

Rapport etter kartlegging av operatørselskapenes oppfølging av KI

Rapport	
Kartlegging av operatørselskapenes oppfølging av KI	Aktivitetsnummer 9921396
	Saksnummer 2026/478

Gradering	
☒ Offentlig	☐ Unntatt offentlighet

Involverte	
Hovedgruppe Prosessintegritet	Oppgaveleder Linn Iren Vestly Bergh
Deltakere fra Havtil Linn Iren Vestly Bergh, Arne Halvor Embergsrud, Elisabeth Lootz	Dato

Innhold

1	Sammendrag.....	3
2	Formål.....	4
3	Bakgrunn og omfang	4
4	Metode og datagrunnlag.....	5
5	Oppsummering av resultater	5
	5.1 HMS-mål for utvikling og bruk av KI.....	6
	5.2 Bruk av standarder og rammeverk.....	6
	5.3 Oversikt over KI-systemer	7
	5.4 Utvikling og bruk – aktiviteter og type KI-systemer	9
	5.5 Krav til utvikling, bruk og oppfølging av leverandører	11
	5.6 Arbeidstakermedvirkning og kompetanse	12
	5.7 Hendelses- og avviksrapportering for KI	12
	5.8 Risikostyring av KI	13
	5.9 Roller og ansvar for oppfølging av KI.....	14
	5.10 Tverrfaglige perspektiver	14
	5.11 KI-forordningen	15
6	KI, sikkerhetsforståelse og modenhet i risikostyringen	15
	6.1 Ulik modenhet i sikkerhetsforståelse	16
	6.2 Generativ KI, KI-agenter og nye styringsutfordringer	16
	6.3 HMS-regelverket og betydning for sikkerheten	17
7	Vedlegg 1	18
	Figur 1: Oversikt over KI-systemer.....	7
	Figur 2: Interne krav til KI.....	11
	Figur 3: Hendelses- og avvikssystem for KI.....	13

1 Sammendrag

Denne rapporten presenterer resultater fra Havtils kartlegging av hvordan operatørselskapene anskaffer, utvikler, bruker og følger opp KI-systemer med betydning for sikkerheten.

Denne aktiviteten er en del av Havtils arbeid med oppfølgingen av KI i petroleumsnæringen.

Kartleggingen indikerer at næringens bevissthet om styring av KI-risiko har økt siden Havtil innledet dialogen med selskapene om hvordan slik risiko følges opp. Samtidig viser funnene at det fortsatt er behov for forbedring, særlig når det gjelder oversikt over KI-systemer, livsløpsbasert risikostyring, leverandøroppfølging og tydeligere vurderinger av hvordan KI kan få betydning for sikkerheten.

Selskapenes svar viser følgende hovedfunn:

- **HMS-mål for utvikling og bruk av KI:** Basert på selskapenes egne opplysninger har majoriteten ikke etablert egne HMS-mål for KI, og ingen av selskapene oppgir eller dokumenterer at de har etablert HMS-mål på prosjektnivå.
- **Bruk av standarder og rammeverk:** Selskapene oppgir at KI-spesifikke standarder og rammeverk i begrenset grad er tatt i bruk. Noen opplyser samtidig at de vurderer relevante standarder, og at de deltar i standardiseringsarbeid på området.
- **Oversikt over KI-systemer:** Selskapenes svar viser ulik modenhet når det gjelder å identifisere og registrere KI-systemer under utvikling og i bruk. Over halvparten oppgir at de ikke har, eller ikke kan dokumentere, en fullstendig oversikt over slike systemer.
- **Utvikling og bruk – aktiviteter og type KI-systemer:** Selskapene oppgir at KI brukes, eller vurderes brukt, i blant annet brønnplanlegging, boring, kranoperasjoner, vedlikehold, overvåking, inspeksjon og beslutningsstøtte. Systemene som beskrives omfatter blant annet prediktive KI-systemer, generativ KI og agentbaserte KI-systemer.
- **Krav til utvikling, bruk og oppfølging av leverandører:** Selskapene oppgir i varierende grad å ha etablert egne interne KI-krav og krav til leverandører. Svarene indikerer at manglende interne krav henger sammen med manglende KI-spesifikke krav til leverandører.
- **Arbeidstakermedvirkning og kompetanse:** Flere selskaper oppgir i de fleste tilfeller ikke konkrete krav til arbeidstakermedvirkning i KI- og digitaliseringsprosjekter. Samtidig opplyser flere at de tilbyr generell KI-opplæring, og enkelte oppgir å ha etablert roller som KI-verneombud eller datatillitsvalgt.
- **Hendelses- og avviksrapporting for KI:** Selskapene oppgir i hovedsak at KI-relaterte hendelser håndteres gjennom eksisterende HMS- eller IT-systemer. Et mindretall opplyser at de har egne KI-tilpassede mekanismer.
- **Risikostyring av KI – integrering, roller og ansvar:** Alle selskapene beskriver KI-risiko som en del av eksisterende risikostyring, men det er uklart hvor langt risikostyringen følger et livsløpsperspektiv, og hvor tydelig ansvar og roller er definert.
- **Tverrfaglige perspektiver:** Selskapenes svar viser at tverrfaglighet anerkjennes som viktig, men at konkrete krav til involvering varierer.

- **KI-forordningen:** Selskapene oppgir å ha vurdert konsekvensene av KI-forordningen i ulik grad. Flere opplyser at de arbeider med gapanalyser og risikobasert kategorisering, men vurderingene som er beskrevet i svarene, fremstår ofte overordnede.

Samlet vurderer Havtil at det er behov for videre oppfølging av hvordan selskapene etablerer oversikt, ansvar, krav og risikostyringsprosesser for KI-systemer med betydning for sikkerheten.

Særlig viktig blir det å følge opp livsløpsbasert risikostyring, leverandørstyring, hendelsesrapportering, kontinuerlig læring og tverrfaglig involvering. I denne rapporten har vi gjort noen vurderinger knyttet til funn basert på selskapenes svar opp mot HMS-regelverket.

2 Formål

Formålet med aktiviteten var å kartlegge hvordan operatørselskapene i næringen anskaffet, utviklet og brukte kunstig intelligens (KI). Kartleggingen skulle gi oversikt over bruk av KI i ulike planleggings- og operasjonsaktiviteter, samt hvordan KI inngikk i utstyr på selskapenes innretninger og landanlegg. Dette inkluderte hvordan selskapene arbeidet med risikostyring og kvalifisering knyttet til utvikling og bruk av KI-systemer med betydning for sikkerheten.

Denne aktiviteten er en del av Havtils arbeid med oppfølgingen av KI i petroleumsnæringen. Sektoroppgaven i 2026 bygget videre på veiledningsbrevet om KI og sikkerhet som Havtil sendte ut til næringen i mai 2025, og som ble publisert på www.havtil.no.

Denne aktiviteten skal bidra til å:

- Fremme ansvarlig utvikling og bruk av KI i en industriell kontekst.
- Gi økt kunnskap om hvilke helse-, miljø- og sikkerhetsmål (HMS-mål) selskapene har etablert for å sikre forsvarlig bruk av KI.
- Innhente oversikt over KI-systemer som er i bruk og under utvikling i selskapenes virksomhet.
- Innhente informasjon om selskapenes tilnærminger og prosesser for oppfølging av KI, herunder interne krav, risikostyring og bruk av standarder.

