2021:00054 - Åpen

# Rapport

## Regulering av IKT-sikkerhet i petroleumssektoren

IKT-sikkerhet – Robusthet i petroleumssektoren 2020

**Forfatter(e)**
Knut Øien, Lars Bodsberg, Martin Gilje Jaatun, Thor Myklebust, Tor Onshus

**SINTEF Digital**
2021-01-29

SINTEF Digital
Postadresse:
Postboks 4760 Torgarden
7465 Trondheim
Sentralbord: 40005100

info@sintef.no

Foretaksregister:
NO 919 303 808 MVA

# Rapport

# Regulering av IKT-sikkerhet i petroleumssektoren

IKT-sikkerhet – Robusthet i petroleumssektoren 2020

EMNEORD:
Regelverk
IKT-sikkerhet
OT-systemer

**VERSJON**
1.0

**DATO**
2021-01-29

**FORFATTER(E)**
Knut Øien, Lars Bodsberg, Martin Gilje Jaatun, Thor Myklebust, Tor Onshus

**OPPDRAGSGIVER(E)**
Petroleumstilsynet

**OPPDRAGSGIVERS REF.**
Arne Halvor Embergsrud

**PROSJEKTNR**
102022556

**ANTALL SIDER OG VEDLEGG:**
36 (3 vedlegg)

**SAMMENDRAG**
Formålet med denne rapporten er å klargjøre hvordan beskyttelse av informasjons- og kommunikasjonsteknologi (IKT-sikkerhet) i petroleumsindustrien blir regulert i gjeldende regelverk og belyse forventninger fra myndighetene innen IKT-sikkerhet.

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**
Knut Øien

SIGNATUR
Knut Øien

**KONTROLLERT AV**
Stefan Lindskog

SIGNATUR
Stefan Lindskog
Stefan Lindskog (28. Jan. 2021 12:14 GMT+1)

**GODKJENT AV**
Maria Bartnes

SIGNATUR
Maria Bartnes

**RAPPORTNR** 2021:00054
**ISBN** 978-82-14-06478-0
**GRADERING** Åpen
**GRADERING DENNE SIDE** Åpen

# Historikk

| VERSJON | DATO | VERSJONSBESKRIVELSE |
|---|---|---|
| 1.0 | 2021-01-29 | Endelig versjon |

# Innholdsfortegnelse

## Forord

Petroleumsvirksomheten preges av høy endringstakt og ambisiøse planer om økt bruk av digital teknologi innenfor hele verdikjeden. Noen stikkord er robotisering, kunstig intelligens, maskinlæring, stordata-behandling, endring av arbeidsprosesser, samt nye samarbeidsformer og forretningsmodeller.

Digitalisering legger til rette for tettere sammenkobling og økt dataflyt mellom forskjellige datasystemer, støttesystemer, sensorinformasjon, databaser og mennesker. Dette bidrar til mer effektive arbeidsprosesser og bedre analyser og beslutninger. Digitalisering vil kunne gi bedre sikkerhet gjennom utvidet tilgang på og mer effektiv bruk av sanntids- og historiske data internt så vel som eksternt i en organisasjon. Imidlertid, når informasjon fra kontroll- og sikkerhetssystemer i større grad blir tilgjengelig i administrative kontorsystemer og i "skyen" vil dette samtidig føre til at kontroll- og sikkerhetssystemer blir mer sårbare og attraktive mål for nettangrep. Angrep på kontorsystemer kan være et springbrett inn mot de industrielle IKT-systemene.

Et hovedmål med dette dokumentet har vært å klargjøre hvordan IKT-sikkerhet i petroleumsindustrien blir regulert i gjeldende regelverk, inkludert å gi en oversikt over regelverket for de aktører som ikke er så kjent med det.

Dokumentet gir også en oversikt over bakgrunnen for og status på den store satsingen på IKT-sikkerhet i petroleumssektoren som startet i 2018 og løper ut 2021. Statusen er vurdert i forhold til forventningene til overordnet myndighet, herunder signaler gitt i *Nasjonal strategi for digital sikkerhet* (2019). Dette er også en orientering til overordnet myndighet om status på det pågående arbeidet.

Dokumentet er laget som en SINTEF-rapport, men er utformet som et kortfattet notat, litt tilsvarende som andre Ptil-notat, slik som *Integrert og helhetlig risikostyring i petroleumsindustrien* (2018). Det er utarbeidet av SINTEF for Ptil, sett fra utsiden. Det er altså ikke sett med Ptils egne øyne, men kan utgjøre et underlag for et fremtidig Ptil-notat om IKT-sikkerhet sett fra Ptils eget ståsted, for eksempel etter at den store satsingen på IKT-sikkerhet er avsluttet i 2021.

Dokumentet dekker utvalgte temaer innenfor IKT-sikkerhet, og bør også ses i sammenheng med annet arbeid i Ptil, slik som det nevnte notatet om risikostyring (2018) og barrierenotatet (2017), presentasjoner gitt av Ptil i ulike faglige fora, og IKT-sikkerhetstilsyn. Sistnevnte dekkes i liten grad i dette dokumentet, da tilsyns-rapportene fra disse tilsynene for det meste er unntatt offentlighet.

For å oppnå god IKT-sikkerhet, forutsettes det at det enkelte selskap erkjenner potensialet for alvorlige IKT-hendelser som kan ramme de industrielle IKT-systemene.

Knut Øien
Seniorforsker, SINTEF Digital

Januar 2021

## Sammendrag


### Innledning
Dette dokumentet beskriver hvordan IKT-sikkerhet i petroleumsindustrien blir regulert i gjeldende regelverk, og det gir en oversikt over bakgrunnen for, forventninger til, og status på den store satsingen på IKT-sikkerhet i petroleumssektoren som startet i 2018 og løper ut 2021.

### Industrielle IKT-systemer og IKT-sikkerhet
I petroleumssektoren benyttes vanligvis begrepene IT-systemer om kontorsystemene, OT-systemer eller industrielle IKT-systemer om de industrielle kontroll- og sikkerhetssystemene, og IKT-systemer som fellesbetegnelse på IT- og OT-systemer. Tilsvarende favner IKT-sikkerhet generelt vidt, og har ikke en entydig definisjon, mens det som har særlig fokus for Ptil er de industrielle IKT-systemene (OT-systemene) og dermed "OT-sikkerhet" som del av IKT-sikkerhet.

### Bakgrunn og forventninger fra overordnet myndighet
Lysneutvalgets rapport *Digital sårbarhet – sikkert samfunn* (2015) og stortingsmeldingen om *IKT-sikkerhet – et felles ansvar* (2016-2017) utgjorde sentrale dokumenter som ledet til den store satsingen på IKT-sikkerhet i petroleumssektoren (2018-2021). Her inngår anbefalinger og forventninger knyttet til overføring av sikkerhetstradisjonen innen helse, miljø og sikkerhet (HMS) til det digitale området, etablering av regelverk for digitale sårbarheter, tydeliggjøring av rolle og kapasitet hos Petroleumstilsynet og tilknytning til responsmiljø for IKT-hendelser. Videre er det forventninger til arbeidet med IKT-sikkerhet generelt i *Nasjonal strategi for digital sikkerhet* (2019) og spesifikt for Petroleumstilsynet (Ptil) i de årlige tildelingsbrevene fra Arbeids- og sosialdepartementet (ASD).

### Generelt om petroleumsregelverket
HMS-regimet i norsk petroleumsvirksomhet anvender i hovedsak funksjonelle prinsipper og bygger på internkontroll, der selskapene har et selvstendig ansvar for å ivareta HMS-hensyn gjennom interne styringssystemer og prosesser. Operatør og rettighetshaver er i tillegg pålagt en særskilt plikt til å følge opp at enhver som utfører arbeid for seg etterlever krav som er gitt i helse-, miljø- og sikkerhetslovgivningen (påseplikten). Regelverket består av fem forskrifter i medhold av petroleumsloven (og flere andre lover), veiledninger til forskriftene, samt henvisning til anerkjente standarder, normer og veiledere.

### IKT-sikkerhet i petroleumsregelverket
IKT er ikke nevnt spesielt i petroleumsloven, og regelverket (forskriftene) er funksjonsbasert hvor IKT-sikkerhet generelt omfattes, men i liten grad nevnes eksplisitt. Videre er NOROG 104 den eneste IKT-relaterte henvisningen til standarder, normer eller veiledere. Det er en pågående diskusjon i næringen om regelverkshenvisning til andre IKT-relaterte standarder, normer og veiledere. Dette gjelder særlig IEC 62443-serien (standarder og tekniske rapporter som definerer prosedyrer for implementering av sikre industri-automatiserings – og kontrollsystemer (IACS/OT)).

### IKT-sikkerhet – robusthet i petroleumssektoren
I løpet av de tre første årene i satsingen *IKT-sikkerhet – robusthet i petroleumssektoren* (2018-2021) har det blitt laget 18 rapporter for Ptil av IRIS, DNV GL og SINTEF. Disse er kort beskrevet og det er gjort en vurdering av status for satsingen i forhold til forventninger og anbefalinger i *Nasjonal strategi for digital sikkerhet* (2019), Lysneutvalgets rapport (2015) og tildelingsbrev fra ASD (2020).

De fleste av de 18 rapportene gir anbefalinger for tiltak og videre kunnskapsinnhenting. Mange av disse er knyttet til forventningene og anbefalingene fra myndighetene som Ptil kan benytte i fortsettelsen av IKT-sikkerhetssatsingen.

## Executive summary


### Introduction

This document describes how ICT security in the petroleum industry is regulated in current regulations, and it provides an overview of the background for, expectations of, and status of the major ICT security initiative in the petroleum sector that started in 2018 and expires in 2021.

### Industrial ICT systems and ICT security

In the petroleum sector, the term IT system is usually used for office systems, OT system or industrial ICT system are used for industrial control and security systems, and ICT system is used as a common term for IT and OT systems. Similarly, ICT security is generally a broad term, not having an unambiguous definition, whereas a focus for the Petroleum Safety Authority (PSA) is the industrial ICT systems (OT systems) and thus "OT security" as part of ICT security.

### Background and expectations from the authorities

The Lysne Committee's report *Digital Vulnerability - Safe Society* (2015) and the White Paper on *ICT Security - A Joint Responsibility* (2016-2017) were key documents that led to the major initiative in ICT security in the petroleum sector (2018-2021). This includes recommendations and expectations related to the transfer of the safety tradition within health, safety and environment (HSE) to the digital area, the establishment of regulations for digital vulnerabilities, clarification of the role and capacity of the Petroleum Safety Authority Norway and collaboration with response teams for ICT incidents. Furthermore, there are expectations for the work with ICT security in general in the *National Strategy for Digital Security* (2019) and specifically for the Petroleum Safety Authority Norway in the annual assignment letters from the Ministry of Labor and Social Affairs.

### General information about the petroleum regulations

The HSE regime in Norwegian petroleum activities mainly applies functional principles and is based on internal control, where the companies have an independent responsibility for HSE through internal management systems and processes. The operator and licensee are also required to follow up that everyone who performs work for them complies with requirements given in the health, environment and safety legislation (duty of care). The regulations consist of five regulations pursuant to the Petroleum Act (and several other laws), guidelines for the regulations, as well as reference to recognized standards, norms and guidelines.

### ICT security in the petroleum regulations

ICT is not specifically mentioned in the Petroleum Act, and the regulations are function-based where ICT security is generally covered, but only to a minor extent is mentioned explicitly. Furthermore, NOROG 104 is the only ICT-related reference to standards, norms or guidelines. There is an ongoing discussion in the industry about regulatory reference to other ICT-related standards, norms and guidelines. This applies in particular to the IEC 62443 series (standards and technical reports defining procedures for implementing secure industrial automation and control systems (IACS/OT)).

### ICT security - robustness in the petroleum sector

During the first three years of the initiative *ICT Security - Robustness in the Petroleum Sector* (2018-2021), 18 reports have been prepared for the PSA by IRIS, DNV GL and SINTEF. These are briefly described, and an assessment has been made of the status of the initiative in relation to expectations and recommendations in the *National Strategy for Digital Security* (2019), the Lysne Committee's report (2015) and the assignment letter from the Ministry of Labor and Social Affairs (2020). Most of the 18 reports provide recommendations for measures and further knowledge acquisition. Many of these are linked to the expectations and recommendations from the authorities, which the PSA can use in the continuation of the ICT security initiative.

# 1 Innledning

## 1.1 Formål

Formålet med dette dokumentet har vært å klargjøre hvordan IKT-sikkerhet i petroleumsindustrien blir regulert i gjeldende regelverk, inkludert å gi en oversikt over regelverket for de aktører som ikke er så kjent med det. Videre er bakgrunnen for og status på den store satsingen på IKT-sikkerhet i petroleumssektoren, som startet i 2018 og løper ut 2021, beskrevet.

Dokumentet skal bidra til at selskapene i petroleumsvirksomheten videreutvikler egen praksis knyttet til IKT-sikkerhet i industrielle IKT-systemer innenfor rammene av dagens regelverk.

## 1.2 Målgruppe

Målgruppen for dokumentet er alle som har et særlig ansvar for å beslutte, utforme, iverksette og følge opp IKT-sikkerhet i petroleumsvirksomheten, inkludert aktører som har begrenset kunnskap om Ptils regelverk.

## 1.3 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 IKT-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.

Prosjektet inngår i satsingen på IKT-sikkerhet i petroleumssektoren (2018-2021), hvor SINTEF for 2020 har utarbeidet seks rapporter, hvorav denne rapporten utgjør en av disse. Alle rapportene, inkludert rapporter utarbeidet i 2018 og 2019, er kort beskrevet i kapittel 6.2.

## 1.4 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. I tabellen nedenfor har vi valgt ut og samlet noen begreper knyttet til IKT-sikkerhet som er benyttet av overordnede myndigheter og Ptil. Ptil har laget en egen nettside "Ord og Uttrykk" som forklarer ord og uttrykk ut fra hvordan de blir brukt i petroleumsvirksomheten (se https://www.ptil.no/fagstoff/ord-og-uttrykk/). Merk at begrepene kan ha andre betydninger i vanlig språkbruk og i andre bransjer enn petroleumsvirksomheten.

