2021:00057 - Åpen

Rapport

Premisser for digitalisering og integrasjon IT-OT

IKT-sikkerhet – Robusthet i petroleumssektoren 2020

Forfatter(e)
Geir K. Hanssen, Tor Onshus, Martin Gilje Jaatun, Thor Myklebust, Maria Ottermo, Mary Ann Lundteigen

SINTEF Digital
2021-01-29

SINTEF Digital

Postadresse:
Postboks 4760 Torgarden
7465 Trondheim

Sentralbord: 40005100

info@sintef.no

Foretaksregister:
NO 919 303 808 MVA

Premisser for digitalisering og integrasjon IT-OT

IKT-sikkerhet – Robusthet i petroleumssektoren 2020

EMNEORD:
Digitalisering
Cybersikkerhet
OT-system
Regelverk

VERSJON
1.0

DATO
2021-01-29

FORFATTER(E)
Geir K. Hanssen, Tor Onshus, Martin Gilje Jaatun, Thor Myklebust, Maria Ottermo, Mary Ann Lundteigen

OPPDRAGSGIVER(E)
Petroleumstilsynet

OPPDRAGSGIVERS REF.
Arne Halvor Embergsrud

PROSJEKTNR
102022556

ANTALL SIDER OG VEDLEGG:
39 (1 vedlegg)

SAMMENDRAG
Formålet med denne rapporten er å gi næringen økt forståelse av pågående digitalisering, status og utfordringer, og hvordan denne utviklingen bør styres videre.

Denne rapporten er en av seks SINTEF-rapporter fra prosjektet: "IKT-sikkerhet – Robusthet i petroleumssektoren 2020". Prosjektet har innhentet kunnskap om risiko, sårbarheter og IKT-sikkerhet for industrielle IKT-systemer.

UTARBEIDET AV
Geir K. Hanssen

SIGNATUR

KONTROLLERT AV
Lars Bodsberg

SIGNATUR

GODKJENT AV
Maria Bartnes

SIGNATUR

RAPPORTNR	ISBN	GRADERING	GRADERING DENNE SIDE
2021:00057	978-82-14-06481-0	Åpen	Åpen

Historikk

VERSJON	DATO	VERSJONSBESKRIVELSE
1.0	2021-01-29	Endelig versjon

Kreditering av bilder:
Side 15: Basert på illustrasjon fra McAfee
Øvrige bilder: Egenprodusert eller Pixabay (Pixabay License)

SINTEF

Innholdsfortegnelse

Sammendrag

Innledning

Formålet med denne rapporten er å belyse digitalisering i olje- og gassbransjen i Norsk sektor og fremheve utfordringer, spesielt knyttet til IKT-sikkerhet og OT-systemer, samt gi anbefalinger til næringen og Ptil.

Arbeidet er i hovedsak basert på dokumentgjennomgang, intervju, og arbeidsmøter. Intervju har blitt gjennomført med operatør- og leverandørselskap.

Digitalisering i næringen

Petroleumssektoren er inne i en omfattende digitaliseringsprosess preget av store muligheter og store utfordringer. Alle aktører i bransjen har digitalisering høyt på sin agenda, mange med en veldig tydelig forankring i sine strategier for å effektivisere drift, øke utvinning, og forbedre sikkerhet. Det er derimot en stor variasjon i modenhet, ofte i sammenheng med selskapets størrelse og kapasitet til å håndtere store teknologidrevne endringer. Digitalisering er en trend i nær sagt alle domener og industrier, men hvor petroleumssektoren med sine tydelige sikkerhetskrav er i en tidligere fase enn flere andre store sektorer. Utviklingen kan sees som en del av den generelle utviklingen av Industri 4.0 hvor fysisk utstyr koples mot distribuerte IKT-systemer og realiseres basert på nyskapende teknologier som maskinlæring, Industrial Internet of Things (IIoT), ny kommunikasjonsteknologi, autonome system, etc. Dette er teknologier som gjør det mulig å produsere, transportere, lagre, og prosessere store datamengder fra den operative siden, som igjen kan utnyttes for å forbedre prosesser og oppgaver, men hvor prosessering skjer ved hjelp av det som er regnet som vanlig informasjonsteknologi. Eksempler er automatisering, ekspertsystemer, og digital tvilling. Vi ser allerede omfattende bruk og nytte av denne type teknologi, men det gjenstår flere utfordringer før potensialet er utnyttet fullt ut. Den mest grunnleggende utfordringen er å forstå begrensninger og tilpasninger i henhold til myndighetenes forskrifter, som fortsatt er grunnleggende for god sikkerhet i næringen.

Identifiserte utfordringer

Utviklingen er kompleks selv for organisasjoner med høy kompetanse og som i utgangspunktet benytter avansert teknologi, og det er vanskelig å danne seg et tydelig bilde av helheten for aktørene, men det virker tydelig at overgangen mot en stadig mer datadreven og sammenkoplet virksomhet er i kjernen av utfordringen. Økende mengder data produseres i OT-laget, i det vi kan kalle edge-løsninger, og prosesseres i IT-systemer og må dermed transporteres i systemarkitekturer som i utgangspunktet ikke var designet for omfanget. Store datamengder må også lagres og behandles i systemer med tilstrekkelig kapasitet, for eksempel i form av skyløsninger, samtidig som de må sikres mot uønsket innsyn og påvirkning. Sist men ikke minst, nye dataintensive tjenester krever også god kontroll på datakvalitet.

Denne utviklingen utfordrer også forholdet til leverandørene, både etablerte og nye, som tilbyr dataintensive skybaserte tjenester. Det er ikke lenger like tydelig hvor og hvordan nettbaserte digitale tjenester tilbys og hvordan de vedlikeholdes og hvilke krav som må stilles. På den annen side har ikke leverandørsiden nødvendigvis god nok innsikt i betingelser som informasjonssikkerhet og prinsipper om uavhengighet og segregering. Eierskap til data utfordres også.

Generelt så fører digitalisering til økt kopling mellom systemer og kan skape utfordringer for informasjonssikkerhet, særlig når systemer og utstyr nær OT-laget og sikkerhetssystemene berøres. Etablerte prinsipper som skallsikring og lagdelte arkitekturer utfordres. Næringen søker retningslinjer og mange aktører peker på IEC 62443, men hvor utvikling og modenhetsnivå fremdeles ikke er på plass.

Alle aktørene har i utgangspunktet de samme grunnleggende utfordringene og det er et tydelig behov for økt kompetanse og ikke minst en koordinert innsats – utfordringene er et felles anliggende. Dette gjelder spesielt for å nå en felles forståelse og standard for grunnleggende prinsipper for IKT-sikkerhet, spesielt i og i tilknytning til OT-systemer som i større grad utstyres med informasjonsteknologi. NAMUR Open Access og

OPC UA synes å være mulige referanser som næringen kan enes om, men her kreves det mer koordinering, kunnskap og modenhet om bruk og begrensninger.

Anbefalinger

Basert på forståelsen av digitalisering i næringen og funn fra intervju avledes følgende anbefalinger til næringen:

- Felles kompetanseløft og samarbeid
- Standardisering (eller valg av standarder) for interoperabilitet og IKT-sikkerhet
- Økt fokus på data*kvalitet* og *integritet*
- Økt bevissthet på rollen som data*eier*
- Økt fokus på flyt av data, særlig der eksisterende systemer utfordres
- Øke fokus på digitalisering for økt sikkerhet (safety), utover mål om effektivisering

I sammenheng med dette gis det også anbefalinger til Ptil:

- Utvikle rollen som pådriver for kompetanseheving i næringen, men innenfor Ptils mandat
- Følge utviklingen av datatransport og teknologier som benyttes for å kople systemer, særlig OT-systemer
- Bidra til å fortolke og tydeliggjøre forskriftene i forhold til den teknologiske utviklingen
- Støtte næringen i klargjøringer rundt IEC 62443 og vurdere veiledning til styringsforskriften
- Bidra til en felles satsning på en omforent referansearkitektur (NAMUR OA er aktuell) og omforent standard for interoperabilitet (OPC UA er aktuell)
- Samkjøre føringer og oppfølging av produksjonsselskap og boreselskap, som har sammenfallende utfordringer.

Executive summary

Introduction

The objective of this report is to address the digitalization in the Norwegian oil- and gas sector and highlight challenges, in particular related to cybersecurity and operation technology (OT), and to provide recommendations to the industry and to Ptil.

The work is mainly based on analysis of documentation, interviews, and meetings. Both operators and suppliers have been interviewed.

Digitalization in the industry

The petroleum industry is undergoing an extensive process of digitalization, driven by considerable opportunities but also facing challenges. All actors in this industry have added digitalization to their agendas, and some with a solid anchoring in their strategies, aiming for more effective operations, increased extraction, and improved safety. Maturity varies though, typically related to the size of the organization, and the capacity to manage large technology-driven transformation processes. Digitalization is a trend within nearly any domain and industry, but where the petroleum industry may be considered at an earlier stage than other domains due to its strong focus on safety. This development can be seen as part of the development of Industry 4.0 where physical devices are connected with distributed ICT-systems, building on technologies such as machine learning, Industrial Internet of Things (IIoT), new communication technologies, autonomous systems, etc. These are all technologies which enables production, transfer, storage and exploitation of very large data from operations, which enables improved processes, exploiting information technologies. Examples are automation, expert systems, and digital twins. We already see an extensive use and benefits from this class of technology, but several challenges remains to be resolved before we see the full potential. The fundamental challenge is to understand and manage limitations with respect to guidelines and requirements from the authorities, which creates a fundamental basis for safety in the industry.

Identified challenges

The ongoing development is complex, even for highly competent organizations that already are advanced users of technology. It is challenging to build a complete understanding of the development, but it seems obvious that the transition towards increasingly data-driven operations is at the core of the challenge. Increasing amounts of data are being produced and retrieved from the operational systems in what can be defined as edge solutions, and then processed in centralized IT-systems, meaning that data in some cases must be transferred through systems and infrastructures that was not intentionally designed for this extent of data flow. Large amounts of data also needs to be stored and processed with sufficient capacity, e.g. in cloud solutions while at the same time being secured against access and influence by outsiders. Last but not least, new data-intensive services also put a demand on data control and data quality.

This development challenges the relationship with suppliers, both those that are well established as well as new actors that are offering data-intensive, cloud-based services. It can be hard to see where and how net-based digital services are offered and how they are maintained, and how to manage these. On the other side, some suppliers may not have the needed insight themselves regarding cyber security and fundamental principles on independence and segregation of safety systems. Data is an important asset and the ownership of data is also being challenged.

Digitalization does in general increase the coupling between systems and thus challenge information security, in particular when systems and equipment is located near operational systems and where the safety systems potentially can be affected. Well established principles such as boundary protection and layered architectures are being challenged. The industry are seeking relevant guidelines and several actors are referring the IEC 62443 series, but where development and the level of maturity are yet not in place.

All actors do have similar challenges and there is a clear need to increase joint competency, preferably as a joint effort; the challenges of the industry – and the solutions – are of common interest. In particular, it is important to build a shared understanding and a standard for fundamental principles for information security. This is particularly important in relation to operational systems that are being influenced by information technology. NAMUR Open Access and OPC UA seems to gain focus in the industry as a common view on interoperability, but do as well require coordination and increased knowledge on use and limitations.

Recommendations

Based on the understanding of the digitalization, and findings from interviews, a set of recommendations are given to the industry.

- A joint effort to increase competency and collaboration
- Standardization (or selection of standards) for interoperability and information security
- Increased emphasis on data *quality* and *integrity*
- Increased awareness of the role as data *owner*
- Increased emphasis on the flow of data, especially in existing systems
- Increased focus on digitalization for improved safety, beyond ambitions on efficiency

Followingly, recommendations are provided to Ptil:

- Develop the role as a driving force to increase competency, although within the mandate of Ptil
- Monitor the development on data transport and technologies for coupling systems, in particular in relation to operational systems
- Contribute to clarify regulations in the light of the technological development
- Contribute to the effort on establishing a joint reference architecture (NAMUR OA is relevant) and a joint standard for interoperability (OPC UA is relevant)
- Coordinate guidelines and follow-up of production and drilling companies, which have common challenges

1 Innledning

1.1 Bakgrunn

Petroleumstilsynet har gitt SINTEF i oppdrag å undersøke ulike sider av temaet IKT-sikkerhet – robusthet i petroleumssektoren. Hovedmålet har vært å innhente kunnskap om risiko, trusler, sårbarheter, samt viktighet av IKT-sikkerhet for industrielle systemer. Prosjektet skal bidra til å øke forståelsen for IKT-sikkerhet i petroleumsvirksomheten og slik være med å øke robustheten mot uønskede hendelser. SINTEF har også gitt innspill til oppdatering av Petroleumstilsynets regelverk for oppfølging av IKT-sikkerhet.

I det følgende gis en kort beskrivelse av de seks delprosjektene:

Datakvalitet
: Hensikten har vært å undersøke hvilke datakilder og data som benyttes i industrielle IKT-systemer og hvordan data behandles og prosesseres før de gjøres tilgjengelig i kontornettet. Styrker og sårbarheter knyttet til datakvalitet og sikring av data er diskutert.

Notat – IKT-sikkerhet i petroleumsindustrien
: SINTEF har utarbeidet et notat som klargjør hvordan IKT-sikkerhet i petroleumsindustrien blir regulert i gjeldende regelverk. Notatet belyser også forventninger fra myndighetene, og gir en oversikt over og status på satsingen innenfor IKT-sikkerhet i petroleumsnæringen de siste årene.

Veileder IKT-sikkerhet
: Det er utarbeidet et veiledningsdokument ("veileder") for norsk petroleumsvirksomhet som skal kunne brukes som et vedlegg til NSMs grunnprinsipper for IKT-sikkerhet. Veilederen er tilpasset de løsningene som er vanlige i petroleumssektoren, samtidig som den har fleksibilitet til å kunne håndtere hovedelementene innen petroleumsindustriens satsing på digitalisering.

Modellkontrollert operasjon
: Rapporten sammenfatter kunnskap og anbefalinger om sikker bruk av data fra modellkontrollerte operasjoner. Det er lagt spesiell vekt på kvalitetssikring av modeller og kommunikasjon mellom programvareløsninger i boreoperasjoner.

Premisser for digitalisering og integrasjon IT – OT – *denne rapporten*
: Hensikten har vært å beskrive og vurdere hvordan digitalisering og bruk av skytjenester påvirker industrielle IKT-systemer, samt hvilke sikkerhetsløsninger man må iverksette for sikker bruk av skytjenester. I Petroleumstilsynets regelverk står spesielt prinsippet om segregering og uavhengighet sentralt som strategi for å etablere sikkerhet.

Kommunikasjonsnettverk
: Hensikten har vært å undersøke hvilken rolle datanettverk ivaretar for ekstern kommunikasjon ved fare- og ulykkessituasjoner. Rapporten beskriver utfordringer knyttet til risiko og sårbarhet i data-nettverkene og utarbeide konkrete forslag til forbedringer.

Dette prosjektet er en del av en større satsing innenfor IKT-sikkerhet i Ptil. Sentrale problem-stillinger for Ptil er:

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

SINTEFs arbeid i dette prosjektet er i stor grad en videreføring av tidligere prosjekter gjennomført av DNV GL og SINTEF innen samme temaområde [1].

1.2 Mål og hensikt

Hovedmålet for denne leveransen er å gi næringen økt forståelse av premisser for digitalisering i olje- og gassbransje i Norsk sektor.