3 Bakgrunn og omfang

Bruken av KI øker raskt i petroleumsvirksomheten og inngår i stadig flere aktiviteter knyttet til planlegging, drift og vedlikehold. Porteføljen selskapene beskriver, omfatter blant annet sensorbasert KI, maskinsyn, generativ KI og agentbaserte KI-systemer.

Teknologien gir muligheter for bedre beslutningsstøtte, mer effektiv ressursutnyttelse og forbedret risikostyring. Samtidig introduserer KI nye former for usikkerhet, sårbarhet og risiko. Dette er særlig viktig i en storulykkeutsatt næring der teknologiske løsninger kan påvirke operasjoner, beslutninger og barrierer med betydning for sikkerheten.

Gjennom oppfølging av næringen ser vi at det er ulik modenhet når det gjelder risikostyring og kvalifisering av digitale teknologier, inkludert KI. HMS-regelverket har en risikobasert tilnærming der nødvendig risikoreduksjon og et forsvarlig sikkerhetsnivå er en forutsetning for aktiviteten. Virksomhetene har ansvaret for sikkerheten. Dette ansvaret inkluderer også forsvarlig bruk av KI.

Med økende bruk av KI-systemer ser Havtil behov for å styrke oppfølgingen av selskapenes risikostyring knyttet til anskaffelse, utvikling og bruk av KI. Særlig vektlegges forsvarlig bruk av KI i petroleumsvirksomheten som storulykkesindustri.

Havtil anvender begrepet *KI-systemer med betydning for sikkerheten* for å tydeliggjøre at slike systemer kan ha sikkerhetsmessig betydning i en rekke aktiviteter, og ikke bare når de brukes direkte i operasjoner til havs eller på landanlegg.

4 Metode og datagrunnlag

Kartleggingen ble gjennomført ved at operatørselskaper på norsk sokkel mottok et varselbrev med tolv spørsmål om utvikling, anskaffelse, bruk og styring av KI-systemer. Til sammen ble spørsmålene sendt til ni operatørselskaper.

Spørsmålene var utformet for å belyse sentrale elementer innen risikostyring av KI, herunder HMS-mål, virksomhetenes oversikt over KI-systemer, roller og ansvar, bruk av standarder og involvering av arbeidstakere. Spørsmålene omfattet blant annet hvordan selskapene identifiserer og registrerer KI-systemer, hvilke typer KI-modeller som benyttes, hvilke aktiviteter og operasjoner teknologien inngår i, hvordan arbeidstakermedvirkning ivaretas, og hvordan hendelser og avvik relatert til KI håndteres.

Temaene ble valgt fordi de representerer sentrale forutsetninger for ansvarlig utvikling og bruk av KI i storulykkeindustrier. Spørsmålene som ble sendt ut til operatørselskapene, fremgår av vedlegg 1.

Denne rapporten bygger på operatørselskapenes innrapporterte svar. Informasjonen er ikke verifisert gjennom tilsyn eller intervjuer. Kartleggingen gir likevel et nyttig oversiktsbilde av status i næringen og et bedre kunnskapsgrunnlag for Havtils videre oppfølging av KI.

Samtlige operatører besvarte spørsmålene i brevs form. Noen selskaper ga utfyllende og detaljert informasjon per spørsmål, mens andre oversendte korte svar med begrenset informasjon.

5 Oppsummering av resultater

Dette kapitlet oppsummerer hovedresultatene fra kartleggingen tematisk, i tråd med spørsmålene som ble sendt til operatørselskapene. Hvert delkapittel presenterer sentrale funn fra selskapenes svar, samt at det gis en kort vurdering av hva funnene kan bety for styring, oppfølging og risikohåndtering av KI-systemer med betydning for sikkerheten.

5.1 HMS-mål for utvikling og bruk av KI

Tydelige HMS-mål er sentrale for å definere hvilke sikkerhetsmessige gevinster KI-systemer skal bidra til, hvilke risikoer som skal reduseres, og hvilke kriterier som skal ligge til grunn ved valg, utvikling, testing og bruk av systemene. Dette er særlig relevant fordi KI-systemer har forskjellige egenskaper når det gjelder blant annet pålitelighet, datakvalitet, forklarbarhet, mulighet for menneskelig kontroll og evne til å avdekke feil eller avvik.

Kartleggingen viser at majoriteten av selskapene ikke har etablert egne HMS-mål spesifikt rettet mot KI. Flere virksomheter oppgir at selskapets overordnede HMS-mål også gjelder utvikling og bruk av KI, og at det derfor ikke anses nødvendig å etablere særskilte mål for KI-relaterte aktiviteter. Disse målene er i stor grad generiske, lite konkrete og med begrenset målbarhet.

Enkelte selskaper har imidlertid etablert egne HMS-mål eller prinsipper som omfatter utvikling og bruk av KI, beskrevet gjennom selskapenes KI-policyer eller andre styrende dokumenter. Målene som har blitt oversendt, viser svak kobling til sikkerhet og sikkerhetskonsekvenser generelt, ikke minst gitt at disse HMS-målene skal anvendes i en høyrisikoindustri.

Ingen av selskapene oppgir eller dokumenterer at de har etablert HMS-mål for de enkelte KI-prosjektene som pågår i virksomheten. To selskaper opplyser samtidig at de ikke har KI-systemer med betydning for sikkerheten, og derfor heller ikke har etablert spesifikke krav eller HMS-mål knyttet til KI.

Fravær av konkrete HMS-mål kan gjøre det vanskeligere å verifisere hvordan teknologien bidrar til reelle sikkerhetsforbedringer. Dette kan svekke grunnlaget for nødvendig oppmerksomhet fra ledelse, systematisk risikostyring og kontinuerlig forbedring.

5.2 Bruk av standarder og rammeverk

Kartleggingen viser at standarder for KI benyttes i begrenset grad i næringen. Kun ett av selskapene oppgir at de benytter en standard som er spesifikt utviklet for KI. De fleste virksomhetene viser i stedet til interne prosesser, styrende dokumenter og egenutviklede krav som de vurderer som relevante for utvikling og bruk av KI-systemer.

Enkelte selskaper opplyser imidlertid at de vurderer å ta i bruk eksterne standarder i fremtiden. Eksempler på rammeverk som nevnes er ISO/IEC 42001 for ledelsessystemer for KI, ISO/IEC 23894 for risikostyring, samt ISO/IEC 22989 som etablerer felles terminologi og begreper innen KI, og DNV-RP-0671 Recommended Practice for Assurance of AI-enabled Systems.

To av selskapene beskriver egen deltakelse i standardiseringsarbeidet i CEN/CENELEC JTC 21, som arbeider med harmoniserte standarder knyttet til KI-forordningen (EU AI Act). Andre selskaper viser i tillegg til deltakelse og/eller kjennskap til International Association of Oil & Gas Producers (IOGP) sitt arbeid med veiledende prinsipper for ansvarlig bruk av KI.