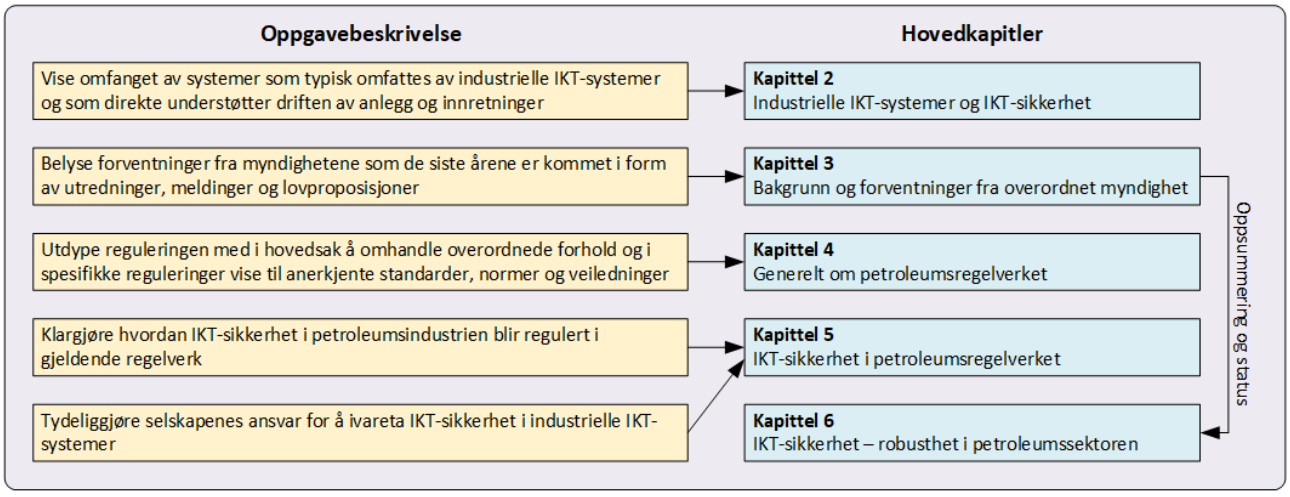
| Begrep | Definisjon/beskrivelse | Referanse |
|---|---|---|
| Definerte fare- og ulykkes-situasjoner (DFU-er) | Et representativt utvalg fare- og ulykkessituasjoner som brukes ved dimensjoneringen av beredskapen | Ptil, Veil. til AF § 73 |
| Barriere * | Tiltak som har til hensikt og funksjon enten 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, Ord og uttrykk |
| HMS | Et samlebegrep som i petroleumsvirksomheten dekker hensynet til mennesker, miljø og materielle verdier | Meld. St. 12 (2017–2018) |
| IKT-sikkerhet/Digital sikkerhet/Cybersikkerhet | 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 |

| Begrep | Definisjon/beskrivelse | Referanse |
|---|---|---|
| IKT-sikkerhetstiltak * | Tiltak for å sikre IKT-systemer og informasjon mot tilsiktede og utilsiktede hendelser | NOU2015: 13 |
| Informasjons- og kommunikasjonssystemer | Systemer som ivaretar behovet for innhenting, bearbeiding og formidling av data og informasjon | Ptil, SF § 15 |
| Integritet (av IKT-system) | At IKT-systemene, informasjonen som behandles i systemene, og tjenestene tilknyttet systemene ikke endres utilsiktet eller uautorisert | NOU 2018: 14 |
| Konfidensialitet (av IKT-system) | At IKT-systemene, informasjonen som behandles i systemene, og tjenestene tilknyttet systemene kun er tilgjengelige for dem som rettmessig skal ha tilgang | NOU 2018: 14 |
| Risiko | Konsekvensene av virksomheten med tilhørende usikkerhet | Ptil, Veil. til RF § 11 |
| Sikkerhet | Sikkerhet innebærer beskyttelse mot farer og trusler som kan forårsake uønskede hendelser | NOU2015: 13 |
| Sårbarhet | 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 |
| Tilgjengelighet (av IKT-system) | At IKT-systemene, informasjonen som behandles i systemene, og tjenestene tilknyttet systemene er tilgjengelig der og når det trengs for brukerne | NOU 2018: 14 |
| Trussel | En tilsiktet uønsket handling | NSM 2015 |
| Usikkerhet | Dreier seg om mangel på informasjon, manglende forståelse eller mangel på kunnskap | Meld. St. 12 (2017–2018) |

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

## 1.5 Rapportstruktur

Rapportstrukturen er vist i figur 1. Hovedkapitlene er relatert til oppgavebeskrivelsen fra Ptil.



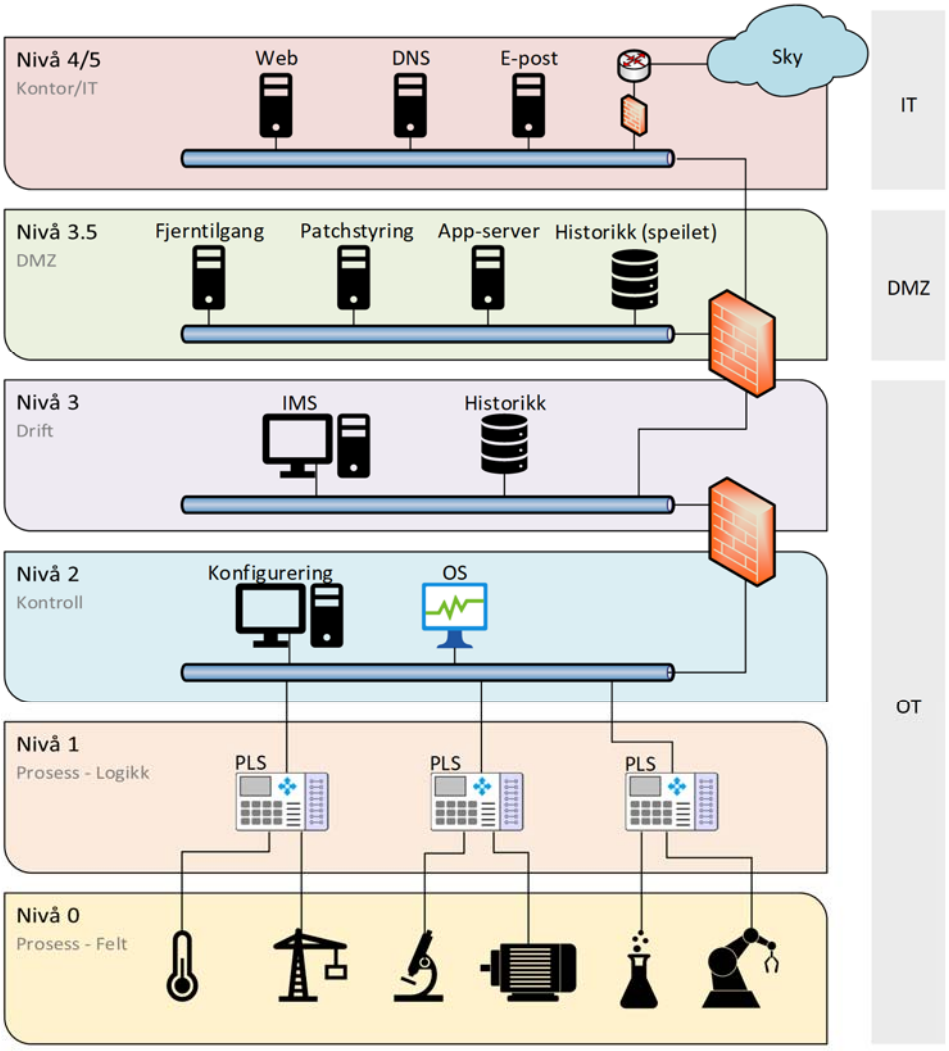

**Figur 1** Hovedkapitler relatert til oppgavebeskrivelsen

Forkortelser er gitt i vedlegg 1, Ptils utdyping av relevante regelverkskrav for IKT-sikkerhet i brev til næringen inngår i vedlegg 2, og en større versjon av figur 3 (sentrale dokumenter) er vist i vedlegg 3.

# 2 Industrielle IKT-systemer og IKT-sikkerhet

## 2.1 Hva er IT-systemer og OT-systemer?

I Ptils regelverk brukes informasjons- og kommunikasjonssystemer (IKT-systemer) om systemer som ivaretar behovet for innhenting, bearbeiding og formidling av data og informasjon (jf. SF § 15 *Informasjon*). Industrielle IKT-systemer brukes om OT-systemer (Operasjonell Teknologi eller Operasjonell IT) som medfører endringer i fysisk utstyr og prosesser så som kontroll- og overvåkingssystemer og sikkerhets-systemer.[1] Skillet mellom IT-systemer (kontorsystemer) og OT-systemer er illustrert med en forenklet versjon av Purdue-modellen[2] i figur 2 (SINTEF, 2021. *Grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer*).




**Figur 2** Forenklet Purdue-modell for illustrasjon av skillet mellom IT og OT

Litt forenklet går skillet mellom IT-systemene og OT-systemene ved demilitarisert sone (De-Militarized Zone (DMZ)).

[1] I (engelske) standarder og rammeverk brukes ulike begreper for industrielle IKT-systemer, slik som SAS (Safety and Automation System), ICS (Industrial Control System), IACS (Industrial Automation and Control System), og SCADA (Supervisory Control and Data Acquisition).

[2] Purdue-modellen ble utviklet av Theodore J. Williams og et konsortium ved Purdue Universitet (Williams, 1992). Figur 2 er en forenkling, og det eksakte innholdet blir ikke diskutert nærmere her.

Historisk har det i industrien vært et skille mellom administrative datasystemer som behandler data og informasjon (IT- og IKT-systemer) og datasystemer som kontrollerer produksjon (OT-systemer). OT-systemer på en innretning som tidligere var adskilt fra omverdenen, moderniseres og blir stadig mer komplekse og sammenkoblet med IT-systemer. Dette åpner opp for mer helhetlige løsninger, inkludert styring og overvåking fra land hvor OT-systemer har flere tilkoblingspunkter mot selskapets IT-systemer og forlengelser til eksterne nettverk som skyløsninger via internett.

Både IT-systemer og OT-systemer inkluderer datamaskiner, nettverk, operativsystemer, applikasjoner og andre programmerbare og konfigurerbare komponenter.

## 2.2 Oversikt over systemer som inngår

Tabell 1 gir eksempler på en mulig oppdeling av IT- og OT-systemer på faste og flyttbare innretninger.

**Tabell 1** Eksempler på en mulig oppdeling av IT- og OT-systemer på faste og flyttbare innretninger

| IT- og OT-systemer |
|---|
| IT-systemer |
| Systemer for ytelsesovervåking |
| Tilstandsovervåking (f.eks. roterende utstyr, ventiler, kraner) |
| Personalregistreringssystemer |
| Telekomsystemer*, PA-, alarm- og nødkommunikasjonssystemer, CCTV, radiokommunikasjon |
| Radar, helikopternavigasjon |
| Kollisjonsvarsling, værdata |
| OT-systemer |
| Styre- og kontrollsystemer for produksjonsinnretninger og landanlegg, inkludert applikasjonsenheter |
| Styre- og kontrollsystemer for boring og brønn, inkludert applikasjonsenheter |
| Sikkerhetssystemer (brann- og gassdeteksjon, nødavstengning, trykkavlastning, prosessnedstengning, brannvann-forsyning) |
| Sikkerhetskritiske marine system (posisjoneringssystem, ballastsystem, lensesystem, overvåkningssystem for vekt og stabilitet) |
| Systemer for å sikre deteksjon og kartlegging av akutt forurensning |
| Ventilasjonssystem |
| Kraftdistribusjon og kraftkontroll, inklusive nødkraft |
| Målesystemer ("metering") |
| Kran og løftesystemer |

* Kan også inngå som del av OT-systemer, eksempelvis ved fjerndrift

## 2.3 Hva er IKT-sikkerhet og OT-sikkerhet?

Begrepet IKT-sikkerhet har ikke en entydig definisjon. Det har grenseflater mot, eller oppfattes som synonymt med, informasjonssikkerhet, cybersikkerhet og digital sikkerhet (NOU 2018: 14 *IKT-sikkerhet i alle ledd*).

NOU 2018: 14 viser videre til at begrepene i noen dokumenter benyttes helt eller delvis synonymt, mens de i andre tillegges ulikt innhold. I tillegg har begrepet IKT-sikkerhet endret seg over tid. Tradisjonelt har beskyttelse av nettverk og systemer vært vektlagt, mens begrepet i dag i større grad omfatter informasjon som behandles i systemene og nettverkene, samt tjenestene som systemene leverer. NOU 2018: 14 legger til grunn en slik vid forståelse av begrepet, og viser til at sikkerhetsmålene for IKT-sikkerhet er *konfidensialitet*, *integritet* og *tilgjengelighet* (se definisjoner i kapittel 1.4).

Den enkelte virksomhet vil vekte sikkerhetsmålene ulikt ut fra hvilket formål den har eller skal understøtte, og hvilke krav og hvilket risikobilde den må forholde seg til. Basert på disse målene og vektingen av dem vil beskyttelsen omfatte teknologiske, menneskelige og organisatoriske barrierer, som skal motvirke uønskede digitale hendelser, evne til å oppdage slike hendelser og påfølgende reaksjon for å gjenopprette en sikker tilstand for IKT-systemene.

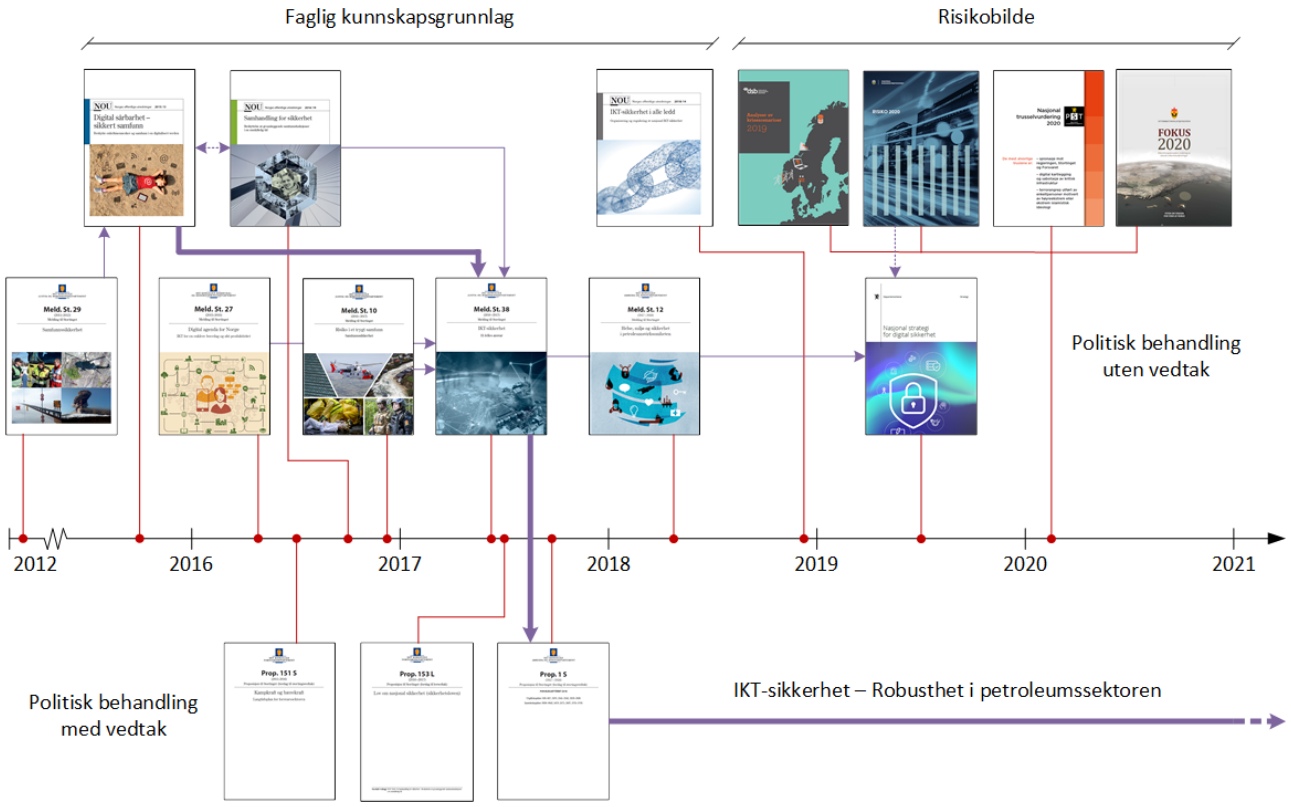
Det som har særlig fokus for Ptil er de industrielle IKT-systemene (OT-systemene) og dermed "OT-sikkerhet" hvor sikkerhetsmålet *tilgjengelighet* er viktigst. Et sikkerhetssystem må være tilgjengelig ved behov for beskyttelse av menneskers liv og helse, miljø og materielle verdier.

En nærmere utdyping er gitt i SINTEF (2021). *Grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer*.

