2019:00361 - Åpen

Rapport

IKT-sikkerhet – Fjernarbeid og HMS

Intervjustudie

Forfattere
Lars Bodsberg, Tor Olav Grøtan, Martin Gilje Jaatun, Tor Onshus, Irene Wærø

SINTEF Digital
2019-04-05

SINTEF Digital
2019-04-05

SINTEF Digital
Postadresse:
Postboks 4760 Torgarden
7465 Trondheim
Sentralbord: 73593000

info@sintef.no

Foretaksregister:
NO 919 303 808 MVA

Rapport

IKT-sikkerhet – Fjernarbeid og HMS

Intervjustudie

EMNEORD:
Petroleum
Sikkerhet
Industrielle IKT-systemer

VERSJON
01

DATO
2019-04-05

FORFATTERE
Lars Bodsberg, Tor Olav Grøtan, Martin Gilje Jaatun, Tor Onshus, Irene Wærø

OPPDRAGSGIVER
Petroleumstilsynet

OPPDRAGSGIVERS REF.
Espen Seljemo

PROSJEKTNR
102018617

ANTALL SIDER OG VEDLEGG:
52+ vedlegg

SAMMENDRAG
Rapporten har som hovedmål å presentere kunnskap om bruk av fjernarbeid på sokkelen. Med fjernarbeid forstås endringer i industrielle kontroll- og sikkerhetssystemer på tvers av geografisk avstand. Rapporten belyser HMS-konsekvenser relatert til fjernarbeid på innretninger, landanlegg og borerigger. Hovedfokus er på arbeidsprosesser, prosedyrer og organisering. Rapporten gir også en oversikt over regelverk og retningslinjer på området.

Rapporten er spisset mot operasjonell teknologi, det vil si teknologi som støtter, kontrollerer og overvåker industriell produksjon, kontroll- og sikkerhetsfunksjoner.

UTARBEIDET AV
Lars Bodsberg

SIGNATUR

KONTROLLERT AV
Stian Antonsen

SIGNATUR

GODKJENT AV
Anita Øren

SIGNATUR

RAPPORTNR
2019:00361

ISBN
978-82-14-06832-0

GRADERING
Åpen

GRADERING DENNE SIDE
Åpen

Historikk

VERSJON	DATO	VERSJONSBESKRIVELSE
01	2019-04-05	Sluttrapport

SINTEF

Innholdsfortegnelse

BILAG/VEDLEGG

Sammendrag og konklusjoner

Petroleumstilsynet (Ptil) har som tilsynsmyndighet behov for oversikt om HMS-konsekvenser og IKT-sikkerhet ved fjernarbeid. Denne rapporten er en del av en større satsing innenfor området hos Ptil.

Det har lenge vært mulig å overvåke og arbeide på industrielle kontroll- og sikkerhetssystemer (industrielle IKT-systemer) fra land både hos operatørselskap og systemleverandører i petroleumsvirksomheten. Fjerntilgang er derfor ikke noe nytt, men søkelys på digitalisering gjør at det etableres nye arbeidsprosesser og samarbeidsformer mellom operatørselskaper og systemleverandører. Når en installasjon er innkjørt (f.eks. etter ett til to år), kan fagfolk med inngående kjennskap til industrielle IKT-systemer (2. linjepersonell), utføre fjernarbeid fra andre lokasjoner, gjerne i samarbeid med ansatte på installasjonen som har noe kunnskap om systemene (1. linjepersonell). Planlegging og utførelse av fjernarbeid kan skje med støtte fra systemleverandørers egne spesialister på systemene (3. linje personell).

Ved vurdering av IKT-sikkerhet er det viktig å skille mellom:
1. Fjernarbeid, hvor det gjøres arbeid på / endringer i industrielle IKT-systemer via fjerntilgang ("skrivetilgang")
2. Fjernstøtte, hvor industrielle IKT-systemer overvåkes og feilsøkes via fjerntilgang ("lesetilgang").

Hovedfokus i denne rapporten er på bruk av fjernarbeid. Rapporten er rettet mot operasjonell teknologi (OT), og ikke mot generell (administrativ) informasjonsteknologi (IT). Det er fokus på HMS-konsekvenser og felles situasjonsforståelse for sikker drift, samt IKT-sikkerhet ved fjernarbeid på innretninger til havs, landanlegg og borerigger. Rapporten gir også en oversikt over relevante standarder og retningslinjer som omhandler fjernarbeid.

Rapporten er basert på 14 gruppeintervju høst 2018/vinter 2019 med representanter fra operatørselskaper, boreselskaper og systemleverandører, samt gjennomgang av relevant litteratur, dokumenter fra operatør- og boreselskaper og SINTEFs generelle kompetanse og erfaring innenfor HMS og IKT-sikkerhet.

Omfang av fjernarbeid

Ifølge informantene er både innretninger, landanlegg og borerigger meget restriktive med å tillate programvareendringer i industrielle IKT-systemer fra andre steder enn på selve installasjonen. Fag- og driftspersonell som er intervjuet, er stort sett skeptiske til å tillate endringer på industrielle IKT-systemer via fjerntilgang. Noen av disse opplever nå et press for å øke omfanget av fjernarbeid og utføre endringer fra land.

Felles for innretninger, landanlegg og borerigger er et stort fokus på å teste endringer på land før de implementeres på installasjonen. Det er en utfordring at testing på land ikke får verifisert hele funksjonen til industrielle IKT-systemer, men er avhengig av at noen observerer hva som faktisk skjer med det fysiske utstyret.

Gruppeintervjuene avdekket at det er forskjellige strategier vedrørende fjernarbeid blant operatørselskaper. Dette kan knyttes til stor variasjon i størrelse på selskapene og alder for innretningene. Eksempelvis, hos ett selskap er strategien å samle eget personell for driftsstøtte i et operasjonssenter på land slik at ingeniørene kan betjene flere innretninger. Hos et annet selskap er strategien å beholde ingeniører offshore for å sikre tilstrekkelig lokalkunnskap om industrielle IKT-systemer, siden disse systemene blir stadig mer komplekse.

Administrasjon av fjernarbeid

Både innretninger, landanlegg og borerigger har spesifikke arbeidsprosesser med tilhørende tekniske løsninger for brukertilgang til industrielle IKT-systemer. Formålet er å bidra til en sikker identitets- og tilgangskontroll slik at kun personell med et definert behov får riktig tilgangsnivå. Ved beslutning om brukertilgang vurderes for eksempel behov for brukertilgang, hvilke systemer som man får tilgang til, hvilken type tilgang som trengs og varighet av tilgang.

Stadig flere systemer og innretninger krever personlig brukernavn/passord for fjernarbeid. På eldre systemer kan det være fellesbrukere og teknisk utfordrende å begrense ulike adganger til enkeltsystemer. Dermed er det krevende å finne tiltak som kan hindre uønskede handlinger fra en bruker som kun har fått tilgang til et mindre kritisk system.

Både innretninger, landanlegg og borerigger gir fjerntilgang som en del av arbeidstillatelsesprosessen, og de som skal gjennomføre fjernarbeid må inviteres inn av en ansvarlig i operatørselskapet. Arbeidsprosesser for sikker drift på en installasjon er de samme for fjernarbeid som for arbeid som gjennomføres på selve installasjonen, dvs. sikker jobbanalyse og systemer for arbeidstillatelser er helt sentralt både med og uten fjerntilgang.

HMS-konsekvenser for involverte i fjernarbeid

Når industrielle IKT-systemer blir mer komplekse, opplever enkelte 1. linjepersonell økt usikkerhet og ekstra behov for støtte fra spesialister. Spesielt telekomsystemer oppleves komplekse, og her kan det være opptil 30 forskjellige underleverandører. Informantene er enige om at fjernarbeid gir økt tilgang til spesialistkompetanse fra 2. og 3. linjepersonell.

Fjernarbeid på innretninger og rigger til havs muliggjør bedre arbeidstidsordninger for servicepersonell og ingeniører gjennom færre reiser ut til innretninger. Ingeniører hos operatørselskaper som i dag sitter på land, opplevde bedre arbeidsforhold og at det var mer sosialt å samhandle med spesialister på land. Samtidig presiserte noen at de opplevde økt arbeidstilfredshet hvis man fortsatt har mulighet til å ta noen turer til havs. Noen systemleverandører opplevde at den sosiale gevinsten ved å gjøre arbeidet til havs, uansett var begrenset fordi det er ikke alltid like enkelt å komme i god kontakt med offshorepersonell som serviceansatt med begrenset tid til rådighet på innretningen.

Bruk av egne rom for fjernarbeid gir ekstra mulighet for konsentrasjon om arbeidsoppgaver. Vaktordninger på land bør organiseres slik at personell har lokalkunnskap om innretningene. Når man har ansvar for flere installasjoner og industrielle IKT-systemer, kan det være utfordrende å forholde seg til de spesifikke teknologiske løsningene på en installasjon. En foreslått praksis er at man ikke arbeider på to forskjellige installasjoner samtidig. Vaktordninger med nattarbeid kan oppleves som usosialt for personell som må sitte i egne avlåste rom.

Felles situasjonsforståelse for sikker drift

Viktige faktorer som påvirker felles situasjonsforståelse og dermed sikkerhet ved fjernarbeid, er klare retningslinjer, god kommunikasjon og lokalkunnskap. God lokalkunnskap er viktig fordi applikasjoner aldri vil være helt standardiserte.

Ved økt fjernarbeid vil det kunne bli en utfordring at servicepersonell ikke er tett nok knyttet til den enkelte installasjon. Spesielt innenfor boring fremheves betydningen av lokalkunnskap om boreutstyret på boreriggen, og at fysisk tilgang til drift og operasjon er essensielt ved arbeid på industrielle IKT-systemer.

IKT-sikkerhet ved fjernarbeid

Programvareendringer fra land medfører ytterligere krav til IKT-sikkerhet for å beskytte mot tilsiktede og utilsiktede uønskede hendelser. Intervjuobjekter forventer at dagens løsninger for fjernarbeid vil bli videreført med enda større vekt på:

- Avlåste rom for fjernarbeid og rutiner for tilgangskontroll, samt forhåndsdefinerte og sterkt begrensede tilganger med klare kjøreregler for hvem som har brukertilgang.
- Bruk av "rensede PC-er" som kun benyttes ved arbeid på industrielle IKT-systemer.
- Krav til IKT-sikkerhet i kontrakter.
- Monitorering og overvåking og analyse av nettverk og tilkoblede systemer.
- Etterlevelse av etablerte retningslinjer og arbeidsprosesser.

SINTEFs anbefalinger til næringen

Med utgangspunkt i denne intervjustudien har SINTEF følgende anbefalinger til næringen:

- Fortsatt søkelys på tilgangskontroll og administrasjonsprosedyrer som også er brukervennlige for autorisert personell.
- Økt samarbeid mellom operatørselskaper og systemleverandører hvor de også regelmessig er fysisk samlet.
- Sterkere søkelys på krav til egnede rom for fjernarbeid, inklusive arbeidsforhold, vaktordninger, adgangskontroll, samt tiltak for å fremme nødvendig tankesett og bevisstgjøring for kritisk arbeid på industrielle IKT-systemer.
- Mer bruk av hardware-baserte informasjonsdioder for å unngå utilsiktet tilgang til spesielt kritiske industrielle IKT-systemer og derigjennom også gi enklere tilgang til de som kun behøver lesetilgang.

1 Innledning

1.1 Bakgrunn

Økt bruk og integrasjon av databaserte systemer har gitt endrete arbeidsforhold på norsk sokkel og på land, samt endrete kontraktsforhold mellom operatør og leverandør av servicetjenester. Når en installasjon er innkjørt (f.eks. etter ett til to år), kan fagfolk med inngående kjennskap til industrielle kontroll- og sikkerhetssystemer (industrielle IKT-systemer), overvåke og arbeide på disse systemene via fjerntilgang fra lokasjoner utenom selve installasjonen. Disse fagfolkene (2. linjepersonell) kan arbeide på systemene i samarbeid med ansatte på installasjonen som har noe kunnskap om systemene (1. linjepersonell), og med støtte fra systemleverandørenes egne spesialister på systemene (3. linje personell).

Industrielle IKT-systemer er sanntidssystemer som har høye krav til pålitelighet, tilgjengelighet og integritet for å unngå driftsforstyrrelser og tapt produksjon (driftssikkerhet). Driftsavbrudd kan i verste fall også føre til HMS-konsekvenser. Ut fra krav til teknisk sikkerhet er industrielle IKT-systemer utviklet for å være uavhengige av andre IT-systemer. IT-systemer derimot har i stor grad kommunikasjon med andre systemer. Dette betyr for eksempel at det historisk har vært forskjellig filosofi for håndtering av tilgangsrettigheter for IT- og industrielle IKT-systemer.

Petroleumstilsynet (Ptil) har som tilsynsmyndighet, behov for å ha oversikt over IKT-sikkerhet- og HMS-konsekvenser ved fjernarbeid; det vil si konsekvenser ved arbeid på / endringer i industrielle IKT-systemer via fjerntilgang på tvers av geografisk avstand. Denne studien og rapporten er en del av en større satsing innenfor IKT-sikkerhet. Sentrale problemstillinger for Ptil er:

- Hvordan håndterer industrien endringsprosesser knyttet til innføring av ny teknologi?
- Hvordan vil digitalisering påvirke HMS-forhold og risikostyring?

Ptil er underlagt Arbeids- og sosialdepartementet (ASD), og har myndighetsansvar for sikkerhet, beredskap og arbeidsmiljø i petroleumsvirksomheten. Ptil skal legge premisser for og følge opp at aktørene i petroleumsvirksomheten holder et høyt nivå for helse, miljø, sikkerhet og beredskap, og gjennom dette også bidra til å skape størst mulig verdier for samfunnet. Ptil skal drive informasjons- og rådgivningsvirksomhet overfor aktørene i petroleumsvirksomheten, samarbeide med andre helse-, miljø-, sikkerhets (HMS)-myndigheter nasjonalt og internasjonalt og bidra til kunnskapsoverføring på HMS-området i samfunnet generelt. Ptil skal gjennom eget tilsyn, og samarbeid med andre myndigheter med selvstendig ansvar på HMS-området, sikre at tilsynet med petroleumsvirksomheten blir ført på en helhetlig måte. Ptils myndighetsområde omfatter også tilsyn med sikkerhet, beredskap og arbeidsmiljø på petroleumsanlegg på land.

1.2 Målsetting

Hovedmålet for rapporten er å presentere kunnskap om bruk av fjernarbeid på innretninger til havs, landanlegg og borerigger i norsk petroleumsvirksomhet. Rapporten er rettet mot industrielle IKT-systemer som støtter, kontrollerer og overvåker produksjon og operasjon; det vil si mot operasjonell teknologi (OT).

Rapporten belyser HMS-konsekvenser, felles situasjonsforståelse for sikker drift og IKT-sikkerhet ved fjernarbeid. Hovedfokus er på bruk av fjernarbeid og ikke på tekniske løsninger. Rapporten gir også en oversikt over relevante standarder og retningslinjer som omhandler fjernarbeid.

Et viktig formål med rapporten er å motivere og bidra til økt kunnskap og innsats om IKT-sikkerhet blant personell i petroleumsnæringen som arbeider med industrielle IKT-systemer.

1.3 Arbeidsmetode

Rapporten er basert på intervju, workshop og gjennomgang av relevant litteratur og dokumenter, samt SINTEFs generelle kompetanse og erfaring innenfor IKT-sikkerhet og HMS-konsekvenser.

Det er gjennomført 14 gruppeintervju med representanter fra operatørselskaper, boreselskaper og systemleverandører i perioden november 2018 til januar 2019. (se oversikt Tabell 1) .

Tabell 1 Deltakere gruppeintervju

Selskap	Antall deltakere	Kompetanse og erfaring
Operatørselskap – offshore innretning	23	Ledere/systemansvarlige/fagpersonell fra operasjonssenter, automasjons-avdeling, boreavdeling, anleggsintegritet, IKT-sikring og IKT-infrastruktur.
Operatørselskap – landanlegg	9	Ledere/systemansvarlige/fagpersonell fra SAS, telekommunikasjon, elektrosystemer, fiskale målesystemer, automasjon, vedlikehold og modifikasjon.
Boreselskap	5	Ledere/fagpersonell innenfor boring, teknisk integritet og IT/OT.
Systemleverandør - innretning/landanlegg	7	Fagpersoner med lang erfaring fra leveranser og driftsstøtte til en rekke innretninger på norsk sokkel.
Systemleverandør - boreriggutstyr	6	Ledere/fagpersoner med lang erfaring innenfor kontrollsystemer, boresystemer, teknisk sikkerhet og driftsstøtte.

Flere av intervjuobjektene hadde lang erfaring fra petroleumsvirksomheten og kjente godt til løsninger og prosedyrer ikke bare i eget selskap, men også i en rekke andre selskaper og innretninger på norsk sokkel. Vårt datagrunnlag dekker derfor flere selskaper enn de selskapene som deltok i gruppeintervjuene.

Alle intervju er basert på en felles intervjuguide som har vært retningsgivende for intervjuene, men enkelte spørsmål har blitt utdypet underveis i intervjuet avhengig av hvilke tema informantene har løftet fram.

Det er gjennomført en halvdags workshop med til sammen 9 deltakere fra operatørselskaper, systemleverandører, Sjøfartsdirektoratet og Petroleumstilsynet.

All informasjon fra informanter er anonymisert i rapporten.

Generelt fikk vi gode tilbakemeldinger fra selskapene etter intervjuene, og signaler om at gruppeintervjuene var nyttige som bidrag til videre diskusjoner internt i egen organisasjon.

1.4 Begreper og forkortelser

Nedenfor omtales noen viktige begreper som brukes i denne rapporten. En oversikt over begreper og forkortelser er gitt Tabell 2 og Tabell 3.

