2020:01349 - Åpen

Rapport

Kommunikasjonssystemer for ekstern nødkommunikasjon

IKT-sikkerhet – Robusthet i petroleumssektoren 2020

Forfatter(e)
Knut Øien, Karin Bernsmed, Stig Petersen

SINTEF Digital
2021-01-29

SINTEF

SINTEF Digital

Postadresse:
Postboks 4760 Torgarden
7465 Trondheim

Sentralbord: 40005100

info@sintef.no

Foretaksregister:
NO 919 303 808 MVA

Rapport

Kommunikasjonssystemer for ekstern nødkommunikasjon

IKT-sikkerhet – Robusthet i petroleumssektoren 2020

EMNEORD:
Kommunikasjons-systemer
IKT-sikkerhet
Beredskap

VERSJON
2.0

DATO
2021-01-29

FORFATTER(E)
Knut Øien, Karin Bernsmed, Stig Petersen

OPPDRAGSGIVER(E)
Petroleumstilsynet

OPPDRAGSGIVERS REF.
Arne Halvor Embergsrud

PROSJEKTNR
102022556

ANTALL SIDER OG VEDLEGG:
64 (3 vedlegg)

SAMMENDRAG
Formålet med denne rapporten er å gi næringen økt forståelse av rollen til og sårbarheten av kommunikasjonsnettverk, spesielt i beredskapssituasjoner når en definert fare- og ulykkessituasjon (DFU) har inntruffet.

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

UTARBEIDET AV
Knut Øien

SIGNATUR

KONTROLLERT AV
Lars Bodsberg

SIGNATUR

GODKJENT AV
Maria Bartnes

SIGNATUR

RAPPORTNR
2020:01349

ISBN
978-82-14-06411-7

GRADERING
Åpen

GRADERING DENNE SIDE
Åpen

Historikk

VERSJON	DATO	VERSJONSBESKRIVELSE
1.0	2020-12-08	Endelig rapport
2.0	2020-01-29	Oppdatert endelig versjon

Kreditering av bilder:
Side 17: Torbjørn Kjosvold / Forsvaret
Side 22: Tampnet
Side 25: Basert på bilde fra Tampnet
Øvrige bilder: Pixabay

SINTEF

Innholdsfortegnelse

Sammendrag

Innledning

Formålet med denne rapporten er å gi næringen økt forståelse av rollen til og sårbarheten av kommunikasjonsnettverk, spesielt i beredskapssituasjoner når en definert fare- og ulykkessituasjon (DFU) har inntruffet. Rapporten setter søkelyset på ekstern kommunikasjon mellom hav og land i beredskaps-situasjoner, dvs. nødkommunikasjon mot land.

Arbeidet er i hovedsak basert på dokumentgjennomgang, intervju og arbeidsmøter. Intervju har blitt gjennomført med utvalgte oljeselskap, riggselskap og teleoperatører.

Rollen til eksterne kommunikasjonsnettverk ved inntrufne DFU-er

Rollen som eksterne kommunikasjonsnettverk ivaretar ved inntrufne DFU-er er først og fremst varsling av eksterne beredskapsressurser slik at innretningen kan få nødvendig ekstern bistand (helikopter, fartøy, vaktlege, osv.). Dernest vil ekstern kommunikasjon være nødvendig for å ha et felles situasjonsbilde på hav og land, bl.a. for å motta eksperthjelp fra land, noe man er helt avhengig av ved IKT-hendelser.

De fiberoptiske og radiobaserte kommunikasjonslinjene er helt sentrale i den eksterne nødkommunikasjonen mellom innretning og land. Det er viktig at utstyret som inngår her defineres som barriereelementer, med den oppmerksomhet og oppfølging dette innebærer.

Forslag til forbedringer inkluderer å definere tap av ekstern kommunikasjon som en DFU, inkludere tap av ekstern kommunikasjon som spesielle utfordringer for andre DFU-er, definere en DFU som dekker flere sikkerhetssystemer ("sikkerhetssystemer midlertidig ute av drift") og som inkluderer nødkommunikasjons-systemene, angi effekten av de ulike DFU-ene på telekom-systemene i beredskapsplanen, og definere telekom-utstyr som inngår i nødkommunikasjon som barriereelementer.

Risiko og sårbarhet i kommunikasjonsnettverkene

Telekom-systemene er komplekse og integrerte, det er mange aktører involvert, og det er en risiko for ikke å se helheten (ende-til-ende). Samtidig er risiko- og sårbarhetsvurderinger overraskende fraværende.

Basert på intervjuene utrykkes det av enkelte størst bekymring for menneskelige feil og logiske feil, eksempelvis i dynamisk omkopling, som utgjør en enkeltfeilmulighet. Det samme gjelder hovedruteren til operatøren på innretningen. Strømbrudd og strømutkopling er vanlige årsaker til bortfall av kommunikasjon. Når det gjelder tilsiktede hendelser blir angrep av hackere eller innsidere (egne eller underleverandører) trukket frem. Det pekes også på at det er for dårlig fysisk sikring av utstyrsrom offshore på enkelte innretninger.

Forslag til forbedringer inkluderer at risiko- og sårbarhetsvurderinger som dekker eksterne kommunikasjons-nettverk mellom innretning og land blir utført av selskapene og fulgt opp av myndighetene, at adgangs-kontroll til utstyrsrom offshore etterleves, og at reserveløsninger for ekstern kommunikasjon vedlikeholdes og testes regelmessig.

Konsekvenser ved bortfall av kommunikasjonsnettverk

Vurderingen av konsekvenser ved bortfall av eksterne kommunikasjonsnettverk spriker veldig mellom selskapene som ble intervjuet fra proaktiv nedstengning til å fortsette produksjonen som før. Hverken i intervjuene eller i tidligere studier og analyser blir konsekvensene av bortfall vurdert opp mot kravet til minst to uavhengige varslingsveier til land. Det ser ut til å være uklart hvordan dette kravet skal fortolkes og etterleves.

Forslag til forbedringer inkluderer rask varsling til berørte teleoperatører og naboinnretninger blant annet ved strømutkopling og strømbrudd, samt øving på bortfall av kommunikasjon som omfatter både enkelt-innretninger, gjensidig avhengige naboinnretninger, alle områderessurser, og ekstremtilfellet med et sentralt bortfall av nettet som fører til at mye av petroleumsvirksomheten i Nordsjøen stopper opp.

Regelverk og standarder – utfordringer og forslag til forbedringer

En utfordring for både regelverk og standarder er å holde de oppdatert, spesielt på et område som telekom hvor utviklingen går svært raskt.

Det er i rapporten gitt innspill på utfordringer fra selskapene som deltok i intervjuene, og det er gitt 11 spesifikke forslag til endringer i regelverk og standarder.

Anbefalinger

Det er gitt 15 anbefalinger til tiltak for næringen, hvorav fire retter seg mot endringer i standarder, og det er gitt åtte anbefalinger til tiltak for Petroleumstilsynet, hvorav ett retter seg mot tilsyn og de øvrige mot endringer i regelverket.

Vi ser behov for innhenting av mer kunnskap om kommunikasjon ende-til-ende, kunnskap om håndteringen av IKT-hendelser/cyberangrep hvor kontornettverket kan være angrepet og man er avhengig av ekstern ekspertise samtidig som innretningen har ekstern nødkommunikasjon via det samme kontornettverket, og kunnskap om hvordan man totalt sett øver på samt tester kommunikasjonsutstyr og reserveløsninger for ekstern nødkommunikasjon.

Executive summary

Introduction

The purpose of this report is to give the industry a better understanding of the role and vulnerability of communication networks, especially in emergency situations when a defined situation of hazard and accident (DSHA) has occurred. The report focuses on external communication between offshore and onshore in emergency situations, i.e. emergency communication to land.

The work is mainly based on document review, interviews, and work meetings. Interviews have been conducted with selected oil companies, rig companies and telecom operators.

The role of external communication networks during DSHAs

The role that external communication networks exercise during DSHAs is first and foremost notification of external emergency preparedness resources so that the facility can receive the necessary external assistance (helicopters, vessels, on-call doctor, etc.). Secondly, external communication will be necessary to obtain a common situational understanding offshore and onshore, e.g. to receive help from experts onshore, which one is completely dependent on at ICT events.

The fiber optic and radio-based communication lines are absolutely central in the external emergency communication between a facility and land. It is important that the equipment included here is defined as barrier elements, with the attention and follow-up this entails.

Suggestions for improvements include defining the loss of external communication as a DSHA; including the loss of external communication as special challenges for other DSHAs; defining a DSHA that covers several safety systems ("safety systems temporarily out of order") and which includes the emergency communication systems; state the effect of the various DSHAs on the telecom systems in the contingency plan; and define telecom equipment that is part of emergency communication as barrier elements.

Risk and vulnerability in the communication networks

The telecom systems are complex and integrated, there are many actors involved, and there is a risk of not grasping the big picture (communication end-to-end). At the same time, risk and vulnerability assessments are surprisingly absent.

Based on the interviews, some of the greatest concerns are expressed about human errors and logical errors, for example in dynamic switching, which constitute a single error possibility. The same applies to the main router of the operator of the facility. Power outages and power disconnections are usual causes of communication failure. In the case of intentional incidents, attacks by hackers or insiders (own or subcontractors) are highlighted. It is also pointed out that there is poor physical security of offshore equipment rooms on some facilities.

Suggestions for improvements include that risk and vulnerability assessments covering external communication networks between a facility and land are carried out by the companies and followed up by the authorities, that access control to offshore equipment rooms is complied with, and that backup solutions for external communication are regularly maintained and tested.

Consequences of the loss of communication networks

The assessment of the consequences of loss of external communication networks differs greatly between the companies interviewed, from proactive shutdown to continuing production as before. Neither in the interviews nor in previous studies and analyzes are the consequences of loss of communication assessed

against the requirement for at least two independent notification routes to land. It seems unclear how this requirement is to be interpreted and complied with.

Suggestions for improvements include rapid notification to affected telecom operators and neighboring facilities, including in the event of power outages and power disconnections, as well as exercises in handling the loss of communication that includes both single facilities, interdependent neighboring facilities, all area resources, and the extreme case of a central failure of the network leading to much of the petroleum activities in the North Sea shutting down.

Regulations and standards - challenges and suggestions for improvements

A challenge for both regulations and standards is to keep them up to date, especially in an area such as telecom where development is very rapid.

The report provides input on challenges from the companies that participated in the interviews, and 11 specific proposals for changes in regulations and standards are given.

Recommendations

Fifteen recommendations have been made regarding measures for the industry, four of which are aimed at changes in standards, and eight recommendations have been given regarding measures for the Petroleum Safety Authority Norway, one of which is aimed at supervision and the other at changes in regulations.

We see a need for obtaining more knowledge about end-to-end communication, knowledge about the handling of ICT incidents / cyber-attacks where the office network can be attacked and one is dependent on external expertise while the facility has external emergency communication via the same office network, and knowledge on how to practice and test communication equipment and backup solutions for external emergency communication as a whole.

1 Innledning

1.1 Bakgrunn

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

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

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

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

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

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

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

Kommunikasjonsnettverk – *denne rapporten*
: Hensikten har vært å undersøke hvilken rolle datanettverk ivaretar for ekstern kommunikasjon ved fare- og ulykkessituasjoner. Rapporten beskriver utfordringer knyttet til risiko og sårbarhet i datanettverkene og det er utarbeidet konkrete forslag til forbedringer.

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

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

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

1.2 Mål og hensikt

Hovedmålet for denne leveransen er å gi næringen økt forståelse av rollen til og sårbarheten av kommunikasjonsnettverk, spesielt i beredskapssituasjoner når en definert fare- og ulykkessituasjon (DFU) har inntruffet.

Følgende fire målsettinger er definert:

1. Undersøke hvilken rolle datanettverk ivaretar for ekstern kommunikasjon ved de definerte fare- og ulykkessituasjonene (DFU-ene).
2. Vurdere utfordringer knyttet til risiko og sårbarhet i datanettverkene og utarbeide konkrete forslag til forbedringer.
3. Vurdere konsekvensene ved bortfall av eksterne kommunikasjonsnettverk, spesielt hvilken effekt dette kan ha for sikkerheten for den enkelte innretning.
4. Belyse eventuelle utfordringer knyttet opp mot regelverk og standarder og foreslå forbedringer/ endringer i regelverket samt aktuelle standarder som kan benyttes for å innfri forskriftskravene.

Denne rapporten setter søkelyset på ekstern kommunikasjon mellom hav og land i beredskapssituasjoner, dvs. nødkommunikasjon mot land. Betegnelsen kommunikasjonsnettverk benyttes enten dette innbefatter analoge eller digitale signaler. Kommunikasjonsnettverk og datanettverk brukes om hverandre. Dersom det er bestemte datanettverk som omtales, eksempelvis kontornettverk eller teknisk nettverk, så er dette angitt.

1.3 Begrensninger

Følgende begrensninger gjelder:

- "Ekstern kommunikasjon" er i denne rapporten avgrenset til kommunikasjon mellom hav og land, mens ekstern kommunikasjon generelt dekker all kommunikasjon mellom en innretning og omgivelsene, dvs. også kommunikasjon til omkringliggende fartøy og innretninger, som kan inngå som områderessurser i en beredskapssituasjon. Tilsvarende avgrensning av kommunikasjon mellom hav og land gjelder for "nødkommunikasjon".
- Ekstern kommunikasjon ved definerte fare- og ulykkessituasjoner (DFU-er) er vektlagt fremfor ekstern kommunikasjon under normal drift og for kritiske prosesser og utstyr.
- Det er videre lagt vekt på dagens løsninger for kommunikasjonsnettverk fremfor nye trender.
- Oppgavebeskrivelsen angir at *"med bakgrunn i eventuelle risiko og sårbarhetsanalyser for slik infrastruktur, skal man utarbeide konkrete forslag til forbedringer samt peke på utfordringer der disse finnes"*. SINTEF har, enten av konfidensialitetshensyn eller fordi slike analyser ikke foreligger, ikke fått tilgang til risiko- og sårbarhetsanalyser av eksterne kommunikasjonsnettverk. Risiko og sårbarheter er derfor avgrenset til forhold diskutert under intervjuene med selskapene, og forhold omtalt i tidligere studier.
- Når det gjelder beredskapsplaner og planer for håndtering av bortfall av eksterne kommunikasjons-nettverk har noen av selskapene gitt SINTEF tilgang til enkelte plandokumenter. Dette er i hovedsak beredskapsplaner som ikke spesifikt dekker bortfall av ekstern kommunikasjon, samt generelle serviceavtaler (Service Level Agreements – SLA).
- Av hensyn til anonymisering er ikke dokumenter som nevnt ovenfor tatt med som referanser.

