28.05.07

Kapittel 3

Sikrere fjerndrift med CRIOP

Stig Ole Johnsen
SINTEF
stig.o.johnsen@sintef.no

Mary Ann Lundteigen
NTNU
mary.a.lundteigen@sintef.no

Fjerndrift og eDrift/integrerte operasjoner er et relativt nytt driftskonsept der informasjons- og kommunikasjonsteknologi (IKT) benyttes for å effektivisere og forbedre driften av offshore-installasjoner. Med eDrift etableres nye arbeidsprosesser, roller og kommunikasjonsmønstre, noe som kan ha både positive og negative sider for risikoen på offshoreinstallasjonen. Dette kapitlet viser hvordan en eksisterende metode for verifikasjon og validering av kontrollrom, CRIOP[1], har blitt utvidet til å omfatte fjerndrift og eDrift slik at vi kan oppnå sikrere drift av offshoreinstallasjoner.

Introduksjon

eDrift beskriver en driftsform der informasjons- og kommunikasjonsteknologi (IKT) brukes for å øke samhandling og informasjonsutveksling uavhengig av fysisk lokasjon (OLF[2], 2003; OLF, 2006b). Et alternativt begrep som ofte benyttes for eDrift er ”integrerte operasjoner”. Fjernstøtte, fjernovervåkning og fjerndrift representerer ulike *grader* av eDrift, og beskriver hvilke *typer* aktiviteter (støtte, overvåkning, styring) man velger å flytte fra installasjonen til en annen lokasjon i oljeselskapets egen organisasjon eller hos leverandøren. Mange oljeselskaper velger å etablere egne kontroll- eller støttesentre på land, der man har tilrettelagt IKT-løsninger for direkte samhandling med offshoreinstallasjonen. Enkelte selskaper som leverer tjenester i drifts-fasen, for eksempel leverandører av prosess- og styringssystemer, har også etablert egne støtte-sentre som gjør at de kan utføre oppgaver fra støttesentre på land.

Innføring av eDrift berører organisering, rollefordeling og arbeidsprosesser både lokalt på offshoreinstallasjonene og på land hos oljeselskapene og hos sentrale leverandører. Ut fra et HMS-perspektiv handler eDrift om muligheten for forbedret HMS, mens mye av drivkraften for

[1] CRIOP ~ Crisis Intervention and Operability Analysis, www.criop.sintef.no
[2] OLF ~ Oljeindustriens Landsforening.

eDrift har vært økt inntjening, reduserte driftskostnader, høyere utnyttelsesgrad av reservoarene og mer effektiv støtte av drift og vedlikehold, ref. St.meld. nr. 38 (2003-2004)[3]. For marginale felt og modne felt der produksjonen er på vei ned, er eDrift en viktig faktor for å få til mer lønnsom drift og muligheten for å bevare arbeidsplasser. Praktiske eksempler på hvordan HMS, effektivitet og lønnsomhet kan forbedres ved innføring av eDrift kan være:

- Personell fjernes fra farekilden offshore og flyttes til land, noe som også leder til redusert risikoeksponering i forbindelse med reiser offshore.
- Driftsmiljøer på land kan overvåke brønner og produksjon i sann tid, og påvirke parametere for driftsoptimalisering, noe som kan lede til store gevinster. (Vi har eksempler på økt avkastning med 5 - 10 % fra feltene).
- Med tilgang til data på land for sitt utstyr kan leverandører i økende grad bidra med problemløsning og overvåkning uten å være fysisk tilstede på installasjonen.
- Bedre IKT-verktøy og høyere overføringskapasitet mellom offshore og land, vil kunne gi raskere tilgang til relevante data for styring, og forbedret samarbeid mellom hav og land. (Erfaring har vist at mange prosjekter har ledet til bedre samarbeid og forståelse mellom hav og land).
- Eksperter som det er knapphet på, for eksempel reservoaringeniører og utstyrseksperter, vil kunne følge opp flere installasjoner eller operasjoner enn tidligere fordi de involveres uten å måtte reise fysisk ut til installasjonen.

For mange oljeselskaper vil eDrift innføres gradvis. Etter hvert som man får tillit og erfaring med bruk av IKT-verktøy og nye arbeidsprosesser, kan man velge å flytte flere oppgaver fra installasjonen til land, og gå over fra fjernstøtte/fjernovervåkning til mer aktiv fjernstyring. En annen faktor som vil være viktig for graden av eDrift, er om installasjonen er tilrettelagt for fjernstyring. På mange eldre installasjoner kan det være svært vanskelig.

I dette kapitlet presenteres utvikling av en sjekkliste for bruk ved omlegging til eDrift, med utgangspunkt i relevant teori og erfaring. Sjekklisten reflekterer det man ofte omtaler som ”beste praksis”, det vil si en praksis som bygger på anerkjente metoder og erfaringer, se Johnsen m.fl. (2004). Sjekklisten er tatt inn i, og har vært en del av CRIOP-metoden fra 2004.

CRIOP er en anerkjent metode for å adressere sikkerhetsrelaterte forhold ved utforming og drift av kontrollsentre offshore, og den dekker både design- og driftsfasen. Metoden har vært benyttet på norsk kontinentalsokkel siden 1990, og har vært gjenstand for flere større oppdateringer fra 2003. Kjernen i CRIOP er analyser vha. sjekklister og scenarier. CRIOP-analysene gir innspill til mulige utfordringer som kontrollrommene må håndtere, og kan brukes som en arena for læring og samhandling for designere, ledere, driftspersonell og aktører fra underleverandører og andre involverte i eDrift.

Tradisjonelt har CRIOP vært anvendt for *lokale* kontrollrom i ulike størrelser, det vil si ifra større sentrale kontrollrom på land eller offshore, til mindre styrerom som borehus og kranhus. I forbindelse med eDrift bør CRIOP benyttes for de distribuerte kontrollrommene og samhandlingen mellom kontrollrommene som etableres offshore og på land.

[3] St.meld. nr. 38 (2003-2004). Om petroleumsvirksomheten.