Tabell 2 Begreper

Begrep	Beskrivelse
1. linjepersonell	Personell på en installasjon som har noe kunnskap om industrielle IKT-systemer
2. linjepersonell	Fagfolk med god kunnskap om industrielle IKT-systemer (kan være på installasjon eller arbeide via fjerntilgang)
3. linjepersonell	Ansatte hos systemleverandører med spesialistkunnskap om industriell IKT-systemer
HMS	Helse, miljø, og sikkerhet
Sikkerhet	Beskyttelse av verdier så som mennesker, ytre miljø, utstyr og informasjon.
IKT-sikkerhet	Beskyttelse av informasjons- og kommunikasjonsteknologi (maskinvare og programvare, samt kommunikasjonssystemer). (Brukes som et felles begrep for IKT- og IT-sikkerhet i denne rapporten).
Installasjon	Fellesbetegnelse for innretninger til havs, landanlegg og borerigger
Cybersikkerhet	Beskyttelse av utstyr (komponenter og enheter) og fysiske prosesser som er sårbare gjennom IKT.
Organisatorisk sikkerhet	Beskyttelse av verdier gjennom tiltak relatert til organisering av arbeid, fordeling av ansvar og myndighet. (Se sikkerhet ovenfor)
Fjerntilgang	Tilgang til industrielle IKT-systemer på tvers av geografisk avstand
Fjernarbeid	Arbeid på / endringer i industrielle IKT-systemer på tvers av geografisk avstand (ved bruk av fjerntilgang).
Fjernstøtte	Overvåking og diagnose av industrielle IKT-systemer på tvers av geografisk avstand (Ikke hovedfokus i denne studien)
Fjernstyring	Styring av prosesser og systemer ved hjelp av industrielle IKT-systemer, og utført fra kontrollrom på tvers av geografisk avstand. (Korte tidskonstanter hvor man er "hands on") (Ikke hovedfokus i denne studien)

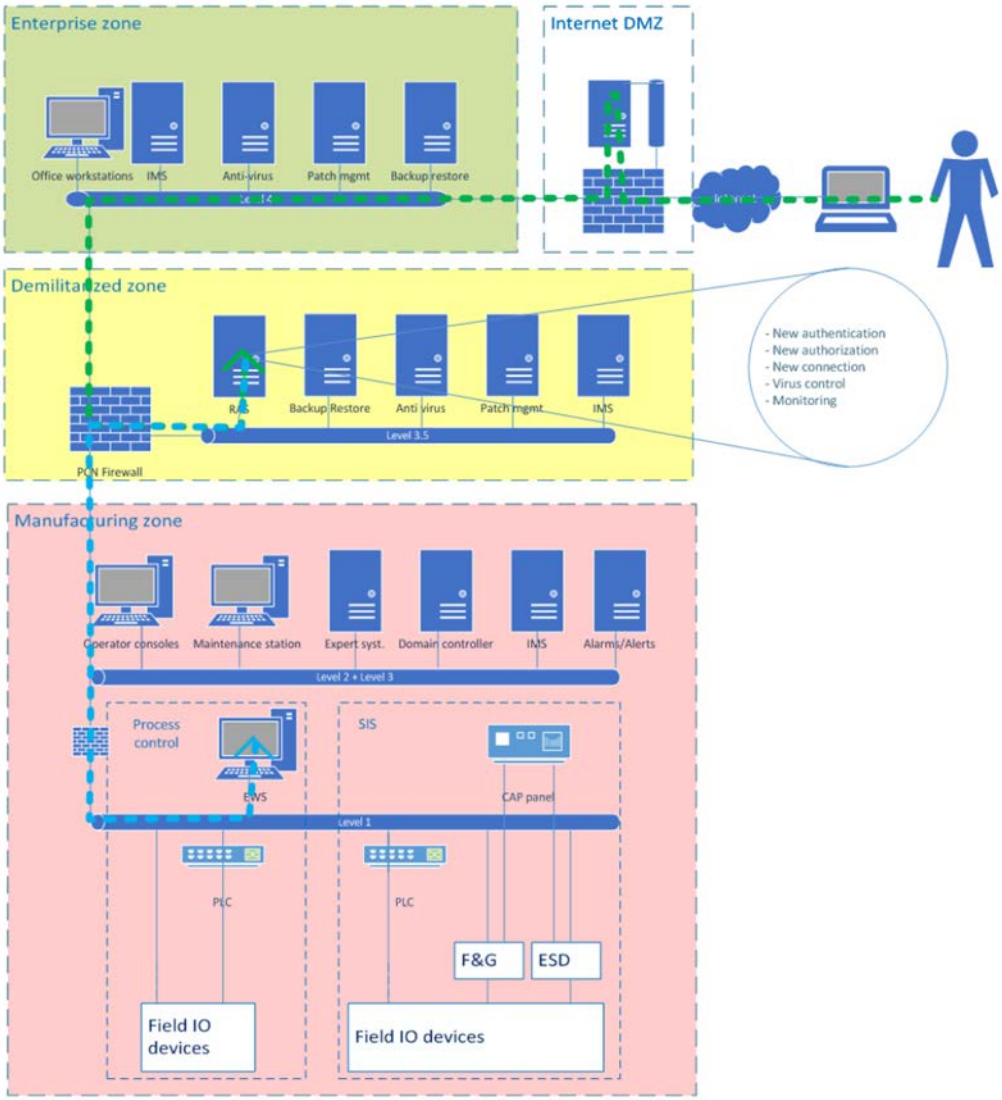
Tabell 3 Forkortelser

Forkortelse	Beskrivelse
AT	Arbeidstillatelse
BOP	"Blow-Out Preventer". (Utblåsingsventil)
IO	Integrerte operasjoner
IT	Informasjonsteknologi. Teknologi som behandler informasjon.
LCM	"Life Cycle Mangement" (Livssyklusstyring)
OT	Operasjonell teknologi. Teknologi som støtter, kontrollerer og overvåker industriell produksjon, kontroll- og sikkerhetsfunksjoner.
PCS	*«Process Control System»* (Prosesskontrollsystem).
SAS	*«Safety and Automation System»*. Brukes om industrielle IKT-systemer i petroleums-virksomheten.
SIS	"Safety Instrumented System" (Instrumentert sikkerhetssystem - del av SAS)

Informasjonsteknologi vs operasjonell teknologi

Ved vurdering av IKT-sikkerhet i industrielle IKT-systemer kan det grovt skilles mellom to teknologier, IT og OT (se Figur 1 som viser soneinndeling):

- Informasjonsteknologi, dvs. teknologi som behandler informasjon, som dokumentbehandling, websider, epost osv. I rapporten brukes begrepet IT-systemer om administrative systemer/kontor-systemer.
- Operasjonell teknologi, dvs. IT-teknologi som støtter, kontrollerer og overvåker industriell produksjon, kontroll- og sikkerhetsfunksjoner. I rapporten brukes begrepet industrielle IKT-systemer.



Figur 1 Soneinndeling og prinsippskisse for fjerntilgang (DNVGL-RP-G108) [1]

Fjernarbeid vs fjernstøtte.
I denne rapporten brukes begrepet fjernarbeid om arbeid på /endringer i industrielle IKT-systemer på tvers av geografisk avstand.

Ved vurdering av IKT-sikkerhet er det viktig å skille mellom
1) Fjernarbeid, hvor det gjøres arbeid på / endringer i industrielle IKT-systemer via fjerntilgang ("skrivetilgang")
2) Fjernstøtte, hvor industrielle IKT-systemer overvåkes og feilsøkes via fjerntilgang ("lesetilgang")

Eksempler på oppgaver som kan kreve lesetilgang:
- Feilsøking basert på sanntidsdata i industrielle IKT-systemer
- Monitorering og overvåking av datatrafikk i kontrollnettverk, inklusive logger
- Analyse av trender, skjermbilder på operatørstasjoner

1.5 Begrensninger

Hovedfokus i rapporten er på fjernarbeid knyttet til industrielle IKT-systemer ("Level" 1-3 i Figur 1). Det vil si at rapporten er spisset mot operasjonell teknologi, og ikke mot generell (administrativ) IT.

Det er likevel verdt å nevne at kontorsystemene ofte er et mål for cyberangrep. Når en angriper har fått tilgang til kontorsystemene, kan denne tilgangen utnyttes til å samle informasjon som kan brukes i planlegging og forberedelser til et cyberangrep på industrielle IKT-systemer. En angriper vil for eksempel kunne utnytte tilgang til kontorsystemene til å opprette nye brukere, samle påloggingsinformasjon eller til skanning og kartlegging av infrastruktur.

Flere private firmaer tilbyr operatørselskaper tjenester knyttet til sikkerhetsmonitorering slik som nettverksanalyse, logganalyse, automatisk sårbarhetsskanning og penetrasjonstester som kan detektere dataangrep. Kartlegging og vurdering av disse tjenestene har ikke vært del av denne studien. Sikring av personopplysninger har heller ikke vært tema for denne studien.

Valg av gruppeintervju som metode for datainnsamlingen kan ha innvirket på manglende utdypelse av psykososiale arbeidsmiljøforhold i intervjuene.

2 Analytisk rammeverk

Det analytiske rammeverket for studien og intervjuguide bygger i stor grad på to tidligere rapporter SINTEF har utarbeidet for Petroleumstilsynet (se Figur 2):

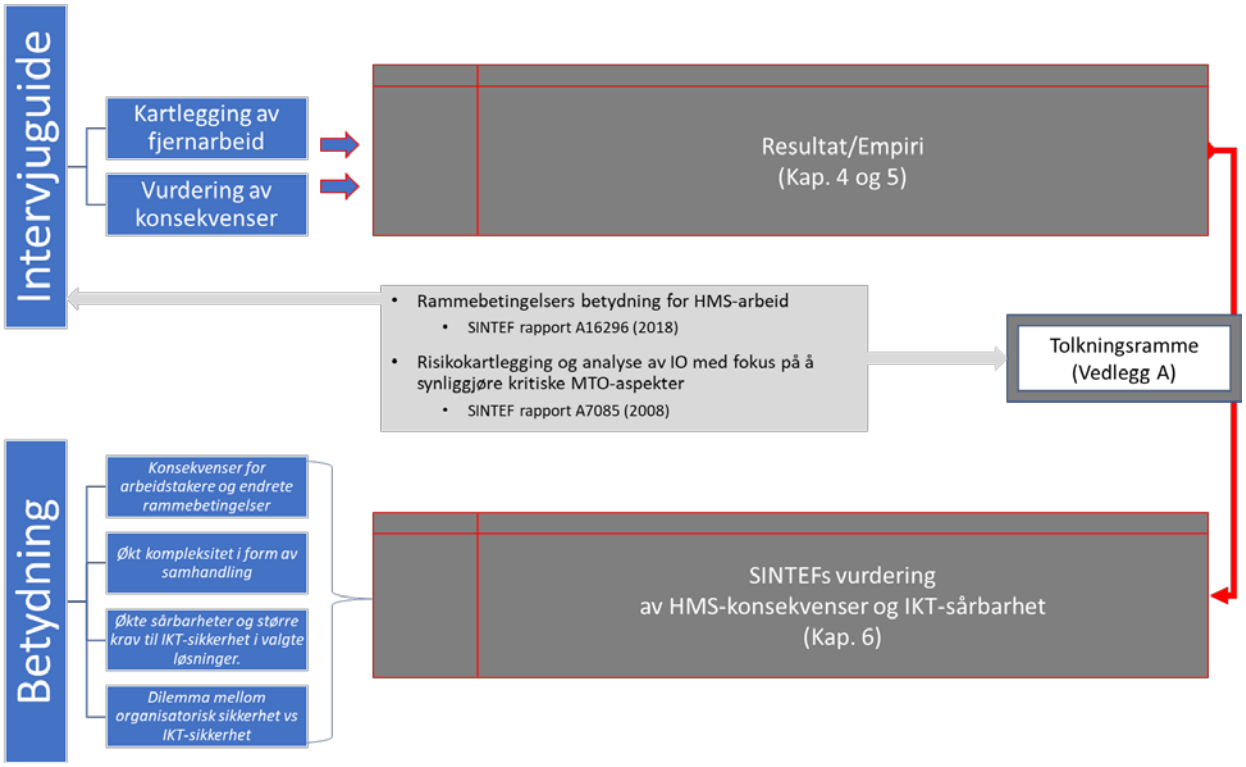
- "Rammebetingelsers betydning for HMS-arbeid" [2]
- "Risikokartlegging og analyse av Integrerte Operasjoner (IO) med fokus på å synliggjøre kritiske MTO aspekter" [3]

Intervjuguiden var hovedsakelig innrettet mot kartlegging av fjernarbeid og informantenes oppfatning av HMS-konsekvenser, felles situasjonsforståelse for sikker drift og IKT-sikkerhet. Resultatene fra intervjuene er systematisert i kapitlene 3 - 5, mens SINTEFs vurdering av disse synspunktene er gitt i kapittel 6.

Kapittel 5 omhandler følgende temaområder og betydning av fjernarbeid som var spesielt trukket frem i Ptils kravspesifikasjon:

- *Konsekvenser for arbeidstakere og endrete rammebetingelser (kontrakter og innleie).*
- *Økt kompleksitet i form av samhandling*
- *Økte sårbarheter og større krav til IKT-sikkerhet i valgte løsninger.*
- *Dilemma mellom organisatorisk sikkerhet vs. IKT-sikkerhet*.

Vi har valgt å tolke disse problemstillingene i et utviklingsperspektiv (se Vedlegg A) basert bl.a. på SINTEF-rapporten [3]. Denne rapporten var utformet som en hypotese om fremtidig utvikling innen IO, og som en analyse av mulige implikasjoner av en slik (hypotetisk) utvikling sett i forhold til seks ulike perspektiver på storulykker og robuste/resiliente organisasjoner. Tolkningsrammen bygger på et inter-organisatorisk kompleksitetsperspektiv på samhandling og et IKT-perspektiv som fremhever IKT sin rolle ift makt og kontroll.



Figur 2 Studiens tilnærming og metode

3 Bruk av fjernarbeid norsk sokkel

I det følgende beskrives innspill fra gruppeintervju om fjernarbeid på innretninger til havs, landanlegg og borerigger. Nedenfor vil vi bruke fellesbetegnelsen ***installasjon*** om disse. Dersom omtalte forhold gjelder kun en type, vil dette bli nevnt eksplisitt. Diskusjonen er begrenset til installasjoner på eller relatert til norsk sokkel, selv om enkelte selskap som ble intervjuet har betydelig internasjonal virksomhet. Noen utsagn fra gruppeintervjuene er tatt med nedenfor og vist i *kursiv.*

3.1 Teknologi

Både gamle og nye installasjoner har verktøy og legger til rette for fjerntilgang på industrielle IKT-systemer, men enkelte installasjoner har kun fjerntilgang for ansatte i eget selskap. Det er en trend å flytte driftsstøtte til land og kontrollfunksjoner til land.

Fjerntilgang for styring og fjernarbeid er ikke noe nytt. Innretninger som fjernstyres fra en annen innretning på norsk sokkel, har eksistert lenge. *"En satt jo ikke "på" når en var offshore heller. Brukte "remote" desktop selv når en var offshore. Den store forskjellen var at en kunne gå inn til kontrollrommet og snakke med de der."*

Ved boreoperasjoner skiller man mellom begrepene fjernarbeid offshore og fjernarbeid onshore. Fjernarbeid offshore innebærer at arbeid skjer uten visuell kontakt med maskinen.

Industrielle IKT-systemer på en installasjon følger prinsippene vist i Figur 1. Det vil si at det via brannmur er mulig å koble seg på nettverket for prosess- og maskinstyring fra arbeidsstasjoner på land.

Industrielle IKT-systemer har typisk segregering og nettverksinndeling som bygger på Purdue-modellen som er en anerkjent praksis for design av slike systemer. For eksempel SIS og PCS, samt segregert toppsystem HMI og underliggende nodenettverk for PCS, og SIS (se Figur 1). Innenfor boreoperasjoner er det vanlig at industrielle IKT-systemer for boring, boreslam og utblåsningssikring (BOP) er uavhengige og segregerte i separate nettverk.

Industrielle IKT-systemer kan legge til rette for å benytte fjerntilgang hos både operatørselskaper, systemleverandører, tredjepartsleverandører og utstyrsleverandører, men bruk av fjernarbeid for forskjellige systemer på en installasjon er svært avhengig av teknologi på den enkelte installasjon.

Alternative muligheter for fjerntilgang er, for eksempel:

1. Adgang ved bruk av dedikert applikasjon for fjerntilgang
2. Adgang via dedikert arbeidsstasjon som er koblet til industrielle IKT-systemer

Generelt er ikke teknologien noe hinder for fjernarbeid, bortsett fra at enkelte frittstående borerigger kan ha lav båndbredde og svak regularitet og pålitelighet i kommunikasjonen mot land. På eldre installasjoner kan det være begrensinger i teknologi for å kunne legge til rette for robuste løsninger for fjerntilgang, samt deling av data mellom systemer. En utfordring vil være å unngå overbelastning av systemer på grunn av datafangst.

3.2 Arbeidsoppgaver

Det er operatørselskap og boreselskap som bestemmer hvilke oppgaver som kan utføres ved fjernarbeid, og her er det forskjeller mellom selskapene. Endring i industrielle IKT-systemer planlegges og kontrolleres av både fagspesialister på land og driftspersonell på installasjonen, og de gjennomføres i henhold til

~~operatør~~selskapets standard arbeidsprosesser. *"Det er aldri slik i dag at man går offshore og gjør ting. Blir testet på land først!".* Systemleverandører har gjerne kopi av programvare og kan simulere effekt av foreslåtte endringer før implementering på installasjon. *Normalt testes 60-70 % av programvare fra land – resterende testes om bord."* Installasjoner har gjerne teknisk personell som kan laste opp programvareendringer, eventuelt med fjernstøtte fra systemleverandør. Det ble nevnt eksempler på operatørselskaper som har meget kompetent teknisk personell på installasjonen. Eksempler på mindre endringer som gjøres ved fjernarbeid fra land, er parameterendringer og feilrettinger som ikke krever omprogrammering.

Informanter fremhever at en viktig fordel ved fjernarbeid, er raskere støtte til operatør- og boreselskaper og at systemleverandør kan være bedre forberedt for arbeidet. Noen kan klargjøre arbeidet på land før man kommer til installasjonen og at både effektivitet og sikkerhet forbedres ved å jobbe på denne måten. Det er bedre å planlegge og utvikle programvareendringer når de sitter på land enn å være ute på installasjonen.

Feilsøking i industrielle IKT-systemer for boreutstyr kan være vanskelig uten å være fysisk tilstede siden feil gjerne er en kombinasjon av feil i de hydrauliske, mekaniske og elektriske systemene, og ikke i de programmerbare systemene. Det hender også at programvaren må tilpasses endret oppførsel eller bruk av boreutstyret. Ved oppgradering av programvaren kan det være aktuelt å bruke simulator, men utvikling og oppdatering av simulatorer for borekontrollsystemer er kostbart.

3.3 Omfang

Alle informanter opplever at industrielle IKT-systemer er stabile systemer, og det er sjeldent behov for fjernarbeid i form av programvareendringer på installasjoner. Noen informanter antydet at det gjennomsnittlig går mer enn ett år mellom hver programvareoppdatering. Lesetilgang i form av å sjekke status, diagnose og feilsøking varierer betydelig mellom installasjoner, fra daglig til kvartalsvis.

Det er svært få situasjoner vedrørende fjernarbeid som kan karakteriseres som hasteoppdrag, og planlegging og utførelse av fjernarbeid skjer hovedsakelig innenfor vanlig arbeidstid. For boresystemer kan imidlertid tidspresset oppleves stort ved utilsiktet nedetid.

Fag- og driftspersonell som er intervjuet, er stort sett skeptiske til å tillate programvareendringer på industrielle IKT-systemer ved fjernarbeid. De mener at lokalkunnskap om den enkelte installasjon, samt fysisk nærhet til drift og operasjon er essensielt ved arbeid på industrielle IKT-systemer.

Noen informanter opplever et press for økt bruk av fjernarbeid ved programvareendringer. Ifølge informantene har operatørselskaper hittil vært meget restriktive med å tillate programvareoppdateringer i sikkerhetssystemer fra land. Hos et av selskapene i studien pågår det diskusjon om man i større grad skal tillate slike endringer også fra land.

3.4 Arbeidsprosesser og brukertilgang

Både innretninger, landanlegg og borerigger håndterer arbeidsprosessen med fjernarbeid på lik linje med annet arbeid på en installasjon. De som skal gjennomføre fjernarbeid, må inviteres inn av en ansvarlig i operatørselskapet. Enkelte selskaper skiller mellom to nivå på arbeidstillatelser (AT) i henhold til NOROG 088:

- AT nivå 1 ved arbeid med høyere risiko og klarering på innretningsnivå (f.eks. utkobling, overbroing og testing av sikkerhetssystemer)
- AT nivå 2 for arbeid som krever klarering innenfor et område eller et system (f.eks. arbeid på kontrollsystemer).

Operatørselskaper og boreselskaper bruker egne applikasjoner for fjernarbeid til industrielle IKT-systemer. Applikasjonene benyttes både av egne ansatte i eget selskap og av leverandører. Enkelte systemleverandører tilbyr fjerntilgangsløsninger som en tjeneste for mindre operatørselskaper. Siden både operatør- og boreselskaper bruker forskjellige applikasjoner for fjernarbeid, må systemleverandører forholde seg til flere forskjellige løsninger for fjernarbeid. Systemleverandører har opprettet egne prosedyrer for fjernarbeid, og tilpasser disse til operatørselskapets prosedyrer for den enkelte installasjonen.

Vi registrerte ikke noen vesentlige forskjeller mellom innretninger, landanlegg og borerigger med hensyn til teknologi og prosedyrer for brukertilgang, det vil si identitets- og tilgangskontroll som skal sikre at kun personell med et definert behov får riktig tilgangsnivå i industrielle IKT-systemer.