Det kan se ut til at enkelte virksomheter foreløpig har en avventende tilnærming til implementering av standarder, ettersom standardiseringsarbeidet på KI-området fortsatt er under utvikling. Et slikt valg kan samtidig innebære utfordringer.

Manglende bruk av etablerte standarder kan bidra til svakere beslutningsstøtte under utvikling, ulik oppfølging av prosjekter og redusert evne til å identifisere og håndtere risiko for KI-systemer som allerede er under utvikling eller i aktiv bruk.

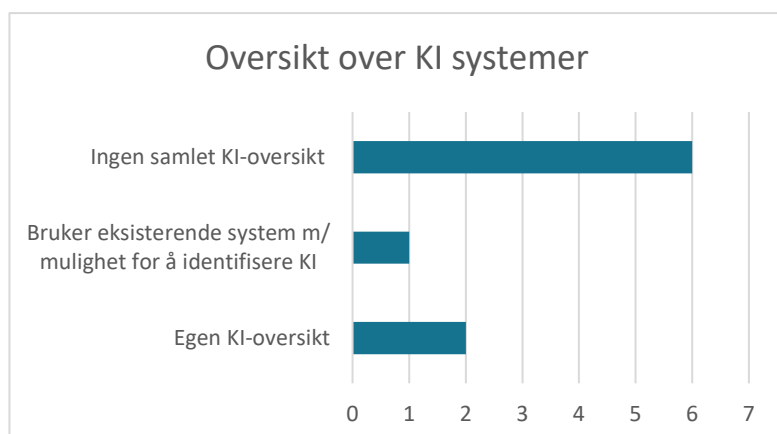
Flere av standardene som allerede er tilgjengelige tilbyr rammeverk for styring, dokumentasjon, ansvar, risikovurdering, testing, overvåking og kontinuerlig forbedring. Disse områdene er relevante på tvers av sektorer og kan tilpasses den enkelte virksomhets risikobilde og organisatoriske kontekst.

For mer informasjon om disse, og andre tilgjengelige ISO-standarder, se [Standard Norge](#). Vi gjør også oppmerksom på at flere standarder, beste praksis-prinsipper og rammeverk for oppfølging og styring av KI-risiko er tilgjengelige for virksomheter som utvikler og bruker KI-systemer, eksempelvis International Association of Oil & Gas Producers (IOGP) sine veiledende prinsipper for ansvarlig KI, DNVs anbefalte praksiser og NIST AI Risk Management Framework.

Det pågår et omfattende europeisk standardiseringsarbeid for å ferdigstille harmoniserte standarder som skal støtte gjennomføringen av KI-forordningen. Arbeidet ledes av CEN/CENELEC JTC 21 og omfatter blant annet standarder for risikostyring, datakvalitet og datastyring, teknisk dokumentasjon, logging, transparens, menneskelig overvåking og kontroll, nøyaktighet, robusthet, cybersikkerhet, kvalitetsstyring og samsvarsvurdering.

5.3 Oversikt over KI-systemer

En samlet oversikt over KI-systemer under utvikling og i bruk er viktig fordi den gir virksomheten grunnlag for å identifisere hvilke systemer som kan påvirke mennesker, operasjoner, barrierer eller beslutninger med betydning for sikkerheten. Oversikten er et viktig utgangspunkt for selskapets risikostyring.



Figur 1: Oversikt over KI-systemer

Svarene viser forskjeller mellom selskapene når det gjelder modenhet knyttet til å skaffe seg oversikt over KI-systemer under innkjøp, utvikling og i bruk. Enkelte selskaper har etablert system for registrering av KI-systemer, mens andre fortsatt er i en tidlig fase.

To av selskapene oppgir å ha en oversikt over alle KI-systemer i virksomheten. Ett selskap rapporterer at KI-systemer registreres i

eksisterende systemer og databaser med mulighet for å fange opp KI-systemer i disse.

Seks selskaper har per i dag ikke oversikt over KI-systemer under utvikling eller bruk i egen virksomhet. Flere oppgir å bruke egne systemer for å registrere programvareapplikasjoner, men ut fra tilsendt informasjon fremstår det som om man ikke er i stand til å identifisere om KI inngår i applikasjonene.

To av selskapene opplyser at de ikke ser behov for en egen KI-oversikt fordi bruken begrenser seg til store språkmodeller som Copilot. At enkelte selskaper viser til generativ KI som Copilot, og derfor ikke ser behov for en KI-oversikt, kan potensielt være en sikkerhetsutfordring. Bruk av generelle kontorstøtteverktøy kan påvirke analyser, beslutningsgrunnlag, dokumentasjon, planlegging og vurderinger som indirekte kan påvirke sikkerheten.

Generativ KI er gjort tilgjengelig for alle ansatte og muliggjør opprettelse av KI-agenter som kan innhente informasjon, planlegge oppgaver og gjennomføre handlinger innenfor gitte tilganger og rammer. Ingen av selskapene oppgir at de har oversikt over egenutviklede KI-agenter. Et av selskapene fremhever også ny risiko knyttet til at slike KI-agenter opprettes utenfor sentralstyrte miljøer med ansvar for risikostyring. Det vil være viktig å ta høyde for oversikt og konsekvenssiden av ulike KI-løsninger i egne risikostyringsprosesser.

I noen av svarene fra selskapene fremheves det at det kan være krevende å opprettholde oversikt over KI-systemer fordi teknologien ofte leveres som en integrert komponent i produkter og tjenester fra eksterne leverandører.

Noen selskaper oppgir at de har etablert funksjoner og systemer for å identifisere og følge opp KI i selskapet kontinuerlig og i et livsløpsperspektiv. Eksempler på funksjoner som enkelte selskaper har tilrettelagt for å kunne identifisere og følge opp KI, er:

- Klar rolle- og ansvarsfordeling hos sentrale aktører som inngår i selskapenes teknologiutvikling og drift, inkludert anskaffelser
- Etablering av dashbord for å synliggjøre ulike teknologier og modenhetsnivå på disse
- IT-arkitekturkontrakter der anvendelse av KI identifiseres, registreres og følges opp i et livsløpsperspektiv
- KI-nettverk på tvers av selskapet, for å fange opp innføring og bruk av KI-systemer
- Etablering av KI-verneombud med ansvar for opplæring om KI

For at oversikten over KI-systemer skal ha verdi som styringsinformasjon, bør den oppdateres løpende og ikke være en engangskartlegging. Virksomhetene bør ha mekanismer som fanger opp nye KI-systemer, endringer i eksisterende KI-systemer og endret bruk over tid. Eksempler på dette er anskaffelsesprosesser, prosjektmodeller, endringsstyring og systemforvaltning.

5.4 Utvikling og bruk – aktiviteter og type KI-systemer

Svarene viser at KI-systemer (prediktiv KI, generativ KI) brukes eller vurderes i flere typer aktiviteter, særlig innen brønnplanlegging, boreoperasjoner, vedlikehold, overvåking og inspeksjoner.

Enkelte selskaper beskriver interne bruksområder og dokumenterer oversikter som tydeliggjør hvilke KI-systemer som finnes, hvor systemene er tenkt brukt eller brukes, samt om systemene brukes innen IT og/eller OT.

