DNV·GL

IKT-SIKKERHET - ROBUSTHET I PETROLEUMSSEKTOREN

# Telekommunikasjon og protokoller

## Petroleumstilsynet

**Rapport nr.:** 2019-0827, Rev. 0
**Dato:** 24-02-2020

| | | |
|---|---|---|
| Prosjektnavn: | IKT-sikkerhet - Robusthet i petroleumssektoren | DNV GL AS |
| Rapporttittel: | Telekommunikasjon og protokoller | Digital Solutions |
| Oppdragsgiver: | Petroleumstilsynet, P.O. Box 599 | Postboks 300 |
| | 4003 Stavanger | 1322 Høvik |
| | Norway | Norway |
| Kontaktperson: | Arne Halvor Embergsrud | |
| Dato: | 2020-02-24 | |
| Prosjektnr.: | 10157212 | |
| Org. enhet: | Cyber Security Services | |
| Rapportnr.: | 2019-0827 Rev. 0 | |

Kontrakt for leveranse av denne rapport:
Avtale om IKT-sikkerhet – Robusthet i petroleumssektoren

Hensikt: Hovedmål med prosjektet er å innhente kunnskap om risiko, trusler, sårbarheter samt viktigheten av IKT-sikkerhet for de industrielle systemer. Denne rapporten tar for seg telekommunikasjon og protokoller.

| Utarbeidet av: | Verifisert av: | Godkjent av: |
|---|---|---|
| Tore Hartvigsen<br>Senior Principal Engineer | Boye Tranum<br>Project Manager | Trond Solberg<br>Head of Section,<br>Cyber Security Services |
| Thröstur Eiriksson<br>Principal Engineer | | |
| Jostein Sund Jensen<br>Principal Engineer | | |



DNV GL Distribusjon:
☒ ÅPEN. Fri distribusjon, intent og eksternt.
☐ INTERN. Fri distribusjon internt i DNV GL.
☐ KONFIDENSIELL. Distribusjon som angitt i distribusjonsliste.
☐ HEMMELIG. Kun autorisert tilgang.

Nøkkelord:

| Rev. Nr. | Dato | Formål | Utarbeidet av | Verifisert av | Godkjent av |
|---|---|---|---|---|---|
| A | 29-11-19 | Høringsutkast | Tore Hartvigsen | Boye Tranum | Trond Solberg |
| B | 24-01-20 | Justert iht. høringsuttalelser | Tore Hartvigsen | | |
| 0 | 24-02-20 | Siste kommentarer innarbeidet | Tore Hartvigsen | Boye Tranum | Trond Solberg |

# INNHOLD

# 1 SAMMENDRAG

DNV GL har på oppdrag fra Ptil gjennomført en studie av IKT-sikkerhet og robusthet i petroleums-sektoren. Dette er rapport fra delprosjekt 6 som omhandler telekommunikasjon og protokoller.

Telekommunikasjon er blitt digital. Informasjonssystemer og telekomløsninger er integrert. Det er svært stor variasjon i funksjonsområdene på de 23 systemkategoriene som i sektoren er definert som tele-kommunikasjonssystemer. Krav til integritet og beskyttelse av konfidensialitet er forskjellig for de ulike systemene. I sektoren kreves det ikke særskilt beskyttelse av telekomsystemer utover de sikkerhetstiltak som gjelder generelt for IKT. Vi har inkludert en liste med 13 anbefalte tiltak som vi mener vil bidra til økt sikkerhet i sektoren.

Telekommunikasjonsdisiplinen er en leverandør av infrastruktur som skal muliggjøre fjernstyring og integrerte operasjoner. Pålitelighet og tilgjengelighet til sikker telekommunikasjon er en forutsetning for trygg og stabil operasjon av installasjonene. Avhengigheten til kontinuerlig operative fiberforbindelser og mangel på høykapasitets alternativer, gjør at noen installasjoner må stenge ned dersom det skjer et totalutfall på fibernettet. Mange eldre telekomsystemer som fortsatt er i drift er basert på gammel teknologi og eldre standarder som ikke har fokus på sikkerhet. Å ivareta kunnskap om de eksisterende systemene blir en utfordring etter hvert som installasjonene nærmer seg slutten på produksjonstiden.

Teleleverandørene har liten eller ingen kjennskap til de sikkerhetskrav og standarder som gjelder i petroleumssektoren. Markedsføringskampanjer blir gjennomført for nye ekspansive løsninger basert på ny teknologi som IoT og 5G. De etablerte sikkerhetsregimene i bransjen utfordres, omgås eller utelates. Teleleverandørene er i stor grad styrt av markedskreftene, og prioriterer funksjonalitet på bekostning av sikkerhet. Det advares mot store uløste sikkerhetsutfordringer i 4G- og 5G-protokollene.

Mindre utstyrsleverandører som tradisjonelt ikke har noen bakgrunn innen IT-utvikling og IKT-sikkerhet tilbyr gunstige avtaler dersom de får ansvar for overvåkning og styring av eget utstyr. De større har et økende fokus på IKT-sikkerhet. Operatørselskapene får i fremtiden en større utfordring med å ivareta og overvåke sikkerheten på helhetsløsningen enn i dag.

Pålitelig, sikker og tilgjengelig kommunikasjon er viktig for trygghet og trivsel. I en beredskaps- eller krisesituasjon er det viktig at telekommunikasjonssystemene fungerer effektivt. Dette stiller ekstra krav til design, redundans og resiliens av systemer og utstyr som benyttes. Gode sikkerhetsrutiner som inkluderer rapportering, oppfølging av hendelser, feil og rutiner er en nødvendighet. En bedriftskultur som motiverer for årvåkenhet og er åpen for kommunikasjon, er en forutsetning for sikkerhet og trygghet. Selskapene etterlyser klarere retningslinjer på hvilke sikkerhetshendelser i telenettet som skal rapporteres til tilsynsmyndighetene, henholdsvis Ptil og Nkom.

Tampnet er blitt en betydelig teleoperatør på norsk sokkel som ikke bare transporterer data fra petroleumssektoren, men også for andre gjennom infrastrukturen i Nordsjøen. Operatørselskapene transporterer offentlige og private data fra andre firma gjennom sine nett og er derfor, etter definisjonen, teleoperatører. Myndighetenes tilsyn med sikkerheten i denne delen av petroleumsvirksomheten er etter vår oppfatning mangelfull og bør gjennomgås.

# 2 ENGLISH SUMMARY

DNV GL has been engaged by Ptil to perform a study on ICT security and robustness in the petroleum sector. This report is the delivery from subproject 6, which is focusing on telecommunications and protocols.

Telecommunication has become digital, with integrated information systems and telecom solutions. There is a vast variety of fields within telecommunication systems, with different requirements for maintaining confidentiality and integrity. There are no special requirements addressing additional protection for telecom systems within the petroleum sector, besides general ICT standards and regulations. DNV GL has included a list with 13 recommendations in this report, aiming to improve safety within the petroleum sector.

Today's telecom suppliers are providing infrastructure enabling remotely controlled and integrated operations. Reliable and available secure communication is essential for safe and stable operations on petroleum installations. The dependency on continuously operating fibreoptic connections with few alternative solutions, will cause several installations to shut down if any downtime on the connections occurs. Many of the operating telecom systems on installations are outdated and based on technology and regulations with little or no focus on security. Maintaining knowledge of existing systems on offshore installations will be a challenge, especially when installations reach their final phase of operations.

Many suppliers within telecom lack knowledge on the standards and regulations applicable to such systems. New technologies such as 5G and IoT are frequently advertised as parts of new emerging solutions from the suppliers. By selling and producing such solutions, without following established security regimes, the security of the delivered products is compromised. Warnings against security flaws in both the 4G and 5G protocols have been stated.

Smaller, less established suppliers are offering favourable deals to customers, given that the supplier can monitor and control their own products. The smaller companies do not have the same experience and knowledge within IT development and security. Such cases are giving operators of the installations challenges, in terms of maintaining and supervising security of all systems.

Reliable, secure and available communication is crucial for having a safe and comfortable environment offshore. If a distress situation occurs, well-functioning telecom systems are of crucial importance. To ensure such availability from the systems, demands for additional requirements in design, redundancy and resilience of the systems and equipment in use, must be given. Well established security policies, including reporting and follow-ups on incidents, errors and routines are necessary. Furthermore, a company culture open to alertness and communication is a prerequisite for establishing and maintaining both safety and security. Companies within the petroleum sector are requesting clearer guidelines regarding what incidents shall be reported to the authorities (Ptil and Nkom). DNV GL recommends the authorities to clarify this soon.

Tampnet is an established telecom operator on the Norwegian continental shelf, transporting data for companies in several industries through their infrastructure in the North Sea. Furthermore, the petroleum operators are transporting both public and private data, from their own and other companies, through their networks. Consequently, these companies are by law also defined as telecom operators. Supervision and audits from the authorities are lacking within this field, and DNV GL recommends Ptil and Nkom to review their routines.

# 3 INNLEDNING

Behovet for informasjonsutveksling og telekommunikasjon har endret seg i bransjen fra de første prøveboringer på 1960-tallet og frem til i dag. På begynnelsen av 1970-tallet var kommunikasjonsnettverket i Norge blant de dårligste i Europa, med blant annet lange ventelister for å få telefon. Televerket var instansen de utenlandske operatører måtte forholde seg til for å få etablert kommunikasjonsløsninger til installasjonene i Nordsjøen. Tradisjonell radiokommunikasjon på mellombølge- og kortbølgeradio var komplisert på grunn av avstander og urolige vind- og værforhold. Utenlandske operatører ønsket å kontrollere og begrense ansattes private bruk av telekommunikasjonsløsninger mens de var om bord i installasjonene /3/.

For Televerkets del var erfaringene og kompetansen vunnet i samarbeid med petroleumsvirksomheten, med på å skape den etter hvert omfattende satellittvirksomheten i etaten. Operatørselskapenes behov representerte en betydelig utfordring for Televerket. Samarbeidet mellom olje- og gassnæringen og Televerket førte etter hvert til etablering av gode telekommunikasjonsløsninger over satellitt til plattformene i Nordsjøen. Norge var det første landet i verden som opprettet satellittsamband til produksjonsplattformer til havs. Televerket ønsket ikke og hadde ikke kapasitet til å operere telekommunikasjonsinstallasjoner i Nordsjøen. Dette ble overlatt til operatørselskapene, selv opererte de installasjonene på land. Dette førte til at selskapene bygde opp egne store og høyt kvalifiserte telekommunikasjonsmiljøer. Styringssystemer for de industrielle prosessene ble automatisert, koplet sammen med telekommunikasjonsløsninger og forgrenet til land, samtidig som administrative systemer på land ble tilgjengeliggjort på installasjonene. Operatørselskapenes behov for å eie infrastrukturen og selv styre utviklingen av telenettene uavhengig av Televerket (som senere ble Telenor), var et diskusjonstema på 1990-tallet. Ønsket om å legge fiberkabler kombinert med strømkabler til land var Telenor lite engasjert i.

For et par tiår siden var det svært liten konkurranse i det norske telemarkedet. Nå er det over 200 tilbydere innen mobiltelefoni, bredbånd, fasttelefoni osv. Veksten har vært særlig sterk etter 2007. Telenor, som den tidligere monopolisten i det norske telemarkedet, er pålagt en rekke forpliktelser. Disse forpliktelser er regulert i en egen avtale mellom staten og Telenor, og åpner for konkurranse av teletjenester til andre, inkludert petroleumssektoren /8/.

I dag er satellittkommunikasjonsløsninger i stor grad erstattet med kommunikasjon over optiske fibre. Løsninger basert på digital teknologi er gradvis innført. Digital teknologi har stor betydning for tradisjonell kommunikasjon innad i og mellom bedrifter, og for oppbygging av omfattende datakommunikasjonssystemer både nasjonalt og internasjonalt. Liberalisering i telebransjen samt behov for økt konkurranse, førte til at det statlige telemonopol ble oppløst. Full konkurranse i telemarkedet ble åpnet i 1998. Telenor ble privatisert og børsnotert i 2000.

Tampnet drifter i dag et omfattende privat telenettverk i Nordsjøen. De har i dag en infrastruktur i Nordsjøen som leverer fibernett, radiolinjer og mobildekning til rundt 240 plattformer, rigger og produksjonsskip /9/. Ringstrukturer er etablert for å sikre redundans og høy tilgjengelighet på tjenestene (se faktaboks 3-1). Gjennom nettet i Nordsjøen transporteres ikke bare data fra petroleumssektoren, men også for andre offentlige og private virksomheter.

Tilgjengeliggjøring av internett på installasjonene utfordret den amerikansk-inspirerte kulturen, som dominerte bransjen de første årene med ønske om å ha kontroll på kommunikasjon fra enkeltpersoner fra installasjonene over det offentlige telenettet. Slik som det ble uttalt fra Phillips: «å kontrollere og rute via hovedkontoret alle uttalelser til offentligheten angående det som skjedde på plattformene også under streikesituasjoner» /3/. Internettbaserte teletjenester gjør at en ansatt som har sitt arbeidsted på en installasjon vil ha de samme kommunikasjonsmuligheter som andre i organisasjonene. I et HMS og

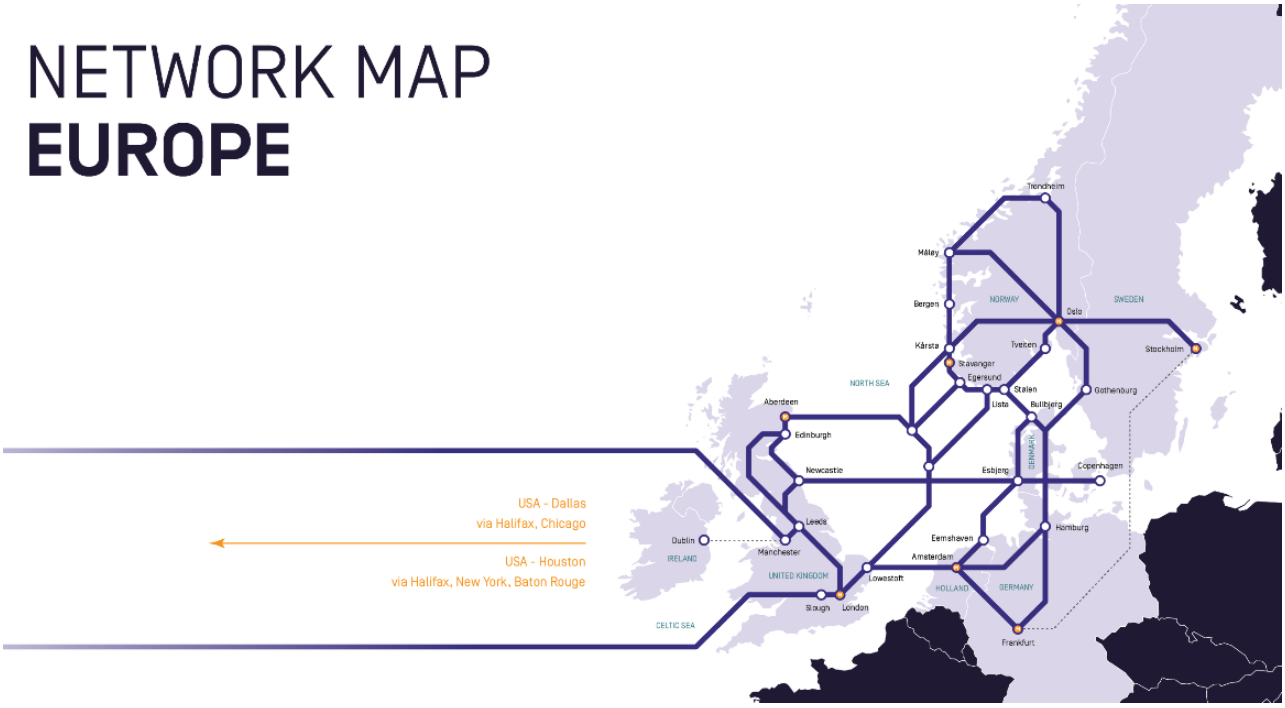
også i et trivselsperspektiv er dette positivt, siden enkeltpersoner kan nå tilgjengelige tjenester og systemer for rapportering og informasjonsinnhenting.

Bedriftenes styringssystemer, offentlige og private tjenester, profesjonell og personlig kommunikasjon skjer i økende grad med digitale media. Informasjonsutveksling skjer i de samme media, og er integrert med andre kommunikasjonsbehov i næringen. Løsningene benytter i stor grad software og utstyr fra store sentrale leverandører. Disse løsningene blir mer og mer avanserte, med stadig flere tjenester integrert.

Krav og retningslinjer som er beskrevet i NORSOK-standardene viser at telekommiljøene har god styring på krav og sikkerhet i sektoren. NORSOK-standardene for telekom har i de siste 20 år definert en felles forståelse for hvilke krav som skal stilles til telekommunikasjonsløsninger i sektoren, og sørger for forutsigbarhet og utvikling.

Trenden er at digitaliseringen av telekomsystemer i næringen vil øke. Telekom- og IT-løsninger integreres og blir mer komplekse. Dermed øker også sårbarheten. De private og offentlige muligheter for bruk av digitale tjenester er etterhvert blitt de samme uavhengig av hvor en befinner seg. En ansatt på en offshore-installasjon har de samme muligheter for å bruke kommunikasjonssystemer til å nå både offentlige og private tjenester, på samme måte som om en skulle befinne seg på et kontor på land eller hjemme.

Oljeselskapene er nå også blitt teleoperatører. De transporterer ikke bare egne data men også data for andre i sine kommunikasjonsnettverk. Når Oljeselskapene tilbyr datakommunikasjonstjenester til andre er de underlagt de samme lover og reguleringer som andre teleoperatører. Som vist i faktaboks 3-1 under som er hentet fra Tampnet sin hjemmeside, forbinder infrastrukturen i Nordsjøen de offentlige nettverk med internasjonale nettverk. Tampnet markedsfører seg nå også som en internasjonal transportør av offentlige og private data, og ser på denne tjenesten som et fremtidig vekstområde /10/.




Faktaboks 3-1: Tampnet sitt nettverk med ringstrukturer i Nordsjøen og til Europa /10/.

Protokoller og løsninger som ble utviklet og tatt i bruk før IKT-sikkerhet ble et tema, har ikke nødvendige innbygde sikkerhetsmekanismer. Dessverre er mange eksisterende systemer som fortsatt er i drift, basert på vel etablerte, men lite sikre protokoller. Dette er en sikkerhetsutfordring i sektoren.

Installasjonene har også blitt fremskutte basestasjoner for telekommunikasjon til havs. De bidrar til økt sikkerhet for sjøfarende og også som et hjelpemiddel til nødetatene.

Økt grad av digitalisering av telekommunikasjonsløsninger, flere involverte aktører, løsninger basert på felles kommunikasjonsbærere og teknologi, og et sterkt press for forbedret lønnsomhet, vil utfordre sikkerheten i næringen de kommende år. Særlig nye løsninger basert på ny 5G-teknologi og IoT vil utfordre de løsninger som er etablert for sikker kommunikasjon. Tilgjengeliggjøring av høyhastighets- og høykapasitets-kommunikasjonsløsninger gjør det mulig å raskt kommunisere store volumer med teknisk informasjon over distanse. Dette gir mulighet for fjernstyring og fjernovervåkning av installasjonene. Samtidig gir dette mulighet for trusselaktører til å få tilgang til og kunne misbruke eller manipulere informasjon. De etablerte sikkerhetsregimer i sektoren utfordres. End-til-ende kryptering er vanlig men løser ikke alle sikkerhetsutfordringer som diskutert videre i dette dokument.

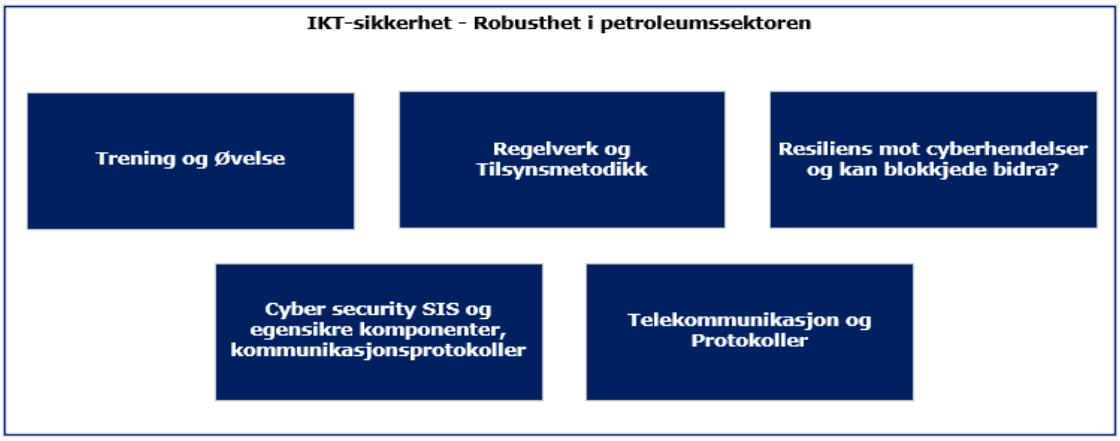
## 3.1 Bakgrunn

Digitalisering i olje- og gassektoren åpner opp for effektivisering, men gjør også sektoren mer sårbar for IKT-sikkerhetshendelser. Olje- og gassektoren er et mål for trusselaktører, både på grunn av de store verdier sektoren representerer og for aktivister med idealistisk eller politisk motivasjon.

