sammen med oppdatert informasjon kan bidra til en mer integrert kultur, hvor organisasjonene tar til seg teknologien ”likt”.

4.3 Mentale modeller

I teorikapittelet fikk vi innsikt i hva mentale modeller var, og deres viktige rolle for sikkerheten. I dette kapittelet skal vi se hva dokumentene sier om viktigheten av mentale modeller i generasjon to. Vi har sett at mentale modeller blir viktig ved innføringen av ny teknologi, fordi modellene er viktige for å forstå informasjonen et komplekst system gir slik at man kan unngå målkonflikter og systemulykker. Manglende mentale modeller vil gi en økt risiko for ulykker fordi designerne ikke klarer å kartlegge sikkerhetsrisikoen i systemet, eller de designer inn ny risiko i systemet fordi de har en manglende forståelse for sikkerhetsinformasjon og klarer ikke å se sammenhengene. Men også fordi ansatte har en manglende forståelse for den daglige driften og derfor utfører handlinger som er farlige, eller

den manglende forståelsen gjør at de feiler å fange opp endringene som skjer når teknologien tilpasser seg den nye konteksten.

Ved innføringen av fjerndrift i generasjon to er mentale modeller viktig, for at enhetene som er separert i tid og rom skal se sammenhengene i systemet uavhengig om de befinner seg langt borte fra produksjonsområdene. *Beslutningstaking på land er annerledes fordi man ikke "er i samme båt" som de offshore. Felles situasjonsforståelse er derfor viktig i beslutningsprosesser som involverer ulike miljøer og lokasjoner* (Sintef, 2008 a: 38). Denis Besnard (Sintef, 2010) påpeker at når den fysiske kontakten med produksjonsprosessen blir borte ved innføringen av IO, vil de mentale modellene være avgjørende. Men at det er en utfordring er å forsikre seg om at alle som samarbeider i IO har samme situasjonsforståelse og at løsninger diskuteres ut fra dette (Johnsen og Lundteigen, 2008). Her ser vi at IO systemet er komplekst og sammen med avstand gjør det vanskelig for partene å ha gode mentale modeller.

Når man i fase en skal designe IO systemet vil det kreve en omfattende kartlegging for å få oversikt over systemet og dets svakheter. Et arbeid som vil være vanskelig fordi IO innebærer økt samhandling og samspill koordinert på tvers av geografi og organisasjoner. Behov for felles situasjonsforståelse og mentale modeller i forbindelse med IO setter nye krav til utforming av organisasjon, rutiner, ansvarsdeling, opplæring, rekruttering og utforming av IKT løsninger (Sintef, 2005). IKT er i seg selv komplekst fordi det består av programmerte systemer med funksjonalitet som ikke alltid er like tydelige for brukere av systemene. I det flere IKT systemer settes sammen i et distribuert nettverk, øker kompleksiteten ytterligere. Det resulterende nettverket av noder og kommunikasjonslinker legger ikke til rette for en enkel oversikt over hva som foregår av prosesser og hvordan eksempelvis uforutsette hendelser håndteres (Sintef, 2005). Man ser ut av dette at designerne må få oversikt over enhetene og koblingene i IO systemet, noe som er en kompleks oppgave. Dette arbeidet krever informasjon, noe vi har sett er en mangelvare i en designprosess, og da særlig når teknologen er ny. Men en fordel kan være at så mange ulike enheter er involvert i IO at man får mennesker med ulike verdier og bakgrunn som kan komme med innspill til worst case scenarioer og fremme sikkerhetsfantasien (Pidgeon og Leary, 2000). Slik kan designere få bred informasjon som kan hjelpe dem å bygge helhetlige mentale modeller, og designe et mer sikkert IO system. Faren kan som Leveson (2004) påpeker være at man til slutt har konstruert et så komplekst system, at det overgår menneskelig fatteevne

Når man har laget en oversikt over systemet og dets risikoer må designerne kartlegge hva man trenger for å best mulig ivareta aktørenes mentale modeller. I følge Leveson (2004) kunne mentale modeller konstrueres gjennom å bygge inn trening eller ha fysiske modeller av systemet tilgjengelig for aktørene. Visuelle IKT løsninger gjør det enklere å synkronisere situasjonsforståelsen hos de ulike aktørene. En kranfører kan ha en oppfatning av en situasjon og en borearbeider har en annen. Dersom disse to gruppene har sett de samme bildene er det større sannsynlighet for at situasjonsforståelsen deres er synkronisert (Tveiten et al., 2008). Det positive her er at selve verktøyene i IO teknologien kan være med på å gi informasjon og konstruere de mentale modellene.

IO gir aktørene en mulighet for å etablere bedre drift via felles forståelse med nye mentale modeller. Sintef (2005) viser til at etablering av (matematiske) modeller og datainnsamling via sensorer kan brukes til å forstå reservoarer bedre. Sanntidsdataene kan være et godt utgangspunkt for å etablere felles forståelse i en prosjektgruppe som skal forsøke å forstå hva som foregår nede i et reservoar. Ekspertene kan raskere forstå problemet – kanskje allerede fra dag en, og kan løse problemer som ellers ikke kunne ha blitt løst eller som har blitt løst etter 1 uke til 1 måned. Men designerne må sørge for å designe systemene slik at aktørene kan skape felles mentale modeller. For å gjøre dette må designerne ha økt vekt på grensesnitt og visuelle presentasjoner som skaper felles forståelse i en sammensatt gruppe av aktører som er separert i tid og rom (ibid).

Det vil derfor være viktig at designerne jobber aktivt for å presentere informasjonen til aktørene på en enkel og forståelig måte. Johnsen og Lundteigen (2008) sier at man må sikre at nye IKT verktøy og nye arbeidsprosesser gir felles situasjonsforståelse og nødvendig samhandling under normal drift og avvikssituasjoner. Kommunikasjon via IKT verktøy, i stedet for direkte kommunikasjon mellom mennesker vil kunne påvirke hvordan de ulike aktørene opplever en driftssituasjon. Når viktige beslutningstakere eller fagekspertise ikke er nært driftssituasjonen eller ikke er godt nok trent for å forstå den nye samarbeidsformen vil sannsynligheten for dårlig situasjonsforståelse og gale beslutninger og prioriteringer kunne øke, dette gjelder ikke bare i tidskritiske situasjoner (johnsen og Lundteigen, 2008). Trening er en viktig faktor for at aktørene skal kunne inneha gode mentale modeller (Leveson, 2004). Derfor må organisasjonene i generasjon to prioritere omfattende treningsprogrammer, som skal bidra til at aktørene har mentale modeller og god situasjonsforståelse selv om de arbeider over avstand. de ansatte trenes for å bygge opp situasjonsforståelsen og de mentale modellene,

dersom dette ikke gjøres er det dessverre slik at felles "dårlige" mentale modeller kan lede til feilhandlinger og systemulykker.

4.3.1 Automatisering

IO fører med seg økt instrumentering og automatisering som et strategisk mål som muliggjøres av IKT infrastruktur. Problemet med automatiseringer er som Leveson (2004) viste at de bidrar til at systemer kan overgå menneskelig fatteevne. Fordi store deler av prosessen ikke er synlig, blir det vanskelig for de involverte aktørene å forstå hva som skjer/har skjedd, de ser bare hva som går inn i systemet og hva som kommer ut.

IKT er en form for organisasjonsteknologi som kan sørge for relevant informasjon og kunnskap er tilgjengelig i enhver kritisk situasjon. For å ikke drukne i informasjon vil automatisk filtrering av data og automatisering av prosesser sørge for at en begrenset mengde informasjon blir presentert for operatørene av systemene (Nystøl, 2008). Mekaniske styringer og komponenter blir elektroniske og programmerte (automatiserte) og det har vist seg at systemene ikke alltid er like vanntette, og har medført til feilfunksjoner i situasjoner som en ikke har tatt høyde for når man designet systemet (Sintef, 2005). Dette samsvarer med det vi har sett, at designfeil kan føre til hendelser, fordi designerne har designet et system som overgår menneskelig fatteevne og de mentale modellene klarer ikke å forstå kompleksiteten i systemet.

Det er ikke nok å bare ha tilgang til informasjon, de må også være i stand til tolke den på riktig måte og forstå implikasjonene, derfor blir nødvendig forestillingsevne helt essensielt. (Grøtan, 2008). Sintef (2005) viser at en høyere automatiseringsgrad gjør at aktørene må forholde seg til prosesser og systemer på en annen måte enn før – ved at systemene tar mer av den løpende oppfølgingen mens kontrollromspersonell må håndtere avvik og det uventede, noe som medfører nye krav til kompetanse og forståelse av produksjonsprosessene. Mentale modeller blir nødvendig dersom man ønsker at operatørene skal klare å fange oppinformasjonen i endringene i fase to. Men det blir vanskelig å fange opp informasjon som prosessene gir, for som Denis Besnard (Sintef, 2010) påpeker vil automatisering gjør det vanskelig for operatørene å følge prosessene når de ikke er synlige lengre. Derfor vil han at man i forbindelse med IO må spørre hvor transparent systemet er, for ønsker man at operatørene skal ha mentale modeller som fanger opp endringer i prosessene, må de være i stand til å forstå og kontrollere prosessene til enhver tid (Leveson, 2004).

Økt automatisering er både en del av pågående utvikling i IO og er sett på som en kritisk faktor for å muliggjøre for eksempel styring fra land. Menneskets forutsetninger for situasjonsforståelse blir derfor utfordret på to måter: 1) det daglige arbeidet vil for en del bære mer preg av monitorering og mindre intervensjon, med påfølgende større krav til operatøren ved avvikssituasjoner. 2) mer komplekse informasjonsgrensesnitt øker de mentale kravene i arbeidet og gir større krav til ekspertise hos operatørene (Sintef, 2008c). Resultatet kan bli kritiske systemer vurderes og styres av mennesker som har liten erfaring med de mer rutinemessige tilpasningene, men som likevel forventes å gjenvinne kontrollen og redde situasjonen når noe ekstraordinært inntreffer (Grøtan, 2008). Også Sintef (2008a) påpeker at automatiseringen vil skape nye utfordringer for operatørene i skarpe enden som pasifiseres i det daglige, men som samtidig vil bli utsatt for forventninger om effektiv intervensjon i unntakssituasjoner. Med andre ord vil IO teknologien innføre økt automatisering som vanskeliggjør det å ha gode mentale bilder av systemet, fordi systemet har så mye informasjon, og deler av den er heller ikke synlig.

Dokumentanalysen avdekket et syn på automatiseringen i IO i tråd med Levesons, at økt automatisering fører til nye og større utfortinger i forhold til situasjonsforståelse og mulighet til å handle korrekt i avvik situasjoner. At det i IO systemet vil være en utfordring for de ansatte å ha mentale modeller som de klarer og benytte seg av i pressede situasjoner, for systemet er så komplekst at det er vanskelig for aktørene å forstå informasjonen de har tilgjengelig. Informasjonen i endringene vil være vanskelig å oppdage da store deler av IO er automatisert slik at systemet ikke er transparent og/ eller fordi det er for mye informasjon fordi systemet er stort og komplekst. Aktørenes mentale modeller vil gjøre dem bedre rustet til å tolke den ”skjulte” informasjonen i systemet. Derfor må designerne arbeide for å bygge inn trening og gode fysiske modeller i systemet for å sikre så gode mentale modeller som mulig.