Pålogging til industrielle IKT-systemer ved fjernarbeid krever autentisering via forhåndsdefinert brukerprofil som administreres av operatørselskap eller boreselskap. Ved søknad om brukertilgang vurderes for eksempel:

- Behov for brukertilgang
- Hvilke systemer man får tilgang til
- Hvilken type tilgang som trengs
- Varighet av tilgang

Ifølge informantene er det ved fjernarbeid stort fokus fra operatører og boreselskaper på å kontrollere identiteten til personell som gjennomfører arbeidet, for eksempel ved at servicepersonell er med på avklaringsmøter før selve gjennomføringen av fjernarbeid. Fagmiljøet i Norge er lite, slik at personlig bekjentskap gir en økt trygghet ved fjernarbeid.

Noen informanter sa at personell i operatør- og boreselskaper overvåker arbeidsoperasjoner fra servicepersonell under fjernarbeid. Enkelte selskaper bruker videokonferanse ved fjernarbeid. Systemleverandører gjennomfører kursing av eget personell og tilordner brukerrettigheter basert på dokumentert spesialistkompetanse innenfor det enkelte industrielle IKT-systemet. Noen operatørselskaper tillater permanent tilgang for fjernarbeid rettet mot støttesystemer, men ikke til prosesskontroll- og sikkerhetssystemer. Fjerntilgang til industrielle IKT-systemer er i dag hovedsakelig via personlig bruker med eget passord forskjellig fra andre IT-løsninger. For mindre kritiske systemer er det eksempler på tilgang via en felles bruker og her er det pågående arbeid med å endre til personlig bruker. Applikasjoner for fjerntilgang kan også ha en "chat"-funksjon som kan brukes ved fjernarbeid. Siden "chat"-samtaler lagres, gir dette bedre dokumentasjon enn vanlig telefonsamtale av hva som ble avtalt/gjort under oppdatering av anlegget. Ved skrivetilgang, hvor tilgang gis innenfor en viss periode, vil bruker automatisk miste fjerntilgang når perioden er utløpt. Dersom installasjonen har egne servere for lesetilgang, kan enkelte brukere få permanent lesetilgang. Informanter vektla at god kontroll med administratorrettigheter er viktig for å unngå uønskede handlinger og hendelser fra personell. Alle selskapene som deltok i studien. har opprettet egne rom for fjernarbeid. Noen selskap stiller krav om at alt fjernarbeid skal skje i egne avlåste rom.

3.5 Organisering

Gruppeintervjuene avdekket at det er forskjellige strategier vedrørende samarbeid med systemleverandører blant operatørselskaper.

Hos et operatørselskap er strategien å samle egne systemingeniører i operasjonssenter på land slik at ingeniørene kan betjene flere innretninger i selskapet. Hos et annet selskap er strategien å beholde ingeniører offshore for å sikre tilstrekkelig lokalkunnskap om industrielle IKT-systemer, spesielt siden disse systemene blir stadig mer komplekse. I intervju med personell på landanlegg ble det spesielt trukket frem betydningen av å ha eget personell som evner å se helheten. *"Eksperter er gode til en ting, men ikke alt. Vi er gode på hvordan ting henger sammen!"*.

Et operatørselskap velger å bygge opp og inneha egen spisskompetanse på industrielle IKT-systemer slik at de kun unntaksvis vil ha behov for assistanse fra systemleverandør. De ønsker å være uavhengig av systemleverandør og selv kjenne og ta ansvar for risiko. Et annet operatørselskap har derimot gått meget langt i å gi systemleverandør ansvar for spesifikke driftsoppgaver.

Det ble gitt eksempler på innretninger som har 24/7/365 driftsstøtte fra operasjonssenter på land. Enkelte innretninger har avtale med systemleverandør om driftsstøtte fra et fast team med spesialkompetanse for den enkelte innretning. Vaktordninger er ikke blitt vesentlig endret på grunn av økt fjernarbeid.

Systemleverandører tilbyr vaktordning 24/7/365 for borerigger. Det ble antydet at 60-70 % av borerigger på norsk sokkel hadde avtale om fjerndiagnostikk. Dette er organisert i egne støttesenter som betjener borerigger på norsk sokkel. Vaktordningen omfatter også systemspesialister på land (for eksempel bakvakter en uke i gangen som kan mobiliseres i løpet av en time). Deltakelse i slike vaktlag oppfattes som en anerkjennelse av fagkompetanse og ansatte vil gjerne være medlemmer i vaktlagene.

Både operatørselskaper og boreselskap gjennomgår og godkjenner foreslåtte endringer i kritiske systemer, identifiserer og foreslår designforbedringer, samt gir teknisk støtte til drift og prosjektering.

Underleverandører til systemleverandør har ikke tilgang til industrielle IKT-systemer på en borerigg. Dette innebærer at programvareoppdatering fra underleverandør gjennomføres av systemleverandørens personell.

Det ble hevdet at det er bedre samarbeid mellom operatør- og boreselskap og systemleverandør i Norge enn andre steder. Dette har med norsk kultur og vilje til å løse problemer i fellesskap.

Innenfor boring ble det hevdet at det er personell med lang felterfaring som ønsker å arbeide med fjernstøtte og at systemleverandørene har personell på land som kjenner både systemet og boreoperasjonen meget godt. Mange har en familiesituasjon som gjør det attraktivt med fast arbeidstidsordning på land. *"Det er ikke den store bekymringen å få kompetent personell pr i dag."*

4 Endringer og trender

4.1 Drivere for fjernarbeid

Gjennom ny teknologi og nye arbeidsprosesser gir digitalisering økt tilgang til data og bedre beslutningsstøtte for optimalisering og effektivisering av produksjon og vedlikehold, inklusive bedre forståelse av utstyrets ytelse og antatt levetid. Økt datafangst muliggjør tilstandsbasert i stedet for tidsbasert vedlikehold. Avansert dataanalyse vil kunne erstatte noe av analysearbeidet som i dag utføres av systemleverandørene, og redusere behovet for periodisk vedlikehold. *"Om 3 år vil maskinen finne ut selv når vedlikehold skal utføres."*

Viktige faktorer for økt fjernarbeid er økonomi og sikkerhet. Økt fjernarbeid gir bedre responstid og tilgang til ekspertise på land. For systemleverandører er det mer effektivt at personell med spesifikk kompetanse utfører samme arbeidsoperasjoner for flere operatør- og boreselskaper. Færre reiser og mindre tid på reising vil gi reduserte kostnader. For innretninger og borerigger vil det være redusert risiko på grunn av færre antall helikopterturer. I dag er helikopterrisiko et vesentlig bidrag til det totale risikobildet på en installasjon.

Endringsvilje hos operatør- og boreselskaper er en annen viktig faktor. Selv om flere operatørselskaper nå har søkelys på digitalisering, er det forskjeller i forhold til hvor villige selskapene er til å prøve nye ting.

Systemleverandører for boreriggutstyr trekker spesielt frem raskere responstid og reduserte besøk på borerigger som viktig drivere for økt fjernarbeid. En del vedlikehold på borerigger vil fortsatt skje ombord. Spisskompetansen flyttes på land og de ute skal holde systemet i gang og gjøre enkle vedlikeholdsoppgaver.

Det blir antakelig mer uniforme systemer for drift og vedlikehold hos operatørene og all informasjon fra drift og sensorer kan deles med andre selskaper og leverandører.

4.2 Endrede arbeidsprosesser og organisering

Informantene forventer at det fremover vil bli redusert arbeidsomfang offshore og økt omfang av fjernarbeid.

De tror det vil bli økt samhandling og partnerskap mellom systemleverandør og operatør- og boreselskap i både tidligfase og i drift. Systemleverandører vil bli tatt mer med i tidligfase fordi de leverer den tekniske løsningen. I drift vil det bli mer samarbeid mellom operasjonssentrene til systemleverandør og operatør- og boreselskap. Økt samarbeid vil også skje ved at personell fra forskjellige organisasjoner samles fysisk i samme lokaler og i felles team.

Det vil trolig utvikles nye forretningsmodeller for service og livsløpstjenester slik at systemleverandører i større grad tar ansvar for drift og oppetid og ikke kun får betalt for utstyr og service. I nye kontrakter vil det i økende grad bli stilt krav til systemleverandører med tanke på responstid, og det vil bli lagt til rette for økt fjernarbeid.

Boreselskaper forventer økt bruk av incentiv-kontrakter og bruk av løsninger som ikke er utviklet selv

Systemleverandører blir mer involvert i operatørselskapenes satsing på digitalisering gjennom utarbeiding av nye applikasjoner og rapporter som bearbeider innsamlet data. De vil også kunne tilby tjenester som overvåking og varsling av cybersårbarheter som en tjeneste.

Digitalisering medfører ønske om økt informasjonsutveksling mellom tidligere adskilte systemer. Spesielt innenfor boring vil dette være krevende hvor det kan være svært mange forskjellige selskaper som er involvert i boring av en brønn. Pr. i dag er det stor grad adskilte systemer for kontroll av for eksempel boring, borevæske og BOP. Sannsynlig scenario er at boreoperasjoner fortsatt vil være fragmentert, men at ny teknologi gjør at borepersonell kan ta på seg flere oppgaver. Enkelte systemleverandører som har vaktordninger opplever at det kan være vanskelig å få god finansiering av disse. De er bekymret for en utvikling hvor de kun får betalt for hva de gjør og ikke tilstrekkelig betalt for den kunnskapen som legges inn i leveransen. Ved arbeid offshore får man betalt time for time. Dokumentasjon av timeforbruk ved arbeid på land er mer krevende, for eksempel ved arbeid knyttet til oppfølging av utstyr og dokumentasjon i etterkant. Utvikling av nye samarbeidsformer skaper nye utfordringer knyttet til forretningsmodeller og hvem som eier driftsdata. For eksempel, opplever systemleverandører at det vanskelig å få betalt for kostnader ved utvikling av databaser og tilgjengeliggjøre informasjon. Juridisk kan det også være utfordringer med deling av data. Det eksisterer avtaler om deling av data, men det er lenge siden de ble utarbeidet og basert på en filosofi: Ikke del uten tvang! Et operatørselskap nevnte eksempel på utfordringer med å få frigitt rådata fra systemleverandør. Under et intervju kom det opp forslag om at argumentasjon måtte snus, dvs. stille spørsmål om hvorfor man ikke skal dele.

4.3 Automatisering av arbeidsprosesser på borerigger

Bransjen ser for seg gradvis automatisering av nåværende maskinpark på borerigger. En mulig utvikling vil være mindre manuell styring og mer fokus på overvåking og feilretting. Enkelte borerigger har for eksempel installert automatisk rørhåndteringssystem. Setting av foringsrør er eksempel på oppgave som kan automatiseres. Eksempler på roller som kan flyttes til land, er f.eks. retningsborer som i dag sitter like ved siden av borer og slamlogger.

Videre automatisering av boreoperasjoner vil kunne skje ved at boreplaner blir direkte implementert i borekontrollsystemet, dvs. uten involvering av borer. Dette vil stille større krav til kvalitetssikring av boreplan siden det ikke er samme person som implementer plan og som overvåker.

Boreoperasjon er krevende å automatisere, siden utstyr skal håndtere store vektforskjeller med til dels meget høy presisjon og er derfor sårbare for mekanisk slitasje. Andre systemer på en borerigg er også krevende å automatisere, men kan la seg fjernstyre. Mye av maskinparken på en borerigg er enda ikke tilpasset fjernstyring.

4.4 Simulator/digital tvilling

Intervjuobjekter forventer at simulatorer og digitale tvillinger vil bli mer aktivt brukt i opplæring og trening for å kompensere for at personell involvert i fjernarbeid får færre reiser offshore. Siden en digital tvilling gir virtuell representasjon av all informasjon om en installasjon og kontinuerlig innsamling av alle relevante data, vil dette blant annet kunne effektivisere tid på å finne ut hvordan ting ser ut på installasjonen. *"Kommer tettere på prosessen!".* Etter en hendelse kan man bruke registrerte data til å gjenskape hendelsen og dermed gjennomføre analyser basert på fakta og ikke bare basert på hukommelsen til involvert personell. På nye installasjoner vil automatisk dokumentasjonsoppdatering være sentralt. "*I det store bildet er kostnad ved simulator så lav at nye rigger vil komme ut med digital tvillling."*

Bruk av digitale verktøy er ikke noe nytt. Det som er nytt, er den økte samhandlingen mellom systemleverandører og operatørselskapenes verktøy.

4.5 Ubemannede plattformer

Ubemannede plattformer vil kunne ha færre sikkerhetssystemer (ikke livbåter, ikke helidekk, mindre brann- og gass-anlegg) som gjør det lettere å oppnå god situasjonsforståelse ved fjernarbeid. Samtidig vil disse installasjonene kunne implementere mer instrumentering for tilstandsovervåking (f.eks."Valve watch", CCTV) for å kompensere for manglende folk. Dette kan føre til at industrielle IKT-systemer og kommunikasjonssystemer på ubemannede installasjoner likevel blir relativt komplekse og dermed gjøre fjernarbeid krevende.

5 Informanters vurdering av HMS-konsekvenser og IKT-sikkerhet ved fjernarbeid

I denne delen av rapporten presenteres resultater fra intervjuer med informanter i forhold til deres oppfatning og vurdering av HMS-konsekvenser og IKT-sikkerhet ved fjernarbeid. Informantene i de ulike selskapene ble bedt om å vurdere både positive og negative forhold av betydning for å kunne ivareta HMS og IKT-sikkerhet ut fra det de har opplevd frem til i dag, samt mulige konsekvenser ved økt omfang av fjernarbeid i fremtiden (3-5 års perspektiv).

Under gruppeintervjuene ble informantene spurt om de viktigste utfordringene relatert til arbeidsforhold ved fjernarbeid. Bakgrunnen for at informantene ble spurt om psykososiale arbeidsmiljøforhold[1] som jobbkrav, sosial støtte, jobbkontroll, arbeidstid, arbeidspress, trening og opplæring, kultur og språk er for å få mer informasjon om hvilke bakenforliggende forhold som oppleves å være de største utfordringene for sikkert arbeid, og som kan ha betydning for ivaretakelse av et godt arbeidsmiljø ved fjernarbeid både på land, offshore og i samhandlingen mellom land-offshore. Når det gjelder dette temaet så var det informanter som opplevde at ingen av disse utfordringene var særlig fremtredende ved fjernarbeid, og vi fikk generelt mindre utfyllende svar her enn det som er presentert tidligere i rapporten. Det kan også være at psykososiale arbeidsmiljøforhold er noe man ikke ønsker å svare utdypende på i et gruppeintervju.

Nedenfor gis en oppsummering av de arbeidsforhold som informantene var opptatt av. Ved presentasjon av konsekvenser skiller vi mellom forhold som påvirker:

- Felles situasjonsforståelse for sikker drift ved bruk av fjernarbeid,
- Arbeidstid,
- IKT sikkerhet ved fjernarbeid.

5.1 Felles situasjonsforståelse for sikker drift

Nedenfor gjengis forhold ved fjernarbeid som påvirker felles situasjonsforståelse mellom ulike lokasjoner og dermed forhold som påvirker risikobildet på et anlegg eller en installasjon. Dette er risikopåvirkende forhold som kommer i tillegg til f.eks. redusert ulykkesrisiko for personell på grunn av mindre eksponering for faresituasjoner og færre helikopterturer ved fjernarbeid.

Ifølge informantene er viktige faktorer som påvirker felles situasjonsforståelse, klare retningslinjer, god kommunikasjon og god lokalkunnskap. Fjernarbeid fører til at kravet til system og anleggskunnskap hos de som skal utføre arbeidet "remote", blir enda viktigere. Spesifikk anleggskunnskap gjør at man er bedre i stand til å forstå konsekvensene av de endringene man gjør i systemet og hvilken påvirkning det vil ha for sikker drift. Det er verdt å merke seg at noen informanter mener at fjernarbeid ikke medfører spesielle endringer i forhold til sikkerhet på en installasjon.

Generelt vil søkelys på redusert bemanning offshore og økt omfang av fjernarbeid medføre mange digitale løsninger på en installasjon som en må stole på. Noen intervjuobjekter trakk frem at økt digitalisering krever økt fokus på situasjonsforståelse siden færre personer vil kunne ha totaloversikt ved økt digitalisering.

[1] En kategorisering av psykososiale farer finnes i "PAS 1010:2011 Guidance on the management of psychosocial risks in the workplace".

Økt og endrede krav til kompetanse og anleggskunnskap

Fjernarbeid fører til økt krav til kompetanse og anleggskunnskap for de som skal utføre arbeidet fra land/"remote". Det ble påpekt av flere informanter i både operatørselskaper og hos systemleverandører at fjernarbeid gjør at god system- og anleggskunnskap blir *enda* viktigere når man utfører arbeid uten å være tilstede på installasjonen eller landanlegget. Dette har ført til endringer hos operatørselskapene ved at de bruker ekstra tid på å verifisere tilstrekkelig kompetanse hos systemleverandør hvis de tilbyr personell som ikke har arbeidet på installasjonen tidligere. Dette kan for eksempel gjøres gjennom kontakt pr. telefon/video før arbeidet igangsettes. "*Jeg vil gjerne se folk i øynene. Må vite at vedkommende gjør det han sier!".* Operatørselskaper forventer at systemleverandører har egne systemer for oppfølging av kompetanse hos egne ansatte.

Fjernarbeid medfører også i så måte en endring i hvordan man må tenke i forhold til trening og opplæring av nytt personell. Flere operatøransatte var opptatt av at man må tenke på dette med rotasjon mellom hav-land slik at man har opplevd å sitte både ute i havet og på land. Dette øker forståelsen for den jobben som skal gjøres og at det blir "kort avstand" til de offshore. Det gjør også at det blir lettere for offshore personell å ta kontakt med land pa grunn av økt tillit til de på land.

Når industrielle IKT-systemer blir mer komplekse, påvirker dette arbeidssituasjonen til de som er til havs. Økt kompleksitet kan føre til usikkerhet og ekstra behov for å støtte seg til spesialister på land (2. og 3. linjepersonell). Spesielt telekommunikasjonssystemer oppleves komplekse med økt krav om oppetid. Her kan det være opptil 30 forskjellige leverandører. Selv om industrielle IKT-systemer blir mer komplekse, var det informanter som hevdet at de ikke opplevde fjernarbeid som mer komplekst. En informant forklarte dette med at det var økt kompleksitet i de systemene som nå skal driftes som endrer arbeidsdagen, og ikke nødvendigvis fjernarbeid som sådan. Dette medfører at støttepersonell på land må ha mer kompetanse for å forstå sammenhengen mellom ulike system, noe som også gjør at de offshore etterspør mer ekspert kompetanse fra land pga. den økte kompleksiteten.

For borerigger ser man en forskjell ved at informantene er mer opptatt av at arbeidsprosesser og oppgaver flyttes fra borerigg til land, og hvilken kompetanse som da er nødvendig for de som blir igjen ute på riggen. Systemleverandør for boreutstyr har stort fokus på opplæring og krever at det kjøpes opplæring som en del av leveransen. De bidrar med personell om bord de første 3-4 måneder for å gi riggpersonell trygghet på operasjon av nytt utstyr. I likhet med andre selskaper og bransjer opplever også systemleverandører for boreutstyr en kamp om spisskompetanse innenfor digitalisering.

Lokalkunnskap om installasjon for innleid personell

Ifølge informantene er det ekstra viktig med god forståelse av hvordan arbeid kan påvirke drift og sikkerhet på en installasjon når man utfører oppgaver uten selv å være tilstede. *"Systemarbeid er en ting, men på applikasjon er det alltid noen spesialiteter!"* Ved økt fjernarbeid vil det kunne bli en utfordring at servicepersonell ikke er tett nok knyttet til den enkelte installasjonen. Hvis faste personer arbeider mot de faste selskapene, er det ikke nødvendigvis et problem at det er mange forskjellige applikasjoner. En sikkerhetsutfordring ved økt fjernarbeid, er at det lett kan bli mer fristende å bruke en person som er tilgjengelig, enn en person med spesifikk kunnskap om det enkelte anlegg.