Utvinning, transport og distribusjon av hydrokarboner medfører en risiko for ulykker med konsekvenser for materielle verdier, helse, miljø og sikkerhet. For å redusere risiko for slike ulykker, er det installert en rekke sikkerhetssystemer. Mange av disse sikkerhetssystemene benytter IKT-teknologi og kan være sårbare for IKT-sikkerhetshendelser. Manglende eller feil funksjonalitet i sikkerhetssystemene kan få katastrofale konsekvenser. Det er et mål at IKT-sikkerhetshendelser ikke skal påvirke sikkerhetssystemene.

Petroleumstilsynet (Ptil) gjennomfører en satsing på IKT-sikkerhet i perioden 2018-2021. Målet er å gå i dybden på en del viktige områder, innhente kunnskap om den teknologiske utviklingen og vurdere hvordan dette påvirker risikobildet. Nylig er det publisert rapporter innen temaene «Kunnskap IKT-sikkerhet og CERT» /4/ og «Fjernarbeid og HMS» /12/. Videre pågår det en utredning om «Industriell IKT og IoT».

Petroleumstilsynet utlyste en konkurranse for å utrede «IKT-sikkerhet – Robusthet i petroleumssektoren», som inneholder flere arbeidspakker og delleveranser, som illustrert i faktaboks 3-2 under. Dette oppdraget ble tildelt DNV GL. Alle arbeidspakker har gjennomført intervjuer og innhentet informasjon fra aktørene i bransjen, samt innhentet erfaringer med tilsyn av IKT-sikkerhet i andre sektorer.




Faktaboks 3-2: Delleveranser i prosjektet.

## 3.2 Hensikt

Denne 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. Noen av de systemer vi mener det er spesielle sikkerhetsutfordringer med, blir grundigere diskutert enn andre.

## 3.3 Metodikk

I rapporten gjennomgås telekommunikasjonssystemer og tilhørende protokoller som anvendes, med vekt på IKT-sikkerhet og sårbarheter i forskjellige prosjektfaser og av forskjellige aktører i sektoren. Vi har skissert en modell av en referanseinstallasjon som inneholder aktuelle problemstillinger og løsninger i forhold til eksisterende og fremtidige telekommunikasjonsløsninger. Modellen er basert på prosjektdeltageres egne erfaringer fra tidligere og pågående prosjekter. Vi har tatt utgangspunkt i relevante standarder og beste praksis dokumenter for telekommunikasjon på norsk sokkel. Litteraturstudier for å belyse de aktuelle problemstillinger har blitt foretatt.

Diskusjoner med sentrale aktører i bransjen er gjort basert på intervjuguider som vi har etablert. Dette omfatter de største teleoperatørene, et utvalg operatørselskaper, riggoperatører, leverandører og tilsynsmyndigheter. Synspunkter og personlige betraktninger er blitt anonymisert.

Det store antall forskjellige systemkategorier som er definert som telekommunikasjonssystemer og protokoller som er involvert, har ikke gjort det mulig å gjøre detaljerte analyser av alle. Vi har fokusert på de kategorier hvor vi har identifisert eller blitt gjort oppmerksomme på vesentligste sikkerhets-utfordringer.

Følgende bedrifter er blitt intervjuet:

<u>Teleleverandører:</u>

- Telenor Maritime
- Telia
- Tampnet

<u>Myndigheter:</u>

- Nkom

- Ptil

Operatørselskap:

- Equinor
- Lundin
- Aker BP

Riggoperatører:

- Transocean

Det er innhentet informasjon fra leverandører intervjuet i delprosjekt 5 «Cyber security SIS og egensikre komponenter, kommunikasjonsprotokoller».

Prosjektgruppen deltok på Tekna-konferansen «Telekommunikasjon Offshore 2019».

## 3.4 Forkortelser og definisjoner

| | |
|---|---|
| CCTV | Closed-circuit television |
| CERT | Computer Emergency Response Team |
| DSB | Direktoratet for samfunnssikkerhet og beredskap |
| DMZ | Demilitarized Zone (nøytral sone) |
| ESD | Emergency Shut Down |
| F&G | Fire and Gas |
| FPSO | Floating Production Storage and Offloading facility |
| GPS | Globalt posisjoneringssystem |
| HEO | High Elliptic Orbit |
| HMI | Human-Machine Interface (Brukergrensesnitt) |
| HMS | Helse, miljø og sikkerhet |
| IKT | Informasjon- og kommunikasjonsteknologi |
| IoT | Internet of Things |
| IP | Internettprotokoll |
| IT | Informasjonsteknologi |
| Ka – bånd | Frekvensområdet 26.5 – 40 GHz |
| Ku - bånd | Frekvensområdet 12 – 18 GHz |
| LAN | Local Area Network |
| LEO | Low Earth orbit |
| MOU | Mobile Offshore Unit |
| NIS | Network and Information Systems |
| NOU | Norsk offentlig utredning |
| NSM | Nasjonal sikkerhetsmyndighet |
| O&G | Olje og gass |
| OT | Operasjonsteknologi |
| PMR | Profesjonell/ Privat Mobil Radio |

| | |
|---|---|
| Ptil | Petroleumstilsynet |
| ROS | Risiko- og sårbarhetsanalyse |
| SNMP | Simple Network Management Protocol. En protokoll som benyttes på IP-nettverk for å administrere og overvåke maskiner og nettverksutstyr. |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TMS | Telekom monitoreringssystem |
| UHF | Ultrahøy frekvens (300 MHz – 3 GHz) |
| UPS | Uninterruptable power supply |
| VHF | Veldig høy frekvens (30-300 MHz) |
| VLAN | Virtual Local Area Network |
| VPN | Virtual Private Network |
| VSAT | Very Small Aperture Terminal |
| WAN | Wide Area Network |

# 4 SIKKERHET I TELEKOMMUNIKASJONSLØSNINGER SOM ANVENDES I DAG

I dette kapittel gjennomgås sikkerhetsutfordringer i noen av de sentrale telekommunikasjonsløsninger som er i bruk i petroleumssektoren i dag. Krav til løsningene er godt beskrevet i NORSOK-standardene og det er ikke hensiktsmessig å gjenta beskrivelsene her. Diskusjonene i dette dokument er fokusert på de sikkerhetsutfordringer og HMS-utfordringer vi har observert.

NORSOK-standard T-101 «Telecom systems», spesifiserer felles krav til telekommunikasjonssystemer. NORSOK-standard T-003 spesifiserer krav til telekomsystemer for mobile offshore units (MOU). Begge standarder er revidert, fornyet og utgitt høsten 2019. Selskapsspesifikke krav vil i tillegg være inkludert i avtaler som tilleggskrav, eller som presiseringer. Sektorens intensjon er å ha flest mulig krav i NORSOK-standardene, og færrest mulig selskapsspesifikke krav. Utfordringen i en disiplin i rask utvikling er å holde standarder og felles sektorkrav løpende oppdatert. Tidligere revisjoner av telekomstandardene kom i 2000, 2004, og 2010. Aktuelle telekomsystemer, slik de er definert i NORSOK-standard T-101 (T-101), er oppført i tabell 4-1.

Dagens telekommunikasjonssystemer består av mange IT-komponenter. For eksempel består et telefonsystem i dag nesten utelukkende av IT-komponenter. IKT-sikkerhet må ivaretas i et langt større omfang enn tidligere, og vil i større grad enn før direkte påvirke design av systemer. En kjent utfordring er at enkelte telekommunikasjonssystemer produseres i liten skala, og at man ikke kan dra nytte av en lang designprosess som de store aktørene i markedene har fordeler av /14/.

T-101 krever at IKT-sikkerhet skal opprettholdes i løpet av livssyklusen til telekommunikasjons-systemene, og at beste praksis kan finnes i følgende publikasjoner:

- DNVGL-RP-G108
- Norsk olje og gass anbefaling 104
- NEK IEC 27001
- NEK IEC 27002
- IEC 62443 (basis for DNVGL-RP-G108)

Intensjonen i T-101 er å definere minimumskrav for IKT-sikkerhet. Dette gjøres ved å kreve at en sårbarhetsvurdering skal gjøres for hvert enkelt telekommunikasjonssystem /11/. Det kreves ikke at vurderingen skal gjøres etter gitte standarder. Dette kunne ha vært klarere definert i T-101, og dermed gitt tydeligere retningslinjer for hva minimumskravet til IKT-sikkerhet for de forskjellige typer systemer skal være.

## 4.1 Telekommunikasjon i bruk i olje- og gassinstallasjoner

Telekomsystemer dekker en rekke forskjellige behov på en installasjon. Som vist i tabell 4-1 er det svært stor variasjon i funksjonsområder som telekomdisiplinen har ansvar for. Ansvaret dekker både telekommunikasjonsløsninger og systemer. I vår gjennomgang har vi fokusert på telekommunikasjons-løsninger som anvendes men også på noen av de systemer som telekomdisiplinene har ansvar for.

Fokus på optimalisering og kostnadsbesparelse har ført til at fjernstyring og sentralisering av systemer er blitt vanlig, sammen med sentralisering av funksjonaliteten i kontrollrommet. Dette betyr at ulike systemer i alle sikkerhetsnivåer eksisterer i flere lokasjoner, noe som gir vesentlige utfordringer for telekommunikasjonsløsningene.

For å ivareta IKT-sikkerhet samt vedlikeholde systemene, er det behov for å koble systemene mot et felles datanettverk hvor mønsterfiler for antivirus, operativsystem- og programvareoppdateringer kan hentes. Disse oppdateringene må ofte hentes fra internett eller fra en tredjepart.

Tabell 4-1: Gruppering av telekommunikasjonssystemer som anvendes i petroleumssektoren /11/.

| Sub-system code | Title |
|---|---|
| 86-00 | General |
| 86-11 | Public address and general alarm (PAGA) |
| 86-21 | Telephone system |
| 86-23 | Data network equipment |
| 86-24 | Office data and telephone cabling network |
| 86-31 | Radio links |
| 86-36 | Wireless broadband access network |
| 86-39 | Fibre optic cable links |
| 86-41 | Mandatory and general radio |
| 86-42 | UHF radio system |
| 86-43 | Audio and video entertainment |
| 86-45 | Personnel registration system |
| 86-46 | Access control system |
| 86-51 | Closed circuit television (CCTV) |
| 86-52 | Environmental monitoring system |
| 86-53 | Vessel traffic Monitoring System |
| 86-55 | Communication recorder |
| 86-61 | Shuttle tanker loading telemetry |
| 86-63 | Pipeline protection telemetry |
| 86-73 | Positioning |
| 86-81 | Main distribution frame |
| 86-82 | Telecom power supply |
| 86-83 | Real time clock |
| 86-84 | Telecommunication monitoring system (TMS) |

Kommunikasjon mellom ulike systemer og sikkerhetsnivå har endret seg fra galvanisk separasjon (seriell, tørr kontakt, analog etc.) til å benytte nettverk og IP-baserte protokoller.

Det å bruke nettverk og IP-baserte protokoller for kommunikasjon mellom systemer gjør samhandling mye enklere og mer fleksibel.

Ut fra etablert praksis og behov som eksisterer, kan en se på dataflyt i minst fire dimensjoner:

- systemintern datakommunikasjon
- systemintern datakommunikasjon, mellom lokasjoner
- datakommunikasjon mellom ulike systemer i samme sikkerhetsnivå
- datakommunikasjon mellom systemer i ulike sikkerhetsnivå

### 4.1.1 Systemintern datakommunikasjon

Velfungerende telekommunikasjonsløsninger på en installasjon er fundamentale for sikkerhet og trygghet for personellet om bord. Det barske miljøet med høyt støynivå, ofte dårlig vær og kulde, behov for å bruke verneutstyr under arbeid, mange arbeidsoperasjoner som skjer i parallell, etc. stiller store krav til kommunikasjonsutstyret som benyttes.

Systemene skal fungere i en beredskapssituasjon uavhengig av om andre systemer er ute av funksjon. T-101 gir detaljerte føringer på hvilke krav som bør gjelde for systemintern datakommunikasjon og de er derfor ikke gjentatt her. Noen aspekter i forhold til sikkerhet er diskutert videre i dette delkapittelet.

**PAGA** (Public Address and General Alarm) systemer er installert for alarmer og meldinger. Design og implementering av PAGA-systemer skal være i henhold til T-101, og fungere slik at systemet er feiltolerant og fungerer selv om andre systemer på en installasjon er ute av drift. PAGA-systemer må også fungere i kritiske situasjoner uavhengig av andre systemer, som for eksempel strømforsyning. PAGA-systemet skal ha grensesnitt til ESD- og F&G-systemene for automatisk initiering av alarmer fra disse systemene.

Et telefonsystem (**PABX –** Private Automatic Branch Exchange) som tillater intern-, ekstern- og nødkommunikasjon, skal være tilgjengelig på en installasjon. T-101 oppmuntrer til bruk av mobiltelefoner, men advarer mot å bruke private telefoner for gitte funksjoner eller roller på en installasjon. Som del av de terrorforebyggende tiltak som diskuteres i sektoren er også opptak av verbal kommunikasjon et tema. Flere av operatørene har tekniske løsninger på plass for å kunne gjøre dette. Siden opptak av tale og bilder er regulert av personvernbestemmelsene må klare retningslinjer for når og hva som kan tas opp avtales mellom bedriftene og organisasjonene. Sektoren burde gå sammen om å etablere slike retningslinjer og en felles praksis.

Andre lokale meldingssystemer kan være kablede eller trådløse intercomsystemer (f.eks. Driller's intercom), eller som på mer moderne anlegg **TETRA** (Terrestrial trunked radio) baserte systemer som kommuniserer i UHF-båndet. TETRA er en standard for digitale radiosystem for lukkede, gruppeorienterte radiosamband som er spesielt utviklet for offentlige nød- og beredskapstjenester, men som også blir benyttet spesielt innen transportsektoren, Forsvaret og lukkede industrigrupper. Det er erfart at TETRA-systemer kan ha et par sekunders forsinkelse fra når en knapp er trykket på til kommunikasjonen starter. Dette kan være kritisk i kommunikasjon mellom for eksempel en kranfører og en signalmann.

På den trådløse siden skjer det en rask utvikling som er diskutert senere i denne rapporten.

Nye kommunikasjonssystemer gir også mulighet for «man-down»-funksjoner; en automatisk melding til kontrollrommet dersom en person faller eller er utsatt for en ulykke.

**Videoovervåkning (CCTV)** av deler av installasjonene med overføring til kontrollrom gjør det mulig å følge utstyr i drift og personell under arbeidsoperasjoner. Det kan være så mye som 140-150 kameraer installert på en installasjon. Dette gjør at man fra det sentrale kontrollrom kan følge med på både arbeidsoperasjoner og overvåkning av utstyr.

SAFE (sammenslutningen av fagorganiserte i energisektoren) har reist bekymringer angående misbruk av CCTV ved å overvåke ansatte, se faktaboks 4-1. Det finnes egne forskrifter knyttet til bruk av kameraovervåkning /5/.

SAFE har varslet Petroleumstilsynet om alarmerende forhold på en borerigg. Dette skriver Roy Erling Furre, SAFE i varslingen til Ptil:

Da plattformen ble bygd, ble de gitt tillatelse til bruk av kameraovervåking, på engelsk ofte kalt «closed-circuit television» og forkortet CCTV. Bruken av disse systemene er nå helt ute av kontroll med omfattende misbruk og ydmykende maktovergrep mot ansatte. Videoer fra hele 12-timers skift blir sendt til land og gjennomgått i jakten på prosedyrebrudd.
Våre tillitsvalgte er via omveier også blitt gjort oppmerksom på at også video og lydkanalene offshore blir overført, blant annet til operatørselskapet sitt kontrollsenter på land. Dette forholdet er ikke klarert med- eller formidlet til arbeidstakerne eller deres tillitsvalgte. Vi har funnet noen lokale oppslag om dette på arbeidsplass, men dette forholdet er ikke behandlet iht. regelverkets krav.

Faktaboks 4-1: Eksempel på varsel til Ptil om ulovlig bruk av data fra CCTV /28/.

### 4.1.2 Systemintern datakommunikasjon, mellom lokasjoner

Når et system eksisterer i to eller flere geografiske lokasjoner, gjelder i utgangspunktet det samme som for intern datakommunikasjon. Forskjellen er at det systemspesifikke nettverket må transporteres gjennom et WAN-transportnettverk, som gjerne er felles for flere systemer og gjerne er definert som eget telekomsystem (se faktaboks 4-2). Her er det viktig å sørge for segregering, uavhengighet og datasikkerhet.

Mange løsninger benyttes både kablet og trådløst. Det kan være private nett, eller offentlig forbindelse fra en telekomleverandør.

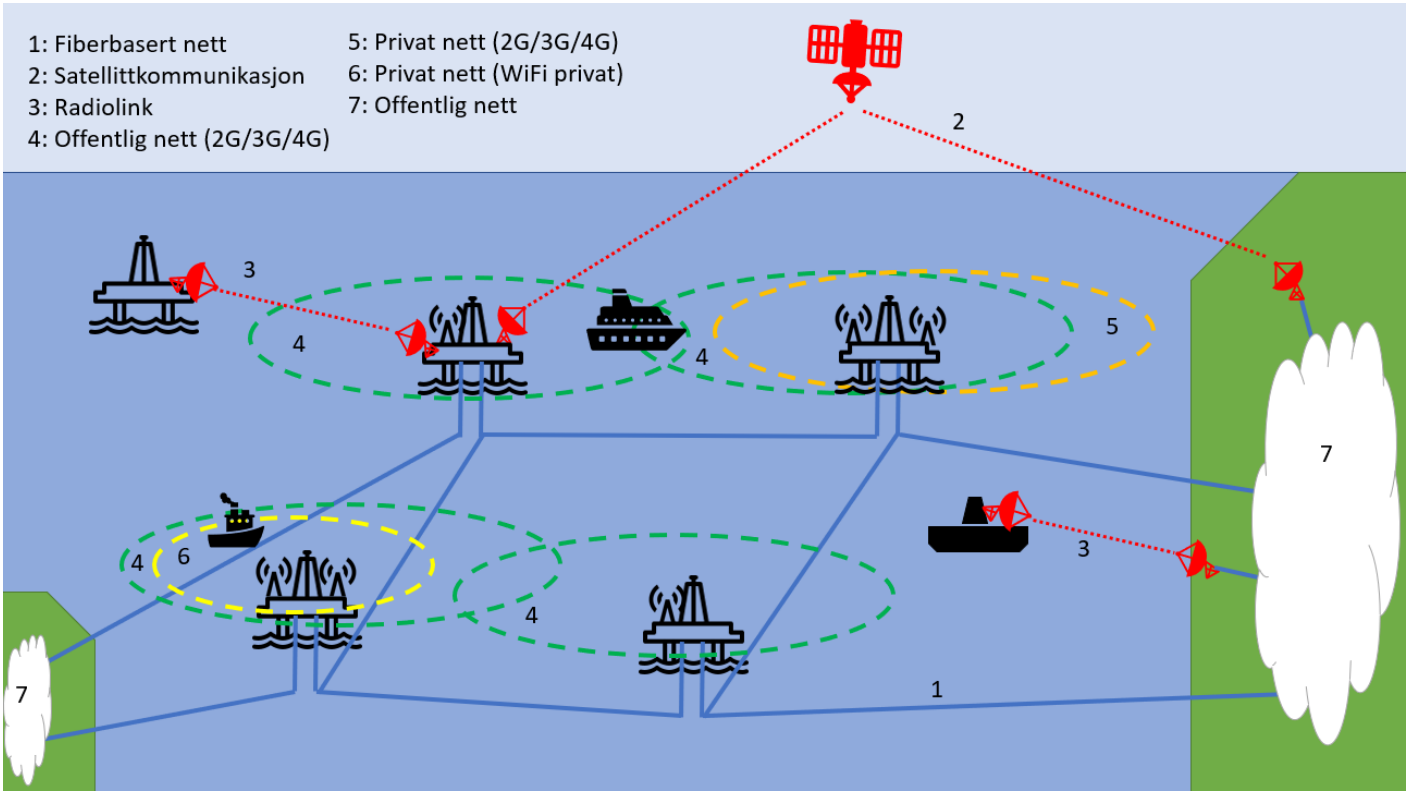
Flere systemer må ofte forlenges over de samme media, men som også må beholdes adskilt. Dette kan gjøres på mange forskjellige måter, f.eks. Lag3 MLPS VPN, Pseudowire (EoMPLS, PPTP etc.), 802.1Q, QinQ samt med enkle tunnelprotokoller som GRE og IPIP. Dette er pakkesvitsjede protokoller i OSI-modellens lag 2 eller 3. Disse protokollene er ikke alle like sikre, og det kan være lurt å vurdere tilleggsprotokoller for å ivareta sikkerhet som IPSec VPN, eller annen type kryptering.

Det finnes også linjesvitsjete protokoller som for eksempel ATM (Asynkron Transfer Mode), FrameRelay og E1/T1. De linjesvitsjete protokollene var tidligere mye brukt, men telekomleverandørene faser ut den linjesvitsjete teknologien, og erstatter med pakkesvitsjet teknologi. Her er MPLS (Multiprotocol Label Switching) den mest brukte av teleleverandørene.

Den tradisjonelle linjesvitsjete teknologien håndterer adskillelse ved å tildele en «timeslot» til hvert virtuelle nett/ hver forbindelse. Dette gjør at det er vanskelig å lytte på trafikken og å utføre man-in-the-middle angrep.

Pakkesvitsjet teknologi innebærer ren dataoverføring. De opprinnelige IP-pakkene er pakket inn med ny header. Det er relativt lett å lytte på pakkesvitsjete protokoller, pakke ut og få tak i innholdet.

IKT-sikkerhet ivaretas i dag med kryptering med f.eks. IPSec VPN, eller tilsvarende form for kryptering. Det gjelder spesielt hvis trafikken går igjennom telekomleverandør, tredjepartsnettverk, internett eller åpent rom (radiobølge). Kryptering gir god beskyttelse men en er avhengig av krypteringsteknologi og utstyr fra eksterne leverandører. Som diskutert senere i rapporten er det sikkerhetsrisikoer forbundet med dette.