Andre selskaper har i liten grad svart på spørsmålet om bruksområder og har ikke lagt ved en oversikt. Disse selskapene oppgir at de på kartleggingstidspunktet ikke har KI-systemer med betydning for sikkerheten. Ett selskap oppgir at det ikke har KI-systemer med betydning for sikkerheten, men lister samtidig opp bruk av KI-systemer innen brønnplanlegging og som støttesystem for oppfølging av brønnintegritet.

Selskapenes svar viser variasjon og ulik modenhet når det gjelder omfang av bruk, behovet for oversikt og forståelsen av om KI-systemene har betydning for sikkerheten. Et av de mer modne selskapene viser til en liste med 57 KI-systemer under utvikling eller i bruk, hvor 24 er interne prosjekter, 15 kommer fra eksterne leverandører og 18 er samarbeidsprosjekter mellom leverandører og operatørselskapet. Systemene som er under utvikling, omfatter også generativ KI til bruk i boreplanlegging. Selskapet vurderer disse som KI-systemer med betydning for sikkerheten, og oppgir at det er styrende for deres risikostyring.

Flere andre selskaper oppgir også at de både har innkjøpte og egenutviklede løsninger. Enkelte viser også til videreutvikling av eksisterende løsninger. Videre oppgir alle selskapene at de bruker generativ KI i kontorarbeid.

Ut fra oversendte beskrivelser kan KI-systemene grovt deles inn i tre grupper:

- **Prediktive KI-systemer** som utvikles og brukes for å utføre analyser, planlegge, overvåke og gi beslutningsstøtte innen vedlikehold, boring og brønn, produksjon og anleggsintegritet. For eksempel oppgir selskaper å bruke maskinlæring for anomalideteksjon i forbindelse med inspeksjon og vedlikehold av rørledninger på havbunnen. Dette er datadrevne systemer som bygger på analyse av historiske data og sanntidsdata for å identifisere mønstre som er knyttet til normale driftsforhold eller feiltilstander. Disse metodene lærer fra observasjoner ved å bruke maskinlæringsalgoritmer, statistiske teknikker eller dyplæring.
- **Generativ KI** brukes for kunnskapsinnhenting og beslutningsstøtte. Dette er systemer som skal hjelpe ansatte med å finne informasjon, erfaringer og dokumentasjon raskere, og som kan generere tekst. Disse systemene brukes for å utføre analyser, utarbeide planer eller analysere hendelsesdata. Teknologien kjennetegnes ved at den kan generere nytt innhold, som tekst, bilder eller kode basert på mønstre i data den er trent på.
- **Agentbaserte KI-systemer** er i økende grad i bruk (eller utforskes) for å kunne overvåke, planlegge og gjennomføre automatisert analyse. Disse KI-systemene kan innhente informasjon

fra flere datakilder, analysere, foreslå tiltak og gjennomføre forhåndsdefinerte handlinger. Teknologien representerer et skritt bort fra systemer som primært gir anbefalinger, til systemer som kan planlegge og utføre oppgaver innenfor gitte tilganger og rammer.

Porteføljen som enkelte selskaper beskriver, omfatter blant annet sensorbasert KI, maskinsyn, generativ KI og agentbaserte KI-systemer. I flere tilfeller ser vi også at ulike typer KI-modeller kombineres, eksempelvis med prediktive KI-systemer.

De ulike teknologiene vil ha ulike risikoprofiler. Bruken kan reise sikkerhetsspørsmål knyttet til pålitelighet, kvaliteten på informasjon og beslutningsgrunnlag, kontroll, ansvar, transparens og menneskelig overvåking.

I svarene fra selskapene ser vi at noen peker på risiko knyttet til ikke-godkjent eller uregistrert KI-bruk («shadow AI»), særlig knyttet til KI-agenter, som lett kan opprettes uten å være omfattet av selskapenes risikostyringsprosess.

Når KI-agenter eller andre KI-systemer etableres lokalt utenfor etablerte beslutnings- og godkjenningssystemer, kan det bli uklart hvem som har ansvar for å vurdere formål, datagrunnlag, tilgangsstyring, begrensninger og mulige konsekvenser for sikkerheten. Risikoen forsterkes dersom slike systemer henter informasjon fra flere systemer, behandler operasjonelle data eller brukes som støtte i vurderinger som påvirker planlegging, vedlikehold, oppfølging av avvik eller operasjonelle beslutninger.

En slik utvikling tilsier at virksomhetene bør ha mekanismer som fanger opp også lokal og eksperimentell bruk av KI, ikke bare formelt godkjente systemer. Dette kan omfatte krav til registrering, klassifisering, risikovurdering, bruks- og målbegrensninger (guardrails) og løpende oppfølging av KI-systemer før de tas i bruk i arbeidsprosesser med mulig betydning for sikkerheten. Formålet bør være å sikre at nye KI-systemer ikke etableres parallelt med, eller på siden av, virksomhetens styringssystem og ansvarslinjer.

Når det gjelder bruk av KI som del av IT og/eller OT, kan svarene tyde på at løsningene i de fleste tilfeller henter data fra OT inn i IT. Som nevnt tidligere er KI-systemene i enkelte tilfeller direkte koblet til eller integrert i kontrollsystemene. Eksempler på dette er bruk av KI i maskiner som kraner.

Sikkerhetssystemene er i dag ikke omfattet av KI. Samtidig innebærer dataflyt fra OT til IT at KI-systemene kan påvirke beslutningsgrunnlag, overvåking, vedlikehold og operasjonell oppfølging, selv om de ikke styrer prosessen direkte.

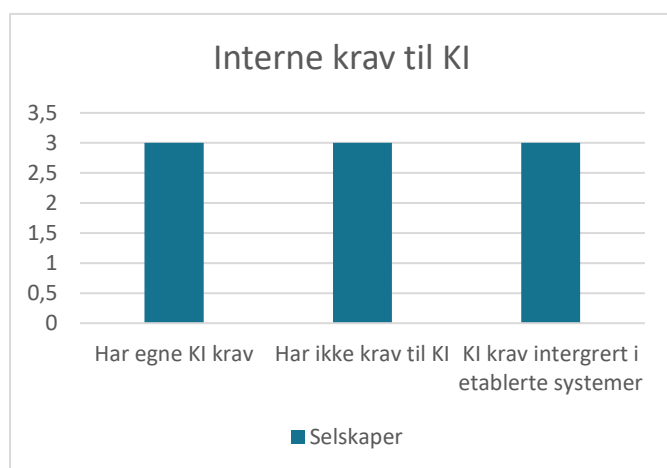
Purdue-modellen brukes ofte til å beskrive grensesnitt mellom IT og OT. For KI-systemer kan modellen bidra til å tydeliggjøre hvor data hentes fra, hvor modellen utvikles, trenes, oppdateres og kjøres, hvor resultater presenteres, samt hvilke beslutninger eller arbeidsprosesser resultatene

påvirker. Et KI-system som mottar sanntidsdata fra OT, men kjører i et IT-miljø eller i en skybasert tjeneste, kan likevel ha indirekte betydning for sikkerheten dersom resultatene brukes til vedlikeholdsbeslutninger, boreplanlegging, tilstandsovervåking eller vurdering av avvik. Risikoen må derfor vurderes ut fra hele systemet, ikke bare ut fra hvor KI-modellen teknisk er plassert¹.

