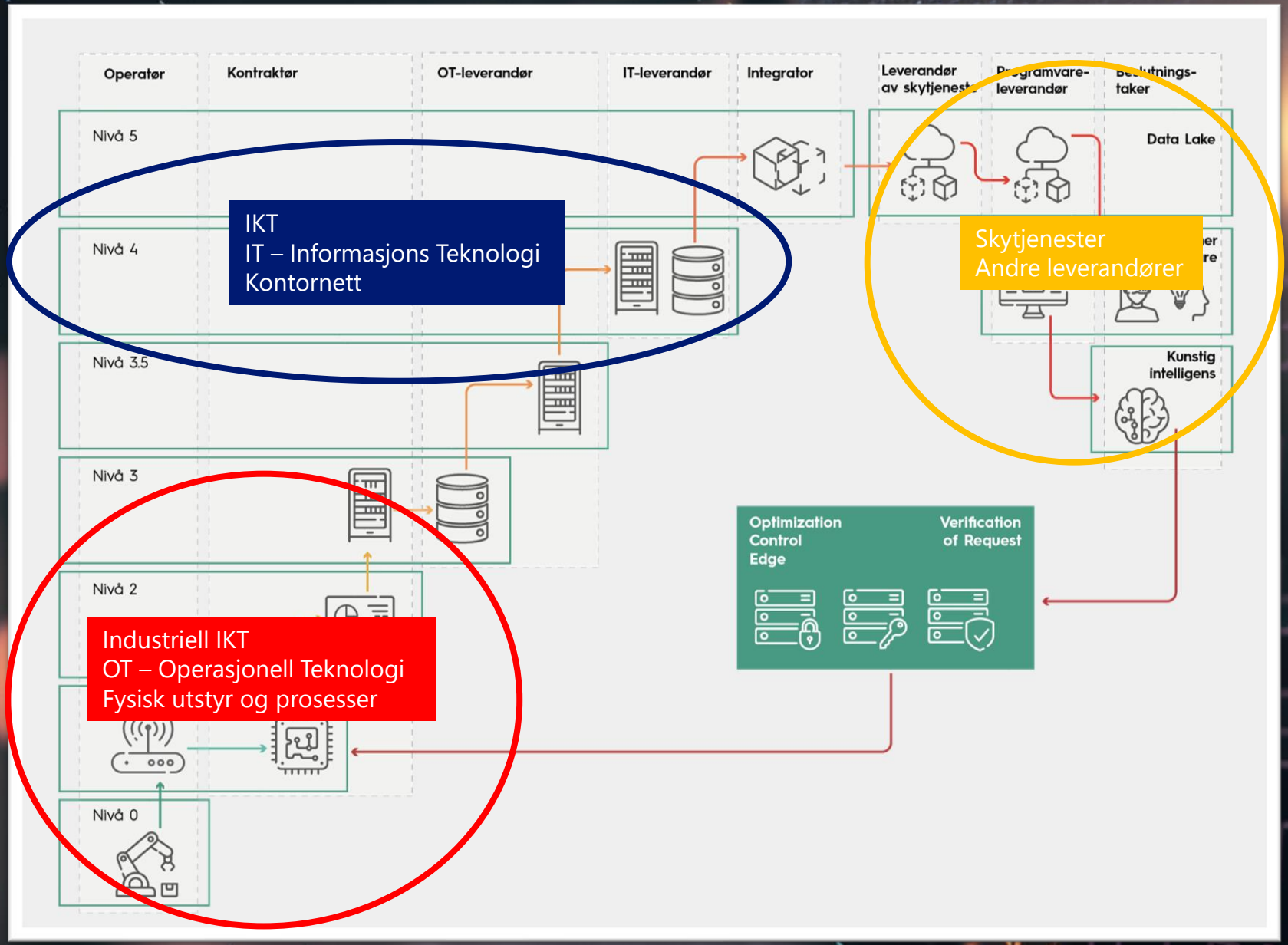
Havtil
Havindustritilsynet

# Industriell IKT-sikkerhet

**Operasjonell Teknologi (OT)**

**Benny Thorrud, Prosessintegritet**

# Industriell IKT, IKT og skytjenester



## Industriell IKT-sikkerhet

- Kunnskapsinnhenting
- Tilsyn
- Sektor Respons Miljø (SRM)
- Nettverk og samhandlingsarena