Definisjoner knyttet til eDrift

Som vi allerede har sett, finnes det mange ulike begreper knyttet til eDrift. De vanligste beslektede uttrykk er: Integrerte operasjoner, eDrift, Smart Drift, Smart Field, Real Time Operations og ifield (OLF, 2006b).

eDrift og integrerte operasjoner
I praksis har integrerte operasjoner (St.meld. nr. 38 (2003-2004); OLF, 2006b) og eDrift (OLF, 2003) blitt synonyme begreper. Dette er driftskonsepter der informasjonsteknologi brukes til å endre arbeidsprosesser, forbedre beslutningstaking, gjennomføre fjerndrift og å flytte funksjoner fra offshore til land. (I dette kapitlet brukes begrepet eDrift gjennomgående, da CRIOP bruker eDrift konsekvent).

Fjernstøtte, fjernovervåkning, fjernstyring og fjerndrift representerer alle ulike implementeringer av eDrift. Det finnes få kilder som definerer disse begrepene mer konkret. Nedenstående fortolkninger er hentet fra artikkelen til Johnsen og Lundteigen m.fl. (2005b).

Fjernstøtte
En vanlig fortolkning er at fjernstøtte er fjernassistanse uten inngrep i de operasjoner som foregår på installasjonen. Fjernstøtte initieres ved behov for å gi nødvendig støtte ved utstyrssvikt, komplekse boreoperasjoner, etc. Ulike informasjons- og kommunikasjonsteknologier kan benyttes, for eksempel videokonferanser og telefoni, samt fjerntilgang til installasjonens datanettverk og utstyr.

Fjernovervåkning
Fjernovervåkning skjer på kontinuerlig basis og kan innebære at en driftsavdeling på land har ansvar for å overvåke driftsmessige parametere og lage forslag til brønnoptimalisering. Det totale driftsansvaret ligger lokalt på installasjonen.

Fjernstyring
Fjernstyring går et steg videre, og beskriver en situasjon der hele, eller deler av driftsansvaret er flyttet fra installasjonen til en annen lokasjon. Ved besøk til installasjonen, overtar installasjonen driftsansvaret lokalt så lenge besøket varer. I noen tilfeller er det ikke aktuelt å ha et kontrollrom lokalt, for eksempel for et subsea anlegg. I dag er fjernstyrte installasjoner normalt ubemannede.

Fjerndrift
Fjerndrift gjelder hele installasjonen, selv om installasjonen kan være bemannet. Driftsansvaret er i sin helhet flyttet fra installasjonen til en annen lokasjon.

Viktigere enn generelle definisjoner og begreper er at man oppnår en felles forståelse for bruk av begrepene, og at dette kommuniseres på en tydelig måte.

Generelle risikofaktorer ved innføring av eDrift

Innføringen av eDrift med IKT-verktøy for å øke samhandlingen og i noen tilfelle flytte funksjoner, gir to umiddelbare effekter:

1. Nye arbeidsprosesser og rollefordelinger tilpasset den nye driftsformen
2. Informasjonssikkerhet får en mye større betydning enn det tradisjonelt har hatt.

Nye arbeidsprosesser og nye rollefordelinger må etableres og verifiseres for å håndtere normalsituasjoner og driftsavvik. I mange tilfeller representerer ikke IKT-verktøyene *ny* teknologi som sådan, men organisasjonene kan være uten tidligere erfaring med bruken av dem. For at IKT-verktøy kan taes i bruk på en sikker og effektiv måte, er det nødvendig med grundig planlegging, involvering og læring gjennom hele prosessen. Å ivareta menneskelige faktorer representerer store utfordringer (Henderson m.fl., 2002). Enkelte studier viser at ca. 60 - 80 % av uønskede hendelser skyldes menneskelige feil eller menneskelige forhold (Chadwell m.fl., 1999). Når personer skal samhandle uten å være tilstede på samme plass, og uten at alle er nær selve hendelsen (for eksempel et utstyrshavari eller håndtering av en kritisk operasjon), 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 uttilsiktede hendelser.

Tradisjonelt har styre- og sikkerhetssystemer (SAS[4]) på en produksjonsinnretning vært isolert fra omverdenen. Med innføring av IKT for å øke samhandling, økes også behovet for lesetilgang, og i noen tilfeller skrivetilgang til disse kritiske systemene. Som et resultat blir styre- og sikkerhetssystemene mer sårbare overfor eksterne tilsiktede og utilsiktede trusler som kan skade programvare og medføre utilsiktede aksjoner på installasjonen.

Vår hovedhypotese er at scenarioanalyser og sjekklister kan benyttes for å skape nødvendig oppmerksomhet om sikkerhet og sårbarhet hos designere, prosjektansvarlige, brukere og andre direkte involverte i forbindelse med innføring og bruk av eDrift.

Den nye versjonen av CRIOP, med sjekklister og scenarier, fokuserer på å avdekke sikkerhetsmessige svakheter ved omlegging til eDrift, og da med tanke på både prosessikkerhet og informasjonssikkerhet. De sikkerhetsmessige svakheter som avdekkes, bør gi et godt utgangspunkt for å definere scenarier hvor en kan teste samhandlingen mellom flere aktører under eDrift.

Avgrensning og strukturering av eDrift sjekklistene

Det har vært mye diskusjon om eDrift på norsk sokkel, og det har vært mange utfordringer med å gjennomføre endringsprosjektene. Ulik måloppfattelse fra de som har blitt påvirket har vært en hyppig nevnt årsak til dette. Uklare mål har skapt usikkerhet og motstand i organisasjonene. I en del prosjekter har teknologifokuset kanskje vært for stort på bekostning av menneskelige og organisatoriske faktorer (Andersen, 2006). Det er derfor viktig med en god prosjektinitiering, der man etablerer klare mål og har fokus på samspillet mellom menneske, teknologi og organisasjon.

Å innføre eDrift betyr en læringsprosess for alle som utfører drift og vedlikehold, enten i et oljeselskap eller hos leverandører. Det er nødvendig å skape balanse mellom de muligheter ny teknologi gir, og det organisasjonene er i stand til å forstå og beherske. Det er derfor viktig at en løpende verifiserer at nytt driftskonsept gjennomføres i henhold til nye prosedyrer og nye

[4] SAS – Safety and Automation System, samlebetegnelse på kontroll og sikkerhetssystemer

arbeidsprosesser, slik at HMS (som innbefatter prosessikkerhet og informasjonssikkerhet) ivaretas på en forsvarlig måte.