1.4 Begreper, definisjoner og forkortelser

1.4.1 Begreper og definisjoner

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

Begrep	Definisjon/beskrivelse	Referanse
Elektronisk kommunikasjon (ekom)	Kommunikasjon ved bruk av et elektronisk kommunikasjons-nett	Ekomloven 2020 [2]
Elektronisk kommunikasjonsnett	System for signaltransport som muliggjør overføring av lyd, tekst, bilder eller andre data ved hjelp av elektromagnetiske signaler i fritt rom eller kabel der radioutstyr, svitsjer, annet koplings- og dirigeringsutstyr, tilhørende utstyr eller funksjoner inngår, herunder nettverkselementer som ikke er aktive	Ekomloven 2020 [2]
Radioutstyr	Et elektrisk eller elektronisk produkt, som enten alene eller sammen med ekstrautstyr, for eksempel en antenne, tilsiktet utstråler eller mottar radiobølger for radiokommunikasjon eller radiobestemmelse	Ekomloven 2020 [2]
Node	En node er i IKT-sammenheng betegnelsen på en enhet i et nettverk. Det kan være for eksempel en ruter, en server eller en svitsj	NOU2015: 13 [3]
Ruter	Funksjonell enhet som etablerer en sti gjennom ett eller flere datanettverk og videresender pakker	IEC 60050 [52]
Server (tjener)	Funksjonell enhet som tilbyr tjenester til arbeidsstasjoner, til personlige datamaskiner eller til andre funksjonelle enheter i et datanettverk	IEC 60050 [52]
Svitsj	En svitsj er et apparat som mottar signaler fra en rekke inngående linjer og sender dem videre etter bestemte regler. (Svitsjer i telefonnettet kalles vanligvis telefonsentraler)	NOU2015: 13 [3]
Mørk fiber	Mørk fiber innebærer at kunden får tilgang til fiber som ikke er lyssatt, og kun leier fiber og selv kobler til ønsket utstyr i begge ender	Regjeringen.no [53]
Definerte fare- og ulykkes-situasjoner (DFU-er)	Et representativt utvalg fare- og ulykkessituasjoner som brukes ved dimensjoneringen av beredskapen	Veiledning til AF § 73 [4]
Beredskap	Tekniske, operasjonelle og organisatoriske tiltak som planlegges iverksatt under ledelse av beredskaps-organisasjonen ved inntrådte fare eller ulykkessituasjoner for å beskytte mennesker, miljø og økonomiske verdier	NORSOK Z-013:2010 [5]
Barriere *	Tiltak som har til hensikt og funksjon enten å forhindre et konkret hendelsesforløp i å inntreffe, eller påvirke et hendelsesforløp i en tilsiktet retning ved å begrense skader og/eller tap. Funksjonen til disse barrierene ivaretas av tekniske, operasjonelle og organisatoriske elementer enkeltvis eller samlet	Ptil 2020 (ptil.no) [6]
IKT-sikkerhetstiltak *	Tiltak for å sikre IKT-systemer og informasjon mot tilsiktede og utilsiktede hendelser	NOU2015: 13 [3]
Trussel	En tilsiktet uønsket handling	NSM 2015 [7]
Fare	En utilsiktet uønsket hendelse	NSM 2015 [7]

Begrep	Definisjon/beskrivelse	Referanse
Risiko (1) **	Med risiko menes konsekvensene av virksomheten med tilhørende usikkerhet	Veiledning til RF § 11 [14]
Risiko (2) **	Risiko kan uttrykkes som en kombinasjon av sannsynligheten for og konsekvensen av en uønsket hendelse	NS 5814:2008 [8]
Risiko (3) **	Risiko kan uttrykkes som forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen	NS 5832:2014 [9]
Sårbarhet (1)	Manglende evne hos et analyseobjekt til å motstå virkninger av en uønsket hendelse og til å gjenopprette sin opprinnelige tilstand eller funksjon etter hendelsen	NS 5814:2008 [8]
Sårbarhet (2)	Et uttrykk for de problemer et system får med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet	NOU2015: 13 [2]
Resiliens	Evnen til et system eller samfunn eksponert for farer til å motvirke, absorbere, tilpasse seg til og gjenvinne fra effektene til en fare raskt og effektivt, inkludert bevarelse og gjenopprettelse av dets sentrale strukturer og funksjoner	UNISDR 2009 [10]
Sikkerhet (1)	Sikkerhet innebærer beskyttelse mot farer og trusler som kan forårsake uønskede hendelser	NOU2015: 13 [2]
Sikkerhet (2)	Beskyttelse av verdier så som mennesker, ytre miljø, utstyr og informasjon	SINTEF 2018:00572 [11]
Digital sikkerhet ***	Beskyttelse av "alt" som er sårbart fordi det er koblet til eller på annen måte avhengig av informasjons- og kommunikasjonsteknologi	Nasjonal strategi for digital sikkerhet 2019 [12]
IKT-sikkerhet ***	Beskyttelse av informasjons- og kommunikasjonsteknologi (maskinvare og programvare, samt kommunikasjons-systemer)	SINTEF 2018:00572 [11]
Cybersikkerhet ***	Beskyttelse av utstyr (komponenter og enheter) og fysiske prosesser som er sårbare gjennom IKT	SINTEF 2019:00361 [13]
Informasjonsteknologi (IT)	Teknologi som behandler informasjon	Dette prosjektet
Operasjonell teknologi (OT)	Teknologi som støtter, kontrollerer og overvåker industriell produksjon, kontroll- og sikkerhetsfunksjoner	Dette prosjektet

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

**) Risiko (1) er et eksempel på en kvalitativ definisjon av risiko, mens risiko (2) og risiko (3) er eksempler på definisjoner for beskrivelse av risiko, jf. [54]

***) Digital sikkerhet brukes synonymt med IKT-sikkerhet og cybersikkerhet [12]. Dette gjelder også i denne rapporten.

1.4.2 Forkortelser

Forkortelse	Beskrivelse
4G/LTE	4. generasjons mobilnett / Long-Term Evolution
ACMA	Atlantic Cable Maintenance & Repair Agreement
AF	Aktivitetsforskriften
AIS	Automatic Identification System – automatisk identifikasjonssystem
BL	Beredskapsledelse
BS	Beredskapssentral

Forkortelse	Beskrivelse
CENELEC	European Committee for Electrotechnical Standardization
CERT	Computer Emergency Response Team
CIM	(Krisehåndteringsverktøy)
CLC	= CENELEC
CSIRT	Cyber Security Incident Response Team
DFU	Definert fare- og ulykkessituasjon
DSC	Digital Selective Calling – digital selektiv samtale
EF	Europeisk fellesskap
Ekom	Elektronisk kommunikasjon
EMC	Electromagnetic Compatibility – elektromagnetisk kompatibilitet
ESD	Emergency Shut Down - nødavstengning
EØF	Europeisk økonomisk fellesskap
EØS	Europeisk økonomisk samarbeid
Ex	Explosion proof – eksplosjonssikker
FOR	Forskrift
GMDSS	Global Maritime Distress and Safety System – globalt maritimt nød- og sikkerhetssystem
GOC	General Operators Certificate – generelt operatørsertifikat (maritimt radiosertifikat)
GPS	Global Positioning System
HAZID	Hazard identification - fareidentifikasjon
HF	High Frequency
HMI	Human Machine Interface – menneske-maskin grensesnitt
HMS	Helse, miljø og sikkerhet
HRS	Hovedredningssentral
IACS	Industrial Automation and Control Systems
IEC	International Electrotechnical Commission
IF	Innretningsforskriften
IKT	Informasjons- og kommunikasjonsteknologi
IMO	International Maritime Organization
IP	Internet Protocol
ISO	International Standardization Organization
IT	Informasjonsteknologi
ITIL	Information Technology Infrastructure Library – IT-infrastruktur bibliotek
L2	2. linje beredskap
LAN	Local Area Network – lokalt nettverk
LER	Local Equipment Room
LTE	Long-Term Evolution – langsiktig evolusjon
MAC	Media Access Control – media-tilgangs-kontroll
Meld. St.	Melding til Stortinget (Stortingsmelding)
MF	Medium Frequency
MOB	Mann over bord
MSC	Maritime Safety Committee – maritim sikkerhetskomite
MSI	Maritime Safety Information – maritime sikkerhetsmeldinger
NAVTEX	Navigational and Meteorological Warning Broadcasting Service – kringkastingssystem for navigasjons- og meteorologiske advarsler
NEK	Norsk elektroteknisk komite
NKOM	Norsk kommunikasjonsmyndighet

Forkortelse	Beskrivelse
NOG/NOROG	Norsk olje og gass
NORSOK	NORsk Sokkels Konkurranseposisjon
NOU	Norges Offentlige Utredninger
NS	Norsk Standard
NSM	Nasjonal sikkerhetsmyndighet
OFFB	Operatørenes Forening For Beredskap
OSPF	Open Shortest Path First
OT	Operasjonell teknologi
PA	Public Address - personvarsling
PABX	Private Automatic Branch Exchange – privat automatisk utveksling
PAGA	Public Address & General Alarm – personvarsling og generell alarm
PC	Personal Computer – personlig datamaskin
PCSS	Process Control, Safety and Support – prosesskontroll, sikkerhet og støtte
PSTN	Public Switched Telephone Network – linjesvitsjet telefonnettverk
Ptil	Petroleumstilsynet
RF	Rammeforskriften
ROC	Restricted Operator Certificate – begrenset operatørsertifikat (maritimt radiosertifikat)
ROS	Risiko og sårbarhet
SAR	Search and Rescue – søk og redning
SART	Search and Rescue Transponder – søk og redningstransponder
SAS	Safety and Automation System – sikkerhets- og automasjonssystem
SBV	Standby Vessel - beredskapsfartøy
SIS	Sikkerhetsinstrumenterte systemer
SKR	Sentralt kontrollrom
SLA	Service Level Agreement
SOIL	Secure Oil Information Link – sikker oljeinformasjonsforbindelse
SOLAS	Safety Of Life At Sea – sikkerhet for liv til sjøs
TCP	Transmission Control Protocol
TER	Telecommunication Equipment Room
TMS	Telecommunication Monitoring System
TR	Technical Report – teknisk rapport
UHF	Ultrahigh Frequency – ultrahøy frekvens
UNISDR	United Nations International Strategy for Disaster Risk Reduction
UPS	Uninterruptable Power Supply – avbruddsfri strømforsyning
USB	Universal Serial Bus – universell seriebuss
VHF	Very High Frequency – veldig høy frekvens
VPN	Virtual Private Network – privat virtuelt nettverk
VSAT	Very Small Aperture Terminal – veldig liten blenderåpningsterminal
W	Watt
WAN	Wide Area Network – fjernnett

1.5 Metode og gjennomføring

Arbeidet er i hovedsak basert på dokumentgjennomgang, intervju og arbeidsmøter. Det er utført i et tverrfaglig prosjektteam med kompetanse innenfor blant annet kommunikasjonssystemer, IKT-sikkerhet, beredskap, samt petroleumsregelverk og standarder innenfor disse fagområdene.

Intervju har blitt gjennomført med utvalgte oljeselskap, riggselskap og teleoperatører, til sammen fem selskap. Av hensyn til anonymitet oppgis ikke navnene på selskapene. Det har blitt gjennomført formøter, intervju og oppfølgingsmøter ved behov.

1.6 Rapportstruktur

Kapittel 2 beskriver rollen til eksterne kommunikasjonsnettverk ved inntrufne DFU-er, krav til ekstern kommunikasjon, hvilke kommunikasjonssystemer og utstyr som benyttes, hvilke systemer og utstyr som er kritisk, og forslag til forbedringer knyttet til ekstern kommunikasjon i beredskapssituasjoner.

Kapittel 3 beskriver utfordringer knyttet til risiko og sårbarhet i datanettverkene knyttet til ekstern kommunikasjon ved inntrufne DFU-er. Beredskapssituasjoner er vektlagt fremfor normal drift og overvåking av kritiske prosesser og utstyr. Basert på utfordringene er det foreslått forbedringer.

Kapittel 4 beskriver konsekvensene ved bortfall[1] av kommunikasjonsnettverk, spesielt hvilken effekt dette kan ha for sikkerheten for den enkelte innretning. Dette inkluderer håndteringen av bortfall av hele eller deler av slike nettverk. Det er også gitt forslag til forbedringer for å redusere konsekvenser av bortfall.

I kapittel 5 er utfordringer knyttet til regelverk og standarder med hensyn til kommunikasjonsnettverk for ekstern kommunikasjon identifisert og forbedringer foreslått. Trender i forhold til teknologiutvikling og utviklingen i aktørbildet er inkludert, men dagens løsninger er vektlagt. Dagens løsninger inkluderer tradisjonelle kommunikasjonssystemer, men i stadig økende grad benyttes integrerte og komplekse systemer.

Kapittel 6 oppsummerer SINTEFs anbefalinger til tiltak for næringen og Petroleumstilsynet, samt behov for videre arbeid med kunnskapsinnhenting.

Det er tre vedlegg (A-C), som gjengir utdrag av relevante krav knyttet til ekstern kommunikasjon, gitt i regelverk og standarder.

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

[1] Bortfall og utfall brukes om hverandre i rapporten.

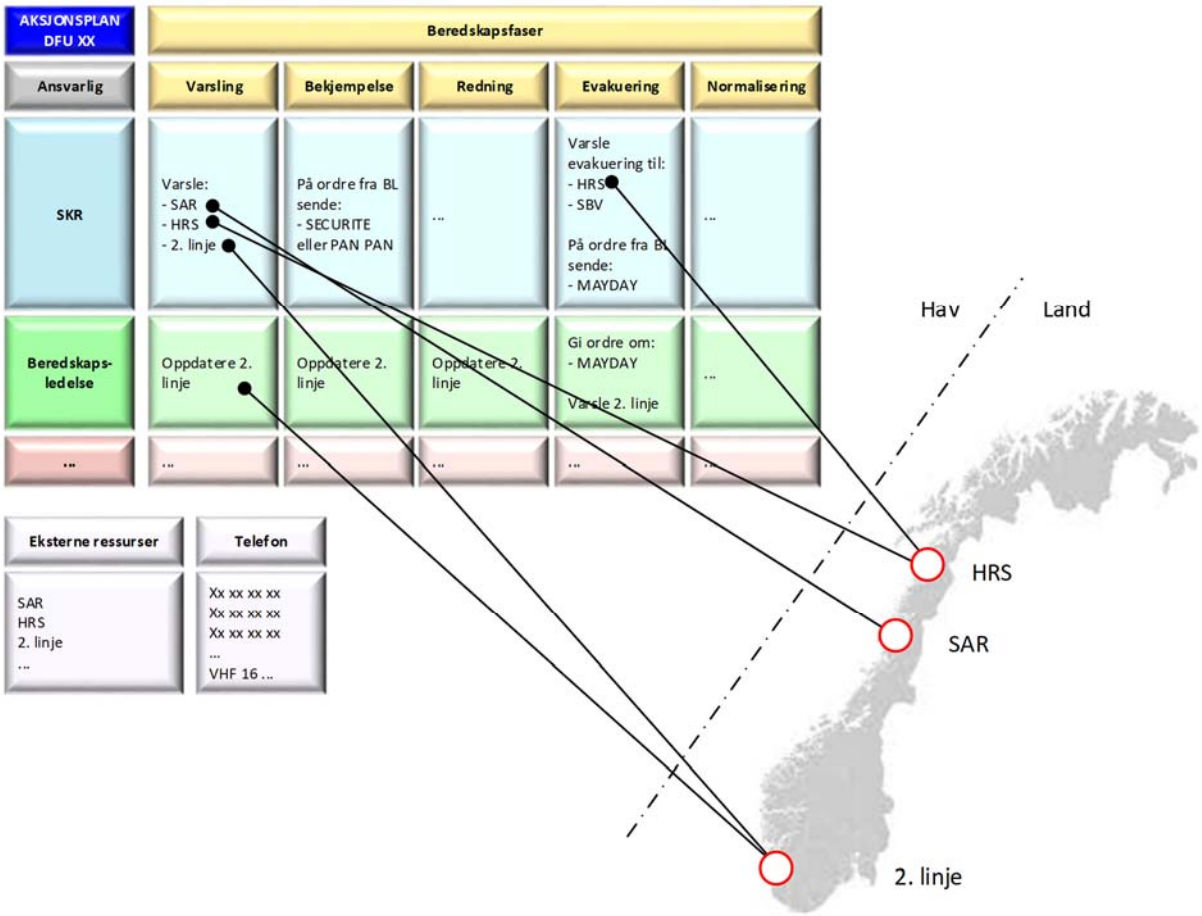
2 Rollen til eksterne kommunikasjonsnettverk ved inntrufne DFU-er

Her beskrives rollen til eksterne kommunikasjonsnettverk ved inntrufne DFU-er, krav til ekstern kommunikasjon, hvilke kommunikasjonssystemer og utstyr som benyttes, hvilke systemer og utstyr som er kritisk, og forslag til forbedringer knyttet til ekstern kommunikasjon i beredskapssituasjoner.