Et viktig virkemiddel for å sikre god lokalkunnskap i drift, er at personell blir med fra prosjektfasen til driftsfasen. Da vil personell få detaljert kunnskap om system/utstyr, spesielt hvis de også får anledning til å være med under igangsetting av installasjonen. Rotasjon mellom offshore og support på land ble fremhevet som et annet viktig virkemiddel for å sikre lokalkunnskap om den enkelte installasjonen.

En konsekvensmatrise som tydeliggjør mulige utfall ved for eksempel oppstart av servere og nettverk, kan være et viktig hjelpemiddel for fjernarbeid. *"Det er nesten viktigere når du ikke er på anlegget at man vet hva som kan skje og ikke. Større krav til kompetanse for de som ikke er på anlegget, enn de som er der."*

Bedre og tettere samarbeid mellom operatørselskaper og systemleverandører

Fjernarbeid muliggjør økt samarbeid mellom operatørselskap og systemleverandører som igjen bidrar til læring og økt samlet kompetanse. Ved flytting og samling av teknisk personell til land har man lettere tilgang til et faglig nettverk og spesialistkunnskap innenfor industrielle IKT-systemer. Dette gjelder spesielt for industrielle IKT-systemer som krever spesialkompetanse og noen ganger også tilgang til personell utenfor Norge. Men en utfordring er at man fjerner personell fra prosess- og boreekspertise. Nye samarbeidsmodeller hvor systemleverandør og operatør- og boreselskap i større grad sitter fysisk samlet på land kan være en mulig løsning på denne utfordringen.

Enkelte informanter opplevde bedre jobbinnhold ved å sitte sammen med spesialister på land. Samtidig presiserte noen av de som hadde blitt flyttet til land, at jevnlige og korte opphold på installasjonen ga økt jobbtilfredshet. Ingeniører i operatørselskaper som var flyttet til land, opplevde at det var mer sosialt å sitte sammen med spesialister på land. Noen systemleverandører sa derimot at sosial gevinst ved å arbeide til havs, er begrenset fordi det er ikke alltid like enkelt å komme i god kontakt med offshorepersonell som serviceansatt. *"Offshore så var det jo ofte at man kunne føle seg alene. Onshore så har man støtte fra kollegaer".*

En informant trakk frem et dilemma vedrørende fjernarbeid som var knyttet til formen på samarbeid mellom systemleverandør og operatørselskap. Aktiv dialog ble vurdert som positivt av systemleverandør. Hvis operatørselskapet derimot kun overvåket arbeidsprosessen, ble dette lett oppfattet som negativt av systemleverandøren og at man da kan føle seg "fotfulgt".

Fysisk nærhet til utstyr og bruk av sanser

Nåværende praksis med fysisk nærhet til utstyr ved gjennomføring av programvareendringer på kritiske industrielle IKT-systemer (for eksempel SAS), gir god sikkerhet siden utøvende personell får umiddelbar tilbakemelding fra anlegget under systemendringer. Ved fjernarbeid mister man en del informasjon som mennesker fanger opp ved å være fysisk tilstede på installasjonen som f.eks lukt og lyder. Dette gjør at man har mindre oversikt over det som skjer og hva som kan skje. *"På en installasjon hører man når en brannpumpe starter - En vil ikke se en alarm når man jobber remote". "Når man kjenner at det rører på seg, gjør dette noe med tankesettet - Personell kan ta større sjanser hvis man sitter på land!". "Følelsen man har når man sitter ute, mister man når man sitter ved en skjerm!".* Det er gjort forsøk med kamera på hjelm og bærbar skjerm for personell i felt for å sikre bedre situasjonsforståelse ved fjernarbeid. Ifølge en av informantene fungerte ikke videoforbindelsen til land særlig godt i dette tilfellet.

For boreoperasjoner er det ekstra viktig at programvareoppdateringer skjer fysisk på installasjonen med tilstedeværelse av kvalifisert personell siden endringer må verifiseres på den fysiske maskinen.

Egne rom for fjernarbeid

Bruk av egne rom ved fjernarbeid bidrar til økt søkelys på arbeidsoppgavene og ekstra bevissthet om risikobildet knyttet til endringer på anlegg i drift. Egne rom for fjernarbeid blir ekstra viktig for å unngå forstyrelser når for eksempel personell sitter i åpne kontorlandskap.

Kommunikasjon, språk og kultur

Flere norske systemleverandører har avdelinger i andre land og ved spesielt store modifikasjonsprosjekter vil det kunne være aktuelt å tilby personell som ikke snakker norsk. Det ble nevnt at tekstmeldinger ("chat") kan være en like god kommunikasjonskanal for å sikre at man forstår hverandre som telefon ved samarbeid mellom hav og land.

Fjerntilgang krever ekstra oppmerksomhet i forhold til uønskede hendelser som for eksempel kommunikasjonssvikt under fjernarbeid eller at det plutselig skjer en kritisk hendelse på installasjonen. Enkelte installasjoner har oversiktsbilder som viser pågående fjernarbeid sammen med andre åpne arbeidstillatelser. I fremtiden forventer informanter at det installeres indikatorlamper både på borerigg og på land som viser at utstyr fjernstyres.

Generelt om arbeidsprosesser for sikker drift

Arbeidsprosesser for sikker drift på en installasjon er de samme for fjernarbeid som for arbeid som gjennomføres på selve installasjonen, dvs. sikker jobbanalyse og systemer for arbeidstillatelser er helt sentralt både med og uten fjerntilgang. Operatørselskaper har løsninger og styrende dokumenter for brukertilgang til industrielle IKT-systemer. Høyt fokus på identitets- og tilgangskontroll sikrer at kun kompetent personell og personell med et definert behov, får riktig tilgangsnivå. Dermed reduseres muligheten for at personell introdusere farlige situasjoner på grunn av feilhandlinger og misforståelser. Samtidig gir selskapenes identitets- og tilgangskontroll redusert risiko for tilsiktet uønsket hendelse. Viktige sikkerhetsbarrierer som spesielt boreselskaper trekker fram, er arbeidstillatelser, prosedyrer for endringsledelse, internrevisjon og trening.

5.2 Arbeidstid

Generelt så oppleves det som positivt for helse og arbeidsmiljø at fjernarbeid fører til mindre reising for den enkelte ansatte. Denne måten å jobbe på muliggjør bedre arbeidstidsordninger for personell gjennom færre lange reiser ut til installasjoner som kan ha en negativ effekt på arbeidsutførelse.

Arbeidstid ved fjernarbeid på land er i dag ikke ansett som noe stort problem. Det er sjelden at man blir ringt opp for å løse akutte oppdrag. Hvis ikke de som har vakt kan løse problemet, blir oppgaven videresendt og løses av en kompetent fagperson innenfor normal arbeidstid. Enkelte store systemleverandører har flere internasjonale kontorer slik at oppgaven kan løses på dagtid et eller annet sted i verden. Generelt ble det påpekt at vaktordninger som medfører nattarbeid til en viss grad oppleves som usosialt siden personell sitter i egne rom.

Informanter anbefaler at vaktordninger på land organiseres slik at personell har lokalkunnskap til installasjonene. Når personell fra systemleverandører får utpekt driftsoppgaver for flere installasjoner og systemer, kan det være utfordrende å forholde seg til de spesifikke teknologiske løsningene på en installasjon. En regel som praktiseres, er at personell fra systemleverandører ikke arbeider på to forskjellige installasjoner samtidig.

Selv om fjernarbeid er regulert i forhold til planlegging av jobber og bruk av AT system, ble det uttrykt en bekymring under ett av intervjuene at økt omfang av fjernarbeid kan føre til mer ad hoc jobbing og mindre detaljplanlegging av arbeidet. Det oppleves som enklere å gjennomføre oppgaver når man sitter på land enn offshore. Personell fra systemleverandører som sitter på land, kan fort bli kastet inn i oppgaver på installasjoner som er ukjente, selv om det i utgangspunktet foreligger grupper som har ansvar for dedikerte installasjoner. Informanter ser ikke nødvendigvis for seg at en systemleverandør får døgnvakt for SAS-systemer på innretninger, men at personell blir satt opp på vakter når noe spesielt skal skje offshore.

5.3 IKT-sikkerhet

IKT-sikkerhet omfatter systemenes evne til å motstå tilsiktede og utilsiktede hendelser, hvor angrep på de industrielle IKT- systemer som oftest er logisk rettet. Mulighet for programvareendringer ved bruk av fjernarbeid fra land, medfører ytterligere krav til IKT-sikkerhet. En fordel ved programvareendringer tilstede på installasjonen, er at man unngår bruk av nettverksstrukturer utenfor de industrielle IKT-systemer, og dermed minimerer mulige angrepsflater og sårbarheter som kan utnyttes ved tilsiktede hendelser. *"Den gangen noen har lyst til å ramme norsk oljevirksomhet så vil det være muligheter"*

Intervjuobjekter forventer at dagens løsninger for fjerntilgang vil bli videreført med enda større vekt på:

- Avlåste rom for fjerntilgang og rutiner for tilgangskontroll, samt forhåndsdefinerte og sterkt begrensede tilganger med klare kjøreregler for hvem som har tilgang.
- Bruk av "rensede PC-er" som kun brukes ved arbeid på industrielle IKT-systemer.
- Cybersikkerhet får økt fokus i kontrakter.
- Overvåking og analyse av nettverk og tilkoblede systemer
- Alle følger etablerte retningslinjer og arbeidsprosesser

Nedenfor presenteres informantenes synspunkter på tiltak som kan forhindre tilsiktede og utilsiktede uønskede handlinger (ikke prioritert liste):

Kontroll av USB minnepinne

Prosedyrer for bruk av USB minnepinne varierer blant operatørselskaper på norsk sokkel. Enkelte selskaper har gjennomført fysisk sikring slik at USB ikke er mulig å bruke, mens andre krever virussjekk før bruk av minnepinne.

Ekstra viruskontroll

Ekstra viruskontroll som gjennomføres før medbrakte PC-er kan kobles opp mot selskapets interne nettverk.

Simulatorer

Hvis operatører opplever en spesiell driftshendelse som de mistenker kan skyldes uautorisert tilgang til industrielle IKT-systemer, kan de prøve å gjenskape forstyrrelsen i en simulator. Simulatoren blir dermed også et viktig tiltak i forhold til cybersikkerhet.

Avlåste rom

Bruk av egne rom med tilgangskontroll ved fjernarbeid er et viktig sikkerhetstiltak.

Kablet nett

Prosedyrer som krever at fjernarbeid skal skje via kablet nettverk og ikke via trådløst nett er et viktig sikkerhetstiltak.

Segregering i systemarkitektur

På nye anlegg med moderne IKT-systemer er det mulig å skille mellom 1) skrivetilgang og lesetilgang, og 2) kritiske og ikke-kritiske systemer. Utvikling av et slikt skille og segregering av nettverk er en vesentlig utfordring for eldre installasjoner hvor industrielle IKT-systemer ble bygd uten tanke på utstrakt deling av data.

På enkelte installasjoner er det egne operatørstasjoner som kun gir lesetilgang og mulighet til å logge seg inn med fjerntilgangsløsning/"remote desktop" for å få tilgang til data som er kopiert ut fra industrielle IKT-systemer. Ifølge informantene er det en utvikling i bransjen mot økt bruk av applikasjoner som kun gir lesetilgang, men arbeidet er krevende siden dette kan medføre omfattende teknologiske endringer i gamle industrielle IKT-systemer. Det er i liten grad anvendt fysiske barrierer som kan forhindre uautorisert tilgang, for eksempel ved bruk av data-dioder som fysisk sikrer at brukere med lesetilgang ikke kan gjøre endringer i systemet [4] I industrielle IKT-systemer med lav grad av segregering, vil en bruker som har fått tilgang til et mindre kritisk system, også kunne få tilgang til andre mer kritiske systemer.

Brannmurer/fysisk begrensning

Både innretninger, landbaserte anlegg og borerigger bruker brannmurer for å hindre uautorisert tilgang fra Internett til selskapenes interne nettverk.

Autentisering

To-faktor autentisering fremheves som et viktig tiltak innenfor IKT-sikkerhet.

Innsiderisiko

Beskyttelse mot innsiderisiko oppleves som vanskelig. Spesiell utfordring hvis betrodde personer mottar trusler. Under intervju ble det gitt eksempler på at personell hadde blitt løst fra kontrakt etter bakgrunnssjekk.

Administrasjonsrettigheter

Søkelys på å begrense antall personer med administrasjonsrettigheter. Spesielt store modifikasjonsprosjekter krever ekstra ressurser for håndtering av cybersikkerhet.

Bevisstgjøring

Intervjuobjektene opplever økt fokus på cybersikkerhet i egne organisasjoner gjennom blant annet kurs og holdningskampanjer. *"Hvis det skjer en driftsforstyrrelse, blir det spurt - "kan det være cyber"? Det skjedde aldri for 5 år siden!"*

6 SINTEFs vurdering av HMS-konsekvenser og IKT-sikkerhet ved fjernarbeid

Nedenfor tolkes og diskuteres resultatene fra intervjuene i forhold til følgende spesifikke tema gitt i Ptils oppgavebeskrivelse (se også Figur 2 i kapittel 2):

- *Konsekvenser for arbeidstakere og endrede rammebetingelser (kontrakter og innleie).*
- *Økt kompleksitet i form av samhandling*
- *Økte sårbarheter og større krav til IKT-sikkerhet i valgte løsninger.*
- *Dilemma mellom organisatorisk sikkerhet vs. IKT-sikkerhet.*

Som teoretisk ramme for diskusjonen om betydningen av funnene knyttet til fjernarbeid, anvendes en tidligere SINTEF-rapport supplert med nyere forskning (se Vedlegg A). SINTEF-rapporten "Risikokartlegging og analyse av Integrerte Operasjoner (IO) med fokus på å synliggjøre kritiske MTO aspekter" [3], ble utarbeidet på oppdrag fra Petroleumstilsynet i 2008. Denne ble utformet som en hypotese om fremtidig utvikling innen IO, og mulige implikasjoner sett i forhold til seks ulike perspektiver på storulykker og robuste/resiliente organisasjoner.

Selv om 2008-rapporten både hadde en bredere inngang ("IO" generelt vs. "fjernarbeid" rettet mot sone 1-3 i denne rapporten, jfr. Figur 1) og var mindre spisset på IKT-sikkerhet, rommet den mange tematikker som er direkte relevante for fjernarbeid, herunder IKT-sikkerhet. Hypotesene om hva IO vil medføre av endringer i arbeidspraksis ut fra et MTO-perspektiv har ikke mistet sin relevans. Tvert imot synes de å være høyaktuelle i forhold til 1) fjernstyring av prosesser og systemer ved hjelp av industrielle IKT-systemer, 2) overvåking av prosesser og systemer og 3) fjernarbeid på industrielle IKT-systemer på tvers av geografisk avstand ved bruk av fjerntilgang (som er fokus i denne studien).

Hovedelementer i vår teoretiske ramme for vurdering av betydning av fjernarbeid er:

- En tilnærming til kompleksitet som handler om å anerkjenne at systemer er under kontinuerlig endring, at endringsdynamikken er knyttet til relasjoner mellom aktørene like mye som lokale tilpasninger, og at dette i sum handler om kontinuerlig balansering av menneskelige, tekniske og organisatoriske forhold (MTO-balanser).
- En beskrivelse av to ulike, men relaterte former for MTO-balanse; 1) balansen mellom arbeidsprosess[2] og arbeidsform[3], og 2) skifte fra et fokus på verdiskaping i den enkelte organisasjon til verdiskaping gjennom grensesnitt for samhandling.
- Et perspektiv på IKT som "re-presentasjons"-teknologi[4] som fremmer et varsku mot at fleksibiliteten i IKT utnyttes slik at fokus blir mer på koordinering av arbeidsprosessen (primærarbeidet) enn på helhetlig forståelse av arbeidet som skal utføres.

Det empiriske materialet i denne rapporten er for lite omfattende til at det kan gjennomføres en hypotesetestende undersøkelse i forhold til dette teoretiske utgangspunktet. Det er imidlertid mulig og etter vår mening rimelig å tolke funnene i lys av dette teoretiske rammeverket som en indikasjon: på en tendens og mulig utvikling. Samtidig gir dette en rettesnor for fremtidig fokus for undersøkelse og forskning.

[2] Omtalt som *primærarbeid* i Vedlegg A.2.1
[3] Omtalt som *sekundærarbeid* i Vedlegg A.2.1
[4] Se Vedlegg A.2

6.1 Konsekvenser for arbeidstakere og endrede rammebetingelser

Utvidelse av fokus fra det å gjennomføre arbeid, til det å planlegge arbeid.

Vi observerer at informantene påpeker:

- Bedre responstid og tilgang til ekspertise på land. Spesifikk kompetanse blir bedre utnyttet mot flere operatør- og boreselskaper.
- Økt samhandling mellom operatør/boreselskaper og systemleverandører i både tidligfase og drift, herunder samarbeid mellom operasjonssentre.
- Personell fra forskjellige organisasjoner samles fysisk i samme lokaler og felles team.
- Bedre muligheter for forberedelse, og at samarbeid etableres mellom "junior" offshore og "senior" onshore.

Høyt endringstempo. Eksperimentering, løpende tilpasninger og fokus på ansvarsforhold i kontinuerlige endringsprosesser.

Vi observerer at informantene påpeker:

- Det er store forskjeller i endringsvilje hos operatør- og riggselskaper.
- Store forskjeller i strategier vedrørende samarbeid med systemleverandører. Dette varierer mellom å samle alle egne SAS-ingeniører på land for å betjene flere innretninger, å beholde SAS-ingeniører offshore for å sikre lokalkunnskap, eller å bygge opp egen spesialistkunnskap på SAS for å være mest mulig uavhengig av systemleverandør vs. å gi systemleverandør ansvar for daglig drift.

Behov[5] for å ikke bare fokusere på arbeidsprosess, men også på underliggende arbeidsform

Vi observerer at informantene påpeker følgende momenter som kan assosieres med arbeidsprosesser:

- Fjernarbeid forventes å gi raskere støtte til operatør- og boreselskap, og systemleverandør kan være bedre forberedt for arbeidet.
- Systemleverandører kan tilby problemløsning 24/7 fra "et eller annet sted i verden".
- Økt kompleksitet i SAS-systemer kan føre til usikkerhet offshore og ekstra behov for å støtte seg til spesialister fra land.
- Deltakelse i studier sammen med operatør gir systemleverandør god systemoversikt og bidrag til utvikling av helhetlige løsninger.
- I boreoperasjoner med svært mange aktører, forventes det at viktige systemer fremdeles vil være atskilte og at operasjonene vil være fragmenterte, men det forventes også at ny teknologi gjør at borepersonell kan ta på seg flere oppgaver.

Vi observerer også at informantene påpeker følgende momenter som kan assosieres med arbeidsformer:

- Det kan bli ad hoc arbeid onshore, når det er problemer offshore som "må" løses. Uregelmessig arbeidstid onshore kan bli resultatet.
- Personell som sitter på land og ikke kjenner at noe "rører på seg" kan ta større sjanser.
- Ved fjernarbeid kan det bli lettere å bruke en person som er tilgjengelig, enn å måtte vente på en som har lokalkunnskap.
- Operatører bruker gjerne tid på å sjekke kompetanse til tilbudt personell, og som ikke har vært på installasjonen tidligere.
- Uttalt skepsis til å tillate programvareendringer på SAS gjennom fjernarbeid. Lokalkunnskap om den enkelte installasjon, fysisk nærhet til installasjon, det vil si forhold utenfor den formelle arbeidsprosessen, fremheves som essensielt.