Ut fra det foregående, har vi gått ut fra at overgang til eDrift kan struktureres og følges opp etter følgende tre hovedsteg:

1. Prosjektinitiering: Avklare målsetning og omfang av nytt driftskonsept. (Det er bl.a. viktig at endringsprosessen har et klart definert hovedmål).
2. Endringsprosess: Planlegge og implementere nytt driftskonsept som sikrer løpende læring underveis.
3. Operasjon med nytt driftskonsept: Løpende verifisering av et tilfredsstillende HMS-nivå.

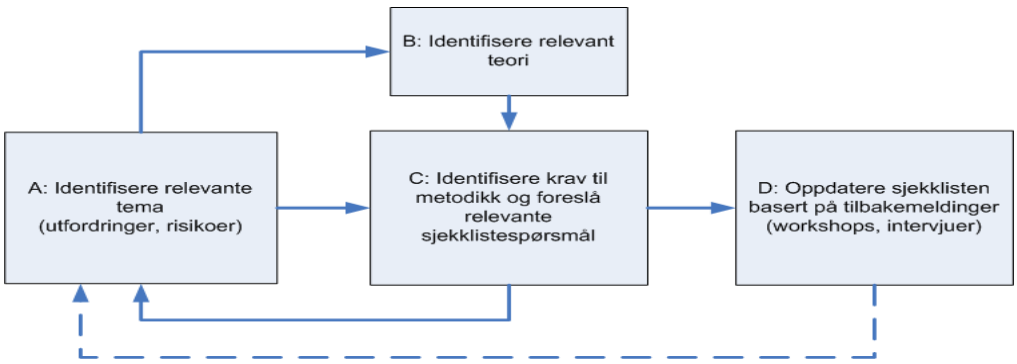
Sjekklisten for eDrift er derfor blitt utformet på basis av den ovenstående strukturen, i første omgang på et noe overordnet nivå.

Det er viktig å avklare mulig risiko knyttet til eDrift så tidlig som mulig av flere årsaker. For det første vil dette tydeliggjøre hvor fokus bør legges i forhold til kompetanse, trening og verktøy i den videre gjennomføringen. For det andre innebærer overgang til nye driftsformer alltid en risiko for ikke planlagte endringer/tiltak, som kan lede til nye kostnader og forsinkelser. Erfaring viser at kostnadene ved ikke planlagte endringer øker nesten eksponentielt etter hvert som prosjektet skrider frem (Boehm 1976; Samset 2001).

Utvikling av eDrift sjekklisten

Utviklingen av sjekklisten er utført i fire faser, slik figur 1 viser:

Fase A: Identifisere utfordringer og risiko knyttet til eDrift.
Fase B: Gjennomgå relevant teori.
Fase C: Utarbeidelse av eDrift sjekkliste.
Fase D: Innhente erfaringer fra bruk av eDrift sjekkliste.



Figur 1. Metodikk for utvikling av ny CRIOP eDrift sjekklister.

Utfordringer og risiko knyttet til eDrift (fase A)

Som input til å foreslå spørsmål til eDrift sjekkliste valgte vi å studere hvilke utfordringer eDrifts-relaterte prosjekter har erfart. I tillegg til å gjennomgå rapporter utarbeidet av olje-industrien selv (OLF, 2003; OLF, 2006b), har vi også gjennomført intervjuer og samtaler med sentrale aktører innenfor industrien (Johnsen og Lundteigen, 2004; Johnsen og Lundteigen m.fl., 2005a).

Følgende utfordringer er blitt identifisert:

- *Mange ulike begreper og definisjoner:* Det benyttes mange ulike begreper og definisjoner innenfor eDrift, noe som kan medføre kommunikasjonsproblemer, misforståelser, frustrasjon eller usikkerhet i endringsprosjekter.
- *"Politisk" endringsprosess:* De som omfattes av et nytt driftskonsept vil ofte ha ulike mål og interesser. Endringsprosessen kan lett trekkes i mange retninger om det ikke er en tydelig ledelse som håndterer de politiske sidene av endringsprosjektet på en god måte.
- *Behov for nye arbeidsprosesser:* eDrift gir mulighet for å jobbe sammen på en ny måte. Det er viktig å utvikle nye arbeidsprosesser som tydeliggjør ansvar, roller og samarbeidsformer både under normal drift og i avvikssituasjoner. Roller og oppgaver som tidligere ikke var så tydelige i driftsmiljøene, slik som IKT-sikkerhet og sårbarhet, må få en rolle i de nye drifts-relaterte arbeidsprosessene.
- *Økt kompleksitet i samhandling*: Nye arbeidsprosesser der aktører som ikke tidligere har samarbeidet så tett, eller der aktører som tidligere samarbeidet på samme fysiske sted, nå må kommunisere fra ulike lokasjoner, medfører at selve samhandlingsformen vil oppleves som mer kompleks. En utfordring er å forsikre seg om at alle som samarbeider, har samme situasjonsforståelse, og at løsninger diskuteres ut fra denne. Mangel på felles situasjons-forståelse var for eksempel medvirkende til Longford-ulykken i Australia (1998), der to menneskeliv gikk tapt og gassforsyningen til staten Victoria var borte i to uker. Her hadde kunnskap og ekspertise blitt sentralisert bort, mens operasjonell drift ble utført lokalt, noe som medførte manglende situasjonsforståelse når noe uventet skjedde (Hopkins, 2000).
- *Økt avhengighet av IKT-verktøy:* Ved eDrift blir man mer avhengig av IKT-verktøy. Tap av informasjons- og kommunikasjonskanaler for beslutningstakere som ikke er fysisk tilstede på installasjonen, kan være svært kritisk og kan være med på å initiere eller eskalere driftsavvik. En utfordring er derfor å sikre at IKT-løsninger er tilstrekkelig robuste og sikre, at brukere har tilstrekkelig kompetanse for å ivareta IKT-sikkerhet og sårbarhet, og at nødvendige prosedyrer etableres for å beskytte kontroll- og sikkerhetssystemer.
- *For stort teknologifokus:* I en del prosjekter oppleves teknologifokuset å ha vært for stort på bekostning av menneskelige og organisatoriske faktorer (Andersen, 2006).