4.3.2 Fange opp endringene og oppdatere de mentale modellene

Som Leveson (2004) har vist må de mentale modellene til enhver tid være oppdaterte. Derfor må endringene i reinovasjonsprosessen fanges opp og implementeres i systemet. Når den nye teknologien tilpasser seg vil endringene føre til at de eksisterende mentale modellene blir utdaterte, slik at man må fange opp endringene og korrigere de mentale modellene. Skal man sørge for at aktørene har korrekte mentale modeller i IO er det i følge Tveiten et. al (2008)

viktig at petroleumsindustrien legger til rette for trening med bruk av ny teknologi i beredskapssituasjoner, slik eksempelvis luftfart, romfart og prosessindustri har erfaring med. Hjelpemidlene vi mennesker benytter oss av når vi skal løse oppgaver, er det slik at det tar tid og krever øvelse for at vi skal bli komfortable med at hjelpemiddelet er der. Når vi har blitt komfortable med hjelpemidlene vil vi nesten ikke merke at de er der. Det viste seg i Krevende og kritiske samhandlingssituasjoner gikk mange tilbake til gamle løsninger, enten fordi de ønsket å møte andre aktører ansikt til ansikt, eller fordi de ikke hadde tilstrekkelig tillitt til den nye samhandlingsteknologien (Ibid). Sintef (2008c) sier at aktøren må ha evne til å operere IO systemet og føle seg trygg på at han eller hun kan det. Trygghet og tillit til at man evner å utføre en oppgave er sterkt knyttet til erfaring og trening i å operere systemene. Det er en utfordring å holde kompetanse og trening på rett nivå dersom man får utfordringer, som normalt ikke er tatt høyde for i kartleggingen av systemet (Ibid).

Også Johnsen og Lundteigen (2008) påpeker viktigheten med å trene på felles situasjonsforståelse og avklaring av at riktige antakelser er gjort av alle involverte når man i IO har enheter som er atskilt i tid og rom. Når man har med separerte enheter er det viktig å sikre en felles forståelse av hverandres roller og ansvar og utvikle en felles kulturell forståelse: det vil si felles mål, holdninger og normer(Ibid). Det er viktig at aktørene har en kulturell forståelse (integrert kultur) for først da kan man sikre at de mentale modellene og situasjonsforståelsen er i overensstemmelse mellom enhetene for å unngå målkonflikter.

Som Leveson påpekte må operatørene være i stand til vite hva som er normal driftssituasjon, og må til enhver tid være i stand til å konstantere systemets status. De mentale modellene kan være utdaterte som følge av utfilfredsstillende kartlegging i fase en, manglende feedback i fase to og manglende trening. Manglende feedback i fase to er når informasjonsdelingen mellom avdelingene og nivåene er dårlig. Informasjonsdelingen mellom avdelingene og nivåene kan være dårlig selv om man i IO har en database med sanntidsinformasjon. Fordi det kan være viktig informasjon som arbeiderne besitter men ikke deles, fordi de ikke ønsker/tørr å dele den. Dersom kulturen er patologisk vil man få mange slike tilfeller, hvor ansatte frykter for konsekvensene av å dele informasjonen. Sikkerhetsledelsen må jobbe aktivt med å fange opp endringene selv informasjon som ikke deles i de formelle kanalene, og de bør ha fokus på å fange opp lokale endringer som kan påvirke systemet som helhet. For deretter å sørge for oppdatering av regler og prosedyrer, endret opplæring/trening for å sørge for relevante mentale modeller og sikre at de teknologiske elementene står i forhold til hverandre.

4.3.3 Fjernstyring og mentale modeller

IO vil i generasjon to innføre fjerndrift av bemannede offshore installasjoner, og da er det er viktig at aktørene som er atskilt (offshore/onshore) har lik situasjonsforståelse og mentale modeller. Men avstanden kan gjøre dette vanskelig, fordi samhandlingen blir mer globalisert i IO, det vil si at den får stadig sterkere karakter av geografisk kulturell og språklig avstand mellom samarbeidende aktører (Grøtan, 2008).

Sintef (2005) mener at økt fjerndrift kan minske tilgang til direkte persepsjon og taus kunnskap overførsel noe som kan lede til dårlig situasjonsforståelse og lede til feilhandlinger. Fjernstyring kan føre til svekket situasjonsforståelse ved at man er avhengig av indirekte informasjonskilder framfor bruk av egne sanser. De som styrer vil mangle rike informasjonskilder som lyder, lukt, samt muligheten til å snakke med folk ansikt til ansikt etc. Med kontrollrom på land og operatører offshore vil uformelle møteplasser mellom disse miljøene forsvinne. Det kan tenkes at slike møteplasser fungerer som en arena for å ta opp sikkerhetsmessige saker, i tillegg til at møteplassene bygger opp om samhold i organisasjonen eller andre forhold vi ikke har identifisert. Det kan derfor være risikofylt å gå fra slike rike kommunikasjonskanaler til fattige informasjonskilder i IO. En fare med avstanden i ”abstrakte teknologier” som IO kan være er at operatørene må lage seg en forenklet modell til erstatning for et fysisk forhold til systemet. IO bør vi ikke for eksempel oppleve at ”hver mann har sin modell”, når man faktisk opererer samme prosess, eller sammenkoplede prosesser. Dersom den teoretiske kunnskapen og opplæring ikke er god, kan en forenklet modell være en risiko, fordi den forenkler for mye (Ibid). Dette er et problem man kan se i forhold til

IO fordi teknologien er ny og endrer seg hurtig er at man mangler kunnskap om den, noe som kan resultere i en modell som er for enkel, og derfor representerer en risiko.

Det vi ser er at fjernstyringen IO introduserer i generasjon to vil skape en utfordring for å ha gode mentale modeller som deles av alle organisasjonene, fordi det er vanskelig å forstå forholdene når man ikke er tilstede og kan føle situasjonene på kroppen. Ulik sikkerhetskultur kan påvirke forståelsen slik at ulike aktører besitter ulike mentale modeller, til tross for at de har identiske fysiske modeller. Det vil også være problematisk å ha mentale modeller som ikke er for enkle, når teknologien er ny og endrer seg så hurtig befinner man seg i en situasjon med manglende informasjon, som gjør det vanskelig å konstruere helhetlige mentale modeller.

4.3.4 Store komplekse systemer

De mentale modellene må være oppdaterte, dersom man skal klare å fange opp endringene som skjer i fase to ved implementeringen av IO. Noe som kan problematisere sikkerhetsledelsens arbeid med å fange opp endringene, er at IO vil både være et stort (mange aktører) og et komplekst system (samhandlingen foregår over avstand). Turner (1997) har vist oss at en viktig årsak til ulykker er systemer som er store eller komplekse, hvor flere ansatte og organisasjoner har tilgang. Dette er fordi det blir så vanskelig å holde oversikten over hvem som gjør hva til hvilken tid. Sammenhengene mellom elementene blir så omfattende og komplekse at man har problemer med å bygge opp tilfredsstillende mentale modeller. Siden IO systemet er stort og omfattende vil det kreve at lederne jobber aktivt med de ulike aktørene som er involvert, for å sørge for at de holder tritt med hverandre.

Sintef (2008c) har identifisert at økt kompleksitet med henhold til hvem som har aktiviteter i driften og ulike geografiske avstander mellom medlemmene i teamet økte usikkerheten i forhold til om man har tilstrekkelig oversikt over risikobildet frem mot generasjon to. I forhold til offshorepersonell har man i IO en spesiell utfordring når det gjelder arbeidstidsordning (to uker på jobb og fire uker fri). Her kan man lett komme i en situasjon der nytt utstyr blir brukt såpass sjeldent at brukeren aldri rekker å bli fortrolig med det. Dermed er det avgjørende at utstyret er enkelt å bruke, at det har et godt tilpasset brukergrensesnitt og at det benyttes teknikker for å vedlikeholde kunnskap og erfaring i friperioder (Tveiten et al., 2008).

De sier videre at det er en utfordring å oppnå felles situasjonsforståelse når man er avhengig av overlevering mellom skift, og der det er avstand mellom systemer som skal forstås og de personene som skal forstå dem. Utfordringene øker også når flere medlemmer av en gruppe skal oppnå felles situasjonsforståelse (Ibid). Endringer i skiftordninger og arbeidstid hav/land kan skape uro i organisasjonen og potensielle hull i oppmerksomhet mot aktivitet og operasjon. Grenseflatene blir mange og utviklingen synes å gå i retning av flere, og mer kompliserte hand- over situasjoner. Hand -over situasjonen er en kritisk aktivitet med sterk innvirkning på situasjonsforståelse blant deltakerne i operasjonen. Mangelfull hand- over med feilaktig situasjonsforståelse som resultat har vært årsak til store ulykker (Sintef, 2008 c).

Vi ser her at IO systemet har mange parter som er involvert og derfor vil det være en utfordring å sørge for at aktørene i de ulike delene av systemet har mentale modeller som er i overensstemmelse. Særlig vanskelig blir det når man i offshore bransjen opererer med så

mange skiftordninger som etter endt arbeid, er borte over en lang periode. Skift ordningene gjør at det blir mange parter involvert, samtidig som ”follow the sun” vil gjøre det mer komplekst når flere operatørsentre også involveres. Når så mange parter har tilgang i IO kan man få problemer med å synkroniserer de mentale modellene de ulike skiftene har i forhold til hverandre.

4.3.5 Avsluttende på mentale modeller

Kapittel tre avdekket at målet for IO systemet bør være å sikre at alle de involverte aktørene besitter så gode og oppdaterte mentale modeller som mulig. Det for å minimere risikoen for målkonflikter som avstanden i IO systemet kan forsterke. I dette kapittelet har vi sett at det vil være utfordrende for operatørene å ha oversikt over all informasjon, særlig når skiftordninger gjør at mer enn en operatør er involvert. For i ”follow the sun” tanke gangen vil plattformene forholde seg til de operatørsentrene som er åpne i ulike land i verden. Dette krever en informasjonsoverføring mellom skiftene for å sørge for at de mentale modellene er oppdaterte. Overføringen kan skje enten i form av ”muntlig oppdateringer”, eller logger som den neste operatøren med enkelthet kan lese. Men som BP ulykken [15]har vist, kan operatørene avvike fra de satte prosedyrene slik at de ikke besitter den nødvendige informasjonen.

Informasjon/feedback er viktig for å sørge for at de mentale modellene er oppdaterte, slik at man klarer å fange opp endringene som skjer når teknologien tilpasser seg den nye konteksten. Det blir vanskelig ved implementering av ny teknologi, fordi den inneholder lite informasjon som kan benyttes til å konstruere mentale modeller. Men IO teknologien introduserer IT verktøy som muliggjør å ha oppdaterte visuelle modeller, som gir gode mentale modeller. Til tross for gode visuelle modeller, kan automatiseringen gjøre det vanskelig for aktørene å forstå prosessene når flere ledd ikke er synlige.

Videre vil avstanden mellom aktørene i IO bidra til at det blir vanskelig å ha korrekte mentale modeller, fordi det kan forekomme endringer i de ulike organisasjonene som ikke fanges opp av sikkerhetsledelsen og integreres i systemet. Dette vil føre til at de mentale modellene er feil, og aktørene innehar ulike modeller som ikke er i overensstemmelse med hverandre. Flere parter er involvert i IO systemet som preges av skiftordninger og komplekse hand – over situasjoner, noe som gjør det enda vanskeligere å ha korrekte og like mentale modeller. For dårlige mentale modeller eller for stort sprik mellom de mentale modellene kan resultere i at

[15] En rekke årsaksforhold førte til ulykken ved BP texas, hvor mangelfull informasjon ved overlapping mellom skift var en av årsakene.

de ulike aktørene gjør handlinger som er i konflikt med hverandre, og føre organisasjonen over til fase tre. Implementeringen av IO vil innføre en sikkerhetsrisiko i form av at det vil være vanskelig å bygge opp gode mentale modeller, når teknologien er ny og systemet er så komplekst og tett koplet.

Skal man ha en mulighet til å ha oppdaterte mentale modeller ved implementering av ny IO teknologi, må organisasjonene sørge for å ha en generativ kultur og en sikkerhetsledelse som jobber kontinuerlig med å fange opp informasjonen i systemet. Gjøres dette kan informasjonen internaliseres i aktørenes mentale modeller gjennom trening av ansatte og gjøre gode fysiske modeller tilgjengelig.