# Kunnskapsinnhenting

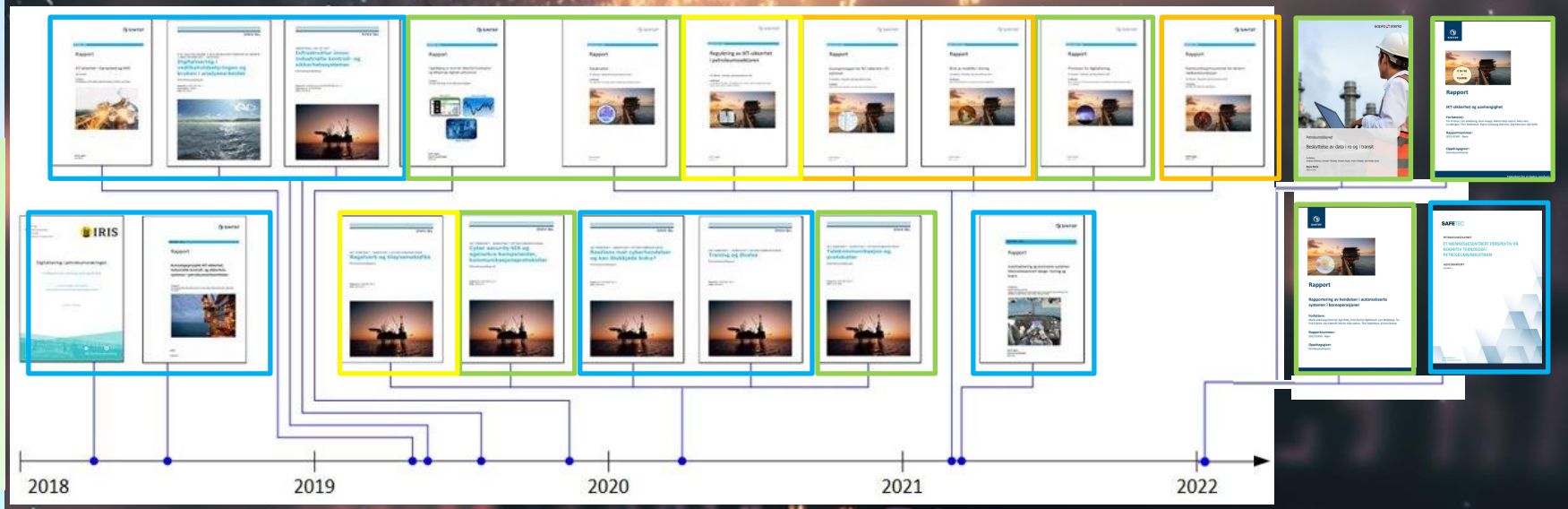
2018 til 2022 gjennomførte Havtil en større kunnskapsinnhenting hvor 20 rapporter rettet mot industrielle IKT-systemer ble publisert

HVA
- IKT-sikkerhet – Fjernarbeid og HMS
- Digitalisering i vedlikeholds-styringen og bruken i analysearbeidet
- Infrastruktur innen industrielle kontroll- og sikkerhetssystemer
- Digitalisering i petroleumsnæringen
- Industrielle kontroll- og sikkerhets-systemer i petroleumsindustrien
- Resiliens mot cyberhendelser og kan blokkjede bidra?
- Trening og Øvelse
- Automatisering og autonome systemer: Menneskesentrert design i boring og brønn
- Kognitive teknologier

HVOR
- Oppfølging av sentrale sikkerhets-funksjoner og relaterte digitale sårbarheter
- Datakvalitet ved digitalisering i petroleumssektoren
- Cyber security SIS og egensikre komponenter, kommunikasjonsprotokoller
- Premisser for digitalisering og integrasjon IT – OT
- Telekommunikasjon og protokoller
- Beskyttelse av data i ro og transit
- Automatisert rapportering
- IIKT-sikkerhet og uavhengighet

HVORDAN
- Grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer
- Bruk av modeller i boring
- Kommunikasjonssystemer for ekstern nødkommunikasjon

REGULERING
- Regelverk og tilsynsmetodikk
- Regulering av IKT-sikkerhet i petroleumssektoren