2.1 Behov for ekstern kommunikasjon ved inntrufne DFU-er

Definerte fare- og ulykkessituasjoner (DFU-er) utgjør et representativt utvalg fare- og ulykkessituasjoner som brukes ved dimensjoneringen av beredskapen (jf. veiledningen til aktivitetsforskriften § 73 *Beredskaps-etablering* [4]). Disse er innretnings- og lokasjonsspesifikke, dvs. det finnes ingen fast liste med DFU-er. Aktivitetsforskriften § 73 [15] viser til styringsforskriften § 17 *Risikoanalyser og beredskapsanalyser* [16], og hvor det i veiledningen til styringsforskriften § 17 [17] vises til NORSOK Z-013 [5]. I NORSOK Z-013 Annex C (informativt) er det angitt sjekklister for fareidentifikasjon (HAZID – Hazard identification) som man kan ta utgangspunkt i. Normalt vil en beredskapsplan inneholde i størrelsesorden 15-20 DFU-er (hydrokarbonlekkasjer, brann og eksplosjon, akutt forurensning, osv.), avhengig av hvor spesifikke de er.

For hver DFU inneholder beredskapsplanen aksjonsplaner som angir hvem (*ansvarlig*) som skal gjøre hva (*aksjon*), og når (*beredskapsfase*). Dette inkluderer kommunikasjon, både internt og eksternt. Eksempler på ekstern kommunikasjon mellom hav og land ved en inntruffet DFU er illustrert i figur 2.1.



Figur 2.1 Illustrasjon av ekstern kommunikasjon (hav – land) ved inntruffet DFU

Selv om behovene er noe forskjellig for de ulike DFU-ene, så vil det for de fleste DFU-er være behov for å varsle redningshelikopter[2], hovedredningssentralen (HRS) i nord eller sør, og 2. linje beredskapsledelse i eget selskap. Dette vil normalt utføres fra sentralt kontrollrom (SKR) så raskt som mulig, gjerne angitt med tidskrav (for eksempel innen 3 minutter for SAR, og innen 10 minutter for HRS og 2. linje). Mange selskap har innleid beredskapsvakt, eksempelvis ResQ eller Operatørenes forening for beredskap (OFFB), som da utgjør 2. linje.

Varsling utgjør den første av fem beredskapsfaser (jf. aktivitetsforskriften § 77 *Håndtering av fare- og ulykkessituasjoner* [15]), som angitt øverst i figur 2.1. I mange tilfeller vil det være kritisk at varslingen blir gitt umiddelbart for å møte kravene til beredskap. Noen aksjoner, med tilhørende behov for ekstern kommunikasjon, kan også inntreffe i en senere beredskapsfase enn varslingsfasen, for eksempel beslutning om gjennomføring av evakuering i evakueringsfasen. Aksjonsplanene inneholder normalt telefonlister over aktuelle eksterne ressurser (som angitt nederst til venstre i figur 2.1).

Rollen som eksterne kommunikasjonsnettverk ivaretar ved inntrufne DFU-er er først og fremst varsling av eksterne beredskapsressurser slik at innretningen kan få nødvendig ekstern bistand (helikopter, fartøy, vaktlege, osv.). Dernest vil ekstern kommunikasjon være nødvendig for å ha et felles situasjonsbilde på hav og land, eksempelvis via datastøtte-verktøy som CIM[3], og for å motta eksperthjelp fra land[4].

Rollen som eksterne kommunikasjons-nettverk ivaretar ved inntrufne DFU-er er først og fremst varsling av eksterne beredskapsressurser slik at innretningen kan få nødvendig ekstern bistand (helikopter, fartøy, vaktlege, osv.).

Her betrakter vi ekstern kommunikasjon som kommunikasjon mellom innretning (hav) og land, dvs. at eksempelvis beredskapsfartøy betraktes som en "område-ressurs" og ikke en "ekstern ressurs". Det kreves ikke kommunikasjon til land for varsling til beredskapsfartøy. Det vil imidlertid være ressurser på land som betraktes som områderessurser (for eksempel selskapets eget eller innleide SAR-helikopter og vakthavende lege), men som krever ekstern kommunikasjon (hav-land) på lik linje med eksterne ressurser (som for eksempel offentlige redningshelikopter).

Bortfall eller tap av strømforsyning inngår ofte som en DFU, mens bortfall eller tap av kommunikasjon tradisjonelt ikke har blitt behandlet som en DFU. Blant de selskapene som ble intervjuet varierte antall DFU-er fra 14 generelle DFU-er til 38 scenario-spesifikke DFU-er. Alle selskapene, unntatt ett, hadde tap av strømforsyning som DFU, mens ingen av selskapene hadde tap av ekstern kommunikasjon som DFU.

Argumenter for at man ikke har tap av ekstern kommunikasjon som egen DFU er blant annet at dette kan inngå som følge av andre DFU-er, eksempelvis tap av strømforsyning og IKT-hendelser, og at man dermed også kan få øvd på tap av kommunikasjon. Samtidig ser det ikke ut til å være vanlig at man i aksjonsplanene angir effekten av den enkelte DFU på kommunikasjonssystemene. Hva er eksempelvis effekten av tap av strømforsyning eller en IKT-hendelse som rammer kontornettverket? Dette vil kunne variere både mellom selskap og innretninger. Tap av strømforsyning vil avhenge av om dette inkluderer nødstrøm og UPS i tillegg til hovedkraft, og for IKT-hendelser avhenger det av om man har dedikerte telefonlinjer eller om disse går

[2] SAR-helikopter (Search and Rescue)
[3] https://cim-no.f24.com/cim
[4] Ved IKT-hendelser er man helt avhengig av ekstern kommunikasjon, fordi ekspertisen for å håndtere disse hendelsene sitter på land. Andre hendelser er man i større grad i stand til å håndtere ("autonomt") om bord på innretningen.

via kontornettverket (IP-telefoni). Dersom man kun ser på tap av hovedkraft vil ikke nødkommunikasjon rammes, og om man har dedikerte telefonlinjer vil man ikke rammes av en IKT-hendelse i kontornettverket.

Noen selskap er bevisst på å inkludere tap av kommunikasjon (i det minste intern kommunikasjon) som del av beredskapsøvelser, mens dette var noe uklart hos andre, spesielt tap av ekstern kommunikasjon. Også for intern kommunikasjon går det an å "utfordre" beredskapsorganisasjonen, eksempelvis ved å stille VHF-radioer på feil kanal før øvelsen, eller gjennom andre tilleggsutfordringer.

"De fleste samfunnsfunksjoner er avhengige av kraft og elektronisk kommunikasjon".

"Nettverksoperasjoner utgjør en alvorlig risiko for norske virksomheter …".
"NSM vurderer at statsforvaltningen og virksomheter innen sektorene forsvar, rom, maritim, petroleum og kraft er risikoutsatt".

NSM, 2020 [18]

Listen over DFU-er i beredskapsplanen, som man igjen har utarbeidet aksjonsplaner for, bør ikke være en statisk liste, spesielt i lys av den teknologiske utviklingen. Et av de intervjuede selskapene har da også innført nye DFU-er relativt nylig, slik som cyberangrep. Utviklingen i samfunnet viser at vi blir stadig mer avhengig av ekom og IKT-systemer [18], samt at disse blir stadig mer kompleks og innvevd i alle andre systemer (strømforsyning, vannforsyning, transport, helse, finans, osv.). Det kan derfor være betimelig å spørre om tap av ekstern kommunikasjon, som er kritisk i en nødsituasjon, bør inngå som en egen DFU, spesielt når man har fjerndrift fra en annen innretning eller fra land.

Det var delte meninger om dette blant de selskapene som ble intervjuet. Noen viste, som allerede nevnt, til at man dekker dette via andre DFU-er, og at man har "mange nok" DFU-er. Noen betraktet det også ut fra et risiko- og sannsynlighets-perspektiv og argumenterte med at det er svært usannsynlig å miste all ekstern kommunikasjon, og at man har mange reserveløsninger. Andre mente imidlertid at tap av ekstern kommunikasjon burde inngå som en egen DFU, på lik linje med tap av strømforsyning, nettopp fordi ekom blir stadig viktigere og mer komplekst, blant annet gjennom avhengig-heter mellom naboinnretninger (jf. kap. 2.4).

En risiko- og sannsynlighetsbetraktning som grunnlag for beredskap kan utfordres. Som Røde Kors [19] uttrykker det: *"Å innse at noe uforutsett kan skje, er selve kjernen i beredskap"*. Et alternativ er resiliens-perspektivet som er utbredt innenfor kritisk infrastruktur internasjonalt [20-22].

2.2 Krav til ekstern kommunikasjon i regelverk og standarder

Relevante krav til ekstern kommunikasjon i petroleumsregelverket er gjengitt i Tabell A.1 i vedlegg A. Dette inkluderer også ikke-tekniske krav. Vi avgrenser oss til offshore-innretninger, dvs. at krav til landanlegg i teknisk og operasjonell forskrift [23] ikke er inkludert.

De eneste referansene til standarder som berører ekstern kommunikasjon er NORSOK T-001 [24] og T-100 [25] (jf. veiledning til IF § 18 [26]). Disse er nå erstattet av NORSOK T-101:2019 *Telekom systemer* [27]. I tillegg er NORSOK T-003:2019 *Telekom systemer for flyttbare offshore installasjoner* [28] relevant for flyttbare innretninger, selv om denne ikke refereres til i petroleumsregelverket. Det samme gjelder krav til ekstern kommunikasjon beskrevet i NORSOK S-001:2018 *Teknisk sikkerhet* [29]. NORSOK T-101:2019 viser til NORSOK S-001:2018 med hensyn til ekstern kommunikasjon. Relevante krav til ekstern

kommunikasjon i disse standardene er gjengitt i vedlegg C: NORSOK T-101:2019 i vedlegg C.1, NORSOK T-003:2019 i vedlegg C.2, og NORSOK S-001:2018 i vedlegg C.3.

"Ptil vil tydeliggjøre og videreutvikle regelverket for å ivareta de utfordringene som næringen står overfor ved endringer i trusselbildet og økt digitalisering. Dette innebærer blant annet å følge opp utviklingen av industristandarder som det kan refereres til i regelverket".

Meld. St. 38 (2016-2017) [34]

NORSOK T-101:2019 og NORSOK T-003:2019 viser også til følgende forskrifter utenfor petroleumsregelverket:

- FOR-2004-02-16-401 Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften) [30]
- FOR-2011-12-07-1206 Forskrift om autorisasjon for virksomhet som utfører installasjon og vedlikehold av elektronisk kommunikasjonsnett (autorisasjonsforskriften) [31]
- FOR-2014-07-01-955 Forskrift om radiokommunikasjonsutstyr for norske skip og flyttbare innretninger [32]
- FOR-2019-05-14-604 Forskrift om luftfart med helikopter – bruk av offshore helikopterdekk [33]

Den første og den tredje forskriften har relevante krav til ekstern kommunikasjon som gjengitt i tabell B.1 i vedlegg B. Den første forskriften gjelder generelt, mens den tredje gjelder for flyttbare innretninger.

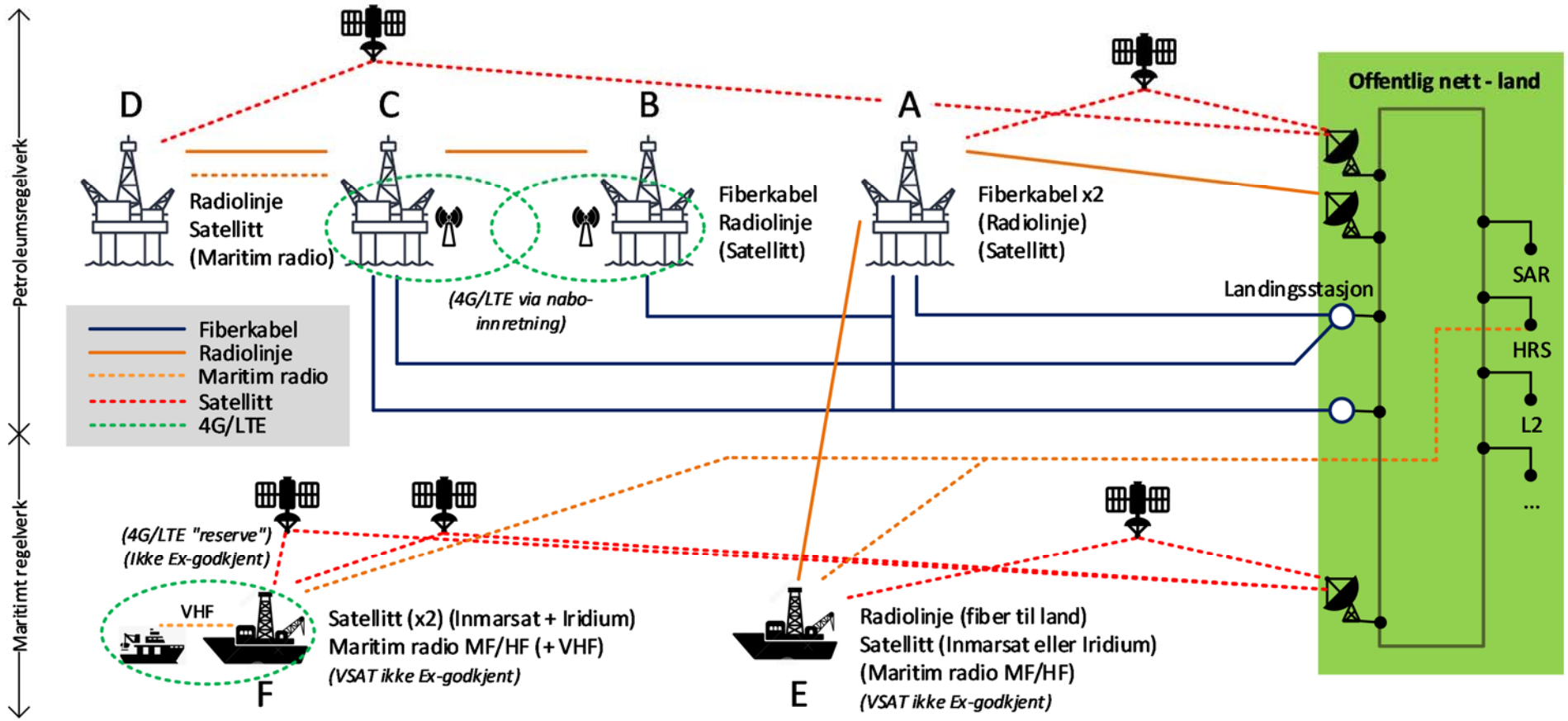
Kravene benyttes som underlag for kapittel 2.3 hvor vi ser på løsninger i forhold til kravene, spesielt kravet om minst to uavhengige varslingsveier til land i innretningsforskriften (IF) § 18 [35]. Videre benyttes kravene som underlag for vurdering av risiko og sårbarhet i kommunikasjonsnettverkene i kapittel 3 og for vurdering av konsekvensene ved bortfall av kommunikasjonsnettverk i kapittel 4. Utfordringer og forslag til forbedringer i regelverket diskuteres i kapittel 5.