4.4 Partene som er involvert i IO systemet

IO involverer mange ulike aktører med ulike verdier, og mentale modeller, derfor må man være oppmerksomme på at målkonflikter kan forekomme. Teori kapittelet ga en forklaring på hva målkonflikter er. Målkonflikter er en sikkerhetsrisiko som kan føre til ulykker, fordi aktører kan gjøre lokale valg som virker sikre, men som sammen med andre aktiviteter utgjør en risiko (se figur 6). I dette kapittelet vil vi benytte oss av denne forståelsen, og sammen med data fra de ulike dokumentene forsøke å si noe om mulighetene for målkonflikter i IO systemet.

IO systemet har mange ulike parter med ulik bakgrunn og oppgaver, partene i IO har Geir Haaland (2008) gruppert slik:

1. **Operatører/partner**: Har eierskap i ulike felt, og selskapet med størst eierandel er som regel operatør på feltet. De andre eierne har rolle som partner, enkelt sagt baserer operatørene sin fortjeneste på produsert mengde av petroleumsforekomster.
2. **Leverandør:** Operatørselskapene varierer i størrelse og besitter ulik grad av kompetanse, fasiliteter og utstyr. Felles for alle er at dersom store operasjoner skal utføres, enten det gjelder bore og brønntjenester eller modifikasjons og vedlikeholdsarbeid på en installasjon, må jobbene settes ut til ulike leverandører. Disse er eksperter på sine områder og baserer sin eksistens på prosjekter og rammekontrakter med operatørene. Kontraktene deler videre opp leverandørene i to undergrupper: Leverandørselskaper som leverer tjenester med Direkte påvirkning på operatørenes fortjeneste for eksempel et borre- og brønnselskap. Og leverandører som

leverer tjenester med indirekte påvirkning på operatørenes fortjeneste for eksempel vedlikeholds og modifikasjonsselskap

3. **Underleverandører**

Høivik (2009) sier at arbeiderne i petroleumsindustrien er enten operatøransatte i et operatørfirma, eller kontraktør ansatt hos et av kontraktør/ leverandør firmaene, som jobber for et operatørfirma. Operatørfirmaene håndterer den daglige arbeidet med produksjonen. Kontraktørene har ansatte fra flere ulike kontraktørfirmaer som tilbyr servicer innenfor brønn og borings service, vedlikehold og catering. Operatør og kontraktør ansatte jobber side om side og samarbeider både på offshore installasjonene og på landanleggene i de ulike jobb kategoriene. Ptil (2008) påpeker at samtidig som Statoil har fått en dominerende posisjon, har antall mindre aktører som Ptil følger opp, økt dramatisk de siste årene. Dette tyder på at aktør bildet kan bli enda mer komplekst i fremtiden.

4.4.1 Roller og målkonflikter

Som vi har sett påpeker Turner at inter organisatorisk gruppering med en eller to store organisasjoner og noen små involvert kan være en faktor som leder til ulykker. IO systemet vil ha flere både store og små organisatoriske grupperinger, derfor vil grenseområdene og rollene være mange og komplekse. Samtidig vil overlappinger mellom operatører i ulike onshore driftssentre og offshore skift kompliserer grenseområdene mellom grupperingene enda mer og gjøre systemet mer utsatt for målkonflikter. Ser man dette i forhold til at informasjon er ulik fordelt mellom gruppene, kan resultatet bli at aktører i IO systemet ikke besitter den informasjonen som kreves for å drifte IO teknologien sikkert. Målkonflikter er en sikkerhetsrisiko fordi hver beslutningstaker kan ha en modell og informasjon av en begrenset del av problemet, og dermed ikke forstår konsekvensene av egne handlinger. Rasmussens (figur 6) viste at sikker atferd som utføres innen ett arbeidsområde kan endre grensene for hvilke atferd som kan utføres i andre arbeidsområder,

Når personer samhandler over avstand, uten at alle er nær selve hendelsen vil IKT verktøyene få en viktig rolle med å skape felles situasjonsforståelse, synliggjøre ansvarsforhold og løpende bistå med koordinering. Uten at dette er ivaretatt kan det lett oppstå misforståelser og utilsiktede hendelser, derfor må man etablere en plan eller prosedyre for hvem som skal involveres i hvilke situasjoner (Johnsen og Lundteigen, 2008). Misforståelse og utilsiktede hendelser i form av målkonflikter, kan skje både når en hendelse inntreffer, eller forårsake en hendelse i IO systemet.

Sintef (2005) påpeker at i forbindelse med endringsprosessen kan det være en fare for uavklarte ansvarsforhold innad i organisasjonen eller utad mot andre organisasjoner. Dersom roller ansvar og funksjoner er riktig organisert og avklart i en slik sammenheng er mange av forutsetningene for god håndtering av normal drift og avvikssituasjoner til stede (Tveiten et al., 2008). Siden grenseflatene er mange vil det være vanskelig å etablere en plan for hvem som skal involveres i hvilke situasjoner og avklare roller og funksjoner fordi de teknologiske løsningene legger rammer og føringer for nye roller og samhandlingsmønstre. Reinovasjonsprosessen åpner for at enkeltpersoner og grupper kan finne sine egne måter å gjøre jobben på, prosessen kan gå over flere år, og kan være avgjørende for hvordan overgangen til integrerte operasjoner påvirker sikkerhet og produktivitet (Rosness et al., 2008). IO vil oppleve at reinovasjonsprosessen kan endre de planlagte rollene og dermed risikobildet. Derfor må sikkerhetsledelsen jobbe aktivt for å fange opp rolleendringer og implementere dem i organisasjonen for å unngå målkonflikter.

Også Tveiten et al. (2008)støtter at man må ha en effektiv koordinering av arbeidsoppgaver og roller, for å unngå at aktiviteter kommer i konflikt med hverandre, og slik at organisasjonen handler koordinert i krisesituasjoner. De viser at rollene offshore har vært uforandret siden 1975, og en forklaring på dette kan være at grunnaktivitetene i borevirksomheten er uforandret. Det har også vist seg vanskelig å endre roller og ansvarsforhold fordi disse er definert i kontraktsforhold og arbeidsavtaler, definert av kontraktsavdelingen til operatørselskapene basert på deres verdier og holdninger. I generasjon to er man avhengig av å ha et fleksibelt system hvor man har muligheten til å endre rollene etter hvert som endringene i systemet krever det. Dersom fleksibiliteten er uoppnåelig kan man få en situasjon hvor noen teknologiske elementer endrer seg og andre ikke, usynkrone endringer representerer som vi har sett en sikkerhetsrisiko.

I tilfeller hvor arbeidsressurser i prinsippet er tilgjengelige i ”hele verden”, vil operatørsenter i andre land ofte arbeide på en tid av døgnet når landansatte i Norge ikke er på jobb (”follow the sun” prinsippet). Sintef (2008 c) påpeker at kontraktene kan begrenses til at aktører langt unna kun har del roller å ivareta og kun har tilgang til ”need to know” informasjon for å utføre oppgaver. Man kan likevel ikke unngå at de vil stå ovenfor situasjoner som ikke er planlagt og ikke faller inn under del ansvaret hvor det blir vanskelig å vite hva som virkelig er ”need to know” informasjon. Dersom dette skjer kan det oppstå situasjoner hvor hver aktør har upresis kunnskap om problemene, noe som kan føre til risikofulle handlinger.

Kontraktforhold må endres frem mot generasjon to slik at verdiene og rollene til operatørene og leverandørene blir mer avklart i forhold til hverandre. Det vil være viktig å få en dynamikk i samarbeidet gjennom klargjøring av rollene og dermed minimerer målkonflikter.

4.4.2 Utfordringer i grenseflatene kan føre til målkonflikter

Turner (1997) har vist at innvolveringen av flere organisasjoner kan føre til ulykker. Sintef (2008 c) problematiserer dette når de påpeker at involvering av flere onshore sentre (boresenter, operasjonssenter hos operatør) øker risikoen for en uklarhet med hensyn til hvem som setter grenser for hva som er risikabelt og fordelingen av ansvar for hvordan en håndterer situasjonen for å gjenvinne kontroll var uklart. Uklarheter i forhold til hvem som har hvilket ansvar skjer til tross for om rollene er avklart fordi det alltid vil eksistere ansvarsområder folk deler til tross for ulike roller. Som Leplat viste vil det være problemer når folk kontrollerer den samme prosessen, fordi det eksisterer en usikkerhet om hvem som er ansvarlig for kontrollen på området, eller i denne delen av prosessen.

Sintef (2008 c) viser at endringer i skiftordninger og arbeidstid hav/land kan skape uro i organisasjonen og potensielle hull i oppmerksomhet mot aktivitet og operasjon. Grenseflatene blir mange og utviklingen synes å gå i retning av flere, og mer kompliserte hand- over[16] situasjoner. IKT, operasjon og samhandlings rom gjør det mulig å få geografisk spredde deltakere med på hand- over, men stor disiplin og større grad av planlegging kreves dersom man skal sikre seg at alle som bør være med faktisk deltar i disse møtene. Hand- over situasjonen er en kritisk aktivitet med stor innvirkning på situasjonsforståelse blant deltakerne i operasjonen. Mangelfull hand– over med feilaktig situasjonsforståelse som resultat har vært årsak til store ulykker (Ibid). Uten gode mentale modeller, vil risikoen ved hand- over situasjoner føre til økt ulykkespotensial, fordi aktører gjør handlinger som kan være i konflikt med handlinger gjort i andre deler av organisasjonen. OLF (2007 a) etterlyser risikoanalyser som også gjenspeiler at folk sitter geografisk spredt, at man ofte forholder seg til en abstrahert IO verden, og at samtaler foregår mellom deltakere med ulike virkelighetsforståelse. Med andre ord er det i dag for lite forskning på det faktum at det vil eksisterer grenseområder hvor sikkerheten beror på koordinering og samarbeid mellom aktører som er separert i tid og rom med ulik virkelighetsforståelse.

[16] "Hand-over" er et skriftlig dokument mellom personer i samme rolle. Et dokument på skrivebordet utgjør en viktig del av overleveringen sammen med samtalen pr telefon. I en friperiode skjer det mye og to "hand-overs" skal gi oppdatert informasjon, for ansatte på land og offshore (www.pep.no). Det vil være logisk å tro at i forhold til IO kan en hand- over være en rapport i systemet.

Målkonflikter i grenseområdene kan forhindres dersom aktørene besitter oppdaterte mentale modeller og har klart definerte roller. Oppdaterte mentale modeller forutsetter at informasjonsspredningen er god, og at sikkerhetsledelsen arbeider aktiv for å fange opp og implementere informasjonen. Det er verdt å merke seg at dersom man ikke ønsker en ulykke må endringer i grenseområdene fanges opp og implementerer i organisasjonene. Slik at alle involverte forstår sine roller og har oppdaterte mentale modeller som kan gi dem en god situasjonsforståelse. Arbeidet med å fange opp endringene vil i generasjon to være utfordrende fordi systemet er komplekst og fjerndrift gjør at grenseflatene er mange. Dette kan tyde på at organisasjonene bør sette av store ressurser til å koordinere grenseområdene, slik at de kan unngå en ulykke som følge av målkonflikter.

4.4.3 Avstand til risikokilden

Vi har sett at avstand til risikokilden kan påvirke om aktører er villige til å ta risiko og utføre handlinger som kan føre til en ulykke. I sin studie påpeker Høivik (2009) at ulykkesfrekvensen er lavere for operatør ansatte enn for kontraktør personell i petroleumsindustrien. Kontraktørene er de eneste som utfører drill og brønn operasjoner. Der hvor jobb kategoriene var mer sammenlignbare slik som administrasjon, catering og konstruksjon/vedlikehold, var det liten forskjell mellom ulykkesraten for operatør og kontraktør ansatte. Disse funnene sier noe om hvem som gjør den farligste jobben, og hvem som vil være mest var på å ta risikofulle valg.