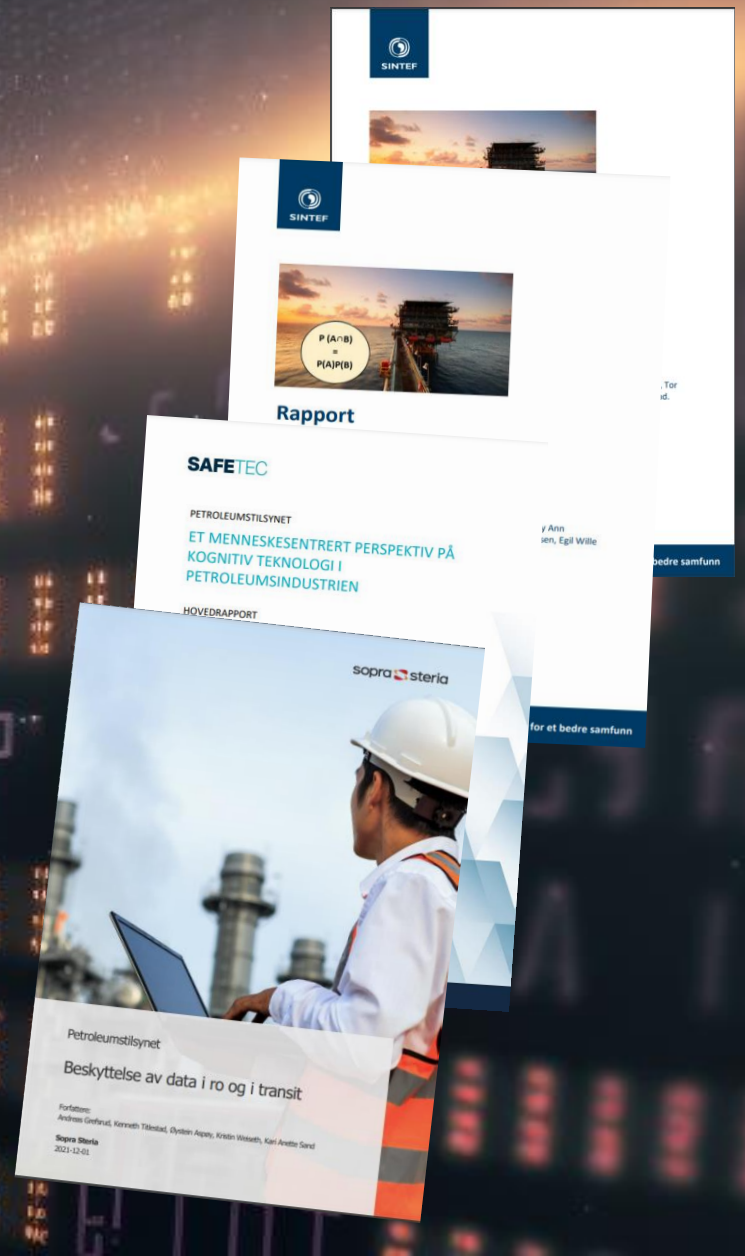



*Utvidet illustrasjon, basert på i Sintefrapporten *Regulering av IKT-sikkerhet i petroleumssektoren*

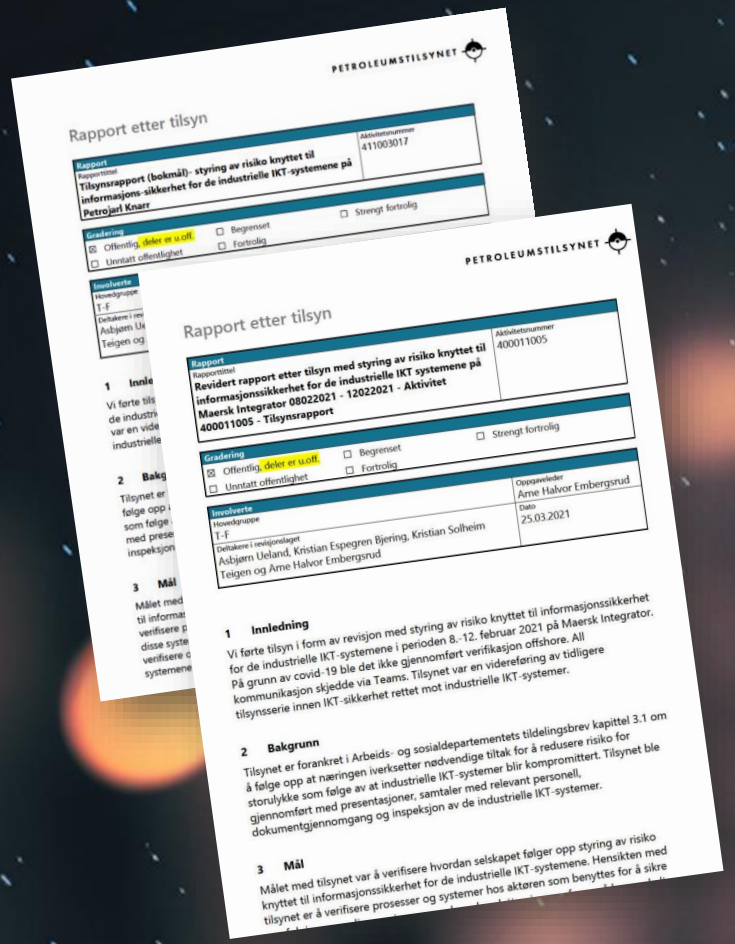
https://www.havtil.no/utforsk-fagstoff/fagstoff/fagartikler/2021/ikt-sikkerhet-i-industrielle-systemer/

# Rapportenes verdi

- Mye av underlaget til rapportene er basert på intervjuer av aktører i næringen
  - Kunnskapsutvikling eller statusbeskrivelse?
- Stor verdi i å sammenfatte og tilgjengeliggjøre kunnskap
  - Setter IKT/industriell IKT på dagsorden
  - Utgangspunkt for deling og videre dialog
- Digital sikkerhet har flere ulike dimensjoner
  - Identifisering, beskyttelse, oppdage, respondere, gjenopprette
  - Helhetlig tilnærming til verdi, sårbarhet og trussel
- Identifikasjon av grunnleggende eller gjennomgående utfordringer og problemstillinger i næringen
- Forberedelse og innspill til fremtidige/pågående oppgaver