Følgende fire målsettinger er definert:

1. Vurdere status, planer, inkludert sannsynlige anvendelser av digitalisering, og da i hovedsak bl.a. skyteknologi, i OT-systemer og integrasjon mot IT-systemer hos operatører (innen Petroleums-tilsynets ansvarsområde).
2. Vurdere tilgjengelige erfaringer med skyteknologi som en viktig digitaliserings- og system-integrasjons-trend fra samme og lignende bransjer for å avdekke typiske IKT-sikkerhetsutfordringer og god praksis for å håndtere disse, inkludert sikring av uavhengighet mellom systemer med spesiell vekt på nødavstengingssystemer (ESD). Det er også relevant å vurdere systemer for ytelsesovervåking av feltutstyr (for eksempel, kan overvåking av lukketid på ESD-ventiler påvirke sikringsfunksjoner negativt?)
3. Beskrive og vurdere hvordan bruk av skytjenester/digitalisering påvirker OT-systemer, hvilken påvirkning dette kan ha på IKT-sikkerhet, og hvilke IKT-sikkerhetsløsninger man må implementere for sikker digitalisering, som for eksempel bruk av skytjenester, og evt. hvilke begrensninger som finnes.
4. Gi innspill til oppdatering veiledningen av Petroleumstilsynets regelverk for oppfølging av IKT-sikkerhet i IT- og OT-systemer.

Denne rapporten setter søkelyset på den pågående digitaliseringen av både gamle og nye installasjoner og er basert på informasjon som er hentet inn fra operatørselskap, boreselskap, og leverandører.

1.3 Begrensninger

Følgende begrensninger gjelder:

- Det er lagt vekt på dagens løsninger, men også utfordringer i nær fremtid som bransjen jobber med i dag. Rapporten er altså ikke ment å gi innspill til utviklingen på lang sikt, men pågående utvikling – basert på erfaringer fra i dag.
- Utvalget av selskap og respondenter er gjort for å sikre best mulig tilgang på kompetanse, men funn er basert på informasjon, uttalelser og vurderinger av enkeltpersoner, noe som naturlig vil påvirke informasjonen som er innsamlet.
- All informasjon som er samlet inn er behandlet konfidensielt og rapporten vil dermed ikke avdekke informasjon som er spesifikk for enkeltselskap. Rapporten er også lagt frem på en slik måte at det ikke skal være mulig å spore funn til enkeltselskap, men heller vise et felles bilde av bransjen.

1.4 Begreper, definisjoner og forkortelser

1.4.1 Begreper og definisjoner

Definisjoner benyttes for at vi skal ha en lik forståelse av sentrale begreper, men definisjoner kan i seg selv gi en begrensning i forståelsen av et begrep, og det er ofte flere definisjoner av samme begrep. Vi har derfor, i noen tilfeller, med hensikt tatt med flere definisjoner av samme begrep.

Begrep	Definisjon/beskrivelse	Referanse
Barriere *	Tiltak som har til hensikt og funksjon enten å forhindre et konkret hendelsesforløp i å inntreffe, eller påvirke et hendelsesforløp i en tilsiktet retning ved å begrense skader og/eller tap. Funksjonen til disse barrierene ivaretas av tekniske, operasjonelle og organisatoriske elementer enkeltvis eller samlet	Ptil 2020 (ptil.no) [4]
Cloud (sky)	Lagring og prosessering av data på eksternt tilknyttet infrastruktur tilknyttet internett.	Dette prosjektet
Cybersikkerhet ***	Beskyttelse av utstyr (komponenter og enheter) og fysiske prosesser som er sårbare gjennom IKT	SINTEF 2019:00361 [5]
DevOps	Integrert iterativ prosess for utvikling (Dev) og operasjon (Ops)	
Digital sikkerhet ***	Beskyttelse av "alt" som er sårbart fordi det er koblet til eller på annen måte avhengig av informasjons- og kommunikasjonsteknologi	Nasjonal strategi for digital sikkerhet 2019 [6]
Digital Tvilling	En digital rekonstruksjon av noe som eksisterer i den virkelige verden. Det kan være en representasjon av et fysisk objekt, et sted, et system, en prosess eller til og med et menneske. Den digitale representasjonen speiler den virkelige tingen, og lærer og endrer seg i takt med det den representerer.	Digital Norway [7]
Edge	Prosessering og lagring av data i nærhet til innhenting og bruk av data.	Dette prosjektet
Fog	Prosessering og lagring av data hentet fra edge-utstyr og potensielt integrert med skyløsninger.	Dette prosjektet
IKT-sikkerhet ***	Beskyttelse av informasjons- og kommunikasjonsteknologi (maskinvare og programvare, samt kommunikasjons-systemer)	SINTEF 2018:00572 [8]
IKT-sikkerhetstiltak *	Tiltak for å sikre IKT-systemer og informasjon mot tilsiktede og utilsiktede hendelser	NOU2015: 13 [9]
Informasjonsteknologi (IT)	Teknologi som behandler informasjon	Dette prosjektet
Internet of Things/ Tingenes Internett (IoT)****	Teknologi som gir muligheten til å fjernovervåke og styre produkter ved å koble dem til Internett.	Digital Norway [10]
Operasjonell teknologi (OT)	Teknologi som støtter, kontrollerer og overvåker industriell produksjon, kontroll- og sikkerhetsfunksjoner	Dette prosjektet
Risiko (1) **	Med risiko menes konsekvensene av virksomheten med tilhørende usikkerhet	Veiledning til RF § 11 [11]
Risiko (2) **	Risiko kan uttrykkes som en kombinasjon av sannsynligheten for og konsekvensen av en uønsket hendelse	NS 5814:2008 [12]
Risiko (3) **	Risiko kan uttrykkes som forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen	NS 5832:2014 [13]

Begrep	Definisjon/beskrivelse	Referanse
Sikkerhet (1)	Sikkerhet innebærer beskyttelse mot farer og trusler som kan forårsake uønskede hendelser	NOU2015: 13 [9]
Sikkerhet (2)	Beskyttelse av verdier så som mennesker, ytre miljø, utstyr og informasjon	SINTEF 2018:00572 [8]
Sårbarhet (1)	Manglende evne hos et analyseobjekt til å motstå virkninger av en uønsket hendelse og til å gjenopprette sin opprinnelige tilstand eller funksjon etter hendelsen	NS 5814:2008 [12]
Sårbarhet (2)	Et uttrykk for de problemer et system får med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet	NOU2015: 13 [9]

*) Begrepet barriere brukes sjelden i IKT-sikkerhetsstandarder. I stedet brukes begreper som tiltak, mottiltak, forsvarsmekanismer, beskyttelsesmekanismer, løsninger, osv.

**) Risiko (1) er et eksempel på en kvalitativ definisjon av risiko, mens risiko (2) og risiko (3) er eksempler på definisjoner for beskrivelse av risiko, jf. [14]

***) Digital sikkerhet brukes synonymt med IKT-sikkerhet og cybersikkerhet [6].

****) Kan utvides til IIoT – Industrial Internet of Things – utstyr designet for industriell bruk (sensorer, instrumentering etc.)

1.4.2 Forkortelser

Forkortelse	Beskrivelse
HMI	Human Machine Interface – menneske-maskin grensesnitt
HMS	Helse, miljø og sikkerhet
IACS	Industrial Automation and Control Systems
IEC	International Electrotechnical Commission
IF	Innretningsforskriften
IKT	Informasjons- og kommunikasjonsteknologi
ISO	International Standardization Organization
IT	Informasjonsteknologi
LAN	Local Area Network – lokalt nettverk
NEK	Norsk elektroteknisk komite
NKOM	Norsk kommunikasjonsmyndighet
NOG	Norsk olje og gass
NORSOK	NORsk Sokkels Konkurranseposisjon
NOU	Norges Offentlige Utredninger
NS	Norsk Standard
NSM	Nasjonal sikkerhetsmyndighet
OT	Operasjonell teknologi
PC	Personal Computer – personlig datamaskin
PLC	Programmable Logic Controller
Ptil	Petroleumstilsynet
RF	Rammeforskriften
SAS	Safety and Automation System – sikkerhets- og automasjonssystem
SF	Styringsforskriften
SIS	Sikkerhetsinstrumenterte systemer
SLA	Service Level Agreement
TCP	Transmission Control Protocol

1.5 Metode og gjennomføring

Arbeidet er i hovedsak basert på dokumentgjennomgang, intervju og arbeidsmøter. Det er utført i et tverrfaglig prosjektteam med kompetanse innenfor blant annet kommunikasjonssystemer, IKT-sikkerhet, beredskap, samt petroleumsregelverk og standarder innenfor disse fagområdene. Det er også gjort en screening av forskningslitteratur (appendix A).

Intervju har blitt gjennomført med flere selskap i forbindelse med denne. Av hensyn til anonymitet oppgis ikke navnene på selskapene. Det er gjort intervju med 5 operatørselskap og 1 leverandør. I tillegg er det gjort observasjoner av til sammen 6 intervju som er gjort i deloppdrag 2 (Datakvalitet), 3 (IKT sikkerhet) og 5 (Modellkontrollert operasjon).

1.6 Rapportstruktur

Kapittel 2 gir en kort innføring i digitalisering rettet mot en ikke-teknisk målgruppe.
Kapittel 3 gir en oversikt over viktige funn i dialogen med selskapene.
Kapittel 4 oppsummerer de viktigste anbefalingene til nøringen og Ptil, samt gir innspill til videre kunnskapsinnhenting.

I tillegg til figurer og tabeller, benytter vi faktabokser (grønne bokser til venstre på siden) og resultatbokser (blå bokser til høyre på siden). Samme fargebruk gjelder for tabeller, dvs. resultattabeller er blå

2 Digitalisering – en kort innføring

Dette kapitlet gir en kort innføring i begrepet digitalisering og relaterte begreper som skyteknologi og skybaserte tjenestemodeller. Innføringen er vinklet mot utvikling og behov i norsk olje- og gass-næring og er ment å danne grunnlag for senere deler av rapporten som diskuterer viktige funn fra dokumentanalyser og intervju med aktører i næringen. Innføringen er holdt på et overordnet nivå og er rettet mot et bredere publikum uten nødvendigvis inngående IKT-kompetanse. Referanser til ytterligere informasjon blir gitt hvor det er relevant.

2.1 En kort innføring i hva som ligger i begrepet digitalisering

Digitalisering er et vidt begrep, men kan forstås som en trend hvor data og digitale teknologier brukes for å forbedre eksisterende organisasjoner og prosesser. Dette er ikke noe nytt, men vi ser nå at informasjons- og kommunikasjonsteknologi i økende grad benyttes for å etablere nye dataintensive tjenester og funksjoner, og at data og prosessorkraft øker i omfang, blir mer distribuert, og mer tilgjengelig med lavere kostnad.

Digitalisering handler om å ta i bruk de mulighetene digitale muliggjørende teknologier gir til å forbedre, fornye og skape nytt.

Derfor handler ikke digitalisering bare om teknologi, men like mye om viljen og evnen til endring.

Digital 21 [2]

Så å si alle moderne organisasjoner har et forhold til digitalisering, enten som brukere, mottagere og/eller tilbydere av digitale tjenester. Dette er en utvikling som drives av stadig større og mer avanserte programvaresystemer med stor kapasitet, økende mengder data og økende grad av kobling mellom systemer over internett som en kommunikasjonskanal med høy fleksibilitet og kapasitet. Dette drives av utsiktene til bedre drift og større fortjeneste hvor data utnyttes for å bygge ny kunnskap og effektivisere prosesser, for eksempel ved økt automatisering og forenkling av manuelle prosesser. For olje og gass-næringen kan dette være effektivisering av bore og produksjonsprosesser, bedre sikkerhet og reduserte utslipp. Et kjent eksempel fra andre domener er bank og finansnæringen, hvor data- og nettbaserte IKT-løsninger for lengst har erstattet det som før var omfattende manuelle prosesser. Gevinsten ved dette er lettere tilgang på nye, raskere og bedre tjenester for kundene som kan utføre de fleste oppgaver hvor som helst og når som helst. Tilsvarende muliggjør dette besparelser, nye tjenester, og mer effektiv drift for bankene. Graden av manuelle prosesser har betydelig redusert over tid. Vi ser det samme i olje- og gassnæringen hvor utviklingen har gått fra innføringen av løsninger som eDrift på 90-tallet - hvor IKT muliggjør integrerte operasjonssenter som gir en effektivisering [15] - til en situasjon i dag hvor stadig mer data samles og benyttes til utvikle nye tjenester, for eksempel basert på digital tvilling og skytjenester.

Digitalisering har nådd et omfang som omfatter så å si alle samfunnsområder og næringer, også definitivt olje og gassbransjen, men hvor utviklingen kan sies å være i startfasen sammenlignet med andre bransjer. Denne utviklingen relateres ofte til begrepet Industri 4.0, eller den fjerde industrielle revolusjon, som hentyder på et tettere samspill mellom programvare, maskinvare og organisasjon – i utgangspunktet i produksjons-virksomheter. Dette omtales også som 'cyber-physical systems' hvor fysisk utstyr koples mot distribuerte programvarebaserte systemer, og realiseres basert på nyskapende teknologier som maskinlæring, Industrial internet of things (IIoT), ny kommunikasjonsteknologi, autonome system, etc.

Selv om digitalisering i olje og gass-næringen er en tydelig trend både i Norge og internasjonalt er det en utvikling i tidlig fase hvor det er vanskelig å danne seg et komplett bilde over utviklingen for aktørene og ikke minst hvor den er på vei [16]. På et overordnet nivå er målet «intelligente oljefelt», «intelligent boring», og «intelligente rørledninger». Dette er utydelige begreper uten tydelige definisjoner, men der hvor et begrep som «det digitale oljefelt» hentyder på teknologi som erstatter eller effektiviserer menneskelige og repetitive arbeidsoppgaver hentyder «det intelligente oljefelt» til teknologi som også skaper, analyserer og anvender kunnskap. Et «intelligent oljefelt» kan beskrives gjennom følgende funksjoner: 1) real-time tilgang til data, 2) analyse av status quo, trendanalyse, og optimalisering, 3) operasjonell integrasjon, 4) automatisert kontroll. Som en antydning om potensiale tilsier erfaringsdata at «intelligente oljefelt» kan gi en produktivitetsøkning på 2-8% med 2-6% bedre utvinning [16].

Selv om digitalisering er et konsept med stort potensiale så snakker vi også om en stor vekst i kompleksitet og distribusjon av data som også må håndteres. Gammelt utstyr og nytt utstyr digitaliseres, store mengder data produseres, samles, analyseres og brukes på nye måter hvor vi enda ikke helt forstår potensial og begrensninger godt nok. Dette krever kompetanse og store ressurser og er utfordrende å håndtere selv for store organisasjoner med i utgangspunktet høy kompetanse. Mange aktører velger å benytte seg av ulike former for skyløsninger som et alternativ til å bygge opp og drifte egen inhouse kapasitet.

Cloud computing:

A computing capability where the architecture surrounding massive clusters of computers is abstracted from the applications using it and a software and server framework (usually based on virtualization) provides clients scalable utility computing capabilities to elastically provide many servers for a single software-as-a-service style application or to host many such applications on a few servers.