# 3 Bakgrunn og forventninger fra overordnet myndighet

## 3.1 Oversikt og tidslinje (utredninger, meldinger og proposisjoner)

Et viktig bakteppe for arbeidet med IKT-sikkerhet, både innenfor petroleumssektoren og andre sektorer, er sentrale politiske dokumenter og det nasjonale og internasjonale risikobildet. Dette er illustrert i figur 3. En større versjon av figuren finnes i vedlegg 3. (Årstall i teksten angir hvilket dokument det vises til).




**Figur 3** Sentrale dokumenter for arbeidet med IKT-sikkerhet utgitt de siste årene[3]

Figuren er ikke uttømmende. Det er særlig vektlagt å ta med de dokumentene som direkte ledet til den store satsingen på *IKT-sikkerhet – Robusthet i petroleumssektoren* (2018-2021), vist med tykke piler.

NOU-er (Norges offentlige utredninger) benyttes ofte for å framskaffe et faglig kunnskapsgrunnlag, som så kan etterfølges av politisk behandling i meldinger til Stortinget (uten forslag til vedtak) eller proposisjoner til Stortinget (med forslag til vedtak: S – Stortingsvedtak og/eller L – Lovvedtak).

Det faglige grunnlaget utfylles også løpende av årlige rapporter om det nasjonale og internasjonale risikobildet, i figur 3 vist med de sist utgitte rapportene[4]. Disse utgis av Nasjonal sikkerhetsmyndighet (NSM), Politiets sikkerhetstjeneste (PST), og Etterretningstjenesten (E-tjenesten), mens Direktoratet for samfunnssikkerhet og beredskap (DSB) utgir rapporter med noen års mellomrom, siste gang i 2019. NSM, PST, E-tjenesten og KRIPOS leverer også klassifiserte rapporter til den norske regjeringen.

[3] NOU 2015: 13 *Digital sårbarhet – sikkert samfunn* (side 61) har en tidslinje med sentrale utredninger og IKT-sikkerhets-initiativer i Norge i perioden 2000-2015.
[4] NSM *Risiko 2020*, PST *Nasjonal trusselvurdering 2020*, E-tjenesten *Fokus 2020*, DSB *Analyser av krisescenarioer 2019*.

Risikobildet dekker alle aktuelle sektorer i Norge, inkludert petroleumssektoren og angrep rettet mot industrielle kontrollsystemer. NSM anser at statsadministrasjonene og foretakene innen forsvar, romfart, maritim, *petroleum* og kraft er i fare (NSM, 2020), og E-tjenesten viser til at nettangrep inkluderer operasjoner mot *industrielle kontrollsystemer* (E-tjenesten, 2020). Denne situasjonen er ikke ny, og baserer seg også på hendelser inntruffet før grunnlaget for satsingen på IKT-sikkerhet i petroleumssektoren ble lagt.

I tillegg til meldinger til Stortinget utgjør *Nasjonal strategi for digital sikkerhet* et viktig politisk dokument for arbeidet med IKT-sikkerhet. Dette ble sist utgitt i 2019 (første gang i 2003 og revidert i 2007 og 2012). Det kan bemerkes at det i forordet, av statsminister Erna Solberg, kun vises til to dokumenter. Disse er Digitalt sårbarhetsutvalgs (Lysneutvalgets) rapport om digitale sårbarheter i det norske samfunnet (NOU 2015: 13 *Digital sårbarhet – sikkert samfunn*) og oppfølgingen av denne gjennom den første stortingsmelding som utelukkende omhandler digital sikkerhet (Meld. St. 38 (2016-2017) *IKT-sikkerhet – et felles ansvar*).

Dette er de samme to dokumentene som direkte ledet til den store satsingen på *IKT-sikkerhet – Robusthet i petroleumssektoren* (2018-2021). Politisk vedtak og bevilgning ble gjort i forbindelse med behandlingen av statsbudsjettet for 2018 (Prop. 1 S (2017-2018) og Innst. 15 S (2017-2018)). I innstillingen fra arbeids- og sosialkomiteen fremgår det at satsingen går over fire år: *"… at det er viktig med en proaktiv innsats for å forebygge sårbarhet både i operative systemer og informasjonshåndteringssystemer. Derfor har regjeringen lagt til en fireårig styrking på IKT-sikkerhet på 5,9 mill. kroner i 2018."*

Anbefalinger gitt av Lysneutvalget (NOU 2015: 13) er beskrevet i kapittel 3.2, mens en statusvurdering av arbeidet med disse anbefalingene, beskrevet i Meld. St. 38 (2016-2017), er oppsummert i kapittel 3.3.

***Øvrige sentrale politiske dokumenter om IKT-sikkerhet***

*Nasjonal strategi for digital sikkerhet* (Regjeringen, 2019) omtaler også Meld. St. 27 (2015-2016) *Digital agenda for Norge* og Meld. St. 10 (2016-2017) *Risiko i et trygt samfunn*, samt Prop. 151 S (2015-2016) *Kampkraft og bærekraft* og Prop. 153 L (2016-2017) *Lov om nasjonal sikkerhet*.

Meld. St. 27 (2015-2016) omhandler regjeringens digitaliseringspolitikk hvor personvern og digital sikkerhet er sentrale elementer, og Meld. St. 10 (2016-2017) omhandler samfunnssikkerhet hvor digital sikkerhet inngår. Begge disse refereres til i tidligere nevnte Meld. St. 38 (2016-2017) *IKT-sikkerhet – et felles ansvar*.

Prop. 151 S (2015-2016) er langtidsplan for prioriteringer i forsvarssektoren, herunder digital sikkerhet. Denne omhandler også NSM, som rapporterer til forsvarsdepartementet (men er administrativt underlagt Justis- og beredskapsdepartementet). NSMs årlige risikobilde er ellers det eneste risikobildet som trekkes frem i *Nasjonal strategi for digital sikkerhet* (2019). I tillegg er både NSM og øvrige nevnte aktører som PST, E-tjenesten og DSB kort omtalt i et vedlegg til *Nasjonal strategi for digital sikkerhet* (2019). Her inngår også Nasjonal kommunikasjonsmyndighet (Nkom) som har et særskilt ansvar knyttet til sikkerhet og beredskap i elektroniske kommunikasjonsnett og -tjenester. Nkom utgir også årlige rapporter, siste gang EkomROS 2020 *Den digitale grunnmuren satt på prøve*, hvor man i tillegg til gjennomgang av hendelser peker på sentrale risikoområder for de kommende årene (Nkom, 2020).

Prop. 153 L (2016-2017) omhandler ny sikkerhetslov, som ble kunngjort 1. juni 2018 og trådte i kraft 1. januar 2019. Avklaringer om og i hvilken grad den vil berøre petroleumssektoren pågår. Ansvaret for hvilke virksomheter sikkerhetsloven skal gjelde for er lagt til hvert enkelt departement (NOU 2018: 14 *IKT-sikkerhet i alle ledd*). Prop. 153 L (2016-2017) viser til NOU 2015: 13 og Meld. St. 38, og også Meld. St. 10, men bygger direkte på Sikkerhetsutvalgets (Traavikutvalget) NOU 2016: 19 *Samhandling for sikkerhet*. NOU 2016: 19 er derfor lagt ved som særskilt vedlegg til Prop. 153 L (2016-2017).

Meld. St. 29 (2011-2012) *Samfunnssikkerhet* har et eget kapittel om IKT-sikkerhet og viser til ansvarsprinsipper som fortsatt er gjeldende, også innenfor petroleumssektoren. Meld. St. 12 (2017-2018) *Helse, miljø og sikkerhet i petroleumsvirksomheten* gir en status på arbeidet med IKT-sikkerhet. NOU 2018: 14 *IKT-sikkerhet i alle ledd* ser blant annet på regulering av IKT-sikkerhet, inkludert petroleumssektoren, hva man legger i begrepet IKT-sikkerhet (jf. kapittel 2.3) og hva man kan forstå med *forsvarlig* IKT-sikkerhet (se kapittel 6).

## 3.2 IKT-sikkerhetsforventninger til petroleumssektoren

*Nasjonal strategi for digital sikkerhet* (2019) viser til at stortingsmeldingen Meld. St. 38 (2016-2017) ikke uten grunn har navnet *"IKT-sikkerhet – et felles ansvar"* ved at vi alle har interesse av, og ansvar for, å sikre våre verdier. God digital sikkerhet er ikke en målsetting myndighetene kan nå alene. Det er næringslivet som har kompetansen og ressursene til å være en driver for digitalisering og innovasjon. Det vises til at *"å ivareta digital sikkerhet er først og fremst et virksomhetsansvar"*.

Dette er basert på, og utdypet i, Meld. St. 29 (2011-2012): *"IKT-sikkerhet er først og fremst et virksomhetsansvar. Dette følger av ansvarsprinsippet, som innebærer at den som har et ansvar for en virksomhet under normale forhold, også har et ansvar ved en krisesituasjon. I praksis innebærer dette at primæransvaret for sikring av informasjonssystemer og nettverk ligger hos eieren."*

Regjeringen har blant annet følgende tre forventninger (*Nasjonal strategi for digital sikkerhet*, 2019):

1. At ***virksomheter*** har en *risikobasert tilnærming* mot uønskede digitale hendelser, og bruker anerkjente rammeverk, standarder og styringssystemer for digital sikkerhet
2. At ***myndigheter og virksomheter*** *deler informasjon* om trusler, sårbarheter, hendelser og effektive tiltak med relevante aktører for å øke samfunnets robusthet mot uønskede digitale hendelser
3. At ***myndighetene*** gir råd, anbefalinger og veiledninger om digital sikkerhet for å gi virksomhetene et *kunnskapsgrunnlag* for sitt sikkerhetsarbeid

Lysneutvalget mener at sikkerhets- og tilsynsregimet gitt med hjemmel i petroleumsloven er for svakt og har følgende fire anbefalinger ("forventninger"):

1. Overføre sikkerhetstradisjonen innen HMS til det digitale området
2. Verdivurdere sektorens anlegg og IKT-systemer, og etablere regelverk for digitale sårbarheter
3. Tydeliggjøre rolle og kapasitet hos Ptil
4. Vurdere tilknytning til responsmiljø for IKT-hendelser

Disse forventningene retter seg både mot ***myndighetene - inklusive Ptil - og virksomhetene*** i sektoren.

Barrierer[5] og barrierestyring kan ses på som sentrale elementer i alle anbefalingene til Lysneutvalget, unntatt anbefaling nr. 3. Barrierestyring har vært arbeidet med systematisk i mange år innenfor HMS, og er eksempel på en sikkerhetstradisjon som kan overføres til det digitale området. For anbefaling nr. 2 viser Lysneutvalget til at forskriftene kun implisitt omfatter digital sikkerhet, og mener at tilsynsmyndigheten (Ptil) bør stille krav om at barrierer mot digitale sårbarheter skal være etablert. De anbefaler også at det i påvente av avklaringer om nedslagsfeltet til ny sikkerhetslov settes i gang et arbeid med verdivurdering og klassifisering av anlegg og IKT-systemer. Dette har mange likhetstrekk med utvelgelser og kritikalitetsvurderinger som gjøres i barrierestyringssammenheng. I anbefaling nr. 4 ligger det, i tillegg til tilknytning til responsmiljø, en anbefaling om at

[5] Lysneutvalget bruker begrepet barrierer, men det brukes sjelden i cybersikkerhetsstandarder og retningslinjer. I stedet brukes ofte begreper som IKT-sikkerhetstiltak, mottiltak, beskyttelser, løsninger og lignende.

sektoren gjennomfører øvelser i håndtering av uønskede IKT-hendelser, slik at man får testet og verifisert kvaliteten på barrierene.

Anbefaling nr. 3 retter seg mot at Petroleumstilsynet har begrenset kapasitet når det gjelder tilsyn med sektorenes IKT-sikkerhet og sårbarhet, og at Ptil derfor bør styrkes betraktelig på dette området.

## 3.3 Satsing på IKT-sikkerhet og bevilgninger/tildelingsbrev

Den store satsingen på IKT-sikkerhet – Robusthet i petroleumssektoren (2018-2021) er som nevnt foranlediget av Lysneutvalgets NOU 2015: 13 og Meld. St. 38 (2016-2017), og bevilgninger ble gitt i statsbudsjettet for 2018. Tildeling til Ptil gis i det årlige tildelingsbrevet fra Arbeids- og sosialdepartementet (ASD 2018, 2019, 2020), og som fortsetter i 2021. Tildelingsbrevene gjenspeiler også krav og forventninger fra ASD til Ptil.

I tildelingsbrevet for 2018 står det: *"Petroleumstilsynet må følge opp at aktørene i næringen iverksetter nødvendige sikringstiltak for å identifisere og hindre bevisste anslag mot innretninger, og at det er etablert en beredskap for å håndtere slike anslag. Dette gjelder også næringens IKT-teknologi og -systemer som kan utnyttes for å gjennomføre sikkerhetstruende handlinger. Petroleumstilsynets bevilgning er i 2018 styrket med 5 mill. kroner til økt oppfølging av IKT-sikkerhet. Petroleumstilsynet skal i tillegg til økt kunnskaps- og kompetanseutvikling og kartlegging av utfordringer også øke sin tilsynsoppfølging av IKT-sikkerhet. Satsingen innebærer også arbeid med styrking av beredskaps- og hendelseshåndtering og gjennomføring av øvelser."* (ASD, 2018).

Dette bidrar til en styrking av arbeidet med IKT-sikkerhet, uten at det er direkte knyttet til de enkelte anbefalingene til Lysneutvalget.

Mye av det samme står i tildelingsbrevet for 2019, og det avsluttes med: *"… Denne satsingen videreføres med 10 mill. kroner i 2019."* (ASD, 2019). I tildelingsbrevet for 2020 står det at: *"Petroleumstilsynet skal blant annet bidra til økt kunnskap om muligheter og risiko knyttet til IKT-sikkerhet og digitalisering."* (ASD, 2020).

***Status på arbeidet med IKT-sikkerhet forut for satsingen (før 2018)***

Arbeid med IKT-sikkerhet ble utført parallelt med etableringen av satsingen (2018-2021), også før Meld. St. 38 (2016-2017) forelå. Derfor ble det i denne stortingsmeldingen foretatt en statusvurdering opp mot de fire anbefalingene fra Lysneutvalget. Her vises det blant annet til at Ptil har bidratt til gjennomføring av egenvurderinger basert på NOROG 104 - *Norwegian Oil and Gas recommended guidelines on information security baseline requirements for process control, safety and support ICT systems*[6], og at DNV GL tok initiativ til det som ble en retningslinje for bruk av IEC 62443 (DNVGL-RP-G108 *Cyber security in the oil and gas industry based on IEC 62443*). Dette ble knyttet til Lysneutvalgets anbefaling nr. 1 (overføring av sikkerhetstradisjonen innen HMS til det digitale området) – tradisjon for samarbeid.

I forhold til Lysneutvalgets anbefaling nr. 2 (verdivurdering av sektorens anlegg og IKT-systemer og etablering av regelverk for digitale sårbarheter) vises det til at Ptil har utarbeidet og hatt på høring et forslag til presisering av HMS-forskriftenes anvendelse på sikringsområdet, herunder IKT-sikkerhet, men at man avventer oppfølgingen av ny sikkerhetslov før regelverksendringer fastsettes. Det vises også til tilsyn gjennomført av Ptil både med sikring generelt og IKT-sikring spesielt.

Når det gjelder behovet for å styrke Ptil på IKT-sikkerhetsområdet (Lysneutvalgets anbefaling nr. 3), vises det til at Ptil deltar i faglige fora, både nasjonalt og internasjonalt, for å sikre kompetanse og bygge nettverk.

[6] NOROG 104 vises til i veiledning til Innretningsforskriften § 34 a. Norsk olje og gass publiserte en ny versjon av NOROG 104-retningslinjen 5. desember 2016.