# Industriell IKT – tilstand og tilsyn


PETROLEUMSTILSYNET

Rapport etter tilsyn

Rapport
Rapporttittel
Revidert rapport etter tilsyn med styring av risiko knyttet til informasjonssikkerhet for de industrielle IKT systemene på Maersk Integrator 08022021 - 12022021 - Aktivitet 400011005 - Tilsynsrapport

Aktivitetsnummer
400011005

Gradering
☒ Offentlig, deler er u.off.
☐ Begrenset
☐ Strengt fortrolig
☐ Unntatt offentlighet
☐ Fortrolig

Involverte
Hovedgruppe
T-F
Deltakere i revisjonslaget
Asbjørn Ueland, Kristian Espegren Bjering, Kristian Solheim Teigen og Arne Halvor Embergsrud

Oppgaveleder
Arne Halvor Embergsrud

Dato
25.03.2021

1 Innledning

Vi førte tilsyn i form av revisjon med styring av risiko knyttet til informasjonssikkerhet for de industrielle IKT-systemene i perioden 8.-12. februar 2021 på Maersk Integrator. På grunn av covid-19 ble det ikke gjennomført verifikasjon offshore. All kommunikasjon skjedde via Teams. Tilsynet var en videreføring av tidligere tilsynsserie innen IKT-sikkerhet rettet mot industrielle IKT-systemer.

2 Bakgrunn

Tilsynet er forankret i Arbeids- og sosialdepartementets tildelingsbrev kapittel 3.1 om å følge opp at næringen iverksetter nødvendige tiltak for å redusere risiko for storulykke som følge av at industrielle IKT-systemer blir kompromittert. Tilsynet ble gjennomført med presentasjoner, samtaler med relevant personell, dokumentgjennomgang og inspeksjon av de industrielle IKT-systemer.

3 Mål

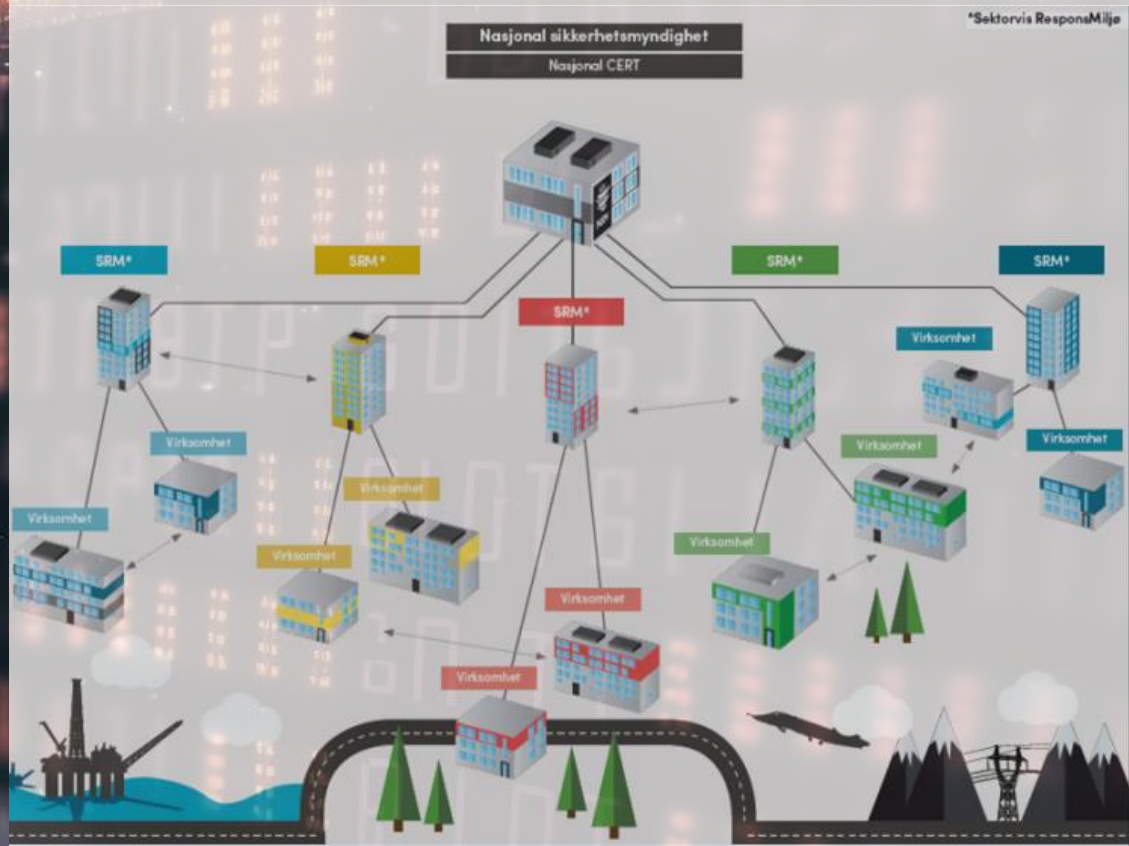
Målet med tilsynet var å verifisere hvordan selskapet følger opp styring av risiko knyttet til informasjonssikkerhet for de industrielle IKT-systemene. Hensikten med tilsynet er å verifisere prosesser og systemer hos aktøren som benyttes for å sikre