Faktaboks 4-2: Prinsippskisse for kommunikasjonsløsninger til faste og mobile offshoreenheter.

### 4.1.3 Datakommunikasjon mellom ulike systemer i samme sikkerhetsnivå

Det er viktig at ulike systemer på samme sikkerhetsnivå er logisk adskilte, for å sørge for at IKT-sårbarheter blir isolert til ett system, og for å unngå at en IKT-hendelse i et system påvirker andre systemer.

Det er viktig at datakommunikasjon mellom ulike systemer er kontrollert, for eksempel ved å rute igjennom brannmur som blokkerer trafikk. Brannmuråpninger bør være begrenset til det som er absolutt nødvendig.

Eksempel på kommunikasjon mellom ulike systemer på samme sikkerhetsnivå:

- tidssynkronisering
- monitorering av tilstand, logging og overvåking
- alarmer
- utveksling av data
- utveksling av styringskommandoer
- fjerntilgang og -administrasjon
- sentralisert HMI
- sentralisert database
- sentralisert brukerdatabase (f.eks. Microsoft AD)
- autentisering
- autorisering
- auditing

- tale og bilde
- back-up

Nødvendigheten av datakommunikasjon mellom system på samme sikkerhetsnivå må vurderes, og en må sørge for at det ikke åpnes sikkerhetshull.

### 4.1.4 Datakommunikasjon mellom systemer i ulike sikkerhetsnivå

Datakommunikasjon mellom system på ulike sikkerhetsnivå og domener kan være nødvendig, men skal begrenses. All kommunikasjon skal rutes igjennom brannmur som blokkerer all trafikk, utenom det som er spesifikt tillatt. Protokoller som anvendes, inkludert protokollens sikkerhet, robusthet og retning, må vurderes.

Det er ofte behov for kommunikasjon mellom systemer på ulike sikkerhetsnivå innen det industrielle domenet, men også mellom et system i det industrielle domenet og et eksternt system (på kontornettverk, hos tredjepart eller tjeneste på internett).

Klare retningslinjer eller regler bør finnes for kommunikasjon mellom sikkerhetsnivå og domener, for å understøtte vurdering når behov dukker opp.

En enkel matrise som den i tabell 4-2 kan hjelpe med å formidle klare retningslinjer.

Eksempel på kommunikasjon mellom system og/eller sikkerhetsnivåer er:

- tidssynkronisering
- tilstandsmonitorering, -logging og -overvåking
- alarmer
- utveksling av data
- utveksling av styringskommandoer
- fjerntilgang og -administrasjon
- sentralisert HMI
- tale og bilde

Tabell 4-2: Eksempel på kommunikasjon mellom system på ulike sikkerhetsnivå.

| FRA | TIL | |
|---|---|---|
| Level 3.5 | Level 4 | Tillatt basert på grundig vurdering |
| Level 4 | Level 3.5 | Ikke tillatt (unntak evalueres) |
| Level 4+ | Level 3, 2, 1 | Ikke tillatt |
| Level 3.5 | Level 3 | Tillatt basert etter grundig vurdering og aktiv godkjenning |
| Level 3.5 | Level 2 | Ikke tillatt |
| Level 3.5 | Level 1 | Ikke tillatt |

(De refererte Levels (sikkerhetsnivåer) er illustrert i faktaboks 4-3)

Arbeidsordresystemer («Work Order systems») blir benyttet for å ha oversikt over, og kunne koordinere aktiviteter i forskjellige systemer på en installasjon. Dette gjelder også for oppgraderinger, endringer og

konfigurasjoner på forskjellige telekommunikasjonssystemer. Styring av slike operasjoner er nødvendig for å kunne ha kontroll på endringer som kan påvirke hverandre.

For helhetsoversikt og som hjelpemiddel til evaluering av dataflyt og sikring, bør det lages et tydelig helhetsbilde av topologien, som deles i sikkerhetslag med barrierer og nødvendig segregering. Modeller som ligner den som vises i faktaboks 4-3, kan benyttes for å gi klar oversikt over topologi og kritikalitet. Figuren viser topologien på en installasjon, samt forlengelse til et kontrollsenter på land. Figuren viser oversikt over alle systemer, telekomsystemene finnes her i de øverste lagene, Level 3 og oppover. Når det skal gjøres en forlengelse av systemer mellom lokasjoner, blir telekom disiplinen involvert i design og implementering helt ned til Level 1. Ved introduksjon av IoT (beskrevet senere i dokumentet) bør telekom disiplinen bli involvert i planlegging av løsninger i alle sikkerhetslag.

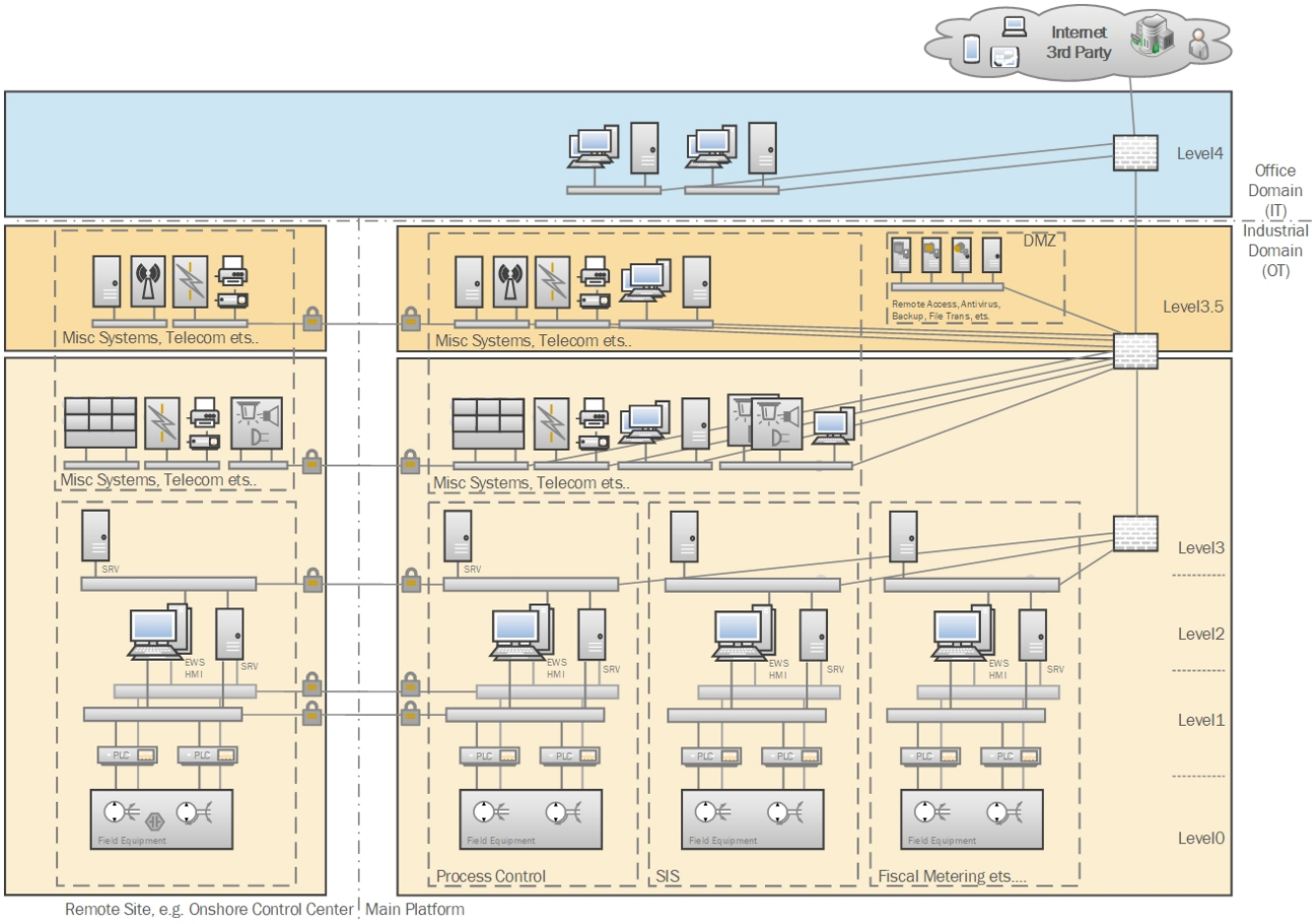
## 4.2 Sikkerhet i telekommunikasjon mellom eksterne aktører

Brannmurer og rutere er typiske nettverkskomponenter som benyttes for å:

- styre kommunikasjon mellom flere aktører
- ha kontroll på hvem som har mulighet til å nå gitte systemer
- tillate kommunikasjon mellom to eller flere definerte tjenester

Petroleumssektoren er avhengig av å kjøpe systemer fra leverandører som de kan stole på. Kompleksiteten i dagens telekommunikasjonsløsninger er så høy at det er umulig å ha tilstrekkelig oversikt, og være trygg på at etablerte sikkerhetstiltak er 100 % sikre (se faktaboks 4-4). Dette er et argument for å begrense trafikk mellom eksterne aktører som er involvert i utbygging, drift eller vedlikehold av en installasjon, til et nødvendig minimum.

Tillates kommunikasjon mellom eksterne aktører, må man også være forberedt på å styre risikoen som er forbundet med det.




Faktaboks 4-3: Soneinndeling og prinsippskisse for fjernoperasjon.

## 4.3 Mobilkommunikasjon internt på en O&G-installasjon

Nkom er ansvarlig for tildeling av tillatelser for radiosamband, og forvaltning av radiofrekvensspekteret for PMR – Profesjonell/Privat Mobil Radio for grupper med egne kommunikasjonsbehov.

**PMR-nett** er mobile radiosambandsnett til intern bruk, for en begrenset gruppe med egne kommunikasjonsbehov. De kan være både en-til-en og en-til-mange. PMR-nett er geografisk avgrenset. Det kreves tillatelse fra Nkom for å bruke gitte frekvenser. En årlig avgift blir betalt til Nkom, og de fører tilsyn med bruken og kan pålegge at endringer blir gjort.

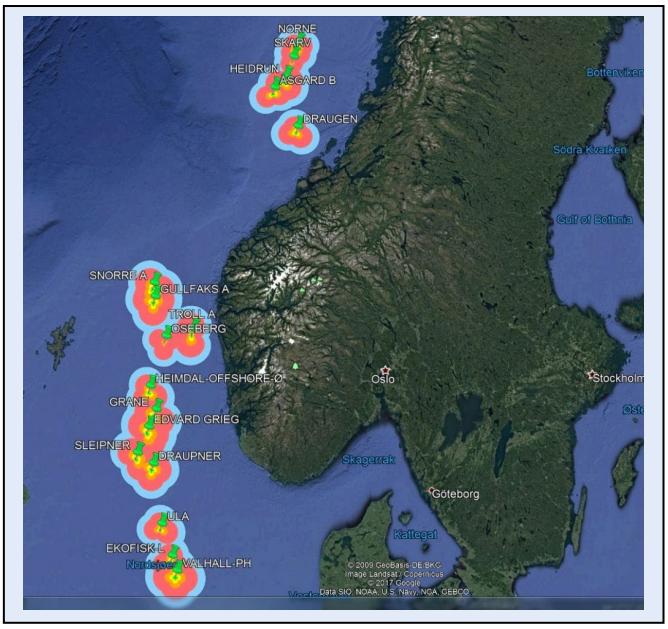
Hvor sikre er egentlig disse nettverkskomponentene? Et vel dokumentert bevis på spionasje er at utstyr fra Cisco, som i mange år har vært en dominerende leverandør av slike systemer, ble manipulert av amerikanske NSA (National Security Agency) til å sende internettrafikk tilbake til dem. Dette ble kjent gjennom dokumenter som Edward Snowden lekket til pressen, og er derfor et eksempel på hvordan spionasje kan bli gjort gjennom manipulering av leverandørutstyr.
Det finnes ikke noe bevis for at Cisco var klar over NSA sine endringer, men eksemplet viser at selv når du kjøper systemer fra en leverandør du stoler på, er det ikke garantert at systemet er sikkert.

Faktaboks 4-4: Hvor sikre er egentlig brannmurene? /43/

**UHF-samband** er spesielt godt egnet for samband over korte avstander når omgivelsene er krevende. Det norske Nødnettet benytter dette frekvensbåndet.

**VHF-samband** gir bedre rekkevidde, og er mest benyttet for kommunikasjonsbehov i friluft. Maritim VHF er et eksempel på bruk av dette frekvensbåndet.

Det er ikke uvanlig at flere innehavere deler samme radiokanal. I dette ligger at andre brukere kan høre hva som sies. Det er normal radioprosedyre å lytte før man aktiverer radiosenderen og begynner å snakke, slik at man ikke forstyrrer andre.




Faktaboks 4-5: Telenor Maritimes dekningskart for mobilkommunikasjon i Nordsjøen /7/

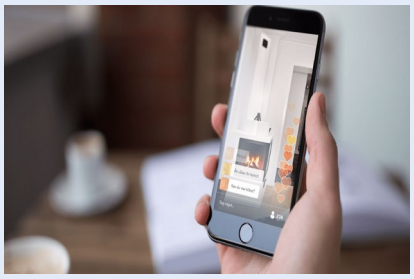
**Digitale PMR**-nett blir stadig mer utbredt, og utviklingen går fort på dette området.

Noen fordeler med digitalradio er:

- kryptering av radiosambandet hindrer avlytting
- bedre talekvalitet
- meldinger kan sendes internt i radionettet
- muligheter for gruppesamtaler eller privatsamtaler
- mulighet for linking av baser via IP
- digitale og analoge kanaler kan integreres i samme radio

**LTE** (Long Term Evolution), bedre kjent som 4G LTE eller bare 4G, er en standard basert på IP og pakkesvitsjing. Den tilbyr betydelig raskere kommunikasjon enn tidligere protokoller.

Telenor Maritim har opprettet egne basestasjoner for mobiltelefoni på flere installasjoner (Se Faktaboks 4-5). De tilbyr både privat og bedriftsintern kommunikasjon til sine kunder offshore fra slike basestasjoner. Telenor Maritime har inngått avtaler med operatørselskaper og Tampnet, for å bruke transportnettverkene til å transportere data fra/til basestasjoner og til land.



19. februar 2016 sviktet sentrale komponenter i Telenors mobilnett på grunn av innkommende signalering (SS7), som viste seg å komme fra et utenlandsk sikkerhetsselskap. Signaleringen trigget en programvarefeil i kjernenettet til Telenor. Det hadde forut for det aktuelle tidspunktet vært oppmerksomhet rundt sårbarheter i SS7.

Selv om det viste seg at utfallet ikke skyldtes en slik sårbarhet eller et forsøk på å utnytte slike, ga det læring i hvordan hendelser knyttet til signalering mellom operatører og over landegrenser må håndteres.

Faktaboks 4-6: Kjente sårbarheter i SS7 protokollen /2/.

Tampnet tilbyr sine 4G LTE basestasjoner til plattformer, borerigger, FPSOer og fartøyer, oppsatt som private virtuelle nettverk. Tampnet tilbyr i tillegg offentlige teleoperatører å samarbeide om etablering av offentlige nettverk gjennom såkalte «roamingavtaler» (se faktaboks 4-7). En slik avtale er blant annet inngått med Telia.

For å få IoT til å fungere, må en etablere kommunikasjon mellom sensorene og styreenhetene som overvåker dem. Der det ikke er tilgjengelige nettverk, vil fremtidens mobilnettverk kunne være en transportkanal for denne kommunikasjonen.


Faktaboks 4-7: Dekningsgrad fra Tampnets 4G LTE basestasjoner (skravert område på kartet) /10/.

**Low-Power Wide-Area (LPWA)**, LTE-M og NB-IOT (Narrow Band – Internet of Things) bygger på internasjonale standarder i 4G-rammeverket. Disse kommunikasjonsprotokollene gjør det mulig å kommunisere fra sensorer, IoT-enheter og via mobilnettet. Telenor og Telia tilbyr allerede disse protokollene på sine 4G-nett. Utstyr som har vært vanskelig å nå med kabler blir nå lettere tilgjengelige.

LPWA-overføringer er godt egnet til batteridrevne små enheter som sender små og få meldinger. Dette muliggjør lavt strømforbruk og lang levetid på batterier.

In 2016, the main standardization body in telecommunications, 3GPP, completed the specifications for two LPWA cellular technologies designed specifically for IoT applications: LTE-M and NB-IoT. These two new standards mainly differ in that LTE-M offers a higher data rate and allow for voice communication and mobility.

In recent years, LTE-M has gained significant traction in the US where AT&T and Verizon have rolled out nationwide networks, while NB-IoT has become more prominent in Europe where many operators have or are in the process of implementing country-wide coverage.
In China both standards are widely deployed with upwards to 250M connections expected during 2018 supported by a massive investment in the electronics and devices sectors for both network technologies to drive economies of scale and needed range of connected devices for consumer and industrial use cases. Major deployments are also underway across APAC and Middle East.

Faktaboks 4-8: Flere parallelle protokoller for IoT-kommunikasjon er under utvikling /22/.

Protokollen SS7 (Signaling System 7) ble utviklet i den tiden da sikkerhet ikke var øverst på prioriteringslisten, og er kjent for å ha en rekke sikkerhetshull. SS7 brukes til å transportere servicedata, for eksempel gjennom en telefonsamtale eller ved sending av en SMS.

Nkom har vurdert sikkerheten i signaliseringssystem nr. 7 (SS7) sammen med de nordiske søster-organisasjonene. De har også vurdert sikkerheten i protokollen Diameter som erstatter SS7 i 4G, samt sikkerheten i tale over LTE (VoLTE). Nkom er kjent med at det i noen av våre naboland har vært rapportert om tjenestenektangrep over telefoni (TDoS) /6/.

Vulnerability in Wi-Fi networks found after Positive Technologies research of 15 telecom operators in Europe and Asia.

All tested networks contain critical vulnerabilities allowing intruders to track subscriber location and cause denial of service. One in three networks is in risk of fraud attacks on operators.
4G subscribers are exposed to the same threats as subscribers as previous generation networks. Practice shows that Diameter networks are prone to attacks aiming to cause denial of service, disclose subscriber and operator information, and defraud operators. However, although the scope of attacks is limited in comparison with previous generation networks, intruders can force a subscriber's device into 3G mode and carry out further attacks on the less secure SS7 system, including eavesdropping, SMS interception, and other actions targeted abgainst subscribers.

Faktaboks 4-9: Fra "Positive Technologies Diameter vulnerabilities 2018 exposure report" /31/.

Falske basestasjoner blir ofte brukt av myndighetene ved overvåkningsbehov. Ved hjelp av hemmelige basestasjoner kan Politiets sikkerhetstjeneste (PST) og norsk politi overvåke mobilaktiviteten i et område.

I 2016 fikk Nkom 71 varsler om oppretting av falske basestasjoner fra politiet, PST og Nasjonal sikkerhetsmyndighet (NSM) /39/.

## 4.4 Radiobølgekommunikasjon

Radiobølgekommunikasjon er i mange tilfeller en foretrukket teknologi i petroleumssektoren. Ofte er radiolinker etablert som reserveløsninger på installasjoner som har fiberlinjer som hovedkommunikasjon for digital trafikk.

Det er ingen transmisjonskostnader siden overføringen er trådløs. Retningsbestemte antenner konsentrerer dataene som skal sendes. På denne måten kan en sende over avstander hvor sender/mottagere er innenfor synsvidde. Den lengste kjente radiolinken er på 123 km, fra Talismans Yme-felt til land. Rigg til-rigg forbindelser er ofte på ca. 50 km /15/, /16/. Ønskes lengre avstander kan reléstasjoner etableres.

Spesielt der hvor legging og drift av fiberkabel er vanskelig, ligger utsatt til, eller er dyrt vil radiobølgekommunikasjon kunne være et godt alternativ. Teknologien er robust, velprøvd og tilbyr høy kapasitet med liten forsinkelse. Spredning av radiosignaler er underlagt de fysiske (elektromagnetiske) lover som gjelder for refleksjon, bøyning, spalting, absorbering, spredning osv. Kraftig snø og regn kan påvirke en mikrobølgelink. Radiobølger (i vakum) sprer seg med lysets hastighet. Ulempen er at kommunikasjonen er retningsbestemt og satt opp mellom to antenner. Siden radiosignalene er elektromagnetiske, kan de utsettes for tapping, avlytting eller forvrengning. Dette vil kreve avansert utstyr og tilstedeværelse nær installasjonene. Siden avstandene er korte, vil slike forsøk være lett å oppdage. Kanskje droner i fremtiden vil bli en økende trussel for radiolinker. I dag anses radiolinker som en trygg kommunikasjonsform.

Mikrobølgesignaler trenger ikke gjennom faste objekter, og kan hindres dersom synslinjen mellom sender/mottager blir blokkert. De er også påvirkelige av interferens og elektromagnetisk stråling fra elektronisk utstyr som strømkabler og elektriske motorer.

Troposcatter-teknologien gjør det mulig å kommunisere mikrobølge-radiosignaler over lengre avstander, som 300 km eller lengre avhengig av terreng og miljøfaktorer. Troposcattere gjør det mulig å kommunisere lengre enn synsvidde ved å utnytte det såkalte «tropospheric scatter phenomen». Radiobølger blir samlet og sendt ut i retning av mottageren, og signalene blir brutt og spredt i troposfæren (laveste lag i jordens atmosfære). Det meste av signalene blir borte, men en liten, tilstrekkelig del av signalene kan fanges opp av mottagere /45/. Tropposcatter-teknologien har ikke fått noen stor utbredelse i norsk petroleumssektor /46/.