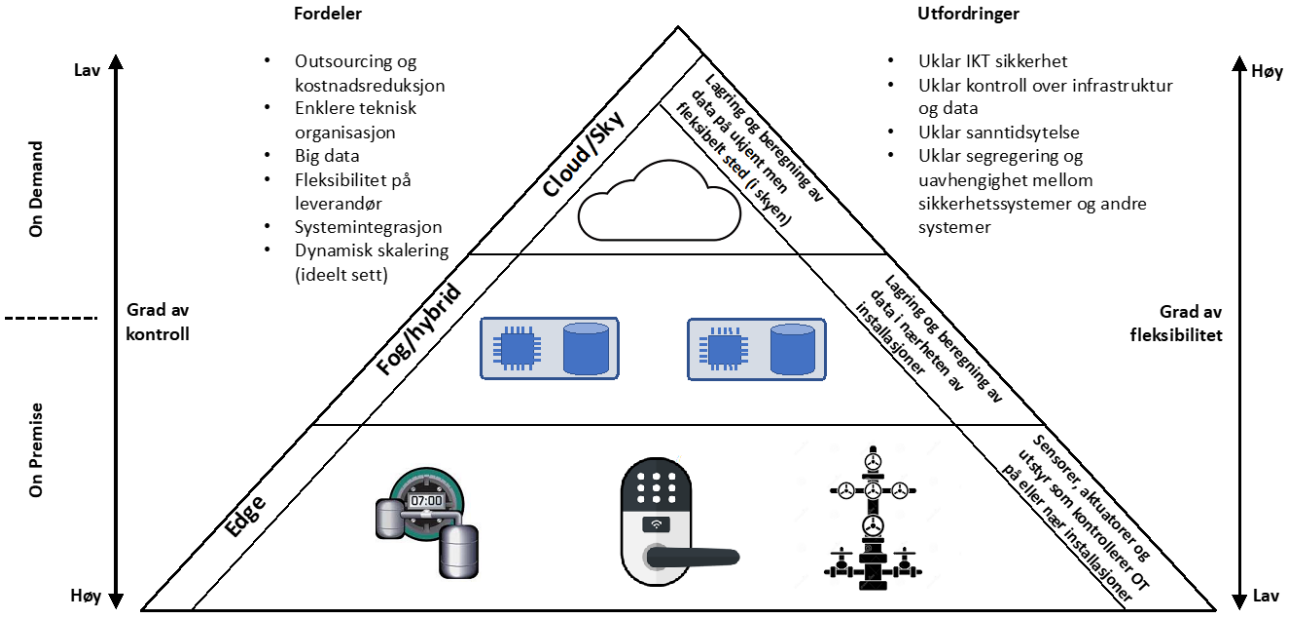
NIST [3]

Alle de store aktørene har tatt i bruk skyløsninger, typisk fra de store markedslederne som Microsoft (Azure), Amazon (AWS), IBM (Cloud), m.fl. 'Cloud' eller 'sky' er begreper som hentyder til at man som kunde eller bruker skjules for kompleksitet og ansvaret for fysisk lagring, prosessorkapasitet, ressurs-pooling og skalerbarhet, ved å overlate dette til en ekstern aktør. Man slipper da å bygge opp egen driftskompetanse, kapsitet og infrastruktur for å heller fokusere på kjernevirksomheten. Disse leverandørene har typisk datasentre med enorm kapasitet og betjener mange kunder samtidig for å realisere effektiviserings-gevinster. I slike tilfeller har man ofte liten kontroll på hvor data fysisk lagres og prosesseres.

Alternativt, dersom det er viktig for en kunde å ha større grad av kontroll på lagring og bruk av data kan man etablere egne private skyløsninger i egen infrastruktur. Da påvirker og kontrollerer en selv fysisk implementering (prosessor, lagring, nettverk etc.) – dette kan omtales som 'fog' eller hybrid-løsninger. Disse kan også, være koblet med rene skyløsninger. Det stiller da større krav til egen kompetanse og investeringer i infrastruktur, og fleksibiliteten er lavere. Et annet viktig begrep er 'edge'. En løsning som ligger fysisk nært utstyr eller systemer. Typisk i tilfeller hvor det er krav om høy grad av sikkerhet, kontroll og ytelse/responstid, og man ikke kan tillate at data lagres i en skyløsning. Manglende kontroll eller forutsigbarhet på tilgjengelighet, oppetid, og responstid (der data transporteres via internett som har uforutsigbar og variabel ytelse) på grunn av fysisk lokasjon kan være grunner for dette. Nedsiden er at man da ikke har samme mulighetsrom for sammenstilling og prosessering av data på tvers av systemer.

Man snakker ofte om ulike typer tjenester i forbindelse med skyløsninger:

- Infrastructure-as-a-Service (Iaas) hvor man kjøper infrastrukturkapasitet, for eksempel lagringsplass eller prosessorkapasitet.
- Platform-as-a-Service (PaaS) hvor man kjøper seg kapasitet på en virtuell systemplattform, for eksempel virtuelle Windows-servere, databaser, e.l.
- Software-as-a-Service (SaaS) hvor man kjøper tjenesten en programvare yter istedenfor selve programvaren for å drifte denne selv i egen infrastruktur, for eksempel et analysesystem.

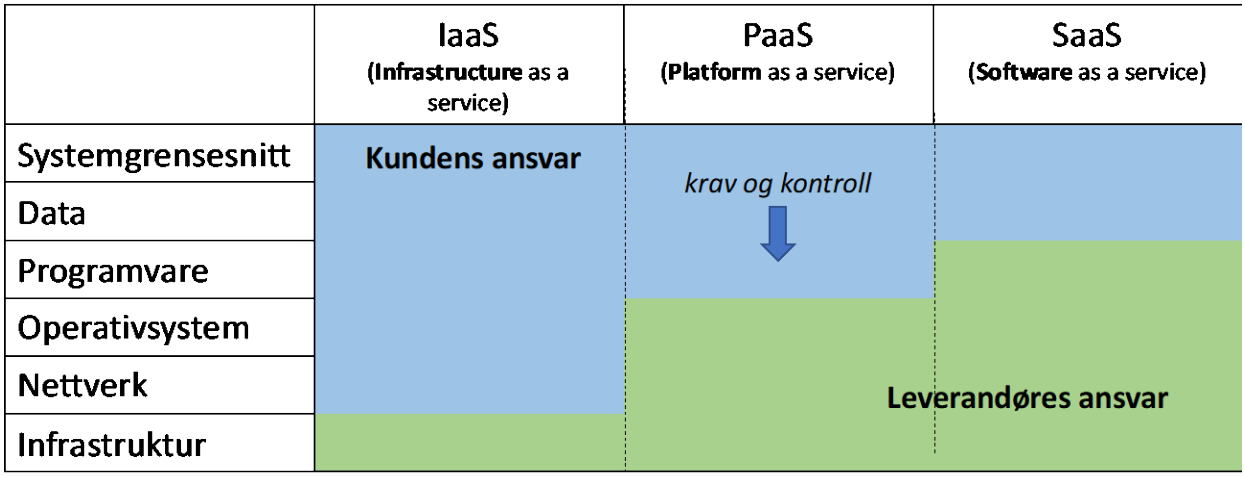


Figur 1 Edge, fog og cloud computing

'Sky' – 'fog' – 'edge' indikerer et spenn mellom grad av kontroll på den ene siden, og fleksibilitet på den andre (Figur 1). For rene skyløsninger hvor alle data lagres og prosesseres i et datasenter som er lokalisert utenfor organisasjonen og driftet av en leverandør, vil man ha høyere grad av fleksibilitet og behovsbasert tilgang på ressurser, men mindre grad av kontroll. Man kan kjøpe kapasitet etter behov uten å måtte skalere egen infrastruktur, men avgir grad av kontroll på hva som skjer med data, hvordan de sikres, og hvem som har tilgang. Dette må da eventuelt uttrykkes i kontrakter og avtaler, og i oppfølging av leverandøren. Motsatt, dersom man lagrer og analyserer data nær operativ virksomhet (i fysisk nærhet til sensorer og aktuatorer, gjerne på samme nett – herav navnet 'Edge') har man stor grad av kontroll, men liten grad av fleksibilitet og må selv ta kostnader og ansvar med å håndtere infrastruktur og drift eller eventuelt inngå en avtale med en leverandør og følge opp denne. Fog, eller hybrid, antyder en mellomvariant , hvor data og prosessering er lokalisert mer sentralt, eksempelvis i eget internt datasenter, hvor det fortsatt er nærhet til utstyret som kontrolleres. Fordelen er da at dette kan fysisk plasseres i en system infrastruktur med etablerte mekanismer for informasjonssikkerhet (brannmur/DMZ). Hybrid kan også indikere kombinerte løsninger mellom lokal og distribuert kapasitet. Graden av kontroll vil være større men graden av fleksibilitet vil være lavere.

En viktig følge av digitalisering er skifte i ansvar for informasjons-sikkerhet. Når alt utstyr og alle systemer kontrolleres av en og samme organisasjon har organisasjonen naturlig nok også ansvaret for alle aspekter av informasjonssikkerheten, og da muligheten for en stor grad av kontroll (gitt gode prinsipper og riktig bruk av teknologi). Når infrastruktur, plattformer og/eller programvarebaserte tjenester flyttes ut av organisasjonen helt eller delvis, flyttes også noe av ansvaret for informasjonssikkerhet ut - men ikke alt. Figur 2 viser

prinsipielt hvordan graden av digitalisering, fra outsourcing av kun infrastruktur til outsourcing av programvare, forskyver dette ansvaret. Når leverandøren tar mer av ansvaret er det naturligvis viktig at kunden er i stand til å sette krav og kontrollere at ansvaret håndteres godt.



Figur 2 Skifte i ansvar og kontroll av informasjonssikkerhet

Dette spennet i kontroll og fleksibilitet er grunnleggende viktig for organisasjoner med virksomhet som omfatter stor risiko og er avhengig av avanserte dataintensive løsninger for å kontrollere risiko. Olje og gass-bransjen er på mange måter et typisk eksempel. Enkelt sagt vil ledelsen kunne ønske en rask utvikling for å hente ut gevinster raskt, mens operasjon og produksjon ser utfordringer ned mot OT. Det kan altså forekomme en spenning mellom ledelse/strategi og operasjon/drift som kan påvirke prioriteringer, kompetansebygging, og utviklingsarbeid.

2.2 Gevinster ved digitalisering og hvorfor dette er en viktig trend

I rapporten Digital 21 [2] fremheves olje- og gassvirksomheten i Norge som ett av 10 viktige områder hvor digitalisering vil skape nye muligheter og økt konkurransekraft som er nødvendig for å møte forventet lavere oljepris og økt konkurranse fra nye energiformer. Kort sagt anses digitalisering som en nøkkel til effektivisering og en forutsetning for bransjens levedyktighet på sikt. Rapporten henviser til McKinseys anslag på et årlig potensial for innsparing ved digitalisering på norsk sokkel på 30-40 milliarder kroner.

«Digitalization technologies contribute significantly to reduce costs and improve recovery.»

OG21 rapport [1]

OG21 rapporten 'Norway's oil and gas technology strategy for the 21st century' [1] presenterer en analyse av bransjen og konkluderer med at digitaliseringsteknologier vil bidra til signifikante kostnadsreduksjoner og øke utvinningsevnen. Rapporten peker spesielt på følgende seks teknologier som «digitaliseringsteknologier»:

- Field model optimization
- Big data exploration analytics
- Wired pipe (borestreng med signalkabler)
- Automated drilling control
- Predictive maintenance
- Unmanned platforms

Dette er alle teknologier som kan beskrives som *dataintensive*, det vil si at de er basert på omfattende innsamling og prosessering av data. Dette kan være data fra OT-laget, for eksempel temperatur, trykk, eller andre data fra reservoar, boring osv. Dersom slike data samles med høy oppløsning og frekvens, for eksempel i en skyløsning med stor kapasitet for lagring og prosessering, kan de utnyttes til for eksempel prediktivt vedlikehold (store datamengder fra mange instanser over lengre tid) som potensielt kan gi lavere vedlikeholdskostnader. En annen åpenbar utnytting av data er oppbygging av modeller eller digitale tvillinger som kan optimalisere for eksempel boring – dette er allerede relativt moden teknologi. Se for øvrig egen rapport om modellkontrollert operasjon [17].

Neste generasjon dataintensive tjenester vil dra nytte av maskinlæringsteknologi (ML) som har potensiale til å utnytte store datamengder bedre enn tradisjonelle løsninger basert på klassiske (deterministiske) algoritmer og matematiske modeller. Et maskinlæringssystem kan interpolere prediksjoner og klassifiseringer om fremtidige situasjoner (nye data) basert på læring fra eksisterende data. Enkelt sagt er et ML-system effektivt for å finne nye sammenhenger i kjente datamengder mens det har problemer med å gjøre gode prediksjoner utenfor kjente datamengder (ekstrapolering). Et ML-system trener opp seg selv til å gjøre beslutninger som da altså ikke er basert på en forhåndsdefinert algoritme. Det vil si at det ikke er trivielt å forstå *hvordan* og *hvorfor* systemet gjør som det gjør og kan enkelt sagt beskrives som en 'black box' [18]. Et kjent eksempel er Googles AlphaZero, et ML-system som trener opp seg selv i sjakk ved å spille mot seg selv innenfor spillets enkle grunnregler. Systemet er nær sagt uslåelig innenfor sitt kjente domene, men gir ingen mening dersom reglene endres.

Johan Sverdrup er et konkret eksempel på et omfattende digitaliseringsprosjekt i olje og gass-bransjen, hvor utbyggingsprosjektet har utviklet en egen Digital Roadmap med to overordnede målsettinger; 1) å sørge for at de store datamengdene som skal samles kan brukes effektivt for å optimalisere håndteringen av reservoaret, og 2) utforske nye måter å arbeide på for å sikre en effektiv operasjon [19]. I praksis er dette omsatt i løsninger for bedre (databasert) beslutningsstøtte og automatisering av prosesser. Eksempler er forbedret drenerings-strategi, optimalisering av brønnplassering, og automatisert produksjon.

Potensiale for produktivitet og utvinning

"From the available statistics, intelligent oil fields can increase production by 2%–8 % and recovery by 2%–6%..."

Oil and Gas 4.0 era:
A systematic review and outlook [17]

I tillegg til rene effektiviseringsgevinster er det også potensielle sikkerhetsgevinster. Nye dataintensive tjenester kan assistere og på sikt delvis automatisere kritiske operasjoner, for eksempel boring, med bedre kick-deteksjon som reduserer risiko for brønn-kontrollhendelser med skadepotensiale for operatør/ driller og andre. Nye digitale tjenester kan altså forbedre pålitelighet og effekt av eksisterende barrierer, men da forutsatt at slike løsninger ikke introduserer nye svakheter eller trusler i seg selv. Det ligger et sikkerhets(safety)-potensiale i digitalisering som så langt antakeligvis ikke er fullt ut forstått og utnyttet. Dette bør være en like viktig driver for utviklingen som mer effektiv drift og utvinning. Dersom data om et anlegg eller en operasjon samles med god kvalitet skaper dette muligheter for å forbedre informasjon og situasjonsforståelse for operatøren, for eksempel via håndholdte løsninger eller VR eller AR-løsninger. Bedre tilgang på informasjon med god kvalitet kan bidra til økt sikkerhet. Man kan også se for seg løsninger som drar nytte av informasjon om operatørens plassering som sammen med data om pågående aktivitet kan benyttes for å forbedre sikkerhet. Det er potensielt mange slike tenkte eksempel som bør utforskes.

Ved siden av de rene tekniske gevinstene byr også digitalisering i bransjen på muligheter for tettere samarbeid og nye samarbeidsformer mellom aktører og leverandører. Så og si alle aktører har en digitaliseringsprosess og det ligger et åpenbart potensiale i å utvikle kunnskap og dele erfaringer basert på felles behov, problemstillinger og løsninger. Dette omfatter også åpning for deling av data på tvers av organisasjoner.

2.3 Skyteknologi i et olje- og gassperspektiv

Begrepene som brukes når vi snakker om skyteknologi kan være utydelige, men kan eksemplifiseres i følgende modell (basert på Purdue-modellen) som viser en typisk inndeling av nivå for et anlegg, for eksempel en plattform.