[5] Se Vedlegg A.2.1 som beskriver primærarbeid og sekundærarbeid i MTO-balanser

- Vektlegging av streng tilgangsregulering (i tid, rom og med tanke på aktivitet) av hensyn til cybersikkerhet gir enda mer fokus på den formelle arbeidsprosessen, og mindre plass til å utvikle arbeidsformer.
- Bruk av chat-funksjoner kan tolkes som et utrykk for behov for å vedlikeholde uformelle arbeidsformer.
- Økt oppmerksomhet på innsiderisiko kan tolkes som et resultat av at personlige inntrykk og relasjoner som skapes gjennom tilstedeværelse på samme fysiske lokasjon, er en del av arbeidsformer som går tapt. Formelle avklaringsmøter, og overvåkning av servicepersonell under arbeid, kompenserer for personlige bekjentskap i et lite faglig miljø
- Vaktordning for systemleverandører av borekontrollsystemer: Deltakelse i vaktlag oppfattes som anerkjennelse av kompetanse, og er derfor attraktivt.
- Fjernovervåking av utførelse av arbeidsprosesser/operasjoner kan oppfattes negativt av systemleverandører.
- Egne rom for fjernarbeid bidrar til bedre konsentrasjon.

Nye beslutningsprosesser som er tuftet på forutsetninger om lett tilgang til store mengder sanntidsdata og uhindret tilgang til variert ekspertise.

Tilgangen på ekspertise vil være knappere enn tilgangen på data

Vi observerer at informantene påpeker:

- Det forventes at avanserte dataanalyse vil erstatte dagens analysearbeid utført av systemleverandørene og redusere behovet for periodisk vedlikehold.
- Vaktordninger bør organiseres slik at personell har lokalkunnskap, og ikke arbeider på to installasjoner samtidig. Likevel betydelig mulighet for at noen blir "kastet inn" i oppgaver på ukjente installasjoner ved ikke-planlagt arbeid utenfor normal arbeidstid. Vakter bør settes opp når noe spesielt skal skje offshore.
- Automatisering av boreoperasjoner gjennom at boreplaner blir direkte implementert i borekontrollsystemet, uten involvering av borer. Dette vil stille større krav til kvalitetssikring av boreplan.
- Utstyr som er vanskelig å automatisere, f.eks på grunn av store vektforskjeller og krav om høyt presisjonsnivå, har likevel et potensial for fjernstyring.
- Systemleverandører for boreutstyr tilbyr spesialtilpassede kurs for operatørpersonell, siden de som blir igjen på boreriggen må ha bedre kompetanse. Opplever en kamp om spisskompetanse innen digitalisering.
- Systemleverandører for boreutstyr krever at operatører kjøper opplæring som en del av leveransen.
- Økt tilgang til spesialistkompetanse er i seg selv et positivt bidrag, men servicepersonell må kjenne anleggets særegenheter.
- Personell som er med fra prosjektfasen til driftsfasen, og som er med på oppstart, vil få bedre lokalkunnskap.
- Rotasjonsordninger bidrar positivt.

Større tilgang til et bredt repertoar av kunnskap, ressurser og ekspertise gjennom grenseflatene mellom ulike aktører

Denne konsekvensen gjelder operatør, systemleverandører og underleverandører i daglige operasjonelle oppgaver og beslutninger, samt i krisesituasjoner.

Vi observerer at informantene påpeker:

- Endringer i SAS planlegges og kontrolleres av både fagspesialister på land og driftspersonell på installasjonen. Systemleverandør kan simulere effekt av foreslåtte endringer før implementering på installasjon.
- Systemleverandører har egne kurs for medarbeidere som skal gjennomføre fjernarbeid.
- Vaktordning for systemleverandører for boreutstyr.

Mulighet og tilrettelegging for tett samarbeid i multidisiplinære team som er uavhengig av den enkeltes organisatoriske og geografiske plassering.

Vi observerer at informantene påpeker:

- Ved kritisk endringer offshore er det lettere å ha tillit til en som sitter i nabostolen, enn en som sitter på land.
- Nye samarbeidsmodeller hvor systemleverandør og operatør sitter samlet på land blir nevnt som en mulighet.

Økt kompleksitet og interaktivitet gjør det vanskeligere å mestre krisesituasjoner

I krisesituasjoner er det avgjørende å vite hvem som faktisk er "til stede".

Vi observerer at informantene påpeker:

- Fjernarbeid krever ekstra oppmerksomhet og beredskap ved uventede hendelser eller situasjoner.
- Enkelte installasjoner har display som viser at "fjernarbeid pågår".

Økt fokus på utvikling og tilgjengeliggjøring av informasjon og kunnskap. Ny kompetanse/forståelse skapes ikke ved deling av data alene

Vi observerer at informantene påpeker:

- Digitalisering vil kunne gi kompetanseheving gjennom økt utnyttelse av data og bedre rapporter.
- Digital tvilling vil kunne medføre økt kunnskap og forståelse om utstyr under drift, og vil kunne fremtvinge (innsats for) økt forståelse.

Personlige/organisatoriske kvalitetsrelasjoner er viktige for å håndtere opplevd inter-organisatorisk kompleksitet.

Opplevd kompleksitet i situasjonen, som (noen ganger) like godt kan benevnes "komplisert", kan i stor grad kompenseres gjennom relasjonsskapende samarbeid. Det relasjonelle perspektivet bør vektlegges.

Vi observerer at informantene påpeker:

- Fjernarbeid er ikke nødvendigvis kompleksitetsskapende. Samarbeid på tvers av selskaper kan virke mer komplekst, men samarbeid bidrar samtidig til at en lærer mer av hverandre.
- Sikkerheten kan til en viss grad forbedres gjennom at tettere samarbeid mellom operatør og systemleverandør gjennom både tidligfase og drift.

Det er imidlertid behov for at næringen skiller klarere mellom hva som er "komplisert" og komplekst". Et begrep som "kvalitetsrelasjoner" er positivt ladet, men bør konkretiseres gjennom eksempler.

Digitale nomader – er det et problem?

Den digitale nomaden kan ha et "hjem", men dette bør være flerfaglig og inter-organisatorisk.

Vi observerer at informantene påpeker:

- Ingeniører opplever at det er mer sosialt å sitte sammen med spesialister på land.
- Jobbinnhold berikes av (periodiske) offshore opphold.
- Den sosiale gevinsten ved å jobbe offshore er begrenset, det er ikke alltid enkelt for serviceansatt å komme i god kontakt med offshorepersonell, og få støtte i arbeidssituasjonen.

Sosialiseringsprosesser mellom digitale nomader, og deres "lokale" samarbeidspartnere", bør studeres nærmere.

Utfordringer ved etablering og vedlikehold av felles situasjonsforståelse over geografiske avstander og kontraktsgrenser.

Det er ingen "quick-fix" for opprettholdelse av situasjonsforståelsen ved fjernarbeid.

Vi observerer at informantene påpeker:

- Kontrollrom flyttes på land samtidig som det utøves fjernarbeid. Selv om f.eks. "remote desktop" også tidligere ble brukt under arbeid på installasjonen, har man mistet muligheten til å ha visuell kontakt med maskinen, lukte/føle, eller å gå til kontrollrom for å få utfyllende opplysninger om hva som foregår.
- Ubemannede installasjoner med færre sikkerhetssystemer må ha mer elektronikk/ instrumentering for å kompensere for manglende folk. Dette påvirker SAS- og kommunikasjonssystemer.
- Lokalkunnskap er viktig. Krevende å sitte i operatørrom når man betjener ulike generasjoner utstyr.
- Større krav til kompetanse for de som ikke er ved anlegget, enn for de som er der.
- Lyd kan være en kilde til situasjonsforståelse, f.eks. ved boreoperasjoner.
- Språk og terminologi gir utfordringer.

"Tap av situasjonsforståelse", "manglende situasjonsforståelse" eller "svak situasjonsforståelse" har ofte blitt referert til som årsak i ulykkesgranskinger [5]. I den praktiske utførelsen av arbeidsoppgaver og arbeidsoperasjoner så er bekymringen i stor grad knyttet til om de som sitter fjernt fra innretningen har eller får den nødvendige informasjonen og innehar lokalkunnskapen som trengs for å utføre oppgavene på en god og riktig måte. I tillegg kan en oversikt over det totale risikobildet, dvs. de andre arbeidsoperasjonene som utføres på innretningen og hvilke konsekvenser ens egen oppgave kan ha for sikker drift, være vanskeligere å oppnå gjennom fjernarbeid. Dette gjelder både for de som utfører fjernarbeid og for de som skal til enhver tid ha oversikt over hvem som er inne i systemene og hvilke andre arbeidstillatelser som er åpne til enhver tid. En er derfor i mange tilfeller i dag avhengig av å ha en "forlenget arm" på innretningen eller anlegget som man kommuniserer med for å vite hva som foregår.

Kommunikasjonen og kontakten mellom kontrollrommet og systemleverandører er i dag tett ved gjennomføring av kritiske systemendringer. Det er derfor nødvendig å identifisere hvilke arbeidsoppgaver som krever tett kontakt med kontrollrommet slik at kontrollromsoperatørene også er informert om det som gjøres av endringer i systemet.

Språk og terminologi kan være en mulig hindring for å oppnå felles situasjonsforståelse og riktig forståelse for oppgaven som skal utføres. Dette er noe man bør være bevisst på ved kommunikasjon, planlegging og utførelse av fjernarbeid.

Behovet for en god felles situasjonsforståelse kan være et argument for at ansatte hos systemleverandører og operatør- og boreselskap bør sitte deler av tiden samlet i et rom/senter for å bygge tverrfaglig kompetanse, forståelse og kunnskap. Man har allerede erfaringer med denne samarbeidsformen både i prosjektorganisering og i drift, noe som blir omtalt som svært positivt av næringen.

Ved fjernarbeid er felles situasjonsforståelse og de informasjonsobjektene som understøtter denne et vesentlig aspekt ved selve arbeidsprosessen. I den grad fjernarbeid vil inngå i mer komplekse samhandlingsmønstre, vil det være behov for økt oppmerksomhet mot de underliggende arbeidsformene som skaper og vedlikeholder situasjonsforståelsen. Det kan da være nyttig å være oppmerksom på at "felles glemsomhet" også kan oppstå gjennom sekundær- og artikuleringsarbeidet (Se Vedlegg A.2.1).

6.2 Økt kompleksitet i form av samhandling

Verdiskapingen skjer i økende grad mellom enhetene, ikke i dem

Vi observerer at informantene påpeker:

- Nye forretningsmodeller for service og livsløpstjenester forventes slik at systemleverandører i større grad tar ansvar for drift og oppetid, og ikke kun får betalt for utstyr og service. Dette medfører krav om oppetid og tilrettelegging for fjernarbeid.
- Systemleverandører involveres i operatørselskapenes satsing på digitalisering gjennom nye applikasjoner og rapporter basert på bearbeidelse av innsamlede data. Tjenester for overvåkning og varsling.
- Systemleverandører er bekymret for en utvikling der de kun får betalt for det de gjør, og ikke for den kunnskapen som legges inn i leveransen.
- Data i seg selv får større verdi, nye samarbeidsformer, samhandling mellom operatørers og systemleverandørers verktøy, og nye forretningsmodeller ledsages av tvil om eierskap, ansvar og betaling.

Dette kan tolkes som et behov for å revidere de formelle beskrivelsene av arbeidsfordeling og ansvar, og at endringsbehovet drives av tilgang til og deling av informasjon. En slik revisjon bør i særlig grad avspeile nettverksdimensjonen. En fruktbar tilnærming til dette kan være å skille mellom linje-, fag- og nettverks-dimensjonene, og forstå dette som bevegelige kompromisser i blandede kunnskapsregimer (se Vedlegg A.2.2 for nærmere beskrivelse).

Kompleksitet kan adresseres positivt gjennom balansen mellom primærarbeid (arbeidsprosess) og sekundærarbeid (arbeidsform), og gjennom skifte mellom selskap og samhandlingsgrensesnitt som forgrunn og bakgrunn.

Vi observerer at informantenes opplysninger reflekterer at:

- Det forventes at personell fra forskjellige organisasjoner samles fysisk i samme lokaler og felles team.
- Data, samhandling mellom systemleverandørers/operatørers verktøy og personell danner i økende grad forgrunn, mens selskapene blir bakgrunn.
- Relasjonsbyggende samarbeid gjør det lettere å håndtere kompliserte/komplekse situasjoner og forhold.

Selv om det ikke foreligger eksplisitte utsagn som understøttet det kompleksitetsbegrepet vi legger til grunn i Vedlegg A, trer det fram et helhetsbilde av en næring som "venner seg til" tanken om at fjernarbeid i overskuelig fremtid vil være en endringsprosess.

I tillegg er det klare indikasjoner på at det teoretiske skillet mellom arbeidsprosess og arbeidsform er meningsfullt for informantene (se f.eks. under punktet " *Store forventninger til utvikling av effektive og ideelle beslutningsprosesser"* i forrige avsnitt*),* og at grenseflatene mellom selskapene blir stadig mer sentrale for informantenes oppmerksomhet. Den tidligere påviste aksepten fra informantene om at kompleksiteten er relasjonell, får dermed en dypere betydning: det er ingen enkeltaktør (i forgrunnen) som kan kontrollere eller redusere kompleksiteten på egen hånd. Det er derfor mulig å anta at aksept av kompleksitet i samhandling også baner veien for aksept av det relasjonelle kompleksitetsperspektivet som er beskrevet i Vedlegg A, som også er knyttet til MTO-balanser.

6.3 Økte sårbarheter og større krav til IKT-sikkerhet i valgte løsninger

Økt bevissthet om cybersikkerhet og systematisk arbeid med risikoreduserende tiltak.
Undersøkelsen indikerer at informantene er oppmerksomme på de ulike IKT-sårbarhetene som kan true den grunnleggende integriteten til de aktuelle tjenestene som inngår i fjernarbeid. Grunnleggende IKT-sikkerhet bør være tydelig og sterkt i overskuelig framtid. Grunnleggende "cyber-hygiene" er helt avgjørende for tilliten til fjernarbeid. Imidlertid, hvis løsningene blir for komplekse, vil det bli praktisk umulig å leve opp til dette idealet.

SINTEFs vurdering er at cybersikkerhet fortsatt er noe umodent på innretninger, landanlegg og borerigger på norsk sokkel. Det er krevende å kombinere IT- og OT-sikkerhet på grunn av kulturforskjeller mellom fagmiljøene.

Fjernarbeid i form av programvareendringer fra land medfører ytterligere krav til cybersikkerhet for å beskytte mot tilsiktede uønskede hendelser. En fordel ved at programvareendringer gjøres på installasjonen, er at man unngår å bruke Internett og dermed er mindre sårbar i forhold til cyberangrep. Generelt er sikkerhetssystemer konstruert for å stenge ned produksjon og gå i sikker tilstand ved uønskede hendelser. Et hacker-angrep vil typisk kunne medføre driftsstans. Det kreves betydelig ekstra lokalkunnskap om anlegget og systemene for å skape en tilsiktet farlig situasjon gjennom for eksempel endring av parametere og settpunkt i et sikkerhetssystem.

Beskyttelse av administratorrettigheter er spesielt viktig siden det på norsk sokkel er lite bruk av datadioder som fysisk sikrer at brukere med lesetilgang ikke kan gjøre enderinger i systemet. Vi merker oss konklusjonen fra PST vedrørende dataangrep mot Helse Sør-Øst [6]. Her har etterforskerne funnet spor som tyder på at dataangrepet mot helseforetaket var organisert fra Kina, og at det er grunn til å frykte at datainntrengerne har klart å kopiere alt de har ønsket av informasjon. Ifølge PST har helseregionen først blitt kompromittert via en server i ekstern sone, som har vært åpen ut mot internett. Herfra har mistenkte tatt seg videre til intern sone, som bare er ment for interne brukere. Mistenkte skaffet seg administratortilganger og har derfor hatt tilganger til intern sone. At inntrengerne har fått administrasjonstilgang, skal være utslagsgivende for at PSTs etterforskning ikke har avdekket hva som er borte.

Ptils satsing og engasjement innenfor cybersikkerhet gir næringen økt fokus på risikoreduserende tiltak.

6.4 Dilemma mellom organisatorisk sikkerhet v. s IKT-sikkerhet

Innen sikkerhetsteori omtales gjerne fravær av ulykker og uønskede hendelser som "Safety-I" og vellykket operasjon under varierende forhold som "Safety-II (se vedlegg A).

Sett i forhold til relasjonell kompleksitet og MTO-balanser må følgende forhold påaktes:

"Safety-I" er en filosofi som

- "klarer seg" med å referere til arbeidsprosessen.
- resonnerer best med selskapet som forgrunn.

"Safety-II" er en filosofi som

- betinger at arbeidsformen også blir vektlagt.
- også resonnerer med grensesnitt som forgrunn (e.g., gjensidig tilpasning).

Vi legger her til grunn at petroleumsnæringen har behov for en organisatorisk sikkerhet som er en dynamisk kombinasjon av "Safety-I" og "Safety-II". Dette forsterkes ytterligere av de foregående perspektivene på IKT som verktøy for makt, beherskelse og kontroll.

Grunnleggende IKT-sikkerhet har tradisjonelt vært basert på premissene for "Safety-I" og arbeidsprosess. Dette resonnerer med informantenes vektlegging av at fjerntilgang til industrielle IKT-systemer må være strengt regulert, og autorisasjonen må være tidsbegrenset og så stram som mulig. Dette innebærer i praksis svært lite rom for utøvelse av fleksible arbeidsformer og "Safety-II", og kan resultere i et virkelighetsbilde basert på urealistiske forutsetninger. I praksis kan man ikke forutsette at alle regler kan overholdes til enhver tid, og det må tas høyde for at det oppstår situasjoner som ligger utenfor det man har tatt høyde for i utformingen av reglene.

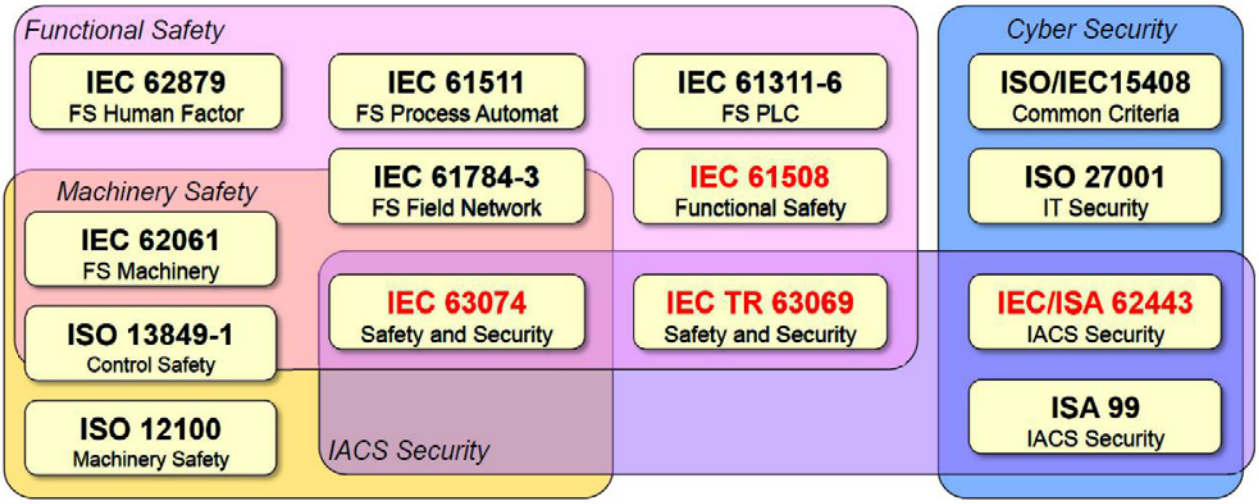
Satt på spissen er det derfor grunnlag for å advare mot at et ensidig fokus på tradisjonell IKT-sikkerhet vil kunne påvirke organisatorisk sikkerhet i negativ forstand, gjennom å gi "Safety-I" forrang på bekostning av "Safety-II". Denne faren er ikke overhengende for fjernarbeid knyttet til industrielle IKT-systemer med klart definerte ansvarsområder så som SAS, men det kan betegnes som et mulig framtidig dilemma.