Tradisjonelt har plattformsjefens rolle i å vurdere alvorlighetsgrad i situasjoner vært udiskutabel. Med IO får man mer involvering og styring fra land og ansvaret for hvem som har rettighetene for å vurdere alvorlighet blir mer utydelig og uenigheter og tap av verdifull tid kan bli blant følgene av denne uklarheten (Sintef, 2008 c). Økt press på regularitet og produksjon kan bidra til at slike konflikter oppstår. Realitetene i den sosiale konteksten hav og land er forskjellig ved at man på innretninger har et isolert sosialt miljø, mens man på land har en normalsituasjon ut fra den samfunnskonteksten man befinner seg i. Den reelle risikoen som de ulike gruppene utsettes for er vesentlig forskjelling, og det vil være en utfordring å få til samme grad av risikooppfattelse offshore og onshore (ibid).

Spørsmålet blir hvordan forholdene beskrevet over påvirker om ansatte i blunt end kan være mer villige til å ta risiko en de som jobber på plattformene (sharp end). Dersom operatørene vil være mer villige til å ta risiko når de er fjernet fra ulykkesområdet, kan det bety at de er mer villige til å foreta risikofulle handlinger. Som fører organisasjonen innenfor den ytre

grensen for hva som anses som sikkert arbeid. Økt risikovillighet er ikke gunstig for et system som er preget av hand- overs mellom ulike skiftordninger og land. Dersom ulike operatører utfører liknende handlinger kan man risikere at man beveger seg til den indre grensen og man kan dermed få en ulykke som rammer flere offshore ansatte. Før man tar i bruk fjerndrifting/styring er det viktig å ta en overveining over hvordan rollene offshore/onshore påvirker hverandre. Man må avdekke hvilke roller (onshore vs offshore) som har mest autoritet når man havner i pressede situasjoner hvor ansvarsforholdene i grenseområdene ikke er like klare, slik at man ikke får handlinger som er direkte motstridende.

Ved innføringen av IO i generasjon to må man ta høyde for at målkonflikter er en trussel for sikkerheten ved innføringen av fjernstyring. Når det er mange parter involvert i et komplekst system vil grenseflatene være mange, og uten klar rolle og ansvarsfordeling vil man kunne oppleve at folk handler usikkert. Mennesker handler usikkert fordi de har manglende kunnskap om problemet vil deres handlinger isolert sett virke fornuftige, men summen av slike handlinger kan føre organisasjonen innenfor rammen av sikre handlinger og føre til en ulykke, eller så handler de mer usikkert fordi de er fjernt fra risikokilden. Men som Rosness (2001) har vist vil ikke mennesker handle usikkert dersom de vet at resultatet vil være katastrofalt, de vil kun være mer utsatt for å undervurdere risikoen og ta valg fordi de antar at ulykken ikke inntreffer. Resultatet av flere slike usikre handlinger kan ifølge Rasmussen være en kostbar ulykke. Vi har også avdekket at manglende adgang på informasjon kan forsterke muligheten for simultane usikre handlinger, fordi ulike aktører kan besitte begrenset informasjon om problemene, og handle på basis av den kunnskapen de besitter. Kontraktforhold må endres frem mot generasjon to slik at verdiene og rollene til operatørene og leverandørene blir mer avklart i forhold til hverandre.

4.4.4 Avsluttende på målkonflikter

Kapittel tre avdekket at det i generasjon to blir viktig at aktørene har en felles forståelse for hovedmål og deres oppgaver/prosedyrer, og forstå ens egen rolle i forhold til andre. Her har vi sett at dette kan bli vanskelig når IO systemer inkluderer mange parter med ulik bakgrunn og oppgaver. Ved innføring av fjerndrift i generasjon to vil man få mer komplekse grenseområder fordi det er flere skift overlappinger enn i dag. Noe som fører til flere sårbare situasjoner når informasjon må skifte hender. Målkonflikter kan være et resultat av manglende koordinering i grenseområdene, fordi noen arbeidsområder er det vanskelig å vite hvem som har ansvaret.

Som dokumentene påpeker blir rolleavklaring viktig i generasjon to for å unngå målkonflikter. Rolleavklaring er også viktig for at sikre at de ulike partene samarbeider og ikke motarbeider hverandre gjennom lokal nyttemaksimering. For at reinovasjonsprosessen ikke skal resultere i ulik praksis hos de ulike partene, må IO systemet gi en mulighet for at rollene i hele organisasjonen kan endres dersom den teknologiske tilpasningsprosessen skulle tilsi det. Da må rollene som har vært uforandret siden 1975 bli kartlagt og oppdatert etter hvert som IO teknologien implementeres og påvirker rollene.

I tillegg til rollekonflikter vil begrenset informasjon kunne forsterke muligheten for målkonflikter. Fordi aktørene ikke forstår hele problemet og gjør lokale valg som påvirker sikkerheten til systemet som helhet. Hand over av informasjonen kan føre til at informasjonen går tapt eller misforstås. Og derfor gjør aktørene valg basert på feil beslutningsgrunnlag. Gode mentale modeller kan redusere antall situasjoner hvor dette skjer. Det er fordi aktører med gode mentale modeller forstår informasjonen bedre, og de klarer lettere å avdekke når deres handlinger er i konflikt med andres.

Målkonflikter vil være en sikkerhetsrisiko ved implementeringen av den nye IO teknologien. Det er fordi ny teknologi vil øke sannsynligheten for målkonflikter ved at det eksisterer lite informasjon i systemet. Og kontinuerlige endringer gjør at partene kan lage en lokal praksis som er i konflikt med andre lokale praksiser. I tillegg til dette vil avstanden til risikokilden som IO introduserer være er et element som kan forsterke målkonflikter. Når operatørene som innehar en viktig beslutningsfunksjon flyttes bort fra risikokilden, kan de bli mer villig til å ta valg som medfører risiko. Ikke fordi aktørene frivillig tar risikofulle valg, men fordi IO preges av en avstand som kan gjøre det vanskelig å overføre sikkerhetskritisk informasjon, sammen med at teknologien er ny og derfor har operatørene i utgangspunktet lite informasjon. Slik kan operatørene ta risikofulle valg basert på en begrenset del av informasjonen som er i konflikt med handlinger gjort i andre deler av systemet. Siden teknologien er ny og derfor utvikler seg må IO systemet avdekke endringene og implementere informasjonen i systemet fortløpende ettersom teknologien endrer seg. Slik at prosedyrer og de mentale modellene er oppdaterte og situasjonsforståelsen tilfredsstillende. Dersom dette ikke gjøres kan IO systemet rammes av målkonflikter i generasjon to.

4.5 Informasjons problematikk tilknyttet IO teknologien

Vi har til nå drøftet ulike sikkerhetsmessige problemstillinger ved innføring av ny teknologi, og hvordan trekk ved IO teknologien kan forsterke risikoen. Alle problemstillingene kan relateres til hvordan informasjon forstås og benyttes, derfor vil vi i dette kapittelet se nærmere på informasjon og kommunikasjons problemer som kan påvirke sikkerheten ved innføringen av IO. Fokuset blir på problemene som kan oppstå når informasjonen i den nye teknologien skal fanges opp og kommuniseres videre (feedback). Det er viktig å analysere informasjonsproblematikk fordi innføring av ny teknologi er avhengig av at informasjonen i endringene fanges opp og implementeres i organisasjonen.

Vi har tidligere sett at ny teknologi innfører en tilstand med lite informasjon i både kartleggings og reinovasjonsfasen. Avstanden og kompleksiteten som introduseres i IO teknologien kan gjøre det vanskeligere å håndtere og forstå informasjonen i den nye teknologien. Når enhetene befinner seg separert i tid og rom og beslutninger tas på avstand kan de være farefulle fordi underliggende informasjon undertrykkes i elektronisk samhandling (Sintef, 2008 a). Underliggende informasjon for eksempel medarbeidernes uro for at ikke alt virker som det skal, vil ikke nødvendigvis bli kommunisert i IKT nettverk. Viktig informasjon kan oppfattes til å ikke være viktig nok til å sende ut varsku om dette i et nettverk, framveksten av faremomenter kan derfor bli oversett (Ibid). Det vil si at selv om man har tilgang til sanntidsdata vil det være informasjon i IO systemet som ikke blir overført, som bør fanges opp. Her vil den generative kulturen spille en viktig rolle for hvor mye av den underliggende informasjonen som blir fanget opp.

Som Weick et al. (1999) har vist blir det viktig å bygge opp uformelle nettverk som kan fange opp og spre informasjon. Selv om planlagt informasjon er delt og overført i sanntid er ikke nødvendigvis uformell og ikke planlagt informasjon det. Slik tilleggsinformasjon kan virke uvesentlig i øyeblikket, men kan bidra til å komplettere et bilde i forståelse av noe som oppstår. Til tross for at kodifisert informasjon i IKT systemer reiser raskt vil ikke nødvendigvis sublim eller underliggende informasjon gjøre det. Underliggende informasjon kan for eksempel være medarbeideres uro for at ikke alt virker som det skal, men som ikke oppfattes som ”viktig nok” til å sende varsko ut i et nettverk (Sintef, 2008 c). Det er uvisst hvor mye underliggende informasjon som går tapt, for eksempel ved å gå fra ansikt til ansikt møter til videokonferanser (Tveiten et al., 2008). Her vil uformelle nettverk være viktige for å fange opp den underliggende informasjonen som sikkerhetsledelsen og de formelle

kommunikasjonskanalene ikke oppfatter. Ofte vil aktører tenke seg om før de rapporterer en situasjon til de formelle instansene, et ideelt uformelt nettverk vil bestå av dyktige aktører som har tillitt fra de ansatte hvor toleransen for å spre informasjonen er lav, som også har autoritet til å melde fra om de situasjonene som vurderes som alvorlige. Dersom man har uformelle nettverk som fanger opp slik uoffisiell infromasjon kan man fange opp endringer i inkubasjonsfasen, og unngår en uønsket hendelse.

4.5.1 Problemer er kompliserte og vanskelige å forstå

Vi har sett at risikoene ikke merkes fordi de er en del av det Turner (1997) kaller" ill structured problems" og "decoy fenomenet". IO systemet kan forsterke forekomsten av ill structured problems fordi mange parter er involvert og jobber parallelt over avstand, slik at det blir vanskelig å oppdage og kartlegge problemene. OLF (2007 a) viser til at distribuert sikker jobbanalyse (SJA) [17]kan gi dårligere årsaksbilde fordi den involverer flere geografisk spredte aktører. Avstanden og kompleksiteten i systemet gjør det vanskeligere å gjennomføre analyser, fordi samarbeidsformene er så komplekse at det stiller enorme krav til aktørenes mentale modeller å identifisere risikoelementene. Med andre ord vil det bli vanskelig for aktørene å identifisere risiko og forstå hvordan eget arbeid kan representere en risiko for andre deler av organisasjonen. Dette kan tyde på at IO er mer utsatt for "ill structured problems" fordi systemet i seg selv er komplekst og uoversiktelig.

"Decoy fenomenet" kompliserer kartleggingen av "ill structured problems" ved at relevant informasjon kan forsvinne i irrelevant informasjon, fordi et problem tar oppmerksomheten vekk fra et viktigere underliggende problem (Turner, 1997). Høyland (2007) avdekket i sine intervjuer av en arbeidsgiver at det var flere eksempler på at aktørene i generasjon null og en har hatt nødvendig informasjon for å unngå et problem. Men av en eller annen grunn var de ikke "smarte nok" til å innse det før etterpå. Informanten uttrykket videre en tro på at IO kan bidra til en bedre informasjonsflyt mellom de ulike aktørene før uønskede hendelser oppstår.