De nevnte utfordringer har vært basis i diskusjonene vi har hatt med prosjektledere, spesialister, ingeniører og ledere i oljeselskaper, prosjekteringsselskaper og forskningsinstitutt (Johnsen og Lundteigen m.fl., 2005a). Utfordringene ivaretas gjennom følgende krav til prosessen ved innføring av nytt driftskonsept:

- Velge mekanismer som sikrer en *god* endringsprosess. Med "god" menes i denne sammen-heng en prosess som håndterer situasjoner hvor ulike aktører har ulike interesser, uten at dette går på bekostning av viktige målsetninger for HMS.
- Sikre at nye IKT-verktøy og nye arbeidsprosesser gir felles situasjonsforståelse og nødvendig samhandling under normal drift og i avvikssituasjoner.

- Sikre at IKT-verktøy tilfredsstiller nødvendige krav til informasjonssikkerhet, at nødvendige prosedyrer etableres og at nødvendig opplæring blir ivaretatt.

Relevante teori (fase B)

Det finnes i dag mye litteratur som er relevant for større endringsprosjekter, som eksempelvis innføring av eDrift. I det følgende har vi valgt å se på teori innenfor de utfordringer som ulike sektorer har erfart ved innføring av eDrift. Teorien er knyttet opp til fire områder som vil være viktige for å gjennomføre en sikker og god endringsprosess:

- Felles forståelse av mål og begreper
- Gode og motiverende endringsprosesser
- Valg av løsninger som bidrar til felles situasjonsforståelse
- Ivaretakelse av informasjonssikkerhet

Felles forståelse av mål og begreper

Kotter (1996) og Karp (1996) peker på viktigheten av å ha klare mål for endringsprosessen, og at mål bør utarbeides i samarbeid med representanter fra alle involverte aktører. Det er viktig at målene omfatter HMS-forhold for så vel endringsprosessen, som for det nye driftskonseptet, etter at det er innført. Med felles målforståelse og felles begreper vil sannsynligheten for misforståelser og tap av tillit reduseres.

Gode og motiverende endringsprosesser

En større endringsprosess i et drifts- og vedlikeholdsmiljø er krevende fordi det er mange aktører som blir berørt, både innenfor olje- og gasselskapene og hos leverandører av tjenester og utstyr. Endring kan også være en stor utfordring dersom inntjening og overskudd er høyt, og eksisterende goder er betydelige i tillegg til at man ikke ser nødvendigheten av raske endringer. I en slik situasjon må man navigere mellom ulike aktørers særinteresser samtidig som nye samarbeidsformer skal utvikles.

I Kotter (1996) og Pinto (1996) finner man en diskusjon om hvordan krevende endringsprosesser i politiske klima kan gjennomføres. Med ”politisk klima” mener vi forhold hvor det er uenighet og interessekonflikter mellom de ulike aktørene, som eksempelvis ansatte og ledelse, når det gjelder mål og virkemidler. Kotter foreslår en syvtrinns prosess for å gjennomføre en større endring i et politisk klima:

1. Skape en felles forståelse for at en endring er nødvendig (f.eks å øke sikkerheten, bevare arbeidsplasser)
2. Etablere en styringsgruppe med de sentrale aktørene som får et ansvar for endringene (slik at tunge beslutningstakere blir involvert med bl.a. tillitsvalgte)
3. Utvikle en visjon og en strategi for den nye driftsformen som kommuniseres godt
4. Gi tilstrekkelig myndighet til prosjektets ledelse og lokale ”propeller”/ansatte

5. Informere om gevinster, dele erfaringer og fortelle gode ”historier”
6. Bruke de gode erfaringer som inspirasjon til å skape mer endring
7. Forankre nye arbeidsformer lokalt i organisasjonskulturen.

Pinto har fokusert spesielt på politiske prosesser. Han understreker betydningen av å analysere ulike aktørers interesser på et tidlig stadium, og bruke dette til å finne mål og tema man kan enes om for å redusere et mulig konfliktnivå. En aktøranalyse anbefales gjennomført av Pinto.

HSE[5] (2003) har systematisert erfaringene fra sikkerhetsarbeidet i endringsprosesser, og fokuserer på:

1. *Få en klart definert organisering og ansvarsdeling:*
   Så tidlig som mulig bør man få på plass en klart definert organisering av endrings-prosjektet, et klart budskap og roller og mandat både innenfor prosjektet og i eksisterende organisasjon. Videre bør det etableres nødvendige rutiner for endringshåndtering, plan for kommunikasjon og inkludering av berørte organisasjoner.
2. *Gjennomføre risikoanalyse:*
   Det bør gjennomføres en risikoanalyse som dekker alle berørte parter og alle organisatoriske endringer. Det bør vurderes hvordan eksempelvis kompetanse, opplæring og arbeidsbelastning blir ivaretatt i den nye driftsformen. Risikoanalysen bør innbefatte ulike scenarier, både innenfor normal drift, avvikssituasjoner og kritiske operasjoner.
3. *Implementere og overvåke endringer:*
   Det er viktig å bevilge nok ressurser for å gjennomføre endringen på en sikker måte. All identifisert risiko bør overvåkes i forkant og i etterkant av ny driftsform, samt gjøre vurderinger av hvordan endringer har vært håndtert.

Valg av løsninger som bidrar til felles situasjonsforståelse

Kommunikasjon via IKT-verktøy i stedet for direkte kommunikasjon mellom mennesker, vil kunne påvirke hvordan de ulike aktørene opplever en driftssituasjon. Dette kan medføre utfordringer når store driftsavvik oppstår. Driftsavvik vil ofte ha nye elementer som man ikke har direkte erfaring med fra før, og beslutninger kan være tidskritiske for å hindre videre eskalering. Når viktige beslutningstakere eller fagekspertise ikke er nær 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.
Henderson m.fl. (2002) har studert menneskelige faktorer i fjernstyrte prosessanlegg. Han har funnet ut at følgende forhold er viktige når man skal samarbeide gjennom bruk av IKT-verktøy, i stedet for direkte kommunikasjon:

- Trene på felles situasjonsforståelse og avklaring av at riktige antagelser er gjort av alle involverte
- Sikre tilstrekkelig kunnskap om ulike driftssituasjoner til alle som skal håndtere disse
- Felles forståelse av hverandres roller og ansvar
- Felles kunnskap om nødvendige prosedyrer som gjelder for ulike driftssituasjoner
- Felles kulturell forståelse, det vil si felles mål, holdninger og normer.