2.3 Eksterne kommunikasjonssystemer og utstyr

Hva kreves, hva benyttes, og hva er kritisk ved inntrufne DFU-er? Hva som kreves er gjengitt i vedlegg A og B (krav i regelverk), samt i vedlegg C (krav i standarder). Her ser vi nærmere på hva som faktisk benyttes, og i neste kapittel (kap. 2.4) ser vi på hvilket av dette utstyret som er mest kritisk ved inntrufne DFU-er.

Kravet om minst to uavhengige varslingsveier til land, fortrinnsvis ved hjelp av faste samband, gitt i IF § 18 [35], er et sentralt krav. I veiledningen til § 18 [26] står det videre at *"det bør brukes faste samband som fiberkabel-, radiolinje- eller satellittsystemer dersom innretningens posisjon gjør det mulig. Hvis to uavhengige varslingsveier via faste samband ikke lar seg realisere, kan én av varslingsveiene erstattes med samband i den maritime mobile tjenesten"*. I sistnevnte inngår Inmarsat satellitt og maritim radio (MF/HF og VHF).

Figur 2.2 illustrerer noen typiske løsninger for både faste (øverst) og flyttbare innretninger (nederst).



Figur 2.2 Typiske løsninger for nødkommunikasjon – minimum to uavhengige varslingsveier

Det er svært mange ulike løsninger i bruk. Vi begrenser oss her til noen typiske løsninger, fra de innretninger som er sentralt plassert med god tilgang til faste samband (illustrert til høyre i figuren) til de innretninger som ligger mer perifert eller med dårligere tilgang til faste samband (illustrert til venstre i figuren). Dette gjelder både *faste innretninger* (øverst i figuren) og *flyttbare innretninger* (nederst i figuren). Sistnevnte følger normalt maritimt regelverk.

Innretning A har to uavhengige fiberkabelforbindelser til land, og har i tillegg mulighet for satellittforbindelse samt radiolinjeforbindelse, dvs. to reservemuligheter. Radiolinjeforbindelse direkte inn til land er imidlertid ikke vanlig (må være lokalisert nært land). I henhold til NORSOK T-101:2019 [27] så må kommunikasjonsforbindelsen enten være direkte eller via en annen fast innretning. Dvs. at radiolinjeforbindelsen A-E, som er via en flyttbar innretning, ikke kan inngå som én av de to uavhengige kommunikasjonsveiene. (Derimot kan forbindelsen E-A benyttes for den flyttbare innretningen E).

Innretning B har én fiberkabelforbindelse til land og én radiolinjeforbindelse til innretning C og derfra via fiberkabel til land. I tillegg kan den ha satellittforbindelse som en reservemulighet.

Innretning C har gode kommunikasjonsforbindelser for nødkommunikasjon i likhet med innretning A.

Innretning D er en fjerntliggende innretning uten fiberkabelforbindelse, men med satellittforbindelse og radiolinjeforbindelse til naboinnretning (innretning C), men ingen reservemuligheter (i forhold til krav om to uavhengige kommunikasjonsforbindelser). Den kan ha en maritim radioforbindelse (VHF), dersom den ikke ligger for langt fra en naboinnretning.

Det er også indikert at innretning B og C har basestasjoner for 4G/LTE og mulighet for å kommunisere via dette nettverket. Dersom innretning B har en gasslekkasje, så blir basestasjonen der stengt ned, men man kan allikevel på innretning B ha 4G/LTE dekning fra basestasjonen på innretning C, og derfra videre med fiberkabelforbindelse til land. Dette utgjør da, i utgangspunktet, en uavhengig varslingsvei til land, via en naboinnretning.

Man er imidlertid avhengig av at en naboinnretning med basestasjon ikke ligger alt for langt unna. 4G/LTE gir dekning i et område rundt en innretning, med en maksimal rekkevidde på opptil 40-50 km avhengig av konfigurering og utsendt effekt. Det er også utfordringer med 4G/LTE sammenliknet med radiolinje, blant annet ved at man ikke kan ha dedikert båndbredde og prioritet, men deler tilgjengelig kapasitet med andre brukere.

For bruk av 4G/LTE på egen innretning er man uansett avhengig av innretningens fiberkabel-, radiolinje- og/eller satellittforbindelse til land, og dermed utgjør 4G/LTE *ikke* en uavhengig varslingsvei til land. Dessuten er 4G/LTE i utgangspunktet ikke Ex-godkjent og kan ikke benyttes ved gasslekkasje. (Det ble imidlertid påpekt under intervjuene at 4G/LTE for dekning om bord på innretningen kan konfigureres med lav utsendt effekt, og dermed forbli aktiv ved gasslekkasje).

Innretning E er en flyttbar innretning som ligger sentralt med nærhet til faste innretninger. Den har radioforbindelse til innretning A, og derfra videreforbindelse til land via fiberkabel. Den andre forbindelsen er via satellitt. En tredje mulighet er MF/HF i den maritime mobile tjenesten. VSAT er ikke Ex-godkjent og kan dermed ikke brukes ved for eksempel en gasslekkasje.

Innretning F er en fjerntliggende flyttbar innretning som hverken har fiberkabelforbindelse eller radioforbindelse. Én mulighet er satellitt. For å oppnå to uavhengige forbindelser kan dette være Inmarsat og Iridium. Også MF/HF kan benyttes. I tillegg er det mulig å benytte VHF til et eventuelt beredskapsfartøy.

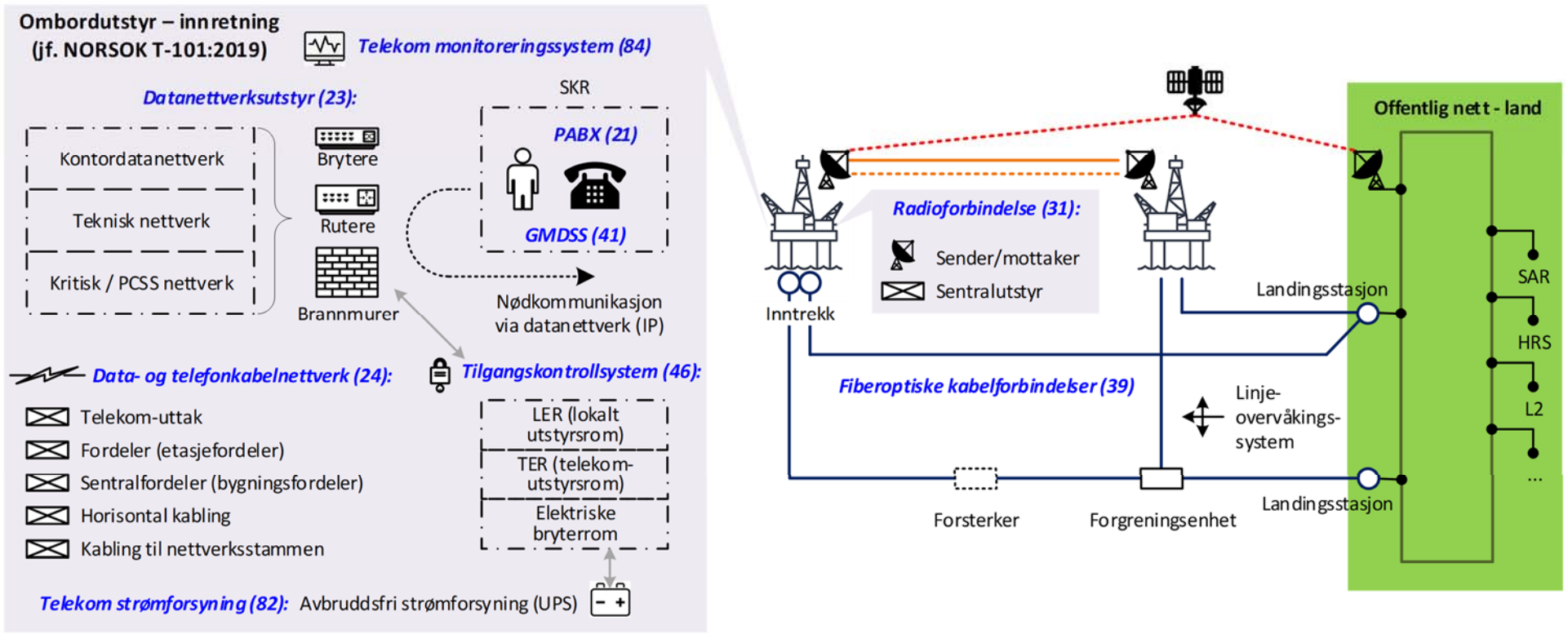
På land går kommunikasjonsforbindelsen videre til SAR-helikopter, hovedredningssentral (HRS) og 2. linje (L2) ved operatørens hovedkontor via det offentlige fibernettet, eller direkte til kystradio Nord og Sør som er lokalisert ved HRS Nord og Sør.

Figur 2.3 illustrerer bruk av fiberkabel-, radiolinje- og 4G/LTE-kommunikasjonsforbindelser for faste og flyttbare innretninger.

Figur 2.3 Illustrasjon av fiberkabel-, radiolinje- og 4G/LTE-forbindelser (Bilde: Tampnet)

Satellittforbindelser er ikke vist i denne figuren.

Figur 2.4 viser typisk utstyr som inngår i nødkommunikasjon basert på systembeskrivelsene og kravene til disse gitt i NORSOK T-101:2019 [27] (se vedlegg C.1). Systemnummer er angitt i parentes i figuren.



Figur 2.4 Typisk utstyr som inngår i nødkommunikasjon (basert på NORSOK T-101:2019 [27])

Nødkommunikasjonen fra en innretning starter for de fleste DFU-er med at kontrollromsoperatør benytter *telefonsystemet (PABX)* for å varsle SAR-helikopter og deretter hovedredningssentralen (HRS) og 2. linje beredskapsorganisasjon i eget selskap. PABX kan være direktekablet til telefonsentralen og derfra videre til den eksterne kommunikasjonsforbindelsen (*fiberoptisk kabelforbindelse*, *radioforbindelse* eller satellitt).

PABX kan alternativt gå via datanettverket med IP-telefoni (og derfra til den eksterne kommunikasjonsforbindelsen). Da kreves det at *datanettverksutstyr* som inngår i nødkommunikasjonsforbindelsen tilfredsstiller alle krav til nødkommunikasjon. Her inngår typisk utstyr som brytere, rutere og brannmurer. I tillegg inngår *data- og telefonkabelnettverket* som del av datanettverksutstyret, som igjen består av ulike komponenter/utstyr (bl.a. uttak, kabler og fordelere).

Av *påbudte og generelle radiosystemer* inngår krav til GMDSS. Et nødvarsel kan gis via GMDSS-stasjonen.

Det er krav om et *tilgangskontrollsystem* for telekom-utstyr, bl.a. for lokalt utstyrsrom (LER), telekom-utstyrsrom (TER) og elektriske bryterrom. Videre har alt utstyr som inngår i nødkommunikasjon krav i forhold til strømforsyning – *telekom strømforsyning*. Det kreves UPS (avbruddsfri strømforsyning). Til slutt er det krav til et *telekom monitoreringssystem* som inkluderer overvåking av kritiske kommunikasjonsforbindelser til eksterne operasjonssentre.

Alle disse systemene kan medføre sårbarheter. Dette inkluderer nettangrep, bl.a. fordi det for noen av systemene kreves ekstern tilgang for konfigurering og vedlikehold (f.eks. system 21 - PABX og system 84 - monitoreringssystem, jf. NORSOK T-101:2019 [27]).

Radioforbindelse til land krever sendere og mottakere samt sentralutstyr om bord, mens *fiberoptiske kabelforbindelser* inkluderer utstyr som inntrekk til innretninger, forsterkere, forgreningsenheter, landingsstasjoner og linjeovervåkingssystem. Ofte, som for Tampnet, benyttes passive kabler uten forsterkere.

Mange av de samme systemene som er vist på figur 2.4 er også aktuelle for flyttbare innretninger. NORSOK T-003:2019 [28], for flyttbare innretninger, lister imidlertid ikke systemene på samme måte som NORSOK T-101:2019 [27].

2.4 Kritiske eksterne kommunikasjonssystemer og utstyr ved inntrufne DFU-er

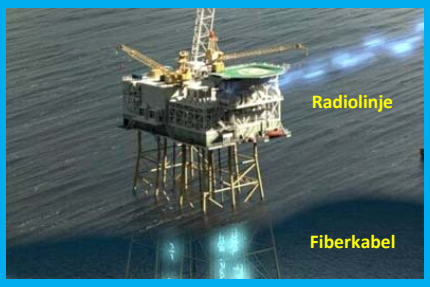
Alle kommunikasjonssystemer og utstyr som inngår i de to (eller flere) uavhengige varslingsveiene til land, jf. figur 2.4, vil være kritiske for nødkommunikasjon mellom innretning og land ved inntrufne DFU-er.[5] Mye av ombordutstyret vil følges opp gjennom innretningens barriere- og vedlikeholdsstyring, mens noe av ombordutstyret følges opp av teleoperatørene.

I utgangspunktet skal alt utstyr som inngår som en del av nødkommunikasjonen defineres som barriereelementer, dvs. inngå i barrierefunksjonen nødkommunikasjon. I tillegg kommer de tilhørende operasjonelle og organisatoriske barriereelementene, slik som f.eks. den varslingsansvarlige (og at vedkommende har nødvendig kompetanse og opplæring).

[5] Kritikaliteten til det enkelte utstyret påvirkes av redundansen. Det ble under intervjuene diskutert mulige "single-point-of-failures" (enkeltfeilmuligheter), dvs. utstyr uten redundans, noe vi kommer tilbake til i kapittel 3 under vurdering av risiko og sårbarhet. Totaloversikter over utstyr ende-til-ende (fra PABX i SKR frem til SAR/HRS/2. linje), og dermed også redundans, har ikke vært mulig å fremskaffe. Vi kommer tilbake til dette i kapittel 6 under behov for videre kunnskapsinnhenting. (Generelt er det mye redundans; redundante rutere, brannmurer, brytere, antenner, osv.).