## 4.5 Bruk av satellittkommunikasjon i petroleumssektoren i dag

Flere leverandører tilbyr satellitt-tjenester til petroleumsnæringen og til maritim industri. Rådende teknologi er VSAT på Ku- eller Ka-frekvensbåndet via HTS (High Throughput Satellites) lokalisert i GEO

VSAT (Very Small Aperture Terminal)
En VSAT terminal er en toveis fastmontert terminal eller en maritim stabilisert parabol antenne med diameter mindre enn 3 m. Antennen kommuniserer med geostasjonære satellitter som er posisjonert 36 000 km over ekvator.

Faktaboks 4-10: VSAT (Very Small Aperture Terminal).

(Geostationary Equatorial Orbit). Maksimal informasjonsrate (MIR) kan være opp til størrelsesorden 125 Mbps (mottak) / 25 Mbps (sending), avhengig av abonnement og utstyr /48/.

Ulemper med VSAT er begrenset båndbredde, høy pris og høy forsinkelse (rundt 500 ms). I petroleumssektoren benyttes nå ofte satellittforbindelser som et supplement til fiberbaserte nett for faste installasjoner, mens for flyttbare innretninger vil satellittforbindelse stå for hovedkommunikasjon.

Maritime VSAT parabolantenner montert på skip, eller innretninger som i større eller mindre grad er i kontinuerlig bevegelse, krever en gyrostabilisering. Åpningsvinkel på en parabol på -3 dB vil være i størrelsesorden én grad avhengig av blant annet frekvens og diameter på antennespeilet. En liten pekefeil vil dermed føre til store tap i overføringen, og fare for interferens med andre GEO-satellitter. Tilgjengeligheten på VSAT-forbindelser er sårbare for interferens med annet utstyr, og fra vedlikeholds-operasjoner hos sentrale satellittoperatører.

Satellittkommunikasjon sammen med fiberbaserte nettverk gir både redundant og uavhengig kommunikasjon til enheten. Hvis kritiske operasjoner er avhengig av kommunikasjon mellom flere enheter, eller enheter og land, vil dette bidra til å redusere nedetid på produksjonen. Det krever en god strategi for å sørge for at nødvendig kommunikasjon blir prioritert og har nødvendig båndbredde over satellitt, og at forsinkelsen i denne linken er håndterbar. Erfaringen er at forsinkelsene med oversendelser av meldinger over satellitt gjør det vanskelig å kommunisere tidskritiske prosess-styringsdata.

## 4.6 Fiberbaserte nett

Datanettverket i Nordsjøen er i dag primært basert på fiberoptisk kabling på havbunnen. Det har vært få skader på denne infrastrukturen, men i områder med grunt vann (15-20 meter) og mye havstrøm har det oppstått 5-6 skader i løpet av de siste 15 årene /20/.

Tampnet opererer det største offshore kommunikasjonsnettverket i Nordsjøen og betjener de fleste olje- og gassinstallasjoner med fiberkabler og punkt-til-punkt radiolinjeforbindelser (se faktaboks 3-1). Tampnet tilbyr fysisk kommunikasjon mellom to punkter. Brukerne kopler sitt utstyr på definerte grensesnitt. Sikring av egen trafikk på nettverket er brukeren selv ansvarlig for.

Den store overføringskapasiteten på fibernettene har muliggjort integrerte operasjoner hvor all eller deler av styringsprosessene på anleggene til sjøs gjøres fra kontrollrom på land.

Fibernettene er passive. Kommunikasjon over lengre avstander enn det som er vanlig på norsk sokkel (>100 km) krever forsterkere («repeatere») som kan være enten aktive eller passive.

UPS fra to uavhengige kilder bør være et designkrav. Tampnets oversikt over og styring av strømforsyning og eget utstyr er informasjon som bør beskyttes.

Ifølge avsløringene fra Snowden pågår det også en omfattende organisert avlytting og tapping av trafikk på fiberkabler utført av forskjellige lands etterretningsorganisasjoner /49/.

## 4.7 Den felles nasjonale «digitale grunnmur» som informasjonsbærer for sektoren

Norge er en av verdens mest digitaliserte nasjoner. Den nasjonale kommunikasjonsmyndigheten (Nkom) omtaler fremtidens nasjonale telekomnettverk som vår «digitale grunnmur». På denne grunnmuren vil samfunnets fremtidige digitale tjenester og telekommunikasjon tilbys som fundamentet for vitale samfunnsfunksjoner /2/.

Ved å etablere felles tjenester som bærer viktige samfunnsfunksjoner, øker sårbarheten og mulig omfang ved uønskede hendelser. Mange sentrale registre og tjenester er samlet hos få aktører. Eksempler her er folke-, foretaks- og eiendomsregistre samt bank, hvor samfunnet vil kunne lammes ved angrep på denne kritiske infrastrukturen. Cyberkriminalitet er blitt en gigantindustri. EUROPOL beregner årlige tap til 20 milliarder euro i 2012, og industrien er ansett for å være mer profitabel enn narkotikaindustrien.

Petroleumsnæringen er også en bruker av den digitale grunnmuren. Transport av data på land fra ilandføringssteder til for eksempel et operatørselskap sitt hovedkontor, blir gjort på samme fiberlinjer som annen offentlig datatransport.

Mandag 14. januar 2018 iverksatte PST etterforskning av nettverksangrep mot datasystemene til Helse Sør-Øst. Forholdet etterforskes ifølge en melding som mulig brudd på straffeloven § 121 Etterretningsvirksomhet mot statshemmeligheter.

Faktaboks 4-11: Nettverksangrepet mot Helse Sør-Øst /18/.

Trusselaktørenes muligheter til å ramme telekominfrastrukturen i sektoren er mange. Det er naivt å tro at slike aktører ikke er bevisste på hvilke muligheter som eksisterer og er i stand til å utnytte dem.

Totalforsvaret av den norske digitale grunnmur er et offentlig ansvar. Her deltar Nkom sammen med Politiets sikkerhetstjeneste (PST), Etterretningstjenesten (E-tjenesten), Nasjonal sikkerhetsmyndighet (NSM), Direktoratet for samfunnssikkerhet og beredskap (DSB) og leverandører.

I løpet av 2016 og første halvdel av 2017 mottok Nkom varsler om 150 uønskede hendelser i kommunikasjonsnettet /2/. Omfanget av hendelser er sammenlignbart med årene før. De vanligste årsaker er fiberbrudd, strømbrudd og utilsiktede feil i utstyr eller programvare. Hendelsene som har hatt størst kundekonsekvens har vært hendelser hvor det har oppstått feil i programvare eller konfigurasjon. Det er slike logiske feil som har størst potensiale til å ramme mange brukere av telekomtjenester samtidig.

IKT-angrep har også rammet telekominfrastruktur og -tilbydere. Foreløpig har dette ikke rammet telekomsektoren i Norge i stor grad, men vi må være forberedt på at dette vil kunne skje. Det har vært en rekke hendelser som skyldes feilkonfigureringer og programvarefeil i telenettet. Nkoms rapport «EkomROS 2019 – risikovurdering av ekomsektoren» beskriver flere av disse /2/.

Sentralisering av teletjenester gir økt skadepotensiale. En av anbefalingene fra det regjeringsoppnevnte Lysneutvalget er å redusere avhengigheten av Telenors kjerneinfrastruktur. Telenors kjerneinfrastruktur inngår som en komponent i nært sagt alle digitale verdikjeder på land. Utvalget anbefaler at det arbeides mot et målbilde der minst ett landsdekkende kjernenett til, som er på samme nivå som Telenor sitt, etableres /20/. Telenor er et attraktivt mål for avanserte trusselagenter på grunn av sin sentrale rolle som operatør av den nasjonale og sosiale infrastruktur, og siden de har kunder fra alle industrier og sektorer.

Olje- og gassnæringen er også en bruker av denne felles digitale grunnmuren. Transport av data mellom landbaserte terminaler og anlegg foregår på det offentlige nett. Fjernstyring av ubemannede installasjoner vil derfor avhenge av at grunnmurens fiberlinjer og kommunikasjonslinjer er operative og sikre.

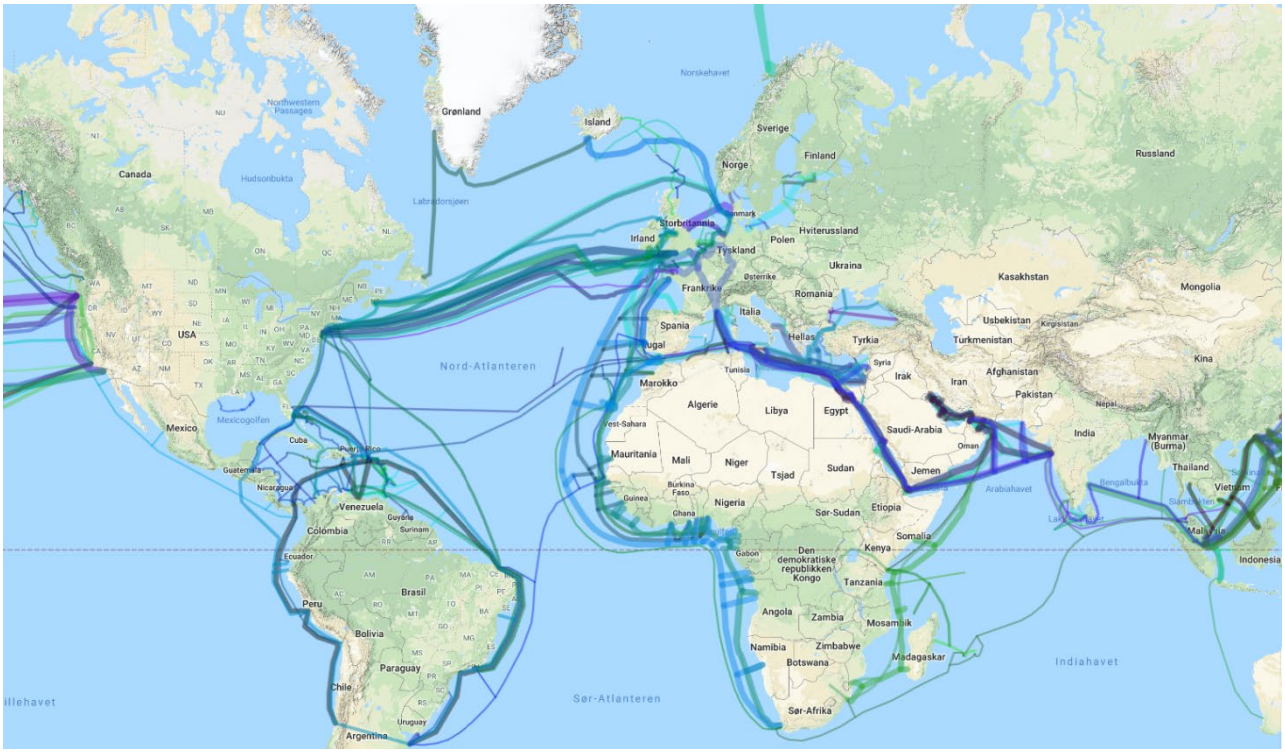
## 4.8 Sikkerhet i felles internasjonale fiberbaserte transportnett

Økt globalisering av næringen og sterkere avhengighet til utenlandske samarbeidspartnere gjør at vi blir mer avhengig av felles, internasjonale telekommunikasjonsløsninger. Økt grad av tjenesteutsetting bidrar til dette. 97 % av all interkontinental elektronisk kommunikasjon går via 223 undersjøiske fiberkabelsystemer /23/. I faktaboks 4-12 har vi tatt med et kart med en oversikt over kjente internasjonale kableruter som finnes.

Som vist i faktaboks 4-12 går fiberforbindelser til land vi kjøper tjenester fra i Asia gjennom Suez-kanalen. Det er liten eller ingen alternativ kapasitet dersom man får linjeutfall på nettene i dette området.

Avhengighet til linjer i andre land gjør at vårt tjenestetilbud på telebaserte tjenester kan bli skadelidende ved politisk uro, konflikter eller interne forhold i et annet land. Sikkerhetstruende hendelser som terror og organisert kriminalitet i andre land vil kunne påvirke våre kommunikasjonssystemer.

Selv om det legges redundante linjer er ofte ilandføringsterminalene felles. Sikkerhet på ilandføringsterminalene er viktig, fordi mange personer fra forskjellige organisasjoner har tilgang her. Det samme gjelder på installasjonene hvor felles kabelgater, koplingsskap, strømforsyning, etc. benyttes for flere forbindelser.




Faktaboks 4-12: Oversikt over internasjonale offentlige fibernettverk /37/.

Rapporten "Treats to undersea cable connections" utarbeidet av det amerikanske Public-Private Analytic Exchange Program (AEP) /23/ analyserer sikkerheten på de internasjonale offentlige fibernettverkene.

Rapporten sier at i tillegg til å tilrettelegge for enorme kommersielle muligheter, representerer forbindelsene stor risiko. Ifølge rapporten skyldes dette at:

- internasjonale kabler som skal dekke mange forskjellige behov
- høy kompleksitet og mangel på oppmerksomhet hos sikkerhetsansvarlige
- variabelt nivå på robusthet og redundans
- få leverandører av fiberkabler, samt stadige organisasjonsendringer med sammenslåinger og oppkjøp
- påvirkning av forskjellige lands lover og politikk
- økning i globale IKT- trusler
- sårbare sentrale komponenter

IKT-domenet har blitt et viktig nytt domene for krigføring. Manipulering og forvrengning av informasjon er et sårbarhetsområde. Vi ser nå også bilder i media av militære marine kapasiteter som er spesialutstyrt for å kunne kappe kabler på store havdyp.

# 5 TELEKOMMUNIKASJONSSYSTEMER

Generelt for lokale systemer gjelder at systemene bør eksistere på egne fysiske nettverk, eller på et logisk nett (VLAN) i felles nettverksinfrastruktur. Det er et mål at flere systemer ikke skal benytte samme logiske nett, dvs. at en ikke samler ulike systemer med ulik funksjonalitet og fra ulike leverandører, på samme logiske nett. De ulike logiske nettverkene skal være adskilt, f.eks. ved bruk av brannmur.

Ulike systemer bruker forskjellige kommunikasjonsprotokoller. Det kan være standard TCP/IP-protokoller, leverandørspesifikke TCP/IP-protokoller samt spesifikke protokoller som ikke bruker TCP/IP som grunnprotokoll. Her kreves det at nettverket støtter intern kommunikasjon uten begrensninger til type protokoll. Mange kommunikasjonssystemer er utviklet for Microsoft Windows-baserte datamaskiner. Dette gir flere fordeler for drift og integrasjon, men representerer sikkerhetsutfordringer pga. det store brukermiljøet og kjente feil som kan bli utnyttet av dem som vil avlytte eller forårsake skade.

På system med intern nettverkskommunikasjon er det ønskelig med overvåking for å oppdage unormal oppførsel. Teknikker som kan anvendes til dette kan være probing/sniffing eller bruk av «low level» trafikklogging med analyser av loggdata, enten i sanntid eller regelmessig i etterkant. Trafikkloggingsmekanismer kan blant annet være med hjelp av protokoller som Netflow, Sflow og Nbar (Network Based Application Recognition).

Gjenkjenning av unormal oppførsel kan bli gjort med hjelp av protokoll-whitelisting (godkjenning av protokoller) og trafikk-«baselining», dvs. data som blir samlet inn over en gitt tid (dager/uker). Etter at «baselining» er gjort, kan større avvik fra baseline (normal oppførsel) bli identifisert som unormalt og utløse en alarm.

## 5.1 Telecommunication Monitoring System (TMS)

I henhold til T-101 er TMS et obligatorisk system på en offshore installasjon. Krav og funksjonalitet til TMS er beskrevet i T-101 §6, men her beskrives ikke krav til IKT-sikkerhet og beskyttelse av systemet.

Telekomsystemer skal monitoreres av TMS, det samme med alle kritiske kommunikansjonslinker, hvis de ikke blir monitorert av et annet system.Tilstanden kan overvåkes på mange måter: ved bruk av IP-protokoll, serielt grensesnitt eller med relékontakt. For systemer som er monitorert ved bruk av IP-basert protokoll er det viktig å ta hensyn til at TMS blir et sentralt knutepunkt for alle monitorerte system, og at monitoreringsprotokollen kan være sårbar. Det er kritisk å herde og beskytte TMS slik at det ikke kan bli misbrukt til å angripe andre telekomsystemer.

De vanligste IP-protokollene som er i bruk er:

- SNMP (Simple Network Management Protocol)
- ICMP (Internet Control Message Protocol)
- ModbusTCP (ikke mye brukt innen telekom)

Dette er gamle protokoller som ble utviklet lenge før IKT-sikkerhet var i fokus.

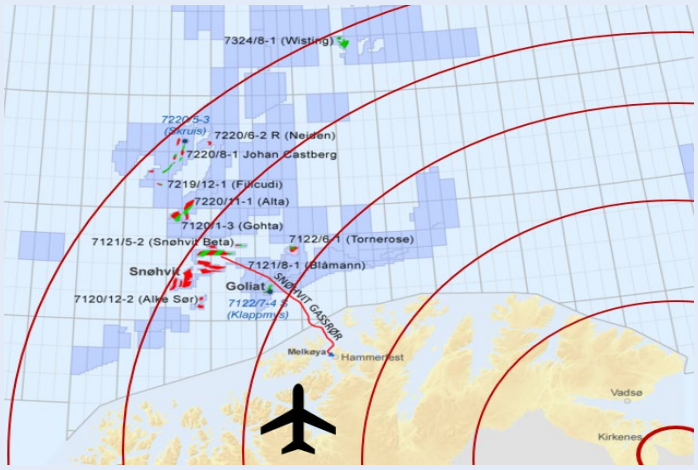
Ettersom systemet er sentralt for de fleste, om ikke alle telekomsystemer, er det viktig å fokusere på IKT-sikkerhet ved implementering og forvaltning av systemet. De mest brukte protokoller og noen av sårbarhetene er beskrevet i kapittel 6.

## 5.2 Sårbarheter i GNSS-baserte systemer

Global Navigation Satellite System (GNSS) er fellesbetegnelsene på satellittbaserte systemer for navigasjon, posisjonering og tidsangivelse. Systemer for navigering, distansemåling, posisjonering og sanntidsklokke, er alle definert som telekommunikasjonssystemer i T-101, og er tradisjonelt basert på informasjon fra GNSS. Det amerikanske GPS og det russiske GLONASS har vært etablert i lang tid, mens europeiske Galileo og kinesiske BeiDou fortsatt er under oppbygging. Mens Galileo er et sivilt system, er de tre andre i utgangspunktet laget for militære formål. For å få en nøyaktig posisjon må GNSS-signalene korrigeres på grunn av forstyrrelser som skyldes atmosfæriske eller andre forhold. Informasjon sendes tilbake til satellittene etter å ha blitt korrigert ved hjelp av et nettverk av bakkestasjoner.

GNSS-signalene kommer fra satellitter. Signalene er svake og sårbare for forstyrrelser. Signalene kan hovedsakelig forstyrres på to måter: gjennom jamming og spoofing. Å jamme betyr å sende støysignaler i det aktuelle frekvensområdet for å forstyrre mottaket av signaler. Spoofing går ut på å sende falske GNSS-signaler som manipulerer tidsinformasjon og posisjon. I de militære nettene er det å forvente at begge disse teknikkene vil kunne bli tatt i bruk i en konfliktsituasjon. Vi har allerede sett at jamming er brukt under store militærøvelser (se faktaboks 5-1). Spoofing vil kunne få mer alvorlige konsekvenser, siden aktive operasjoner kan bli villedet. Spoofing krever mer avansert utstyr enn jamming. Billig utstyr for jamming er lett tilgjengelig, og blir blant annet brukt av personer som ønsker å skjule sin posisjon av forskjellige grunner.

Nkom angir i sin EkomROS-rapport fra 2019 at økt avhengighet til satellittnavigasjonstjenester er et risikoområde /2/. Utfall av GNSS-signaler kan få alvorlige konsekvenser for sanntidsoperasjoner i olje- og gassnæringen. GPS-systemet har eksistert i mer enn 25 år og er blitt en sentral, innarbeidet del i mange applikasjoner. Synkroniserte prosesser for sending og mottak kan bli forstyrret. I forsendelsesprotokoller innen telekommunikasjon ønsker en å øke hastighetene ved å bruke tidsstyrte protokoller i stedet for tradisjonelle protokoller med aktiv kvittering for mottak.




I oktober og november 2018 opplevde flere fly forstyrrelser i sine navigasjonssystemer i luften mellom Kirkenes og Lyngen i Troms.

Forsvarsdepartementet har bekreftet til NTB at Russland sto bak jammingen av GPS-signaler fra 16. oktober til 7. november. Ifølge departementet ble blokkeringen av GPS-signalene gjennomført av russiske landstyrker på Kolahalvøya.

Faktaboks 5-1: Jamming og spoofing av GPS-signaler /36/.

Elektroniske sjøkart er blitt en viktig del av maritim navigasjon. I tillegg til å bestemme skipets posisjon brukes GNSS systemer blant annet til «tracking» systemer hvor skip skal følge en bestemt rute. Dynamisk posisjoneringssystemer benyttes hvor skip eller offshore innretninger skal holde en bestemt posisjon over havbunnen uten bruk av anker, men ved hjelp av egne propeller.