- 2010 – 2012: NOROG 104 selv evaluering – postalt
- 2017 - Møteserie med alle aktører (operatører og borekontraktører)
- 2018 – 2020: Tilsyn med land/offshore – operatører
- 2020 - 2021: Møter, risikostyring i digitalisering
  - Operatører med høy offentlig profil på digitaliseringsaktiviteter
- 2021 - 2023: Tilsyn redere og gjenværende operatører
- 2023 - Møter med operatører
  - Tverrfaglig team, IKT-sikkerhet og fysisk sikring
- 2024 - Tilsyn med land/offshore

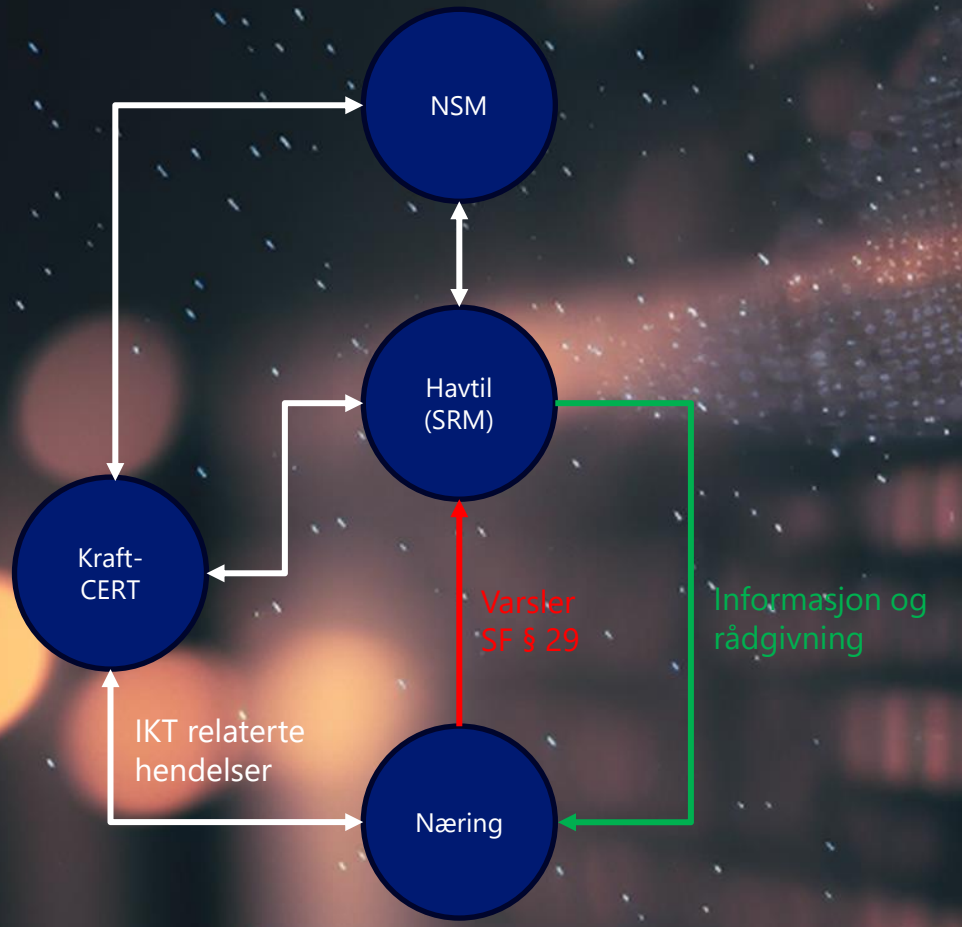
# Sektor Response Miljø

- Departementene skal påse at det er etablert sektorvise responsmiljøer (SRM) med operativt ansvar for å dekke virksomheter innen hele eller deler av departementets myndighetsområde
- Havtil er delegert ansvaret som SRM for petroleumssektoren
- For håndtering av oppgaver innen varsling, informasjonsdeling og analyse av IKT-relaterte hendelser, har Havtil inngått avtale med KraftCERT