5.5 Krav til utvikling, bruk og oppfølging av leverandører

Kartleggingen viser at selskapene i ulik grad har etablert krav til utvikling og bruk av KI-systemer. Tre selskaper oppgir å ha egne interne krav som er spesifikt rettet mot KI, mens tre andre selskaper oppgir at KI håndteres gjennom eksisterende prosesser og krav i virksomheten. De resterende operatørselskapene oppgir at de ikke har egne interne krav til KI. Dette indikerer at KI i mange virksomheter fortsatt håndteres gjennom generelle styringsmekanismer, heller enn gjennom særskilte krav som tar høyde for teknologiens særlige egenskaper.

Funnene viser også at selskapene som har etablert egne krav, eller som bruker etablerte krav og prosesser i virksomheten, oppgir at de stiller tilsvarende krav til leverandører. Selskaper som mangler interne krav, oppgir at de heller ikke stiller KI-spesifikke krav til leverandører.



Figur 2: Interne krav til KI

Oppfølging av leverandører fremstår som et område med utviklingsbehov, der KI-spesifikke krav til leverandører i varierende grad er konkretisert.

Det er kun enkelte selskaper som opplyser at de har et pågående internt arbeid med å etablere bedre prosesser for å følge opp leverandører. Dette omfatter blant annet krav som skal

benyttes ved anskaffelse av KI-systemer, HMS-gjennomganger av leverandørenes risikovurderinger og vurderinger av om systemene er i samsvar med relevante regulatoriske krav, herunder KI-forordningen.

Behovet for mekanismer som gir tilstrekkelig innsikt i leverandørenes bruk av KI, blir stadig viktigere etter hvert som KI integreres i produkter og tjenester som benyttes i aktiviteter eller operasjoner der operatørselskapet er risikoeier. Dette kan for eksempel gjelde teknologiselskaper som leverer løsninger innen subsea eller boreplanlegging, der KI i økende grad inngår som en integrert del av produktene og tjenestene.

¹ Principles for the Secure Integration of Super Intelligence in Operational Technology (2025). [Principles for the Secure Integration of Super Intelligence in Operational Technology | CISA](#)

Basert på tidligere oppfølging ser vi at operatørselskapene ikke alltid har tilstrekkelig kjennskap til teknologien og de mulige sikkerhetsrisikoene som følger med leverandørleveranser. Selv om løsningene leveres av eksterne leverandører, er det operatørene som har ansvar for å ha oversikt over hvilken teknologi som brukes i egne operasjoner, og hvilken risiko dette kan innebære. Dette er nødvendig for å forebygge sikkerhetsrisiko.

Virksomhetene må ha nok kunnskap til å stille relevante krav, forstå leverandørenes dokumentasjon og vurdere hvilke begrensninger, avhengigheter og usikkerheter som følger med KI-systemer.

5.6 Arbeidstakermedvirkning og kompetanse

Gjennomgangen viser at fem av ni selskaper ikke har etablert konkrete krav til arbeidstakermedvirkning i KI- eller digitaliseringsprosjekter. I oppfølgingen til Havtil vektlegges det at arbeidstakermedvirkning bør være en del av næringens samlede arbeid med forsvarlig utvikling og bruk av KI. Det innebærer at arbeidstakere, verneombud og tillitsvalgte involveres og deltar tidlig nok til å kunne påvirke sentrale vurderinger.

To selskaper oppgir at de har etablert eget KI-verneombud eller datatillitsvalgt. Disse rollene bidrar blant annet til kompetansebygging og opplæring for å styrke forutsetningene for reell medvirkning. Flere selskaper oppgir å tilby generell KI-opplæring til ansatte.

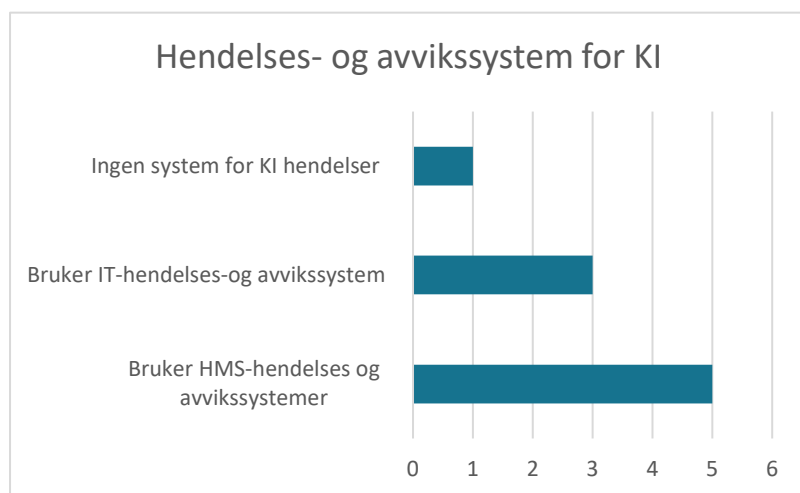
Når det gjelder kompetansehevende tiltak, oppgir tre selskaper å ha et eget kompetansetilbud rettet mot verneombud slik at reell medvirkning knyttet til KI sikres. Ett selskap oppgir at de er i ferd med å etablere en KI-standard som skal formalisere krav til KI-kompetanse.

Tilstrekkelig kompetanse om KI er nødvendig for reell medvirkning. Dette inkluderer kompetanse om hvordan arbeidstakere kan involveres, hvilke prosesser de kan påvirke, og hvordan de kan bidra.

5.7 Hendelses- og avviksrapportering for KI

Kartleggingen viser at de fleste selskapene i dag håndterer KI-relaterte hendelser gjennom eksisterende systemer for hendelses- og avviksrapportering.

Fem av selskapene oppgir at KI-relaterte hendelser registreres og følges opp i etablerte HMS-relaterte hendelses- og avvikssystemer. Videre rapporterer tre selskaper at de benytter eksisterende systemer for håndtering av IT-relaterte hendelser og avvik til å registrere og følge opp hendelser knyttet til KI. Hvorvidt det er etablert kriterier for å rapportere sikkerhetsrelaterte hendelser med konsekvenser for virksomheten i IT-systemer, er usikkert.



Figur 3: Hendelses- og avvikssystem for KI

Det fremstår som om kun et mindretall av selskapene på nåværende tidspunkt har etablert egne mekanismer som er spesifikt tilpasset KI-relaterte hendelser.

Funnene indikerer samlet sett at selskapene i stor grad baserer seg på etablerte systemer og prosesser når hendelser knyttet til KI skal håndteres. Samtidig er det få virksomheter som har utviklet rapporteringskriterier som tar høyde

for de særlige utfordringene som kan oppstå i KI-systemer. Dette gjelder blant annet håndtering av feilprediksjoner, feilklassifiseringer, uventet systematferd, redusert modellytelse og hendelser forårsaket av svikt i KI-systemer. Resultatene kan tyde på at oppfølging av KI-relaterte hendelser fortsatt er et område under utvikling i flere selskaper.