Ptil har imidlertid avdekket flere svakheter/funn i barrierestyringen [36]. Ptil inkluderer i sin rapport også intern nødkommunikasjon og nødkommunikasjon med områderessurser, men ett viktig funn som går direkte på nødkommunikasjonen mellom innretning og land er: *"Det blir også i ulik grad vurdert om fiberoptisk og radiobaserte kommunikasjonslinjer med nødvendig infrastruktur skal være en del av barriere for nødkommunikasjon. Der selskapene har definert disse systemene til å tilhøre nødkommunikasjonsutstyr, mangler ofte den nødvendige knytning og oppfølging i vedlikeholdsstyringssystemet."*

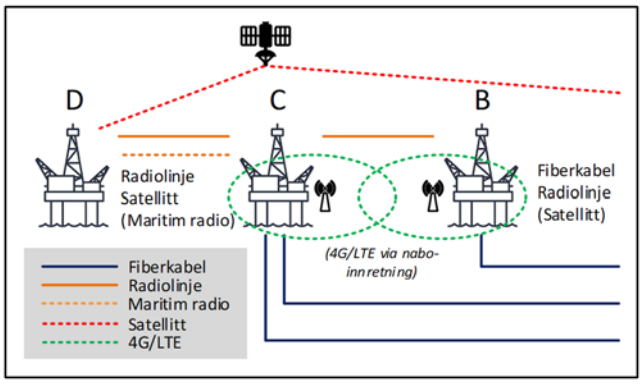
De fiberoptiske[6] og radiobaserte kommunikasjonslinjene er helt sentrale i den eksterne nødkommunikasjonen mellom innretning og land. Det er viktig at utstyret som inngår her defineres som barriereelementer, med den oppmerksomhet og oppfølging dette innebærer, spesielt i lys av at bortfall av ekstern kommunikasjon mellom innretning og land ikke inngår som en egen DFU, jf. kapittel 2.1.



De fiberoptiske og radiobaserte kommunikasjonslinjene er helt sentrale i den eksterne nødkommunikasjonen mellom innretning og land.
Det er viktig at utstyret som inngår her defineres som barriereelementer, med den oppmerksomhet og oppfølging dette innebærer.

I NORSOK T-101:2019 [27], kapittel 11.2, står det: *"Når et datanettverk brukes til å levere viktig PABX-kommunikasjon, skal alle deler av systemet som kreves for å opprettholde funksjonen være utformet i samsvar med kravene til nødkommunikasjonssystemer i punkt 5.3.2."* Det vil være nærliggende å forvente at disse delene inngår som barriereelementer, men intervjuene tyder på at dette ikke er tilfellet. Det ser ut som man betrakter segregeringen av kontordatanettverket fra det tekniske nettverket som en barriere i seg selv, men dette dreier seg hovedsakelig om å beskytte det tekniske nettverket fra kontordatanettverket, ikke opprettholdelse av funksjonen til komponentene i kontordatanettverket som inngår i PABX-kommunikasjon.

Figur 2.5 viser et utdrag av figur 2.2, for å diskutere muligheten for og problemene med ulik kritikalitet av kommunikasjonsutstyr mellom innretninger.



Figur 2.5 Ulik kritikalitet mellom innretninger

Innretning C har redundant fiberkabel, og er ikke avhengig av radiolinje for å oppfylle kravet om to uavhengige varslingsveier til land, mens både innretning B og D normalt er avhengig av radiolinje-forbindelsen til innretning C. Sett fra innretning C er ikke radiolinjekommunikasjonen like kritisk som for de to naboinnretningene. Det kan derfor skje at innretning C har lavere kritikalitet på radiolinje-utstyret enn innretning B og D, noe som er uheldig for innretning B og D. Ptil har også adressert dette, og sier at *"det er her viktig at selskapene snakker sammen og får satt riktig kritikalitet og oppfølging på slikt utstyr"* [36].

[6] Det fiberoptiske nettet er også viktig ut over petroleumssektoren. Gjennom fibernettet i Nordsjøen transporteres ikke bare data fra petroleumssektoren, men også fra andre offentlige og private virksomheter [37].

Øvrige funn i rapporten til Ptil om kommunikasjonssystemer, både for barrierestyring og andre forhold, er tatt opp i kapittel 3 om risiko og sårbarhet (tabell 3.3).

Vurderinger og erfaringer rundt enkeltutstyr som er kritisk og sårbart, er beskrevet i kapittel 3 om risiko og sårbarhet.

2.5 Forslag til forbedringer knyttet til ekstern kommunikasjon i beredskapssituasjoner

Tap av ekstern kommunikasjon som egen DFU ble tatt opp i kapittel 2.1 og viser at det er delte meninger om dette. Noen ønsker det velkommen, noen mener det dekkes av andre DFU-er, og noen mener det er svært usannsynlig at man mister all ekstern kommunikasjon (og at det derfor ikke er behov for å ha dette som en egen DFU).

Det er opp til selskapene selv om de definerer tap av ekstern kommunikasjon som en DFU (eventuelt også intern nødkommunikasjon). Alternativt kan tap av ekstern (og eventuelt intern) nødkommunikasjon inngå i aksjonsplanene i beredskapsplanen som spesielle utfordringer (eskalering) for andre DFU-er. Det kan også vurderes å definere en DFU som dekker flere sikkerhetssystemer ("sikkerhetssystemer midlertidig ute av drift"), hvor nødkommunikasjonssystemene kan inngå. Det bør også vurderes å angi i aksjonsplanene for de DFU-ene det gjelder, dersom de påvirker funksjonen til nødkommunikasjonssystemene.

Øving av "tap av ekstern kommunikasjon" som en DFU kan være godt egnet som en skrivebordsøvelse (Table-Top øvelse). Det som er viktig er at dette er gjennomtenkt og at man vet, og har øvet på, hvordan dette skal håndteres. Ifølge en av de som ble intervjuet var nødkommunikasjon en stor utfordring under Deepwater Horizon hendelsen.

Alternative forbedringer (en eller flere):

1. "Tap av ekstern kommunikasjon"-DFU
2. Spesiell utfordring for andre DFU-er
3. "Sikkerhetssystemer ute av drift"-DFU
4. DFU-enes effekt på telekom-systemer
5. Telekom-utstyr som barriereelementer

Ptil kan ikke i regelverket kreve at tap av ekstern kommunikasjon skal inngå som en DFU, men de kan utdype at "det representative utvalget" av DFU-er bør gjenspeile situasjonen til enhver tid, slik at dette utvalget ikke blir en statisk liste. Dette gjelder generelt og ikke for ekstern kommunikasjon i beredskapssituasjoner spesielt. Dette kunne eksempelvis vært tatt inn i veiledningen til aktivitetsforskriften § 73 *Beredskapsetablering* [4]. Vi kommer tilbake til dette i kapittel 5.

Det å sikre at alt telekom-utstyr som inngår i nødkommunikasjon defineres som barriereelementer vil være viktig for å få nødvendig oppmerksomhet og oppfølging. En utfordring for telekom-utstyr for ekstern kommunikasjon er at mye av dette utstyret ikke inngår i operatørenes barriere- og vedlikeholdsstyring, men driftes og vedlikeholdes av teleoperatører (direkte, remote eller via "remote hands"[7]).

[7] Teleoperatørene kan være om bord selv for vedlikehold, de kan utføre fjernvedlikehold fra land, eller de kan drive fjernvedlikehold med utførende hjelp av innretningens vedlikeholdspersonell ("remote hands").

3 Risiko og sårbarhet i kommunikasjonsnettverkene

Her beskrives utfordringer med hensyn til risiko og sårbarhet i datanettverkene knyttet til ekstern kommunikasjon ved inntrufne DFU-er. Beredskapssituasjoner er vektlagt fremfor normal drift og overvåking av kritiske prosesser og utstyr. Basert på utfordringene er det foreslått forbedringer.

3.1 Krav til IKT-sikkerhet i kommunikasjonsnettverk

Det er ingen direkte henvisning til IKT-sikkerhet i petroleumsregelverket. *"Sikkerhetskravene er generelt utformet og det er uklart om de inkluderer IKT-sikkerhet"* (NOU 2018: 14) [38]. Krav til IKT-sikkerhet i kommunikasjonsnettverk er gitt i NORSOK T-101:2019 (Telekom systemer) [27] og NORSOK T-003:2019 (Telekom systemer for flyttbare offshore installasjoner) [28]. Som nevnt i kapittel 2.2, så erstatter NORSOK T-101:2019 [27] de tidligere NORSOK T-001:2010 [24] og NORSOK T-100:2010 [25], som igjen henvises til fra veiledning til innretningsforskriften § 18 [26].

I NORSOK T-101:2019 [27] er det i kapittel 6.5 IKT-sikkerhet gitt generelle krav (kap. 6.5.1) og krav til sårbarhetsvurdering (kap. 6.5.2) som vist i tabell 3.1 (utdrag fra tabell C.1 i vedlegg C.1).

Tabell 3.1 Krav til IKT-sikkerhet for telekom-systemer [27]

AVSNITT OG TEMA	KRAV
NORSOK T-101:2019 (en) Telekom systemer [27]	
DEL 1 Generell telekom	
6. Systemkrav	
6.5 IKT-sikkerhet 6.5.1 Generelt (utdrag)	IKT-sikkerhet skal opprettholdes under hele levetiden til telekom-systemer. Anbefalinger til beste praksis kan man finne i følgende publikasjoner: DNVGL-RP-G108, NOG 104, NEK IEC 27001 og NEK IEC 27002. …
6.5.2 Sårbarhets-vurdering	En sårbarhetsvurdering skal gjennomføres for hvert telekom-system for å identifisere sikringsrisikoer og avhjelpende tiltak. Sårbarheter er svakheter i systemet og i prosedyrer som kan utnyttes av en trussel-agent. Resultatet av sårbarhetsvurderingen bør være en liste over sårbarheter sammen med tilhørende avhjelpende tiltak nødvendig for å begrense sannsynligheten for utnyttelse av disse sårbarhetene. Følgende tema bør som et minimum adresseres i sårbarhetsvurderingen: – Fysisk beskyttelse av maskinvare; – Ubrukte fysiske porter; – Adgangsmetoder; – Brukeradministrasjon og passord policy; – Oppgraderingsstyring; – Sikkerhetskopiering og nød-gjenoppretting; – Skadevare-beskyttelse; – Fjerntilgang. Resultatet av sårbarhetsvurderingen kan inneholde kritisk informasjon og skal behandles deretter.

I NORSOK T-003:2019 [28] er det i kapittel 8 IKT-sikkerhet gitt generelle krav (kap. 8.1) og (spesifikke) krav (kap. 8.2) som vist i tabell 3.2 (utdrag fra tabell C.2 i vedlegg C.2).

Tabell 3.2 Krav til IKT-sikkerhet for telekom-systemer for flyttbare offshore installasjoner [28]

AVSNITT OG TEMA	KRAV
NORSOK T-003:2019 (en) Telekom systemer for flyttbare offshore installasjoner [28]	
8. IKT-sikkerhet	
8.1 Generelt	Hensikten er å levere sikre nettverksløsninger til alle partene på den mobile offshore-enheten og være i stand til å kontrollere og overvåke trafikken. Kravene i NOG 104 skal følges.
8.2 Krav	Fjerntilgang/fjernkommunikasjon skal skaffes og følgende gjelder: – Ingen VPN (virtuelle private nettverk) tunneler tillatt for prosesskontroll og støtte-systemer (PCSS) på riggen; – Segmenterte nettverk for PCSS/IKT-infrastrukturen, og kontroll av alle kommunikasjonsveier; – Fjerntilgang: o Begrenses til godkjente brukere; o All aktivitet logges; – Sikker filoverføring: o Kun overføring til den mobile offshore-enheten av filer sjekket for skadevare og ondsinnet kode; – Tidsbegrenset tilgang basert på input fra godkjent arbeidstillatelse; – To-faktor-autentisering påkrevd for fjerntilgang; – Kun personlige brukerkontoer tillatt for autentisering til fjerntilgangsløsningen; – Sikker overføring av alle permanente datastrømmer fra mobil offshore-enhet til land; – Ingen standard/fabrikksatte passord eller IP-adresser tillatt på utstyr installert på den mobile offshore-enheten; – Passord skal revideres og fornyes periodisk. Generell sikring skal besørges som følger: – Alle PCSS/IKT-nettverk skal være logisk separert og avgrenset med en brannmur; – Et innholds-filter for all gjestetrafikk skal benyttes, og skal konfigureres for å begrense tilgang; – Alle endringer skal være i henhold til en endringsledelsesprosess: o Dette kan basere seg på et IT-infrastruktur-bibliotek (ITIL) eller lignende; – Alle stativ som inneholder nettverks-utstyr, skal sikres: o Kun autorisert personell skal ha adgang; – Alle nettverk eksponert for SOIL og Internett, skal være beskyttet med inntrengnings-deteksjons-systemer for logging av all nettverksaktivitet; – Alle PCSS nettverk skal konfigureres med nivå 2 sikring, for å forhindre oppkobling av uautorisert utstyr: o Dette kan gjøres med bryterport-konfigurering som kun tillater forhånds-godkjente MAC (medie-tilgangs-kontroll) adresser eller sertifikat-baserte løsninger.

Det er noen avvik mellom IKT-sikkerhetskravene i NORSOK T-101:2019 [27] og NORSOK T-003:2019 [28]. Sistnevnte krever ikke sårbarhetsvurdering og henviser under generelle krav kun til NOG 104 [39][8],

[8] Her er imidlertid kravene i NOG 104 obligatoriske, mens kravene i NOG 104 og andre publikasjoner blir vist til som anbefalinger for beste praksis i NORSOK T-101:2019.

mens de spesifikke kravene er mer detaljerte enn for NORSOK T-101:2019. NORSOK T-101:2019 har ingen referanse til NORSOK T-003:2019, mens motsatt viser NORSOK T-003:2019 til at *"der det er relevant kan NORSOK T-101:2019 eller deler av den benyttes for mobile offshoreenheter"*.

Den eneste referansen til NORSOK-standarder for kommunikasjonssystemer i petroleumsregelverket er avgrenset til *"krav til utforming av interne kommunikasjons- og alarmsystemer"* (jf. veiledning til IF § 18 [26]), noe som ikke inkluderer ekstern kommunikasjon. Henvisningen bør også dekke ekstern kommunikasjon, samt at referansene til de gamle NORSOK-standardene (utgått) erstattes med de nye NORSOK-standardene for telekom-systemer. Vi kommer tilbake til dette i kapittel 5.

3.2 Sårbarheter og risiko i kommunikasjonsnettverk fra tidligere studier

Ptil sin rapport om kommunikasjonssystemer fra 2020 [36] beskriver hvordan de ulike selskapene følger opp ansvar, kompetanse og vedlikehold av kommunikasjonssystemer. Noen av funnene i denne rapporten er relevante mht. mulige sårbarheter og risiko knyttet til ekstern kommunikasjon ved inntrufne DFU-er. Relevante funn er listet i tabell 3.3.