*Når SRM blir varslet om en hendelse eller flere sammenfallende hendelser, varsler SRM videre til NSM og vurderer behov for å varsle andre SRM etter en initial kartlegging av situasjonen*
*SRM skal også vurdere å varsle NSM dersom noe tyder på at det kan dreie seg om en avansert hendelse eller en trusselaktør med betydelig kapasitet og/eller det antas at hendelsen omfatter flere sektorer.*



# Varsling, informasjonsdeling og analyse av IKT-relaterte hendelser




- Samle, systematisere, analysere og vurdere IKT-sikkerhets hendelser
- Dele informasjon om sårbarheter, trusler og hendelser
- Koordinerende funksjon
- Gjennomføre øvelser - varsling og respons
- Publiserer årlige trusselvurderinger for sektoren

# Nettverk og samhandling

- *Nasjonalt nivå*
  - Partnerskap i NCSC – nært samarbeid med NSM
  - Faste møter og samhandlingsarenaer
    "SIG-IKT": DSB, NVE, SDIR, Kystverket, Nkom
- *Næringsnivå*
  - Offshore Norge
  - CDS forum (ledet av Sintef)
  - Presentasjoner i en rekke fag og industriforum (NPF, NFEA ++)
- *Akademisk*
  - NTNU Center for Cyber and Information Security
  - Amos / Caros
  - CIAM UiS, IFE cybwin + + +
- *Internasjonalt*
  - IRF opportunity statement, Digitalization
  - Møter med b.la National Institute for Standards & Technology (USA)

International Regulators' Forum
GLOBAL OFFSHORE SAFETY

Norwegian National Cyber Security Centre (NCSC)

NCSC is a part of the Norwegian Security Authority, and is Norway's national cyber security hub and the national CERT.