[5] HSE ~ Health & Safety Executive, Storbritannia.

De ovennevnte tema er viktige elementer for å sikre at alle som samarbeider har samme bilde (eller modell) av situasjonen, slik at de kan treffe de riktige beslutningene sammen.

I forkant av den tidligere omtalte Longford-ulykken hadde man flyttet fagstøttefunksjoner fra Longford til hovedkontoret. Den nye organisasjonsformen medførte at kommunikasjonen og situasjonsopplevelsen ble ulik for de som satt på anlegget og de som var flyttet til hovedkontoret. Ulykkesgranskningen avdekket at manglende felles situasjonsforståelse ga uheldige prioriteringer, som igjen var med på å bidra til at ulykken inntraff. En del lærepunkter fra denne ulykken kan dermed være viktig også for innføringen av eDrift, for eksempel:

- HAZOP[6]-analyser eller tilsvarende, bør benyttes for å kartlegge hva som kan gå galt, slik at man i forkant kan trene på å håndtere uønskede situasjoner som lokale operatører ikke har forutsetninger for å forstå.
- Alle aktører som har en rolle i problemløsning, enten det er utstyrsrelatert eller prosessrelatert, bør utarbeide prosedyrer for å håndtere driftsavvik og trene på det.
- Man bør sikre at man har rask tilgang til ekspertise på prosess og utstyr som kan håndtere en normalisering av driftsavvik. God fagmessig ledelse bør prioriteres.
- Det er viktig at alarmsystemene gir riktig og prioritert informasjon til aktørene, slik at man kan konsentrere seg om de viktigste problemstillingene først.

Ivaretakelse av informasjonssikkerhet

Samhandling på tvers av fysiske lokasjoner skaper større avhengighet av IKT-verktøy. Sikkerhetsbegrepet er dermed ikke bare begrenset til prosessikkerhet, men også informasjonssikkerhet. Feil kan oppstå i styre- og sikkerhetssystemene dersom ikke nødvendige prosedyrer er på plass for å kontrollere og styre tilgang til disse systemene. Når IKT-systemene åpnes opp for ekstern lese-, og eventuelt skrivetilgang, blir styre- og sikkerhetssystemer mer sårbare for angrep fra ”hackere”. Informasjonssikkerhet blir derfor viktig å håndtere innenfor eDrift.

Flere standarder gir krav og retningslinjer for hvordan informasjonssikkerhet kan håndteres. ISO 17799 (Nå ISO/IEC 27002) dekker mange krav til IKT som er relevante for eDrift sjekklisten. Denne standarden har dermed vært en viktig referanse.

Utarbeidelse av eDrift sjekkliste (fase C)

Fra å være rettet mot tradisjonelle kontrollrom, skal nå også CRIOP-metoden med eDrift sjekkliste kunne håndtere fremtidens kontrollsentre. Fremtidens kontrollsentre vil skille seg fra tradisjonelle kontrollrom på flere måter:

- Kontrollsentrene vil ha tilgang til ny teknologi og avanserte IKT-verktøy
- Organisasjonsendringer og outsourcing vil øke, noe som gjør at endringsledelse blir en viktig aktivitet
- Kontrollsentre trenger ikke å ligge i nærheten av prosessanlegget

[6] HAZOP ~ Hazard and Operability Analysis.

- Kontroll og oppfølging kan skje fra ulike geografiske steder, flere aktører vil ha tilgang til driftsrelatert informasjon i sann tid og være aktive
- Større krav til å være proaktiv, kontinuerlig optimalisering for å få mest mulig ut av feltet og fokus på driftsstabilitet. Drift vil skje 24 timer, 7 dager i uka.

Utkast til sjekklistespørsmål er blitt utarbeidet med utgangspunkt i teori, samt kartlagte utfordringer og risiko når det gjelder innføring av eDrift. Deretter er det gjort grundige oppdateringer etter høringsrunder i intervjuer og møter. Den komplette sjekklisten er vist i tabell 1. Til hvert sett av spørsmål er det gitt en beskrivelse av formålet med spørsmålene. Når det i spørsmålene henvises til interessenter, siktes det til de som berøres av omlegging til eDrift, det vil si ledelse på ulike nivå, driftspersonell, vedlikeholdspersonell, IKT støttepersonell og fagforeningsrepresentanter.

Sjekklisten for eDrift er inndelt i fire temaområder, tilsvarende den inndelingen som er gjort i teorigjennomgangen:

- Felles forståelse av mål og begreper innenfor eDrift
- Tilrettelegge for en god endringsprosess
- Tilrettelegge for felles situasjonsforståelse hos aktører som er fysisk spredt
- Håndtere informasjonssikkerhet i ny samarbeidsform

Erfaringer fra bruk av eDrift sjekkliste (fase D)

CRIOP med eDrift sjekklisten har vært utprøvd på to eDrift installasjoner og den har blitt justert etter diskusjoner med personer som har erfaring med eDrift i følgende sammenhenger:

- Fjernstyring av et kjemisk prosessanlegg i Norge, fra en sentral i Sverige
- Fjernstøtte av bore- og brønnoperasjoner
- Fjernstyring av offshore installasjon, fra annen offshore installasjon
- Kontrollromsoperatør offshore som har benyttet samhandlingsrom mot eksperter på land.

Tilbakemeldingen på spørsmålsstillingen har vært positiv. Spørsmålene fyller et behov som ikke har vært dekket på en god nok måte tidligere.