Videre vises det til at staben i Ptil er planlagt styrket innenfor IKT-sikkerhet. Ptil vurderer også muligheten for å utarbeide et årlig risikobilde innenfor IKT-sikkerhet i petroleumsnæringen.

Angående tilknytning til responsmiljø for IKT-hendelser (Lysneutvalgets anbefaling nr. 4) vises det til at KraftCERT er blitt tilgjengelig også for petroleumsvirksomheten, men at mange dekker behovet enten gjennom avtaler med NSM eller via moderselskapet i utlandet.

Både i forhold til Lysneutvalgets anbefaling nr. 1 og nr. 2 henvises det i stortingsmeldingen til at et viktig arbeid i tiden som kommer er at Ptil vil tydeliggjøre og videreutvikle regelverket for å ivareta de utfordringene som næringen står overfor ved endringer i trusselbildet og økt digitalisering. Dette innebærer blant annet å følge opp utviklingen av industristandarder som det kan refereres til i regelverket.

Den foreløpig siste stortingsmeldingen om helse, miljø og sikkerhet i petroleumsvirksomheten, (Meld. St. 12 (2017-2018)) fra 6. april 2018, gir en kort status på *IKT-sårbarhet og sikring*. Her fremgår det at Ptil har styrket sine ressurser på tilsyn med IKT-sikkerhet, jf. Lysneutvalget anbefaling nr. 3. Det understrekes at kravene til sikring, i likhet med HMS-regelverket, er utformet som funksjonskrav. Myndighetene mener at det totalt sett har vært en forbedring av sikringsarbeidet de siste årene, men at utviklingen krever en styrket oppfølging i næringen.

Status i forhold til annet relatert arbeid i næringen, slik som risikostyring og barrierestyring, er beskrevet i kapittel 5.

***Status på arbeidet med IKT-sikkerhet i satsingen (etter 2018)***
En status på arbeidet i IKT-satsingen (2018-2021) ved utgangen av 2020, dvs. etter tre fjerdedeler av satsingen er gjennomført, og som direkte relaterer seg til rapportene som er utgitt som del av satsingen, er beskrevet i kapittel 6. Rapportene bidrar til å gi både Petroleumstilsynet og virksomhetene et *kunnskapsgrunnlag* for sitt sikkerhetsarbeid, jfr. Regjeringens forventning nr. 3 i kapittel 3.2.

# 4 Generelt om petroleumsregelverket

## 4.1 Ptils rolle og ansvar

Beskrivelsen nedenfor av Ptils rolle og ansvar[7] er utdrag fra kronprinsregentens resolusjon om opprettelsen av Petroleumstilsynet (19. desember 2003). Ptil ble etablert med virkning fra 1. januar 2004.

Ptil skal legge premisser for, og følge opp, at aktørene i petroleumsvirksomheten holder et høyt nivå for helse, miljø, sikkerhet og beredskap, og gjennom dette også bidra til å skape størst mulig verdier for samfunnet. Oppfølgingen skal være systemorientert og risikobasert. Oppfølgingen skal komme i tillegg til, og ikke som erstatning for, den oppfølging av egen virksomhet som gjennomføres av næringen selv. Det skal være en balansert avveining mellom Ptils rolle som høyrisiko-/teknologitilsyn og arbeidstilsyn. Medvirkning og partssamarbeid inngår som viktige forutsetninger for og prinsipper i Ptils virksomhet.

Ptil skal videre drive informasjons- og rådgivningsvirksomhet overfor aktørene i virksomheten, etablere hensiktsmessige samarbeidsrelasjoner med andre HMS-myndigheter nasjonalt og internasjonalt, samt aktivt bidra til kunnskapsoverføring på helse- miljø- og sikkerhetsområdet i samfunnet generelt. Ptil kan supplere egen kompetanse ved å trekke på sakkyndig bistand fra andre offentlige etater, institusjoner og selskaper som har særskilt kompetanse, i samsvar med inngåtte samarbeidsavtaler.

Ptil skal føre tilsyn med sikkerhet, beredskap og arbeidsmiljø, samt ivareta oppgaven som koordinerende myndighet for HMS-myndighetene for petroleumsvirksomheten på norsk kontinentalsokkel (ca. 80 faste innretninger, 60 rigger, 300 havbunnsinnretninger samt 15400 km undervannsrørledninger) og for den samlede virksomheten ved åtte landanlegg (Kårstø, Kollsnes, Sture, Tjeldbergodden, Mongstad, Melkøya, Nyhamna og Slagentangen).

Regelverket stiller krav om at det til enhver tid skal opprettholdes effektiv beredskap med sikte på å møte fare- og ulykkessituasjoner som kan medføre tap av liv eller personskade, forurensning eller stor materiell skade, herunder skade forårsaket av eksempelvis terror eller sabotasje.

Ptil er delegert myndighet til å fastsette utdypende forskrifter for sikkerhet og arbeidsmiljø i virksomheten, og å fatte enkeltvedtak i form av tillatelser og samtykker, pålegg, tvangsmulkt, stansing av virksomheten, forbud, unntak mv.

Ptil skal ha myndighetsansvaret for teknisk og operasjonell sikkerhet, herunder beredskap, samt for arbeidsmiljø i alle faser av virksomheten; som ved planlegging, prosjektering, bygging, bruk og ved eventuell senere fjerning.

## 4.2 Prinsipper (funksjonsbasert, risikobasert, osv.)

HMS-regimet i norsk petroleumsvirksomhet anvender i hovedsak funksjonelle prinsipper og bygger på internkontroll, der selskapene har et selvstendig ansvar for å ivareta HMS-hensyn gjennom interne styringssystemer og prosesser. Dette innebærer krav om risikoanalyse, fastsetting av risikoakseptkriterier, risikovurdering og -evaluering, risikohåndtering og -reduksjon, jf. Engen-utvalget.[8]

Det at regelverket er funksjonsbasert kan ses på som et overordnet prinsipp, som videre medfører behov for at det også er risikobasert. Engen-utvalget viser ellers til at det i internasjonal sammenheng i stor grad anerkjennes

[7] I tillegg har Petroleumstilsynet fra 17. august 2020 blitt delegert forvaltningsansvaret for lov 4. Juni 2010 nr. 21 om fornybar energiproduksjon til havs (havenergilova) § 5-1.
[8] *Helse, arbeidsmiljø og sikkerhet i petroleumsvirksomheten*. Rapport fra partssammensatt arbeidsgruppe, 09/2017.

at et risikobasert, funksjonelt og målorientert regelverk, er en god måte å regulere industrier med potensial for storulykker.

***Funksjonsbasert***

HMS-regelverket for petroleumssektoren er i hovedsak utformet som funksjonskrav. I motsetning til detaljerte bestemmelser som stiller krav til spesifikke fremgangsmåter og handlinger, angir funksjonskrav hvilke resultater som skal oppnås, uten å beskrive hvordan. Hensikten bak den funksjonsbaserte tilnærming er blant annet å unngå detaljstyrende bestemmelser og synliggjøre aktørenes ansvar for å finne løsningene, og gjennom dette legge til rette for fleksibilitet i valg av metoder, fremgangsmåter, og teknologiutvikling. Denne fleksibiliteten utgjør handlingsrommet i regimet. Handlingsrommet legger til rette for at partene kan utfordre hverandre og myndighetene med hensyn til fortolkning og oppfølging av rammer og muligheter. På enkelte områder er imidlertid regelverket mer preskriptivt. Preskriptive bestemmelser brukes i hovedsak for å regulere områder der det er ønskelig med en bestemt løsning eller for å unngå tvil om minstekrav, jf. Engen-utvalget.

***Risikobasert***

Begrepet *risikobasert* benyttes mye, men betyr ikke at man utelukkende baserer seg på analyser og vurderinger av risiko for de beslutninger som tas. For å understreke dette brukes av og til begrepet *risikoinformert*, blant annet i Ptils notat om *Integrert og helhetlig risikostyring i petroleumsindustrien* (2018). Her vises det videre til at risikostyringen og regelverket er basert på tre hovedkategorier av måter å møte risiko, som er risiko-informert virksomhetsstyring, forsiktighetsprinsippet og føre-varprinsippet, og dialog mellom beslutnings-takere, fageksperter og utførende personell.

Forsiktighetsprinsippet kommer til anvendelse nettopp fordi risikovurderingene ikke er perfekte. Derfor har mange krav i regelverket, og oppmerksomhet om kunnskap og usikkerhet i forutsetninger, sin bakgrunn i forsiktighetsprinsippet. Et eksempel på at regelverket er forsiktighetsbasert er at en ikke kan sette til side spesifikke krav, for eksempel kravet om brannskille mellom hovedområder. Regelverket har altså en del spesifikke krav til robusthet. Føre-var er et spesialtilfelle av forsiktighetsprinsippet. Dette vises det til i veiledningen til RF § 11 *Prinsipper for risikoreduksjon*, hvor også risikobegrepet, inkludert usikkerhet, beskrives. Det vises her også til at beste tilgjengelige teknologi skal benyttes, det såkalte BAT-prinsippet.

***Andre prinsipper***

Under sin utredning om overordnede krav og prinsipper i regelverksregimet i petroleumsvirksomheten viser Engen-utvalget til at det følger av petroleumsloven at petroleumsvirksomheten skal foregå på forsvarlig måte, og at rettighetshavers organisasjon i Norge skal ha en struktur og størrelse som gjør at rettighetshaver til enhver tid kan fatte informerte beslutninger om sin virksomhet.

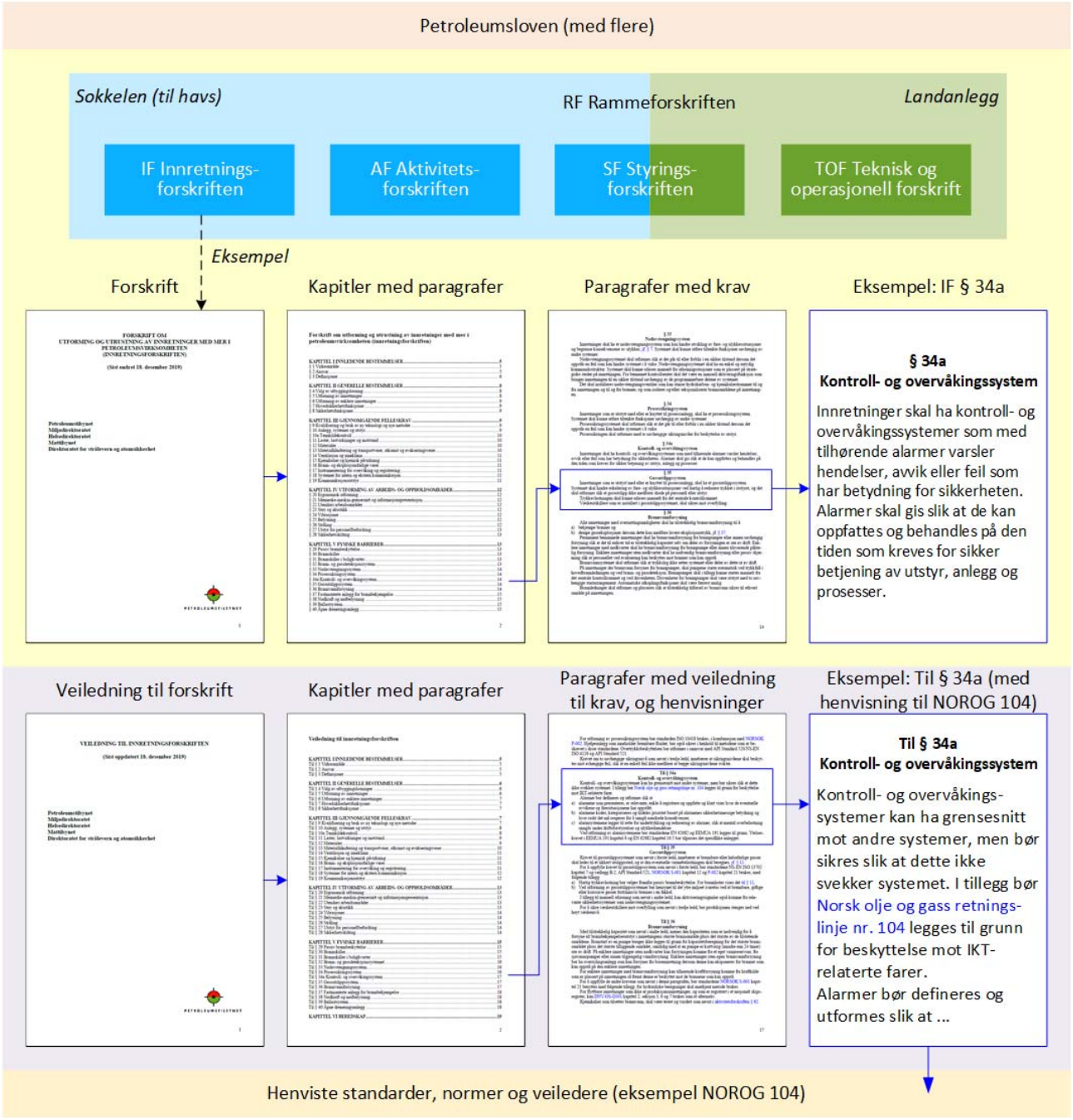
Dette er to av prinsippene som inngår i rammeforskriftens kapittel II – *Grunnleggende krav til helse, miljø og sikkerhet (§§ 9-16)*. RF § 9 *Bruk av prinsippene i kapittel II* viser til at dette omhandler *prinsipper*. Herunder inngår:

RF § 10 Forsvarlig virksomhet
RF § 11 Prinsipper for risikoreduksjon
RF § 12 Organisasjon og kompetanse
RF § 13 Tilrettelegging for arbeidstakermedvirkning
RF § 14 Bruk av norsk språk
RF § 15 God helse-, miljø- og sikkerhetskultur
RF § 16 Helsemessige forhold

I tillegg til forsvarlig virksomhet, jf. RF § 10, er det krav om kontinuerlig forbedring, jf. SF § 6 *Styring av helse, miljø og sikkerhet*, og SF § 23 *Kontinuerlig forbedring*.

## 4.3 Oppbygging og henvisning (standarder, normer og veiledere)

Figur 4 viser oppbyggingen av regelverket med fem forskrifter i medhold av petroleumsloven (og flere andre lover) og veiledninger til forskriftene, samt henvisning til standarder, normer og veiledere.




**Figur 4** Oppbyggingen av regelverket samt henvisning til standarder, normer og veiledere

Rammeforskriften (RF) er overordnet de andre forskriftene, dvs. styringsforskriften (SF), innretnings-forskriften (IF), aktivitetsforskriften (AF) og teknisk og operasjonell forskrift (TOF). RF og SF gjelder for både hav og land, IF og AF for innretninger til havs og TOF for landanlegg. Illustrasjonen av de fem forskriftene i figur 4 er basert på tilsvarende figur i DNV GL-rapport *Regelverk og tilsynsmetodikk* (2020).

De fem forskriftene dekker flere myndigheters ansvarsområde, og må sees i sammenheng med hverandre. I tillegg håndhever Ptil seks felles forskrifter til arbeidsmiljøloven. Hver av forskriftene består av et antall kapitler med paragrafer, som igjen består av ett eller flere krav (*"skal"*), eksempelvis to krav i IF § 34a *Kontroll- og overvåkingssystem*.

Veiledninger til forskriftene viser hvordan bestemmelser i en forskrift *kan* oppfylles. Forskriftene og veiledningene må sees i sammenheng for å få best mulig forståelse av hvordan forskriftskravet skal innfris.