IMO Polar Code krever at skip som skal gå nord for 80 grader nordlig bredde skal ha GNSS kompass. Bakgrunnen for dette er at nøyaktigheten til magnetkompass og gyrokompass gradvis blir dårligere desto lenger nord et skip går. Teststandarden for gyrokompass definerer nøyaktighetskrav opp til 60 grader nordlig / sørlig bredde /57/. Avhengig av teknologi vil gyrokompass virke lenger nord og sør, men med avtagende nøyaktighet. Tradisjonelle gyrokompass vil ikke virke ved polene. Gyrokompass vil trenge informasjon om fart, kurs og bredde-korreksjon. GNSS mottaker kan være et hjelpemiddel til dette.

Posisjonen til personer om bord på en installasjon kan følges med stor nøyaktighet dersom de er utstyrt med en sender som rapporterer til et sentralt system. En slik posisjonssender kan plasseres i en mobil-radio eller i en klokke. Prosesser som må synkroniseres på tid benytter GNSS-klokken som gir nøyaktig synkronisert tid uavhengig av lokasjon. Fravær av denne kilden vil kunne medføre at prosesser stopper opp. Forvrengning av data kan få alvorlige konsekvenser for pågående prosesser.

## 5.3 PRS (Personnel Registration System)

PRS, også kjent som PTS («Personnel Tracking System») og POB (Personnel on Board) er beskrevet i T-101 §19.

Registrering av mannskap som skal være ombord på en installasjon, blir gjort ved ombordstigning på helikopter. Helhetsoversikt over personale som er om bord på en installasjon er alltid kjent. Et eget elektronisk PRS på installasjonen er ikke et obligatorisk krav.

På større installasjoner og når flere plattformer er knyttet sammen, er det viktig å ha oversikt over mannskapet samt på hvilken plattform hver enkelt person befinner seg til enhver tid. PRS har en viktig funksjon i kritiske situasjoner. Systemet må defineres som sikkerhetskritisk og må designes og beskyttes deretter.

T-101 beskriver krav til funksjonalitet og intern design på høyt, men tilstrekkelig nivå. T-101 beskriver ikke krav til IKT-sikkerhet og beskyttelse av PRS.

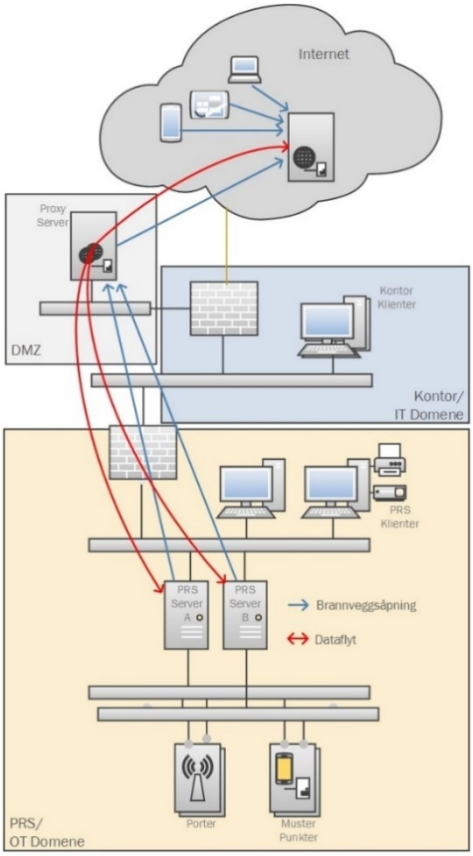
Når et PRS er installert lokalt må systemet få mannskapsoversikt fra det sentrale PRS systemet (Dawinci). Lokalt PRS holder informasjon om hvem som kommer om bord, hvem som forlater installasjonen samt lugar- og livbåttildeling. I det lokale PRS er det en oversikt over hvor på installasjonen hver enkelt person er.

Dawinci-tjenesten har til nå vært gjort tilgjengelig via SOIL (Secure Oil Link – omtalt senere i dokumentet), men flyttes nå til skyen og er dermed tilgjengelig via internett. Det er nå mulig for de som reiser offshore å sjekke status på flight og sjekke inn via internett.

PRS på en installasjon må få oppdateringer på mannskapsendringer fra denne felles databasen som er plassert på internett. Her kan det brukes direkte eller indirekte databasekobling, for eksempel en WebSocket-protokoll som er beskrevet i kapittel 6. I faktaboks 5-3 vises et eksempel på en helhetsoversikt over dataflyt hvor PRS er involvert.

Her er det viktig å se på det store bildet, og ikke introdusere unødvendige sårbarheter. Dawinci er et kritisk system i petroleumssektoren, og det bør være høyt fokus på IKT-sikkerhet. At Dawinci er tilgjengelig fra internett gjør at systemet har stor angrepsoverflate, og som regel er potensielle angripere allerede kjent med mulige sårbarheter før driftsansvarlige er det.

Det må være fullt fokus IKT-sikkerhet ved implementering og forvaltning av systemet, og ikke minst i datasynkroniseringen mellom lokale PRS og Dawinci.




Faktaboks 5-3: Dataflyt av PRS data på tvers av sikkerhetssoner.

## 5.4 SOIL (Secure Oil Link)

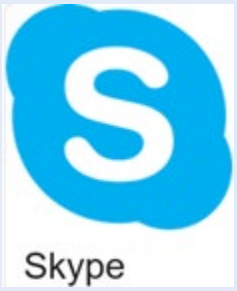
SOIL er et privat nettverk som sørger for at aktører som er involvert i aktiviteter i petroleumssektoren på den norske kontinentalsokkel, kan utveksle data på en sikker måte. SOIL tilbyr også flere fellestjenester for sektoren i nettet. Nettet ble åpnet i 1998, og har i dag mer enn 140 registrerte firma som brukere. Brukere er operatørselskaper, lisenseiere, leverandører og servicekontraktører. Et utvalg med SOIL-tjenesteleverandører opererer nettet på oppdrag fra EPIM /38/.

SOIL har vært et positivt bidrag til sikkerheten i telekomløsningene i bransjen. Et så omfattende privat nettverk vil ha begrenset beskyttelse for de avanserte og målrettede trusselaktører. Mange tjenesteleverandører er engasjert i drift av nettet, og rutinene for å skaffe seg tilgang er mulig å utfordre.

Med virtuelle nettverk og internett sine muligheter til å opprette lukkede brukergrupper, blir det enkelt å etablere private nettverk. Eksisterende privatopererte nettverk som SOIL, utfordres.

## 5.5 Talebaserte systemer

VOIP er et akronym for «Voice over Internet Protocol» eller «Voice over IP». VOIP har blitt implementert på flere forskjellige måter, og med forskjellige protokoller basert på åpne standarder. De siste 10 årene har det vært en massiv omlegging fra tradisjonelle kabelbaserte teleløsninger til VOIP over trådløse nett. For bedrifter har dette vært et betydelig kostnadsbesparende tiltak. VOIP kommunikasjon kan enten gjøres ved spesiallaget teleutstyr, ved tjenester som Skype, Google Talk eller ved bruk av moderne smarttelefoner.




Companies may also willingly or unwillingly introduce backdoors to their software that help subvert key negotiation or bypass encryption altogether. In 2013, information leaked by Edward Snowden showed that Skype had a backdoor which allowed Microsoft to hand over their users' messages to the NSA despite the fact that those messages were officially end-to-end encrypted.

Faktaboks 5-4: Meldingsovervåkning av Skypemeldinger /29/.

# 6 PROTOKOLLER

I dette kapittelet gjennomgår vi noen av de nettverksprotokollene som er mest vanlige i tele-kommunikasjonssystemer i petroleumssektoren. Dette gjelder der hvor ulike systemer kommuniserer, nettverkstrafikk passerer grenser mellom systemer eller sikkerhetsdomener, samt protokoller som er brukt for systemstyring og -monitorering.

Beskrivelsen dekker kun et utvalg og er på ingen måte komplett. Det finnes et utall protokoller på flere nivå. OSI-modellen er en internasjonal referansemodell for datakommunikasjon. Denne modellen deler datakommunikasjon inn i syv lag[1]:

[1] Mer detaljert beskrivelse av OSI modellen finnes blant annet i Store Norske Leksikon: https://snl.no/OSI

- Lag 1 - fysiske lag: omhandler måter å sende datastrøm ut på en media som kan være kabel, fiber, radiobølger etc. For eksempel 10/100/1000/10gBASE, blåtann og T1.
- Lag 2 – DataLink-laget: protokollene som to naboenheter bruker for å kommunisere. Eksempler er Ethernet, ATM, FrameRelay, Profibus og MPLS.
- Lag 3 t.o.m. 7: nettverksprotokollstakken som to enheter (klient og server) bruker for å kommunisere seg mellom i alt fra nettverks- til applikasjonslag.

IP er den dominerende Lag 3-protokollen som er i bruk i dag, men historien går tilbake til tidlig 70-tallet. Det finnes uendelig mange IP-baserte protokoller og protokollvarianter, og kun et utvalg omtales i denne rapporten.

## 6.1 Internet Control Message Protocol (ICMP)

ICMP (også kalt PING) er en enkel protokoll brukt ved feilsøking og verifisering. ICMP ble utviklet tidlig på 1980-tallet, da IKT-sikkerhet ikke var i fokus. ICMP er en nyttig og mye brukt protokoll.

ICMP kan bli brukt til å angripe systemer. Ping of Death (PoD) er en kjent angrepsemetode for å utføre tjenestenekt (DoS) og distribuert tjenestenekt (DDoS). PoD utføres ved å sende manipulerte ICMP-pakker hvor målet er å krasje, fryse eller gjøre et system ustabilt.

## 6.2 SNMP (Simple Network Management Protocol)

Historien til SNMP går tilbake til 1988 da første versjon av SNMP (v1) ble tatt i bruk. Senere kom SNMP v2 i noen varianter, men det var ikke før i 1999 da SNMPv3 ble introdusert at sikkerhet ble lagt til i protokollens standard. I de tidligste versjonene er autentisering manglende eller svak. I v3 ble autentisering og kryptering introdusert.

Det finnes to hovedvarianter av protokollen:

- SNMP-Trap er en protokoll hvor endeutstyr (klient) initierer og sender tilstandsinformasjon til mottakers server
- SNMP (typiske funksjoner er: get og set) hvor sender (server) sender en forespørsel til en enhet for å spørre om tilstand, endre parametere etc.

Som navnet på protokollen tilsier er SNMP i utgangspunkt en styrings-protokoll som tillater at:

  - konfigurasjon kan endres
  - konfigurasjonsfil kan slettes
  - tjenester kan stoppes
  - nettverksport kan tas ned

Når protokollen ikke er brukt til monitorering, kan den brukes til å endre og ødelegge funksjonalitet. Det er viktig med høyt fokus på IKT-sikkerhet når protokollen er brukt i kritiske systemer.

Til bruk i industrielle systemer i petroleumsvirksomheten bør kun SNMPv3 brukes med sterk autentisering.

## 6.3 Telnet / SSH (kommandolinje- og terminalprotokoller)

Telnet og SSH (Secure Shell) er mye brukte protokoller for blant annet administrasjon av teknisk utstyr.

Telnet ble utviklet i 1969, og er en av de første TCP/IP-standardene. Denne protokollen har ingen sikkerhetsmekanisme, all kommunikasjon er i klartekst inkludert brukernavn og passord. Avlytting kan

på en enkel måte gi uautoriserte personer full tilgang til kritisk utstyr. Telnet burde ikke brukes til administrasjon av telekomutstyr eller generelt i det industrielle domenet.

SSH protokollen kan brukes til samme formål. Den er designet for å ivareta IKT-sikkerhet, kryptere datakommunikasjon og har sterk autentisering.

SSH bør brukes når formålet med terminalprotokoll er administrasjon eller tilsvarende. SSH kan også brukes til filoverføring, og er beskrevet senere i dokumentet.

## 6.4 HTTP / HTTPS

HTTP (Hyper Text Transfer Protocol) er protokollen som er brukt for å få tilgang til webinnhold. Protokollen er mye benyttet som brukergrensesnitt til systemer og applikasjoner, inkludert telekom og andre industrielle IKT systemer. Nettlesere er mye brukt for administrasjonsgrensesnitt for telekom-utstyr og da er HTTP ofte standardprotokollen. HTTP er en klartekst protokoll. Ved autentisering brukes enkel koding av brukernavn og passord, men kryptering benyttes ikke. Passord er lett å dekode.

På grunn av sikkerhetsproblemer har HTTP generelt vært erstattet av HTTPS som protokoll for å gjøre nettsider tilgjengelige på internett. HTTPS er den sikre versjonen av HTTP. HTTPS bruker som regel TCP port 443 og styrker HTTP ved å inkorporere SSL (Secure Socket Layer) og senere TLS (Transport Layer Security) protokoller for kryptering, og sertifikatbasert autentisering. SSLv1 ble ikke tatt i bruk, SSLv2 ble introdusert i 1995 og hadde da flere sårbarheter. Den ble fulgt opp med SSLv3 ett år senere. TLS ble introdusert i 1999 som ny versjon av SSL. SSL protokollene ble avskrevet av IETF (Internet Engineering Task Force) for noen år siden.

HTTPS er den verdensomspennende standarden som brukes for betalingstransaksjoner og for andre datasensitive Internett-transaksjoner.

HTTP brukes fortsatt endel som bruker- og administrasjons-grensesnitt på telekom og industrielle systemer.

Det anbefales på det sterkeste at HTTP deaktiveres og at HTTPS benyttes med TLS som sikkerhetsmekanisme.

## 6.5 WebSocket, WSS over HTTP(S)

HTTP(S) er i utgangspunktet en enveis-protokoll som sender forespørsler til server og stenger forbindelsen når svar er mottatt.

WebSocket er forskjellig fra HTTP(S), men begge protokollene er lokalisert i lag 7 i OSI-modellen og er avhengige av TCP.

WebSocket-protokollen gjør interaksjon mellom klient og server ved dataoverføring i sanntid mulig. Dette inkluder en standardisert måte for serveren å sende innhold til klienten, uten først å bli bedt om dette fra klientsiden. Meldingene sendes fram og tilbake samtidig som forbindelsen er åpen. På denne måten kan en toveissamtale finne sted mellom klienten og serveren igjennom en enveis (utgående) brannmursåpning.

Eksempler på bruk av WSS er datautveksling og databasesynkronisering. På en tegning ser utgående datakommunikasjon fra et industrielt system til en server hos en tredjepart trygt ut, hvor HTTP(S) er brukt og proxyserver i DMZ er brukt som mellomlag for å øke sikkerhet. I et slikt scenario kan det være skjult en toveis tunnel som proxyserver ikke beskytter mot. Sårbarheten i serveren hos tredjepart kan da i prinsippet benyttes til å direkte angripe servere i det industrielle domenet.

Kort sagt, det er viktig å ta hensyn til at en enveis HTTP(S) brannmursåpning kan være bærer for en permanent tunnel som kan brukes for kommunikasjon i begge retninger. Dette selv om en anser forbindelsen som sikker, og selv om en kommuniserer gjennom en proxyserver.

## 6.6 RPC (Remote Procedure Call)

RPC er en protokoll som brukes for å utføre en oppgave (prosedyrekall) på en annen datamaskin, men oppgaven er kodet som om det var et lokalt prosedyrekall, uten behov for å eksplisitt spesifisere detaljene for interaksjonen. Programmereren skriver med andre ord det samme programmet, uten å ta hensyn til om prosedyren for det utførende programmet er lokalt eller på en annen maskin.

Bruk av denne protokollen, spesielt mellom systemer og/eller sikkerhetslag kan føre til flere IKT-sårbarheter.

RPC Portmapper er en tjeneste som brukes for å hjelpe et system med nettverksoppgaver. Dette kan tillate en tredjepart / angriper uautorisert tilgang til et system, hvor angriperen kan utføre DoS eller DDoS angrep rettet mot andre maskiner.

Svakheter relatert til RCE («Remote Code Execution») kan også benyttes til angrep. En angriper kan for eksempel benytte svakhetene til å installere programvare, opprette nye brukere med fulle rettigheter samt endre eller slette data.

RPS er designet for å øke fleksibilitet, men ikke sikkerhet. Bruk og tillatelse i brannmur for RPC imellom sikkerhetslag burde ikke praktiseres i industrielle miljø, eller brukes på en veldig forsiktig måte.

## 6.7 Filoverføringsprotokoller

Det finnes flere protokoller som benyttes for filoverføring. Når en protokoll er valgt for filoverføring mellom systemer innen OT-domenet, samt for filoverføring imellom OT og IT, må både protokollens sikkerhet og systemenes interoperabilitet vurderes. I de neste delkapitlene beskrives kort de mest brukte protokollene.

### 6.7.1 FTP (File Transfer Protocol)

Filoverføringsprotokollen FTP er nok den første protokollen mange tenker på når det er behov for filoverføring.

Ulempen med FTP er at den ble utviklet lenge før det var fokus på IKT-sikkerhet, protokollen er ikke sterk på sikkerhetssiden. All kommunikasjon er i klartekst, inkludert brukernavn og passord. Dersom en trenger beskyttelse med tanke på personvern og forskrifter om datasikkerhet som HIPAA, PCS og SOX, bør ikke FTP velges som protokoll.

En må forstå funksjonaliteten i protokollen når FTP skal rutes igjennom brannmuren. Protokollen kjører en sesjon for styring, og en annen sesjon for selve datastrømmen. Protokollen kan kjøre i to moduser: passiv og aktiv. I aktiv modus velger serveren en tilfeldig TCP-port for datastrømmen, og forteller klienten hvilken port som skal brukes. Brannmuren må «lytte» og forstå protokollen slik den kan legge til en åpning for datastrømmen basert på beskjed fra FTP-server. De fleste moderne brannmurer har innebygd funksjonalitet for, og støtter protokollen.

FTP-protokollen brukes mye i OT-domenet i petroleumssektoren. IKT-sikkerhet og sårbarhet må vurderes nøye når denne protokollen anvendes.

### 6.7.2 HTTP / HTTPS

HTTP(S)-protokollen kan brukes til filoverføring. HTTP protokollen har som beskrevet tidligere vesentlige sårbarheter som en må være klar over, spesielt ved bruk i et OT-miljø.

Den sikre varianten (HTTPS) med TLS som krypteringsmekanisme bør brukes for filoverføringer.

### 6.7.3 FTPS (File Transfer Protocol - SSL)

Det finnes en variant av FTP hvor IKT-sikkerhet er ivaretatt, dvs. FTPS som er beskyttet med SSL eller TLS. Ved bruk av FTPS beholdes fordelene med FTP, men i tillegg inkluderes SSL eller TLS sikkerhetsfunksjoner som kryptering samt sertifikatbasert server- og klientautentisering. Som nevnt tidligere, ble SSL avskrevet i 2015 og TLS bør heller brukes.

FTPS benytter samme mekanisme som FTP, og må ha en brannmur som støtter protokollen når den kjører i aktiv modus.

### 6.7.4 SFTP (SSH File Transfer Protocol)

SFTP er en filoverføringsprotokoll som bruker SSH (beskrevet i delkapittel 6.3) som grunnprotokoll. Styring og datastrøm benytter samme sesjon/TCP-port 22 og er dermed ikke en utfordring når den rutes gjennom en brannmur.

En av ulempene med protokollen er at den ikke er standardisert, og generelt ikke er en del av et operativsystem. Det kan være kompatibilitetsutfordringer mellom programvarer fra forskjellige leverandører.

# 7 PETROLEUMSSEKTORENS ROLLE I NØDKOMMUNIKASJON TIL HAVS

Telekommunikasjon i petroleumssektoren inkluderer også systemer for nødkommunikasjon. I dette kapittel er systemene som inngår i denne kategorien kort gjennomgått.

Global Maritime Distress and Safety System (GMDSS) er et sett med internasjonalt godkjente prosedyrer og kommunikasjonsprotokoller for økt sikkerhet og for å kunne redde fartøy, offshore innretninger og fly i nød.

GMDSS består av en rekke systemer. Systemene er ment å dekke følgende funksjoner: sende nødmelding (inkludert angivelse av posisjon for enhet i nød) fra enhet til land og motta nødmelding fra land til enhet, sende og motta nødmelding fra enhet til enhet, koordinering av søk og redning, lokalisering, kringkasting av maritim sikkerhetsinformasjon, generell kommunikasjon og bro til bro-kommunikasjon. Behov for radioutstyr er i GMDSS avhengig av skipets seilingsområde eller offshore innretningens lokasjon.

Installasjons krav, bestykningskrav og referanser til ytelsesstandarder for GMDSS systemene er blant annet gitt i IMO (International Maritime Organization) publikasjonene SOLAS (Safety of Life at Sea) og MODU (Mobile Offshore Drilling Unit) Code. I tillegg til GMDSS kraven gitt av IMO publikasjonene, kan nasjonale myndigheter ha tilleggskrav.

Telenor kystradio drifter kystradiostasjonene sør og nord som er en del av redningstjenesten i Norge og er et bindeledd mellom fartøyer i nød og Hovedredningssentralen /58/. Telenor Kystradio ha ren teknisk infrastruktur med blant annet 123 VHF basestasjoner som dekker kysten fra svenskegrensen i sør til den russiske grensen i nord.  Flere av de norske olje- og gassinstallasjonene har VHF basestasjoner for å kunne sende å motta nødmeldinger fra skip som seiler i området. Nødprosedyrer og kanalplaner samt kart over basestasjonene finnes på Telenor Kystradio sin hjemmeside /59/.

NORSOK standard S-001, «Technical Safety», stiller krav til funksjonalitet og tilgjengelighet for telekommunikasjonssystemer i en beredskapssituasjon /27/.

Aktivitetsforskriften §80 sier at det skal sikres at nødvendig intern og ekstern varsling og kommunikasjon er ivaretatt til enhver tid under installering og drift, og i fare- og ulykkessituasjoner. Det skal pekes ut en kommunikasjonsansvarlig ombord på bemannede innretninger /25/.