"Decoy fenomenet" vil ikke forsvinne med innføringen av IO teknologien i generasjon to selv om teknologien baserer seg på sanntidsdata. Det kan være underliggende informasjon som ikke avdekkes fordi aktørene kommuniserer over avstand. Situasjoner kan oppstå dersom organisasjonene ikke er flinke nok til å koordinere problemene de står ovenfor. Organisasjonene kan feile i å avdekke et bakenforliggende problem fordi det

[17] SJA er en systematisk og trinnvis gjennomgang av alle risikoelementer i forkant av en konkret arbeidsoppgave eller operasjon, slik at tiltak kan iverksettes for å fjerne eller kontrollere de identifiserte risikoelementene under forberedelse til og under gjennomføringen av arbeidsoppgaven eller operasjonen (www.olf.no)

bakenforliggende problemet kan ligge hos hvilken som helst aktør. Og vise seg som overfladiske problemer hos de andre aktørene. Her blir det vanskelig å avdekke de bakenforliggende problemene og løse de forårsakende problemene, med mindre det settes av ressurser til kartlegging (Turner 1997). Her ser man igjen viktigheten av å ha en generisk kultur hvor partene sprer informasjon om hvilke problemer de opplever, slik at organisasjonene i fellesskap kan forsøke å avdekke de forårsakende problemene.

Implementeringen av IO teknologien i generasjon to medfører økt kompleksitet i IKT styringssystemene som utfordrer aktørenes mentale modeller og situasjonsforståelse. Dagens brukergrensesnitt på mange installasjoner er basert på gammeldags skjermteknologi, med mye numerisk informasjon presentert på komplekse skjermbilder. Med nye informasjonskilder, nye samhandlingsverktøy og behov for å forholde seg til informasjon og data i en større sammenheng øker kompleksiteten i IKT styringssystemene (Sintef, 2005). Kompleksiteten vil gjøre det vanskelig for dem som operere systemet å fange opp feedbacken systemet gir, fordi det vil kreve mye av aktørenes mentale modeller å sette sammen informasjonen systemet gir.

Frem mot generasjon to er det nødvendig å oppdatere IKT verktøyene dersom operatørene skal ha en mulighet til å overvåke prosessene og sikkerhetsledelsen fange opp informasjonen. Verktøyene må bli enklere å bruke og overføre informasjon på best mulig vis. Det vil si at informasjonen må presenteres på en oversiktelig måte, hvis operatørene/sikkerhetsledelsen skal ha kapasitet til å forstå og beherske komplekse problemer. Bra utstyr er ikke nok for å fange opp endringene, i tillegg må aktørenes oppmerksomhet rettes mot å avdekke symptomer som viser seg i den daglige driften (minfullness). Fordi informasjon den daglige driften produserer kan være avgjørende for om organisasjonene klarer å forstå og avdekke underliggende problemer. Dersom IO systemet i tillegg klarer å fange opp den viktige informasjonen som ikke deles i de formelle nettverkene, vil systemet være bedre rustet til å fange opp store og små endringer og unngå uønskede hendelser.

4.5.2 Dårlig kommunikasjon

Dersom informasjonen blir fanget opp må informasjonen kommuniseres til de riktige personene som kan implementere endringene i organisasjonens regler og prosedyrer. Men som vi har sett er ikke dette arbeidet alltid like enkelt, da ulike personer vil i noen situasjoner ha problemer med å overføre mening (Turner, 1997).

Ved innføringen av IO forventer man at mennesker som er lokalisert på ulike steder skal kunne kommunisere og utføre komplekse arbeidsoppgaver i fellesskap, spørsmålet er imidlertid hvilke betingelser som må oppfylles for at IO virkelig skal fungere. Dersom man mislykkes, vil manglende samlokalisering av arbeidskraft føre til svekket kommunikasjon. (OLF, 2007 b). Vi har tidligere sett at feil- og kommunikasjonsproblemer er et sentralt moment i inkubasjonsfasen, fordi misforståelser, forbigåelser og feil antakelser mellom parter vil bidra til at uønskede hendelser akkumulerer i en organisasjon (Turner, 1997). Ved implementeringen av IO i generasjon to blir det derfor viktig å jobbe med å minimere kommunikasjonsproblemer, og sikre overføring av mening. Dette kan blant annet gjøres gjennom å sørge for å bygge opp en integrert sikkerhetskultur hvor de ansatte har like fortolkningsrammer og benytte seg av gode kommunikasjonskanaler.

4.5.3Kommunikasjon mellom ulike parter

En sentral problemstilling har vært hvordan en skal samhandle ved større avvik og hvordan en skal sikre at en har felles mentale modeller i en virtuell organisasjon når avvik skal håndteres (Sintef, 2005) I likhet med Turner (1997) og Kaufmann og Kaufmann(1997), ser Sintef (2005) at det kan oppstå språklige problemer når man etablerer landsenter i ulike land kan føre til dårlig kommunikasjon. Funksjoner vil i økt grad flyttes til lavkostland, noe som gjør at man kan få økte problemer med kommunikasjon og forståelse. Sintef (2008 a) beskriver samarbeid mellom grupper i IO som ulike ”arter” eller ”nisjer” som gir rom for variasjon og utvikling i samspill med andre arter. Kommunikasjon mellom disse nisjene/subkulturene må forsøke å gjøre seg forstått utenfor sin egen nisje, mens den som er mottaker må bestrebe seg på å gjøre innholdet forståelig innen sin egen nisje. Det som kommuniseres i grensene mellom subkulturene må forstås tilstrekkelig likt skal samarbeidet fungere, det betyr ikke nødvendigvis at det må forstås helt likt. Den resterende forskjellen kan imidlertid gjøre en stor forskjell under uvanlige eller uvante omstendigheter.

I forbindelse med fjerndrift kan det bli en høyere terskel for å ta opp et problem, dersom funksjoner flyttes til operasjonssenter på land. Avstanden kan føre til forsinkelse på problemløsningen og misforståelser som kan lede til en ulykke. Det kan være vanskeligere for en norskspråklig å ta opp problemer med en kontrolloperatør med skotsk aksent framfor en som snakker østlandsdialekt. Kan også være barrierer i form av at det er vanskeligere å ta opp problemer med personell med ekspertkompetanse. Dersom aktører drøyer å ta opp problemer

med eksperter i andre land eller organisasjoner kan lede til forsinkelser eller misforståelser og resulterer i en uønsket hendelse (Sintef, 2005).

Mange forskjellige begreper benyttes for eDrift og man snakker ofte ”forbi hverandre” og ”for overordnet”. Det er utfordringer knyttet til kommunikasjon både mellom ledelse og ansatte men også mellom de forskjellige fagmiljøene internt i selskapene (Sintef, 2005). Dårlig kommunikasjon mellom partene gjør det vanskelig å overføre meningsinnholdet i ulike situasjoner. Dårlig kommunikasjon kan være mellom to parter fordi de ikke går sammen, eller fordi de kan ha ulik kulturell bakgrunn som resulterer i ulik situasjonsforståelse (Turner, 1997; Kaufmann og Kaufmann, 1997).

Ulike kulturelle fortolkningsrammer gjør at man har ulike kommunikasjonsproblemer, fordi grupperingene forstår situasjoner og informasjon ulikt. En svært differensiert kultur vil øke dette problemet, fordi forståelsesrammene vil være så ulike, at de forstår og vil løse problemene ulikt., derfor blir det viktig å utvikle en integrert kultur for å redusere hyppigheten av dårlig kommunikasjon og sette av ressurser til å kartlegge problemene og sikre en felles forståelse (Turner, 1997)

4.5.4 Problemet med meningsoverføring

For å minimere kommunikasjonsproblemene beskrevet av Kaufmann og Kaufmann (1997), og sikre en høy grad av informasjonsoverføring har OLF (2005) og Nystøl sett på behovet for datastandardisering i IO. Datastandardisering t sørger for en flyt av ”lik” data mellom enhetene. Slik unngår organisasjonene å havne i situasjoner hvor man ikke er i stand til å få tilgang til visse data, fordi de er i annet format.

Man får ved IO en standardisering av ”alt” fra teknisk infrastruktur, datagrunnlag for arbeidsprosessene, mann- masking grensen snitt, rutiner, prosedyrer, samhandlingsmønstre og forståelser av sammenhenger og systemer (Sintef, 2008 a). Datastandardisering reduserer også muligheten for at de ulike artene snakker sitt eget språk, gjennom standardisering sikrer organisasjonene at de deler informasjon begge partene forstår. Men det er verdt å merke seg at dette ikke betyr at meningsinnholdet overføres, fordi det vil bero på partene som gir og mottar informasjonen tolker de standardiserte dataene likt.

Både Tveiten et al. (2008), Sintef (2008 a) og Høyland (2007) skriver om hvordan IO vil påvirkes av rike vs fattige kommunikasjonskanaler. Flytting av funksjoner til land fører til at personer som i dag kommuniserer ansikt til ansikt vil i fremtiden bli henvist til å bruke

fattigere kommunikasjonsmidler. Spørsmålet er om de fattige kommunikasjonskanalene klarer å overføre mening på lik linje som ansikt til ansikt kommunikasjon. Dokumentene i analysen hadde problemer med å slå fast om meningsinnholdet blir fattigere ved bruk av videokommunikasjon. Men Sintef (2008 a) viser til at det i IO vil være vanskelig å gjøre seg forstått gjennom fattige kommunikasjonskanaler, og tilsvarende vanskelig for mottaker og tolke budskapet inn i egen kontekst. Johnsen og Lundteigen (2008) sier at derfor må man undersøke om de nye og eventuelt eksisterende informasjons og kommunikasjonsverktøyene i IO er tilrettelagt slik at ulike samarbeidende aktører får samme situasjonsforståelsen. En felles situasjonsforståelse og oppdaterte mentale modeller kan gjøre en meningsoverføring lettere. Tveiten et al. (2008) antar at meningsinnholdet er dårligere i videokommunikasjon, men at det i dag (generasjon en) ikke vises i det fulle og hele fordi man i dag fortsatt har stor kontakt mellom aktørene. Nystøl (2008) avdekket i sin forskning at ingeniørene ikke hadde tenkt over hvilke ulemper tap av ansikt til ansikt kommunikasjon medfører. Dette tyder på at man bør forske mer på forhold som påvirker kommunikasjon av mening ved fjernstyring, før man tar i bruk teknologien. Dersom organisasjonene opplever å miste mye av meningsinnholdet når de kommuniserer over avstand er det er sikkerhetsproblem, fordi det kan føre til farlige handlinger eller målkonflikter.

For å muliggjøre kommunikasjon og meningsoverføring mellom offshore og onshore er det vitalt at organisasjonene har teknologiske verktøy som gjør det mulig. Dersom de teknologiske verktøyene bryter sammen, vil det være umulig å overføre mening i de eksisterende kommunikasjonskanalene (Turner, 1997). Ved innføringen av fjernstyring er vi avhengige av å ha kommunikasjonskanaler som virker både i normalsituasjon og i pressede situasjoner. OLF (2003) sier at for å sikre en kommunikasjon mellom hav og land som er robust nok, må det etableres et bredbånd stamnett på sokkelen med tilstrekkelig redundans, samtidig som nettet må utvides til å dekke alle installasjoner på sokkelen. Arbeidet med å bedre kommunikasjonsverktøyene bør gjøres før man går inn i generasjon to, fordi et kommunikasjonssystem som bryter sammen vil utgjøre en for stor sikkerhetsrisiko. Tilgang til informasjon er som vist vitalt for å unngå en ulykke ved implementeringen av IO og fjerndrift frem mot generasjon to.

I tillegg til å ha et fungerende kommunikasjonsnett, er det viktig at man vet hvilke kommunikasjonskanaler som skal benyttes til enhver tid. Man må sikre at rett folk får rett informasjon i IO noe som kan være vanskelig fordi som vi har sett er systemet utrolig komplekst. Derfor sier Sintef (2005) at det er viktig å få konstruert organisasjonsmodeller og

samhandlingsmodeller som avspeiler samhandlingsmønster og muligheter og trusler på tvers av tradisjonelle organisatoriske grenser. Behovet for infrastrukturer er ikke bare på teknisk plan, men også på et informasjonsplan, organisatorisk plan og en kulturell infrastruktur for samhandling på tvers. Behovet for å bygge opp informasjonsstrukturer er for å unngå at for mye tillitt tillegges det uformelle nettverket, som er opprettet for andre funksjoner (Turner, 1997). Det er viktig at de offisielle kommunikasjonskanalene benyttes, det uformelle systemet er ment til å fange opp informasjon som kan virke for triviell til å rapporteres som man er bekymret for kan representere en risiko. Dersom de formelle kanalene ikke brukes kan de uformelle kanalene overbelastes og kommunikasjonen bryte sammen, noe som er katastrofalt i pressede situasjoner. Derfor må organisasjonene frem mot generasjon to kartlegge og lage en informasjonsplan for å sørge for at informasjonen flyter til de riktige personene for å unngå en informasjons ”overflow” i det uformelle nettverket.