Veiledningene viser på enkelte områder til industristandarder, som en anbefalt måte å oppfylle forskriftens krav på. Veiledningene til forskriftene er ikke rettslig bindende, og aktørene kan derfor velge andre løsninger. Dersom den ansvarlige aktøren velger å benytte den anbefalte løsningen, kan det normalt legges til grunn at forskriftenes krav er oppfylt. Hvis aktøren velger andre løsninger, som for eksempel andre standarder eller selskapsspesifikke prosedyrer, må de kunne dokumentere at den valgte løsningen er minst like god som, eller bedre enn, den anbefalte. Dette er beskrevet i RF § 24 *Bruk av anerkjente normer*.

Et eksempel på henvisning (*"bør"*) er i veiledningen til IF § 34 a *Kontroll- og overvåkingssystem*, hvor det blant annet henvises til NOROG 104. Se kapittel 5.2 for andre aktuelle standarder som aktørene *kan* vise til, men da må dokumentere at er minst like god som NOROG 104.

I den web-baserte versjonen av regelverket (https://www.ptil.no/regelverk/alle-forskrifter/) er det også lenke til *fortolkninger* av (enkelte paragrafer i) forskriftene. Fortolkningene er gitt samlet for hver forskrift. I tillegg er det lenke til tilsynsrapporter med avvik fra den aktuelle paragrafen.

## 4.4 Selskapenes ansvar og Ptils forventninger

I likhet med andre deler av norsk arbeidsliv, er det virksomhetene selv som er ansvarlig for HMS-nivået i virksomheten. Operatør og rettighetshaver er i tillegg pålagt en særskilt plikt til å følge opp at enhver som utfører arbeid for seg etterlever krav som er gitt i helse-, miljø- og sikkerhetslovgivningen (påseplikten).[9]

Petroleumsregelverket stiller krav om at aktørene skal etablere nødvendige styringssystemer for å påse at regelverket blir etterlevd i alle faser av virksomheten. Dette innebærer at aktøren skal organisere sin virksomhet for å sikre og verifisere at denne planlegges, utføres og vedlikeholdes i samsvar med myndighetenes regelverk. Myndighetenes oppfølging skal komme i tillegg til, og ikke som erstatning for aktørenes egen oppfølging (Engen-utvalget, 2017).

Ansvar og forventninger rettet spesifikt mot ivaretakelse av IKT-sikkerhet i industrielle IKT-systemer er beskrevet i kapittel 5.5.

[9] Jf. Petroleumsloven § 10-6 om plikt til å påse at bestemmelser blir overholdt, og RF § 7 *Ansvar etter denne forskriften.*

# 5 IKT-sikkerhet i petroleumsregelverket

## 5.1 Oversikt

IKT er ikke nevnt spesielt i petroleumsloven, og regelverket (forskriftene) er funksjonsbasert hvor IKT-sikkerhet generelt omfattes, men i liten grad nevnes eksplisitt. Unntak er veiledningene til SF § 29 som inkluderer IKT-hendelser, og IF § 34a som viser til NOROG 104 (jf. kapittel 4.3).

Ptil har informert næringen om en del paragrafer som er relevante for IKT-sikkerhet[10]. Disse er vist i tabell 2, sammen med de paragrafer Holteutvalget (NOU 2018: 14) vurderte som de mest relevante reglene, og innspill fra DNV GL (*Regelverk og tilsynsmetodikk*, 2020) på hvilke paragrafer hvor IKT-sikkerhet bør inngå.

**Tabell 2** Vurderinger av IKT-sikkerhet i petroleumsregelverket

| Forskrift | | NOU 2018: 14 | Ptil | DNV GL |
|---|---|---|---|---|
| **SF** | **Styringsforskriften** | | | |
| § 4 | Risikoreduksjon | x | x | x |
| § 5 | Barrierer | | | x |
| § 7 | Mål og strategier | x | | |
| § 8 | Interne krav | | x | x |
| § 14 | Kompetanse - veiledning | | | x |
| § 17 | Risikoanalyser og beredskapsanalyser | x | | x |
| § 25 | Samtykke | | | x |
| § 29 | Varsling og melding – veiledning | x | x | x |
| **IF** | **Innretningsforskriften (Teknisk og operasjonell forskrift)** | | | |
| § 8 | Sikkerhetsfunksjoner – veiledning (TOF § 10) | | | x |
| § 9 | Kvalifisering av bruk ny teknologi og nye metoder (TOF § 9) | | | x |
| § 18 | Systemer for intern og ekstern kommunikasjon – veil. (TOF § 22) | | | x |
| § 32 | Brann- og gassdeteksjonssystem – veiledning (TOF § 32) | | x | x |
| § 33 | Nødavstengningssystem – veiledning (TOF § 33) | | x | x |
| § 34 | Prosessikringssystem – veiledning (TOF § 34) | | x | x |
| § 34a | Kontroll- og overvåkingssystem – veiledning (TOF § 33a) | | x | x |
| **AF** | **Aktivitetsforskriften (Teknisk og operasjonell forskrift)** | | | |
| § 21 | Kompetanse | | x | x |
| § 23 | Trening og øvelser | | x | x |
| § 26 | Sikkerhetssystemer – veiledning | | | x |
| § 45 | Vedlikehold | | x | x |
| § 46 | Klassifisering – veiledning (TOF § 59) | | | x |
| § 47 | Vedlikeholdsprogram – veiledning | | | x |
| § 48 | Planlegging og prioritering | | x | x |
| § 73 | Beredskapsetablering – veiledning (TOF § 64) | | | x |
| § 74 | Felles bruk av beredskapsressurser – veiledning | | | x |
| § 75 | Beredskapsorganisasjon – veiledning (TOF § 65) | | | x |
| § 76 | Beredskapsplaner – veiledning (TOF § 66) | x | | x |
| § 77 | Håndtering av fare- og ulykkessituasjoner (TOF § 67) | x | | x |

[10] I brev av 18.9.2019 *Informasjon om håndtering av IKT-sikkerhetshendelser*. Se vedlegg 2.

Holteutvalget diskuterer de "mest relevante reglene" uten å indikere at disse bør adressere IKT-sikkerhet eksplisitt, mens Ptil gir sin forståelse av hvordan IKT-sikkerhet er relevant for 11 paragrafer. DNV GL viser til 26 paragrafer hvor det er relevant å ta inn Ptils presiseringer, behov for ytterligere klargjøringer, synliggjøring av IKT-sikkerhet, eller referering til standarder og retningslinjer.

Det å gi råd og veiledning om hvilke forskriftsparagrafer og krav som er spesielt relevante for IKT-sikkerhet er i tråd med forventninger og anbefalinger fra overordnet myndighet, jf. kapittel 3.2. Samtidig er det utfordringer med å kun nevne noen krav. Dette er ikke ensbetydende med at alle andre paragrafer og krav er irrelevante – virksomhetene må allikevel ha en helhetlig forståelse av regelverket.

Tilsvarende er det utfordrende å velge ut de paragrafer hvor IKT-sikkerhet bør inkluderes eksplisitt i regelverket, både i forhold til at dette blir "komplett" og at andre paragrafer kan oppfattes som mindre viktig for IKT-sikkerhet. Samtidig er IKT-sikkerhet (IKT-hendelser/-farer) allerede tatt inn i to paragrafer, og Lysneutvalget (NOU 2015: 13) var klar på at krav til IKT-sikkerhet bør gjøres tydelig i forskrifter.

## 5.2 Henvisning (IKT-standarder, normer og veiledere)

I gjeldende regelverk er NOROG 104 den eneste IKT-relaterte henvisningen til standarder, normer eller veiledere. Det henvises til NOROG 104 fra veiledningen til IF § 34 a *Kontroll- og overvåkingssystem*, og tilsvarende i veiledningen til TOF § 33a for landanlegg.

Her står det, i første avsnitt: *"Kontroll- og overvåkingssystemer kan ha grensesnitt mot andre systemer, men bør sikres slik at dette ikke svekker systemet. I tillegg bør Norsk olje og gass' retningslinje nr. 104 legges til grunn for beskyttelse mot IKT-relaterte farer."*

Det er en pågående diskusjon i næringen om regelverkshenvisning til andre IKT-relaterte standarder, normer og veiledere. Dette gjelder særlig IEC 62443-serien (standarder og tekniske rapporter som definerer prosedyrer for implementering av sikre industriautomatiserings – og kontrollsystemer (IACS/OT)), innenfor sikring som en parallell til IEC 61508/61511[11] innenfor sikkerhet og en tilhørende retningslinje, slik som DNVGL-RP-G108 eller lignende, som en parallell til NOROG 070[12]. Dette er diskutert i flere av rapportene utgitt som del av satsingen på IKT-sikkerhet, jf. kapittel 6.3.

Alle deler av IEC 62443-serien er ennå ikke utgitt i endelige utgaver, og Ptil følger opp utviklingen av denne og andre industristandarder som det kan refereres til i regelverket.

## 5.3 IKT-sikkerhet, risikostyring og barrierestyring

Notatene *Integrert og helhetlig risikostyring i petroleumsindustrien* (2018) og *Prinsipper for barrierestyring i petroleumsvirksomheten* (2017) gir synspunkter og føringer fra Ptil - "uttrykker Ptils ståsted" - selv om det presiseres at de ikke er en del av regelverket, og ikke innfører noen nye krav. Begge notatene omtaler IKT-sikkerhet.

***Integrert og helhetlig risikostyring i petroleumsindustrien***

Gode prosesser for styring av risiko er et premiss for at det funksjonsbaserte regelverket skal fungere. Risikostyring må inkludere sikringsrisiko: *"I en helhetlig tilnærming til risikostyring, er sikringsrisiko (tilsiktede uønskede handlinger) et av flere forhold en organisasjon må ta hensyn til. Kunnskapen om tilsiktede*

[11] IEC 61508 (2010). *Functional safety of electrical/electronic/programmable electronic safety related systems*.
IEC 61511 (2016). *Functional safety of safety instrumented systems for the process industry sector*.

[12] NOG 070 (2018). *Guidelines for the Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry (Recommended SIL requirements)*, June 2018.

*uønskede handlinger som fenomen, og metoder for å iverksette sikringstiltak, må være med i en helhetlig risikostyring."*

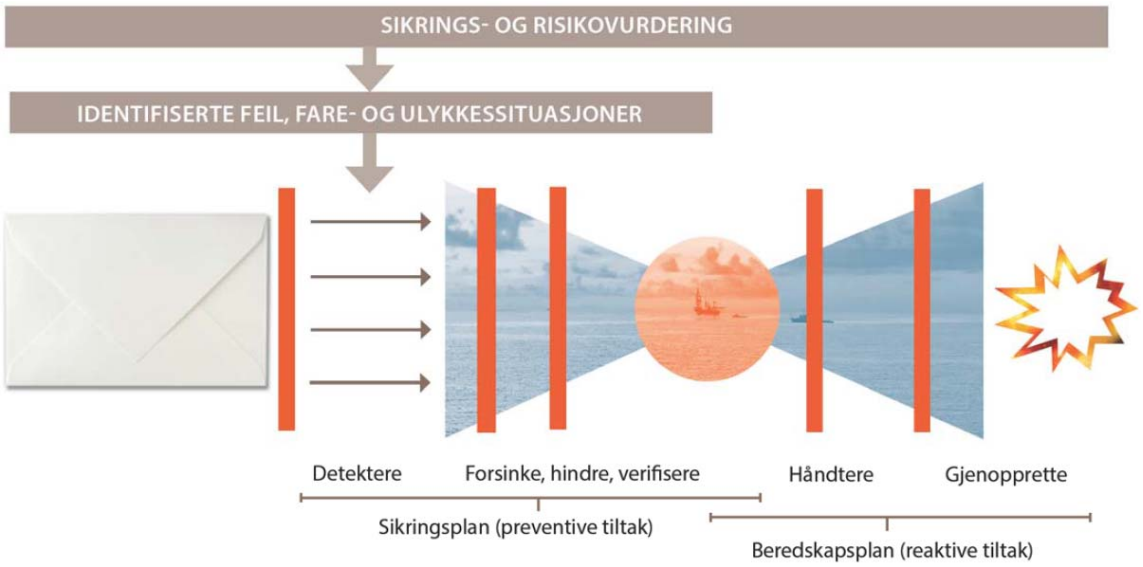
*"En utfordring som mange har i dag, er at det ikke bare er et skille mellom sikring og andre fagmiljøer, men også innad i fagmiljøet sikring. Vi har sett at det har vært skille mellom fagområder for fysisk sikring, personellsikring, IT (kontornettverket) og industrielle prosess- og sikkerhetssystemer (OT). Dette har ført til at man ikke får en helhetlig forståelse av risiko forbundet med sikring."*

Notatet diskuterer viktigheten av å vurdere og ta hensyn til usikkerhet. Her vises det til at det i sikringsrisiko-analyser er få som i dag beskriver kunnskapsstyrken eller usikkerheten, noe som fører til et urealistisk bilde av risiko, og at det tas beslutninger på feil grunnlag. Eksempelvis at det konkluderes med at alvorlige sikringshendelser har så lav sannsynlighet at man ser bort fra hendelsen, selv om kunnskapen som ligger til grunn er svak.

Ledelsesadferd er av stor betydning for en god sikkerhetskultur. Ptil viser til organisasjoner hvor ledelsen har satt sikring på agendaen slik at sikring får nødvendig oppmerksomhet, og bidrar til at det kontinuerlig jobbes med å identifisere og håndtere risiko i forbindelse med tilsiktende uønskede handlinger.

***Prinsipper for barrierestyring i petroleumsvirksomheten (barrierenotatet)***

SF § 5 *Barrierer* krever at det etableres barrierer for å identifisere forhold som kan føre til eller redusere muligheten for feil, fare og ulykkessituasjoner. IKT-hendelser (nettangrep) er ikke nevnt eksplisitt som eksempler i veiledningen til SF § 5, men barrierenotatet viser at Ptil inkluderer IKT-hendelser. I den siste versjonen av notatet (2017) er sikring inkludert som et anvendelsesområde med eksempler presentert i vedlegget. Figur 5 illustrerer en prinsippfigur for barrierer anvendt på sikring.




**Figur 5** Barriereprinsipper brukt for sikring (Ptil 2017)

*"Eksempler på barrierefunksjoner innen sikring er å avskrekke, oppdage, forsinke, nekte og verifisere eksistensen av et angrep, svare på trusselen og gjenopprette funksjonaliteten. Sikringsplanen dekker primært forebyggende og beskyttende tiltak, eller sannsynlighetsreduserende tiltak (for eksempel redusere sårbarhet), mens beredskapsplanen dekker de reaktive og konsekvensreduserende tiltakene. Det vil imidlertid være en viss overlapping mellom disse to planene samt tiltak som finner sted samtidig."* (Ptil 2017).

Det vises til at bruk av prinsippene for barrierestyring på sikringshendelser bidrar til en mer systematisk tilnærming til selve identifiseringen, etableringen og vedlikeholdet av barrierene.

## 5.4 IKT-sikkerhet og hendelser (DFU-er)

Beredskapen dimensjoneres ut fra et sett med definerte fare- og ulykkessituasjoner (DFU-er), som utgjør et representativt utvalg av fare- og ulykkessituasjoner, jf. AF § 73 *Beredskapsetablering*. Disse skal det øves på gjennom beredskapsøvelser. Det er imidlertid ingen fast liste i regelverket med fare- og ulykkessituasjoner som bør eller skal inngå som DFU-er, hverken IKT-hendelser eller andre hendelser.