OFFSHORE NORGE

Norges Rederiforbund
Norwegian Shipowners' Association

CIAM

NTNU
Center for Cyber and Information Security

Norsk Petroleumsforening

nfea

dsb

InfraCERT

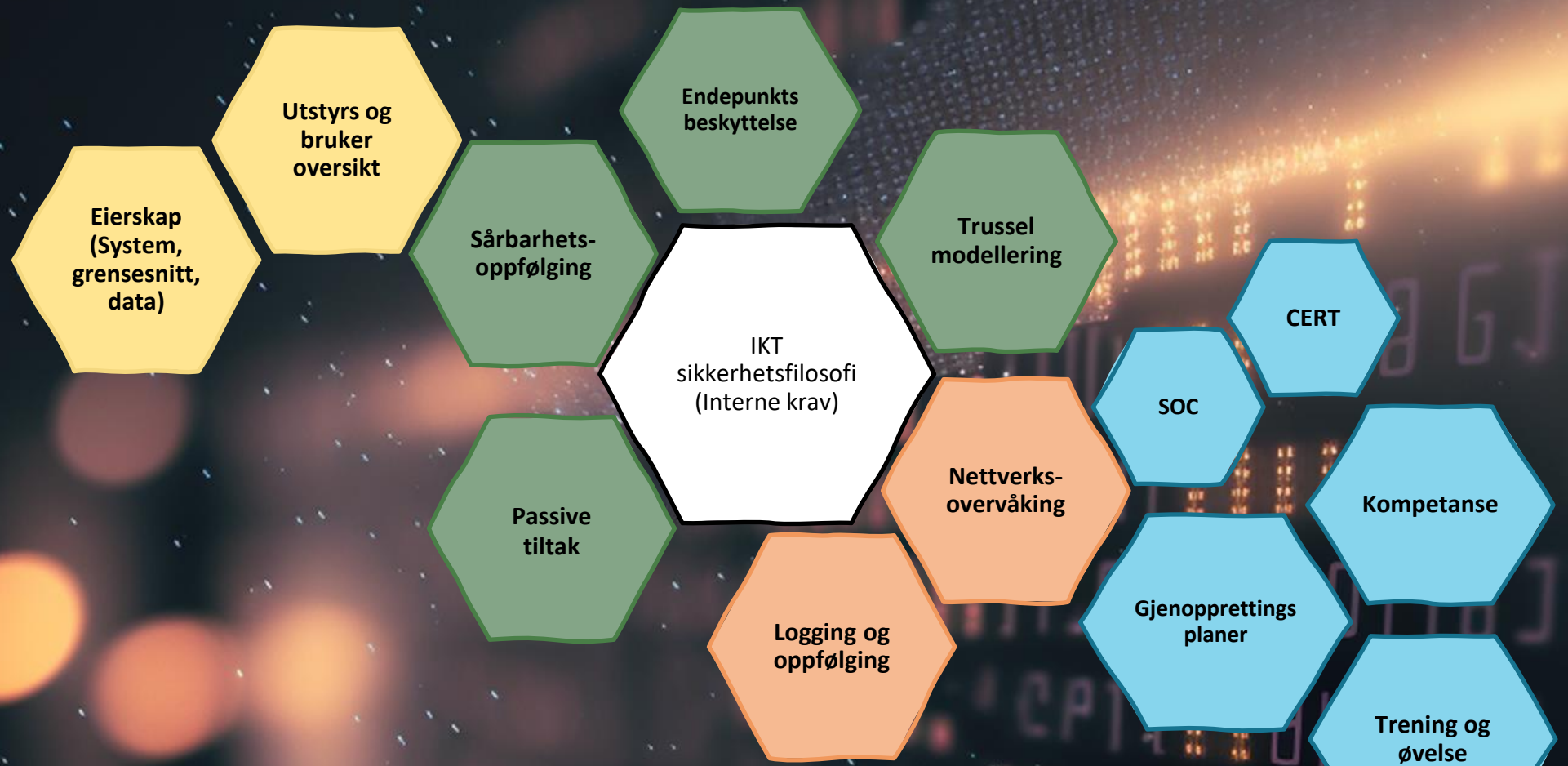
Kraft CERT

InfraCERT is a CERT (Computer Emergency Response Team) with cutting-edge expertise in industrial control systems (OT/ICS).

**CDS-forum - Industry Forum for Cybersecurity of Industrial Automation and Control Systems**

CDS-forum is a co-operation between oil companies, engineering oil companies, consultants, vendors and researchers, with a special interest in cybersecurity and the relation to Industrial Automation and Control Systems (IACS). The participants meet twice a year for workshops, presentations and technical discussions.

# Hva ser vi etter




Identifisere og kartlegge

Beskytte og opprettholde

Oppdage

Håndtere og gjenopprette

# Hva ser vi?

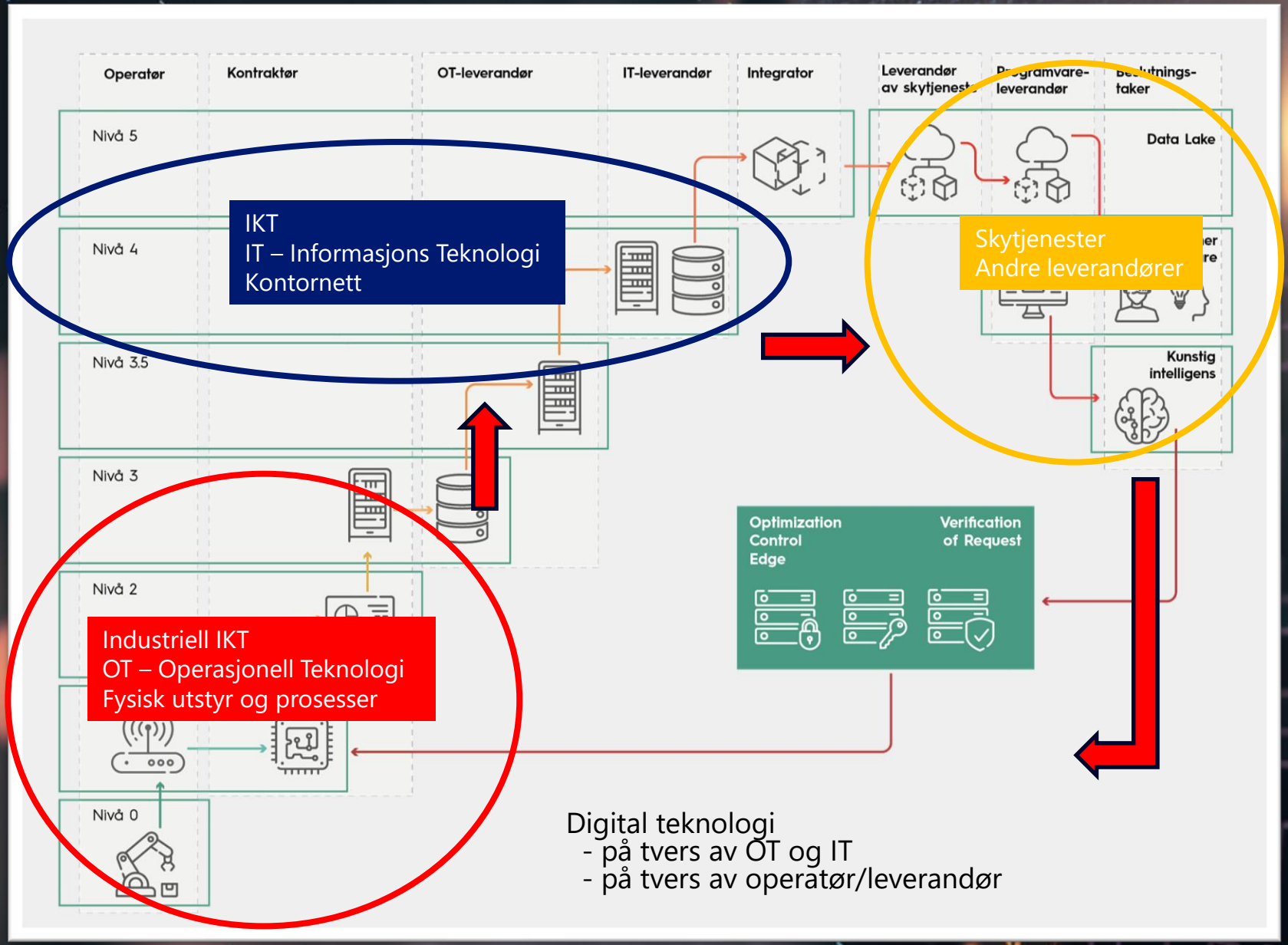
- Ulik grad av modenhet, ressurser og fokus (positiv utvikling)
- Risikostyring
  - Forståelse av trusselbilde og egen verdi/sårbarhet
  - Mangelfulle metoder og bruk av feil ressurser
  - Mangelfull formidling internt i selskapet
- Operasjonalisering av interne krav
- Beskyttelse, oppfølging og vedlikehold
  - Åpen tilkomst og felles brukere
  - Grensesnitt mot tredjepart, lite bevissthet rundt eksponering
  - Eierskap, krav til og oppfølging av leverandør (stor grad av tillitt, lite verifikasjon)
  - Mangelfull lukking av sårbarheter i programvare (patch management)
- Gjenopprettingsplaner
  - Avhengighet til leverandører (stor grad av tillitt, lite verifikasjon)
- Krav til kompetanse
  - Stillingsbeskrivelse, manglende henvisning til ansvarsområder innen industriell-IKT
  - Manglende ferdighetstrening for ansvarsområder (generelle kurs for alle ansatte)
- Øvelser
  - Det øves, men ikke nødvendigvis på alle skift
  - Mangelfull deling av læring på tvers