I rapporten «Ett hav – SAR ressursene i oljenæringen og fiskerinæringen», utarbeidet av SAFETEC for Norges Fiskarlag /24/, beskrives hvordan petroleumssektorens tilstedeværelse bidrar til økt sikkerhet og tilstedeværelse av SAR- og telekommunikasjonsressurser til havs. I en større søk- eller redningsaksjon vil informasjonsutveksling mellom mange aktører være nødvendig for å koordinere aktiviteter. Her vil kommunikasjonssystemer på installasjonene kunne spille en viktig rolle. Eksempelvis kan mobildekning som er tilgjengelig rundt installasjonene brukes av redningspersonell i området. Fremtidig 5G-nett vil kunne gjøre det mulig å isolere og prioritere nødkommunikasjon på reserverte frekvenser for bruk av nødetatene.

Spesielt i havområder med lange avstander og mindre utbygd SAR-beredskap, slik som i de nordlige havområdene på norsk sokkel, vil petroleumsnæringen kunne bidra vesentlig til beredskapen i området. Både faste og midlertidige installasjoner vil bidra med flere lytte- og kommunikasjonskanaler /56/.

HOPPET I HAVET OMRINGET AV MONSTERBØLGER:

**– Den mest ekstreme situasjonen vi har opplevd**

Sent onsdag kveld sendte en seilbåt i Nordsjøen ut et mayday-signal. Båten hadde to personer om bord, og var fanget i en storm.
Situasjonen var kritisk. Seilbåten lå ca. 60 nautiske mil vest for Fedje i Hordaland. Det var orkan i kastene og opp mot tolv meter høye bølger.
Redningsskøyten Stril Merkur var allerede på vei mot båten. I tillegg ble det tilkalt hjelp fra redningshelikopter, et såkalt SAR-team, på oljeplattformen Statfjord B.

Faktaboks 7-1: Olje- og gassinstallasjonene har en viktig funksjon som lytte- og meldingssentral for skipsfarten og småbåtbrukerne /35/.

Mulige basestasjoner for maritim VHF og for mobiltelefoni plassert på installasjonene i nordlige havområder vil også kunne komme fiskeri- og skipstrafikk i områdene til nytte.

# 8 PRINSIPPER FOR GOD SIKKERHET I TELEKOMMUNIKASJON

Siden telekommunikasjon er blitt digitalisert, vil de sikkerhetsstandarder og praksiser som gjelder for sikkerhet i digitale nettverk, også være de samme når det gjelder sikkerhet i telekommunikasjons-systemer. DNV-GL-RP-G108, «Cyber security in the oil and gas industry based on IEC 62443» /17/ beskriver en anbefalt felles praksis for sektoren for OT systemer. Det innebærer at når et telekom system blir definert som et OT system så gjelder denne standarden for dette systemet.

Norsk olje- og gass retningslinje 104 gir krav til informasjonssikkerhetsnivå i IKT-baserte prosesskontroll-, sikkerhets- og støttesystemer. Den inneholder også en sjekkliste for selvsjekk av eget sikkerhetsnivå.

NIST (National Institute of Standards and Technology) sitt «Cyber Security Framework» refereres ofte til internasjonalt når det gjelder retningslinjer for hvordan organisasjoner skal forbedre sine rutiner i forhold til å beskytte, oppdage og respondere på IKT-angrep. Fokus er beskyttelse av kritisk

infrastruktur hos en bedrift. NIST rammeverket inneholder også en sjekkliste for selvsjekk av bedrifters beredskapsnivå.

Standardene beskrevet over er relevante for bedriftskritiske telekommunikasjonssystemer som defineres som OT-systemer. Krav til en bedrifts styringssystem for IKT-sikkerhet og beredskap er gitt i ISO/IEC 27000-serien. Et ledelsessystem for IKT-sikkerhet skal være integrert med en organisasjons overordnede styringssystem og prosesser. Krav i ISO/IEC 27000-serien er også aktuelle for telekommunikasjonssystemer på alle sikkerhetsnivå. Kravene relaterer seg både til OT- og IT-system.

En forutsetning for en god sikkerhetskultur er et synlig engasjement fra lederne. Uttrykte sikkerhetskrav og «policy statements» bør forankres i en organisasjons toppledelse. Et sikkerhetssystem som også innbefatter telekommunikasjonssystemene bør bli regelmessig gjennomgått, testet og forbedret.

T-101 krever at sårbarhetsanalyser skal gjennomføres for hvert enkelt telekomsystem. I T-101 skiller en ikke mellom beskyttelse for IT- og OT-systemer, men foreslår beskyttelse tilsvarende OT-nivåer på alle telekomsystemer /11/. Telekommunikasjonssystemer transporterer data på tvers av IT- og OT-systemer, og det må bedømmes hvilke sikkerhetstiltak som skal iverksettes i hvert enkelt tilfelle (ref. tabell 4-2).

Virksomheter som tilbyr elektroniske kommunikasjonsnett eller tjenester i det norske markedet, er pålagt å utarbeide beredskapsplaner og tiltak for å opprettholde forsvarlig sikkerhet i sine nett og tjenester. Som bakgrunn for slike tiltak skal det gjøres risiko- og sårbarhetsanalyser (ROS-analyser) /2/.

## 8.1 Sikkerhet lokalt på en installasjon

Grenselinjer mellom sikkerhet i OT-, IT-, og telekomsystemene er ikke alltid godt definert. Noen telekomsystemer er kritiske for transport av teknisk styringsinformasjon, nært knyttet til driften av en installasjon og bør karakteriseres som et OT-system. Andre telekomsystemer dekker behov som ikke krever et tilsvarende sikkerhetsnivå.

Siden felles infrastruktur brukes som bærere for de forskjellige systemene, er det påkrevd med fysisk og logisk adskillelse som illustrert i faktaboks 4-3.

Fjernstyring av installasjoner kan utføres fra land. Leverandørene tilbyr å ta mer ansvar dersom de får direkte tilganger. Krav stilles til petroleumssektoren om økt lønnsomhet, effektivisering og besparelser ved å etablere nye samarbeidsmodeller. Dette gir utfordringer for fremtidens telekommunikasjons-løsninger. Samtidig utfordres sikkerheten om bord, samt stiller krav til etableringen og drifting av sikre telekommunikasjonsløsninger.

Sikkerhetsprosesser, håndbøker og prosedyrer skal være kjent av alle. Sikkerhetsanalyser, bedømmelser, revisjon og kontroll bør gjennomføres jevnlig. Tilsynsmyndighetene må påse at dette praktiseres.

## 8.2 Sikkerhet i telekommunikasjon på internasjonale, «åpne» media

Myndighetene stoler på at produsenter og leverandører av standard internettilkoblet utstyr som datamaskiner, mobiltelefoner og nettbrett forstår viktigheten av og ivaretar god sikkerhet. Det forventes gode prosesser og rutiner for å videreutvikle programvare, og for å sørge for at brukerne har tilgang til siste programvareversjon og nødvendig funksjonalitet for å beskytte seg mot angrep (f.eks. brannmur og virusprogrammer). Det forventes sikkerhet satt i system i hele verdikjeder, fra utvikling til industrialisering /19/.

Utviklingen av telekomutstyr og -systemer er markedsstyrt, og leverandørene opplever en knallhard konkurranse. Sikkerhetsløsninger i systemene er ofte usynlige, og prioriteres ned på bekostning av

funksjonalitet. Vi opplever gjennom oppslag i media at leverandører pålegges å bygge inn mulighet til overvåkning og sensur av informasjon, som kommuniseres både nasjonalt og internasjonalt.

Telekommunikasjonssystemene er blitt så komplekse at det er en umulig oppgave å sikre fullstendig integritet. Olav Lysne diskuterer dette i sin bok «The Huawei and Snowden Question» /43/. Det er ikke mulig å bevise at et element eller en funksjon i nettet, av en viss kompleksitet, ikke gjør noe i tillegg til det den skal gjøre. Som eksempler nevnes å avlytte en samtale, ødelegge seg selv på et tidspunkt, eller ha en bakdør for tilgang til systemfunksjoner. Det vil ifølge Lysne være mulig for en produsent å legge inn slike uønskede egenskaper uten at vi i praksis kan oppdage det. Det vil også være umulig å oppdage om bakdører plantes inn som en del av oppgraderinger i systemet.

## 8.3 Overholde GDPR-regelverket

Telekom i sektoren dreier seg også om transport og oppbevaring av informasjon om privatpersoner. GDPR-regelverket har derfor relevans også for sektorens telekommunikasjonsløsninger og systemer.

GDPR-regelverket skal bidra til opprettholdelse av våre grunnleggende samfunnsverdier, som kommer til uttrykk i både nasjonal og internasjonal rett. Regelverket regulerer statens og bedriftenes rett til å gripe inn i enkeltpersoners liv og rettigheter. Digitalisering og telekommunikasjonsløsninger gjør at samspillet mellom enkeltpersoner, bedrifter og myndigheter i dag er enklere enn noen gang tidligere. Offentlige og private tjenester har blitt lettere tilgjengelige etter at de er blitt digitalisert. Dette gjelder også for personell som har sin arbeidsplass på en flytende eller fast olje- og gassinstallasjon. Tilgang til nyheter via digitale medier er i stor grad mulig.  Internettilgang og nettpublisering har gjort det mulig for enkeltpersoner å ytre seg på et utall av media. IKT-plattformer brukes som forsamlingsarenaer i ulike sammenhenger /20/.

For at ansatte på olje- og gassinstallasjonene skal kunne delta på samme måte som andre i samfunnet, må bedriftenes telekommunikasjonsløsninger tilrettelegges også for privat bruk. Regelverkene skal sikre at slik kommunikasjon kan foregå uten innsyn fra bedrifter eller offentlighet. Bedriftene skal legge til rette for nødvendige telekommunikasjonsløsninger som sikrer dette. Bedriftene har ansvar for at enkeltpersoners bruk av telekommunikasjonssystemer ikke overvåkes og kontrolleres.

Innsamling av informasjon om bruk og oppførsel på teknisk utstyr kan, dersom en er i stand til å assosiere denne informasjonen til brukerne av utstyret, føre til at brukerens oppførsel er det som blir overvåket (som vist i eksemplet i faktaboks 4-1).

Bruk av private medier som smarttelefoner og nettbrett som kommuniserer via bedriftenes nettverk, er også en sikkerhetsutfordring. Behovet for å overvåke nett-trafikk kan fort komme i konflikt med å ikke overvåke personlig kommunikasjon. Sikkerhetstiltak kan lett bli sett på som et overvåkningstiltak.

T-101 gir også krav til prosessering og lagring av persondata. Slike data skal begrenses til å tilfredsstille et systems formål, og ikke tjene andre formål enn det som er spesifisert. Funksjonalitet for å sikre korrekte data, integritet og konfidensialitet skal være en integrert del av systemet.

## 8.4 Kryptering

Kryptering av meldinger og sterke krypteringsmetoder er noe vi stoler blindt på, og som vi bør bruke og kreve brukt i ekstern kommunikasjon. Kryptering blir utført av systemer eller elektroniske enheter som også kan ha innebygde svakheter. Dersom en ikke har absolutt tillit til de som bygger krypteringsutstyret eller systemet som en benytter, kan en heller ikke stole på krypteringen. Kryptering er et hjelpemiddel for å hindre tyvlytting og «man-in-the-middle»-angrep. Der er ingen garanti for at meldingene som overføres ikke har innhold som har skadelig formål /43/.

## 8.5 Årvåkenhet

«Du snakker – hvem lytter?» var en melding mange hadde klistret på telefonene i gamle «analoge» dager. Dette spørsmålet er like relevant i dag. Selv om mesteparten av vår kommunikasjon er digital, er det viktig å være klar over hvem som kan ha tilgang til den informasjonen vi kommuniserer. Vi stoler på at våre digitale kommunikasjonsmedier er sikre. Erfaringer og ny kunnskap viser at det ikke nødvendigvis er tilfelle. Mulighetene til å kommunisere er blitt flere og lettere tilgjengelige. Men det har også ført til at mulighetene for å stjele, overvåke, tyvlytte, kontrollere og manipulere informasjon har blitt flere.

Trusselbildet for bruk av teletjenester i petroleumssektoren er dynamisk og vil endre seg over tid. Det er viktig at enkeltpersoner er bevisste og opplært i å håndtere og rapportere det de mener er unormal oppførsel i systemer og tjenester. Bedriftene må ha tilstrekkelig beredskap og kunnskap til å håndtere slike meldinger.

Ledelsens engasjement er viktigst for å oppnå en god sikkerhetskultur. Leverandører og telekomoperatører vil tilby kostnadsbesparende løsninger hvis de får tilgang til og kan styre egne systemer fra distanse. Ofte mangler de det store bildet og forståelsen for de sammenhenger som eksisterer på en kompleks installasjon. Dette kan bare ivaretas av de som har totaloversikt og er tilstede. Metodikk som sikker jobbanalyse, koordinerte og styrte arbeidsordrer samt løpende risikovurderinger må ikke bli skadelidende ved at økte besparelser hentes ut ved å tillate ukoordinerte systemoperasjoner. Erfaring med fjernoperering av systemer er at dette skaper utrygghet på installasjonene for de ansatte som har sin arbeidsplass der.

## 8.6 Beredskapsplanlegging

Vi har i vår undersøkelse spurt bedriftene om hvor lenge en installasjon kan fortsette å operere dersom telekommunikasjonsløsningene blir satt ut av drift. For noen installasjoner betyr et slikt utfall at produksjonen må stenges ned, andre har alternative løsninger og vil kunne fortsette driften en stund.

Utfall av slike telekommunikasjonsløsninger blir ikke testet og øvd på, da man er bekymret for de konsekvensene en total nedstengning av installasjonen vil kunne få.

Standarden ISO/IEC 22301 «Security and resilience- Business continuity management systems-requirements», spesifiserer generelle krav for å planlegge og vedlikeholde et styringssystem for å håndtere, redusere sannsynligheten for samt respondere på driftsavbrudd /30/. Denne standarden kan være et godt utgangspunkt for å lage en beredskapsplan for en installasjon. Det henvises også til vår delrapport om «Resiliens mot cyberhendelser og kan blokkjeder bidra?».

## 8.7 Risikovurdering av kommunikasjonssystemer

Næringslivets Sikkerhetsråd (NSR) gjennomfører hvert annet år undersøkelsen KRISINO (Kriminalitets- og sikkerhetsundersøkelsen i Norge). I 2017 rapporterte kun 17 % av private virksomheter at de hadde gjennomført en risikoanalyse av IKT systemene. Tallet for offentlige virksomheter var 46 %. Dette viser at det er et betydelig underskudd på risikoforståelse i norsk næringsliv, og at mange virksomheters leveranser vil være i fare dersom de ikke hever sin kompetanse og tilfredsstiller lovens krav i de delene av organisasjonen som eksponeres /44/.

Beredskapsplaner bør utvikles for å håndtere utfall av telenettet.

Vi har gjennom våre intervju spurt bedriftene om det gjennomføres risikovurderinger som omfatter telekommunikasjonssystemer. Samtlige vi har intervjuet svarer bekreftende på at dette gjøres i henhold

til bedrifts interne prosedyrer. Det virker ikke som om sektoren er samordnet i rapportering og håndtering av IKT-trusler. Det er heller ikke etablert et felles responssenter for bransjen.

Det er ikke etablert rutiner eller praksis for rapportering av telekomhendelser til Nkom. Dette er krav i Ekomforskriften for teleoperatører /33/. I forhold til definisjonen av en teleoperatør i Ekomloven, vil flere bedrifter i petroleumssektoren defineres som teleoperatører /32/. Tampnet er et slikt selskap, men flere operatørselskaper er også transportører av data for andre gjennom sine nett.

Tabell 8-1: Topp 10 IKT-sårbarheter for petroleumsvirksomheten. Kilde: DNV GL rapport til Lysneutvalget /42/.

| Scenario # | Topp 10 digitale sårbarheter i petroleumssektoren |
|---|---|
| 1 | Manglende oppmerksomhet og opplæring hos de ansatte |
| 2 | Fjernarbeid |
| 3 | Bruk av standardprodukter med kjente sårbarheter i produksjonsmiljø |
| 4 | Mangelfull sikkerhetskultur hos underleverandører |
| 5 | Mangel på separasjon av datanett |
| 6 | Mobile lagringsenheter (inklusive smarttelefoner) |
| 7 | Datanett mellom landinstallasjoner og oljefelt |
| 8 | Manglende fysisk sikring av datarom, koblingsskap, m.m. |
| 9 | Sårbar programvare |
| 10 | Utdaterte styresystemer på installasjoner |

I tillegg bør følgende mulige uønskede hendelser som minimum vurderes når man utfører en risikoanalyse av kommunikasjonssystemer[2] /21/:

- Uautoriserte personer som får tilgang til kommunikasjonslenken
- Jamming av trådløse kommunikasjonslenker
- Avskjæring av datatrafikk av tredjepart
- Forfalskning av data fra tredjepart
- Skadevare inn i systemene
- Svikt i elektroniske komponenter i kommunikasjonslenkene
- Mindre enn ideell radiodekning for trådløse koblinger
- Feil i overføring av data (også kjent som bit-feil)
- Mangel på anerkjennelse av kommando(er)
- Feil konfigurasjon av kommunikasjonsfunksjoner
- Uventet reduksjon av tilgjengelig båndbredde under operasjoner
- Uventet økning av latenstid under operasjoner
- Ustabile datalinker over tid

[2] Teksten er basert på DNVGL-CG-0264 "Autonomous and remotely operated ships", Sec. 7 "Communication functions".

- Nettverksstormer
- Tap av strøm

### 8.7.1 Datakommunikasjon mellom installasjon og operasjonssenter på land

Kommunikasjonsforbindelsen mellom en installasjon til havs og et operasjonssenter på land skal være tilgjengelig, sikker og i stand til å støtte den tiltenkte bruken. Jo mer ansvar det landbaserte operasjonssenteret har for driften av enheten, jo mer tilgjengelig og robust må kommunikasjonsforbindelsen være.

Dekningsanalyse av de forskjellige kommunikasjonsløsningene må utføres for hvert konseptkvalifiseringsprosjekt for å bestemme egnetheten til en spesifikk løsning eller teknologi.

Aspektene nedenfor fungerer som grunnleggende veiledning for enhver kommunikasjonsforbindelse mellom installasjonen og det landbaserte kontrollsenter:

- Maksimal båndbredde som kreves, skal beregnes og dokumenteres. Beregningen skal ta i betraktning det verste tilfellet basert på den tiltenkte bruken, f.eks. overføring av sensordata fra flere sensorer som videokameraer, bilder og lyd overføres og mottas samtidig i sanntid
- De faktiske forsinkelseskrav (basert på den tiltenkte bruken) skal beregnes og spesifiseres
- Kommunikasjonen mellom installasjon og operasjonssenter bør overvåkes slik at ombordsystemet og operasjonssenteret uavhengig vil oppdage tap av kommunikasjon innen rimelig tid
- Alle grensesnitt og protokoller som brukes i kommunikasjonslenken skal spesifiseres og beskrives

### 8.7.2 Kommunikasjon for kontroll av enhetens nøkkelfunksjoner

Hvis det landbaserte operasjonssenteret er ansvarlig for kontrollen av noen av installasjonens kritiske OT-systemer, forventes tilgjengelighet, pålitelighet, fleksibilitet og robusthet å være høy; og overvåking av koblingen å være omfattende. Følgende aspekter må tas i betraktning:

- Den faktiske kommunikasjonsforsinkelse bør overvåkes slik at ombordsystemet og landbasert operasjonssenter uavhengig av hverandre vil oppdage om latenstiden overstiger det angitte maksimumet
- Kommunikasjonslenken skal være feiltolerant slik at den kan fungere med 100 % kapasitet selv med en enkelt komponentfeil
- Kommunikasjonslenken skal bestå av minst to uavhengige kommunikasjonskanaler, fortrinnsvis ved å bruke forskjellige underliggende teknologier og leverandører
- Hvis den faktiske båndbredde er mindre, eller forsinkelsen er høyere enn de nødvendige nivåene, bør det gis alarmer til operatøren
- Dersom båndbredde er en begrensning skal det være mulig å prioritere spesifikke kommunikasjonstyper for å sikre at de viktigste blir prioritert
- Operatøren skal være i stand til å teste og diagnostisere all funksjonalitet og egenskaper ved den ene kommunikasjonskanalen, mens de(n) andre er brukt til faktiske operasjoner
- Det er anbefalt at nettverkskomponentene på enheten og i den landbaserte operasjonssentralen skal være testet etter IEC 62443-4.2 SL 2 og 3
- Status og hendelser relatert til kommunikasjonslenken skal logges slik at de kan analyseres på et senere tidspunkt

### 8.7.3 Informasjonsprioritet

I tilfeller det er utilstrekkelig båndbredde mellom installasjonen og fjernkontrollsentralen, må det gjøres en prioritering for å sikre at kritisk informasjon blir overført og kritiske funksjoner blir opprettholdt. Prioriteringsrekefølge må dokumenters. Det må også gjennomføres en konsekvensanalyse med tiltak hvis utilstrekkelig båndbredde gjør at informasjonsoverføringen ikke er tilstrekkelig, og funksjoner ikke kan opprettholdes.

### 8.7.4 Ekstern kommunikasjon

Når kontrollfunksjoner er underlagt fjernstyring fra et landbasert operasjonssenter, skal dette kunne kommunisere med eksterne interessenter til installasjonen.