Regelverket (AF § 73) viser til at utvalget av DFU-er skal være *representativt*. Dette er ikke noe som er statisk, men som påvirkes av teknologisk utvikling, samfunnsutvikling og trender i risiko-/trusselbildet, jf. kapittel 3.1. Listen med DFU-er, som det er etablert aksjonsplaner for i beredskapsplanen, må sees på som en *dynamisk* liste som oppdateres ved behov, slik at den er representativ til enhver tid. Dette gjelder både for IKT-hendelser og andre hendelser (som f.eks. bortfall av eksterne kommunikasjonsnettverk/nødkommunikasjon, jf. SINTEF, 2021. *Kommunikasjonssystemer for ekstern nødkommunikasjon*.).

IKT-hendelser er annerledes enn mange av de øvrige DFU-ene ved at de som håndterer hendelsene om bord på innretningen (eller landanlegget) i større grad er avhengig av bistand fra ekspertise på land, internt eller fra eksterne responsmiljø.

Ifølge DNV GL, så har omtrent halvparten av petroleumsaktørene definert en egen DFU for sikkerhets-hendelser i industrielle IKT-systemer, og flere aktører uttaler at de synes det ville vært nyttig å ha en etablert DFU.[13]

I tillegg til beredskapsøvelser knyttet til DFU-er er det krav til trening og øvelser jf. AF § 23 *Trening og øvelser*. Krav til trening og øvelser for håndtering av IKT-hendelser inngår ikke eksplisitt i regelverket, i likhet med de fleste andre temaer knyttet til IKT-sikkerhet, som nevnt i kap. 5.1. IKT-sikkerhet gjelder generelt, der det er relevant. Ptil har imidlertid presisert at AF § 23 *Trening og øvelser* også innbefatter IKT-hendelser: *"Kravet om trening og øvelser er også relevant for de som skal håndtere faresituasjoner i forhold til IKT-hendelse med de industrielle kontroll- og sikkerhetssystemene og samhandle med responsmiljøer."* [14]

## 5.5 Selskapenes ansvar for IKT-sikkerhet og Ptils forventninger

Operatører har et særlig ansvar for at virksomheten foregår på en forsvarlig måte og i samsvar med regelverket. De skal påse at alle som utfører arbeid for seg etterlever kravene i HMS-regelverket (påseplikt, jf. kapittel 4.4). Påseplikten kommer i tillegg til det enkelte selskapets plikt til å etterleve regelverket. Dette betyr, for eksempel, at operatører har ansvar for å følge opp at leverandører av OT-systemer etterlever krav til regelverket.

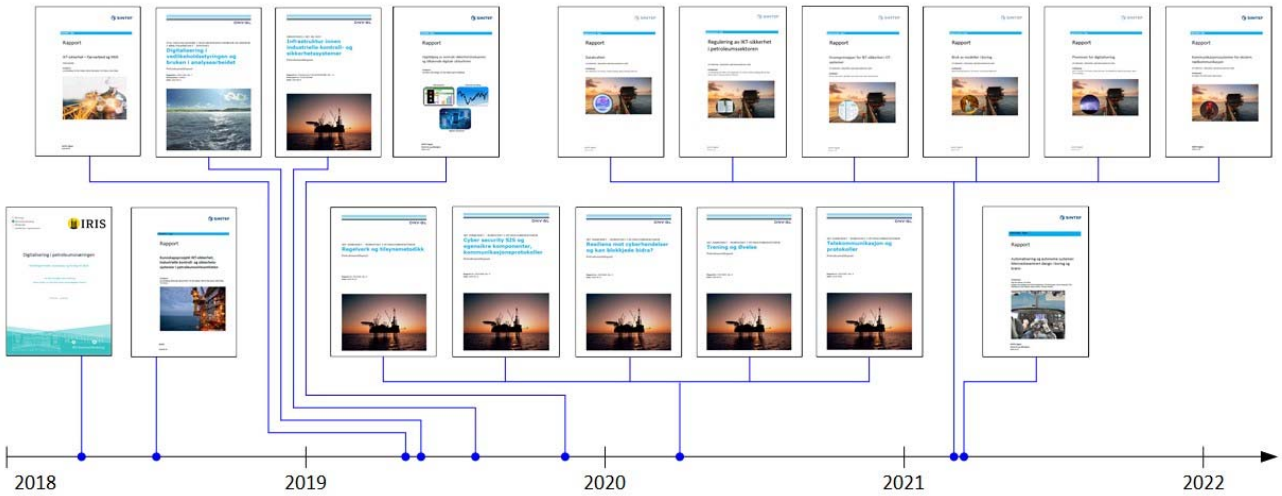
Til tross for økt automatisering, vil næringen i stor grad være avhengig av mennesker for å overvåke systemene og gripe inn dersom teknologien svikter. Systemer og utstyr skal utformes med sikte på å gjenvinne kontroll. Digitalisering kan bidra til forenkling og bedre beslutningsstøtte for involvert personell, men det kan også føre til endringer i roller og ansvar og innføring av nye kompetansekrav til personell. Den ansvarlige må sikre at utførende personell har nødvendig kompetanse tilpasset endrede arbeidsoppgaver og ny teknologi og at det blir satt av nok tid til opplæring, trening og øvelser.

[13] DNV GL-rapport *Trening og Øvelser* (2020).
[14] I brev av 18.9.2019 *Informasjon om håndtering av IKT-sikkerhetshendelser*.

# 6 IKT-sikkerhet – robusthet i petroleumssektoren

## 6.1 Oversikt og tidslinje

I løpet av de tre første årene i satsingen *IKT-sikkerhet – robusthet i petroleumssektoren* (2018-2021) har det blitt laget 18 rapporter for Ptil av IRIS, DNV GL og SINTEF, som illustrert i figur 6.




**Figur 6** Kunnskapsrapporter laget for Ptil innenfor IKT-sikkerhetssatsingen i perioden 2018-2020[15]

Rapportene er listet i tabell 3, med de eldste rapportene øverst, tilsvarende fra venstre mot høyre i figur 6.

**Tabell 3** Kunnskapsrapporter – rapporttitler, ansvarlig utgiver og dato

| Nr. | Tittel | Utgiver | Dato |
|---|---|---|---|
| 1 | Digitalisering i petroleumsnæringen | IRIS | Mars 2018 |
| 2 | Industrielle kontroll- og sikkerhetssystemer i petroleumsindustrien | SINTEF | Mai 2018 |
| 3 | IKT-sikkerhet – Fjernarbeid og HMS | SINTEF | April 2019 |
| 4 | Digitalisering i vedlikeholdsstyringen og bruken i analysearbeidet | DNV GL | April 2019 |
| 5 | Infrastruktur innen industrielle kontroll- og sikkerhetssystemer | DNV GL | Juni 2019 |
| 6 | Oppfølging av sentrale sikkerhetsfunksjoner og relaterte digitale sårbarheter | SINTEF | Nov. 2019 |
| 7 | Regelverk og tilsynsmetodikk | DNV GL | Februar 2020 |
| 8 | Cyber security SIS og egensikre komponenter, kommunikasjonsprotokoller | DNV GL | Februar 2020 |
| 9 | Resiliens mot cyberhendelser og kan blokkjede bidra? | DNV GL | Februar 2020 |
| 10 | Trening og Øvelse | DNV GL | Februar 2020 |
| 11 | Telekommunikasjon og protokoller | DNV GL | Februar 2020 |
| 12 | Datakvalitet ved digitalisering i petroleumssektoren | SINTEF | Januar 2021 |
| 13 | Regulering av IKT-sikkerhet i petroleumssektoren – *denne rapporten* | SINTEF | Januar 2021 |
| 14 | Grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer | SINTEF | Januar 2021 |
| 15 | Bruk av modeller i boring | SINTEF | Januar 2021 |
| 16 | Premisser for digitalisering og integrasjon IT – OT | SINTEF | Januar 2021 |
| 17 | Kommunikasjonssystemer for ekstern nødkommunikasjon | SINTEF | Januar 2021 |
| 18 | Automatisering og autonome systemer: Menneskesentrert design i boring og brønn | SINTEF | Januar 2021 |

[15] Rapportene fra DNV GL for 2019 ble gitt ut tidlig i 2020, og rapportene fra SINTEF for 2020 gis ut tidlig i 2021.

## 6.2 Fremskaffet ny kunnskap

### 6.2.1 Kort gjennomgang

Innholdet i de enkelte rapportene er kort gjengitt i tabell 4. Dette baserer seg blant annet på beskrivelsene gitt på Ptil sine hjemmesider.

**Tabell 4** Kunnskapsrapporter – kort beskrivelse av innhold

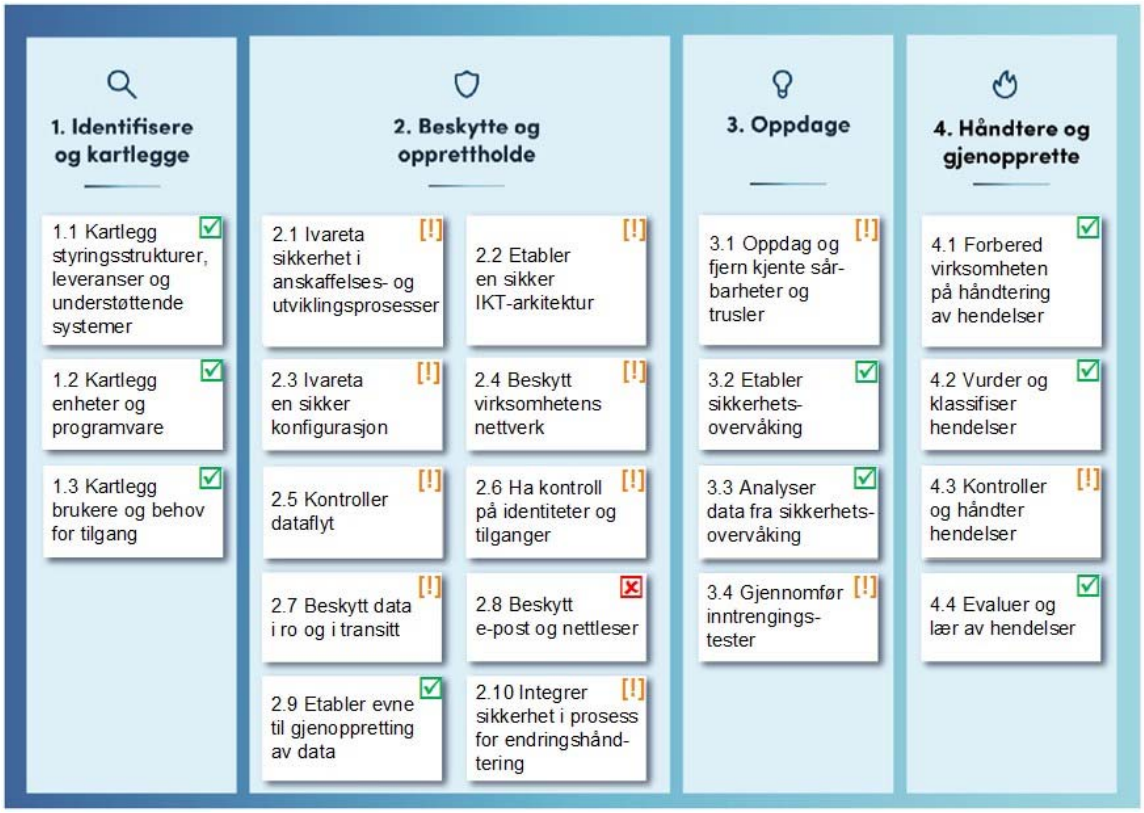
| Nr. | Tittel og innhold |
|---|---|
| 1 | **Digitalisering i petroleumsnæringen (IRIS, 5. mars 2018)**<br>Denne rapporten sammenfatter og analyserer kunnskap om positive og negative effekter av digitalisering for helse, miljø og sikkerhet (HMS) i petroleumsnæringen. Hovedmålet med prosjektet er å gi økt forståelse for utviklingstrender innen digitalisering, konsekvenser av digitalisering for menneske, teknologi og organisering, samt å komme med anbefalinger om strategier og tiltak for å følge dette opp. |
| 2 | **Industrielle kontroll- og sikkerhetssystemer i petroleumsindustrien (SINTEF, 29. mai 2018)**<br>Rapporten tar utgangspunkt i de endringene/driverne som påvirker risikobildet innen industrialisert kontrollteknologi (IKT) på innretningene på norsk sokkel. Formålet med rapporten er å gi økt forståelse for aktørenes egne og sektorvise oppfølginger av IKT-sikkerhet. Rapporten oppsummerer hovedinntrykk fra intervjuer med fageksperter, herunder fageksperter i nasjonale og internasjonale responsmiljø for IKT-sikkerhet (CSIRT/CERT). Rapporten gir også oversikt over relevante standarder og tilstøtende regelverk, samt aktuelle tilsynsmetoder for Ptil og selskapene selv. |
| 3 | **IKT-sikkerhet – Fjernarbeid og HMS (SINTEF, 5. april 2019)**<br>Rapporten har som hovedmål å presentere kunnskap om bruk av fjernarbeid på sokkelen. Rapporten belyser HMS-konsekvenser relatert til fjernarbeid på innretninger, landanlegg og borerigger. Hovedfokus er på arbeidsprosesser, prosedyrer og organisering. Rapporten gir også en oversikt over regelverk og retningslinjer på området. Rapporten er spisset mot operasjonell teknologi, det vil si teknologi som støtter, kontrollerer og overvåker industriell produksjon, kontroll- og sikkerhetsfunksjoner. |
| 4 | **Digitalisering i vedlikeholdsstyringen og bruken i analysearbeidet (DNV GL, 11. april 2019)**<br>Rapporten sammenstiller informasjon om status og utfordringer med hensyn til digitalisering i petroleumsvirksomheten basert på en gjennomgang av dokumenter og et møte med utvalgte selskaper. Den gir et grunnlag for valg av problemstillinger for nærmere utdyping i en hovedstudie. I tillegg danner den et kunnskapsgrunnlag som kan benyttes både internt i Ptil og i næringen. |
| 5 | **Infrastruktur innen industrielle kontroll- og sikkerhetssystemer (DNV GL, 21. juni 2019)**<br>Rapporten gir en oversikt over infrastrukturer innen industrielle kontroll- og sikkerhetssystemer som benyttes til styring og overvåkning av ulike prosesser og systemer på faste og flyttbare innretninger og på landanlegg. Rapporten beskriver kompleksitet til disse systemene, levetid, oppbygning av infrastruktur og grensesnitt mot ulike typer nettverk inklusive kommunikasjonsprotokoller fra instrument/sensornivå til styre og kontrollnivå (HMI). Det diskuteres også hvilken utvikling og mulig påvirkning Industrial Internet of Things (IIoT) og andre trender kan ha på slike systemer når disse kobles til nettverksstrukturen. |
| 6 | **Oppfølging av sentrale sikkerhetsfunksjoner og relaterte digitale sårbarheter (SINTEF, 7. november 2019)**<br>Rapporten sammenstiller informasjon om tilgjengeliggjøring av informasjon om tilstand og risiko, tilstandsovervåking av tidlig feilutvikling, og sårbarheter som de digitale løsningene kan medføre, og som kan påvirke sikkerheten. Målet med prosjektet er å bidra til at næringen styrker sin oppfølging av egne krav til tilstand for tekniske, operasjonelle og organisatoriske funksjoner som er viktige for sikkerheten, og sikrer at disse opprettholder sin påkrevde ytelse i alle faser av levetiden. |
| 7 | **Regelverk og tilsynsmetodikk (DNV GL, 24. februar 2020)**<br>Hensikten med dette delprosjektet har vært å vurdere om Ptils regelverk, slik det fremstår i dag, er hensiktsmessig i forhold til temaet IKT-sikkerhet og trusselbildet innenfor dette området. Tilsvarende om metodikken Ptil anvender for å utføre tilsyn med IKT-sikkerheten er hensiktsmessig gitt omfang av tilsynsobjekter og trusselbilde. |
| 8 | **Cyber security SIS og egensikre komponenter, kommunikasjonsprotokoller (DNV GL, 21. februar 2020)**<br>Delprosjektet har undersøkt IKT-sikkerhet i instrumenterte sikkerhetssystemer («Safety Instrumented System» (SIS)) og hvordan IKT-sikkerhet bygges inn i design av slike systemer og ivaretas i igangsetting og drift. En viktig del av leveransen er å vurdere hvordan sikkerhetsprinsippene beskrevet i IEC 61508/511 og IEC 62443 blir ivaretatt. Delleveransen beskriver også trender og utvikling innen industrielle IKT-systemer knyttet til nettverksbaserte komponenter. |