# Digitalisering - Muligheter vs Utfordringer

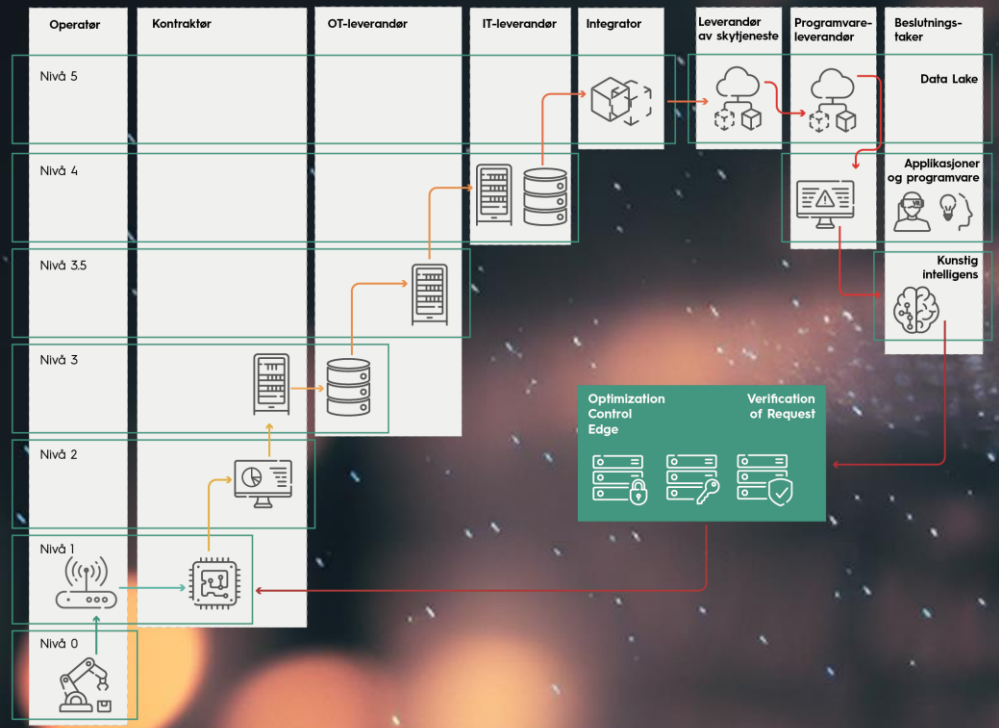
- **Effektivitet**
- **Optimalisering**
- **Kostnadsreduksjon**
- **Fleksibilitet**
- **Bedre beslutningsstøtte**
- **Innovasjon**
- **Prediktiv vedlikehold**
- **Fjernovervåkning og styring**
- **Kundetilpasning**
- **Miljøfordeler**

- **Økt angrepsflate**
- **Økt kompleksitet**
- **Økt sårbarhet**

# Digital verdikjede



# Økt avhengighet og kompleksitet




| Operatør | Kontraktør | OT-leverandør | IT-leverandør | Integrator | Leverandør av skytjeneste | Programvare-leverandør | Beslutnings-taker |
|---|---|---|---|---|---|---|---|