Med tanke på fremtidig utvikling er det likevel grunn til å anbefale F&U for å formulere en form for IKT-sikkerhet som understøtter organisatorisk sikkerhet på en balansert måte. Organisatorisk sikkerhet må ikke forveksles med IKT-sikkerhet, det vil si rekonstrueres ut fra akutte cyber-beskyttelsesbehov slik at det blir en slagside mot "Safety-I" i form av overdrevent stramme rammer for tilgangene.

7 Standarder og retningslinjer som omfatter fjernarbeid

Figur 3 viser standarder innenfor funksjonell sikkerhet, maskinsikkerhet og IKT-sikkerhet som er relevant for industrielle IKT-systemer relatert til Ptils myndighetsområde.

Det pågår arbeid relatert til standardene IEC 63073 og IEC 63069 som spesielt ser på harmonisering av "safety-" og "security-"krav til industrielle IKT-systemer. Dokumentasjon av dette arbeidet finnes foreløpig kun som utkast [7].



Figur 3 Sammenheng standarder innenfor funksjonell sikkerhet, maskinsikkerhet og IKT-sikkerhet [7]

Ifølge gruppeintervjuene legger operatørselskaper IEC-standarder til grunn for sin virksomhet (IEC 61511 og 62443). Boreleverandører bruker ISO 13849 vedrørende maskinsikkerhet.

Boreleverandører opplever at det er utfordrende å finne utstyr som både tilfredsstiller ISO 13849 og som har ATEX klassifisering. Markedet er lite så det er vanskelig å få sertifisert utstyr som er tilpasset kravene. På grunn av restriksjoner og manglende muligheter for tilkobling av sensorer, er det svært utfordrende å implementere komplisert styring av maskiner i en PLS som er sertifisert i henhold til IEC 61508.

I Tabell 4 presenteres en oversikt over utvalgte standarder og retningslinjer rettet mot industrielle IKT-systemer og som også omhandler fjernarbeid, HMS og IKT-sikkerhet. I oversikten er det tatt med referanse for nedlasting eller bestilling av dokumentet.

En mer detaljert oversikt er gitt i Vedlegg B.

Tabell 4 Utvalgte standarder og retningslinjer spesielt relevant for fjernarbeid, HMS og IKT-sikkerhet

Referanse	Tittel	Lenke
Standarder		
ISA/IEC 61511 series	Functional safety - Safety instrumented systems for the process industry sector	Bestilles http://www.standard.no/nettbutikk/sokeresultater/?search=61511
ISA/IEC 62443 series	Industrial Automation and Control Systems Security	Bestilles: http://www.standard.no/nettbutikk/sokeresultater/?search=62443
ISO 13849 series	Safety of machinery -- Safety-related parts of control systems	Bestilles https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=805783
IEC 63069	Industrial process measurement, control and automation. Framework to bridge the requirements for safety and security	*Working draft*
IEC 63074	Security aspects related to functional safety of safety related components	*Working draft*
Retningslinjer		
Norwegian Oil and Gas RP 104	104 – Norwegian Oil and Gas recommended guidelines on information security baseline requirements for process control, safety and support ICT systems. (Rev 06. December 2016)	https://www.norog.no/contentassets/15263fd7f781409286f319bbeb427d93/104-recommended-guidelines-on-security-baseline-requirements.pdf
DNV-GL-RP-G108	Cyber security in the oil and gas industry based on IEC 62443 (2017)	https://www.dnvgl.com/oilgas/download/dnvgl-rp-g108-cyber-security-in-the-oil-and-gas-industry-based-on-IEC-62443.html
DNV GL-RP-G0496	**MARITIME** Cyber security resilience management for ships and mobile offshore units in operation (2016)	https://www.dnvgl.com/maritime/dnvgl-rp-0496-recommended-practice-cyber-security-download.html
NIST 800-82 R2	Guide to Industrial Control Systems (ICS) Security (2015)	http://dx.doi.org/10.6028/NIST.SP.800-82r2
NIST 800-46 R2	Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security (2016)	https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final#pubs-abstract-header
NCSC End user Technology	Deployment and management of technology used by the employees, partners, or customers of an organisation.	https://www.ncsc.gov.uk/topics/end-user-technology
NIST	Framework for Improving Critical Infrastructure Cybersecurity, V1.1 Draft 2 (2017)	https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf
ISA-TR84.00.09	Cybersecurity Related to the Functional Safety Lifecycle (2017)	Bestilles: https://www.isa.org/store/isa-tr840009-2017,-cybersecurity-related-to-the-functional-safety-lifecycle/56889051
ISACA COBIT 5	COBIT 5	https://www.isaca.org/ecommerce/Pages/Cobit5-Download-Registration.aspx
Veiledninger myndigheter		
HSE	Cyber Security for Industrial Automation and Control Systems (IACS)	http://www.hse.gov.uk/foi/internalops/og/og-0086.pdf

8 Anbefalinger og videre arbeid

8.1 SINTEFs anbefalinger til næringen

Med utgangspunkt i denne intervjustudien har SINTEF følgende anbefalinger til næringen:

- Fortsatt søkelys på tilgangskontroll og administrasjonsprosedyrer som også er brukervennlige for autorisert personell.
- Økt samarbeid mellom operatørselskaper og serviceselskaper hvor de også regelmessig er fysisk samlet.
- Sterkere søkelys på krav til egnede rom for fjernarbeid, inklusive arbeidsforhold, vaktordninger, adgangskontroll, samt tiltak for å fremme nødvendig tankesett og bevisstgjøring for kritisk arbeid på industrielle IKT-systemer.
- Mer bruk av hardware-baserte informasjonsdioder for å unngå utilsiktet tilgang til kritiske industrielle IKT-systemer og derigjennom også gi enklere tilgang til de som kun behøver lesetilgang.

8.2 Behov for kunnskapsinnhenting

I tillegg til de kunnskapsinnhentingene Ptil allerede har igangsatt vedrørende innsiderisiko og infrastruktur og teknologi innen industriell kontroll- og sikkerhetssystemer, anbefaler SINTEF at det innhentes ytterligere kunnskap om:

- Hvordan kombinere "safety" og "security" for industrielle IKT-systemer, inklusive håndtering av kulturforskjeller i utvikling og drift av IT-systemer og industrielle IKT-systemer?

Det er behov for å etablere et bredere empirisk grunnlag for å verifisere tendensene i de fire temaområder som ble spesifisert i Ptils oppdragsbeskrivelse. Dette gjelder spesielt kunnskap om:

- Hvordan håndtere arbeidstidsordninger (f.eks vaktordninger) ved økt grad av fjernarbeid?
- Hvordan håndtere uventede situasjoner under samhandling, inklusive kunnskap om hvorfor ting går bra?
- Hvordan balansere krav til IKT-sikkerhet, arbeidsprosesser og driftssikkerhet for å unngå at personell omgår IKT-sikkerhetstiltak. Dette kan danne grunnlag for en veiledning som setter grenser for teknisk kompleksitet og digital sårbarhet.
- Hvordan unngå at rigide regler for IKT-sikkerhet begrenser mulighetsrommet for håndtering av uforutsette hendelser?

Referanser

[1] DNV-GL-RP-G108. (2017) "Cyber security in the oil and gas industry based on IEC 62443", https://www.dnvgl.com/oilgas/download/dnvgl-rp-g108-cyber-security-in-the-oil-and-gas-industry-based-on-IEC-62443.html

[2] Rosness, R, U. Forseth & I. Wærø (2010), Rammebetingelsers betydning for HMS-arbeid, https://www.sintef.no/globalassets/upload/teknologi_og_samfunn/sikkerhet-og-palitelighet/sintef-a16296-rammebetingelsers-betydning-for-hms-arbeid.pdf

[3] Grøtan, T.O. & E. Albrechtsen (2008), Risikokartlegging og analyse av Integrerte Operasjoner (IO) med fokus på å synliggjøre kritiske MTO aspekter, SINTEF report A7085

[4] M. G. Jaatun, M. B. Line & T.O Grøtan "Secure Remote Access to Autonomous Safety Systems: A Good Practice Approach", *International Journal of Autonomous and Adaptive Communications Systems* 2.3 (2009): 297-312. https://brage.bibsys.no/xmlui/bitstream/handle/11250/2431792/SINTEF%2BS8699.pdf

[5] Dekker Sidney (2013), "On the epistemology and ethics of communicating a cartesian consciousness", *Safety Science*, 56, pp. 96-99.

[6] Trym Mogen og Gunnar Hultgreen, Hacket norsk helseregion - PST henlegger saken, Dagbladet, 5. desember (2018) https://www.dagbladet.no/nyheter/hacket-norsk-helseregion---pst-henlegger-saken/70535470

[7] Kanamaru, Hiroo (2017), "Bridging Functional Safety and Cyber Security of SIS/SCS", In Proceedings of the SICE Annual Conference 2017, Kanazawa, Japan

Vedlegg

A Teoretisk fundament

Dette vedlegget gir et teoretisk fundament for vurdering av de empiriske funnene under gruppe-intervjuene. Vedlegget er basert på nyere forskning som adresserer interorganisatorisk og relasjonell kompleksitet relevant for fjernarbeid, og to tidligere rapporter SINTEF har utarbeidet for Petroleumstilsynet:

- "Rammebetingelsers betydning for HMS-arbeid"[6]
- "Risikokartlegging og analyse av Integrerte Operasjoner (IO) med fokus på å synliggjøre kritiske MTO aspekter"[7]

Formålet er å avtegne et større bilde vedrørende:

- Konsekvenser for arbeidstakere og endrete rammebetingelser (kontrakter og innleie).
- Økt kompleksitet i form av samhandling
- Økte sårbarheter og større krav til IKT-sikkerhet i valgte løsninger.
- Dilemma mellom organisatorisk sikkerhet vs. IKT-sikkerhet.

Oppsummert gir vedlegget:

- En tilnærming til kompleksitet som handler om å anerkjenne at organisasjoner er under kontinuerlig endring, at endringsdynamikken er relasjonell, og et søkelys på å balansere menneskelige, tekniske og organisatoriske forhold (MTO-balanser)
- En beskrivelse av to ulike, men relaterte former for MTO-balanse; 1) balansen mellom primærarbeid (arbeidsprosess) og sekundærarbeid (arbeidsform), og 2) et skifte i verdiskaping slik at den i økt grad skjer ***mellom*** organisatoriske enheter og ikke ***i*** enheter.
- Et perspektiv på digital teknologi som bærer av en "hyper-virkelighet" der tekniske og sosiale systemer og komponenter, satt på spissen, blir representert hovedsakelig ut fra deres evne til rekonstruksjon av helheten ut fra ulike og skiftende formål.

A.1 Konsekvenser for arbeidstakere og endrete rammebetingelser (kontrakter og innleie)

Rammebetingelser er *forhold som påvirker de praktiske muligheter en organisasjon, organisasjonsenhet, gruppe eller individ har til å holde storulykkesrisiko og arbeidsmiljørisiko under kontroll* (Rosness m. fl., 2010). Dette innebærer at rammebetingelser har en indirekte påvirkning på arbeidsmiljørisiko og stor-ulykkesrisiko ved at de påvirker handlingsrom, samhandlingsmuligheter, ressurser mm. Kontrakter og innleie, kunnskap og kompetanse, incentivordninger og organisatoriske endringsprosesser kan være eksempler på slike rammebetingelser.

[6] Rosness, R, U. Forseth & I. Wærø (2010), Rammebetingelsers betydning for HMS-arbeid, https://www.sintef.no/globalassets/upload/teknologi_og_samfunn/sikkerhet-og-palitelighet/sintef-a16296-rammebetingelsers-betydning-for-hms-arbeid.pdf

[7] Grøtan, T.O. & E. Albrechtsen (2008), Risikokartlegging og analyse av Integrerte Operasjoner (IO) med fokus på å synliggjøre kritiske MTO aspekter, SINTEF report A7085

Rammebetingelser handler altså ikke bare om næringens forhold til myndigheter og andre eksterne faktorer, men også om økt interorganisatorisk kompleksitet i næringen som er et lite adressert felt mht. sikkerhet generelt (Milch, 2018)[8], og i endra mindre grad adressert med hensyn på IKT-sikkerhet.

Rammebetingelser slår også ut på individnivå. I SINTEF (Rosness m.fl., 2010) har vi tidligere brukt begrepet *nomader* for å sette søkelys på effekten av at arbeidstakere mister sosial forankring til omgivelsene der samarbeidet foregår. Med økt digitalisering får vi en dobbel effekt; *digitale* nomader og økt interorganisatorisk kompleksitet som følge av nye IKT-skapte muligheter for arbeidsdeling og organisering. Digitale nomader kan i kraft av egen spesialkompetanse enda lettere bli invitert til sporadiske, usammenhengende eller "flyktige" relasjoner, og/eller bli henvist til å overta "stafettpinnen" fra kolleger, med få muligheter til å sosialiseres inn i felles referanser. Slike felles referanser kan i tillegg i seg selv fremstå som mindre stabile enn de tidligere har vært. Dette bidrar til å gjøre det vanskelig å utvikle f.eks. "høykvalitetsrelasjoner" på et personlig plan, og/eller støtte seg på langvarige organisatoriske relasjoner på mellomlederplan, tiltak som i prinsippet kan kompensere for interorganisatorisk kompleksitet (Milch & Laumann 2016[9], 2017[10], 2018[11], Milch 2018).

Ulike konsepter og former for fjernarbeid har imidlertid ikke oppstått verken tilfeldig eller i et diskursivt vakuum. Selv om utviklingen på ingen måte kan beskrives som deterministisk, og selv om begrepet "IO" til tider kan ha fremstått like mye som floskel som substans, er det vanskelig å se bort fra at begrepet og oppmerksomheten rundt "IO" har formet både forventninger, prioriteringer og muligheter over en tiårsperiode og vel så det i norsk petroleumsvirksomhet. SINTEF-rapporten (Grøtan m. fl., 2008) identifiserte følgende mulige hovedendringer knyttet til menneskelige og organisatoriske faktorer i IO-utviklingen:

- Mer eksplisitt tydeliggjorte operasjoner basert på definerte scenarier og integrert planlegging. Utvidelse av fokus fra det å drive operasjoner, til det å planlegge (integrerte) operasjoner
- Høyt endringstempo. Eksperimentering, løpende tilpasninger og fokus på ansvarsforhold i kontinuerlige endringsprosesser
- Store forventninger til utvikling av effektive og ideelle beslutningsprosesser med koordinert samhandling som resultat. Dette innebærer spesielle utfordringer knyttet til mange aktører i nye konstellasjoner, herunder spenning mellom ønsker om utvikling av effektive arbeidsprosesser og mer tidkrevende utvikling av tilhørende samarbeidsformer
- Nye beslutningsprosesser som er tuftet på forutsetninger om lett tilgang til store mengder sanntidsdata og uhindret tilgang til variert ekspertise.
- Endrede kommunikasjonsformer og nye gruppesammensetninger gir både fattigere og rikere kommunikasjonskanaler.
- Utfordringer ved etablering og vedlikehold av felles situasjonsforståelse over geografiske avstander.
- Økt fokus på utvikling og tilgjengeliggjøring av informasjon og kunnskap

[8] Milch, V. 2018. The influence of interorganizational complexity on safety: Safety challenges and opportunities in the petroleum industry. Doctoral Thesis at NTNU, Trondheim (2018:219)

[9] Milch, V. & K. Laumann. 2016. Interorganizational complexity and organizational accident risk: A literature review. Safety Science 82 (2016), 9-17.

[10] Milch, V. & K. Laumann. 2017. Which types of leadership behaviours can promote safety in an interorganizational context? Risk, Reliability and Safety: Innovating Theory and Practice -Walls, Revie and Bedford (eds) © Taylor & Francis Group, London, ISBN 978-1-138-02997-2 ESREL 2017

[11] Milch, V. & K. Laumann. 2018.Sustaining Safety Across organizational boundaries: a qualitative study exploring how interorganizational complexity is managed on a petroleum-producing installation. Cognition, Technology and Work, https://doi.org/10.1007/s10111-018-0460-8

- Større tilgang til et bredt repertoar av kunnskap, ressurser og ekspertise gjennom grenseflatene mellom ulike aktører (hos operatør, systemleverandører og underleverandører) i daglige operasjonelle oppgaver og beslutninger, samt i krisesituasjoner
- Mulighet og tilrettelegging for tett samarbeid i multidisiplinære team som er uavhengig av den enkeltes organisatoriske og geografiske plassering.
- "IO-fisering" av sikkerhetsstyring. Nye måter for presentasjon og analyse av sikkerhetsdata, og dermed potensial for forbedringer av metoder/verktøy og arbeidsprosesser. Sanntidsdata i kombinasjon med tilgang på spesialister gir mulighet til styrking av tekniske barrierer, herunder raskere feildeteksjon og normalisering. Endringer i premisser kan svekke menneskelige og organisatoriske barrierer og robust arbeidspraksis
- Økt kompleksitet og interaktivitet gjør det vanskeligere å mestre krisesituasjoner

I 2008 ble dette utviklet og presentert som et mulig endringsbilde[12] knyttet til IO. Vi tror at dette er et godt grunnlag for empirisk undersøkelse av utviklingen fram til i dag, ikke minst fordi de ble utarbeidet med tanke på MTO-samspill og mulige HMS-konsekvenser.

A.2 Økt kompleksitet i form av (IKT-støttet) samhandling

Kompleksitet er et begrep som er fristende å ta i bruk når usikkerheten råder, men er samtidig vanskelig å definere. Det har ganske lenge vært et "monsterbegrep" med mange betydninger, og blitt brukt på temmelig ulike måter.

En av de vanligste tilnærmingene for å definere kompleksitet er å peke på uoversiktligheten som oppstår når antallet aktører/komponenter, og antallet koplinger mellom dem, øker sterkt. Tendensen i nyere vitenskapelige tilnærminger, f.eks i aktør-nettverk teori, til å nedtone forskjellen eller reformulere relasjonen mellom det menneskelige og det tekniske, bidrar også til at det blir mer nærliggende å benevne slike systemer som "komplekse" (les: uoversiktlige eller uforståelige ut fra tradisjonelle forståelsesrammer).

Fjernarbeid/IO hører definitivt med i dette "feltet", ikke minst fordi de kapasitetene ved digital teknologi som det fokuseres på (stadig) endres/utvides dramatisk. For få år siden var vi opptatt av dataoverføring fra A til B, i dag er vi opptatt av å dra nytte av "kunstig intelligens" (AI) som etter manges mening kan endre (MTO) spillereglene dramatisk. Gårsdagens opplevde "kompleksitet" blir derfor smålåten sammenlignet med dagens eller fremtidens teknologi. Det blir stadig mindre relevant å peke på at digital teknologi "egentlig" bare handler om å skille mellom og "trikse" med 0-ere og 1-ere i spektakulært tempo. Selv om utsagnet er riktig, forteller det praktisk talt ingen ting om hva som er implikasjonene av f.eks. fjernarbeid med dagens teknologiske status og utsikter.

Det kan imidlertid stadig stilles spørsmål ved om hvorvidt *uoversiktligheten* bør betegnes[13] som *komplisert* eller *kompleks*. Det kan være greit å ha i mente at et komplekst system *ikke bare er vanskelig* (komplisert) å modellere eller forklare; betegnelsen "kompleks" bør reserveres for systemer der det må forventes at innsikten i og kunnskapen om systemets funksjonsmåte er flyktig, at systemet per se er i bevegelse og dermed kan ha endret seg innen man er ferdig med å modellere, eller på annen måte forstå en avgrenset hendelse eller funksjonsmåte. At (tekniske) systemer hele tiden endres eller oppdateres uten at alle – eller kanskje noen - overskuer konsekvensene er én viktig side av dette, men det hører også med at kompleksitet har et holistisk premiss; MTO-helheten kan være *mer enn summen* av delene, og "mer" kan slå ut både

[12] Benevnt "Den store muligheten" (DSM)
[13] Se f.eks Kurtz og Snowden 2003: http://alumni.media.mit.edu/~brooks/storybiz/kurtz.pdf . Her benevnes "komplisert" som "knowable"

positivt og negativt i forhold til akseptable intensjoner og forventninger. Et system benevnt som "komplekst" kan følgelig også forventes å være "selv-organiserende"; det kan oppstå nye funksjonsmåter eller samhandlingsmønstre uten at det foreligger et design eller en intensjon fra en "styrende" eller "ansvarlig" aktør. "Graden" av kompleksitet behøver heller ikke være konstant, det er ikke urimelig å anta at ett og samme system f.eks. kan "pendle[14] " mellom komplisert og komplekst, avhengig av omstendighetene.