4.5.5 Avsluttende på kommunikasjon og informasjon

Kapittel tre viste at det vil være avgjørende for sikkerheten å avdekke og kommunisere informasjonen som ligger i ny teknologien, og at dette ikke er en enkel oppgave. Det er et sikkerhetsproblem fordi den nye teknologien kontinuerlige produserer informasjon gjennom tilpasningsprosessen som IO systemet må fange opp og implementere. Klarer aktørene kun å overføre informasjonen og ikke meningen, kan mottakerne misforstå informasjonen slik at forebyggingen av problemene blir ufullstendig. Når endringene ikke fanges opp blir de teknologiske elementene i ubalanse og kan forårsake en uønsket hendelse

Særtrekk ved IO teknologien kan forsterke problemene med å avdekke informasjonen. IO systemet er komplisert og preget av avstand. Systemet produserer informasjonsbiter som det er vanskelig å se sammenhengen mellom, samt at kan bli vanskelig å overføre informasjonsbitene.

Dokumentanalysen avdekket at organisasjonene frem mot generasjon to bør arbeide for å utvikle en kommunikasjonsteknologi som er robust og funksjonell. Å utarbeide en teknologi som både tåler stor belastning og uvante situasjoner, samt være enkel å benytte og forstå. Videre må organisasjonene kartlegge hvilke kommunikasjonskanaler som bør benyttes til hvilken tid, samt å arbeide for å bygge opp felles fortolkningsrammer som sikrer meningsoverføring.

For å få en oversikt over kommunikasjonskanalene og informasjonsflyten bør disse kartlegges. Ved implementeringen av fjerndrift og kompliserte IKT systemet må organisasjonene sørge for at aktørene har kunnskap om hvilke kommunikasjonskanaler som skal benyttes til riktig tid. Og opparbeide uformelle kommunikasjonskanaler preget av tillitt mellom aktørene.

Det er viktig å huske på at selv om kommunikasjonskanalene kartlegges, standardiseres og aktørene utvikler like fortolkningsrammer, vil det alltid være en mulighet for anomalier. Situasjoner organisasjonen ikke har forusett som representerer en utfordring fordi designerne ikke har planlagt for hvordan problemene skal løse ved hjelp av de standardiserte kommunikasjonsprosessene. Som vi så vil avsendere i slike situasjoner ha problemer med å plassere informasjonen i de riktige klassene når de forhåndsdefinerte klassene ikke passer for situasjonen. Det er stor sannsynlighet for at store deler av meningsinnholdet kan falle bort i slike situasjoner og kan derfor gjøre mottaker mer forvirret enn opplyst.

Før man implementerer generasjon to på norsk sokkel bør det settes av ressurser på å forske mer på fjerndrift og kommunikasjonskanalenes kapasitet til meningsoverføring ved normal og stresset situasjon. Fordi en utilstrekkelig meningsoverføring kan føre til at informasjonen i endringene ikke avdekkes og implementeres

5.0 SIKKERHETSMESSIGE PROBLEMSTILLINGER VED IMPLEMENTERING AV NY TEKNOLOGI

Hovedmålet med oppgaven er å finne svar på hvilke risikoer innføring av IO i generasjon to innebærer, derav problemstillingene:

- **Å avdekke hvilke sikkerhetsmessige utfordringer som oppstår ved implementering av ny teknologi.**
- **For så å vurdere hvordan utfordringene vil vise seg ved implementeringen av integrerte operasjoner.**

Hvilke sikkerhetsmessige utfordringer som oppstår ved implementering av ny teknologi: Analysen av dokumentene som skulle avdekke hvilke sikkerhetsmessige utfordringer som oppstår ved implementering av ny teknologi, viser at implementering innfører en tilstand med manglende informasjon. Som er et resultat av utfordringene ved å overføre informasjonen fra utvikler til mottaker, og at mottaker har manglende erfaring med teknologien. Oppgaven har analysert den nye IO teknologien ut fra Engen og Olsen (2010) og Lindøes og Olsen (2008) teori som sier at innføring av ny teknologi kan være risikofullt.

På grunn av at organisasjonen mangler informasjon om teknologien skapes en reinovasjonsfase der teknologien tilpasser seg den nye konteksten. Her vil både store og små endringer representere en sikkerhetsrisiko, fordi de teknologiske elementene kan komme i utakt. Basert på dette har oppgaven behandlet innføringen av ny teknologi og medfølgende endringer i et informasjonsperspektiv. Hvor katastrofer og ulykker er et resultat av energi og feilinformasjon.

Fremveksten av ulykker ble analysert i forhold til Turners (1997) ulykkes modell, med fokus på kartlegging av risiko i fase en og etterfølgende inkubasjonsfase. Kartleggingen er ofte ufullstendig på grunn av manglende informasjon og dermed kan resultatet av kartleggingen representere en risiko. Den ufullstendige kartleggingen kan forsterkes av at teknologien er ny og designerne ikke kan basere seg på erfaring. Risikoen blir først ”synlig” når teknologien kommer i drift. I oppgaven var det nyttig å tolke reinovasjonsprosessen og inkubasjonsfasen som sammenfallende, fordi endringene som skjer i drift kan være et resultat av mangelfulle eller dårlig tilpassede prosedyrer. Det innebærer at ny teknologi innfører en risiko i form av at organisasjonen mangler informasjon til å kartlegge risikoen ved å ta teknologien i bruk. Samtidig som reinovasjonsfasen produserer informasjon som må fanges opp og

implementeres i organisasjonen, for å unngå at de teknologiske elementene havner i ubalanse og skaper en ulykke.

Hvordan utfordringene vil vise seg ved implementeringen av integrerte operasjoner: Analysen av dokumentene som skulle avdekke hvordan utfordringene vil vise seg ved implementeringen av integrerte operasjoner, viste at IO teknologien har særtrekk som kan forsterke risikoen som ligger i å ta i bruk ny teknologi. Generasjon to preges av avstand mellom aktørene, der deler av samhandlingen går gjennom komplekse IKT systemer. Dette resulterer at IO systemet får mer komplekse interaksjoner og tettere koplinger, som gjør det vanskelig for designerne å forstå systemet og lage en tilfredsstillende kartlegging av risiko. Avstanden mellom aktørene vil videre gjøre det vanskelig å fange opp endringene i reinovasjonsprosessen lokalt og samkjøre dem sentralt, slik at hele systemet oppdateres.

Analysen avdekket videre at sikkerhetskulturen vil påvirke sikkerhetsfokuset i generasjon to og sette rammer for hvor mye av informasjonen i endringene som fanges opp, deles og implementeres i IO systemet. En generativ sikkerhetskultur vil være viktig for å identifisere og implementere informasjonen i reinovasjonsprosessen. Bransjen preges i dag av differensiering der fokuset på sikkerhet tidvis ikke var tilfredsstillende på grunn av dårlige oljepriser og lav tillitt mellom partene. Dersom bransjen preges av dette i generasjon to vil det være vanskelig å dyrke en integrert og generativ kultur, dette kan resultere i at teknologien implementeres ulikt i organisasjonene og at endringene ikke fanges opp og derfor representerer en sikkerhetsrisiko. Videre vil ulik implementering utgjøre en sikkerhetsrisiko fordi ulik praksis kan skape målkonflikter.

Analysen viser at ved implementeringen av ny teknologi er mentale modeller sentralt for å forstå informasjonen endringene skaper. Når teknologien er ny, vil det være vanskelig å ha tilstrekkelig informasjon til utvikling av korrekte mentale modeller. Modellene kan bli utdatert og feilaktige dersom sikkerhetsledelsen ikke implementerer endringene i systemet. Analysen viste at i generasjon to vil det bli vanskelig å konstruere gode mentale modeller, fordi systemet blir komplekst når prosessene automatiseres, inkluderer mange parter og hand-over situasjoner. Avstanden vil også gjøre det vanskelig for aktørene å forstå sammenhengene mellom prosesser som foregår offshore og onshore. Uten gode mentale modeller vil innføring av ny teknologi representere en sikkerhetsrisiko.

Ny teknologi kan forsterke faren for målkonflikter fordi aktørene mangler informasjon om egne og andres arbeidsprosesser, og derfor besitter feilaktige mentale modeller. Analysen avdekket at IO vil i generasjon to få flere komplekse grenseområder siden flere skift inkluderes. Manglende koordinering i grenseområdene kan føre til målkonflikter og ulykker. Avstanden i IO kan forsterke forekomsten av målkonflikter, fordi ansatte ikke forstår at eget arbeid påvirker andre deler av systemet. Faren for målkonflikter kan forsterkes ved at operatørene som innehar en viktig beslutningsfunksjon, flyttes bort fra risikokilden og tar valg som medfører høyere risiko basert på mangelfull informasjon.

Ny teknologi preges av manglende informasjon i begge fasene, og dersom informasjonen ikke brukes riktig vil det utgjøre en sikkerhetsrisiko. Derfor var det viktig å undersøke hvilke faktorer som påvirker bruken og forståelsen av informasjon. Analysen avdekket at IO i generasjon to er avhengig av å ha kommunikasjonsteknologi som er både robust og funksjonell. Robust fordi teknologien ikke må bryte sammen ved press i uvante situasjoner. Og funksjonell for å ivareta høy grad av meningsoverføring mellom avsender og mottaker i ulike situasjoner. Tillitt mellom partene og gode uformelle kommunikasjonskanaler blir viktig for informasjonsspredningen.

5.1 Anbefalinger

Dokumentanalysen viste tydelig de sikkerhetsmessige utfordringer som oppstår ved innføring av ny teknologi. Manglende informasjon vil innebære en risiko fordi organisasjoner ikke klarer å se hele risikobildet, når de bare besitter biter med informasjon. Og implementeringen av IO teknologien vil vanskeliggjøre informasjonsprosessene når systemets særtrekk vanskeliggjør bruk og deling av informasjon. Men dokumentanalysen avdekket også områder hvor forskningen er mangelfull.

Dokumentanalysen avdekket at forskningsrapportene mangler et fokus på sikkerhetskulturens innvirkning på hvilke sikkerhetsmessige risikoer IO teknologien kan implementere i generasjon to. Derfor bør det i utviklingen mot generasjon to forskes mer på sikkerhetskulturens rolle ved fjerndrift som involverer mange parter, med ulik bakgrunn. Og hvordan feil verdier samt en patologisk kultur er fatalt når mange parter skal håndtere informasjonen som produseres i den nye teknologien.

Selv om det i dag er en del rapporter som har sett på kommunikasjonskanalene, bør det settes av ressurser til å forske mer på fjerndrift og kommunikasjonskanalenes kapasitet til

meningsoverføring ved ulike situasjoner. Denne forskningen bør være grunnlag når det foretas en vurdering av hvor stor grad av fjerndrift som kan oppnås uten å gå på bekostning av sikkerheten. En gjennomgående analyse kan avdekke hvor mye av kompetansen som bør beholdes offshore, slik at de er rustet til å beherske en kritisk situasjon på egenhånd dersom kommunikasjonskanalene svikter.

Til slutt er det ønskelig at fremtidige rapporter som avdekker verdi potensialet til IO, også vurderer treningskostnadene i generasjon to. Det vil trolig kreves mye trening for å samkjøre de mentale modellene og unngå målkonflikter. Graden av trening som må gjennomføres for å samkjøre antall team kan føre til at det blir større kostnader ved å ta i bruk IO teknologien enn mange antar.