| Nr. | Tittel og innhold |
|---|---|
| 9 | **Resiliens mot cyberhendelser og kan blokkjede bidra? (DNV GL, 21. februar 2020)**<br>Rapporten presenterer hvordan resiliens, med tilhørende metoder, kan anvendes for å gjøre IKT-sikkerhet knyttet til industrielle IKT systemer mer robust. Videre diskuteres om prinsipper for IKT-sikkerhet kan anvendes i relasjon til blokkjedeteknologi og hvordan sikkerheten kan ivaretas og eventuelt styrkes ved implementering av blokkjede. Det diskuteres også, på bakgrunn av dagens informasjon og tilgjengelig forskning, om blokkjede kan bidra positivt til oppbygging av resiliens og muliggjøre nye metoder for å fremme cyber-sikkerhet knyttet til industrielle IKT-systemer (OT) og i skjæringspunktet mellom IT og OT. |
| 10 | **Trening og Øvelse (DNV GL, 21. februar 2020)**<br>Rapporten gir anbefalinger til krav og beste praksis relatert til trening og øvelse, inkludert beredskap for IKT-sikkerhetshendelser som er rettet mot industrielle IKT-systemer. Skillet mellom industriell IKT og IT utfordres og et angrep på administrative IT-systemer i kontornettet kan være et springbrett inn mot de industrielle IKT-systemene. Digitalisering medfører at informasjon fra de industrielle IKT-systemer i stadig større grad blir tilgjengelige i kontor-systemer. Rapporten gir derfor også anbefalinger som er rettet mot IT-systemer som indirekte vil kunne påvirke virksomhetens industrielle IKT-systemer. |
| 11 | **Telekommunikasjon og protokoller (DNV GL, 24. februar 2020)**<br>Rapporten beskriver utfordringer og risiko i dagens telekommunikasjonsløsninger. Trender innen telekommunikasjon som vil kunne påvirke sikkerheten i petroleumssektoren de kommende år blir beskrevet. Mulige tiltak for å øke robustheten i telekommunikasjonsløsningene er diskutert. Det er fokus på telekommunikasjonssystemer som er relevante for de tekniske installasjonene, både på land og til havs, samt forhold rundt mennesker, miljø og sikkerhet. Systemer DNV GL mener det er spesielle sikkerhetsutfordringer med, blir grundigere diskutert enn andre. |
| 12 | **Datakvalitet ved digitalisering i petroleumssektoren (SINTEF, januar 2021)**<br>Formålet med denne rapporten er 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 blir diskutert. Datakvalitet handler om å ha tilgang til riktige data når det er nødvendig. Datakvaliteten i IKT-systemer påvirkes av flere faktorer. Noen eksempler er dataintegritet, nøyaktighet i datainnsamling, pålitelighet i dataoverføring, miljø osv. |
| 13 | **Regulering av IKT-sikkerhet i petroleumssektoren (SINTEF, januar 2021)** – *denne rapporten*<br>Formålet med denne rapporten er å klargjøre hvordan IKT-sikkerhet i petroleumsindustrien blir regulert i gjeldende regelverk, herunder henvisning til anerkjente standarder, normer og veiledninger. Rapporten belyser også forventninger fra myndighetene, og gir en oversikt over og status på satsingen innenfor IKT-sikkerhet i petroleumsnæringen de siste årene. Rapporten skal bidra til at selskapene i petroleumsvirksomheten videreutvikler egen praksis knyttet til IKT-sikkerhet i industrielle IKT-systemer innenfor rammene av dagens regelverk. Den kan også benyttes som et underlag for et Ptil-notat om IKT-sikkerhet. |
| 14 | **Grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer (SINTEF, januar 2021)**<br>Hovedmålet med denne rapporten er å gi næringen økt forståelse av hvordan de kan bruke NSMs grunnprinsipper for IKT-sikkerhet (versjon 2.0) i industrielle IKT-systemer i petroleumsvirksomheten. Relevante elementer i NVEs kraftberedskaps-forskrift er også vurdert, og det er identifisert enkelttiltak i NIST CyberSecurity Framework (CSF) som ikke dekkes av grunnprinsippene, men som er relevante for OT-systemer. |
| 15 | **Bruk av modeller i boring (SINTEF, januar 2021)**<br>Formålet med denne rapporten er å diskutere utfordringer og muligheter ved bruk av modellkontrollerte operasjoner, spesielt knyttet til hvordan modellene og data fra modellene kan brukes på en sikker måte og hvordan IKT-sikkerhet ivaretas. Hovedfokus er på boreoperasjoner. Rapporten sammenfatter kunnskap og anbefalinger om sikker bruk av modellkontrollerte operasjoner. Det legges spesiell vekt på kvalitetssikring av modeller og data fra modeller samt IKT-sikkerhet og kommunikasjon mellom programvareløsninger i boreoperasjoner. |
| 16 | **Premisser for digitalisering og integrasjon IT – OT (SINTEF, januar 2021)**<br>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. Denne rapporten setter søkelyset på den pågående digitaliseringen av både gamle og nye innretninger og er basert på informasjon som er hentet inn fra bore- og operatørselskap. |
| 17 | **Kommunikasjonssystemer for ekstern nødkommunikasjon (SINTEF, januar 2021)**<br>Formålet med denne rapporten er å gi næringen økt forståelse av rollen til og sårbarheten av kommunikasjonsnettverk, spesielt i beredskapssituasjoner når en definert fare- og ulykkessituasjon (DFU) har inntruffet. Rapporten setter søkelyset på ekstern kommunikasjon mellom hav og land i beredskapssituasjoner, dvs. nødkommunikasjon mot land. |

| Nr. | Tittel og innhold |
|---|---|
| 18 | **Automatisering og autonome systemer: Menneskesentrert design i boring og brønn (SINTEF, januar 2021)**<br>Rapporten sammenfatter kunnskap om menneskelige faktorer i utvikling, testing, implementering og bruk av ny automatisert teknologi/autonome systemer som vil være nyttig/kritisk for bore- og brønnoperasjoner. Det er i denne rapporten samlet kunnskap og erfaring relatert til automatiserte systemer både i petroleumsbransjen og andre bransjer. Relevant regelverk og standarder for petroleumsnæringen er vurdert. |

### 6.2.2 Utdypende eksempel – NSMs grunnprinsipper tilpasset OT-systemer

*Grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer* (rapport nr. 14 i tabell 4) er et eksempel på kunnskapsgrunnlag som er fremskaffet som del av IKT-sikkerhetssatsingen. Resultatet er oppsummert i figur 7.




**Figur 7** Relevans av NSMs grunnprinsipper for IKT-sikkerhet for industrielle IKT-systemer

Formålet var blant annet å vurdere i hvilken grad tiltakene i NSMs grunnprinsipper for IKT-sikkerhet versjon 2.0 er relevante for industrielle IKT-systemer (OT-systemer) i petroleumsvirksomheten. Konklusjonen er at NSMs grunnprinsipper for IKT-sikkerhet i store trekk ("80 prosent") er relevante også for OT-systemer, men at det er enkelttiltak som må tilpasses eller utvides for å dekke behovet fullt ut.

Hver av de 21 grunnprinsippene vist i figur 7 inneholder mellom tre og ti tiltak. Dersom alle tiltak innenfor et grunnprinsipp i sin helhet er relevant for OT-systemer er dette angitt med ☑, dersom et eller flere tiltak er kun delvis relevant for OT-systemer, eller krever ytterligere tiltak er dette angitt med [!], og dersom et eller flere tiltak ikke er relevant for OT-systemer, er dette angitt med ☒. Kun ett (2.8 *Beskytt e-post og nettleser*) av de 21 grunnprinsippene er ikke relevant for OT-systemer, og for mange av de 11 grunnprinsippene som kun er delvis relevant er det kun ett eller få tiltak som ikke er relevant. Totalt er 96 av 118 tiltak i sin helhet relevant for OT.

Disse grunnprinsippene for IKT-sikkerhet i OT-systemer er spesielt interessante ut fra vurderingen om hva som er *forsvarlig* IKT-sikkerhet i NOU 2018: 14 *IKT-sikkerhet i alle ledd*, hvor Holte-utvalget forstår forsvarlig som et minimumsnivå på sikkerheten, og legger til grunn at forsvarlig IKT-sikkerhet kommer godt til uttrykk i NSMs grunnprinsipper for IKT-sikkerhet. En virksomhet som etterlever disse prinsippene, vil ha forsvarlig IKT-sikkerhet, hevder utvalget.

Dette vil også kunne gjelde OT-systemer når grunnprinsippene er tilpasset OT-systemer som beskrevet i rapport nr. 14, jf. tabell 4.

## 6.3 Status i forhold til myndighetenes forventninger og veien videre

I tabell 5 presenteres SINTEFs vurdering av status for satsingen på IKT-sikkerhet (ved utgangen av 2020), spesielt bidragene fra de 18 rapportene som har blitt utarbeidet som del av satsingen, men også generelt. Vurderingen er gjort i forhold til følgende forventninger og anbefalinger gitt i *Nasjonal strategi for digital sikkerhet* (S), i NOU 2015: 13 av Lysneutvalget (L), og i tildelingsbrev fra ASD (T):

S1. Benytte en risikobasert tilnærming og bruke anerkjente rammeverk, standarder og styringssystemer
S2. Dele informasjon om trusler, sårbarheter, hendelser og effektive tiltak
S3. Gi råd, anbefalinger og veiledninger om digital sikkerhet
L1. Overføre sikkerhetstradisjonen innen HMS til det digitale området
L2. Verdivurdere sektorens anlegg og IKT-systemer, og etablere regelverk for digitale sårbarheter
L3. Tydeliggjøre rolle og kapasitet hos Ptil
L4. Vurdere tilknytning til responsmiljø for IKT-hendelser
T1. Ptil skal i tillegg til økt kunnskaps- og kompetanseutvikling og kartlegging av utfordringer også øke sin tilsynsoppfølging av IKT-sikkerhet

**Tabell 5** SINTEFs vurdering av status for satsingen på IKT-sikkerhet i petroleumssektoren

| Nr. | Vurdering av status i forhold til myndighetenes forventninger | Relevante bidrag |
|---|---|---|
| S1 | Petroleumsregelverket er funksjonsbasert noe som fordrer risikobaserte/-informerte beslutninger, med henvisning til standarder og veiledninger. Regelverk og henvisning til bl.a. standarder omtales i rapport nr. 2, 7, 8, 13, 14 og 17. | Nr. 2, 7, 8, 13, 14 og 17 |
| S2 | De fleste rapportene inneholder informasjon om trusler, sårbarheter, hendelser og/ eller tiltak. En utfordring er gradert informasjon unntatt offentlighet. | De fleste |
| S3 | Alle rapportene bidrar med råd, veiledning og anbefalinger til næringen. | Alle |
| L1 | Lysneutvalget gir en generell anbefaling om å overføre sikkerhetstradisjonen innen HMS til det digitale området, og Meld. St. 38 (2016-2017) gir en status på dette. I vurderingen til Lysneutvalget som ledet til anbefalingen pekes det mot barrierer. Barrierer innenfor IKT-sikkerhet inngår i vedlegg til Ptils barrierenotat, jfr. kap. 5.3. Barrierer omtales i rapport nr. 6, 7, 8, 10, 13 og 17. | Nr. 6, 7, 8, 10, 13 og 17 |
| L2 | Lysneutvalget peker på at krav til IKT-sikkerhet bør gjøres tydelig i forskrifter. Meld. St. 38 (2016-2017) viser til at Ptil vil tydeliggjøre og videreutvikle regelverket, herunder å følge opp utviklingen av standarder som kan refereres til i regelverket. Vurdering av regelverket, herunder diskusjoner rundt IEC 62443, inngår blant annet i rapport nr. 2, 7, 8, 13 og 17. | Nr. 2, 7, 8, 13 og 17 |
| L3 | Kapasiteten er økt, som angitt i Meld. St. 12 (2017-2018). Alle rapportene har bidratt til å øke kompetansen, og det samme har deltakelse i ulike faglige fora. Blant annet har det blitt etablert et nytt faglig forum CDS[1] hvor Ptil deltar i arbeidsutvalget. | Alle ift. kompetanse / Nr. 7 ift. kapasitet |
| L4 | Status på vurdering av tilknytning til responsmiljø beskrives i Meld. St. 12 (2017-2018). Responsmiljø er diskutert i rapport nr. 2 og 7. | Nr. 2 og 7 |

| Nr. | Vurdering av status i forhold til myndighetenes forventninger | Relevante bidrag |
|---|---|---|
| T1 | Alle rapportene har bidratt til økt kunnskapsutvikling, og mange har kartlagt utfordringer. Tilsynsmetodikk er behandlet i rapport nr. 2 og 7, mens status på tilsyns-oppfølging er beskrevet i Meld. St. 38 (2016-2017) og Meld. St. 12 (2017-2018). | Alle ift. kunnskap / Nr. 2 og 7 ift. tilsyn |

[1] CDS – Cybersikkerhet av Datamaskinbaserte Sikkerhetssystemer (https://www.sintef.no/projectweb/cds-forum/)

Tabell 5 gir noen hovedinntrykk og er ikke uttømmende. De fleste rapportene gir anbefalinger for tiltak og videre kunnskapsinnhenting. Mange av disse er knyttet til forventningene og anbefalingene til myndighetene angitt ovenfor, og som Ptil kan benytte i fortsettelsen av IKT-sikkerhetssatsingen.

## Referanser


Arbeids- og administrasjonsdepartementet (2003). *Kronprinsregentens resolusjon om etablering av Petroleumstilsynet og fastsettelse av instruks om koordinering av tilsynet med helse, miljø og sikkerhet i petroleumsvirksomheten på norsk kontinentalsokkel, og på enkelte anlegg på land.*

Arbeids- og sosialdepartementet (2017). *Helse, arbeidsmiljø og sikkerhet i petroleumsvirksomheten*. Rapport fra partssammensatt arbeidsgruppe, 09/2017. (Engen-utvalget).

Arbeids- og sosialdepartementet (2018). *Tildelingsbrev 2018 – Petroleumstilsynet*.

Arbeids- og sosialdepartementet (2019). *Tildelingsbrev 2019 – Petroleumstilsynet*.

Arbeids- og sosialdepartementet (2020). *Tildelingsbrev 2020 – Petroleumstilsynet*.

Direktoratet for samfunnssikkerhet og beredskap (2019). *Analyser av krisescenarioer*.

DNVGL-RP-G108 (2017). *Cyber security in the oil and gas industry based on IEC 62443.* Sept. 2017.

DNV GL (2019). *Digitalisering i vedlikeholdsstyringen og bruken i analysearbeidet*. 11.04.2019.

DNV GL (2019). *Infrastruktur innen industrielle kontroll- og sikkerhetssystemer*. 21.06.2019.

DNV GL (2020). *Regelverk og tilsynsmetodikk*. 24.02.2020.

DNV GL (2020). *Cyber security SIS og egensikre komponenter, kommunikasjonsprotokoller*. 21.02.2020.