Det er imidlertid vanskelig for ikke å si umulig å lokalisere, gripe eller styre "kompleksitet" som selvstendig eller håndgripelig fenomen. Vår tilnærming til kompleksitet handler derfor mer om å akseptere et premiss om at det tilsynelatende forståtte og stabile er i endring, at innsikt/forståelse kan ha en flyktig karakter, at funksjonsmåter kan endre seg både umerkelig og plutselig/radikalt (som en såkalt diskontinuitet), og at disse karakteristikkene opptrer innen en tidshorisont som gjør at de må tas på alvor i det daglige, ikke bare som en fjern eller eksotisk mulighet.

Kompleksitet er med dette ikke noe som oppstår med fjernarbeid, det er mer et premiss man (omsider) velger å akseptere, og dermed forbereder seg på å forstå og håndtere implikasjonene av. Men en slik aksept vil være retningsløs og til dels meningsløs hvis den ikke er ledsaget av en interesse for hvilke forhold som kan generere kompleksitet, eller påvirke "Intensiteten" i denne. Vårt hovedgrep i denne rapporten er i så måte (som for 2008-rapporten) å sette fokus på *relasjonelle* aspekter. Dette er i tråd med nyere forskning på interorganisatorisk kompleksitet og sikkerhet i petroleumsnæringen på norsk sokkel (Milch 2018)[15] der det anbefales å legge vekt på kvalitets*relasjoner* mellom fagarbeidere i ulike selskaper og langvarige, tillitsskapende relasjoner mellom mellomledere for å motvirke inter-organisatorisk kompleksitet. Det er også i samsvar med nyere forskning på kompleksitet i kriser (Johannesen 2017)[16], der fokuset dreies mer mot "Complex *Responsive* Systems/Processes" enn det tradisjonelle fokuset på "Complex *Adaptive* Systems".

Et nøkkelspørsmål vil derfor bli om og på hvilken måte IKT og fjernarbeid bidrar til, eller påvirker (kompleksiteten i/fra) viktige relasjoner knyttet til, f.eks., drift og håndtering av driftsforstyrrelser, eller modifikasjon og vedlikehold av industrielle IKT-systemer.

Én måte å adressere relasjonelle aspekter på er å fokusere på (presumptivt skjøre) MTO- balanser og -likevekter for å forstå samarbeid i en IO-kontekst, slik det ble gjort i SINTEF 2008 rapporten. En slik tilnærming vil ikke handle om å finne og verne én enkelt kritisk MTO-balanse, men flere samtidige balanser i ulike, men overlappende (økologiske) nisjer av samhandling der fjernarbeid inngår. Hver av disse forventes å være i en dynamisk likevekt, der likevekt er et resultat av kontinuerlig tilpasning.

Vi vil i det følgende fokusere på to ulike perspektiver på slike MTO-balanser som kan bidra til å belyse potensiell kompleksitet i samhandling der fjerntilgang inngår.

[14] Se Kurtz og Snowden 2003: http://alumni.media.mit.edu/~brooks/storybiz/kurtz.pdf
[15] Milch, V. 2018. The influence of interorganizational complexity on safety: Safety challenges and opportunities in the petroleum industry. Doctoral Thesis at NTNU, Trondheim (2018:219)
[16] Johannessen, S., 2017. Strategies, Leadership and Complexity in Crisis and Emergency Operations. Routledge Advances in Management and Business Studies

A.2.1 Grunnleggende MTO-balanser; primærarbeid, sekundærarbeid, artikuleringsarbeid og felles glemsomhet

Den grunnleggende MTO-balansen vi fokuserer på her handler om å forstå og ta hensyn til samarbeidets relasjonelle og sosiale natur. Dette er påpekt av Hepsø (2006)[17] som i IO-sammenheng oppfordret næringen til å være mer oppmerksom på sosiale og relasjonelle forhold som faktisk bidrar til robusthet i organisatorisk samhandling. Hepsø legger til grunn et skille mellom primærarbeid og sekundærarbeid, og argumenterer for en balansert integrasjon av disse. Primærarbeid er kort fortalt de aktivitetene som direkte adresserer spesifikke agendaer og mål i en gitt arbeidssituasjon, og som dermed også er det primære grunnlaget for å identifisere et sett av aktiviteter i en samhandlings*kjede*. Når flere aktiviteter griper inn i hverandre, kan dette kalles en samhandlings*matrise*. Alt arbeid som kommer i tillegg til primærarbeidet, *for å gjøre primærarbeidet gjennomførbart*, inkludert re-organisering og vedlikehold av kjeden eller matrisen, kalles sekundærarbeid. En spesiell variant av sekundærarbeid er *artikuleringsarbeid*; essensen i dette er å forene og forsone usammenlignbare antakelser og prosedyrer i fravær av relevante standarder/prosedyrer som kan "påtvinges" partene. Artikuleringsarbeidet kjennetegnes av at det løser inkonsistenser ved å pakke sammen kompromisser som "får jobben gjort", som løser situasjonen lokalt og temporært slik at man kan gå videre. "Lukkingen" handler om å skape enighet, men denne enigheten kan også handle om å se bort fra noe som ikke lar seg løse på annen måte. Hvis, eller når artikuleringsarbeidet ikke er representert i arbeidsbeskrivelsene, så vil det være vanskelig å analysere det faktiske arbeidet som foregår. For denne rapporten er implikasjonen at hvis fjernarbeid skal forstås som noe mer enn enkeltaktørers bruk av teknologi, så må vi forsøke å forstå aktørenes felles konstruksjon og integrasjon av primærarbeid, sekundærarbeid og artikuleringsarbeid, grunnleggende forstått som MTO-balanser.

Premisset om at artikuleringsarbeidet også kan kreve eller føre til en "felles glemsomhet" kan virke uvant, men resonerer med historiske røtter i sikkerhetsforskningen, formulert lenge før dagens IKT-løsninger og -prospekter var aktuelle. Med referanse til Barry Turner (1978)[18] skrev f.eks. Karl Weick i 1998[19] at "*organizations are defined by what they ignore – ignorance that is embodied in assumptions – and by the extent to which people in them neglect the same kinds or considerations*". Dette er et viktig *kontrapunkt* til mer alminnelige organisasjonsforståelser der det intuitivt søkes etter løsninger for "felles kunnskap/situasjonsforståelse" o.l. som understøtter primærarbeidet på en direkte og instrumentell måte. Hvis forståelsen av sekundærarbeidet blir for ensidig innrettet mot denne ene melodilinjen, det å skape fellesnevnere som "alle" forstår på samme måte slik at primærarbeidet glir lettere, står man også i fare for å overse noe helt vesentlig ved inter- så vel som intra-organisatorisk kompleksitet, nemlig at bindemiddelet (sekundærarbeidet) like godt kan være felles glemsomhet, som felles referanser. Fenomenet "variable disjunction[20] " (Turner 1978) er sannsynligvis uunngåelig, selv med "uendelig" informasjonstilgang - og kanskje nettopp da.

[17] Hepsø, V., 2006. Intelligent energy in E&P: When are we going to address organizational robustness and collaboration as something else than a residual factor? Paper at the 2006 SPE (Society of Petroleum Engineers) Intelligent Energy Conference and Exhibition in Amsterdam, The Netherlands, 11-13 April 2006. See https://www.onepetro.org/conference-paper/SPE-100712-MS

[18] Turner, B., 1978. Man-made disasters. Wykeham Publications, London.

[19] Weick, K.E., 1998. Foresights of Failure: An Appreciation of Barry Turner. Journal of Contingencies and Crisis Management. Volume 6, Number 2, June 1998, pp 72-75

[20] "A complex situation in which a number of parties handling a problem are unable to obtain precisely the same information about the problem so that many different interpretations of the problem exist". …when problems use symbolic or verbal variables, have vague, non-quantifiable goals and lack available routines for their solutions, relying instead on ad hoc procedures, variable disjunction of information is likely to be found"

I forhold til fjernarbeidets sosiale og relasjonelle natur risikerer man altså å undervurdere noe som både er potensielt farlig, men også en mulig strategi for forbedring. Hvis Hepsø, Turner og Weick (og mange andre) har rett, så har altså næringen (og mange andre) lange tradisjoner for å overse en kilde til kompleksitet, nemlig behovet for artikuleringsarbeid, inkludert at dette kan arte seg som en "felles glemsomhet" som kamuflerer "variable disjunction". Denne "tradisjonen" har eksistert lenge før IKT/fjernarbeid ble anerkjent som en utfordring på den måten som legges til grunn i denne rapporten.

Vår vurdering er at det nå er på høy tid å løfte opp slike perspektiver, og Hepsø's (2006) forelegg av dette er fremdeles et godt utgangspunkt for å komme videre, både for å forstå det underliggende bidraget til (inter- så vel som intra-organisatorisk) kompleksitet, og det potensielle bidraget til økt robusthet og resiliens som artikuleringsarbeid representerer ift "hovedmelodilinjen[21]" primærarbeid. Slik sett er sekundærarbeidet et kontrapunkt til primærarbeidet. Samtidig rommer artikuleringsarbeidet i seg selv et kontrapunktisk element i form av "felles glemsomhet" som løper parallelt med anstrengelsene for å skape felles referanser som legitimerer "lukking".

Viktige spørsmål er hvordan en slik balanse kan skapes og opprettholdes når fjernarbeid inngår, hvordan den kan påvirkes, tapes eller forskyves. Vil fjernarbeid kunne påvirke artikuleringsarbeidet i retning av felles eksplisitte referanser eller felles glemsomhet, eller vil det bare kunne understøtte et forsøk på å eliminere behovet for artikuleringsarbeid gjennom å styrke primærarbeidet?

Hepsø (2006) fokusere på hvordan delte informasjonsobjekter skapes gjennom dialog der man forsøker å gjøre seg forstått på tvers av fag- og profesjonsgrenser ("perspective making" og "perspective taking"), og betegnelsen "grenseobjekter[22]", dvs. objekter som fungerer som mer eller mindre automatiserte "oversettere" mellom samhandlende "arter" eller aktører innen en samhandlingsnisje. Formelle representasjoner av kunnskap (datamodeller, formaliserte informasjonsstrukturer, "dashboards") kan i prinsippet aldri bli snarveier til å skape slike grenseobjekter, og er derfor heller ikke tilstrekkelig underlag for beslutningstaking uten tilhørende artikuleringsarbeid. For at grenseobjekter skal fungere må det være rom for en aktiv forhandling og meningsskaping[23] rundt disse objektene, og dette (artikuleringsarbeidet) er i seg selv en "balansegang" som er sensitiv, bl.a., for hvem som deltar, og hvilke relasjoner disse har fra før. Det sier seg da nærmest selv at en "digital nomade" vil kunne møte spesielle utfordringer når han eller hun involveres sporadisk i dette. Et tilsynelatende velfungerende grenseobjekt, som aktørene stoler *for mye* på, vil dessuten kunne være farlig i seg selv. Undersøkelsen bør derfor være innrettet på å forstå om, og hvordan, aktørene utvikler mekanismer for å håndtere åpenbart inkonsistente IKT-systemer og infrastrukturer, men også om eller hvordan de er i stand til å *identifisere de mindre åpenbare* behov for slike mekanismer og strategier, når situasjonen krever dette.

Hepsø (2006) påpeker dessuten at det er en fundamental sammenheng mellom artikuleringsarbeid og tillit, og viser til at opparbeidelse av tillit og forpliktelser i ulike situasjoner er komplekse prosesser i seg selv[24]. Dette avleder viktige spørsmål slik som: Hva er "primærarbeid", hva er "sekundærarbeid", og hva er "artikuleringsarbeid" for etablering og vedlikehold av tillit og forpliktelse i fjernarbeid?

Så langt har vi beskrevet IKT-løsninger (for fjernarbeid) som noe avansert/komplisert som er "passivt" tilgjengelig for bruk i arbeidsprosesser, og som inngår i en MTO-konstellasjon der det hovedsakelig er den menneskelige/sosiale komponenten som forårsaker at den sosiotekniske helheten beveger seg, f.eks.

[21] I tråd med metaforen kan vi da kanskje si at "balansering" er det samme som "harmonisering"
[22] "Boundary objects"
[23] F.eks. som foreslått av Ellingsen og Monteiro 2003: "enacting, orchestrating and organizing"
[24] "Work organizations can be seen as a complex structure of organized commitment"

mellom komplisert og komplekst. Vi skal ikke rokke ved dette og derved tillegge teknologien en overdreven egen-kompleksitet, men vil likevel påpeke at dette MTO-samspillet kan være/bli enda mer intrikat/komplekst enn det vi har beskrevet så langt. IKT kan nemlig også forstås som en *re*[25]-presentasjonsteknologi (Grøtan, 2007)[26] som skaper nye betingelser for beherskelse og kontroll i et komplekst system. IKT kanaliserer dermed en ny form for *makt*[27] der virkelighet avløses eller suppleres av en "re-presenterert" og stadig re-organisert virkelighetsforståelse. En slik "hyper-virkelighet[28]" er attraktiv fordi den kan endres løpende ut fra rådende/skiftende mål og intensjon. Et slikt IKT-perspektiv kan medføre at vi må reformulere begreper som "rike vs fattige informasjonskanaler" radikalt, og det kompliserer også forståelsen av det som Hepsø referer til som "perspective making/taking" og grenseobjekter, herunder tillit og forpliktelser knyttet til disse. Vil responsen bli en mer aktiv meningsskapings- og forhandlings-prosess utøvd som artikuleringsarbeid, eller en kapitulasjon for "overmakten" og derved et mer amputert artikuleringsarbeid?

Et annet, nærliggende[29] perspektiv er å se på den stadig økende produksjonen av informasjon som en selvdreven spiral som understøtter en "garbage can" beslutningsprosess snarere enn en prosess med et klart definert mål og mening. Grøtan (2007:84) oppsummerer dette med at

- Informasjon er både
    a. en beskrivelse av, og en referanse til tilstander og relasjoner i et gitt referanseområde, men også
    b. selvrefererende, dvs. en relasjon til andre, tidligere beskrivelser innen samme domene. Eksisterende informasjon "produserer" derved ny informasjon når den kombineres med "fersk" informasjon
- Evnen til samspill mellom moderne, standardiserte IKT-infrastrukturer øker kombinasjonsmulighetene dramatisk
- Informasjonen er forgjengelig og kan lett erstattes. Informasjonsinnholdet – *nyhetsverdien* – er per definisjon et *forbigående og forgjengelig* resultat. Forringet informasjonsinnhold må stadig kompenseres gjennom oppdatering og reproduksjon

Denne ti år gamle beskrivelsen av informasjonsspiralen kan leses som en parafrase over hva vi forventer av kunstig intelligens (AI) i dag. Informasjonsspiralen avspeiler imidlertid en relativt "blind" menneskelig og organisatorisk *nyhetsappetitt* igjennom, der *det mulige og tilgjengelige får forrang* framfor en planlagt og omhyggelig utvelgelsesprosess. Dagens forventninger til AI er i sammenligning mer preget av en forestilling om noe "magisk" ved selve teknologien. Uansett kan vi ikke se bort fra at en "overproduksjon" av informasjon, med eller uten et intelligens-stempel, vil kunne påvirke både primærarbeid og artikuleringsarbeid, og ikke minst balansen mellom dem. Man kan allerede i dag se tendenser til at tilgang på store datamengder og bruk av maskinlæring blir brukt som argument for å redusere fokus på modeller

[25] Som bokstavelig talt "presenterer noe (materielt) på nytt, og på nytt, og på nytt …"
[26] Grøtan, T.O. (2007). ”IKT som bidrag til robusthet i integrerte operasjoner – et skråblikk”. I Tinmannsvik, R.K. (red) *Robust arbeidspraksis. Hvorfor skjer det ikke flere ulykker på sokkelen?* Tapir, Trondheim
[27] Makt i organisasjoner et vanskelig tema med mange ulike definisjoner. Den som passer best her er rett og slett muligheten til å se bort fra ting som ikke passer inn i "hyper-virkeligheten": "power to afford not to pay attention".
[28] Grøtan, 2007, p 86: "Store systemkomplekser blir omskrevet og rekonstruert ut fra skiftende formål. Virkelighet erstattes av hyper-virkelighet. Dette betyr ikke at det produseres en fiktiv verden men at natur og tekniske og sosiale systemer blir re-presentert hovedsakelig ut fra deres evne til re-konstruksjon". Dvs, deres viktigste egenskap er at de fungerer som, innehar kvaliteter som (originale) "Lego-brikker". Se også: Lilley et. al. 2004. Representing Organization. Knowledge, management and the information age. Oxford University Press
[29] Inspirert av Kallinikos, J. 2006. Information out of information. On the self-referential dynamics of information growth. Information Technology & People, 19(1), 98-115

og hypoteser om hvordan systemer fungerer. Hvis primærarbeidet blir "datadrevet", hva vil artikuleringsarbeidet da handle om? Vil premisset om kompleksitet bli "glemt"? Vil dette også medføre mindre forhandling og meningsskaping, og derved et mer amputert artikuleringsarbeid?

Et kritisk spørsmål som også kan/bør belyses er hvor og hvordan "virkelig" HMS blir forstått, beskrevet og ivaretatt i en kontekst der artikuleringsarbeid er et viktig (og anerkjent?) supplement til primærarbeid. Vil HMS som fenomen bli (er?) tatt som "gissel" og utelukkende beskrevet i "primærbetydning"? Hvordan vil HMS ved fjernarbeid bli spesifisert og beskrevet?

A.2.2 Organisatorisk forgrunn og bakgrunn, blandede kunnskapsregimer

En annen potensiell kilde til MTO-ubalanse er et (da forventet) skifte mellom hva som er forgrunn og bakgrunn i beslutningsprosessene (Sørhaug 2004)[30]. Vi har vært vant til å se organisasjonen som en "besluttet verden" i forgrunnen, mens andre aktører/samarbeidspartnere og derved grensesnittene mot disse danner bakgrunnen. Tendensen er nå at arbeid og kapital strømmer *gjennom* bedriftene, med grensesnittene som forgrunn. Med digitalisering kan vi akselerere en utvikling der verdiskapingen skjer *mellom* enhetene, ikke i dem. Verdiskapingen, ikke enhetene, er konstanten i en slik ligning. Inter-organisatorisk kompleksitet (Milch 2018) er en av implikasjonene.

En annen nøkkel til forståelse av disse problemstillingene (også i grensesnittene) er begrepet *blandede kunnskapsregimer*, som bygger på et tydeligere skille mellom kollegium, linje og nettverk (Sørhaug, 2004), der nettverksdimensjonen er på frammarsj, men som også har et tydelig premiss om nødvendigheten av *bevegelige kompromisser* mellom disse dimensjonene.

Viktige spørsmål er om slike forskyvninger avspeiles i betingelsene for og utføringen av fjernarbeid, individuelt og kollektivt, spesifikt om dette påvirker hhv primærarbeid og artikuleringsarbeid og balansen mellom dem. Hvor, og av hvem defineres kriteriene for vellykket samhandling i samhandlingsmatrisen, i eller mellom virksomhetene, og kan vi se spor av "bevegelige kompromisser" i dette? Har (den nye) "økologien" av aktører endret seg, hvem er de dominerende "nøkkelartene"? Er "nettverket" en fremtredende aktør i seg selv?

Det er også av interesse å vite hvordan slike endringer slår ut i organiseringen av HMS-arbeidet. Kunnskap er den nye kapitalen, selskapene bruker *kunnskap til å rasjonalisere kunnskap*, ikke bare for å rasjonalisere prosesser. Hva/hvor er HMS(-kunnskap), når kunnskap brukes til å rasjonalisere kunnskap?