Følgende funksjoner må tas vare på:

- kommunikasjon med fartøyer med VHF-sender om bord på enheten
- overføring av nødmeldinger fra enheten
- videresending av nødmeldinger mottatt av enheten
- svar på meldinger fra andre fartøyer
- stemmekommunikasjon med mannskap om bord på enheten
- stemmekommunikasjon med mennesker i nærheten av enheten

Personellet om bord skal kunne kommunisere pålitelig og sikkert med eksterne interessenter som nødetatene, forsyningsskip, etc. ved å bruke kommunikasjonsmidler som ikke er avhengig av kommunikasjonsforbindelsen mellom land og installasjonen.

## 8.8 Myndighetenes tilsyn

LOV 2003-07-04 nr. 83 (ekomloven) /32/ gjelder også for norske skip og luftfartøy, samt for anlegg og innretninger av enhver art med tilknytning til petroleumsvirksomhet på kontinentalsokkelen (§1-3). I loven defineres en «tilbyder» som enhver fysisk eller juridisk person som tilbyr andre tilgang til elektronisk kommunikasjonsnett eller -tjeneste. (§1-5) Tilbydere har krav til å måle kvaliteten på tjenester og informere om de tjenester som leveres til sluttbruker. §2-10 omhandler en rekke krav til sikkerhet og beredskap. Vårt inntrykk er at i tillegg til de rene telekommunikasjonsleverandørene, er også operatørselskapene i henhold til bestemmelsene over, og bør også være underlagt de gitte bestemmelsene. Loven pålegger myndighetene å ha tilsyn med leverandører av teletjenester.

FOR-2004-02-16-401 (ekomforskriften) /33/, kapittel 8 handler om sikkerhet og beredskap. Her kreves det at tilbyder skal utarbeide og vedlikeholde planer, og gjennomføre tiltak for å opprettholde forsvarlig sikkerhet i elektroniske kommunikasjonsnett. Tilbyder skal også på forespørsel fra Nkom utlevere planer, samt risiko- og sårbarhetsvurderinger. Nkom fører tilsyn med planene og kan sette krav til form og innhold. Tilbyder skal også på forespørsel delta i beredskapsøvelser arrangert av myndighetene.

Vår gjennomgang har vist at det er manglende oppfølging av planer og risikoarbeidet relatert til telekommunikasjon i petroleumssektoren fra myndighetenes side. Det er behov for styrking av myndighetenes oppfølging av den kritiske infrastrukturen for telekommunikasjon i petroleumssektoren.

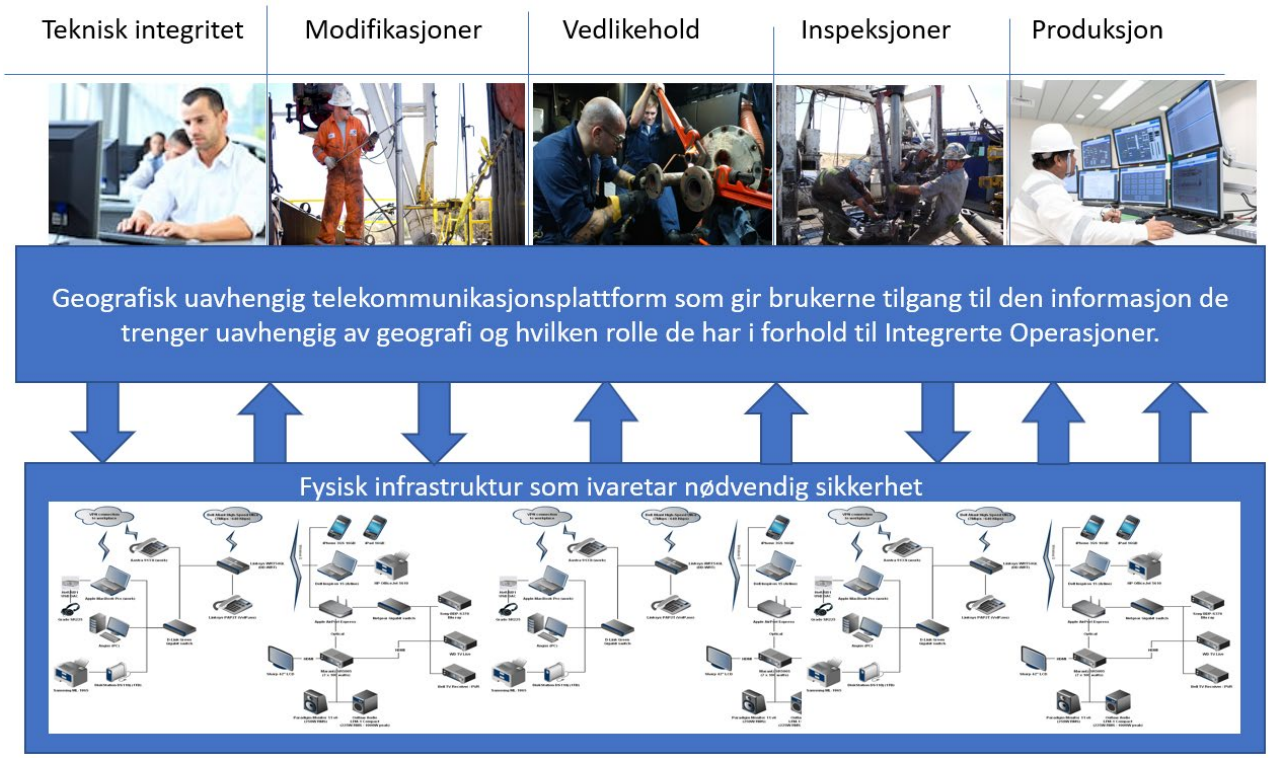
Vår observasjon er at det mangler en klar forståelse i sektoren for hvor, hvordan og når hendelser skal rapporteres til myndighetene. Dette bør klargjøres av myndighetene.

Et regime for rapportering av hendelser og statusrapportering av sikkerhetshendelser som inkluderer telekommunikasjonssystemene, bør etableres. Her bør det også komme klart frem hvilke hendelser som skal rapporteres til myndighetene, og til hvilken myndighetsinstans.

# 9 TEKNOLOGIUTVIKLING OG FREMTIDIGE TRENDER SOM KAN UTFORDRE SIKKERHETEN

Den teknologiutviklingen som nå skjer innen digitalisering og telekommunikasjon vil gi grunnlag for en eksplosiv vekst i nye tilbud for drift av utstyr på en olje- og gassinstallasjon. Konkraft er et samarbeidsforum for aktører involvert i norsk olje- og gassproduksjon som setter opp agenda for den nasjonale strategien for petroleumssektoren. I Konkraft sin rapport fra 2018 oppfordres det til økt bruk av digitale løsninger, automatisering og robotisering. Samtidig oppfordres sektoren å styrke samarbeidet mellom leverandører og operatører gjennom utvidet interaksjon /26/.

I faktaboks 9-1 er en mulig fremtidig organisering av integrerte operasjoner for en olje- og gassinstallasjon skissert. Nye samarbeids- og organisasjonsmodeller vil kreve tilgang til sanntidsdata og mulighet for operering uavhengig av geografisk lokalisering.




Faktaboks 9-1: Telekommunikasjon er en forutsetning for integrerte operasjoner på en produksjonsinstallasjon.

Den norske olje- og gassnæringen er ikke lenger en ung næring. Ikke minst hvis en ser den i lys av hastigheten på utviklingen av telekommunikasjon og digitale løsninger. For mange installasjoner vil det være sårbarheter ved at eldre løsninger vil måtte sameksistere med nye løsninger i overgangsperioder. Muligens vil det for de eldste installasjonene ikke være grunnlag for å innføre nye løsninger i det hele tatt. Dette vil kreve at nye effektive telekommunikasjonsløsninger integreres med de gamle, samtidig som disse opereres på en sikker måte.

Som vist i faktaboks 9-1 kan integrerte operasjoner organiseres uten at geografisk tilstedeværelse er en avgjørende faktor. Telekommunikasjonsløsninger gjør det mulig å dele og kommunisere informasjon uavhengig av om en befinner seg på land eller offshore, hos operatørselskapet eller hos

servicekontraktører. Begrensningene ligger i de sikkerhetsløsningene en må etablere for å beskytte og begrense tilgang.

Trivsel for de ansatte på installasjonene er også en viktig faktor. I dag er bruk av smarttelefoner, nettbrett og bærbare PCer blitt en naturlig del av hverdagen for å holde kontakt med familie, venner og også for personlige og jobbmessige tjenester. Tilgang til mobilnett eksisterer i dag, men fungerer ofte ikke slik en er vant med fra land. Sømløs overgang fra land til offshore er for mange installasjoner ikke på plass. Nettmøter og konferanser vil kunne gjøre at en kan delta på aktiviteter selv om man geografisk ikke er tilstede. Dette er tjenester hvor det vil skje teknologiske nyvinninger som vil bli mer tilgjengelige fremover.

## 9.1 5G

5G-nettet er en videreføring av 4G-nettet. 5G-nettet gjør det først og fremst mulig å sende mer data over telenettet med større hastighet. Dette gjøres ved å benytte et større frekvensbånd enn 4G (700 – 3800 MHz utvidet fra dagens 800 – 3600 MHz). 5G vil gradvis overta flere av de frekvensområdene som 4G bruker i dag.

5G vil i industrien gi mulighet til å montere sensorer på komponenter og systemer som ikke lett lar seg kable opp for transport av tilstandsinformasjon, for å tidlig oppdage feil som er under utvikling. En kan også se for seg bruk av sensorer som sender posisjon og identifikasjon slik at en kan spore utstyr, komponenter eller personer som er om bord i en installasjon.

Forventningene til nye tjenester og produkter som vil bli tilgjengelige med 5G-nettet er store. Enkle og lavterskel-grensesnitt for utvikling og tilgjengeliggjøring av tjenester vil gjøre at de utvikles raskt. Korte responstider vil gjøre at sanntidsoperasjoner kan foregå over 5G. Bedrifter, offentlige etater og husholdninger vil kunne lage sine egne «private» nett av sensorer og maskiner som kan styres via nettet.

5G-nettet vil bære flere og større samfunnsverdier. Nød- og beredskapsbrukere vil etter all sannsynlighet realisere sine behov for telekommunikasjon gjennom kommersielle mobilnett /1/.

Under et uformelt nordisk statsministermøte i mai 2018 ble en intensjonserklæring om utviklingen av 5G i Norden signert. Erklæringen uttrykker felles mål om å bli den første og mest integrerte 5G-regionen i verden:

"As the development of fifth generation wireless systems (5G) breaks through, the Nordic countries will be at the forefront of that development to become world leaders in using 5G technology for the development and digitalisation of all sectors of society."

Faktaboks 9-2: En felles nordisk politisk ambisjon om å være verdensledende på utvikling av 5G /2/.

Skivedeling av nett er å opprette flere logiske nett av samme underliggende fysiske nett, ved å bruke virtualiserte nettfunksjoner. Hver skive av nettet kan settes sammen slik at den har egenskaper som er optimalisert for en spesiell anvendelse, for eksempel lav forsinkelse. En annen grunn til å ha en egen skive av nettet, kan være krav til sikkerhet og uavhengighet fra andres belastninger på nettet. Oppdragskritisk kommunikasjon, som i dagens Nødnett, er en anvendelse der det er naturlig å tildele en egen skive.

### 9.1.1 Sikkerhet i 5G-nettet

Sikkerhet i signalprotokollene som skal gjøre at flere teleoperatører skal kunne utveksle data, er en utfordring. Alle mobile nettverk har sin egenart, men alle offentlige nett er sammenkoplet i et felles globalt nett hvor abonnenter i de forskjellige nettverk kan kommunisere med hverandre. For at dette skal virke, må de forskjellige operatørene implementere de samme signaleringsprotokollene for datautveksling. ENISA, som er EUs kompetansesenter for nettverks- og informasjonssikkerhet vurderer i sin rapport «Signalling Security in Telecom SS7/Diameter/5G – EU level assessment of the current situation» kvaliteten på de signalprotokollene som benyttes i dagens mobile nettverk. De beskriver en rekke sårbarheter som må løses for at 5G skal kunne bli det sikre nettet som ambisjonen er. I dagens mobilnettverk benyttes fortsatt sikkerhetsprotokoller utviklet for 2G og 3G. Signalprotokoller som SS7, SIGTRAN, GTP og Diameter er vanlige i dagens 4G-nett, og er kjent for å ha flere alvorlige og kjente svakheter som kan bli utnyttet av IKT-angripere. Selv om det er registrert få hendelser, så kan konsekvensene bli alvorlige. På samme tid er det vanskelig å løse svakhetene i signaleringsprotokollene /22/.

**5G-nettet**

Målet med 5G-nettet er å gi brukerne mye raskere, mer tilgjengelige og sikrere digitale tjenester. I 5G innføres det såkaltes "skivedelte" nett. Det betyr at det er mulig å tilby flere logiske nett tilpasset ulike brukergruppers behov for båndbredde, pålitelighet og systemforsinkelse over samme fysiske nett. 5G-teknologien vil gi stor fleksibilitet i tjenestetilbudet og kan tilrettelegges for svært ulike kundebehov over en felles infrastruktur.

Nettet vil tilby lett tilgjengelige programmerbare enheter til brukerne, noe som skaper mulighet for mange nye applikasjoner. Eksempler på nye mulige anvendelsesområder er

- droneteknologi
- autonome kjøretøy
- AR/VR
- nødkommunikasjon
- e-helse
- sensorer i omgivelsene
- bredbåndtjenester

5G kan være opptil 20 ganger raskere enn 4G. Det samme fysiske nettet vil være så dynamisk og fleksibelt at det effektivt kan knytte brukerenhetene sammen og levere alle slags tjenester til disse. Den vesentligste forskjellen fra 4G vil være i hvordan ulike brukergrupper kan få sine offentlige tjenestetilbud levert over nettverksløsninger som bruker ett og samme fysiske nett.
5G-nettet må standardiseres før det kan lanseres. Dette kan ta tid, men 2020 nevnes ofte som et realistisk årstall.

Faktaboks 9-3: 5G-nettet – nye muligheter /1/.

## 9.2 IoT (Internet of Things)

IoT, også kjent som tingenes internett, består av et nettverk med fysiske enheter som er forbundet via internett slik at data om enhetene kan samles inn, kommuniseres og analyseres. Slike enheter kan være komponenter som inngår i systemer på en olje- og gassinstallasjon med påkoplede sensorer som samler inn data om enhetens tilstand og bruk. Dataene kan så analyseres for å vurdere enhetens tilstand og ytelse. Slike analyser kan være vurderinger om det er behov for tilsyn, justeringer, reparasjoner eller utbytting. Ved å kontinuerlig ha tilgang til å overvåke enheten, kan en tidlig identifisere mulige defekter som er under utvikling, og dermed oppnå mer pålitelig drift. Fjernovervåkning og -styring av komponenter gjør at leverandørene kan tilby kostreduksjoner, samt bedre oppetids- og

tilgjengelighetsgarantier. Ytelsesbaserte avtaler gir tilsynelatende kostnadsbesparelser (se faktaboks 9-5).

Ønsket om kontinuerlig tilgang til data og muligheten for å endre konfigurasjoner av enheter utfordrer de eksisterende datasikringsregimer på installasjonene. Endringer på enkeltkomponenter uten at helhetsperspektivet er tilstrekkelig tatt i betraktning, er en trussel. Enheter som er koplet til internett er sårbare for inntrengning fra uvedkommende dersom de ikke er tilstrekkelig beskyttet. Med den store utbredelsen som en forventer for IoT, er det sannsynlig at ikke alle systemleverandører har den samme forståelsen for utvikling av sikker programvare. Muligheten til å kontrollere og overvåke alle enheter blir vanskelig, slik at dette vil bli en sikkerhetsutfordring fremover. Manipulering av enheter som er del i et kritisk system kan føre til skade på mennesker, utstyr og miljø.

Utstyrsleverandørene må utvikle seg til å bli dataleverandører med tilstrekkelig kunnskap om datasikkerhet og -forvaltning. Data blir tilgjengelig for flere, og angrepsflatene på prosesskritisk utstyr større. Behovet for tilsyn med kompetanse, forståelse og etterlevelse av datasikringskrav hos leverandørene vil øke. Med IoT vil det komme nye produsenter og leverandører, som i mange tilfeller har liten kunnskap og vilje til å etablere tilstrekkelige IKT-sikkerhetsmekanismer i produktene. Mange av produktene de leverer som tradisjonelt ikke har vært knyttet til internett, blir online og må beskyttes mot IKT-trusler.

Sårbarhetene vil forsterkes ytterligere med energieffektive løsninger som gjør det mulig for IoT-enheter å oppnå en forventet levetid på mange år. Forlenget levetid stiller strengere krav til at programvaren blir kontinuerlig oppdatert. Produsenter og leverandører av IoT-utstyr må sørge for at det er mulig å oppgradere og vedlikeholde programvare, og dermed ivareta sikkerheten gjennom hele levetiden til produktet /19/.

Den opplevde trygghet for personell som arbeider på installasjonene blir dårligere hvis en mangler oversikt over endringer som blir gjort, eller kan gjøres, utenfra på kritiske komponenter. Behovet for koordinering av arbeidsoperasjoner og forståelse av helhetsbildet vil øke hos operatørene. Kompetansebehovet innenfor IKT-sikkerhet hos operatørene vil øke siden overvåkning av datasikkerhet blir en integrert del i de fleste disipliners oppgaver.

Det blir viktig å ikke eksponere IoT-enheter på nett slik at de kan nås av uvedkommende. Dette betyr at strenge regimer som regulerer hvilke enheter som kan kommunisere med andre må administreres, kommuniseres og verifiseres. Dette betyr igjen merarbeid for sikkerhetsansvarlige i bedriftene som skal etablere, administrere og implementere sikkerhetsløsninger.

I Norge har Nasjonal kommunikasjonsmyndighet (Nkom) relativt nylig publisert sin rapport «På vei mot et IoT-samfunn». Der fremgår det blant annet at EU etter påtrykk fra medlemsstatene har satt i gang en reguleringsprosess for å sette krav til styrking av sikkerheten i utstyr som er koplet mot internett. I rapporten heter det: «Foreløpig utredes problemområdet og grunnlaget for regulering. En ferdig konsekvensanalyse er forventet å foreligge i tredje kvartal 2019» /19/.

## 9.3 Planer for videre utvikling av satellittkommunikasjon

Nkom sier i sin årsrapport for 2018 at de forventer en betydelig økning i antall satellitter i fremtiden, og at det vil bli mer tilsynsaktiviteter med satellittkommunikasjon /34/. Firmaet SpaceX ønsker å tilby internettilgang til alle steder på jorden gjennom nettjenester fra et nettverk av 12.000 LEO-satellitter[3] i

[3] LEO = Low Earth Orbit (Satellitter i typisk 500 – 1000 km høyde).

flere skall rundt jorden. De vurderer å senere utvide med ytterligere 30.000 satellitter /51/. Prosjektet har fått navnet Starlink og skal etter planen være operativt i midten av 2020.

> "As demand escalates for fast, reliable internet around the world, especially for those where connectivity is non-existent, too expensive or unreliable, SpaceX is taking steps to responsibly scale Starlink's total network capacity and data density to meet the growth in users' anticipated needs."

Faktaboks 9-4: SpaceX statement /51/.

Også andre har annonsert samme visjon som SpaceX: verdensomfattende internettdekning. OneWeb har annonsert en tilsvarende plan som SpaceX med mer enn 600 LEO-satellitter i bane 1200 km ut i rommet /50/. Andre planlagte LEO-systemer er blant annet LeoSat (108 LEO-satellitter) /52/. Flere av deres investorer holder nå tilbake investeringene, og fremtiden er nå litt uklar for LeoSat /54/, Samsung (4600 satellitter), Amazon (3236 LEO-satellitter) /53/, Telesat (Kanadisk selskap, 117 satellitter)/41/ og Honyan (Kina). I tillegg er det også pågående aktiviteter for å utvide MEO-satellittløsninger og investeringer i GEO-satellittsystemer.

Hvordan disse initiativene vil påvirke fremtidens tilbud om globale teletjenester er vanskelig å forutse. Det er store investeringer som skal på plass for å få systemene operative, og det er ikke gitt at alle planlagte systemer vil bli ferdigstilt slik at de får betydning for petroleumssektoren.

## 9.4 Behov for kommunikasjonsløsninger for Barentshavet

Den nasjonale infrastrukturen i den digitale grunnmur er dårlig utbygd i Nord-Norge. De lange avstandene gjør at redundante linjetilbud er dyrt å få på plass og mangler i dag.

Feltutbyggingen i Barentshavet bringer installasjonene lengre nord, og etablering av fiberlinjer vil kreve betydelige investeringer. Selv om det er kostbart å etablere fiberforbindelser over lengre avstander til sjøs, er dette en kostnad operatørselskapene er villige til å ta, sett i forhold til nyttegevinsten.

Statsaksjeselskapet Space Norway, som forvaltes av Nærings- og fiskeridepartementet, har som formål å bidra til nærings- og infrastrukturutvikling relatert til norsk romvirksomhet. Space Norway har inngått avtaler med satellittoperatøren Inmarsat og med Forsvarsdepartementet for å tilby bredbånd for både sivile og militære brukere i Arktis. To satellitter vil bli skutt opp i 2022. Bakkestasjonen vil bli etablert i Nord-Norge sammen med Kongsberg Satellite Services og dermed sikre full nasjonal kontroll med denne kritisk viktige kapasiteten. Begge satellittene vil bli sent opp til en høyelliptisk bane som vil gi kontinuerlig dekning nord for 65 grader – som tilsvarer hele området nord for Polarsirkelen. Space Norway har også ansvaret for fiberforbindelsen fra fastlandet til Svalbard som ble lagt i 2004 /55/.

Det er lange avstander fra land til feltene i Barentshavet, slik at etablering og drift av fibernett vil bli dyrt. Avhengig av fremtidige funn og beslutninger om utbygginger, bør bedriftene gå sammen om fellesløsninger som sikrer redundans og deling av utgifter.