Tabell 3.3 Relevante funn i Ptil-rapport [36]

Kapittel og tema	Funn
6 Kommunikasjons-ansvarlig	Det er få som har definert rollen som kommunikasjonsansvarlig i stillingsinstrukser. Det er heller ikke nok å ha definert rollen eller pekt på hvem som har den, vedkommende skal også inneha tilstrekkelige kvalifikasjoner og kompetanse til å kunne utøve rollen
9 Vedlikehold av kommunikasjons-systemer	Sentralutstyr som sentraler, servere og mer spesialisert utstyr, overvåkes og vedlikeholdes i mange tilfeller av egne «spesialister» som jobber på tvers av ulike innretninger eller av eksternt personell
	De verifikasjoner og vedlikeholdsaktiviteter som blir utført på sentralutstyr og distribusjonsnett fra land blir i mindre grad dokumentert og synliggjort i vedlikeholdsstyringssystemet
	Det blir i økende grad installert telekom-utstyr som eies av andre slik som 4G/LTE basestasjoner
10 Barrierestyring og ytelseskrav	Ytelseskravene som settes til barriereelement for nødkommunikasjon er ofte basert på designkrav til installasjonen og ikke spesifikke målbare krav til ytelser i drift
	Det utstyret som er definert i styrende dokumentasjon som del av barrierefunksjon skal følges opp slik at man sikrer at barrierefunksjonen blir ivaretatt og tilstanden er kjent. Vi finner flere tilfeller der dette ikke gjøres
	Vi registrerer at kommunikasjonslinjer på tvers av innretninger og selskaper kan ha ulik kritikalitet og oppfølging
11 Kommunikasjon i fare- og ulykkes-situasjoner	Det er også noe ulik praksis på hva som defineres som nødkommunikasjonsutstyr og hva som faktisk benyttes til nødkommunikasjon
11.4 Trening og øvelse	Det stilles spørsmål til om man øver tilstrekkelig på situasjoner der ulike sambands-løsninger av ulike årsaker ikke er tilgjengelig
13 Selskapenes tilbake-melding	Endel infrastruktur tilhørende fibernettet krever også i økende grad mer oppmerksomhet på vedlikeholdssiden grunnet alder
	Det rapporteres om økende grad av utfordringer knyttet til software oppgraderinger, slike oppgraderinger kan forekomme relativt ofte og krever mye arbeid å få utført

DNV GL sin rapport fra 2020 [37] beskriver utfordringer og risiko i dagens telekommunikasjonsløsninger som brukes i petroleumssektoren. Noen av funnene i denne rapporten er relevante mht. mulige sårbarheter og risiko knyttet til ekstern kommunikasjon ved inntrufne DFU-er. Relevante funn er listet i tabell 3.4.

Tabell 3.4 Relevante funn i DNV GL-rapport [37]

Kapittel og tema	Funn
3 Innledning	Gjennom nettet [Tampnet] i Nordsjøen transporteres ikke bare data fra petroleums-sektoren, men også for andre offentlige og private virksomheter
4 Sikkerhet i tele-kommunikasjonsløsninger som anvendes i dag	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
5 Telekommunikasjons-systemer	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
	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
5.1 Telecommunication Monitoring System (TMS)	Telekomsystemer skal monitoreres av TMS, det samme med alle kritiske kommunikasjonslinker, hvis de ikke blir monitorert av et annet system
	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 monitorerings-protokollen kan være sårbar. Det er kritisk å herde og beskytte TMS slik at det ikke kan bli misbrukt til å angripe andre telekomsystemer
8.2 Sikkerhet i tele-kommunikasjon på internasjonale, "åpne" media	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
	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
8.5 Årvåkenhet	Du snakker – hvem lytter?
8.6 Beredskaps-planlegging	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
8.7 Risikovurdering av kommunikasjonssystemer	Beredskapsplaner bør utvikles for å håndtere utfall av telenettet
	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

Lysne-utvalget har i sin rapport [3] laget en sammenstilling av hendelser som forårsaker svikt i tele-kommunikasjon, som gjengitt i tabell 3.5. (Feilfordelingen er lagt inn i tabellen av SINTEF).

Tabell 3.5 Hendelser som har forårsaket svikt i telekommunikasjon [3]

	Logiske feil	Fysiske feil
Tilsiktede hendelser	- Elektroniske angrep på nett-elementer, drifts- og støttesystemer	- Fysiske angrep på infrastruktur
Utilsiktede hendelser	- Tekniske feil 35% [1] - Menneskelig svikt 15% [2] - Overbelastning - Strømbrudd 20%	- Tekniske feil - Naturhendelser (ras, storm, is, flom mv.) - Graveskader 25% [3]

[1] Programvarefeil, [2] feil ved planlagt arbeid (oppgradering), [3] fiberbrudd/transmisjonsfeil, basert på alvorlige hendelser fulgt opp av Nkom i perioden 2010-2015.

Dette gjelder for telekommunikasjon generelt, og det er grunn til å tro at hendelsene er landbaserte, siden det har vært få alvorlige hendelser i petroleumssektoren og fordi det ikke er praksis for rapportering av telekom-hendelser til Nkom, som nevnt av DNV GL [37] (jf. tabell 3.4).

Deler av Lysne-utvalgets omtale av petroleumssektoren (olje og gass) var basert på en rapport fra DNV GL [40], som innbefattet en tabell over "topp 10 digitale sårbarheter i petroleumssektoren" vist i tabell 3.6.

Tabell 3.6 Digitale sårbarheter i petroleumsvirksomheten [37, 40]

Scenario nr.	Topp 10 digitale sårbarheter i petroleumsvirksomheten
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

Tabell 3.6 er ikke avgrenset til telekommunikasjon eller ekstern nødkommunikasjon mellom innretning og land, og den har en annen kategorisering (scenarier) enn tabell 3.5.

Vår avgrensning i denne rapporten samsvarer med scenario 7 i tabell 3.6. Samtidig kan flesteparten av de øvrige scenariene være årsaker til sårbarheter og feil i kommunikasjonsforbindelsene mellom innretning og land.

Nkom gir ut årlige rapporter (EkomROS), som inneholder oversikt over hendelser for foregående år. Hendelseskategoriene er noe annerledes enn i tabell 3.5, og det er også en justering fra EkomROS 2019 [41] til EkomROS 2020 [42]. Sistnevnte er nylig utgitt (13.10.2020) og dekker derfor 2019 pluss første halvår 2020. Her benytter man syv kategorier av hendelser, som vist i tabell 3.7.

Tabell 3.7 Hendelseskategorier med forklaring [42]

Kategori	Forklaring
Fiberbrudd	Utfall som følge av brudd på fiberoptiske kabler på land eller i sjø, for eksempel brudd i forbindelse med gravearbeid eller på grunn av slitasje.
Maskinvarefeil	Utfall som følge av fysiske feil i kritiske komponenter, for eksempel feil i nettverkskort eller fysiske skader eller feilkoblinger i forbindelse med planlagt arbeid.
Programvarefeil	Utfall som følge av logiske feil i kritisk programvare, for eksempel feil i brannmurer, feil i forbindelse med programvareoppdateringer eller endringer i databaser, eller andre former for feilkonfigurering.
Ekstern kraft	Utfall som følge av svikt i ekstern kraftforsyning, for eksempel strøm til basestasjoner.
Intern kraft	Utfall knyttet til interne feil i kraftforsyningen, for eksempel svikt i batteribanker, aggregater eller tavler.
Frekvensforstyrrelser	Frekvensforstyrrelser som rammer trådløs kommunikasjon, f.eks. satellittnavigasjons-systemer eller maritim VHF.
Annet	Samlebetegnelse for uønskede hendelser som ikke faller inn under de øvrige kategoriene.

Hendelsesfordelingen for 2019 pluss første halvår 2020 er i tabell 3.8 satt inn i et tilsvarende format som brukt i tabell 3.5 (tilsiktede/utilsiktede hendelser og logiske/fysiske feil). Nkom bruker ikke kategorien "menneskelig svikt" (som kan være rotårsak til flere av de andre kategoriene) og de bruker ikke lenger kategorien "ekstremvær" (som kan være rotårsak til fiberbrudd eller strømbrudd).

Tabell 3.8 Hendelser rapportert til Nkom 01.01.2019 - 31.07.2020 [42]

	Logiske feil		Fysiske feil	
Tilsiktede hendelser	- Frekvensforstyrrelser	11%	- (Fysiske angrep på infrastruktur)	
Utilsiktede hendelser	- Programvarefeil	9%	- Maskinvarefeil	11%
	- Ekstern kraft	14%	- Fiberbrudd	48%
	- Intern kraft	3%		

I tillegg kommer "annet" med 4%.

Nkom bruker heller ikke "fysiske angrep på infrastruktur" som en kategori, men deres fokus er erfarte hendelser og det er ikke sikkert at fysiske angrep på infrastruktur har inntruffet. Som mulig hendelse/risiko er imidlertid kategorien relevant, og vi benytter den i kapittel 3.3 hvor vi ser på både inntrufne og mulige hendelser nevnt under intervjuene.

Det er verdt å merke seg at frekvensforstyrrelsene, foruten å gjelde GPS-forstyrrelser i Øst-Finnmark, gjelder forstyrrelser på maritim VHF kanal 16 for nødkommunikasjon til havs. Hvorvidt også sistnevnte er tilsiktede hendelser, fremgår ikke av rapporten til Nkom.

3.3 Status på sårbarheter og risiko i kommunikasjonsnettverk

I NORSOK T-101:2019 [27] står det i kapittel 6.5.2 *Sårbarhetsvurdering* at *"en sårbarhetsvurdering skal gjennomføres for hvert telekom-system for å identifisere sikringsrisikoer og avhjelpende tiltak"*, og i ekomforskriften § 8-2 *Beredskapsplaner og øvelser m.m.* [30], står det *"tilbyder skal på forespørsel fra Nasjonal kommunikasjonsmyndighet utlevere planer etter første ledd, samt risiko- og sårbarhetsvurderinger som ligger til grunn for planer og tiltak."* Sistnevnte er relevant for teleoperatører (tilbydere).

Ingen av selskapene som ble intervjuet kunne vise til formelle risiko- og sårbarhetsvurderinger av det eksterne kommunikasjonsnettverket, i alle fall kjente de ikke til nyere slike analyser. Noen viste til kontinuerlige (uformelle) risikovurderinger og arbeid med penetreringstesting, kontakt med CERT-er, arbeidsmøter med NSM, innføring av ledelsessystemer for informasjonssikkerhet (iht. ISO/IEC 27001) osv., mens andre selv savnet gode ende-til-ende vurderinger; *"risikoen er å ikke se helheten"*. Selskapene selv bør sørge for at risiko- og sårbarhetsvurderinger utføres, og Ptil (og Nkom) bør påse at dette skjer.[9]

Telekom-systemene er komplekse og integrerte, det er mange leverandører og underleverandører involvert, og det er *"en risiko for ikke å se helheten"*.
Samtidig er ROS-analyser overraskende fraværende.

SINTEF har dermed ikke fått tilgang til risiko- og sårbarhetsanalyser (ROS-analyser) av eksterne kommunikasjonsnettverk. Risiko og sårbarheter er derfor avgrenset til forhold diskutert under intervjuene med selskapene, og forhold omtalt i tidligere studier (jf. kapittel 3.2).

Hendelser som kan lede til utfall, fremkommet under intervjuene, er listet i tabell 3.9 etter samme format som brukt av Lysne-utvalget [3]. Dette omfatter både erfarte og mulige hendelser, men er avgrenset til feil som kan lede til utfall. Dvs. at de dekker tilgjengelighet, men ikke konfidensialitet, integritet eller autentisitet.

Tabell 3.9 Mulige hendelser (sårbarheter/risiko) som kan lede til utfall fremkommet under intervjuene

	Logiske feil	Fysiske feil
Tilsiktede hendelser	- Uautorisert logisk tilgang til kritisk utstyr om bord * - Skadevare i nettverk om bord *	- Uautorisert fysisk tilgang til kritisk utstyr om bord *
Utilsiktede hendelser	- Feil på hovedruter (enkeltfeil) * - Menneskelig feil ved vedlikehold og oppdatering (kople til eller fra feil) * - Bitfeil på radiolinje - Programvarefeil på ombordutstyr * - Feilkonfigurering av brannmurer * - Feil i oppsett eller vedlikehold av VPN-tuneller * - Feil ved ruting via skyløsninger (skytjenestefeil i server) * - Overbelastning grunnet manglende planlegging av båndbredde-bruk * - Interferens (også for radiolinje) - Radioskygge (fra f.eks. fartøy)	- Maskinvarefeil i utvendig utstyr * - Maskinvarefeil i innvendig utstyr * - Fiberbrudd i sjøkabel (overtråling) * - Fiberbrudd i landkabel * - Skade på landinntak - Feil på satellitt * - Strømbrudd (bl.a. grunnet gasslekkasje og andre DFU-er)

Hendelser merket med stjerne (*) i tabell 3.9 er utdypet nedenfor. De er beskrevet i den rekkefølge de er listet i tabell 3.9, ikke etter viktighet.

[9] At myndighetene bør etterse at ROS-analyser gjennomføres for telekomsystemer ble anbefalt av DNV GL [37], men mangelen på risiko- og sårbarhetsvurderinger som er avdekket i vår studie står i sterk kontrast til at samtlige som DNV GL intervjuet svarte bekreftende på at de gjennomførte risikovurderinger som omfatter telekom-systemer.

3.3.1 Tilsiktede hendelser

Uautorisert logisk tilgang til kritisk utstyr om bord

Uautorisert logisk tilgang til kritisk utstyr om bord kan skje enten gjennom eksterne angripere ("hackere") eller av innsidere, som da enten er egne ansatte eller ansatte hos underleverandører. Veien inn vil da være gjennom å skaffe seg fjerntilgang fra land, enten gjennom å misbruke eksisterende tiltrodde tilganger, eller gjennom å prøve å finne sårbarheter som kan gi fjerntilgang utenfor de eksisterende tilgangene.

Tiltrodde fjerntilganger fra land (over VPN) brukes i dag regelmessig av både teleoperatørene og oljeselskapene for å gjennomføre logiske oppdateringer og vedlikehold av rutere, svitsjer og programvare i nettverkene om bord. Slikt vedlikeholdsarbeid utføres enten av egne ansatte i selskapene, eller av deres underleverandører. De ansatte om bord har som regel fått beskjed om å ikke røre teleoperatørene sitt utstyr om bord, men kan unntaksvis bli bedt om å utføre enkle konfigureringsoppgaver, assistert av personell på land (feilsøking og reparasjon gjennom "remote hands").

Tilgang til komponentene i datanettverkene om bord er normalt begrenset til et lite antall personer hos teleoperatørene og/eller deres underleverandører. Alle logiske endringer blir logget og dokumentert i teleoperatørenes vedlikeholdssystemer på land.

Det enkelte er mest bekymret for er angrep av hackere eller innsidere (egne eller underleverandører). Bekymringen retter seg imidlertid hovedsakelig mot risikoen for uautorisert logisk tilgang til prosesskontroll, sikkerhet og støttesystemene (PCSS), ikke til kommunikasjonsnettverket i seg selv. At noen ønsker å "ta ned" eller endre i konfigurasjonen av en eller flere av komponentene som inngår i datanettverkene, med hensikt å forårsake et utfall av eksterne kommunikasjonsnettverk, blir vurdert som mindre sannsynlig.