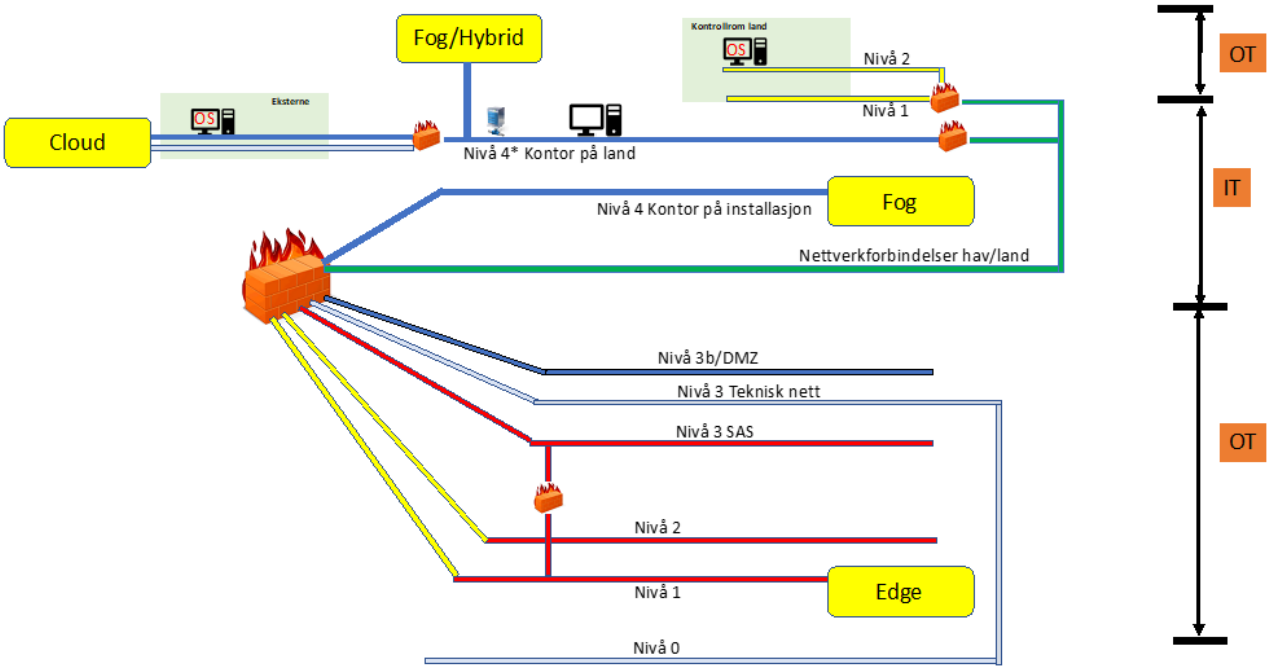
Edge hentyder på at data prosesseres *i nærheten* av der data er lokalisert og at det ikke i utgangspunktet overføres til et sentralt system over stor avstand. Dette kan være data som hentes fra utstyr med sensorer og aktuatorer i OT-laget slik som ventiler, trykkmålere, vibrasjonsmålere etc. Det kan også være data fra IIoT-utstyr. Hensikten er å sikre ytelse/responstid (direkte kobling eller få omveier for data) i tillegg til at man enklere ivaretar IKT-sikkerhet ved å holde både produksjon, transport og prosessering av data i for eksempel lag 1. Edge computing vil også redusere problemer med dataintegritet og kvalitet siden transport av data oppover i lagmodellen via flere systemer (historians, Pie-servere, etc.) kan føre til at data påvirkes, for eksempel dersom data fra en sensor konverteres til andre format. Konsekvensen av edge computing på den annen side er at data og funksjonalitet har begrenset tilgjengelighet og anvendelighet for andre systemer. Selv

om edge hentyder på nærhet mellom data og prosessering kan det likevel være mulig å i tillegg dele data med andre system. Foundation Fieldbus er et eksempel på allerede etablert teknologi som innehar egenskapene til en edge-device i og med at applikasjon kan legges på sensor eller pådragsorgan.

Fog kan være en intern tjeneste på et høyere lag – nivå 3 (OT) eller nivå 4 (IT). Her samles data i større grad fra Edge-utstyr, typisk IIoT-enheter og gir dermed en større potensiell verdi gjennom sammenstilling av data og analyser av data fra flere datapunkt. Data er i relativ nærhet til operasjonen og systemeier må i utgangspunktet selv ta ansvar for infrastruktur, drift og vedlikehold – inkludert nødvendige tiltak for informasjonssikkerhet. En Fog-tjeneste kan også være koblet mot Cloud-tjenester på enda høyere lag.

Cloud indikerer at data og funksjonalitet fysisk er plassert utenfor arkitekturen, men kan være driftet enten internt (on premise) eller av en skyleverandør (on demand). Skyløsninger kan ha stor kapasitet på lagringsplass og prosesseringskapasitet, noe som er relevant med tanke på økningen av data som produseres i et moderne anlegg. Igjen er det en balanse mellom kontroll og fleksibilitet; en cloudserver i egen infrastruktur gir mer kontroll, spesielt på sikring og bruk av data, mens kjøp av tjenester fra en skyleverandør gir mer fleksibilitet hvor kapasitet kan kjøpes etter varierende behov, men hvor man overfører en del av kontrollansvaret til en ekstern leverandør.

Figur 3 vise hvordan disse begrepene kan plasseres i en typisk lagdelt arkitektur.



Figur 3 Cloud-Fog-Edge mappet med en fysisk Purdue-modell

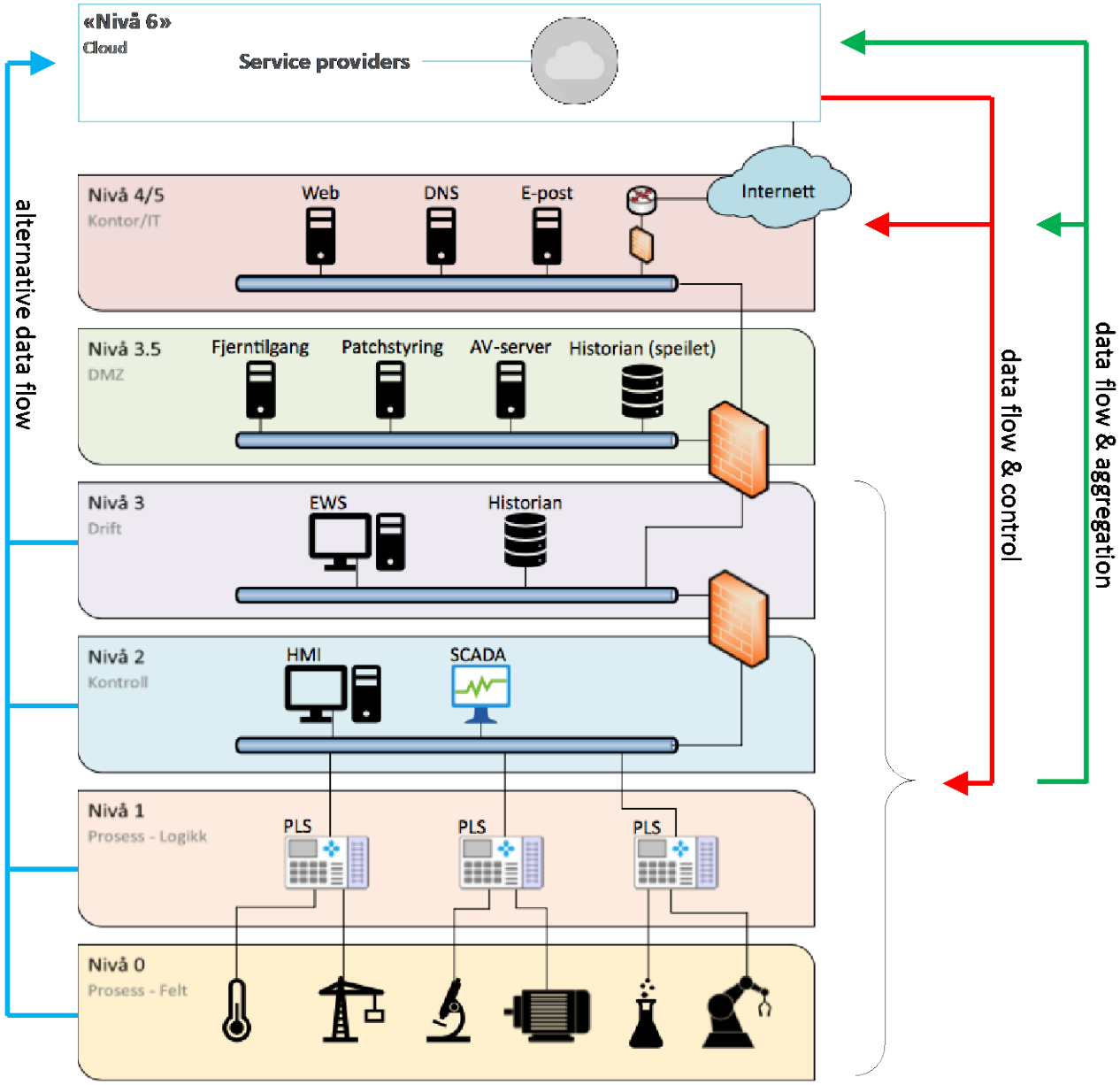
De fleste operatørene samt en del av leverandørene har gjort store investeringer i skyteknologi som bl.a. Microsoft Azure eller Amazon Web Services eller IBM Cloud – dette er drevet av et økt behov for *kapasitet* og *fleksibilitet*. Det er også inngått strategiske partnerskap med sky-leverandør for å sikre både kompetanse og kapasitet, samt sikring av data hvor det bl.a. er spesifisert *hvor* datasenteret er plassert geografisk, for eksempel for å holde det innen EU-området og da i henhold til gjeldende regelverk som følger med. I tillegg benyttes også egne skyløsninger fra tradisjonelle leverandører, for eksempel ABB Utility Sky.

Det finnes flere definisjoner og varianter av begrepene, som kan være uklare. Det essensielle er likevel *behovet for kapasitet* som følger den økende mengden data som produseres, og følgelig potensialet som ligger i å utnytte data, for eksempel for prediktivt vedlikehold, operatørstøttesystemer, digitale tvillinger, etc. Denne utviklingen krever kapasitet for lagring og prosessering av data som det kan være uhensiktsmessig eller vanskelig å passe inn i eksisterende infrastruktur men hvor man kan planlegge for dette i nye anlegg.

2.4 Forventede utfordringer med digitalisering i og olje- og gass-virksomheten

På et generelt nivå gir den pågående digitaliseringen i olje- og gassbransjen et sett av nye eller forsterkede utfordringer knyttet til sikring av data (transport, lagring, tilgang). Følgende modell (Figur 3) utvider Purdue-modellen som representerer godt etablerte prinsipper for hvordan man kan sikre sammenkopling og dataflyt mellom OT-lagene og opp mot IT-laget. Tradisjonelt vil en lagdelt arkitektur med DMZ og brannmur mellom lagene gi god kontroll og informasjonssikkerhet (så lenge prinsippene følges). Utfordringen vi nå ser som følge av digitaliseringstrenden er at behovet for å aggregere data oppover mot IT-laget og videre mot det vi kan beskrive som et nytt lag 6 (Cloud) samt eventuelle tilfeller av direkte påvirkning av OT fra et slikt lag utfordrer de etablerte prinsippene. Dette er ikke nødvendigvis et bilde av situasjonen i dag, men heller et bilde av hvor utviklingen er på vei. Eksisterende infrastruktur – inkludert mekanismer for informasjonssikkerhet – er ikke bygget for en dataflyt som vi nå ser komme i forhold til både informasjonssikkerhet og kapasitet (Figur 3 – grønn pil). Tilsvarende er ikke eksisterende OT-systemer i utgangspunktet bygget for kopling utover laget ovenfor (Figur 3 – rød pil). Som en del av den teknologiske utviklingen og behov for å ha kontroll på datakvalitet og ytelse (frekvens) kan vi komme til å se direkte koblinger mellom OT-lagene og skylaget (Figur 3 – blå pil). Det er viktig å merke seg at intervjuene med selskapene ikke viser at slike koblinger er gjort i dag, men signaler fra leverandørsiden tyder på at det er *ønskelig* med hensyn på responstid og tidsoppløsning. Dersom det er snakk om typiske edge-løsninger hvor data ikke flyttes ut av OT-laget er det greit, men dersom data flyttes til en skytjeneste vil det kreve meget gode tiltak for å sikre data. Noen leverandører selger inn diode-løsninger som en sikringsmekanisme, men dette er teknologi som har vist seg vanskelig å få til å fungere i praksis, bl.a. med utfordrende drift.

Eksisterende installasjoner og systemer (brownfield) har naturlig nok begrensninger på integrasjon og økt dataflyt. Utvidelser og ekstra utstyr som kobles mot OT-systemer og spesielt sikkerhetssystemene vil utfordre prinsippet om segregering og uavhengighet. Men nye installasjoner (greenfield) vil fra tidlig fase kunne designes for å kunne produsere og håndtere store datamengder. Utbyggingen av Johan Sverdrup er et eksempel på en slik utvikling hvor teknologivalg, bruk av dataintensive løsninger og derigjennom nye arbeidsformer vil prege utviklingen og andre installasjoner fremover. Begrepet 'the digital field-worker' skapes gjennom nye løsninger for automatiserte og digitaliserte arbeidsprosesser, digital tvilling, og modeller for deteksjon av avvik (anomaly detection models) basert på maskinlæring [20]. Dette er det vi kan kalle dataintensive løsninger som bygger på en langt større produksjon, transport og bruk av data enn tidligere installasjoner – spesielt fra OT-laget. Dette er også teknologier som i stor grad er basert på avanserte programvareløsninger som krever stor kapasitet for lagring og beregning og som muliggjør en større grad av forbedringer og videreutvikling av løsningene gjennom hele livsfasen til installasjonen.



Figur 4 En "utvidet" Purdue-modell

- **Konvergens mellom IT og OT**
  Det tradisjonelle skillet mellom IT og OT som ulike funksjonsområder med ulikt behov for beskyttelse, både i forhold til teknologi og organisasjon, bli mer utvisket. Standard informasjonsteknologi og programvareløsninger blir i økende grad også anvendt i OT-lagene, med edge-komponenter i lag 0-1 (IIoT) som koples mot fog og cloud-løsninger fra lag 2 og oppover. Kravene til beskyttelse av *funksjonen* er derimot de samme – ny teknologi og organisasjon må derfor tilby samme grad av sikkerhet.

- **Kompetanseløft**
  Utviklingen går raskt og krever oppdatert kompetanse, både på digitalisering og skyteknologi og på nye informasjons-sikkerhets utfordringer, og hvordan skybaserte tjenester kan påvirke sikkerhet (safety). Kompetansebehovet spenner fra organisatorisk til teknisk nivå og går på tvers av operatører og

leverandører. Dette behovet sees både hos operatør- og boreselskap (muligheter og begrensninger i teknologien), og på leverandørsiden (forståelse for etablerte sikkerhetsprinsipp og forskrifter).

- **Økt fokus på datakvalitet**
  Produksjon, flyt og bruk av data mot OT har tradisjonelt vært begrenset. Nå som dette er i vekst og blir viktig for både effektivisering og bedre sikkerhet (safety), blir sikring av tilstrekkelig *kvalitet* på data viktig. Dette for å realisere effektiviseringsgevinster og samtidig ivareta sikkerhet (safety). Herunder kommer god praksis og gode løsninger for konsolidering og aggregering av data. Dette kan være utfordrende siden ulike kilder har ulike format og ulik ytelse. Tradisjonelle OT-systemer har ikke vært utviklet med tanke på deling av data. Se egen rapport for en mer utdypende vurdering av behovet for å aktivt sikre datakvalitet [21].

- **Ytelse og tilgjengelighet**
  Leverandører av nye digitale og data-intensive tjenester kan stille krav til ytelsen i systemer som gir data inn til løsningen, hvor det for eksempel ikke vil gi tilstrekkelig ytelse eller oppløsning å hente data fra historians. I tilfeller hvor data hentes fra OT-laget kan det være snakk om store datamengder hvor det kan være viktig at data er oppdaterte til enhver tid for at tjenesten skal kunne fungere. Flowmeter nevnes som eksempel hvor «man får mer ut av data ved bedre frekvens». Motsatt, sett fra OT-siden, kan det være krav om tilstrekkelig responstid og tilgjengelighet. Dette er krav som det kan være vanskelig å tilfredsstille når dataflyt skal passere alle sikkerhetslagene, fra OT, til IT. Det kan dermed komme et økt press på *direkte kobling* fra OT lagene (0-3) mot skyløsninger, nettopp for å sikre ytelse for de skybaserte løsningene. Krav til ytelse og konsistens i oppløsning på tvers av datastrømmer og kilder kan føre til at press på transport fra OT lagene øker. Vurderinger av behovet for økt frekvens for signaler og funksjoner som i seg selv ikke nødvendigvis gir merverdi av høyere oppløsning må derfor holdes opp mot både den enkelte tjenestes ytelse og anleggets integritet. Det er god grunn til å stille tydelige krav til slike eventuelle løsninger og hvordan IKT-sikkerhet håndteres.