5.2 Oppgavens relevans

Det er fristende å anse situasjonen på norsk sokkel som unik, men det er mer nærliggende å påstå at situasjonen på norsk sokkel er sjelden heller enn særegen. Den teknologiske utviklingen presser organisasjoner til å ta i bruk teknologiske nyvinninger for å kunne overleve i et hardt presset marked. Systemer som er preget av avstand mellom enhetene er heller ingen særegen situasjon. Flyindustrien har i årevis benyttet seg av flyveledere som styrer fly fra bakken. Derfor kan petroleumsnæringen trekke lærdom av liknende industrier som benytter tilsvarende teknologi, og hvordan disse har løst problemene/risikoene oppgaven har undersøkt. Læringspotensialet av å studere tilsvarende teknologiske implementeringer er stort, det er fordi designerne kan få kunnskap om risikoen ved å ta i bruk ny teknologi i et system preget av avstand.

Informasjonshåndtering vil i følge Turner være medvirkende årsak i alle ulykker. Derfor må organisasjoner som innfører ny teknologi i tilsvarende komplekse systemer preget av avstand, være oppmerksomme på medfølgende risiko. De må ha kunnskap om hvordan sikkerhetskulturen kan forebygge ulykker, men også skape uønskede hendelser. Se viktigheten av å bygge opp mentale modeller, slik at aktørene er i stand til å forstå den nye teknologien til tross for mangelfull informasjon. Jobbe aktivt for å unngå at de teknologiske endringene skaper ulik praksis og bidrar til målkonflikter. Og sikkerhetsledelsen må fokusere på å fange opp og unngå at informasjonen misforstås, samt å sikre en god kommunikasjon mellom aktørene. Arbeidet med å opprettholde en sikker organisasjon ved implementering av ny teknologi er omfattende. Men i god HRO tradisjon kan man hevde at det er mulig å operere slike komplekse tett koplede systemer sikkert, til tross for at ny teknologi vil forsterke

risikoen. Men sikker implementering krever innsats og samarbeid for at informasjonsbitene skal passe sammen.

6.0 LITTERATURLISTE

Aven Terje (2006). *Pålitelighets og risikoanalyse*, 4 utgave. Universitetsforlaget, Oslo.

Aven Terje, Boysen Marit, Njo Ove, Olsen Kjell Harald, Sandve Kjell (2008). *Samfunnssikkerhet,* 3 opplag. Universitetsforlaget, Oslo.

DeJoy, D. M. (2005). Behaviour *change versus culture change:* Divergent approaches to managing workplace safety. Safety Science, 43.

Engen Ole Andreas og Olsen Odd Einar (2010). *Small steps towards big accidents*. Reliability, Risk and Safety: Theory and Applications-Bris Guedes Sorares & Martorell. Taylor & Francis Group. London.

Flin, R (2007). *Measuring safety culture in healthcare: A case for accurate diagnosis*. Safety Science, 45.

Grøtan Tor Olav (2008). *IKT som bidrag til robusthet i integrerte operasjoner – et skråblikk.* hentet fra Tinmannsvik Ranveig Kviseth. *Robust arbeidspraksis- Hvorfor skjer det ikke flere ulykker på sokkelen?* Tapir Akademiske Forlag, Trondheim.

Guldenmund FW., 2007. "*The use of questionnaires in safety culture research an evaluation*". Safety science, 45, 723-743.

Hatch Jo Mary og Schultz Majken (2003). *Bringing the corporation into corporate branding.* European journal of marketing Vol. 37 (No 7/8): s 1041-1064.

Haukelid Knut (2004). Oljekultur og sikkerhetskultur – del 3. Senter for teknologi, innovasjon og Kultur. Arbeidsnotat nr. 28/2004.

Høivik Dordi (2009). *Helse, miljø og sikkerhetskultur i petroleumsindustrien i Norge*. Universitetet i Bergen.

Johnsen Stig Ole og Lundteigen Mary Ann *"Sikrere fjerndrift med CRIOP"* hentet fra Tinmannsvik Ranveig Kviseth (2008). *Robust arbeidspraksis- Hvorfor skjer det ikke flere ulykker på sokkelen?* Tapir Akademiske Forlag, Trondheim.

Jackobsen Dag Ingvar (2003). *"Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskaplig metode".* Høyskoleforlaget, Kristiansand.

Jackobsen Dag Ingvar (2005). *"Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskaplig metode".* Høyskoleforlaget, Kristiansand.

Johnsen Stig Ole og Lundteigen Mary Ann. *Sikrere fjerndrift med CRIOP*. Hentet fra Tinmannsvik Ranveig Kviseth (2008). *Robust arbeidspraksis- Hvorfor skjer det ikke flere ulykker på sokkelen?* Tapir Akademiske Forlag, Trondheim.

Kaufmann, G., & Kaufmann, A (1997). *Psykologi i organisasjon og ledelse*". Bergen: Fagbokforlaget.

Leplat J (1987*). Occupational accident research and system approach.* Hentet fra Rasmussen J., Duncan, K., Leplat, J. New Technology and Human Error, s 181 – 191, John Wiley & sons, New York.

Leveson Nancy (2004). *A New Accident Model for Engineering Safer Systems*. Hentet fra Safety Science Vol 42. Side 237 -270.

Nævestad Tor Olav og Olsen Espen (2006). *Kultur og atferd som tilnærming for å bedre sikkerheten: en evaluering av kollegaprogrammet*. IRIS, Stavanger.

Olsen Odd Einar og Lindøe H Preben (2008a). ”*Risk on the Rumble -The international transfer of risk and vulnerability”.* Safety Science.

Olsen Odd Einar og Lindøe H Preben (2008b). ”*Risiko på vandring”* hentet fra Tinmannsvik Ranveig Kviseth. *Robust arbeidspraksis- Hvorfor skjer det ikke flere ulykker på sokkelen?* Tapir Akademiske Forlag, Trondheim.

Olson Gary M og Olson Judit S (2000). *Distance matters*, Universitiy of Michigan.

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

Pidgeon N og M. O`Leary (2000). *Man-made disasters: why technology and organizations (sometimes) fail,* Safety Science, 34, 15-30.

Rasmussen (1994). *Risk management, adaptation, and design for safety*. In B. Brehmer and N.-E. Sahlin. Future Risks and Risk Management, (s 1-36). Kluwer Academic Publishers.

Reason, J (1997). *Managing the Risk of organizational accidents.* Ashgate, Burlington USA.

Richter, R., & Koch, C (2004). *Integration, differentiation and ambiguity in safety cultures*. Safety Science, 42, 703-722.

Rosenthal Uriel, Boin Arjen.R, Comfort Louise K. (2001). *Managing Crises – Threats, Dilemmas, Opportunities*. Charles C Thomas Publisher. Springfield USA.

Rosness Ragnar, Guttormsen Geir, Steiro Trygve, Tinmannsvik Ranveig K., Herrera Ivonne A. (2004). *Organisational Accident and Resillient Organisations: Five perspevtive*. Sintef Rapport.

Rosness Ragnar (2001). ”*Om jeg hamrer eller hamres, like fullt så skal der jamres”,* Målkonflikter og sikkerhet. Sintef Rapport.

Ryggvik, Helge (2008). *Adferd, teknologi og system – en sikkerhetshistorie.* Tapir: Akademisk forlag.

Schein Edgar H. (1987). *Organisasjonskultur og Ledelse: Er kulturendring mulig?* Mercury Media Forlag AS.

Scott John (1990). *A Matter of Record – Documentary Sources in Social Research*. T.J. Press Ltd. , Padstow, Cornwall.

Tinmannsvik Ranveig Kviseth (2008) .*Robust arbeidspraksis- Hvorfor skjer det ikke flere ulykker på sokkelen?* Tapir Akademiske Forlag, Trondheim.

Turner, Barry A. And Pidgeon, Nick F (1997). Man-Made Disasters, Oxford: Butterwoth Heineman.

Tveiten Camilla Knudsen, Andresen Gisle, Rosness Ragnar og Tinmannsvik Ranveig Kviseth "*underveis mot integrerte operasjoner*" hentet fra Tinmannsvik Ranveig Kviseth (2008). *Robust arbeidspraksis- Hvorfor skjer det ikke flere ulykker på sokkelen?* Tapir Akademiske Forlag, Trondheim.

Weick , K.E, Sutcliffe, K.M., Obstfeld, D.(1999.*) Organizing for high reliability: Process of collective mindfulness.* Research in Organizational Behavior, 21, 81 – 123.

Westrum, R. (1993). Culture with Requisite imagination. In J.A. Wise, V.D. Hopkin and P Stager (eds9: *Verification and Validiation of Complex Systems*: Human Factors Issues. Berlin: Springer, 401-416.

Yin, R.K (2009). *Case Study Research: Design and Methods*. 4 opplag. Sage Inc., Thousand Oaks. California.

6.1 Master oppgaver

Nystøl Anders (2008). *Databehandling i komplekse og integrerte operasjoner, fra et MTO-perspektiv*. Universitetet i Stavanger.

Høyland Elisabeth (2007). *Sikkerhetsbetraktninger ved implementeringen av integrerte operasjoner i norsk petroleumsvirksomhet.*. Universitetet i Stavanger.

Haaland Geir (2008). *Integrerte operasjoner i V&M kontrakter*. Universitetet i Stavanger.

6.2 Internett adresser og rapporter

Beskrivelse	**Linker:**	**Hentet og lest:**
Sitat	http://www.quotegarden.com/technology.html	02.02.10
Artikkel	http://www.aftenbladet.no/energi/olje/article602007.ece	15.04.10
Oljedirektoratets	http://www.npd.no/Global/Norsk/3%20-%20Publikasjoner/Faktahefter/Fakta2009/Kapitler/Kap%2	25.02.10

faktabok 2009	01%20norsk.pdf	
Stortingsmelding 38 2003/04	http://www.regjeringen.no/Rpub/STM/20032004/038/PDFS/ STM200320040038000DDDPDFS.pdf	22.03.10
Definisjon: informasjon	http://no.wikipedia.org/wiki/Informasjon	31.03.10
Artikkel Ptil 2008	http://www.ptil.no/vedlikeholdsstyring/lavt-tempo-for-innfoering-av-integrerte-operasjoner-article4985-96.html	20.03.10
Definisjon: hand over	http://www.pep.no/files/nyhetsbrev/2007/pdf/PEPspes_Transocean_trivsel_og_effektivitet.pdf	15.04.10
Definisjon: sikker jobb analyse	http://www.olf.no/getfile.php/Dokumenter/Retningslinjer/081-100/090_SikkerJobbAnalyse_rev2.pdf)	28.03.10
Definisjon anomali	http://no.wikipedia.org/wiki/Anomali	20.05.10

Beskrivelse	**Rapporter:**	**Hentet og lest:**
Sintef 2005	http://www.sintef.org/upload/Teknologi_og_samfunn/Sikkerhet%20og%20p%C3%A5litelighet/Rapporter/STF38%20A04433.pdf	18.03.10
Sintef 2008 a	http://www.sintef.no/upload/Teknologi_og_samfunn/Sikkerhet%20og%20p%C3%A5litelighet/Rapporter/SINTEF%20A7085.pdf	12.03.10