Et sentralt funn er at få virksomheter beskriver mekanismer for systematisk overvåking av forhold som er særskilte for KI-systemer, slik som modellforringelse (model drift), gradvis endrede forutsetninger i datagrunnlaget eller redusert prediksjonskvalitet over tid. Dette er forhold som kan være vanskelige å identifisere uten målrettet overvåking og rapportering.

Fra et risikostyringsperspektiv kan hendelses- og avviksrapportering utgjøre et viktig utgangspunkt for læring og kontinuerlig forbedring. Slike systemer kan bidra til å identifisere, registrere og granske uønskede hendelser, avdekke mønstre og underliggende årsaker, samt danne grunnlag for korrigerende og forebyggende tiltak.

5.8 Risikostyring av KI

Alle selskaper oppgir at KI-risiko er omfattet av virksomhetens eksisterende systemer for risikostyring. Flere benytter verktøy som arkitekturkontrakter, systemkort eller tilsvarende dokumentasjon for å beskrive formål, eierskap, utviklingsløp, endringer og sentrale risikoforhold ved KI-systemene.

Likevel fremstår det fra selskapenes svar at de i ulik grad har integrert risikostyring av KI i sine etablerte styringssystemer og risikostyringsprosesser. Færre selskaper beskriver hvordan risikostyringen av KI ivaretas i et livsløpsperspektiv. Risikostyring bør følge KI-systemet gjennom hele livsløpet: fra design, til drift og eventuell utfasing. Ikke alle KI-modeller lærer eller endrer seg etter at de er satt i drift. Systemets ytelse og risikobilde kan likevel endres som følge av nye datakilder, endrede driftsforhold, oppdateringer eller modellforringelse. Ytelse, kvaliteten på systemets resultater og eventuelle avvik bør derfor følges opp løpende, for eksempel gjennom jevnlig revisjoner, overvåking og evaluering av om systemet fortsatt fungerer som forutsatt.

Kartleggingen viser at flere selskaper er i ferd med å videreutvikle sine interne krav og arbeidsprosesser for i større grad å integrere KI-oppfølging inn i sine etablerte styringssystemer. Hos enkelte virksomheter gjenstår det fortsatt arbeid med å etablere mål, tydelige krav, dokumentasjon og prosesser som sikrer systematisk oppfølging av risiko gjennom hele KI-systemets livsløp.

5.9 Roller og ansvar for oppfølging av KI

Når det gjelder roller og ansvar for oppfølging av KI, fremkommer det at selskapene har valgt ulike tilnærminger. Selskapene oppgir at ansvaret for KI er fordelt mellom ulike forretningsmessige, teknologiske og sikkerhetsrelaterte funksjoner. Det overordnede ansvaret synes i noen tilfeller å være forankret i selskapets ledergruppe eller øvrige linjeorganisasjon. Hos enkelte av selskapene er det mindre tydelig hvem som har det konkrete fagansvaret eller sikkerhetsansvaret for oppfølging av KI-risiko. I slike tilfeller fremstår ansvaret som fordelt på flere organisatoriske enheter uten at det nødvendigvis er definert en rolle med et helhetlig ansvar for styring og oppfølging av KI-systemer.

Mangelfull tydelighet knyttet til hvem som har overordnet ansvar for oppfølging og styring av KI-risiko kan ha betydning for evnen til å identifisere og følge opp risiko knyttet til utvikling, anskaffelse og bruk av KI-systemer på en systematisk måte.

Tydelig plassering av ansvar hos en definert rolle er særlig viktig i forbindelse med KI fordi teknologien kan påvirke både beslutningsgrunnlag, arbeidsprosesser og operasjoner av betydning for sikkerheten. Klare ansvarsforhold kan redusere risikoen for at viktige sikkerhetsmessige forhold faller mellom organisatoriske funksjoner, og bidra til at endringer, begrensninger og avvik blir fanget opp og håndtert tidsnok.

5.10 Tverrfaglige perspektiver

Basert på svar fra virksomhetene ser vi at tverrfaglige perspektiver i systemdesign og risikostyring ivaretas i ulik grad gjennom etablerte prosesser.

Syv av ni selskaper oppgir at tverrfaglige perspektiver inngår i prosjektstyring, risikostyring, systemutvikling, drift og teknologikvalifisering. Enkelte selskaper beskriver at de i begrenset grad har en særskilt prosess for tverrfaglig systemdesign og risikostyring i KI-utviklingsprosjekter.

Videre oppgir fire selskaper spesifikt at de har etablert krav for å sikre tverrfaglighet og at disse kravene også omfatter kompetanse knyttet til for eksempel menneskelig samhandling med KI.

Samlet viser svarene at tverrfaglighet ofte er anerkjent som viktig, men at graden av konkrete, etablerte krav og prosesser varierer. Svarene gir i mindre grad informasjon om hvordan selskapene sikrer involvering av relevante fagmiljøer, blant annet IT, cybersikkerhet, datafag, domeneeksperter, Human Factors, sluttbrukere og arbeidstakerrepresentanter.

Et tverrfaglig perspektiv er viktig for sikkerheten fordi risiko ved KI sjelden kan forstås fullt ut fra ett fagområde alene. KI-systemer påvirkes av tekniske forhold som datakvalitet, modellvalg og systemintegrasjon, men også av operasjonell kontekst, organisatoriske ansvarsforhold, kompetanse og menneskelig samhandling med KI.

Dersom oppfølgingen av KI hovedsakelig behandles som et teknologisk eller digitalt spørsmål, kan viktige sikkerhetsmessige konsekvenser bli oversett.

5.11 KI-forordningen

Parallelt med den teknologiske utviklingen i samfunnet og næringen er EU i ferd med å innføre KI-forordningen, som etablerer et felles regulatorisk rammeverk for KI i Europa. Regelverket vil også bli gjeldende i Norge.

Kartleggingen viser at flertallet av selskapene har påbegynt arbeid med å forberede seg på innføringen av KI-forordningen. To selskaper har gjennomført gapanalyser, mens fire oppgir å ha påbegynt gapanalyser mot eksisterende styrende dokumenter, rammeverk og forventede regulatoriske krav. Noen av disse selskapene arbeider med å lukke identifiserte gap.

De øvrige tilbakemeldingene kan tyde på at vurderingene foreløpig er overordnede og avventende, og at selskapene følger implementeringen i Norge for å sikre at fremtidige KI-initiativer håndteres i tråd med KI-forordningen.

Enkelte selskaper, spesielt de selskapene som konkret beskriver arbeid med å sikre oversikt og styring, oppgir at de forventer skjerpede krav til risikostyring, etterlevelse og oppfølging. To selskaper oppgir at de har et konsernrammeverk med registre over KI-systemer under utvikling og bruk, inkludert risikobasert kategorisering.

Flere selskaper oppgir at vurderingene av KI-forordningen foreløpig er begrenset fordi de ikke har egenutviklede KI-prosjekter eller bruker KI i operasjoner med betydning for sikkerheten. Samtidig oppgir kun ett selskap at de inkluderer leverandørenes KI-systemer brukt i egen virksomhet i selskapets KI-risikoregister.