DNV GL (2020). *Resiliens mot cyberhendelser og kan blokkjede bidra?* 21.02.2020.

DNV GL (2020). *Trening og Øvelse*. 21.02.2020.

DNV GL (2020). *Telekommunikasjon og protokoller*. 24-02-2020.

Etterretningstjenesten (2020). *Fokus 2020*.

IEC 62443-serien (2020). *Industrial communication networks - IT security for networks and systems.*

IEC 61508 (2010). *Functional safety of electrical/electronic/programmable electronic safety related systems*.

IEC 61511 (2016). *Functional safety of safety instrumented systems for the process industry sector*.

Innst. 15 S (2017–2018). *Innstilling til Stortinget fra arbeids- og sosialkomiteen* Prop. 1 S (2017–2018).

IRIS (2018). *Digitalisering i petroleumsnæringen. Utviklingstrender, kunnskap og forslag til tiltak*. 5.3.2018.

Meld. St. 29 (2011–2012). *Samfunnssikkerhet*.

Meld. St. 27 (2015–2016). *Digital agenda for Norge – IKT for en enklere hverdag og økt produktivitet*.

Meld. St. 10 (2016–2017). *Risiko i et trygt samfunn*.

Meld. St. 38 (2016–2017). *IKT-sikkerhet – et felles ansvar*.

Meld. St. 12 (2017-2018). *Helse, miljø og sikkerhet i petroleumsvirksomheten.*

Nasjonal kommunikasjonsmyndighet (2020). *EkomROS 2020*.

Nasjonal sikkerhetsmyndighet (2015). *Helhetlig IKT-risikobilde 2015.*

Nasjonal sikkerhetsmyndighet (2020). *Risiko 2020*.

Nasjonal sikkerhetsmyndighet (2020). *NSMs grunnprinsipper for IKT-sikkerhet. Versjon 2.0*. 15.04.2020.

NIST (2014). *Framework for Improving Critical Infrastructure Cybersecurity.*

NOG 070 (2018). *Guidelines for the Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry (Recommended SIL requirements)*, June 2018.

NOROG 104 (2016). *Norwegian Oil and Gas recommended guidelines on information security baseline requirements for process control, safety and support ICT systems*

NOU 2000: 24. *Et sårbart samfunn – Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet*.

NOU 2006: 6. *Når sikkerheten er viktigst – Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner*.

NOU 2015: 13. *Digital sårbarhet – sikkert samfunn.* (Lysne-utvalget).

NOU 2016: 19. *Samhandling for sikkerhet – Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid*. (Traavik-utvalget).

NOU 2018: 14. *IKT-sikkerhet i alle ledd*. (Holte-utvalget).

Petroleumsloven (lov 29. november 1996 nr. 72 om petroleumsvirksomhet).

Petroleumstilsynet (2019). *Informasjon om håndtering av IKT-sikkerhetshendelser.* Brev av 18.9.2019.

Petroleumstilsynet "Ord og Uttrykk". https://www.ptil.no/fagstoff/ord-og-uttrykk/
Petroleumstilsynet (2017). *Prinsipper for barrierestyring i petroleumsvirksomheten. Barrierenotat 2017*.
Petroleumstilsynet (2018). *Integrert og helhetlig risikostyring i petroleumsindustrien.*
Petroleumstilsynet (2019). *Aktivitetsforskriften.* 18.12.2019.
Petroleumstilsynet (2019). *Veiledning til aktivitetsforskriften*. 18.12.2019.
Petroleumstilsynet (2019). *Innretningsforskriften*. 18.12.2019.
Petroleumstilsynet (2019). *Veiledning til innretningsforskriften*. 18.12.2019.
Petroleumstilsynet (2019). *Styringsforskriften*. 26.04.2019.
Petroleumstilsynet (2019). *Veiledning til styringsforskriften*. 26.04.2019.
Petroleumstilsynet (2019). *Rammeforskriften*. 26.04.2019.
Petroleumstilsynet (2019). *Veiledning til rammeforskriften*. 26.04.2019.
Petroleumstilsynet (2019). *Teknisk og operasjonell forskrift*. 18.12.2019.
Petroleumstilsynet (2019). *Veiledning til teknisk og operasjonell forskrift*. 18.12.2019.
Politiets sikkerhetstjeneste (2020). *Nasjonal trusselvurdering 2020*.
Prop. 1 S (2017–2018). *Justis- og beredskapsdepartementet*.
Prop. 151 S (2015–2016). *Kampkraft og bærekraft*.
Prop. 153 L (2016–2017). *Lov om nasjonal sikkerhet (sikkerhetsloven).*
Regjeringen (2019). *Nasjonal strategi for digital sikkerhet*.
SINTEF (2018). *Kunnskapsprosjekt IKT-sikkerhet; Industrielle kontroll- og sikkerhetssystemer i petroleumsvirksomheten*. 29.05.2018.
SINTEF (2019). *IKT-sikkerhet - Fjernarbeid og HMS*. 05.04.2019.
SINTEF (2019). *Oppfølging av sentrale sikkerhetsfunksjoner og relaterte digitale sårbarheter*. 07.11.2020.
SINTEF (2021). *Datakvalitet ved digitalisering i petroleumssektoren*. Januar 2021.
SINTEF (2021). *Regulering av IKT-sikkerhet i petroleumssektoren.* Januar 2021.
SINTEF (2021). *Grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer*. Januar 2021.
SINTEF (2021). *Bruk av modeller i boring*. Januar 2021.
SINTEF (2021). *Premisser for digitalisering og integrasjon IT – OT*. Januar 2021.
SINTEF (2021). *Kommunikasjonssystemer for ekstern nødkommunikasjon*. Januar 2021.
SINTEF (2021). *Automatisering og autonome systemer: Menneskesentrert design i boring og brønn.* Januar 2021.
Williams, T.J. (1992). *The Purdue enterprise reference architecture: a technical guide for CIM planning and implementation*. Research Triangle Park, NC: Instrument Society of America.

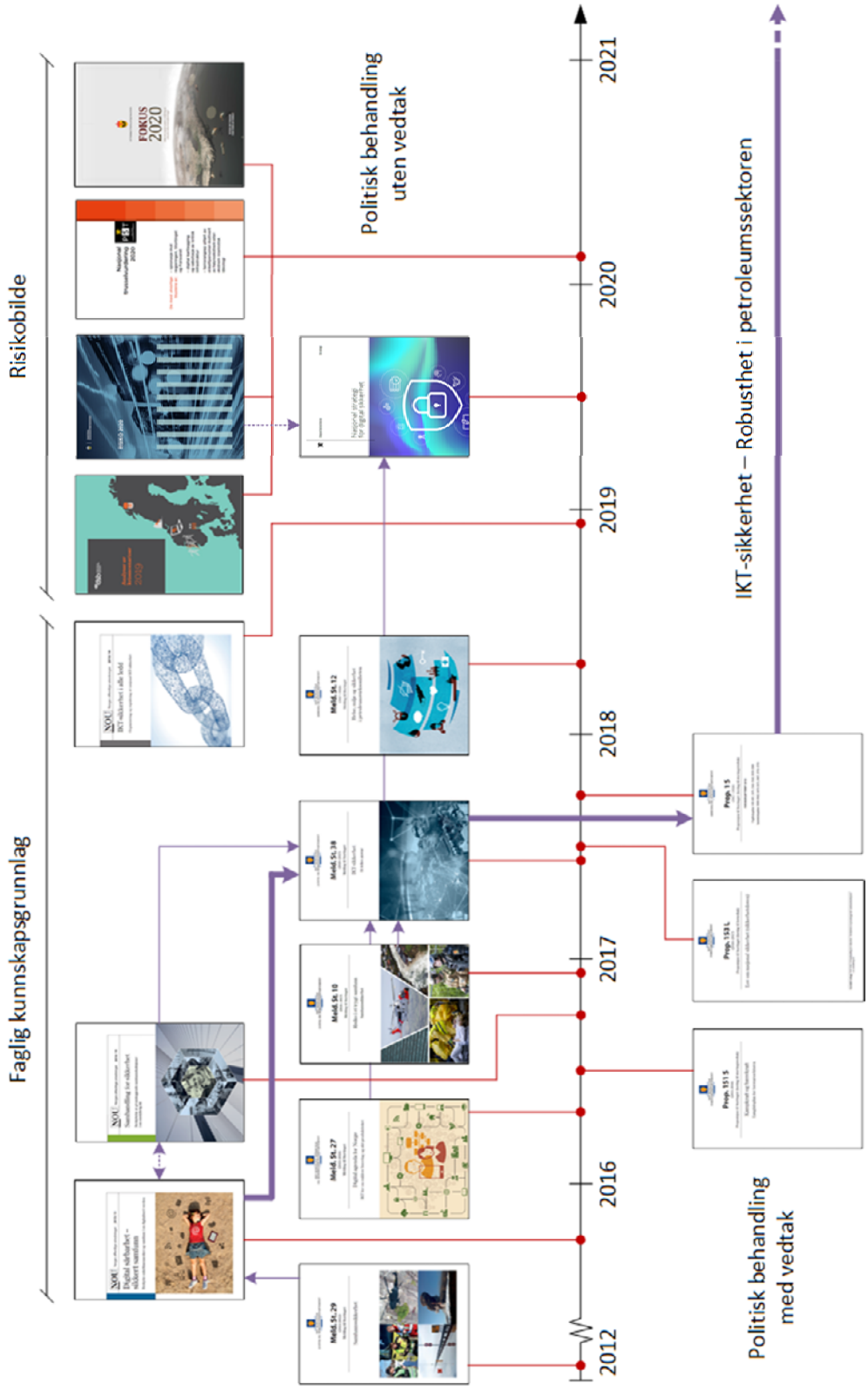
## Vedlegg 1: Forkortelser

| Forkortelse | Beskrivelse |
|---|---|
| AF | Aktivitetsforskriften |
| ASD | Arbeids- og sosialdepartementet |
| BAT | Best Available Technologi |
| CCTV | Closed Circuit Television |
| CDS | Cybersikkerhet av Datamaskinbaserte Sikkerhetssystemer |
| CERT | Computer Emergency Response Team |
| CSF | Cybersecurity Framework |
| CSIRT | Cyber Security Incident Response Team |
| DFU | Definert fare- og ulykkessituasjon |
| DMZ | De-Militarized Zone |
| DSB | Direktoratet for samfunnssikkerhet og beredskap |
| Ekom | Elektronisk kommunikasjon |
| E-tjenesten | Etterretningstjenesten |
| HMI | Human Machine Interface – menneske-maskin grensesnitt |
| HMS/HSE | Helse, miljø og sikkerhet/Health, Safety and Environment |
| IACS | Industrial Automation and Control Systems |
| IEC | International Electrotechnical Commission |
| IF | Innretningsforskriften |
| IKT/ICT | Informasjons- og kommunikasjonsteknologi/Information and Communication Technology |
| IMS | Information Management System |
| IT | Informasjonsteknologi |
| Meld. St. | Melding til Stortinget (Stortingsmelding) |
| MTO | Menneske, teknologi og organisasjon |
| NIST | National Institute of Standards |
| NKOM | Norsk kommunikasjonsmyndighet |
| NOG/NOROG | Norsk olje og gass |
| NORSOK | NORsk Sokkels Konkurranseposisjon |
| NOU | Norges Offentlige Utredninger |
| NSM | Nasjonal sikkerhetsmyndighet |
| OS | Operatørstasjon |
| OT | Operasjonell teknologi |
| PA | Public Address - personvarsling |
| PLS | Programmerbar Logisk Styring |
| Prop. | Proposisjon |
| PST | Politiets sikkerhetstjeneste |
| Ptil/PSA | Petroleumstilsynet/Petroleum Safety Authority |
| RF | Rammeforskriften |
| ROS | Risiko og sårbarhet |
| SAS | Safety and Automation System – sikkerhets- og automasjonssystem |
| SF | Styringsforskriften |
| SIS | Sikkerhetsinstrumenterte systemer |
| TOF | Teknisk og operasjonell forskrift |

## Vedlegg 2: Ptils utdyping av relevante regelverkskrav for IKT-sikkerhet

| Forskrift og forskriftstekst | Ptils forståelse |
|---|---|
| Styringsforskriften § 4 Risikoreduksjon:<br><br>Den ansvarlige [skal] velge tekniske, operasjonelle og organisatoriske løsninger som reduserer sannsynligheten for at det oppstår skade, feil og fare- og ulykkessituasjoner. | Dette innebærer at det velges løsninger for IKT-sikkerhet som reduserer sannsynligheten for IKT-angrep som forårsaker skade, feil eller faresituasjoner. |
| Styringsforskriften § 8 Interne krav:<br><br>Den ansvarlige skal sette interne krav som konkretiserer krav i regelverket, og som bidrar til å nå målene for helse, miljø og sikkerhet. | Det må settes krav til hvordan IKT-sikkerhet håndteres, både teknisk, operasjonelt og organisatorisk. |
| Innretningsforskriften §§ 32-34 Sikkerhetssystemer:<br><br>Systemet skal kunne utføre tiltenkte funksjoner uavhengig av andre systemer.<br><br>Veiledning: systemet kan ha grensesnitt mot andre systemer dersom det ikke kan bli negativt påvirket som følge av systemsvikt, feil eller enkelthendelser i disse systemene. | Kravet om at grensesnitt mot andre systemer ikke skal påvirke negativt innebærer at heller ikke IKT-angrep skal hindre at systemene kan utføre tiltenkte funksjoner. |
| Innretningsforskriften §§ 34a Kontroll- og overvåkingssystem:<br><br>Veiledning: I tillegg bør Norsk olje og gass retningslinje nr. 104 legges til grunn for beskyttelse mot IKT-relaterte farer. | Veiledningen viser til anerkjent retningslinje, men også andre standarder kan benyttes. |
| Aktivitetsforskriften § 21 Kompetanse:<br><br>Den ansvarlige skal sikre at personellet til enhver tid har den kompetansen som er nødvendig for å kunne utføre aktivitetene i henhold til helse-, miljø- og sikkerhetslovgivningen. I tillegg skal personellet kunne håndtere fare- og ulykkessituasjoner. | Kravet om kompetanse er også relevant for de som skal håndtere faresituasjoner i forhold til IKT-hendelse med de industrielle kontroll- og sikkerhets-systemene. |
| Aktivitetsforskriften § 21 Trening og øvelser:<br><br>Den ansvarlige skal sikre at det utføres nødvendig trening og nødvendige øvelser, slik at personellet til enhver tid er i stand til å håndtere operasjonelle forstyrrelser og fare- og ulykkessituasjoner på en effektiv måte | Kravet om trening og øvelser er også relevant for de som skal håndtere faresituasjoner i forhold til IKT-hendelse med de industrielle kontroll- og sikkerhetssystemene og samhandle med responsmiljøer. |
| Aktivitetsforskriften § 45 Vedlikehold:<br><br>Den ansvarlige skal sikre at innretninger eller deler av disse holdes ved like, slik at de er i stand til å utføre sine krevde funksjoner i alle faser av levetiden. | Oppdatering og patching av programvare når det oppdages sikkerhetssvakheter er å forstå som vedlikehold. |
| Aktivitetsforskriften § 48 Planlegging og prioritering:<br><br>Det skal utarbeides en samlet plan for utføring av vedlikeholdsprogram og korrigerende vedlikeholdsaktiviteter | Kravet om planlegging innebærer en systematikk for hvordan selskapet har kontroll på hvilke oppdateringer som er relevante og hvilke utstyrskomponenter som må ha vedlikeholdsprogram. |

## Vedlegg 3: Større versjon av figur 3 – sentrale dokumenter



Teknologi for et bedre samfunn

**www.sintef.no**