Følgende er bl.a. avdekket ved bruk av eDrift sjekkliste:

- Målene for innføring av eDrift har vært uklare, og aktørene har til tider lite tillit til endringene
- Ingen systematisk risikoanalyse har vært gjennomført av de nye eDrifts-konseptene for å avdekke nye risikomomenter og å sette inn tiltak
- Ingen systematisk scenarioanalyse har vært gjennomført mellom flere organisasjoner som utfører eDrift eller fjerndrift, for å finne kritiske utfordringer med samhandlingen, eller for å trene på samhandling
- En har ikke spredt informasjon om uønskede IKT-hendelser på en slik måte at de som sitter i sentralt kontrollrom, har god oversikt over dem.

Tabell 1. eDrift sjekkliste.

Felles forståelse av mål og visjoner	**Formål**
1. Er det etablert en felles visjon og et felles sett av mål for omlegging til eDrift, som har fått aksept hos relevante interessenter? 2. Er det oppnådd en felles forståelse av hvorfor endringene er nødvendige? 3. Er oppnådd en felles forståelse av graden av endring, og er dette nøyaktig nedskrevet? Graden av endring bør dekke hvilke hovedfunksjoner som eventuelt blir berørt av fjernstøtte eller fjerndrift, og hvilke nye verktøy og samarbeidsformer som er nødvendig.	Tilrettelegge for positivt samarbeidsmiljø, der alle interessenter erkjenner hvorfor en omlegging til eDrift er nødvendig, hvilke mål og visjoner som er satt for den aktuelle omleggingen, og hva disse endringene innebærer.
Tilrettelegge for en god endringsprosess	**Formål**
4. Er alle mål og visjoner tilstrekkelig formidlet i organisasjonen? 5. Er man sikker på at alle interessenter er blitt identifisert? 6. Er det identifisert hvem (enkeltpersoner eller styringsgruppe) som er ansvarlig for innføringen av eDrift? 7. Er det laget en kommunikasjonsplan som sikrer at alle interessenter blir holdt orientert om status og fremdrift? 8. Kommer fordeler og gevinster med den nye drifts-formen klart frem for alle i kommunikasjonsplanen?	Tilrettelegge for et godt samarbeidsmiljø og en aktiv deltagelse fra alle interessenter, for å realisere visjoner og mål. Det er viktig at man verifiserer at alle interessenter er identifisert, slik at man har full oversikt over hvilke miljøer som blir berørt, både av formelle årsaker og på grunn av de tekniske omleggingene. Et godt samarbeids-klima er også avhengig av at alle formelle prosesser som kreves ved organisasjonsendringer, blir igangsatt på riktig tidspunkt.
9. Er delmål identifisert og en plan for hvordan status for disse kan kommuniseres til organisasjonen?	eDrift representerer ofte en stor omlegging av måten å jobbe på. For økt motivasjon, og for å sikre at endringene skjer i ønsket retning, er det viktig å ha fokus på delmål.
10. Gjenspeiler nye prosedyrer og arbeidsprosesser de nye samarbeidsformene? 11. Er det etablert et program for trening og læring i nye samarbeidsformer og bruk av nye verktøy? 12. Er det etablert en arena (f.eks. et samarbeidsforum) der man kan diskutere erfaringer med de nye samarbeidsformene?	Tilrettelegge for at endringene blir tydelige i organisering, arbeidsprosesser og opplæring/-trening. eDrift vil på noen områder bety endret praksis for måten arbeidsoppgaver gjennomføres på.
13. Er en ansvarlig leder eller ledergruppe identifisert for endringsprosjektet? 14. Er det klare rutiner eller prosedyrer for hvordan endringsprosjektet skal ledes? 15. Håndterer endringsprosjektet både teknologi-utfordringer, organisatoriske utfordringer og menneskelige faktorer?	Et vellykket endringsprosjekt vil ofte avhenge av at prosjektet forankres hos organisasjonens ledelse. Dette er nødvendig for at prosjektet skal få fokus, at nødvendige beslutninger blir tatt og at fremdrift etterspørres.
16. Er det gjennomført en risikovurdering av ny driftsform? 17. Dekker risikoanalysen ulike scenarier, både knyttet til normal drift og avvikssituasjoner? 18. Er faktorer som arbeidsbelastning, kompetanse og menneskelige faktorer vurdert i risikoanalysen?	Sikre at risiko knyttet til den nye driftsformen er identifisert og håndtert.
19. Er det etablert en plan for hvordan identifisert risiko og tiltak følges opp og kommuniseres?	Sikre at identifisert risiko og kompenserende tiltak følges opp ved implementering og igangsetting av ny driftsform.
Tilrettelegge for felles situasjonsforståelse	**Formål**
20. Er nye (og eventuelt eksisterende) informasjons- og	Tilrettelegge for at informasjons- og kommunika-

kommunikasjonsverktøy tilrettelagt for at ulike samarbeidende aktører får samme situasjons-forståelse? 21. Er nye (og eventuelt eksisterende) informasjons- og kommunikasjonsverktøy tilrettelagt for at det tydelig går frem hvilke aktører som har hvilket ansvar og roller? 22. Er nye (og eventuelt eksisterende) informasjons- og kommunikasjonsverktøy tilrettelagt for at alle aktører har samme tilgang til styrende verktøy og prosedyrer? 23. Har alle som samarbeider felles forståelse av under-liggende kultur, som etterleving av prosedyrer, holdninger, atferd, etc.? 24. Har samarbeidende aktører fått trening i de nye samarbeidsformene, inkludert bruk av nye verktøy og prosedyrer? 25. Er det etablert en arena i driftsfasen av eDrift for å utveksle erfaringer og læring?	sjonsverktøy gir samarbeidende aktører den samme situasjonsforståelsen, opplevelse av nødvendige tiltak og samme forståelse av hvilke aktører som har hvilke oppgaver.
26. Har operatører fått trening i å samarbeide med sine støttefunksjoner, enten ingeniørtjenester i eget selskap eller eksterne selskaper? 27. Er det etablert en plan eller prosedyre for hvem som skal involveres i hvilke situasjoner?	Tilrettelegge for å ha tilgang på ressurser med nødvendig kjennskap til risiko knyttet til eDrift, og som kan gi driftsstøtte og vedlikeholdsstøtte.
Håndtere informasjonssikkerhet i ny samarbeidsform	**Formål**
28. Er det etablert rutiner for hvordan informasjons-sikkerhet ivaretas ved bruk av nye informasjons- og kommunikasjonsverktøy, og ved nye adgangs-muligheter til prosess- og styringssystemer? (ISO 17799 eller ISBR 104 fra OLF kan benyttes til dette formålet.)	Tilrettelegge for at informasjonssikkerhet blir ivaretatt. Økt grad av samhandling ved bruk av informasjons- og kommunikasjonsverktøy betyr at tidligere beskyttede systemer er mer sårbare.