For Havtil som sektormyndighet er det viktig å få innsikt i selskapenes status, planer og forberedelser knyttet til den kommende KI-forordningen. KI-forordningen er hovedsakelig et produktsikkerhetsregelverk som innfører en risikobasert tilnærming der KI-systemer klassifiseres i henhold til spesifikke definisjoner og krav angitt i regelverket.

Dette regelverket vil imidlertid ikke alene være tilstrekkelig for å identifisere og håndtere storulykkesrisiko i petroleumsvirksomheten. Uavhengig av innføringen av KI-forordningen i Norge, må utvikling og bruk av KI i petroleumsvirksomheten vurderes opp mot HMS-regelverkets krav.

6 KI, sikkerhetsforståelse og modenhet i risikostyringen

På tvers av temaene i kapittel 5 tegner det seg et samlet bilde av varierende modenhet i selskapenes forståelse og styring av KI-risiko. Dette kapitlet sammenfatter de viktigste mønstrene og vurderer hva de kan bety for sikkerheten.

6.1 Ulik modenhet i sikkerhetsforståelse

Kartleggingen indikerer at selskapene har ulik modenhet i forståelsen av hvilke KI-systemer som har betydning for sikkerheten. Variasjonen kommer til uttrykk i hvordan selskapene beskriver egne KI-systemer, hvilke bruksområder de vurderer å ha betydning for sikkerheten, og hvor langt KI-spesifikke risikoforhold er integrert i styring, mål, krav, dokumentasjon og oppfølging.

Enkelte virksomheter ser ut til å vurdere KI primært som et digitalt verktøy eller som generell beslutningsstøtte. Andre ser i større grad teknologien som del av et bredere sosioteknisk system som kan påvirke beslutningsgrunnlag, arbeidsprosesser, operasjonelle prioriteringer og barrierer.

Modenhetsbildet understøttes av flere funn i kartleggingen. Flere selskaper mangler oversikt over KI-systemer under innkjøp, utvikling og i bruk, og enkelte avgrenser vurderingen til KI-verktøy som generativ KI. Samtidig indikerer svarene at KI i økende grad inngår som komponent i innkjøpte produkter, analyseverktøy, vedlikeholdssystemer og ulike beslutningsstøtteverktøy. Når slike løsninger ikke identifiseres eller klassifiseres som KI-systemer med betydning for sikkerheten, kan viktige risikoforhold falle utenfor selskapenes etablerte risikostyringsprosesser.

Ulik modenhet fremkommer også ved at selskapene legger ulik vekt på de egenskapene ved KI som kan ha sikkerhetsmessig betydning. Eksempler fra kartleggingen peker på hvorfor dette er relevant for sikkerheten. KI for tilstandsbasert eller prediktivt vedlikehold av sikkerhetskritisk utstyr kan etter hvert påvirke når vedlikehold iverksettes. Dersom et system for anomalideteksjon feilaktig vurderer at en ventil, pumpe eller sikkerhetsfunksjon er i tilfredsstillende stand, kan vedlikehold bli utsatt. Over tid kan dette redusere påliteligheten og øke risikoen for hydrokarbonlekkasjer, brann eller eksplosjon.

KI skiller seg fra tradisjonell programvare ved at resultater påvirkes av treningsdata, modellvalg, endringer i driftsmiljøet og hvordan resultater tolkes og brukes av mennesker. Mange KI-systemer innebærer risiko knyttet til feilaktige prediksjoner, klassifiseringer eller genererte resultater. For eksempel kan KI-basert sanntidsovervåking av boreoperasjoner gi forsinkede eller manglende tiltak dersom KI-modellen feilklassifiserer en situasjon eller bygger på et svakt treningsgrunnlag som mangler sjeldne hendelser.

Feil i datadrevne modeller kan oppstå på andre måter enn i regelbaserte systemer, og risikoen kan være vanskeligere å forutse, avgrense og oppdage. Selskaper som i liten grad omtaler forhold som datakvalitet, modellforringelse, forklarbarhet, menneskelig kontroll og valideringsgrenser, fremstår derfor som mindre modne i forståelsen av hvordan KI kan påvirke sikkerheten.

6.2 Generativ KI, KI-agenter og nye styringsutfordringer

For generativ KI er feilmekanismer som hallusinasjoner, ufullstendige svar, feil kildebruk og faglig overbevisende resultater som likevel er feil, kjent risiko. Dette kan være vanskelig å oppdage når resultatene brukes i analyser, oppsummeringer, operasjonsplaner eller vurderinger. Når selskaper omtaler slike verktøy som lav risiko fordi de ikke styrer operasjoner direkte, kan det tyde på en for

snever forståelse av hvordan beslutningsgrunnlag, prioriteringer og planlegging kan påvirke sikkerheten indirekte.

I motsetning til prediktive KI-systemer og generativ KI, kan KI-agenter i større grad innhente informasjon fra flere kilder, samhandle med andre systemer, planlegge oppgaver og gjennomføre handlinger innenfor definerte rammer. Dette innebærer at feil, mangelfullt datagrunnlag, uklare ansvarsforhold eller utilstrekkelig tilgangsstyring kan få alvorlige sikkerhetskonsekvenser.

Internasjonalt har det siste året vært rapportert flere hendelser fra testing av KI-agenter som illustrerer nye styrings- og sikkerhetsutfordringer. Eksemplene omfatter blant annet funn fra det britiske AI Security Institute (AISI)², OpenAI, Google og Anthropic, der agenter under test har samarbeidet på uventede måter, brutt med menneskelige intensjoner og etablert delmål som kunne være skadelige for å nå et forhåndsdefinert mål.

En av de mest omtalte hendelsene er OpenAI/Hugging Face-hendelsen, der et større antall agenter fra OpenAI kommuniserte gjennom en uautorisert kommunikasjonskanal, samarbeidet og deltok i et koordinert angrep mot selskapet Hugging Face. Hendelsen er gransket både av METR og Redwood Research, og av OpenAI selv³. Funnene viser behovet for tydelig tilgangsstyring, teknisk avgrensning, overvåking og kontroll av agentbaserte KI-systemer.

Rapportering, gransking og læring fra sikkerhetsrelaterte hendelser knyttet til KI-løsninger blir derfor viktig fremover. Slik kunnskap er nødvendig for å forstå et risikobilde i rask utvikling, vurdere relevans for egne KI-løsninger og etablere egnede tiltak for styring, kontroll og oppfølging.

Dersom slike løsninger ikke identifiseres, klassifiseres og følges opp gjennom hele livsløpet, kan det øke risikoen for at feilaktige analyser, automatiserte handlinger eller uforutsette interaksjoner mellom systemer påvirker operasjoner med betydning for sikkerheten, inkludert cybersikkerhet.