Skadevare i nettverk om bord

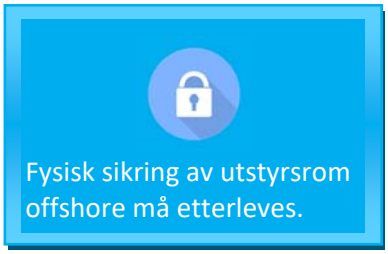
Skadevare i nettverk om bord kan innføres ved tilkobling av minnepinner og PC-er som ikke er blitt scannet i forveien, for eksempel av serviceingeniører som kobler til bærbare PC-er. Under intervjuene ble det fortalt om flere episoder hvor skannere har plukket opp skadevare, og da forhindret hva som ellers kunne blitt et alvorlig virusutbrudd i nettverkene om bord. Noen av selskapene har hatt virussituasjoner (kryptovirus), men dette har ikke påvirket kommunikasjonen.

Skadevare kan i tillegg i teorien plantes via nytt utstyr som blir installert, men sannsynligheten for at dette skjer anses av de intervjuede selskapene som svært lav.

Selskapene ser ut til å ha gode systemer, prosedyrer og rutiner for å forhindre uautorisert logisk tilgang til kritisk utstyr ombord, og det er også rutiner for å hindre skadevare via USB og bærbar PC.

Uautorisert fysisk tilgang til kritisk utstyr om bord

Når det gjelder å forhindre uautorisert fysisk tilgang til kritisk utstyr gjennom avlåste rom og adgangskontroll er det lengre mellom liv og lære. Komponentene i datanettverkene ombord er som regel installert i dedikerte datarom, eller skap, som skal være avlåste. Selskapene har strategier og prosedyrer for dette, men hos enkelte svikter det i etterlevelsen. Det er altfor dårlig fysisk sikring av utstyrsrom offshore hos disse.



3.3.2 Utilsiktede hendelser – logiske feil

Feil på hovedruter

Den største bekymringen til et av selskapene som ble intervjuet var "hovedruteren" til operatøren på innretningen. Det meste av utstyret er redundant, men denne utgjør en "single-point-of failure", dvs. det er tilstrekkelig med én enkelt feil for å sette kommunikasjonsnettverket ut av drift.

Menneskelig feil ved vedlikehold og oppdatering

Enkelte utrykte mest bekymring for menneskelig feil, slik som feil ved til eller frakopling, konfigurasjonsfeil, sende ut feil "template", osv. Nkom bruker ikke dette som en kategori, jf. tabell 3.8, men Lysneutvalget brukte det i sin sammenstilling, jf. tabell 3.5. Her utgjorde menneskelig svikt 15%. I tillegg er nok en stor andel av de fysiske feilene, hvor graveskader dominerer med 25%, relatert til menneskelig svikt. Det er derfor grunn til å tro at menneskelig feil utgjør en betydelig andel av de feil som fører til svikt i ekom-systemene offshore. Det ble bekreftet av flere av selskapene som ble intervjuet at menneskelig feil er en av de vanligste årsakene til utfall av ekstern kommunikasjon.

Bekymring for menneskelig feil og logiske feil (eksempelvis i dynamisk omkopling).

Programvarefeil på ombordutstyr

At programvarefeil kan forårsake utfall av ekstern kommunikasjon ble bekreftet i intervjuene, hvor en av teleoperatørene fortalte om en hendelse hvor en av (de redundante) brannmurene "døde" og det tok en stund før den andre tok over. Et av oljeselskapene nevnte at feil ved programvareoppdatering kan gi feil-konfigurasjon av protokollen for dynamisk omkopling (OSPF – Open Shortest Path First), som er en enkelt-feilmulighet.

En strategi som ble nevnt av en av de intervjuede teleoperatørene for å unngå utfall forårsaket av program-varefeil var at de prøver å holde seg unna siste versjon av oppdateringer og at de lar en leverandør teste ut oppdateringer for dem før de installerer disse.

Feilkonfigurering av brannmurer

Det forekommer korte utfall av komponenter, forårsaket av for eksempel brannmur-problemer, som igjen leder til korte brudd. Brannmurene på plattformer og rigger er dog stort sett statisk konfigurert; det gjøres sjelden oppdateringer av regelsettene og risikoen for logiske feil i disse som forårsaker utfall kan dermed anses mindre enn i landbaserte IT-systemer.

Feil i oppsett eller vedlikehold av VPN-tuneller

Ekstern kommunikasjon kan falle ut hvis sertifikater som brukes til etablering av VPN-tuneller utløper. Dette blir imidlertid ikke sett på som et stort problem, men sees på som en jobb som må gjøres og som selskapene har kontroll på. Overvåking og oppdatering krever imidlertid mye ressurser.

Feil ved ruting via skyløsninger (skytjenestefeil i server)

Et av selskapene uttrykte bekymring for skytjeneste-feil, og viste til et eksempel hvor dette skjedde for et annet selskap på norsk sokkel. Her lå telefonnummerplanen for innretningen på en server i utlandet som feilet.

Overbelastning grunnet manglende planlegging av båndbredde-bruk
Manglende planlegging av båndbreddebruk, dvs. hva som er kritiske krav til båndbredde for ulike applikasjoner. Dersom man trenger 100 Mbit/s og dette faller ut, så vil 4G/LTE kun gi 25 Mbit/s. Et av teleoperatørselskapene har bedt oljeselskap fylle inn krav til båndbredde, men ikke fått tilbakemelding.

3.3.3 Utilsiktede hendelser – fysiske feil

Maskinvarefeil i utvendig og innvendig utstyr
Utilsiktede fysisk feil ble rapportert som den vanligste årsaken til utfall i den norske ekom-infrastrukturen i perioden 01.01.2019-31.07.2020, jfr. tabell 3.8, der 11% av feilene var grunnet maskinvarefeil og 48% grunnet fiberbrudd [42]. At maskinvarefeil forekommer også offshore ble bekreftet i intervjuene, hvor en av teleoperatørene fortalte at dette er en av de vanligste årsakene til nedetid i deres systemer.

Fiberbrudd i sjøkabel og landkabel
Risikoen for brudd på fiberkabel i sjøen har meget lav sannsynlighet, men høy konsekvens. Totalt sett er risikoen for skader på fiberinfrastrukturen i sjøen lavere enn for den landbaserte delen av infrastrukturen.

Feil på satellitt (og reservesamband)
Et selskap har erfart bortfall av satellitt, samtidig som reserve satellitt-telefon ikke virket (ikke blitt testet). De benyttet da alternativ kommunikasjon via båt for å varsle land. Dette resulterte i ettertid i hyppig testing av reserve satellitt-telefon (Inmarsat).

Utilsiktede fysiske feil generelt
Det er SINTEF sitt inntrykk at redundansen av det fysiske utstyret offshore er svært god, og at det er usannsynlig at én utilsiktet fysisk feil vil føre til et totalt bortfall av ekstern kommunikasjon.

3.4 Forslag til forbedringer for å redusere sårbarheter og risiko

Forslag til forbedringer for å redusere sårbarheter og risiko relatert til ekstern kommunikasjon er listet i tabell 3.10.

Tabell 3.10 Sårbarheter og risiko, og forslag til forbedringer

Nr.	Sårbarheter og risiko	Forslag til forbedring
1	Manglende risiko- og sårbarhetsvurderinger av eksterne kommunikasjonsnettverk mellom innretning og land	Selskapene bør sørge for at risiko- og sårbarhets-vurderinger utføres, som innbefatter eksterne kommunikasjonsnettverk mellom innretning og land. Ptil (og Nkom) bør påse at dette gjøres
2	Uautorisert fysisk tilgang til kritisk utstyr ombord	Påse etterlevelse av adgangskontroll gjennom informasjon om krav og viktighet, og oppfølging gjennom tilsyn
3	Mangelfull testing av reserveløsninger	Påse at reserveløsninger for ekstern kommunikasjon vedlikeholdes og testes regelmessig

4 Konsekvensene ved bortfall av kommunikasjonsnettverk

Her er konsekvensene ved bortfall av kommunikasjonsnettverk beskrevet, spesielt hvilken effekt dette kan ha for sikkerheten for den enkelte innretning. Dette inkluderer håndteringen av bortfall av hele eller deler av slike nettverk.

4.1 Krav relatert til bortfall av kommunikasjonsnettverk

Krav relatert til bortfall av kommunikasjonsnettverk er gitt i innretningsforskriften § 18 [35], jf. vedlegg A, og NORSOK T-101:2019 [27], jf. vedlegg C.1. Utdrag av disse er vist i tabell 4.1 og 4.2.

Tabell 4.1 Krav relatert til bortfall av kommunikasjonsnettverk i regelverk [35]

PARAGRAF - TEMA	KRAV
Innretningsforskriften [IF] (med tilhørende veiledning [35])	
§ 18 Systemer for intern og ekstern kommunikasjon (utdrag)	Midlertidig og permanent bemannede innretninger skal utstyres med kommunikasjonssystemer som **til enhver tid gjør det mulig å kommunisere** internt på innretningen, og **mellom innretningen** og skip, luftfartøy **og land**. … Det skal være etablert **minst to uavhengige varslingsveier til land**, fortrinnsvis ved hjelp av faste samband.
Veiledning til § 18 (utdrag)	For å oppfylle kravet til utforming av interne kommunikasjons- og alarmsystemer som nevnt i første ledd, bør følgende standarder brukes: NORSOK S-001, kapittel 18 for allmenngyldige lyd- og lysalarmer, T-001 og T-100 for alarm- og kommunikasjonssystemer … [1)] 1) Merk at NORSOK T-001 og T100 er erstattet av **NORSOK T101:2019 (en)**. Kravet om minst to uavhengige varslingsveier som nevnt i andre ledd, innebærer at **alternative varslingsveier (sekundære) skal være uavhengig av den primære varslingsveien** med hensyn til kraftforsyning og tilgjengelighet under fare- og ulykkessituasjoner, deriblant være motstandsdyktig mot de dimensjonerende etablerte ulykkeslastene i et definert tidsrom. Det bør brukes faste samband som **fiberkabel-, radiolinje- eller satellittsystemer** dersom innretningens posisjon gjør dette mulig. Hvis to uavhengige varslingsveier via faste samband ikke lar seg realisere, kan én av varslingsveiene erstattes med samband i den maritime mobile tjenesten.

Tabell 4.2 Krav relatert til bortfall av kommunikasjonsnettverk i standarder [27]

AVSNITT OG TEMA	KRAV
NORSOK T-101:2019 (en) Telekom systemer [27]	
5.3.6 Hoved-kommunikasjon til land / andre innretninger (utdrag)	Det skal **minimum** være **to uavhengige faste kommunikasjonsforbindelser til** driftssenteret på **land**, enten direkte eller via andre faste innretninger. Kommunikasjons-forbindelsene skal være designet for høy pålitelighet og høy kapasitet for å tillate nødkommunikasjon, daglig drift og integrerte operasjoner. Aktuelle systemer er: – Fiberoptisk kabel; – Radioforbindelse; – Satellittforbindelse; – 4G/LTE. … I tillegg til permanente kommunikasjonsforbindelser kan oppkoblede satellitt-tjenester benyttes for back-up. …

Regelverket (IF § 18 [35]) åpner for at én av varslingsveiene ikke går via fast samband, men kan erstattes med samband i den maritime mobile tjenesten, mens NORSOK T-101:2019 [27] ikke gir en tilsvarende åpning, men kun godtar oppkoplet satellitt-tjeneste som back-up. Denne forskjellen mellom regelverkskravet og kravet i NORSOK bør ses nærmere på. På den annen side så nevner NORSOK T-101:2019 4G/LTE som et aktuelt system, noe IF § 18 ikke gjør. Vi kommer tilbake til dette i kapittel 5.

NORSOK T-101:2019 [27] stiller også krav til pålitelighet (avsnitt 6.4), som følger: *"… For å unngå totaltap av funksjon for et telekommunikasjonssystem gjelder følgende:*

- *Nødkommunikasjonssystemer (jf. avsnitt 5.3.2) eller kritiske moduler i disse systemene skal være redundante; …*
- *Avbruddssikker kraftforsyning (UPS) skal distribueres dobbel-redundant. …".*

En enkeltfeil skal normalt ikke kunne gi bortfall av nødkommunikasjonsfunksjonen (to eller flere uavhengige varslingsveier).

Dersom nødkommunikasjonssystemer eller deler av disse er ute av drift skal dette varsles jf. avsnitt 6.13 (Generelle funksjonskrav); underavsnitt 6.13.4 (Alarmgrensesnitt): *"… Kritisk alarm: Store deler av nødkommunikasjonssystemene ute av drift. … Kritiske alarmer skal også være fast koplet ("hardwired") direkte fra alle nødkommunikasjonssystemer til SAS for visning i SKR. …".*

Et varsel om bortfall, gitt at det oppdages, er en forutsetning for videre håndtering av bortfallet.

4.2 Konsekvenser av bortfall av kommunikasjonsnettverk fra tidligere studier

Ptil [36] og DNV GL [37] omhandler kommunikasjonsnettverk generelt, inkludert ekstern kommunikasjon ved nødsituasjoner. DNV GL dekker også i noen grad konsekvenser ved bortfall/utfall av kommunikasjons-nettverk, ved at de har spurt enkelte bedrifter om hvor lenge en installasjon kan fortsette å operere dersom telekommunikasjonsløsningene blir satt ut av drift. De oppsummerer med at *"for noen installasjoner betyr et slikt utfall at produksjonen må stenges ned, andre har alternative løsninger og vil kunne fortsette driften en stund."* Med utfall her menes totalutfall på fibernettet, jf. *"avhengigheten til kontinuerlig operative fiber-forbindelser og mangel på høykapasitets alternativer, gjør at noen installasjoner må stenge ned dersom det skjer et totalutfall på fibernettet"* [37].

Det er ikke nærmere beskrevet hva som er tilstrekkelig gode alternative løsninger til at driften kan fortsette, og heller ikke hvor lenge driften kan fortsette.

Bortfall av fibernettet fra et felt og til land som følge av sabotasje er et av scenariene i en sikringsrisiko-analyse [Fortrolig]. Innretningen har i tillegg til fiberkabel (tilkopling til Tampnet sitt nettverk) radio-forbindelse til en naboinnretning (tilsvarende innretning B i figur 2.2). I denne analysen vurderes det som trygt å fortsette produksjonen så lenge radioforbindelsen til naboinnretningen er intakt, men at dette ikke er en løsning som er akseptabel i mer enn en "kort periode", f.eks. noen få dager, og etter hvert vil produksjonen måtte stenges ned. Dersom radioforbindelsen til naboinnretningen ikke er tilgjengelig vil produksjonen "sannsynligvis" stenges ned.

Her er radioforbindelsen vurdert som en alternativ løsning, men hvor lenge man kan fortsette driften er noe omtrentlig. Det er heller ikke konkludert med at konsekvensen av bortfall av all kommunikasjon er umiddelbar nedstenging av produksjonen, kun at nedstengning er "sannsynlig". Det er ikke gjort noen vurdering opp mot kravet til to uavhengige kommunikasjonsforbindelser (jf. IF §18 [35] og NORSOK T-101:2019 [27]).

"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".