- **Informasjonssikkerhet og uavhengighet**
  Digitalisering utvider i utgangspunktet angrepsflaten: 1) Økt kopling og dataflyt kan gi et økt antall mulige veier inn i systemer som skal beskyttes, 2) behandling av store sammensatte datamengder kan gi økt mulighet for manipulering av data og analyser, 3) større kodebaser hvor funksjonalitet implementeres i programvare fremfor elektronikk kan manipuleres, 4) distribuert prosessering av data utenfor et, i utgangspunktet, beskyttet lag kan øke eksponering av beskyttelsesverdige data, og 5) standard IT infrastruktur (hyllevare) som OS og kommunikasjonsløsninger kan ha sikkerhetshull hvor det er utfordrende å patche i et OT-nært miljø.

  I eksisterende installasjoner er informasjonssikkerhet i stor grad ivaretatt av systemer som er bygd opp iht. lagdelte arkitekturer med informasjonssikkerhets-mekanismer mellom lagene, hvor de laveste og mest kritiske lagene nederst er beskyttet via lagene over. Den mest kritiske komponenten (for safety) - sikkerhetssystemene - skal være uavhengige systemer som er segregert fra øvrige system (ref. IF fra Petroleumstilsynet). Det er så langt ikke tegn på at sikkerhetssystemer som gass- og brannvarsling og nødavstegning har blitt koblet mot andre systemer i IT-laget med økt risiko, men gitt utviklingen mot datadreven virksomhet er det grunn til å anta at disse prinsippene utfordres, noe som krever et spesielt fokus med eksplisitt vurdering av risiko. Tidligere undersøkelser [22] viser at nødavstengingssystemer og sentrale deler av brann- og gass-systemer kan være på samme nett som kontrollsystemene (på lag 1) for å knyttes til samme operatørstasjon og arbeidsstasjoner, og for å forenkle datainnsamling. Ved slike designvalg vil det være enda mer kritisk om for eksempel kontrollsystem kompromitteres, enten ved direkte påvirkning av systemet eller ved manipulasjon av data inn til systemet. Det vil da være behov for å beskytte prosesskontrollsystemet som om det var et sikkerhetssystem.

2.5 Screening av forskningen om digitalisering av IT og OT

For å danne et overblikk over *forskningen* på tematikken ble det gjort et enkelt litteratursøk (appendix A). Følgende korte sammendrag uthever fokus i de identifiserte publikasjonene:

Det er et tydelig og stort fokus i bransjen på potensialet i big data og at data kan danne grunnlag for økt innovasjon, optimalisering, bedre kostnadseffektivitet, og bedre safety [23-25] [26, 27]. Potensialet for å utnytte den økte mengde data som blir tilgjengelig, til mer effektiv drift er ikke fullt utnyttet [27, 28]. Det er også fokus på begrensninger med Big Data, bla. relatert til cybersecurity og privacy, men dette er så langt underfokusert i regelverk og standarder [29]. En betydelig utfordring er at data fortsatt er fordelt i siloer og man forventer større effekt når tilgang på og integrasjon av data øker [30, 31].

Erfaringer viser spesielt betydelige besparelser for løsninger for tilstandsbasert vedlikehold [30]. Det er identifisert et potensiale for bedre HMS hvor økt automatisering reduserer behovet for mennesker offshore, for eksempel ved hjelp av løsninger for deteksjon av avvik (anomaly detection) [23]. Nye prosjekt og utbygginger gir store digitaliseringsmuligheter når løsninger kan planlegges fra tidlig fase. Johan Sverdrup er et godt eksempel [20].

Pågående endrings- og digitaliseringsprosesser øker outsourcing av komplekse IKT-løsninger som igjen kan øke risiko for uønskede hendelser [24]. Forskningen så langt indikerer at denne risikoen ikke forstås godt nok med tanke på kausalitet, kompleksitet og gjensidig avhengighet [32]. Økt digitalisering utvider risikobildet og muligheten for å ramme næringen, også fra fiendtlige stater [33]. Angrep direkte mot OT-systemer regnes for å være krevende å utføre per i dag (altså lavere risiko), men angrep rettet mot IT-systemer har en lavere terskel og kan være en vei inn mot OT, for eksempel ved å skaffe tilgang til passord eller manualer [33]. Dette betyr at man må ha samme standard for sikring av IT-systemer som for OT-systemer gitt økende grad av kopling fra det godt kontrollerte safety-domenet mot IT-systemer [25, 26]. God IKT-sikkerhet er derimot en utfordring, bl.a. med en økt avhengighet til leverandører [26].

Dagens forståelse og tiltak for cybersecurity holder ikke tritt med utviklingen [27]. Fokuset på digitaliserings*gevinster* kan synes å få et større fokus enn cybersecurity i kunnskap som formidles [20, 31].

Selv om det er et stort strategisk fokus på digitalisering og flere løsninger er i drift, er digitalisering (i næringen) i en tidlig fase. Dette reflekteres av forskningen med en overvekt av konseptuelle studier og hvor underleverandører dominerer over operatører. I en systematisk kartlegging av tilgjengelig forskning ble det funnet at hele 14 av 34 artikler som primært omhandler *utfordringer* rangerer 'cybersecurity' som den største utfordringen for IoT-adopsjon i olje- og gass industrien (internasjonalt) [34].

Denne oversikten antyder at cybersecurity, generelt, er et fokus i forskningen per i dag (2021). Men, det er så langt få spor etter spesifikke problemstillinger knyttet til økt kobling mellom IT og OT-systemer. Spesielt kan man legge merke til et så langt lavt fokus på digitaliseringens mulige implikasjoner for sikkerhetssystemer.

2.6 Relevante erfaringer fra digitalisering av øvrig kritisk infrastruktur

Mange bransjer som det er naturlig å sammenligne oljebransjen med har også vurdert bruk av sky i større eller mindre grad. Norsk Vann engasjerte Powel og SINTEF i en studie som omfattet denne problemstillingen, dokumentert i rapporten "Informasjonssikkerhet og skybaserte tjenester for vannbransjen" [35]. Her presenteres et utvalg sikkerhetskrav til skytjenester som er relevante for vann- og avløpsverk i Norge – mange av disse vil også være relevante for petroleumsbransjen.

Både i vannbransjen og i kraftbransjen har fokuset på nettsky vært konsentrert rundt innsamling og prosessering av sensordata, der resultatene av prosesseringen ikke direkte og automatisk brukes til å styre

driftkontrollsystemer (SCADA). En vesentlig forskjell mellom petroleumsbransjen på den ene siden, og vann- og kraftbransjen på den andre siden, er tilnærmingen til nødavstengningssystemer (ESD). Kraft og vann er definert som kritisk infrastruktur, og fokuset er primært forsyningssikkerhet, dvs. at kundene har vann i springen og strøm i kontakten.

I kraftbransjen er man opptatt av uavhengighet, men dette realiseres primært ved at kontrollromsfunksjoner (SCADA) holdes adskilt fra åpne nett, og distribusjonsstyringssystemer (DMS) har ikke anledning til å manipulere SCADA-brytere direkte. På tilsvarende måte har man per i dag i Norge adskilt smarte strømmålere (AMS) fra kontrollrommet, men dette skillet finnes ikke nødvendigvis hos kraftbransjen i utlandet. SINTEF har på oppdrag fra NVE [36] studert hvordan risikoen vil påvirkes av økt integrasjon av disse systemene; og mens det kan konkluderes at risikoen øker, identifiserer rapporten også flere mulige tiltak som virker avbøtende på risikoen. Det er grunn til å tro at det vil bli tettere integrasjon i framtiden, og det er derfor avgjørende at IKT-sikkerhetstiltak ivaretas for å unngå strømbruddssituasjoner slik som fant sted i Ukraina i 2015 og 2016 [37].

Bruk av skyløsninger forskyver kostnader fra investering (CAPEX) til drift (OPEX), og gjør det også lettere å skalere hurtig opp eller ned for å håndtere f.eks. sesongvariasjoner. Man kan også få stordriftsfordeler på den måten at nettskyleverandører har mulighet til å ansette en IKT-sikkerhetsgruppe med "kritisk masse" i langt større grad enn det mindre aktører kan.

Annen kritisk infrastruktur, som elkraft og vann har primært fokus på oppetid og leveransedyktighet og mindre på HMS. Et cyberangrep truer ikke først og fremst HMS men forretningsdrift og samfunnskritiske funksjoner. Det er også enklere å gå til sikker tilstand, for eksempel strømkutt, enn for olje- og gass-næringen som avhenger av at spesielt slukkesystemer fungerer som de skal. Disse ulikhetene gjør at systemer, rutiner og krav ikke er direkte overførbare utover generell sikring av skytjenester.

3 Viktige funn

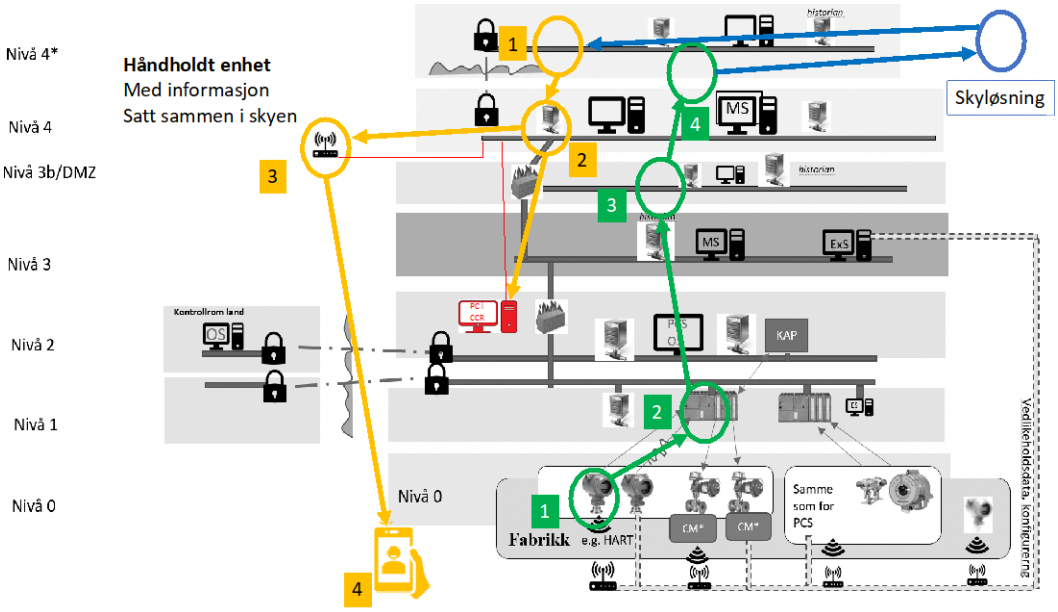
Dette kapitlet gir en oversikt over funn fra intervju og dokumentasjon som er mottatt fra selskapene.

3.1 Hva digitaliseres og hvordan?

Intervjuene understøtter at digitalisering i norsk olje- og gassvirksomhet er en svært tydelig trend og berører alle aktører. Store selskap har egne omfattende digitaliseringsstrategier og definerte roller og funksjoner i organisasjonen. Mindre aktører har ikke i samme grad uttalte strategier, men like fullt en stor bevissthet og satsning på digitalisering – innenfor rammen av sine ressurser. Det er viktig å merke seg at dette ikke bare er uforpliktende målsettinger – dette er tydelig reflektert i investeringer, kompetansebygging, nye organisatoriske funksjoner, og nye prosedyrer og retningslinjer. Digitalisering er ingen hype, det er et reelt paradigmeskifte som er i full gang. Som et eksempel har Equinor en 'digital visjon' om 1) å gjøre data tilgjengelig, 2) å bygge kompetanse for å utnytte data, 3) forutse og forhindre sikkerhetshendelser (safety & security), og 4) robotisering for å redusere menneskelig belastning [38].

Digitaliseringstrenden adresserer først og fremst IT-laget, men berører også OT-systemer i økende grad hvor data fra SAS og operasjonelle systemer (lag 0-3) samles for å kunne skape databaserte verdiøkende tjenester. Målet er naturligvis effektiviseringsgevinster (for eksempel prediktivt vedlikehold), *men også* bedre sikkerhet ved for eksempel å etablere bedre beslutningsstøtte (for eksempel operatørstøtte til boreoperatør/driller. Dette betyr at vi nå også ser at data fra OT-systemer i økende grad finner veien opp i skyløsninger eller skylignende løsninger. Data samles fra ulike sensorer og lav-nivå utstyr, for eksempel vibrasjonsdata, temperatur- og trykkmålinger, boring, sandmonitorering, m.m. Dette er data som samles og konsolideres over tid og som danner grunnlag for f.eks. ekspertsystemer, operatørstøtte, digitale tvillinger og modeller, som igjen brukes for å forbedre eller støtte prosesser og mennesker i nærheten av OT-laget, for eksempel boring (modellbasert kick-deteksjon) og prediktivt vedlikehold. Ekspertsystemer som i dag er fysisk plassert på anlegget og hvor leverandør styrer dette via fjerninnlogging kan etter hvert komme til å bli flyttet opp i skyløsninger, hvor da data og logikk er plassert på et annet sted enn der virksomheten foregår og hvor man da «mister» de informasjonssikkerhets-tiltakene man nyter godt av i dag.

Kort sagt blir data mer verdifulle jo mer data man har samlet på samme sted eller i samme system. I dag finnes det en rekke ulike løsninger, basert på ulik teknologi, men det er rimelig å forvente at utviklingen går mot stadig mer sentraliserte og standardiserte datakilder, som plasseres i høyere lag.



Figur 5 Mulige transportveier for data

Det tegnes et broket bilde av dagens installasjoner og hvordan data transporteres i det totale systemet, via hvilke systemer, og hvordan data behandles, kvalitetssikres, lagres og ikke minst sikres mot tilgang fra utenforstående (cybersikring) – det finnes mange mulige veier og tekniske løsninger og det gis eksempler på data som løftes fra få nivå til mange nivå, opp til IT-lag og til skyløsning. Vi kan også skille mellom vertikal integrering som er integrasjon mellom OT og IT i egen infrastruktur, og horisontal integrering som går mellom en installasjon og ekstern tjenesteleverandør som videre kan integrere med sine(e) underleverandører av for eksempel Infrastructure as a Service (IaaS). Figur 5 viser en konseptuell skisse over et tenkt men realistisk eksempel hvor data flyter fra OT-lagene til IT-laget (inkludert en skyløsning), og tilbake til operatøren som er ute i anlegget. Kompleksiteten er stor og de fleste aktørene gir uttrykk for at de strever med å holde oversikt – og kontroll.