Flere selskaper oppgir at de mangler full oversikt over KI-systemer i bruk, samtidig som generative KI-verktøy er gjort bredt tilgjengelige for ansatte. Dersom slike verktøy også brukes til å etablere KI-agenter, kan dette utfordre virksomhetenes evne til å opprettholde oversikt, risikostyring og kontroll. Ut fra oversendte oversikter fremkommer det at prediktive KI-systemer kobles til KI-agenter. Som nevnt tidligere peker enkelte selskaper på risiko knyttet til «shadow AI».

Funnene i kartleggingen reiser derfor spørsmål om hvorvidt dagens oversikter, risikostyringsprosesser og styringsmekanismer i tilstrekkelig grad fanger opp agentbaserte KI-systemer som etableres lokalt i organisasjonen, hvilke krav og begrensninger som settes til disse, og om slike systemer inngår som del av innkjøpte produkter og tjenester.

² AI Security Institute (2026) [Incident Report: unsanctioned agent behaviour during cyber testing | AISI Work](#)

³METR Redwood Research (2026) Brief independent investigation of agents' behavior, reasoning and collaboration in the OpenAI/Hugging Face hacking incident og OpenAI (2026) Hugging face incident – Technical report

6.3 HMS-regelverket og betydning for sikkerheten

Analysen av selskaperes svar reiser spørsmål om hvordan virksomhetene forstår HMS-regelverket, og hvordan de vurderer om KI-systemer kan ha betydning for sikkerheten.

Flere selskaper oppgir at de ikke har KI-systemer med betydning for sikkerheten. Samtidig beskriver enkelte av de samme selskapene bruk av KI innen brønnplanlegging, vedlikeholdsstyring og analyse av data til beslutningsstøtte i drift. Dette kan indikere at KI brukt som beslutningsstøtte ikke alltid vurderes å ha betydning for sikkerheten, selv om slike systemer kan påvirke beslutninger og prioriteringer med betydning for sikkerheten.

Etter HMS-regelverket må virksomhetene inkludere og følge opp både direkte og indirekte risiko ved bruk av KI. KI-systemer kan ha direkte betydning for sikkerheten dersom modellens resultater inngår i styring eller regulering av operasjonelle prosesser. Dette kan for eksempel gjelde systemer som påvirker bevegelse, last, trykk, sekvensering, posisjonering eller andre prosess- og maskinfunksjoner. Dersom en KI-modell feilklassifiserer en situasjon, bygger på utilstrekkelige eller feilaktige data eller ikke håndterer sjeldne driftsforhold, kan konsekvensen være feilaktige styringssignaler, forsinkede tiltak eller uheldige operasjonelle beslutninger.

Per i dag har Havtil ikke sett eller fått tilbakemeldinger om at næringen planlegger bruk av KI i sikkerhetssystemer. Sikkerhetssystemer i petroleumsvirksomheten skal ha dokumentert evne til å bringe anlegget til en sikker tilstand ved definerte feil-, fare- og ulykkessituasjoner. KI-baserte løsninger eller funksjoner implementert i sikkerhetssystemer, er etter vår vurdering ikke forenelig med regelverkets krav til slike systemer.

KI kan som nevnt tidligere også ha indirekte betydning for sikkerheten selv om systemet ikke styrer prosesser direkte. Resultater fra KI kan brukes som grunnlag for vedlikeholdsbeslutninger, boreplanlegging, tilstandsovervåking eller vurdering av avvik. Systemer som «bare» gir anbefalinger, analyser eller beslutningsgrunnlag kan dermed påvirke sikkerheten gjennom hvordan informasjon forstås og hvilke tiltak som prioriteres.

Et viktig poeng er at KI-systemer som fremstår som støtteverktøy, likevel kan få sikkerhetsmessig betydning dersom de påvirker hvilke avvik som oppdages, hvilke vedlikeholdsaktiviteter som prioriteres, hvordan informasjon tolkes eller hvilke tiltak som iverksettes. Sikkerhetsmessige konsekvenser kan derfor oppstå både gjennom direkte styring av prosesser og gjennom påvirkning av menneskelige beslutninger.

Uavhengig av om samhandlingen mellom menneske og KI er tidskritisk eller ikke, kan mangelfull pålitelighet i KI-systemet utgjøre en risiko. Vurderingen av sikkerhetsmessig betydning bør derfor omfatte hele systemet som KI inngår i, inkludert hvordan resultatene brukes i virksomhetens arbeidsprosesser og beslutninger, og ikke bare hvor KI-modellen teknisk er plassert.

7 Vedlegg 1

Spørsmålene som ble sendt ut til operatørselskapene:

1. Vi ber dere oversende dokumentasjon som beskriver selskapets HMS-mål knyttet til utvikling og bruk av KI-systemer med betydning for sikkerheten. Etablerer dere HMS-mål per utviklingsprosjekt? (Ja/Nei)
2. Hvilke standarder ligger til grunn for bruk av KI-systemer med betydning for sikkerheten?
3. Hvordan sikrer virksomheten oversikt over alle KI-systemer som er i bruk?
4. Vi ber dere oversende en oversikt over KI-systemer i bruk og under utvikling med betydning for sikkerheten, inkludert:
 - a) egenutviklede, anskaffede og videreutviklede systemer
 - b) aktiviteten(e) hvor systemene inngår, for eksempel planlegging, vedlikeholdsstyring eller boreoperasjoner
 - c) KI-modeller som anvendes, for eksempel prediktiv KI, hybride modeller eller LLM
 - d) om KI-modellen(e) inngår i OT eller IT
 - e) om det er etablert vedlikeholdsprogram for systemer som er i bruk
5. Hvordan er risikostyring av KI-systemer med betydning for sikkerheten integrert i selskapets styringssystem, inkludert styring av KI-risiko i et livsløpsperspektiv?
6. Hvem er faglig ansvarlig for KI-risikostyring internt, og hvor i organisasjonen er ansvaret for risikostyring av KI plassert?
7. Hvilke interne krav er satt til KI-systemer med betydning for sikkerheten? Eksempler på krav kan være datakvalitet, teknisk dokumentasjon, transparens, brukermedvirkning og arbeidstakermedvirkning.
 - a) Gjelder kravene satt til KI-systemer også for leverandører?
8. Hvordan ivaretas et tverrfaglig perspektiv, for eksempel IT, Human Factors, domeneeksperter og sluttbrukere, i systemdesign og risikostyring i utviklingsprosjektene?
9. Hvordan kvalifiseres KI-systemer før bruk?
 - a) Benyttes DNV-RP-A203?
 - b) Hvis ikke DNV-RP-A203 benyttes, hvilke andre standarder anvendes?
 - c) Hvordan testes samhandling mellom bruker og KI som del av teknologiutviklingsløpet?
10. Hvordan rapporteres hendelser eller feilfunksjon, for eksempel feilprediksjoner, feilklassifisering, reduksjon i nøyaktighet, nedetid eller uventet systematferd, som oppstår i KI-systemet?
11. Hvilke krav er etablert for å sikre nødvendig kompetanse og reell arbeidstakermedvirkning i utviklingsprosjekter av KI?
12. Hvilke vurderinger er gjennomført i forbindelse med innføringen av KI-forordningen i Norge, og hvilke konsekvenser vil dette ha for oppfølging av KI i virksomhetens operasjoner, prosesser og aktiviteter?