Sintef 2008 b	http://www.ptil.no/getfile.php/Presentasjoner/Vedlikeholdsstyring%20og%20IO/SINTEF%20rapport%20IO%20i%20vedlikeholdsstyring%20MTIyNTQ1NzE1Nzc5MDEzOTc1Mg.pdf	18:03.10
Sintef 2008c	http://www.sintef.no/upload/Teknologi_og_samfunn/Sikkerhet%20og%20p%C3%A5litelighet/Rapporter/SINTEF%20A7078%20Hva%20inneb%C3%A6rer%20egentlig%20Integrerte%20Operasjoner.pdf	19.03.10
Sintef 2010	http://www.sintef.no/upload/Teknologi_og_samfunn/Sikkerhet%20og%20p%C3%A5litelighet/Rapporter/SINTEF%20A14732%20Essays%20on%20socio-technical%20vulnerabilities%20and%20strategies%20of%20control%20in%20Integrated%20Operations.pdf	03.04.10
Ptil 2008	http://www.ptil.no/getfile.php/PDF/Sikkerhet%2009.indd.pdf	01.05.10
OLF 2003	http://www.ntnu.no/gass/conferences/System_seminar271003/OLF-rapport%20e-drift.pdf	
OLF 2005	http://www.olf.no/getfile.php/zKonvertert/www.olf.no/Rapporter/Dokumenter/051101%20Integrerte%20arbeidsprosesser,%20rapport.pdf	
OLF 2007 a	http://www.olf.no/getfile.php/zKonvertert/www.olf.no/Rapporter/Dokumenter/080125%20Oppdatering%20av%20verdipotensialet%20i%20IO.pdf	
OLf 2007b	http://www.olf.no/getfile.php/zKonvertert/aSLETTES/Aktuelt/Dokumenter/070115%20-%20IO%20og%20HMS.pdf	

7.0 VEDLEGG

Dokument	Problemstilling/tittel	Mål med dokumentet
Sintef 2005	*Trusler og muligheter knyttet til eDrift*	**Ny teknologi:** Beskriver at endringene kan gjøre sikkerhetsvurderinger utdaterte **Sikkerhetskultur:** Viser at ulikheter i fortolkningene (subkulturer) kan være en sikkerhetsutfordring. **Mentale modeller**: Viser hvordan kompliserte IKT nettverk og fjerndrift skaper en utfordring for å ha felles mentale modeller **Mentale modeller:** Viser hvordan IO teknologien kan bidra til å bygge felles mentale modeller gjennom modeller og sanntidsdata. **Mentale modeller**: Viser at automatiseringer har ført til feilfunksjoner i situasjoner, fordi designerne ikke har tatt høyde for risikoen i planleggingen. Og at automatiseringer gjør det vanskelig for aktørene å ha gode mentale modeller. **Målkonflikter**: Viser at rolleavklaring er viktig for å unngå målkonflikter. **Informasjonsprosesser:** Viser at det enda brukes gammel skjermteknologi, som presenterer informasjonen utilfredsstillende. **Informasjonsprosesser**: Viser at det er utfordring å dele informasjon mellom ulike aktører.
Sintef 2008 a	*Risikokartlegging og analyse av Integrerte Operasjoner (IO) med fokus på å avdekke viktige MTO aspekter*	**Mentale modeller:** Fokuserer på viktigheten med felles mentale modeller offshore/onshore. **Mentale modeller**: Viser hvordan automatiseringer utfordrer de mentale modellene ved at operatørene pasifiseres i det daglige. **Informasjonsprosesser:** Viser at avstanden IO teknologien kan føre til at sikkerhetskritisk informasjon ikke avdekkes. **Informasjonsprosesser**: Påpeker at IO innebærer en standardiseringer, for å sikre overføring av informasjon. **Informasjonsprosesser:** Beskriver at IO vil gå fra rike til fattigere kommunikasjonskanaler til å overføre informasjonen.
Sintef 2008 b	*Kartlegging av bruken av integrerte*	**Ny teknologi:** Beskriver statusen på

	operasjoner i vedlikeholdsstyring	implementeringen **Sikkerhetskultur**: Viser at det ikke er en generisk kultur i generasjon en fordi tilgangen på informasjon ikke er god nok.
Sintef 2008c	*Hva innebærer egentlig Integrerte Operasjoner?* *Fenomenforståelse og generiske elementer med mulige konsekvenser for storulykkespotensialet.*	**Ny teknologi**: Beskriver risikopotensialet i teknologien som har tette koplinger og komplekse interaksjoner. **Mentale modeller:** Viser hvordan automatiseringer utfordrer de mentale modellene ved at operatørene pasifiseres i det daglige. **Mentale modeller:** Påpeker at aktørene må trenes for å bygge opp forståelsen. **Mentale modeller:** Påpeker at det er en utfordring å ha gode mentale modeller når offshore personell har lange friperioder **Målkonflikter:** Viser at det vil bli vanskelig å sikre at aktører langt borte har tilgang til informasjonen de trenger i ulike situasjoner, slik at det kan skape målkonflikter. **Målkonflikter**: Viser at involvering av flere ulike organisasjoner kan skape uklare ansvarsforhold og dermed målkonflikter. **Målkonflikter:** Viser at skift ordningene representerer en økt risiko for målkonflikter, fordi det kan bli hull i oppmerksomheten ved informasjons overlevering. **Målkonflikter**: Viser at risikoen partene utsettes for er forskjellig og derfor kan påvirke risikooppfattelsen. **Informasjonsprosesser:** Viser at aktørene kan unngå og spre informasjon fordi de misforstår informasjonen
Sintef 2010	*Interdisciplinary risk assessment of Integrated Operations addressing human and organizational factors*	**Mentale modeller:** Viser viktigheten av mentale modeller når den fysiske kontakten blir borte. **Mentale modeller:** Påpeker at automatiseringer gjør det vanskelig for aktørene å forstå prosessene fordi de ikke er synlige.
Ptil 2008	*Sikkerhet - status og signaler*	**Målkonflikter:** Beskriver aktørbildet på norsk sokkel.
OLF 2003	*Edrift på norsk sokkel – det tredje effektiviseringsspranget*	**Informasjonsprosesser:** Viser at for å sikre informasjonsoverføring må kommunikasjonskanalene være robuste nok.
OLF 2005	*Integrated work process: Future workprocess on the*	**Ny teknologi**: Beskriver endringene i

	Norwegiancontinental shelf	informasjonsprosessen **Mentale modeller:** Viser at samhandling over avstand krever mentale modeller. **Målkonflikter:** Påpeker at det bør fokuseres på risikoen for målkonflikter ved at aktører sitter geografisk spredt. **Informasjonsprosesser**: Behov for datastandardisering for å sikre en høy grad av informasjonsoverføring **Informasjonsprosesser:** Viser viktigheten med å kartlegge kommunikasjonskanalene og informasjonsstrukturene. For å utforme bedre informasjonsstruktur som er mer robust.
OLF 2007 a	*Oppdatert verdipotensial for integrerte operasjoner på norsk sokkel*	**Sikkerhetskultur:** Ser på manglende tillitsforhold mellom partene offshore/onshore, og ulike fortolkningsrammer som skaper subkulturer. **Informasjonsprosesser**: Avstanden og kompleksiteten kan gjøre det vanskeligere å gjennomføre analyser som skal avdekke sikkerhetskritisk informasjon, fordi aktørene ikke har mentale modeller til å forstå informasjonen i systemet.
OLf 2007b	*HMS og integrerte operasjoner: forbedringsmuligheter og nødvendige tiltak*	**Ny teknologi:** Beskriver endringene i arbeidsprosessene **Mentale modeller**: Viser at det er en utfordring å sikre at alle som samarbeider i IO har like mentale modeller.
Olsen og Lindøe 2008	*Ny teknologi og organisasjoner i endring. Risiko på vandring*	**Ny teknologi:** Viser hvordan innføring av ny teknologi kan skape risiko
Olsen og Engen 2010	*Small steps towards big accidents*	**Ny teknologi:** Viser hvordan innføringen av ny teknologi kan skape risiko med store og små endringer.
Tveiten et. al 2008	*Underveis mot integrerte operasjoner – en borekontraktør tilegner seg nye IKT- løsninger*	**Ny teknologi:** Drøfter om IO er ny teknologi. **Sikkerhetskultur**: Beskriver subkulturer offshore. **Mentale modeller:** Viser at IKT teknologien kan bidra til å konstruere gode mentale modeller gjennom visuelle IKT løsninger. **Mentale modeller**: Påpeker at modellene bygges gjennom trening. **Mentale modeller**: Viser at det er vanskelig å samkjøre de ulike gruppenes mentale modeller **Målkonflikter:** Viser at det er viktig med avklarte roller for å unngå målkonflikter.

		Samt en effektig koordinering av arbeidsoppgaver. **Informasjonsprosesser:** Påpeker at man ikke vet hvor mye informasjon som vil tapes ved fjerndrift. **Informasjonsprosesser**: Beskriver at IO vil gå fra rike til fattigere kommunikasjonskanaler til å overføre informasjonen. Men er usikker på meningstapet.
Johnsen og Lundteigen 2008	*Sikrere Fjerndrift med CRIOP*	**Ny teknologi**: Viser at IO er ny teknologi som utvikler seg. **Mentale modeller**: viser at det er en utfordring å forsikre at alle har like mentale modeller. **Mentale modeller:** Avstanden kan forsterke at dårlig situasjonsforståelse kan føre til målkonflikter. **Mentale modeller:** Påpeker at aktørene må trenes for å få felles situasjonsforståelse. **Målkonflikter:** Viser at avstand krever mentale modeller for å unngå målkonflikter. **Informasjonsprosesser:** Påpeker at det er viktig å vurdere om kommunikasjonskanalene bidrar til meningsoverføring i informasjonsprosessen.
Rosness et al	*Organisational Accident and Resillient Organisations*	**Målkonflikter:** Viser at IO i generasjon to vil endre rollene og dermed kan forårsake målkonflikter
Grøtan 2008	*IKT som bidrag til robusthet i integrerte operasjoner – et skråblikk*	**Mentale modeller:** Viser at mentale modeller er viktig for å forstå informasjonen i systemer. Særlig når samhandlingen blir globalisert **Mentale modeller:** Viser hvordan automatiseringer utfordrer de mentale modellene ved at operatørene pasifiseres i det daglige.
Espen Olsen	Kultur og atferd som tilnærming for å bedre sikkerheten: En evaluering av kollegaprogrammet	**Sikkerhetskultur:** Beskriver subkulturene på norsk sokkel
Høivik Dordi	*Helse, miljø og sikkerhetskultur i petroleumsindustrien i Norge*.	**Sikkerhetskultur***:* Beskriver subkulturene på norsk sokkel **Målkonflikter:** Beskriver partene på norsk sokkel og produksjonsforholdet mellom dem **Målkonflikter:** Viser at offshore ansatte er

		utsatt for høyere risiko enn landansatte.
Haukelid Knut	*Oljekultur og sikkerhetskultur*	**Sikkerhetskultur:** Beskriver subkulturene på norsk sokkel og sikkerhetskulturens historie. Relevant for å avdekke hvilken sikkerhetskultur som dominerer på norsk sokkel
Ryggvik, Helge	*Adferd, teknologi og system – en sikkerhetshistorie.*	**Sikkerhetskultur:** Presenterer sikkerhetskulturens historie. Relevant for å avdekke hvilken sikkerhetskultur som dominerer på norsk sokkel
Nystøl Anders:	*Databehandling i komplekse og integrerte operasjoner, fra et MTO-perspektiv. (masteroppgave)*	**Mentale modeller:** Viser at automatiseringen er nødvendig for å unngå informasjons overbelastning. **Informasjonsprosesser:** Viser at det er behov for datastandardisering for å sikre en høy grad av informasjonsoverføring. **Informasjonsprosesser:** Viser at aktører ikke har tenkt over konsekvensene av å gå over til fattigere kommunikasjonskanaler.
Høyland Elisabeth	*Sikkerhetsbetraktninger ved implementeringen av integrerte operasjoner i norsk petroleumsvirksomhet.(Maste oppgave)*	**Ny teknologi:** Beskriver endringene i IO teknologien **Sikkerhetskultur**: Beskriver tillitten mellom partene offshore/onshore **Informasjonsprosesser:** Viste at det har vært situasjoner hvor informasjonen har blir misforstått og ført til uønskede hendelser. **Informasjonsprosesser**: Beskriver at IO vil gå fra rike til fattigere kommunikasjonskanaler til å overføre informasjonen
Haaland Geir:	*Integrerte operasjoner i V&M kontrakter. (Master oppgave)*	**Målkonflikter:** Illustrerer partene i norsk offshore virksomhet.