eDrift sjekklisten har blitt verifisert og er støttet av den standardutvikling som har blitt gjennomført i etterkant, f.eks. retningslinjene utviklet av NISCC (2006), ISBR-sjekklistene utviklet av OLF (2006a), ISA SP99 "*Manufacturing and Control Systems Security*" (ISA, 2004; Teumim 2004). [7]

Spørsmålene i eDrift sjekklisten er relativt overordnede, og det kan være behov for mer detaljert oppfølging. Her kan sjekklister i OLF Guideline no. 104 *"Information Security Baseline Requirements for Process Control, Safety and Support ICT Systems"* (OLF, 2006a) være aktuelle å benytte. På www.checkit.sintef.no har vi dokumentert relevante standarder til bruk i dette arbeidet.

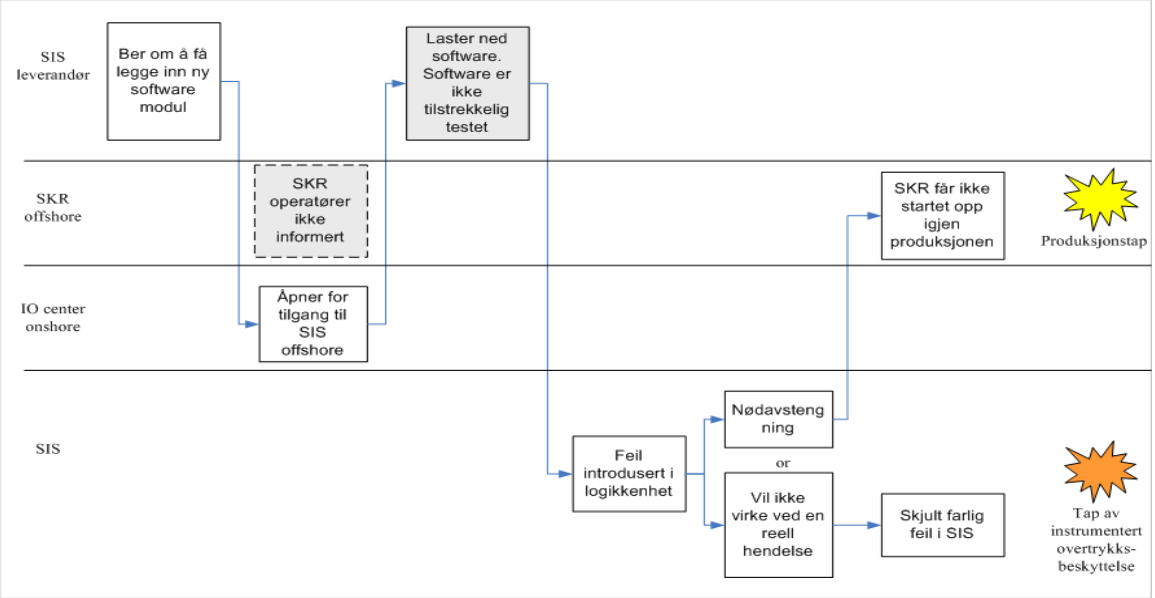
CRIOP sin webside[8] beskriver den nye CRIOP-versjonen med eDrift sjekkliste. Her kan brukere gi sine tilbakemeldinger, og disse vil bli tatt hensyn til ved fremtidige oppdateringer av sjekk-listen.

[7] NISCC ~ National Infrastructure Security Co-ordination Centre. ISBR ~ Information Security Baseline Requirements utviklet av OLF. ISA ~ Instrumentation, Systems and Automation Society.
[8] www.criop.sintef.no

Bruk av scenarioanalyser for å utforske fjerndrift

En CRIOP-analyse innebærer ikke bare gjennomgang av sjekklister, men også en analyse av ulike scenarier, både knyttet til normal situasjon og avvikssituasjoner. Viktige scenarier for eDrift kan være knyttet til arbeidsprosesser og aktiviteter der ulike aktører skal samarbeide på tvers av fysisk lokasjon ved hjelp av IKT-verktøy.

Et relevant eksempel kan være håndtering av fjerntilgang til det instrumenterte sikkerhets-systemet (på engelsk ofte forkortet SIS[9]). En SIS leverandør kan ved hjelp av etablerte rutiner og prosedyrer få adgang til SIS for å laste ned nye software-moduler. En slik aktivitet vil være beheftet med ulike risikomomenter, som eksempelvis feil i software, feil under nedlastning av software, mangel på informasjon til alle involverte aktører om pågående arbeid, etc. Aktuelle aktører som er involvert, er SIS-leverandør (programmerer), operatør i sentralt kontrollrom (SKR), driftsleder i senter for integrerte operasjoner (IO) og SIS.



Figur 2. Forenklet STEP[10]-diagram for scenarioanalyse for eDrift.

Scenarioanalyse kan gjennomføres på samme måte som beskrevet i CRIOP-metodikken. De ulike aktører kan settes opp i et STEP-diagram, se figur 2. Hvis man ønsker å studere mulig betydning av IKT-verktøy og styre- og sikkerhetssystemer, kan disse gis hver sin aktørrolle. Det er mange måter å sette opp et STEP-diagram. I CRIOP anbefaler man ofte å ta utgangspunkt i aktiviteter som innebærer en viss risiko, eller å trene på en kjent ulykke. I forhold til eDrift kan man trene på å gi fjerntilgang for leverandør for å legge inn en ny software-modul i sikkerhets-systemet. Dersom det gjøres feil, kan det lede til en uønsket hendelse, for eksempel at en sikker-hetsventil stenger utilsiktet, eller at feilen vil hindre fremtidig respons fra SIS ved en farlig hendelse. Man kan også ta utgangspunkt i en konkret ulykke, og kombinere elementer fra kjente ulykker i et scenario.