Intervjuer med selskapene viser en svært stor bevissthet på at digitalisering og skyteknologi utfordrer uavhengighet (ref. IF) og sikkerhet. Dette står høyt på agendaen og ingen funn i intervjuene tyder på avvik i forhold til sikkerhetssystemene. Holdningen er at det er trygt å hente data opp fra OT til IT, men at det er risiko forbundet ved å sende data ned, for eksempel i form av styring av utstyr på OT-nivå, men det er grunn til å følge med på utviklingen her. Det er identifisert fire usikkerhetsmomenter:

- **Usikkerhet om dataflyt**
  Data som hentes fra OT-laget opp til IT-laget, eller til en skyløsning, kan potensielt gå via mange nivå, systemer og sikringsmekanismer, for eksempel ulike historians, IMS'er, kontrollsystem, brannmurer og switcher. Enkelte nye løsninger kan også gå utover eksisterende infrastruktur og hente data opp direkte via egne kanaler. Noen leverandører av tjenester kan ha behov en direkte kopling i tilfeller der ytelsen i eksisterende infrastruktur ikke er tilstrekkelig, for eksempel i forhold til ytelse og responstid (fordi det ikke er bygget for slik bruk). Dersom det er snakk om data som samles fra mange kilder og

med stor frekvens kan det blir utfordrende å ha oversikt og kontroll. Denne kompleksiteten forverres ytterligere når det på høyt nivå, i IT eller i et sky-lag, er flere systemer som henter og bruker data for å levere tjenester – spesielt dersom dette er systemer som kontrolleres av andre aktører.

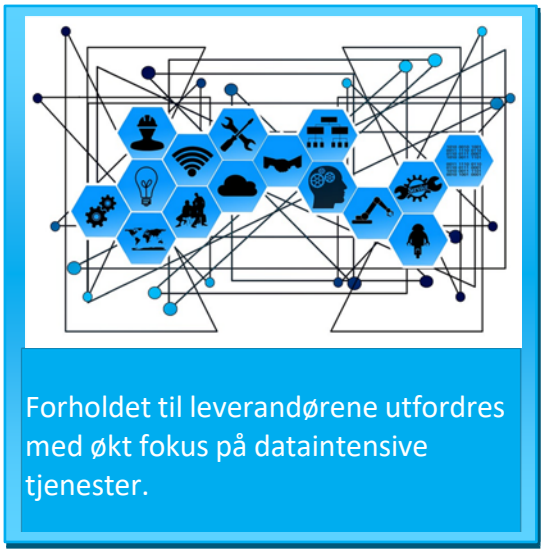
- **Usikkerhet om behandling av data**
  Når data løftes opp i systemer utenfor OT-laget, og spesielt i skyløsninger på leid infrastruktur (on demand) vil det være utfordrende å ha kontroll på hvordan data behandles og lagres. Dette omfatter i utgangspunktet kontroll av hvordan data sikres, hvor lenge data lagres, hva som skjer av endringer av data, hvordan data fra flere kilder sammenstilles, og hvem som har tilgang til data dersom data lagres i en infrastruktur som deles med flere. Eierskap til data blir uklart. Denne usikkerheten blir naturlig nok spesielt fremtredende i tilfeller hvor dette er data som inngår i tjenester som direkte eller indirekte påvirker OT-laget. Inntrykket er at selskapene har for lav bevissthet rundt sin rolle og ansvar som dataeier.

- **Usikkerhet om sikring av data (økt angrepsflate)**
  Økt integrasjon mot OT-laget gir en økt angrepsflate og kan påvirke uavhengigheten til et system, for eksempel SIS. Dette blir naturlig nok enda mer utfordrende jo høyere opp integrasjonen går. Dette er en risiko som selskapene er klar over og det er uttrykt et tydelig prinsipp om at ingen systemer på OT-nivå skal påvirkes direkte av nye digitale løsninger i IT- eller sky-lag. Det er derimot grunn til å tro at dette er et prinsipp som utfordres kraftig av gevinstpotensialet som nettopp ligger i økt dataintegrasjon.

- **Usikkerhet om datakvalitet**
  For dataintensive tjenester vil kvalitet på data være svært styrende for kvaliteten på tjenesten. For eksempel vil kvaliteten og presisjonen for en løsning for prediktivt vedlikehold avhenge av kvaliteten på data som samles inn. Dette betyr at sikkerhet (safety) avhenger av kvalitet på data, for eksempel om det blir tatt feilaktige beslutninger om vedlikehold. Tidsstempling av data fremstår som en særlig utfordring og nevnes av flere aktører. Ulike systemer kan operere med ulike tids-format og ulike systemer kan ha ulik ytelse/responstid som påvirker tidsstemplingen. Dette kan påvirke kvalitet på aggregerte og sammenstilte data.

3.2 Forholdet til leverandørene

Operatør og boreselskapene er nært knyttet til sine leverandører og har over lang tid etablert en god praksis for spesifikasjoner, bruk av omforente standarder, kontrakts-praksis og tydelig ansvarsfordeling, spesielt når det kommer til kontrollsystemer og sikkerhetskritiske systemer i OT-laget. Dette bildet utfordres også av den pågående digitaliseringen i bransjen og vi ser en helt ny type leverandører som tilbyr nye typer tjenester. Rent digitale tjenester betyr at det i større grad blir uklart *hvor* og *hvordan* rene programvarebaserte, dataintensive, og nettbaserte tjenester utføres og hvordan ansvar fordeles. Slike tjenester kan også ha et annet endringsregime enn systemer som befinner seg fysisk på for eksempel en plattform, det vil si at programvare som utgjør forretningslogikk kan forbedres og endres i en kontinuerlig prosess med hyppige oppdateringer, for eksempel patching ved nyoppdagede trusler. Dette er tydelig trenden innen IKT generelt siden sentralisert programvare enklere kan (og bør) endres enn systemer som må installeres på fysiske maskiner.



Forholdet til leverandørene utfordres med økt fokus på dataintensive tjenester.

DevOps [39] er – generelt sett – en utstrakt drifts- og utviklings-modell for systemer hvor programvare enten er lokalisert i en skyløsning eller tilkoblet leverandøren. Drift/bruk synkroniseres som en sammenhengende prosess hvor erfaringer og nye behov fra brukersiden (bl.a. relatert til IKT-sikkerhet) spilles tilbake til leverandørsiden som kan svare raskt med oppdateringer. Dette angår i liten grad utvikling og drift av IACS-systemer (i olje- og gassbransjen), men gitt den pågående digitaliseringen er det grunn til å forvente at leverandører av skybaserte eller tilkoblede systemer vil kunne ønske å fremme en slik modell i fremtiden. Det er derimot viktig å merke seg at hyppige oppdateringer av operative systemer med krav om høy tilgjengelighet og oppetid vil være svært utfordrende.

Vi ser også nye leverandører av dataintensive tjenester som ikke tidligere har levert mot olje- og gassbransjen og som dermed ikke har samme domeneforståelse som de etablerte har, inkludert spesielle krav og retningslinjer for olje og gass. I tillegg uttrykkes det også bekymring for nye og særlig små leverandørers kompetanse og kapasitet til å håndtere informasjonssikkerhet, særlig der kunden tvinges til å måtte stole på leverandøren fordi de selv ikke har kompetanse og kapasitet. Dette er verdt å merke seg spesielt siden det er snakk om leverandører som i stor grad baserer sin virksomhet på samling, behandling og bruk av data som definitivt kan sies å ha en påvirkning på sikkerhet og robusthet i operasjoner. Dersom man sammenholder dette med bransjens egen vurdering av at bransjen selv også mangler tilstrekkelig kompetanse på å håndtere informasjonssikkerhet i stadig mer tilknyttede og datadrevne systemer så fremstår dette som en viktig utfordring som må adresseres. Store selskaper og leverandører derimot er langt mer robuste. Blant annet så tilbyr etablerte SAS-leverandører digitale tjenester, som er basert på inngående kjennskap til bransjen og som har bedre løsninger for informasjonssikkerhet.

Leverandører som baserer sine tjenester på sammenstilling av data fra OT-laget har ikke nødvendigvis god nok forståelse for dataflyt og hvordan systemer sikres vha. soner, tuneller, switcher, og brannmurer – kort sagt, hvordan systemer forholder seg til Purdue-modellen som ligger til grunn for nettverkstopologien på mange installasjoner og som er en forutsetning for segregering og uavhengighet. Videre så vil enkelte nye dataintensive tjenester kreve mer i forhold til hastighet og kapasitet enn eksisterende infrastruktur kan tilby. Eksisterende anlegg ble naturlig nok ikke designet i forhold til integrasjon med løsninger i et skylag og enkelte nye leverandører ønsker derfor å kunne koble sine løsninger direkte med mot OT-laget, først og fremst for å samle data

En annen utfordring, som langt i fra er ny, er at enkelte leverandører av systemer «bokser inn» data og funksjonalitet. Det vil si at kunden, for eksempel et operatørselskap, ikke uten videre har tilgang på egne data. Enkelte selskap uttrykker ønske om å bryte opp denne situasjonen, både for å bedre kunne kontrollere egne data og for å kunne åpne for å anvende data i nye sammenhenger, på tvers mellom systemer og leverandører. Dette utfordrer derimot enkelte leverandører som må finne nye forretningsmodeller; dersom de ikke kan ta betalt for eksempel i form av lisenser så må deres tjenester og systemet verdisettets på en annen måte.

Noen selskap melder også om leverandører som ber om eller ønsker mer data enn de strengt tatt behøver for å levere sine tjenester. Det er forståelig sett fra leverandørens ståsted siden data er hele grunnlaget for å skape verdi, spesielt med tilgang på data fra flere kunder og installasjoner eller anlegg. Her må kundesiden og de som eier data i større grad ta kontroll og styre hva og hvor mye som deles.

Selskapene bør utvikle en bedre forståelse av sin rolle som dataeier og hvilke krav som må stilles til leverandører som samler data. Eierskap til data bør reflekteres i krav og kontrakter på samme måte som krav til funksjonalitet, ytelse, tid, og kostnad. For eksempel er det relevant å stille krav om 1) sikring av data der data lagres og behandles utenfor egen infrastruktur, 2) tilgang og deling der samme infrastruktur deles mellom kunder, 3) ivaretakelse av data over tid, og 4) utnyttelse av data utover det som er nødvendig for tjenesten som ytes.

Prinsipielt er behovet det samme som for personlige data, som nå reguleres av EU's General Data Protection Regulation (GDPR); eierskap til industrielle data må også vernes, både fra et forretningsmessig ståsted og et sikkerhets-ståsted. EU kommisjonen er i gang med utarbeidelse av Data Governance Act som vil kunne støtte data-eiere både i å beskytte eierskap og i å utnytte data.

3.3 Digitalisering og IKT-sikkerhets-utfordringer for OT

Digitalisering som omfatter OT, og dermed gir økt kobling (Figur 3) kan i utgangspunktet skape nye IKT-sikkerhetsutfordringer og utfordre prinsippet om uavhengighet. Basert på intervjuene med aktører i bransjen er det en tydelig bevissthet på IKT-sikkerhets utfordringer, også i forhold til OT, men det er fremdeles behov for å forstå dette bedre og finne riktige tiltak. Kompleksiteten er stor og vanskelig å håndtere – hvordan har man kontroll på segregering/sikkerhet dersom man ikke har kontroll på flyt, plassering, kvalitet og bruk av data?

Selv om bevisstheten rundt IKT-sikkerhet i OT er sterk blant alle operatør- og boreselskap som ble intervjuet er det igjen de største aktørene som har mest ressurser for å utvikle kompetanse og kapasitet i form av dedikerte roller og funksjoner, og utvikling av egne rutiner og prosedyrer. De har dermed også en viktig rolle i å dele kunnskap med resten av bransjen.

En viktig del av helhetsbildet er at den pågående digitaliseringen i stor grad skjer gjennom samarbeid med leverandører og ved bruk av nye digitale og dataintensive løsninger og tjenester. Dersom disse kan ha direkte eller indirekte påvirkning på sikkerhet (safety) er det avgjørende at systemeier (operatøren) oppfyller sitt ansvar med å tilrettelegge, kontrollere og påse at også denne type leverandører oppfyller gjeldende krav i regelverket: Rammeforskriften '*§ 18 Kvalifisering og oppfølging av andre deltaker'* og '*§ 7 Ansvar etter denne forskriften'* som pålegger operatøren å: *«påse at alle som utfører arbeid for seg, enten personlig, ved ansatte, ved entreprenører eller underentreprenører, etterlever krav som er gitt i helse-, miljø- og sikkerhetslovgivningen.»*

Det er i seg selv ukomplisert å skallsikre systemer for å ha få veier inn og ut, men dersom utviklingen går mot mange systemer og koblinger blir det også mer krevende å ha kontroll på oppsett og vedlikehold (bl.a. patching) av brannmurer og switcher som sørger for sikringen.

Enkelte selskap praktiserer prinsippet om at alle system som avgjør integritet skal være hostet på stedet, eksempelvis en plattform. Dette prinsippet utfordres også i jakten på mer effektive dataintensive tjenester som forutsetter samling av større datamengder.

Det er en tydelig holdning om at det er risiko forbundet med koblinger *ned* til OT-systemene, for eksempel automatisert styring av OT-utstyr. Samtidig er det en holdning om at det er trygt å hente data *opp* fra OT-systemene til IT-laget eller et skylag under antakelsen om at en kompromittering av data ikke direkte vil påvirke OT-systemene. Men, dette forutsetter at det faktisk er en trygg overføring. Til og med løsninger hvor et system *kun* kan spørre om data har i prinsippet mulige svakheter, for eksempel i form av DOS-angrep. Dioder nevnes som en mulig løsning og markedsføres for sikker (enveis) overføring av data fra et OT-system til et IT-system, men er nødvendigvis ikke en løsning som dekker alle behov [40].

Det som derimot ofte er tilfelle er at slik styring skjer manuelt ved at en operatør mottar data (for eksempel om trykk i rør via en bærbar enhet), som er kritisk for sikker operasjon. I dag er tillitten til slik styring ikke god nok og i praksis skal en operatør, iht. detaljerte prosedyrer, verifisere data manuelt med kontrollrommet. Fra operatørsiden uttrykkes det bekymring for tredjepartssystemer og overholdelse av prosess og prosedyrer. I prinsippet spiller det ingen rolle om styringsinformasjon går direkte til system eller via menneske (operatør), konsekvensen av feil informasjon kan likevel være den samme og det er i praksis krav om dobbel kontroll uansett.

Dersom det etableres mange ulike løsninger med flere uavhengige databaser og eventuelt skyløsninger, basert på ulike teknologier, så blir *totalbildet* svært komplekst med flere data-siloer som må håndteres. Noen selskap anerkjenner denne utfordringen og ønsker å samle data i ett 'superobjekt' eller én sentral skyløsning. Dette reduserer kompleksitet og øker mulighet for å skape verdiøkende tjenester – men det betyr samtidig at sårbarheten er svært stor dersom en utenforstående skulle klare å skaffe seg tilgang og kunne påvirke data og tjenester og det er da viktig at informasjon i en slik database ikke benyttes på en måte som kan påvirke OT-systemene.

For å håndtere kompleksitet og IKT-sikkerhetsutfordringer mot og i OT-laget peker flere aktører til NOG104 og nettopp IEC62443 som et grunnlag. Førstnevnte anses i en viss grad til å være utdatert i forhold til digitalisering og sistnevnt anses å være uferdig og vanskelig (så langt) å omsette i praksis. Det er også, naturlig nok, de store aktørene som har ressurser og kapasitet til å styre sin utvikling iht. standarden, og til en viss grad bidra inn i utviklingen av IEC 62443.

Det er et stort fokus på IEC 62443-serien som et viktig hjelpemiddel for å håndtere nye utfordringer for IKT-sikkerhet, men denne standarden er fortsatt under utarbeidelse . Det er viktig å følge opp utviklingen og forstå hvordan prinsippene kan anvendes i praksis.