Økt redundans i fibernettet vil kreve flere linjer, men vil forbedre sikkerheten vesentlig.

## 9.5 Bruk av droner til overvåkning

Den sivile bruken av droner er i kraftig vekst. Droner gjør det mulig å sende kameraer og annet sensorutstyr i luften raskere, enklere og billigere enn med bemannende fly og helikoptre. Fordi de er ubemannet, kan de brukes i risikofylte operasjoner og miljøer. At droner kontrolleres via satellitt- og

datanettverk, åpner for nye muligheter innen fjernhandling. Selskaper som Statnett har store planer for fremtidig bruk av droner for kontroll av høyspentledninger /47/.

Bruk av droner vil kreve reguleringer og avklaringer i forhold til en organisasjons operasjonsprosedyrer. For å forhindre personskader må det sikres at droner ikke benyttes i områder hvor det pågår menneskelig aktivitet. Spesielt må avgangs- og landingsområder etableres. Styring av droner må ikke forstyrre telekommunikasjon. Aktiviteter utført med droner må tas hensyn til i sikker jobbanalyser og være styrt av arbeidsordre.

Det anbefales ved design av nye installasjoner å planlegge for fremtidig tilgang for droner, eksempelvis for landingsområder og operasjonsområde for dronene.

Droneteknologien er i rask utvikling, og fremtidige muligheter for bruk kan være mange i petroleumssektoren.

## 9.6 Virtualisering

Virtualisering er et konsept hvor en deler dataressurser på en slik måte at brukerne har en opplevelse av å ha sitt eget system, selv om dette er en integrert del av et totalsystem. Hensikten er å utnytte ressurser effektivt for å oppnå kostbesparelser, eller for å skape uavhengighet til fysiske system. Et virtuelt system kan enten være satt sammen av flere fysiske system, eller ett fysisk system som deles av flere virtuelle system. Virtualisering er en teknikk (funksjon) og ikke en standard.

5G-konseptet er et eksempel på et virtuelt system hvor flere «skiver» deler samme fysiske grunnstruktur. Virtualisering av infrastruktur er en overgang fra dedikerte fysiske til logiske nettverk. Tjenester som før ble levert på dedikerte linjer blir nå levert integrert med andre teleleveranser på felles infrastruktur. Brukerne kjøper tjenester uten å ha noe forhold til hvilke kommunikasjonsmedier som tjenesten blir utført på.

Funksjonaliteten i telekomnettene er i økende grad realisert gjennom konfigurerbar programvare som er «frikoblet» fra den fysiske infrastrukturen. På den ene siden skaper dette større effektivitet og fleksibilitet ved produksjon av teletjenester, og gir grunnlag for reduserte kostnader. På den andre siden medfører slike løsninger høy grad av kompleksitet i programvare, integrasjon og konfigurasjon samt avhengighet av underleverandører. I tillegg introduserer de nye sårbarheter knyttet til både utilsiktede hendelser som programvarefeil og konfigurasjonsfeil, samt tilsiktede hendelser som IKT-angrep /20/.

VPN (virtuelt privat nettverk) er en teknikk hvor en etablerer en punkt-til-punkt-forbindelse (tunneler) gjennom et nettverk. VPN gir sammen med kryptering en relativt sikker forbindelse (med de begrensninger som er spesifisert andre steder i dette dokument).

Virtualisering øker kompleksiteten og brukernes oversikt, siden funksjonaliteten må administreres.

På samme måte mener vi at Tampnet har en svært viktig rolle i forhold til å ivareta sikkerheten i den sentrale og felles infrastrukturen som forbinder nesten alle installasjonene i Nordsjøen. Et sentralt utfall av dette nettet vil føre til at mye av petroleumsvirksomheten i Nordsjøen stopper opp. Vi mener dette er en usikkerhet som sektoren i dag ikke er godt nok forberedt på å håndtere. Faren for hvilke konsekvenser et slikt utfall kan få, gjør at ingen tør å utføre øvelser for å teste reserveløsninger.

Utfall fra et virtuelt system kan få store konsekvenser. Ved å utnytte sårbarheter i styringssystemer kan mange systemer bli berørt. Systemadministratorer og brukere kan f.eks. få tilgang til andres data.

Oljeselskapene vil kunne spare enormt i kostnader sierAndreas Carlsson, sjef for innovasjonsavdelingen Telia Next.
Sensorene kan brukes på nesten alt mulig, som å måle trykket i et rør, måle vibrasjoner i konstruksjonen, gi beskjed når en maskin trenger vedlikehold, oppdage lekkasjer og registrere personell som befinner seg på området.
– Det automatiserer en rekke prosesser og systemer. Oljeselskapene vil kunne spare enormt i kostnader, gjøre arbeidsplassen tryggere for de ansatte og redusere miljøpåvirkning.
Potensialet med NB-IoT er ubegrenset, sier Carlsson i Telia.
Det er spesielt på de gamle plattformene i Nordsjøen, som er fra 70-, 80- og 90-tallet, at den nye teknologien vil ha størst effekt.
– På noen plattformer går man fremdeles rundt med blokk og noterer ned målerverdier og andre tall fra maskinene. Å få dette automatisk loggført og dokumentert er mye bedre bruk de ansattes tid, sier Carlsson.

Faktaboks 9-5: Samarbeid mellom Tampnet og Telia om utrulling av IoT /40/.

# 10 ANBEFALINGER

I tabell 10-1 har vi summert opp anbefalinger vi har gitt i dokumentet.

Tabell 10-1: Oppsummering av anbefalinger

| Nr | Anbefaling | Begrunnelse | Referanse |
|---|---|---|---|
| 1 | Petroleumssektoren bør spesifisere konkrete minimumskrav til sikkerhet for de forskjellige typer telekomsystemer. | T-101 inneholder ikke konkrete krav til IKT-sikkerhet.<br>Det burde etableres en NORSOK IKT-sikkerhetsstandard som også gjelder for telekom. | Kap. 4 |
| 2 | Krav i EUs NIS (Nettverk og Informasjons System) direktiv bør gjennomgås og implementering planlegges. | Direktivets betydning for krav til sikkerhet i telekom systemer bør avklares | Kap. 8.8 |
| 3 | Det bør klargjøres hvilke IKT-hendelser som skal rapporters til henholdsvis Nkom eller Ptil. | DNV GL avdekket gjennom intervjuer at det er uklart for bransjen hva som skal rapporteres til myndighetene. Praksis er at få hendelser rapporteres. | Kap. 1, 8.8 |
| 4 | Ptil bør ta initiativ til å få etablert en felles plattform for rapportering og erfaringsutveksling av IKT-hendelser. | Det finnes i dag ikke noe eget CERT for petroleumssektoren. Flere vurderer å gå inn i KraftCERT. Ptil bør ta initiativ til å etablere et samarbeidsforum for kunnskaps- og erfaringsutveksling om IKT-trusler. Det er viktig å forholde seg til de samarbeidsorganer som jobber for å redusere trusselnivået. Her kan ikke bedriftene klare seg alene. | Kap. 8.8 |
| 5 | Myndighetene må øke sin tilstedeværelse gjennom tilsyn av telekommunikasjons-systemer i sektoren. | Det er avdekket gjennom intervju at Ptil/Nkom er lite tilstede når det gjelder telekom i sektoren. | Kap. 8.8 |

| | | | |
|---|---|---|---|
| 6 | Myndighetene bør etterse at ROS (risiko- og sårbarhetsanalyser) analyser gjennomføres for telekomsystemer. | Det er avdekket gjennom intervju at de forskjellige aktørene i petroleumssektoren har valgt forskjellige IKT-løsninger i forbindelse med den operasjonelle driften på installasjonene. De har derfor forskjellig eksponeringsflate med tanke på IKT-sikkerhet, og konsekvensene ved en hendelse vil også være forskjellig. | Kap. 8 |
| 7 | Ptil bør spesifisere klare retningslinjer og regler for kommunikasjon mellom sikkerhetslag. | Forskriftene fra Ptil inneholder ikke klare retningslinjer. RP og NOG 104 gir guidelines, men spesifikke krav mangler kravdokumenter (f.eks. T101). Ptil bør ta initiativ til å få etablert en NORSOK IKT-sikkerhetsstandard. | Kap. 4, (4.1.4) |
| 8 | Det bør gjennomføres en sårbarhetsanalyse av nettverkstjenestene som også inkluderer fiber-infrastrukturen. | Nettverkstjenestene er i stor grad redundante, men ikke uavhengige.<br>Sikkerhet i forhold til monopolsituasjon bør avklares. | Kap. 8.2 |
| 9 | Dawinci- sårbarhetsanalyse. | Konsekvensen av å implementere en løsning basert på internett med grensesnitt til interne PRS systemer bør avklares. Forhold til GDPR direktivet bør verifiseres. | Kap. 5.3<br>Kap. 8.3 |
| 10 | Grundigere gjennomgang av sikkerheten i de protokoller som anvendes for kommunikasjon mellom sikkerhetslag. | NORSOK IKT-sikkerhetsstandard bør inneholde spesifikasjon av hvilke protokoller som kan anvendes for sikker kommunikasjon i de forskjellige sikkerhetssoner. | Kap. 6 |
| 11 | Rekruttering og ivaretagelse av telekomkompetansen i sektoren | Rekrutteringen gjelder for både nye og gamle anlegg. Kompetansen om systemer på de gamle anleggene må ivaretas. Spesielt viktig er det at kunnskap om de eldre og dårlig sikrede systemene opprettholdes når anleggene nærmer seg produksjonsslutt. | Kap. 9 |
| 12 | Hyppige oppdatering av NORSOK-standardene. | Datakommunikasjon handler om samhandling og systemer som kan utveksle informasjon. Skal dette fungere optimalt må samme standarder og metodikk anvendes. NORSOK-standardene bidrar til at behovet for selskapsspesifikke krav blir mindre | Kap. 4 |
| 13 | Beredskapsplaner bør etableres og øves på. | Det anses for utrygt og risikabelt å øve på tiltak ved utfall av sentrale telekommunikasjonsløsninger. Beredskapsplaner bør etableres i fellesskap i sektoren og øvelser gjennomføres. | Kap. 8.6 |

# REFERANSER


/1/ Telenor: Hva vet vi om 5G: https://www.telenor.no/om/teknologi-norge/femg.jsp (nedlastet 7-nov-2019)

/2/ Nkom: EkomROS 2019: Den digitale grunnmuren. Risikovurdering av ekomsektoren - Juni 2019, https://www.nkom.no/aktuelt/nyheter/_attachment/42430?_ts=16b4a976ad8 (nedlastet 7-nov-2019)

/3/ Paulsen, Gard: Handelshøyskolen BI: Informasjon over Nordsjøen Telekommunikasjoner på norsk sokkel, Forskningsrapport 3/2015, https://core.ac.uk/download/pdf/52040504.pdf (nedlastet 7-nov-2019)

/4/ Ptil: Kunnskap IKT-sikkerhet og CERT, https://www.ptil.no/contentassets/d67ffa5187c846fe9a074d1e68f2ce1c/kunnskapsprosjekt-ikt-sikkerhet-sluttrapport-med-underskrift.pdf (nedlastet 28-nov-2019)

/5/ Datatilsynets oversikt over hva som er lov med kameraovervåkning, https://www.datatilsynet.no/personvern-pa-ulike-omrader/overvaking-og-sporing/kameraovervaking/ (nedlastet 19-nov-2019)

/6/ Nkom: EkomROS 2017: Risikovurdering av ekomsektoren, 2017, https://www.nkom.no/aktuelt/rapporter/_attachment/29084?_ts=15c9b3cff27 (nedlastet 19-nov-2019)

/7/ Telenor Maritime, https://telenormaritime.com/business/offshore/ (nedlastet 7-nov-2019)

/8/ NKOMs hjemmeside, https://www.nkom.no/ (nedlastet 7-nov-2019)

/9/ Telia sin hjemmeside, https://www.telia.no/magasinet/smartere-oljeplattformer-med-ny-teknologi/ (nedlastet 7-nov-2019)

/10/ Tampnet sin hjemmeside, https://www.tampnet.com/north-sea/(nedlastet 7-nov-2019)

/11/ NORSOK-standard T-101:2019 – Telecom systems

/12/ Ptil: Fjernarbeid og HMS, https://www.ptil.no/contentassets/92b2f32146e346acac52546c53b72a46/sluttrapport-ptil-ikt-sikkerhet---fjernarbeid-og-hms-med-underskrift-og-vedlegg.pdf (nedlastet 28-nov-2019)

/13/ Mørketallsundersøkelsen 2018 – NSR, https://www.nsr-org.no/getfile.php/1311411-1539949973/Dokumenter/NSR%20publikasjoner/M%C3%B8rketallsunders%C3%B8kelsen/M%C3%B8rketallsunders%C3%B8kelsen%202018_ENG.pdf (nedlastet 7-nov-2019)

/14/ Presentasjon av NORSOK T-101/T-003 på Teknas seminar «Telekommunikasjon offshore 2019», av Alf Frimandslund, Equinor og Lars Bahr, Conocophillips, 22-okt-2019

/15/ Wikipedia mikrobølge-transmisjon, https://en.wikipedia.org/wiki/Microwave_transmission (nedlastet 28-nov-2019)

/16/ Ceragon PointLink System, Off-Shore_Operations_Made_Simple - PointLink Platform - Oil and Gas brochure 2016 Online (nedlastet 28-nov-2019)

/17/ DNVGL-RP-G108 Cyber security in the oil and gas industry, 2017, http://rules.dnvgl.com/docs/pdf/DNVGL/RP/2017-09/DNVGL-RP-G108.pdf (nedlastet 6-nov-2019)

/18/ Finansavisen: https://finansavisen.no/nyheter/politikk/2018/01/spioner-stod-bak-cyberangrepet-mot-helse-soer-oest (nedlastet 29-nov-2019)

/19/ NKOM: På vei mot et IoT-samfunn. Utvikling og betydning for Nkom, mars 2019, https://www.nkom.no/aktuelt/nyheter/_attachment/41264?_ts=1694d36843f (nedlastet 7-nov-2019)

/20/ NOU 2015:13 Digital sårbarhet – sikkert samfunn, https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000ddpdfs.pdf (nedlastet 20-sep-2019)

/21/ DNVGL-CG-0264 Autonomous and remotely operated ships, section 7 Communication functions

/22/ ENISA. Signalling Security in Telecom SS7/Diameter/5G – EU level assessment of the current situation: March 2018, https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g (nedlastet 7-nov-2019)

/23/ AEP (Public-Private Analytic Exchange Program (AEP): Threats to undersea cable communication: 28-sep-2017, https://www.dni.gov/files/PE/Documents/1---2017-AEP-Threats-to-Undersea-Cable-Communications.pdf (nedlastet 7-nov-2019)

/24/ SAFETEC: Ett hav. SAR-ressursene i oljenæringen og fiskerinæringen- rapport til Norsk Fiskarlag, https://docplayer.me/2991141-Ett-hav-sar-ressursene-i-oljenaeringen-og-fiskerinaeringen-hovedrapport-dokument-nr-st-04555-2.html (nedlastet 7-nov-2019)

/25/ Aktivitetsforskriften. Forskrift om utføring av aktiviteter i petroleumsvirksomheten FOR-2010-04-29-613, https://lovdata.no/dokument/SF/forskrift/2010-04-29-613 (nedlastet 29-nov-2019)

/26/ Konkraft rapporten:2018, http://konkraft.no/konkraft_statement/ (nedlastet 6-nov-2019)

/27/ S-001 NORSOK: Technical Safety:2018

/28/ SAFE – Et rettferdig arbeidsliv, https://safe.no/ydmykende-overvaking-i-transocean/ (nedlastet 09-okt-2019)

/29/ Wikipedia, end-to-end encryption, https://en.wikipedia.org/wiki/End-to-end_encryption (nedlastet 29-nov-2019)

/30/ ISO 22301:2019 « Security and resilience-Business continuity management systems – Requirements »

/31/ Positive Technologies: Diameter vulnerabilities exposure report 2018, https://www.ptsecurity.com/ww-en/analytics/diameter-2018/ (nedlastet 11-okt-19)

/32/ EKOM loven https://lovdata.no/dokument/NL/lov/2003-07-04-83 (nedlastet 29-nov-2019)

/33/ EKOM forskriften FOR-2004-02-16-401, Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste, https://lovdata.no/dokument/SF/forskrift/2004-02-16-401?q=ekomforskriften (nedlastet 29-nov-2019)

/34/ NKOM: Årsrapport 2018, https://www.nkom.no/aktuelt/rapporter/_attachment/41814?_ts=16a6dc64dea (nedlastet 29-nov-2019)

/35/ TV2-nyhet om båt i nød, https://www.tv2.no/a/10250247/ (nedlastet 30-okt-19)

/36/ NRK Finnmark: Norske fly mistet GPS signaler, https://www.nrk.no/finnmark/norske-fly-mister-plutselig-gps-signalene_-dette-er-_jamming_-1.14282767 (nedlastet 28-nov-2019)

/37/ Oversikt over internasjonale offentlige fibernettverk, https://cablemap.info/_default.aspx (nedlastet 4-nov-2019)

/38/ SOIL – EPIM: https://epim.no/soil/ (nedlastet 4-nov-2019)

/39/ Digi.no: Økning i bruk av falske basestasjoner, https://www.digi.no/artikler/kraftig-okning-i-bruk-av-falske-basestasjoner/376635 (nedlastet 4-nov-2019)

/40/ Telia hjemmeside: annonsering av samarbeid med Tampnet om IoT satsning, https://www.telia.no/magasinet/smartere-oljeplattformer-med-ny-teknologi/ (nedlastet 26-nov-2019)

/41/ Wikipedia Satellite constellation https://en.wikipedia.org/wiki/Starlink (nedlastet 4-novt-2019)

/42/ Digitale sårbarheter Lysneutvalget. DNV GL rapport om digitale sårbarheter Olje & Gass, https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/sved/5.pdf (nedlastet 21-nov-2019)

/43/ Lysne.O, The Huawei and Snowden Questions, Simula SpringerBriefs on Computing 4. 2018, https://doi.org/10.1007/978-3-319-74950-1_1 (nedlastet 29-nov-2019)

/44/ Sikkerhetsloven, https://blogg.onevoice.no/blogg/aldri-forholdt-deg-til-sikkerhetsloven-fra-1.jan-kan-det-hende-du-ma-det / (nedlastet 29-nov-2019)

/45/ Wikipedia artikkel, Tropospeheric scatterteknikk, https://en.wikipedia.org/wiki/Tropospheric_scatter

/46/ Comtech Systems: Communication links for Offshore Platforms, https://www.comtechsystems.com/wp-content/uploads/2014/05/Communication-Links-for-Offshore-Platforms-2012.pdf (nedlastet 13-nov-2019)

/47/ Statnett har store planer for bruk av droner, https://www.statnett.no/om-statnett/nyheter-og-pressemeldinger/Nyhetsarkiv-2018/droner-skal-passe-pa-statnetts-stromledninger/ (nedlastet 21-nov-2019)

/48/ Telenor satellite Anker Ka-Band services (nedlastet 29-nov-2019)

/49/ Snowden-lekkasje, https://www.theregister.co.uk/2014/11/26/snowden_doc_leak_lists_all_the_compromised_cables/ (nedlastet 14-nov-2019)

/50/ Oneweb system design, https://www.youtube.com/watch?v=REzA_SYInvc&feature=youtu.be (nedlastet 14-Nov-2019)

/51/ SPACENEWS: SpaceX statement, https://spacenews.com/spacex-submits-paperwork-for-30000-more-starlink-satellites/ (nedlastet 14-nov-2019)

/52/ Leosat system; http://leosat.com/ (nedlastet 14-nov-2019)

/53/ SPACENEWS, Amazone satellite communication system, https://spacenews.com/amazon-planning-3236-satellite-constellation-for-internet-connectivity/ (nedlastet 14-nov-2019)

/54/ SPACENEWS, LeoSat, absent investors, shuts down, https://spacenews.com/leosat-absent-investors-shuts-down/ (nedlastet 14-nov-2019)

/55/ Space Norway sin hjemmeside, https://spacenorway.no/om-oss/ (nedlastet 27-nov-2019)

/56/ Kommunikasjon – Utfordringer og løsninger https://www.norskoljeoggass.no/globalassets/dokumenter/drift/hms-utfordringer-i-nordomradene/beredskap/02-resyme-02---torvet----utfordringer-og-losninger.pdf (nedlastet 30-jan-20)

/57/ ISO 8728 Ships and marine technology –Marine gyro-compass

/58/ Kystradiostasjonene http://www.kystradio.no/bedrift/kystradio/ (nedlastet 26-feb-20)

/59/ Kystradioen: Nødprosedyrer og kanalplaner http://www.kystradio.no/bedrift/kystradio/noedprosedyrer-og-kanalplaner/ (nedlastet 26-feb-20)

## Om DNV GL

DNV GL er et internasjonalt selskap innen kvalitetssikring og risikohåndtering. Siden 1864 har vårt formål vært å sikre liv, verdier og miljøet. Vi bistår våre kunder med å forbedre deres virksomhet på en sikker og bærekraftig måte.
Vi leverer klassifisering, sertifisering, teknisk risiko- og pålitelighetsanalyse sammen med programvare, datahåndtering og uavhengig ekspertrådgivning til maritim sektor, til olje- og gass-sektoren, og til energibedrifter. Med 80,000 bedriftskunder på tvers av alle industrisektorer er vi også verdensledende innen sertifisering av ledelsessystemer.
Med høyt utdannede ansatte i 100 land, jobber vi sammen med våre kunder om å gjøre verden sikrere, smartere og grønnere.