A.3 Økte sårbarheter og større krav til IKT-sikkerhet i valgte løsninger

Økt IKT-avhengighet kan forventes å føre til strengere krav til IKT-sikkerhet. Mye tyder imidlertid på at det er et betydelig etterslep, også på områder som berører fjernarbeid. Nye angrepsvektorer og -flater oppstår med økt digitalisering i industrien og i samfunnet. Fjernarbeid omfatter både IT og OT, og denne kombinasjonen innebærer spesielle utfordringer med tanke på forskjellig teknologi, språk, og kultur. Implikasjonene av dette er svært viktig å forstå.

Erfaring med dataangrep mot industrielle anlegg og kritisk infrastruktur tyder på at slike anslag ikke (bare) er "innskytelser", men også basert på (kriminell, statlig) etterretningsvirksomhet og kartlegging over tid, med sikte på orkestrerte og utstuderte anslag. Økt omfang av fjernarbeid vil kunne gjøre det vanskeligere å

[30] Sørhaug, T. (2004). Managementalitet og autoritetenes forvandling. Ledelse i en kunnskapsøkonomi. Fagbokforlaget

beskytte seg mot uvedkommende som ønsker å kartlegge operative sårbarheter, f.eks. som del av forberedelsen til et anslag.

Internett er dessuten en etterretningsarena uten nasjonale grenser (og uten noen "Geneve-konvensjon" eller andre overnasjonale, juridiske/etiske rammeverk). Professor Olav Lysne har tilkjennegjort sin bekymring for at noen kan "slå av Norge" digitalt (Adresseavisen, 8.2.2018). Den tidligere lederen for Europol er bekymret for at statlige aktører knytter seg til kriminelle på nett (Aftenposten, juni 2018).

Vi vet at tilsynelatende triviell digital atferd har fått en enorm verdi i en digital økonomi, der selve forretningsideen til de største aktørene er å samle inn mest mulig data om brukernes gjøren og laden, og der praktisk talt ingen detalj er for liten. Den industrielle parallellen til dette kan være at det gjennom storstilt datainnhenting vil være mulig å finne interessante mønster over et bredt spekter, for industrielle anvendelser, e.g., digitale tvillinger, for HMS, men også for økonomisk, finansiell eller politisk vinning. Dette gjelder ikke minst anvendelse av "big data" og "kunstig intelligens" for å observere og analysere atferd, fenomener og trender, med helt andre ambisjonsnivåer enn det man tidligere kunne forestille seg. BBS[31] kan få en renessanse, men slike innsikter på avveie kan veldig lett snus til å bli et våpen for uvennlige hensikter. Slik sett bør vi anta at fjernarbeid vil komme til å inngå i komplekse landskap av trusler og sårbarheter som overskrider det meste man tidligere har forberedt seg på gjennom IKT-sikkerhet.

Konsekvensene av å forstyrre kontrollprosesser på en subtil måte ble synliggjort gjennom (det første) Stuxnet-angrepet, der noen, over relativt lang tid, kunne forvirre operatørene og prosesstyringen ved å manipulere verdiene på målingene. Kommersiell og politisk påvirkning gjennom digital kommunikasjon har blitt et svært aktuelt tema[32] i løpet av det siste året. Også beslutningstakere i næringen kan være utpekte mål for slik påvirkning. De fleste ansatte/arbeidstakere er også eksponert på sosiale medier der deres profiler også kan brukes til å forutse eller påvirke atferd/reaksjon i en industriell kontekst.

På bakgrunn av dette finner vil det være hensiktsmessig å skille mellom fire fokusområder for å undersøke IKT-sårbarhet knyttet til fjernarbeid:

A. IKT-sårbarheter som kan forstyrre eller skape tvil om tryggheten i den enkelte arbeidstakers fjerntilgang til ett eller flere systemer på "innsiden"
B. IKT-sårbarheter knyttet til fjernarbeid der dette inngår i samhandling slik vi har beskrevet i det foregående (som en MTO-balanse mellom primær- og sekundærarbeid), og som kan true integriteten i slik samhandling
C. IKT-sårbarheter knyttet til muligheten for at trender og komplekse industrielle trussel-landskap som fremtrer på andre samfunnsområder, som hacking, forberedte/orkestrerte anslag, kommersiell, finansiell og politisk påvirkning, også smitter over og manifesterer seg i næringens industrielle IKT-systemer.
D. IKT-sårbarheter knyttet til at industrielle trussel-landskap blir koplet til utenforliggende IKT-trussel-landskap (f.eks gjennom at ansatte og selskaper er tilgjengelige på sosiale medier)

Fjernarbeidet berøres av IT/OT problematikken. Selv om fjerntilgangen i prinsippet skal gå direkte inn i OT-domenet, vil sikkerheten i veien inn være påvirket av den generelle IKT-sikkerheten og tilhørende praksiser i utenforliggende (IT-) domener.

Kombinasjonen av IT og OT er stadig utfordrende. Det er regnet som betydelig vanskeligere å holde oversikt og overvåke IKT-sikkerhet i industrielle IKT-systemer. Tekniske og kulturelle forskjeller gir ringvirkninger

[31] "Behaviour Based Safety"
[32] Jfr Facebook plug-ins, Cambridge Analytica osv

som både skaper sårbarhet og legger begrensninger på bruk av alminnelige tiltak for IKT-sikkerhet. For eksempel kan ikke verktøy som IDS brukes i OT-domenet på samme måte som for IT, praksiser for administrasjon av brukerrettigheter kan være forskjellige, og industrielle IKT-systemer skiller seg generelt ut ved å være laget med tanke på høy pålitelighet og funksjonell integritet, og større grad av autonomi. Avhengigheten av dedikerte systemsystemleverandører for vedlikehold og feilretting av OT kan være betydelig, grensene mellom operasjonelle forstyrrelser og sikkerhetsbrudd kan være uklare (og vanskelig å tolke fra et mer generelt IT-perspektiv), og ulike praksiser og fortolkningsrammer kan til og med skape grunnlag for misforståelser i disse grenselandene. Mens interessen for "agile" systemutvikling er økende på den generelle IKT-siden også i petroleumsnæringen, møtes slike trender med (begrunnet) skepsis i OT-domenet, noe som bekrefter gapet i sikkerhetstilnærming mellom de to domenene.

I det følgende utdypes spesielt de to punktene A og B ovenfor.

A.3.1 IKT-sårbarheter som kan forstyrre eller skape tvil om tryggheten

På grunnlag av IT/OT problemforståelsen beskrevet ovenfor er det interessant å forstå hvordan de antatte sårbarhetene fortoner seg for næringen og dens forventninger til og erfaringer med fjernarbeid, og om regimene for IKT-sikkerhet faktisk understøtter fjernarbeidet på en god måte, slik at det ivaretar tryggheten og tilliten i den grunnleggende fjernarbeidsituasjonen.

Vi kan i dette også dra nytte av distinksjonen primærarbeid vs sekundærarbeid (artikuleringsarbeid) som vi har diskutert ovenfor gjennom kompleksitetsperspektivet, gjennom å undersøke om og i hvilken grad både selve fjernarbeidet og de underliggende sikkerhetspraksisene som skaper nødvendig trygghet utøves i henhold til en "oppskrift" eller standarder som er legitimert gjennom policyer eller prosedyrer, og/eller om de er "sekundære"[33] (dvs. skjer uformelt "i det stille"). Det vil også være interessant å forstå om disse praksisene i tillegg krever artikuleringsarbeid mellom, f.eks., systemeiere, systemleverandører, underleverandører og brukere.

A.3.2 IKT-sårbarheter som kan true integriteten i samhandling

En viktig problemstilling er hvordan IKT-relatert sårbarhet kan påvirke fjernarbeid-basert samhandling som beskrevet under "Økt kompleksitet i form av (IKT-støttet) samhandling" i det foregående. Interesseområdet peker derfor i siste instans mot former for IKT-sikkerhet som bidrar til ivaretakelse av kritiske MTO-balanser, og vi vil være opptatt av potensiell påvirkning av balansen mellom primærarbeid og sekundærarbeid, herunder artikuleringsarbeid. Spørsmålene som kan stilles vil være avledet fra (et utvalg av) spørsmålene vi definerte ovenfor under temaet "økt kompleksitet i samhandling", med orientering mot:

- om vi ser noe faktisk skille/prioritering mellom sårbarhet og beskyttelse av hhv primær/sekundær/artikuleringsarbeid,
- om vi ser at perspektivskapking/-taking er en prosess som verdsettes og understøttes (i den grad den involverer delte informasjonsobjekter),
- om "grenseobjekter" gis adekvat støtte/beskyttelse/verdsetting,
- om IKT-støtten bidrar til "felles glemsomhet", evt. kunne bidratt til å loggføre dette,
- om "hyper-virkelighet" understøttes/legitimeres,

[33] Gjennom arbeidet med SINTEF rapport 2018:00572 fikk vi et klart inntrykk av at svært mye av det viktige IKT-sikkerhetsarbeidet i næringen (og i lignende domener) er av en type arbeid som ikke er spesielt godt dokumentert og beskrevet, og som derfor ikke enkelt kan puttes i båsen "primærarbeid"

- om informasjonsspiraler gis "energi" gjennom at "ferske" data gis forrang/prioritet,
- om regimene for IKT-sikkerhet er sensitive for endringer i forgrunn/bakgrunn; er det noen "bevegelige kompromisser" knyttet til IKT-sikkerheten i nye beslutningskontekster; hvem har ansvaret for (felles) IKT-sikkerhet under skiftende omstendigheter; hvem får gjennomslag, siste ord hvis det er uenighet om beskyttelsesnivå?
- om praksisene for IKT-sikkerhet understøtter en økologi av aktører/arter med ulike interesser, og samspillet mellom disse (eller er det en standardisert beskyttelse "for alle"?
- om tillitsaspektet er fremtredende i definisjonen av sikkerhetskrav.

Disse problemstillingene er av en slik art/karakter at de ikke umiddelbart vil bli gjenkjent som IKT-sikkerhet i tradisjonell forstand. For det første vil det være relativt krevende å "mappe" typiske sikkerhetskategorier som konfidensialitet, integritet, tilgjengelighet, autentisitet, ikke-benekting[34] etc til de informasjonsobjektene som inngår i samhandlingen og som korresponderer med problemstillingene. I tillegg vil det være en grense for i hvilken grad og på hvilken måte tekniske mekanismer kan erstatte de sosiale/relasjonelle mekanismene som Hepsø (2006) peker på som essensielle for tillit og gjensidig forpliktelse, f.eks hvilke (andre) personer en gitt person stoler på i den grad at dette kompenserer for egen tvil om integriteten i et kritisk informasjonsobjekt. Selv om IKT-sikkerhet kan ivareta autentisitet ift person, må denne personens troverdighet og integritet understøttes på annen måte. På et eller annet punkt vil vi derfor måtte søke en "IKT-sikkerhet" som understøtter tvil heller enn blind tillit (f.eks. til "nyheter"), og som tilbyr brukeren verktøy for å håndtere denne tvilen gjennom å avklare f.eks opprinnelse og historikk til informasjonskilder, og eventuelt foreslå andre kilder og filtreringer av informasjon på en slik måte at brukerens kunnskapsprosess understøttes i riktig retning[35]. Her er det mye upløyd mark.

A.4 Dilemma mellom organisatorisk sikkerhet vs IKT-sikkerhet

Organisatorisk sikkerhet, herunder MTO-samspill, har fått en stadig sterkere plass i sikkerhetsarbeidet i næringen. Dette inkluderer en stadig sterkere trend mot anerkjennelse av behovet for en god blanding av "Safety I" og "Safety-II" (resiliens).

> ***Safety-I and Safety-II***
>
> *"The traditional view of safety, called Safety-I, has consequently been defined by the absence of accidents and incidents, or as the 'freedom from unacceptable risk.' As a result, the focus of safety research and safety management has usually been on unsafe system operation rather than on safe operation. In contrast to the traditional view, resilience engineering maintains that 'things go wrong' and 'things go right' for the same basic reasons. This corresponds to a view of safety, called Safety-II, which defines safety as the ability to succeed under varying conditions. The understanding of everyday functioning is therefore a necessary prerequisite for the understanding of the safety performance of an organisation."*
>
> *http://erikhollnagel.com/ideas/safety-i%20and%20safety-ii.html*

En mulig utvikling er at premissene for vellykket Safety-II blir svekket gjennom fjernarbeid, fordi de faktiske handlingene krever lokal innsikt og nærhet. De mer subtile delene av dette kan bli mindre håndgripelige, og

[34] "Non-repudiation"

[35] "IKT som kunnskapsmedierende teknologi" (Grøtan 2007)

endog gå tapt i en "re-presentert" hyper-virkelighet. Safety-I kan paradoksalt nok igjen bli den trygge havn. IKT-sikkerhet kan "binde" samhandlingen, og "digitalisert sikkerhet" kan med dette bli mer forspent mot Safety-I alene, enn hva virkeligheten faktisk krever.

Vedlegg

B Standarder, retningslinjer og veiledninger

Standarder

Referanse	Tittel	Tema
Standarder		
IEC 61511 series	Functional safety - Safety instrumented systems for the process industry sector	The standard series provides guidance on the specification, design, installation, operation and maintenance of safety instrumented functions (SIF) and related safety instrumented systems (SIS). It deals with the interface between SISs and other safety systems in requirering that a process hazard and risk assessment be carried out. The SIS includes sensors, logic solvers and final elements. The standard consists of three parts: 1) Framework, definitions, system, hardware and software requirements, 2) Guidelines in the application of IEC 61511-1, 3) Guidance for the determination of the required safety integrity levels
IEC 62443 series	Industrial Automation and Control Systems Security	The goal in applying the 62443 series is to improve the safety, availability, integrity and confidentiality of components or systems used for industrial automation and control, and to provide criteria for procuring and implementing secure industrial automation and control systems. Conformance with the requirements of the 62443 series is intended to improve electronic security and help identify and address vulnerabilities, reducing the risk of compromising confidential information or causing degradation or failure of the equipment (hardware and software) of processes under control. The content of the series is directed towards those responsible for specifying, designing, developing, implementing, or managing industrial automation and control systems. This information also applies to users, system integrators, security practitioners, and control systems manufacturers and vendors.
ISO 13849 series	Safety of machinery -- Safety-related parts of control systems	ISO 13849-1:2015 provides safety requirements and guidance on the principles for the design and integration of safety-related parts of control systems (SRP/CS), including the design of software. For these parts of SRP/CS, it specifies characteristics that include the performance level required for carrying out safety functions. It applies to SRP/CS for high demand and continuous mode, regardless of the type of technology and energy used (electrical, hydraulic, pneumatic, mechanical, etc.), for all kinds of machinery. It does not specify the safety functions or performance levels that are to be used in a particular case.

Retningslinjer

Referanse	Tittel	Tema
Retningslinjer		
Norwegian Oil and Gas RP 104	104 – Norwegian Oil and Gas recommended guidelines on information security baseline requirements for process control, safety and support ICT systems. (Rev 06. December 2016)	This document contains guidance on how to implement the Norwegian Oil and Gas information security baseline requirements (ISBRs) in process control, safety and support (PCSS) ICT systems. The implementation guidance in this document is considered "good practice" for information security, but the organisation should adapt these proposed solutions in accordance with their own information security policy and regulations, and aligned with their national legislation. Implementing the information security controls and measures exactly as described in this guidance is not mandatory. Other methods and techniques may be used as long as the objectives of the ISBRs are achieved.
DNV-GL-RP-G108	Cyber security in the oil and gas industry based on IEC 62443 (2017)	This recommended practice for implementing IEC 62443 (3-2, 3-3 and 2-4) in the oil and gas sector was produced based on a joint industry project (JIP) with participation from industry and Petroleum Safety Authority (PSA) Norway, A common and practical approach on how to secure industrial automation and control systems (IACS) in the oil and gas sector is provided. The recommended practice intends to follow the regulatory requirements defined by PSA for the Norwegian continental shelf and by Health and Safety Executive (HSE) for the UK oil Sector.
DNV GL-RP-G0496	Cyber security resilience management for ships and mobile offshore units in operation (2016)	This recommended practice guides owners, managers and operators of ships and mobile offshore units towards enhanced cyber security of their assets in operation. In addition, this RP is intended to help IT and industrial automation control system professionals to join their efforts towards building and maintaining cyber security resilience of the total set of the assets and processes employed to conduct the company's business. Following a risk based approach, the decisions of what is critical and high priority is then left at the discretion of the organisation.

Referanse	Tittel	Tema
Retningslinjer		
NIST 800-82 R2	Guide to Industrial Control Systems (ICS) Security (2015)	This document provides guidance on how to secure Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), while addressing their unique performance, reliability, and safety requirements. The document provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks
NIST 800-46 R2	Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security (2016)	This publication provides information on security considerations for several types of remote access solutions, and it makes recommendations for securing a variety of telework, remote access, and BYOD technologies. It also gives advice on creating related security policies. For many organizations, their employees, contractors, business partners, vendors, and/or others use enterprise telework or remote access technologies to perform work from external locations. All components of these technologies, including organization-issued and bring your own device (BYOD) client devices, should be secured against expected threats as identified through threat models.
NCSC End user Technology	Deployment and management of technology used by the employees, partners, or customers of an organisation.	This guidance is for organisations considering a 'Bring Your Own Device* (BYOD) approach, and describes the key security aspects to consider in order to maximize the business benefits of BYOD whilst minimizing the risks. It should be used to inform risk management decisions for BYO deployment.
NIST	Framework for Improving Critical Infrastructure Cybersecurity, V1.1 Draft 2 (2017)	The Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses. The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization’s risk management processes. The Framework consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational Profiles. Through use of the Profiles, the Framework will help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources.

Referanse	Tittel	Tema
Retningslinjer		
ISA-TR84.00.09	Cybersecurity Related to the Functional Safety Lifecycle (2017)	This document is intended to address and provide guidance on integrating the cybersecurity lifecycle with the safety lifecycle as they relate to Safety Controls, Alarms, and Interlocks (SCAI), inclusive of Safety Instrumented Systems (SIS). This scope includes the work processes and countermeasures used to reduce the risk involved due to cybersecurity threats to the Industrial Automation and Control System (IACS) network. This scope provides recommendations to ensure SCAI are adequately secured due to the potential for cyber attacks that can act like common mode failures that initiate a hazardous demand and also prevent instrumented protection functions, including the SIS, from performing their intended purpose. The scope is intended to address cybersecurity from both external and internal threats. Although not directly within the scope, enterprise networks, business networks and process information networks (demilitarized zones) that represent a threat vector to the SCAI systems or contain countermeasures that reduce the risk to the SCAI systems from external cyber threats, are included.
ISACA COBIT 5		COBIT 5 is an overarching business and management framework for governance and management of enterprise IT. It incorporates enterprise governance and management techniques, and provides globally accepted principles, practices, analytical tools and models to help increase the trust in, and value from, information systems. COBIT 5 may help enterprises of all sizes to: •Maintain high-quality information to support business decisions •Achieve strategic goals and realize business benefits through the effective and innovative use of IT •Achieve operational excellence through reliable, efficient application of technology •Maintain IT-related risk at an acceptable level •Optimize the cost of IT services and technology •Support compliance with relevant laws, regulations, contractual agreements and policies

Veiledninger myndigheter

Referanse	Tittel	Tema
Veiledninger myndigheter		
HSE	Cyber Security for Industrial Automation and Control Systems (IACS)	This Operational Guidance represents the Health and Safety Executive (HSE) interpretation of current standards on industrial communication network and system security, and functional safety in so far as they relate to major hazards workplaces. This guidance does not cover protection of critical infrastructure (e.g. utility networks) or protection of information on corporate networks. For the purpose of the enforcement management model, this guidance is an interpretive standard. This Operational Guidance could contribute towards a suitable demonstration of compliance with relevant H&S legislation, in order to demonstrate cyber security risks have been managed to as low as reasonably practicable (ALARP). Alternative equivalent means may also be used to demonstrate compliance.