3.4 Samarbeidsbehov – og vilje, på tvers i bransjen

Selskapene som er intervjuet gir tydelig inntrykk for et behov for samarbeid i bransjen for å forstå og løse utfordringene med en felles retning, og utnytte mulighetene som følger digitaliseringen. Samtidig uttrykkes det også en vilje til slikt samarbeid. Dette ser vi allerede gjennom stor aktivitet i fagfora som for eksempel PDS-forum og det nyopprettede CDS-forum som er dannet for å adressere spesielt cyber-security utfordringer. Dette er viktige møteplasser som bør drives og videreutvikles. Alle aktører jobber i bunn og grunn med å løse de samme utfordringene som har høy kompleksitet og som krever en viss form for standardisering for å dempe behovet for å måtte håndtere for mange ulike strategier og teknologier. De aller største aktørene med mest ressurser er viktige for å utvikle kunnskap og påvirke standardiseringsarbeid på vegne av aktører med mindre ressurser – dette fordrer åpenhet og deling av informasjon. De store SAS-leverandørene har etablert stor kompetanse og know-how om digitalisering og nye teknologier, og et faglig samarbeid utover enkeltprosjekt og installasjoner vil være verdifullt for selskapene. Vi ser også at noen aktører har formalisert samarbeid, bl.a. om utvikling av en OPC-UA informasjonsmodell. Dette er et spesielt relevant samarbeid for å understøtte behovet for utveksling av data som forutsetter en viss grad av standardisering og som vil redusere skreddersydde en-til-en løsninger.

3.5 Interoperabilitet

Trenden er tydelig økt interoperabilitet mellom systemer i OT-laget, mellom OT og IT, og videre mot løsninger basert på skyteknologi. Det finnes et utall løsninger og teknologier i eksisterende anlegg hvor kompleksiteten synes å øke i form av utbedringer i eksisterende anlegg og ikke minst i form av nye løsninger og tjenester. I tillegg er det rimelig å forvente at denne trenden fortsetter for å utnytte potensialet i dataintensive løsninger for mer effektiv drift og utvinning. Dette betyr at det blir mange teknologier og forholde seg til og ikke minst mange systemer fra mange etablerte og nye leverandører. Det er et behov for en omforent arkitektur og en standardisering på interoperabilitet som balanserer åpenhet/integrasjon og IKT-sikkerhet.

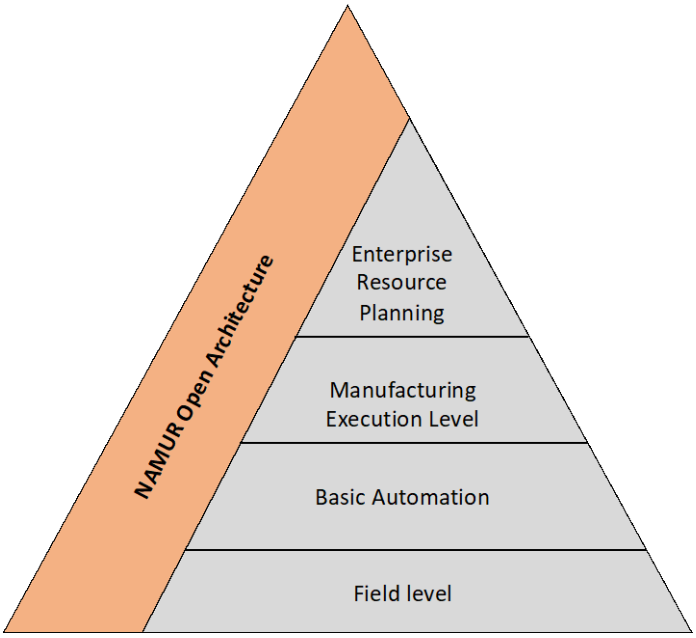
OPC Unified Architecture - OPC-UA (IEC 62541 [41]) er allerede identifisert av noen selskapene og virker å være en satsning i bransjen, både i Norge men også internasjonalt for prosess-automatisering.

Open Process Automation (OPA) er et industrisamarbeid for å definere en standard (O-PAS) for en åpen, sikker og interoperabel automasjonsarkitektur [42]. Denne omfatter blant annet 'O-PAS Connectivity Framework' (OCF), hvor OPC UA benyttes for å definere *grensesnitt* mellom ulike programvarebaserte eller dataproduserende system. OPA har gjennomført en vurdering av ulike alternativer hvor det spesielt er lagt vekt på følgende kvaliteter: 1) interoperabilitet, 2) cyber-sikkerhet, 3) portabilitet, 4) tilgjengelighet, og 5) gjenfinnbarhet (discoverability). Følgende tre hovedbegrunnelser ligger bak valget av OPC UA:

- Har allerede omfattende støtte fra leverandører av industrielle kontrollsystemer
- Støtter Open Groups utviklingsprosess
- Støtter de prioriterte kvalitetene (nevnt over)

Dette er per i dag (2020) [42] en standard under utvikling hvor det er spesielt viktig å vurdere spesielt ytelse (throughput) og cyber-sikkerhet. Det vil også være en forutsetning at dette faktisk blir adoptert som en bransjestandard, både på systemeiersiden og på leverandørsiden. På den positive siden er det verdt å merke seg at denne utviklingen er basert på et svært omfattende samarbeid mellom de ledende teknologiaktørene i bransjen og ikke minst en rekke andre standardiseringsprosesser og initiativ, bla. ISA-95, OMAC, Indistrie 4.0 m.fl.

NAMUR Open Architecture (NOA) [40] er en arkitekturmodell basert på prinsippet om at systemer (OT og IT) integreres *på siden* av eksisterende arkitektur (etablert iht. IEC 62443). OPC UA er kjerne-standarden i NOA for dataoverføring. NOA skal ivareta krav til IKT-sikkerhet og baseres på prinsippet om retningskontroll på data (data direction control) hvor alle system skal følge security-by-design prinsippet i IEC 62443.



Figur 6 NAMUR Open Architecture

Som nevnt, næringen jobber med dette og NAMUR OA, OPC-UA, og IEC 62443 kan samlet være en riktig satsning for å dekke behovet for integrasjon, fleksibilitet/åpenhet, IKT-sikkerhet, og en koordinert og standardisert innsats. Dette er imidlertid standarder som er *i utvikling* og hvor det er et stort behov for kompetansebygging, deltakelse i standardiseringsarbeid, utprøving for å bygge erfaring, og ikke minst en grundig vurdering av hvorvidt krav til IKT-sikkerhet og sikkerhets-systemenes uavhengighet ivaretas, bl.a. iht. Ptils forskrifter.

3.6 Digitalisering i et MTO-perspektiv

Digitaliseringsprosesser skaper naturlig nok et stort fokus på teknologi men det er da også relevant å forstå hvordan nye digitale tjenester påvirker menneskene og deres oppgaver og ansvar. Selv om tekniske sikkerhetsbarrierer er viktige og selv om nye dataintensive løsninger vil kunne bidra til bedre sikkerhet vil mennesket fortsatt spille en viktig rolle. Vi ser en utvikling hvor teknologi forenkler, støtter eller delvis erstatter operatøren eller deler av operatørens oppgaver og ansvar. Dette kan være ekspertsystemer, bedre tilgang på

informasjon, digitale tvillinger, eller andre løsninger. Men hvordan påvirker dette operatøren over tid, og ikke minst hans/hennes evne til å påvirke i kritiske situasjoner? Dersom en operatør med ekspertise og lang erfaring over tid passiviseres og lar støttesystemene «gjøre jobben» er det grunn til å anta at operatøren erfaring og rolle svekkes. På den annen side blir noen operasjoner mer komplekse og avanserte og krever mer av operatøren. Rolle, ansvar, og samspill med ny teknologi er i utvikling.

Det er viktig å vedlikeholde et perspektiv på menneske-teknologi-organisasjon (MTO) og planlegge med tiltak som kan redusere denne type konsekvenser av digitaliseringsprosesser. Trening og kompetansebygging (for eksempel ved hjelp av simulatorer) er naturlige forslag, men det kan være grunn til å tro at dette er underfokusert. Se rapporten 'Automatisering og autonome systemer: Menneskesentrert design' [43].

4 Anbefalinger

I dette kapitlet oppsummeres SINTEFs anbefalinger til tiltak for næringen og Petroleumstilsynet, samt behov for videre arbeid med kunnskapsinnhenting.

4.1 Næringen

Anbefalinger til tiltak for næringen er gitt i tabell 1.

Tabell 1 Oppsummering av SINTEFs anbefalinger til tiltak for næringen

Nr.	Utfordring	Anbefaling
1a	Næringen, inkludert leverandørene har et stort *felles* kompetansebehov som spenner vidt; digitalisering som trend generelt, teknologi, informasjonssikkerhet i sammenkoblingen mellom OT og IT, inkludert skyløsninger. Kompetansen er ulikt fordelt, hvor de største aktørene har størst kapasitet mens de mindre aktørene i større grad må støtte seg på andre, bl.a. leverandørenes kompetanse (som også varierer i stor grad).	Videreføre pågående kompetansebygging, men i enda større grad som en koordinert innsats i næringen. Det er viktig for næringen som helhet at de store aktørene tar et ansvar og viser vilje til å inkludere de mindre og å dele kompetanse.
1b		Utnytte og utvikle felles læringsarenaer. CDS-forum nevnes som en av de viktigste i Norge, men det er også viktig å investere nok ressurser i å følge utviklingen i andre land, i andre næringer (kritisk infrastruktur), og den internasjonale forskningen.
2	Det er et behov for standardisering som spenner fra arkitektur (som inkluderer digitale tjenester), modeller for interoperabilitet, og informasjons-sikkerhet i stadig mer koplede (OT) systemer.	Følge opp, og bidra, utviklingen av IEC62443-serien – som fremstår som den mest relevante for informasjonssikkerhet i næringen. Tilsvarende bør næringen også følge og, hvis mulig, bidra i utvikling av felles referansearkitektur som eksempelvis NAMUR Open Architecture og OPC UA.
3	Næringen opplever NOG104 som utdatert, men henviser likevel fortsatt til denne.	Næringen bør enten henvise til andre og mer oppdaterte standarder (ref. anbefaling #2), eller bidra til at NOG104 oppdateres og da involvere Ptil (veiledningen til Innretningsforskriften §34a henviser til NOG104).
4	Det er og har lenge vært et tydelig fokus på informasjonssikkerhet i bransjen, men med fokus på *sikring* av data (lagring, tilgang, overføring, brannmurer, DMZ, virus, hacking, etc.), men det er et underfokus på data *kvalitet* og data *integritet*. Kvaliteten på dataintensive digitale tjenester, for eksempel tvillinger/modeller, avhenger *direkte* av kvalitet på data. Dersom utviklingen nå går mot tettere integrasjon av digitale (dataintensive) tjenester og OT så blir data*kvalitet* like styrende for sikkerhet(safety) som data*sikkerhet* (security).	Næringen bør sette et tydelig, og gjerne felles, fokus på datakvalitet. Dette omfatter strategi og løsninger for bl.a. konsolidering, vasking, kvalitetskontroll, feilkorreksjon, etc. På samme vis som næringen ser mot utviklingen av IEC62443-serien for cybersecurity bør den også vurdere å følge utviklingen av tilsvarende standard-initiativ for data kvalitet, samt forskning på dette feltet. Relevante standarder og retningslinjer kan være ISWG Data Safety Guidance Version 3.2 [44], ISO 8000 *Data Quality [45],* og DNVGL-RP-0497 *Data quality assessment framework* [46].
5	Leverandørbildet endrer seg med flere leverandører som tilbyr digitale dataintensive *tjenester*. Dette omfatter både etablerte leverandører, for eksempel SAS-leverandørene, men også helt nye aktører. Slike leverandører avhenger av tilgang på data, også fra OT, og hvor tilgang på data skaper stor forretningsverdi. Næringen er så langt relativt umoden i dette forholdet, for eksempel i forhold til	Næringen bør utvikle en bedre forståelse av sin rolle som dataeier og hvilke krav som må stilles til leverandører som samler data. Eierskap til data bør reflekteres i krav og kontrakter, og i selskapenes oppfølging i drift.

Nr.	Utfordring	Anbefaling
	avklaringer om eierskap til data, krav om lagring over tid, og kontroll på hvordan data som flyttes ut til eksterne brukes og håndteres.	
6	Digitalisering kan skape nye utfordringer for informasjonssikkerhet som ikke nødvendigvis dekkes av eksisterende teknologi, lagdelt arkitektur, rutiner, og kompetanse. En økende grad av dataflyt fra OT-lag til IT-lag i eksisterende infrastruktur kan skape utfordringer, både ift. ytelse og økt angrepsflate. Samtidig kan eventuelle sidekanaler (direkte fra OT til eksterne system) skape nye informasjonssikkerhets-utfordringer.	Næringen bør utvikle en bedre forståelse av hvordan digitale tjenester utfordrer eksisterende arkitektur: 1) Nye transportveier for data, 2) omfang av dataflyt, kapasitet og ytelse, 3) mulige nye angrepsflater, inkludert direkte kanaler OT-IT. Det må etableres tilstrekkelig informasjonssikkerhet og oppfølging av leverandører hvor eksisterende systemer og prinsipper ikke er tilstrekkelige.
7	Pågående digitalisering ser ut til å drives først og fremst av effektiviseringsmål hvor potensialet for økt sikkerhet (safety) har mindre fokus.	Næringen bør øke fokus på hvordan tilgang på digitale tjenester basert på mer data, med bedre kvalitet og økt prosesserings-kapasitet kan utnyttes for å styrke sikkerheten på installasjoner og i operasjoner.

4.2 Ptil

Anbefalinger til Petroleumstilsynet er gitt i tabell 2. Anbefalingene er basert på informasjon som er samlet inn fra selskapene og analysen som er gjort (denne rapporten). Enkelte av innspillene uttrykker ønsker fra næringen som ikke naturlig faller inn under Ptils funksjon og ansvarsområde. Næringen opplever pågående digitalisering som utfordrende spesielt med hensyn på IKT-sikkerhet i OT-systemer som kobles med IT-systemer. Generelt uttrykkes det et ønske om mer direkte og spesifikke krav fra Ptil, men hvor Ptils funksjon og ansvar avgrenser graden av detaljstyring. Anbefalingene er tilpasset deretter.

Tabell 2 Oppsummering av SINTEFs anbefalinger til tiltak for Ptil

Nr.	Utfordring	Anbefaling
1a	Næringen etterlyser tydelige føringer på cybersikkerhet og safety fra Ptil. Det er i dag stor uklarhet rundt hvordan cybersikkerhet skal håndteres når OT i voksende grad påvirkes av digitaliseringstiltak og det etableres i dag mange ulike tiltak i selskapene. Næringen opplever Ptil og NSM som for lite oppdaterte på utviklingen. Kundene har frem til nå vært en større pådriver for cybersikkerhet enn Ptil.	På overordnet nivå bør Ptil ta et større ansvar i føringer for cybersikkerhet med spesiell fokus på digitaliseringsløsninger som berører OT-laget.
1b		Det bør gis føringer utover skallsikring siden etablerte prinsipper om sikring av lag/funksjonsområder utfordres av nye digitale løsninger og dermed nye koblinger mellom OT og IT/sky.
1c		Ptil investerer i videre utvikling av egen kompetanse på digitalisering generelt, og med spesiell fokus på teknologi og leverandører som er aktuell for næringen.
2	Næringen ønsker tydeligere føringer på IKT-sikkerhet fra Ptil. Dette skaper legitimitet og mandat i egen organisasjon og ovenfor leverandører og samarbeidspartnere – og derigjennom en bedre evne til kontroll over utviklingen.	Ptils bør være synlige i diskusjonen rundt utfordringer, teknologivalg, trender, og hvordan Ptils forskrifter forstås og kan overholdes.
3a	Næringen henviser selv til IEC62443 og NOG104 som de mest relevante standardene, men førstnevnte oppleves som uferdig og sistnevnte som utdatert (i	Ptil støtter næringen i utarbeidelsen av IEC62443 og klargjøringer av hvordan denne standarden skal anvendes for næringen.