[9] SIS ~ Safety Instrumented System - sikkerhetssystemer som omfatter Nødavstegning, Brann&Gass.
[10] STEP ~ Sequentially Timed Events Plotting (Hendrick og Benner, 1987).

Den økende oppmerksomheten omkring eDrift har resultert i flere studier som diskuterer forholdet mellom eDrift og sikkerhet. Et eksempel er en masteroppgave gjennomført hos Statoil (Andersen, 2006), som omhandler samhandling mellom operatørselskapets sentrale kontrollrom, SKR på Snøhvit-anlegget, og leverandørens støttesenter for kontroll og sikkerhetssystemer. I studien kom man frem til at CRIOP (med tilhørende utvidelser for eDrift) er egnet som verktøy for å identifisere utfordringer med samhandlingen, samt til å forbedre sikkerheten mellom SKR og leverandørens støttesenter.

Konklusjoner

eDrift/integrerte operasjoner introduserer både menneskelige, organisatoriske og tekniske utfordringer. Organisatoriske og menneskelige utfordringer er knyttet til nye samarbeidsformer, nye arbeidsprosesser og nye rollefordelinger understøttet av IKT. Den viktigste tekniske utfordringen er å ivareta informasjonssikkerhet, spesielt driftsstabilitet når tradisjonelt atskilte styre- og sikkerhetssystemer åpnes opp for omverdenen.

En ny sjekkliste er utviklet innenfor CRIOP, med fokus på utfordringer innen menneske, teknologi og organisasjon (MTO) knyttet til eDrift. Tilbakemeldingene viser at denne utvidelsen dekker et behov industrien har. Den nye sjekklisten for eDrift vil oppdateres løpende, på lik linje med øvrige sjekklister innenfor CRIOP-metodikken.

Referanser

Andersen, S., 2006. *Improving safety through integrated operations*. Masteroppgave, NTNU, Trondheim

Boehm, B.W., 1976. Software engineering. *IEEE Transactions on Computers C-25(12)*, 1226-41.

Chadwell, G.B., Leverenz, F.L., Rose, S.E., 1999. *Contribution of Human Factors to Incidents in the Petroleum Refining Industry*. American Institute of Chemical Engineers 33rd Annual Loss Prevention Symposium. Houston, Texas.

Henderson, J., K. Wright and A. Brazier, 2002. *Human factors aspects of remote operation in process plants*. HSE Books, Sudbury, Suffolk.

Hendrick, K., Benner, L., 1987. *Investigating accidents with STEP*. Marcel Dekker, New York.

Hopkins, A., 2000. *Lessons from Longford.* The Esso Gas Plant Explosion. CCH, Sydney.

HSE, 2003 *Organisational change and major accident hazards.* Chemical Information Sheet no. CHIS7. http://www.hse.gov.uk/PUBNS/chis7.pdf

ISO/IEC 27002. *Information technology - Security techniques - Code for practice for information security management* (Tidligere ISO 17799) ISO/IEC, Geneva.

ISA, 2004. ISA SP99 "*Manufacturing and Control Systems Security*", omfatter:

- ANSI/ISA-TR99.00.01-2004. Security Technologies for Manufacturing and Control Systems.
- ANSI/ISA-TR99.00.02-2004. Integrating Electronic Security into the Manufacturing and Control Systems Environment.

Johnsen, S.O., Bjørkli, C., Steiro, T., Fartum, H. Haukenes, H., Ramberg, J., Skriver, J., 2004. *CRIOP: A scenario method for Crisis Intervention and Operability analysis*, Rapport nr. STF38 A03424 SINTEF, Trondheim.

Johnsen, S.O., Lundteigen, M.A., 2004. *Viktigste risiki og muligheter knyttet til eDrift og fjerndrift*. Presentasjon, seminar om HMS petroleum: Endring, Teknologi og Organisasjon. Sola Strandhotell, 22. september 2004.

Johnsen, S.O., Lundteigen, M.A., Albrechtsen, E., Grøtan, T.O., 2005a. *Trusler og muligheter knyttet til eDrift*. Rapport nr. STF38 A04433, SINTEF, Trondheim.

Johnsen, S.O., Lundteigen, M.A., Fartum, H., Monsen, J., 2005b. Identification and reduction of risks in remote operations of offshore Oil and Gas installations. In K. Kolowrocki, K. (ed.) *Advances in safety and reliability*. Proceedings from the European Safety and Reliability Conference -ESREL 2005. Leiden, Balkema, Vol. 1 (of 2), 957-964.

Karp, H.B., 1996. *The Change Leader*. Using a Gestalt Approach with Work Groups. Pfeiffer, San Diego, California.

Kotter, J.P., 1996. *Leading Change*. Harvard Business School Press, Boston.

NISCC, 2006. *Good Practice Guide*. Process Control and Scada Security. National Infrastructure Security Co-ordination Centre (NISCC), London. http://www.cpni.gov.uk/Products/guidelines.aspx

OLF, 2003. *eDrift på norsk sokkel - det tredje effektivitetsspranget*. Oljeindustriens Landsforening (OLF), Stavanger. http://www.olf.no

OLF, 2006a. *Information security baseline requirements for process control, safety and support ICT systems.* OLF Guideline no. 104. Oljeindustriens Landsforening, Stavanger. http://www.olf.no/hms/retningslinjer

OLF, 2006b. *Verdipotensialet for Integrerte Operasjoner på Norsk Sokkel*. Oljeindustriens Landsforening. Stavanger.

St.meld. nr. 38 (2003-2004). *Om petroleumsvirksomheten*. Olje- og energidepartementet.

Pinto, J.K., 1996. *Power and Politics in Project Management*. Project Management Institute (PMI), Sylva, North Carolina.

Samset, K., 2001. *Prosjektvurdering i tidligfasen*. Tapir Akademisk Forlag, Trondheim.

Teumim, D.J., 2004. *Industrial Network Security*. Instrumentation, Systems and Automation Society (ISA). http://www.isa.org/