Nr.	Utfordring	Anbefaling
3b	forhold til digitalisering og OT). Gjeldende revisjon 06 ble sist gjort i 2016).	Veiledningen til Innretningsforskriften §34a henviser til NOG104. Ptil bør vurdere å oppdaterte veiledningen med relevant standard (f.eks. DNVGL-RP-G108) eller bidra til at NOG104 oppdateres.
4	Næringen opplever utviklingen (digitalisering) som «kaotisk» og drevet av svært store målsettinger med et stort potensiale, men med en kompleksitet som er utfordrende. Alle aktører adresserer utfordringer knyttet til nye cybersikkerhets-utfordringer (OT) men på svært ulikt vis og med stor variasjon i modenhet. Næringen etterlyser selv en felles referanse-arkitektur for næringen. Dette vil styrke samarbeidet internt i næringen og mot leverandørsiden som i voksende grad også består av digitale tjenesteleverandører.	Ptil bør bidra, utfra sin rolle, til at det etableres en omforent referansearkitektur for næringen. NAMUR Open Architecture blir nevnt som en mulig relevant felles modell. (Andre modeller kan også være relevante. Det er ikke gjort en omfattende analyse av dette i forbindelse med oppdraget – denne anbefalingen er så langt utelukkende basert på innspill fra næringen selv.)
5	I sammenheng med ovenstående punkt, så er det også et behov for en omforent standard/protokoll for interoperabilitet mellom systemer internt, mot samarbeidspartnere, og leverandører.	Ptil bør bidra til at det etableres en omforent standard for interoperabilitet. OPC UA blir nevnt som en mulig felles modell. (Andre modeller kan også være relevante (det er ikke gjort en omfattende analyse av dette i forbindelse med oppdraget – denne anbefalingen er så langt utelukkende basert på innspill fra næringen selv.)
6	Produksjon og boring fremstår ulikt, hvor sistnevnte har operert friere i forhold til digitalisering.	Ptil bør samkjøre føringer og oppfølging i større grad likt mot produksjonsselskap og boreselskap. Mulighetene og utfordringene de jobber med (ift. OT-rettet digitalisering) er i prinsippet like.

4.3 Behov for kunnskapsinnhenting

Formålet med denne rapporten har vært å gi næringen økt forståelse for hva som er premissene for digitalisering. Dette omfatter en kort oversikt over konseptet digitalisering, hva som er erfaring og status så langt, og hvilke tiltak som vil føre næringen videre.

Den største utfordringen per i dag er kompleksiteten som følger en allerede fullt pågående digitalisering i næringen. Det er krevende å se helheten siden det nå pågår en endring som påvirker eksisterende systemer fra lavt (OT) til høyt (IT) nivå, både på organisatorisk og teknisk nivå, og på tvers av selskaper og leverandører. Dette skaper behov for ny kunnskap:

1. Det er et generelt behov for å bygge kompetanse i næringen, både hos selskapene som brukere av og premissgivere for teknologi, og for leverandørene som skal oppfylle krav fra både kunder og myndigheter. I første omgang er det behov for å ytterligere forstå implikasjonene av digitaliseringen i næringen bedre og da både organisatoriske og tekniske aspekter. Utviklingen i dag er uoversiktlig med mange aktører, tiltak, teknologier og nye standarder som er i utvikling, hvor spesielt IEC62443 serien anses som relevant av næringen selv. Det er behov for å forstå balansen mellom muligheter og begrensninger samt utvikle kompetanse om selskapenes muligheter og ansvar for å kontrollere og følge opp leverandørene.
2. Aktørene i næringen deler mange av *de samme* utfordringene rundt økende integrasjon mellom OT og IT – inkludert skyløsninger. Det er derfor behov for en *felles innsats*, eller i det minste, en konsolidering mot en referansearkitektur og felles konsepter for interoperabilitet – utover eksisterende lagdelte modeller (Purdue) som vi ser blir utfordret av økt dataflyt og nye digitale tjenester, både på kapasitet/ytelse og på informasjonssikkerhet. NAMUR OA og OPC UA peker seg ut som en felles satsning som kan dekke

behovene både i etablerte og nye installasjoner. Her vil det være behov for ny kunnskap om anvendelser og tilpasninger.

3. Datakvalitet er direkte koblet til effektivitet og sikkerhet (safety) dersom digitale tjenester påvirker OT. Det er behov for økt kunnskap om aggregering, konsolidering, vasking, kvalitetssikring, og bruk av data i verdiøkende digitale tjenester. Herunder kommer også kunnskap om eierskap og forvaltning av data, og fordeling av ansvar mellom selskap og tjenesteleverandører. Basert på dette er det behov for kunnskap om hvordan datakvalitet sikres i krav til leverandører og i kontrakter. (Se for øvrig egen rapport om datakvalitet ved digitalisering i petroleumssektoren [21]).
4. AI og ML er en klasse teknologi med et stort potensiale i anvendelser hvor det er behov for å analysere store datamengder og er dermed relevant for næringen hvor tilfang på data øker kraftig og med en tydelig satsning på digitalisering. AI regnes som en av de sentrale 'digitaliseringsteknologiene' i tillegg til bl.a. Big Data, Cloud, og IIoT, men det er så langt lite kunnskap om potensialet og ikke minst hva som er muligheter og begrensninger i forhold til dagens forskrifter. Spesielt er temaet 'Explainable AI' (XAI) et kunnskapsfelt hvor det er behov for økt fokus, spesielt i forhold til sikkerhetskritiske system.
5. Tilkoplede programvaresystemer muliggjør DevOps-modeller for integrert utvikling og drift hvor bl.a. informasjons-sikkerhetshull i utgangspunktet kan oppdages og korrigeres raskere. Dette er derimot en svært utfordrende modell for systemer med store krav til oppetid, tilgjengelighet, og uavhengighet. Det er dermed behov for ny kunnskap om muligheter og begrensninger.

Referanser

[1] OG21, Technologies for cost and energy efficiency (Final Report), 2019.

[2] Digital 21, Digitale grep for norsk verdiskaping, 2018.

[3] P. Mell and T. Grance, The NIST definition of cloud computing, 2011.

[4] Petroleumstilsynet. Fagstoff, Ord og uttrykk. https://www.ptil.no/fagstoff/ord-og-uttrykk/ (nedlastet 14.11.2020)

[5] L. Bodsberg, Grøtan, T.O., Jaatun, M.G,. Wærø, I., IKT-sikkerhet – Fjernarbeid og HMS, SINTEF2019, SINTEF rapport 2019:00361, sluttrapport-ptil-ikt-sikkerhet---fjernarbeid-og-hms-med-underskrift-og-vedlegg.pdf. (nedlastet 31.10.2020)

[6] Departementene, Nasjonal strategi for digital sikkerhet, 2019. :https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhet/id2627177 (nedlastet 31.10.2020)

[7] Digital Norway, Hva er en digital tvilling? https://digitalnorway.com/lessons/hva-er-en-digital-tvilling/ (nedlastet 19.11.2020)

[8] L, Bodsberg, Hale, B., Dahl, Ø., Grøtan, T.O., Jaatun, M.G., Moe, M. Onshus, T., Kunnskapsprosjekt IKT-sikkerhet; Industrielle kontroll- og sikkerhetssystemer i petroleumsvirksomheten, SINTEF rapport 2018:00572, 2018, https://www.ptil.no/contentassets/d67ffa5187c846fe9a074d1e68f2ce1c/kunnskapsprosjekt-ikt-sikkerhet-sluttrapport-med-underskrift.pdf. (nedlastet 31.10.2020)

[9] NOU 2015:13, Digital sårbarhet – sikkert samfunn. Departementenes sikkerhets- og serviceorganisasjon, 2015, https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/.

[10] Digital Norway, Hva er egentlig IoT?, https://digitalnorway.com/topic/hva-er-iot-definisjon/ (nedlastet 19.11.2020)

[11] Petroleumstilsynet, Veiledning til rammeforskriften, 2019, https://www.ptil.no/contentassets/332166193108427e978accb21449436c/rammeforskriften20_veiledning_n.pdf, (nedlastet 14.11.2020)

[12] NS 5814:2008. Krav til risikovurderinger, 2008.

[13] NS 5832:2014. Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger - Krav til sikringsrisikoanalyse, 2014.

[14] Society of Risk Analysis, Society for Risk Analysis Glossary, 2018. https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf (nedlastet 31.10.2020)

[15] S. O. Johnsen, Lundteigen, M. A., Albrechtsen, E., Grøtan, T. O., Trusler og muligheter knyttet til eDrift, SINTEF rapport nr STF38 A04433, 2005.

[16] H. Lu, L. Guo, M. Azimi, and K. Huang, Oil and Gas 4.0 era: A systematic review and outlook, *Computers in Industry*, vol. 111, pp. 68-90, 2019.

[17] M. V. Ottermo, T. Onshus, and K. S. Bjørkevoll, Bruk av modeller i boring, SINTEF rapport 2021:00056, 2021.

[18] W. Knight, *The Dark Secret at the Heart of AI*, 2017 https://www.technologyreview.com/2017/04/11/5113/the-dark-secret-at-the-heart-of-ai/ (nedlastet 20.11.2020)

[19] T. Meling, T. Bjarke, G. Veire, T. Bok, Johan Sverdrup: Lessons-Learned from the Field-Development of a North Sea Giant, *Offshore Technology*, 2020.

[20] P. Larsen, T. Tønnessen, F. Schuchert, Johan Sverdrup: The Digital Flagship," *Offshore Technology*, 2020.

[21] T. Myklebust, T. Onshus, S. Lindskog, and M. V. Ottermo, Datakvalitet ved digitalisering i petroleumssektoren, SINTEF Raport nr STF 2021:00053, 2021.

[22] P. B. Kristoffersen, O. Haugenhåtveit, and K. Omberg, Infrastruktur innen industrielle kontroll- og sikkerhetssystemer, DNV GL CyberSecurity/J-24/25154785/DNV, Rev. 1.1, 2019.

[23] J. S. Brekke, Machine learning effects on the norwegian oil and gas industry, MSc, Universidade Católica Portuguesa, 2020.

[24] A. Gezdur and J. Bhattacharjya, Digitization in the Oil and Gas Industry: Challenges and Opportunities for Supply Chain Partners, *Working Conference on Virtual Enterprises*, 2017.
[25] E. Grange, A Roadmap for Adopting a Digital Lifecycle Approach to Offshore Oil and Gas Production, *Offshore Technology Conference*, 2018.
[26] L. J. Gressgård, K. Melberg, M. Risdal, J. T. Selvik, and R. Ø. Skotnes, Digitalisering i petroleumsnæringen, International Research Institute of Stavanger AS2018.
[27] T. Kruger and E. Marotta, Big Data and Digital Transformation Summary… Three 3 Years of Panel Discussions, *Offshore Technology Conference*, 2020.
[28] E. Knutsen and M. Ileby, Harnessing data effectively to develop a low-manned platform in a remote, North Sea operating environment, *Offshore Technology Conference*, 2018.
[29] T. Nguyen, R. Gosine, and P. Warrian, A Systematic Review of Big Data Analytics for Oil and Gas Industry 4.0, *IEEE Access*, 2020.
[30] H. Devold, T. Graven, and S. Halvorsrød, Digitalization of Oil and Gas Facilities Reduce Cost and Improve Maintenance Operations, *Offshore Technology*, 2017.
[31] F. Laborie, O. Røed, G. Engdahl, and A. Camp, Extracting value from data using an industrial data platform to provide a foundational digital twin, *Offshore Technology*, 2019.
[32] S. Ertenstein and S. Løfgren, Risikovurderinger i forbindelse med outsourcing av informasjons-og kommunikasjonsteknologi (IKT) i petroleumssektoren. uis.brage.unit.no, 2018.
[33] L. Muller, L. Gjesvik, and K. Friis, Cyber-weapons in International Politics: Possible sabotage against the Norwegian petroleum sector (NUPI Report). nupi.brage.unit.no, 2018.
[34] T. Wanasinghe, R. Gosine, L. James, The Internet of Things in the Oil and Gas Industry: A Systematic Review," *IEEE Internet of Things*, 2020.
[35] J. Røstum, Jaatun, M.G., Informasjonssikkerhet og skybaserte tjenester for vannbransjen, 2018, https://norskvann.no/index.php/kompetanse/va-bokhandelen/produkt/681-a238-informasjonssikkerhet-og-skybaserte-tjenester-for-vannbransjen. (nedlastet 31.10.2020)
[36] C. Frøystad, M. G. Jaatun, K. Bernsmed, and M. Moe, Risiko-og sårbarhetsanalyse for økt integrasjon av AMS-DMS-SCADA, Norges vassdrags- og energidirektorat. Rapport nr.: 8241017898, 2018, http://publikasjoner.nve.no/eksternrapport/2018/eksternrapport2018_15.pdf. (nedlastet 31.10.2020)
[37] A. Cherepanov, WIN32/INDUSTROYER: A new threat for industrial control systems, White paper, *ESET (June 2017)*, 2017.
[38] Equinor. Our digital vision, 2020 https://www.equinor.com/en/how-and-why/digitalisation-in-our-dna.html (nedlastet 14.11.2020)
[39] P. Abrahamsson *et al.*, Towards a Secure devops Approach for Cyber-Physical Systems: An Industrial Perspective, *International Journal of Systems and Software Security and Protection (IJSSSP)*, vol. 11, no. 2, pp. 38-57, 2020.
[40] NAMUR, NE 175 NAMUR Open Architecture – NOA Concept, 2020.
[41] I. E. Commission, IEC TR 62541-1: 2016-OPC unified architecture-Part 1: Overview and concepts, IEC, Geneva, CH, Technical Report, 2016.
[42] OPC UA Users and Experts – Conveying Knowledge and Experience: Automation.com, 2020. https://www.automation.com/en-us/products/forms/ebook-opc-technology-specifications-solutions-volu. (nedlastet 31.10.2020)
[43] S. O. Johnsen, Holen, S., Aalberg, A.L., Bjørkevoll, K.S., Evjemo, T.E., Johansen, G., Myklebust, T., Okstad, E., Pavlov, A., Porathe, T., "Automatisering og autonome systemer: Menneskesentrert design," SINTEF, 2021:01442, 2021.
[44] Safety-Critical Systems Club, Data Safety Guidance Version 3.2, 2020, https://scsc.uk/publication (nedlastet 31.10.2020)
[45] ISO/TS 8000-1:2011 Data Quality, 2011.
[46] DNVGL-RP-0497 Data quality assessment framework, 2017.

Vedlegg A: Litteratursøk

Det er gjort et søk etter forskningslitteratur for å identifisere relevante publikasjoner som omhandler digitalisering som involverer noen av de sentrale aktørene på norsk sokkel og med tematikk som er relevant for denne rapporten. Hensikten har vært å gjøre en screening av forskningslitteraturen og gi et overblikk over hva som er fokuset i det som er formidlet Vi har benyttet Google Scholar som dekker et bredt spekter av konferanser, workshops og journaler.

Følgende søkestreng ble brukt for å avgrense søket:

- Alle ord: *digitalization oil safety*
- Og minst ett av følgende ord: *statoil equinor lundin akerb "aker bp"*

Det ble ikke definert et tidsrom for søket for å unngå å ekskludere publikasjoner som er feilregistrert eller mangler årstall.

Målet med søkestrengen er å identifisere publikasjoner som:

- Omhandler digitalisering relatert til olje og gassbransjen i Norge, gjerne med empiri eller eksempler fra relevante aktører
- Omhandler digitalisering relatert til tematikken i rapporten
- Gir innsikt i identifiserte problemstillinger

Dette søket ga 560 publikasjoner. For å finne relevant materiale er det gjort en trinnvis ekskludering av irrelevante publikasjoner:

Trinn	Ekskluderingskriterier	Ekskludert	Gjenstående
1. Søk			560
2. Tittel	- Tittel åpenbart irrelevant - Duplikater - Ikke engelsk eller norsk - Bøker eller samlinger	450	110
3. Abtract	- Publikasjonen er utenfor scope	84	26
4. Fulltekst	- Publikasjonen er utenfor scope - Fulltekst er ikke åpent tilgjengelig	13	13

Teknologi for et bedre samfunn

www.sintef.no