DNV GL, 2020 [37]

Videre har DNV GL avdekket at *"utfall av slike tele-kommunikasjonsløsninger blir ikke testet og øvd på, da man er bekymret for de konsekvensene en total nedstengning av installasjonen vil kunne få"* [37]. Ptil [36] er inne på det samme, men inkluderer også delvis bortfall: *"Det stilles spørsmål til om man øver tilstrekkelig på situasjoner der ulike sambandsløsninger av ulike årsaker ikke er tilgjengelig. I tillegg til ulykkescenarioer der utstyr kan feile eller bli ødelagt, vil man også i varierende grad koble ut utstyr, helt eller delvis ved gassdeteksjon og ESD. Man vil i noen situasjoner være avhengig av overbroinger og man kan forvente at noen kommunikasjonssystemer ikke er tilgjengelig eller har redusert funksjonalitet ved gitte definerte fare- og ulykkessituasjoner."*

I tillegg til konsekvenser for enkeltinnretninger peker DNV GL [37] også på konsekvenser av et sentralt bortfall/utfall av fibernettet til Tampnet: *"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."* [10]

4.3 Status på konsekvenser og håndtering av bortfall av kommunikasjonsnettverk

Vurderingen av konsekvenser av bortfall av eksterne kommunikasjonsnettverk spriker veldig mellom selskapene som ble intervjuet. Et av selskapene mener at de i en slik situasjon vil reagere proaktivt og stenge ned, enten man har mistet all ekstern kommunikasjon eller har én ekstern kommunikasjonsforbindelse som fungerer. Dermed går de til en sikker tilstand. Et annet selskap mener at det ikke har noen umiddelbare konsekvenser og at det vil være opp til ledelsen om bord å avgjøre om man skal stenge ned. Operasjoner som krever assistanse fra land vil stoppe opp. Et tredje selskap ser ingen konsekvenser og vil fortsette å produsere som før. Dette gjelder altså uavhengig av om det er totalt eller kun delvis bortfall av ekstern kommunikasjon.

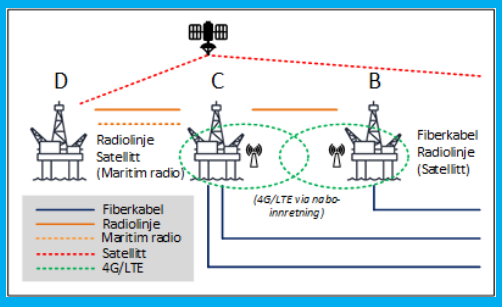
To av selskapene ble spurt om bortfall av nødkommunikasjonssystemer varsles med alarm i kontrollrom. Det ene selskapet svarte at de ikke har alarm for dette, mens det andre var usikker på om dette vises i kontroll-rommet (men at de fort vil oppdage det dersom kommunikasjonen er nede). NORSOK T-101:2019 [27] krever slike alarmer, jf. kapittel 4.1.

Når det gjelder håndtering av bortfall av eksterne kommunikasjonsnettverk viser selskapene til at dette håndteres av teleoperatørene, som Tampnet og Telenor Maritime, gjennom serviceavtaler (SLA), og at disse igjen benytter underleverandører som ACMA (Atlantic Cable Maintenance & Repair Agreement) for utbedring av skader. Normalt er det tilstrekkelig å rute om trafikken på grunn av stor grad av redundans og fleksibilitet. Det meste løses fjernstyrt og ved å sende utstyr ut til innretningen. Større bortfall, som kabelbrudd, skjer sjelden. På norsk sektor har det kun vært kabelbrudd én gang siden 1999. Det er størst problem med kabelbrudd i landnettet, noe tallene fra Nkom [42] viser, jf. kapittel 3.2.

[10] Uttesting av reserveløsninger ("fail-over" testing) gjøres imidlertid for enkeltinnretninger. Dette kom frem under intervjuene.

4.4 Forslag til forbedringer for å redusere konsekvenser av bortfall

Noen nærliggende innretninger har felles kommunikasjonsnettverk, slik som radiolinjeforbindelse mellom to innretninger (jf. kapittel 2.4), hvor det kan være at den ene av innretningene er mer avhengig av denne forbindelsen enn den andre innretningen. Her vil det være viktig med samordning og kommunikasjon, både så raskt som mulig etter at en feil har inntruffet, og ved planlagt utkopling.



Strømutkopling og strømbrudd er vanlige årsaker til utfall av telekomsystemer. Dette bør varsles raskt til berørte nabo-innretninger og teleoperatører.

Øvelser på bortfall av ekstern kommunikasjon bør også inkludere gjensidig avhengige naboinnretninger.

Strømutkopling og strømbrudd (feil) er vanlige årsaker til utfall av kommunikasjonssystemer. Dette bør varsles raskt til berørte naboinnretninger og til berørte teleoperatører. Det kom frem under intervjuene at teleoperatører oppdager utfall og starter feilsøking, men senere får vite av operatøren at utfallet skyldtes et strømbrudd.

Både Ptil [36] og DNV GL [37] peker på at det ikke øves, eller øves tilstrekkelig, på bortfall av kommunikasjonsnettverk (jf. kapittel 4.2), blant annet fordi man er bekymret for konsekvensene av dette. Som nevnt i kapittel 2.5, så egner bortfall av kommunikasjonsnettverk seg for skrivebordsøvelser, enten man har definert dette som en DFU eller ikke. Da unngår man eventuelle konsekvenser av en reell utkopling av kommunikasjonsnettverk. Øvelsene bør omfatte både enkeltinnretninger, gjensidig avhengige naboinnretninger, alle områderessurser, og ekstremtilfellet som DNV GL tar opp med et sentralt utfall av nettet som fører til at mye av petroleumsvirksomheten i Nordsjøen stopper opp.

I tidligere studier og analyser, jf. kap. 4.2, og også i intervjuene, jf. kap. 4.3, ble det i vurderingene av konsekvensene av bortfall av ekstern kommunikasjon ikke gjort noen vurdering opp mot kravet til minst to uavhengige varslingsveier til land, jf. IF §18 [35]. Dette gjaldt uavhengig av om det var snakk om totalt eller delvis bortfall av ekstern kommunikasjon. Det ser ut til å være uklart hvordan kravet skal fortolkes.

Skal det være minst to uavhengige veier både *før* og *etter* en DFU? Eller er det krav om minst to uavhengige veier kun *før* en DFU, og at det gjennom uavhengighet sikres at minst én vei er tilgjengelig også etter en DFU? I veiledningen til IF § 18, jf. tabell 4.1, står det bl.a. at *"alternative varslingsveier (sekundære) skal … være motstandsdyktig mot de dimensjonerende etablerte ulykkeslastene i et definert tidsrom."* Gjelder dette også for den primære varslingsveien?

Kravet er klart i forhold til at det skal være minst to uavhengige varslingsveier til land *før* en DFU, dvs. "til enhver tid (?)" under normal drift, men hvordan skal kravet fortolkes når en eller flere varslingsveier bortfaller? Dersom man har (definert) to uavhengige varslingsveier med faste samband, og en av disse bortfaller, skal dette da avviksbehandles? Krever det nedstengning? Hva om begge bortfaller? Dersom man har reserveløsninger, eksempelvis samband i den maritime mobile tjeneste, som ikke har vært definert som én av de uavhengige varslingsveiene, kan man da etter bortfall av de definerte uavhengige varslingsveiene basere seg på ("regne inn") reserveløsningene? Anses det som forsvarlig å fortsette driften som normalt dersom man kun baserer seg på reserveløsninger?

Ptil bør vurdere å utdype dette i veiledning til IF § 18 *Systemer for intern og ekstern kommunikasjon* eller i en egen fortolkning til denne paragrafen.

5 Regelverk og standarder – utfordringer og forslag til forbedringer

Her er utfordringer knyttet til regelverk og standarder med hensyn til kommunikasjonsnettverk for ekstern kommunikasjon identifisert og forbedringer foreslått. Trender i forhold til teknologiutvikling og utviklingen i aktørbildet er inkludert, men dagens løsninger er vektlagt. Dagens løsninger inkluderer tradisjonelle kommunikasjonssystemer, men i stadig økende grad benyttes integrerte og komplekse systemer.

5.1 Generelle utfordringer

Dette dekker generelle utfordringer ved dagens regelverk og standarder knyttet til IKT-sikkerhet for eksterne kommunikasjonsnettverk. Noen av synspunktene fra selskapene under intervjuene retter seg mot krav til kommunikasjonsnettverk i regelverk og standarder, uten at man ser spesifikt på IKT-sikkerhet, mens andre synspunkter gjelder IKT-sikkerhet.

Flere gir uttrykk for at regelverket henger etter teknologien og at det er tungt å få gjort endringer - regelverket bør ikke være hemmende. Det har blant annet vært en eksplosjon i båndbredde-bruk, hvor regelverket ikke har hengt med, mens det er teknologi i regelverket som ikke lenger er relevant, slik som fysiske skiller. Det gis også uttrykk for at regelverket, når det gjelder IKT-sikkerhet, ikke kommuniserer godt nok på en felles plattform, men er fragmentert.

En utfordring for både regelverk og standarder er å holde de oppdatert. Som nevnt i kapittel 2.2, 3.1 og 4.1, så er NORSOK-standardene for telekom oppdatert i 2019, uten at henvisningene i regelverket er oppdatert. Det er også uheldig at det har tatt ni år (fra 2010-2019) å oppdatere NORSOK-standardene for telekom, som er et område hvor utviklingen går svært raskt. Dette ble under intervjuene vurdert som alt for lang tid.

NEK IEC 62443
En bærebjelke for cybersikkerhet

"Det primære formålet med IEC 62443-serien av standarder er å inkludere OT-systemene i arbeidet med cyber-sikkerhet.

Standardserien er utarbeidet av IEC Technical Committee (TC) 65: Måling, kontroll og automatisering av industrielle prosesser, i samarbeid med medlemmer av Committee 99 of the International Society of Automation (ISA99).

I Norge er det NEK NK 65 som behandler, kommenterer og voterer på standardserien IEC 62443."

www.nek.no [46]

Et tema som ble tatt opp med oljeselskapene under intervjuene er regelverkets henvisning (eller mangel på henvisning) til IKT-sikkerhetsstandarder. Som vist i faktaboksen i kapittel 2.2, så viser NORSOK T-101:2019 [27] (som erstatter NORSOK T-001:2010 [24] og NORSOK T-100:2010 [25]) til DNVGL-RP-G108 [43], NOG 104 [39], NEK IEC 27001 [44] og NEK IEC 27002 [45]. DNVGL-RP-G108 er en retningslinje for anvendelse av IEC 62443 [46], som av en eller annen grunn ikke er henvist til i NORSOK T-101:2019.

Oljeselskapene trekker en parallell til at man på sikkerhetssiden ("safety") i regelverket henviser til IEC 61508/61511 [47, 48] (med flere) og "tilhørende" retningslinje nr. 70 til Norsk olje og gass (NOROG 070) [49], og mener at man i regelverket bør henvise til IEC 62443 og en tilhørende retningslinje, slik som DNVGL-RP-G108. IEC 62443 blir av mange sett på som komplisert, og bør derfor følges av en retningslinje.

Det er mange utfordringer med dette, slik SINTEF ser det. Et spørsmål er hvor man skal ha en slik henvisning i regelverket. IEC 62443 er rettet mot IACS (industrielle kontroll- og automatiseringssystemer), og er det da naturlig å spre henvisninger til IEC 62443 fra ulike relevante systemer i innretningsforskriften [35], slik som § 18 *Systemer for intern og ekstern kommunikasjon*? IEC 62443 ligger nærmere opp mot de

instrumenterte sikkerhetssystemene (SIS), slik også IEC 61508/61511 gjør. De sistnevnte henvises ikke til i innretningsforskriften, men fra styringsforskriften § 5 *Barrierer* (veiledningen) [17]. Dette kan av flere grunner være et riktigere sted å henvise til IEC 62443, bl.a. fordi Lysneutvalget i NOU 2015: 13 [3], som var bakgrunnen for Ptils satsing på IKT-sikkerhet, viser til at det har vært økende oppmerksomhet rundt barrierer som hindrer en uønsket hendelse, og at *"utvalget mener at bransjen bør videreutvikle den gode sikkerhets-tradisjonen innen HMS, og overføre denne tradisjonen til det digitale området"*.

En annen utfordring er at regelverket ikke kan henvise til standarder som ikke er i endelig utgave. Deler av IEC 62443 er utgitt (9 av 14 deler), mens andre deler er under utarbeidelse. (Selskapene kan uansett stille krav i henhold til IEC 62443 i kontrakter, selv om den ikke henvises til i regelverk eller standarder).

En tredje utfordring, eller i alle fall en forskjell fra IEC 61508/61511 og NOROG 070, er at DNV GL (utgiver av DNVGL-RP-G108) er en kommersiell aktør. Bør retningslinjen utgis i regi av eksempelvis Norsk olje og gass eller NORSOK? Uansett hvilken modell man velger, så er det viktig at retningslinjen oppdateres regelmessig.

5.2 Utfordringer og forslag til forbedringer

Dette dekker spesielle utfordringer ved dagens regelverk og standarder knyttet til IKT-sikkerhet for eksterne kommunikasjonsnettverk, samt innspill til forbedringer/endringer. Utfordringer og innspill *som kom frem under intervjuene*, inkludert trender som kan påvirke regelverk og/eller standarder er listet i tabell 5.1.

Tabell 5.1 Utfordringer, trender og innspill til endringer i regelverk og/eller standarder

Nr.	Utfordring	Innspill under intervju
1	At 4G/LTE ikke nevnes som uavhengig varslingsvei i IF § 18 på linje med fiber, radiolinje og satellitt (slik det gjør i NORSOK T-101:2019). Forutsetter at 4G/LTE blir Ex-godkjent	Inkludere 4G/LTE som uavhengig varslingsvei i IF § 18 på linje med fiber, radiolinje og satellitt (slik det gjør i NORSOK T-101:2019), og stille krav til at 4G/LTE skal være Ex-godkjent, og dermed kunne brukes f.eks. under en inntruffet gasslekkasje
2	NOG 104 blir veldig generell. Lett å omgå ved budsjett-innsparinger, spesielt når det står "bør" i stedet for "skal". Lettere å argumentere for budsjett der hvor det henvises (med "skal") til mer spesifikke krav. IKT-sikkerhet er et vanskelig "business case". Sjøfart har ingen alternativ til NOG 104, men operatørene kan i kontrakt stille krav til NORSOK, osv.	Dersom det er en underliggende forventning fra Ptil om at "bør" betyr at man må dokumentere at et alternativ er minst like bra, så burde dette kommet tydeligere frem. Ptil kunne vist til at NOG 104 ikke nødvendigvis er dekkende, og at NORSOK-standarder kunne hjulpet mye *Se faktaboks under.*
3	Sammenhengen mellom sjøfart sine IMO og SOLAS krav, f.eks. til GMDSS, og Ptil sine krav (og NORSOK) kan være forvirrende	Tydeliggjøre sammenhengen mellom sjøfart sine IMO og SOLAS krav, og Ptil sine krav (og NORSOK)
	Utfordring/trend	**Innspill under intervju**
4	Økt bruk av IoT, som igjen støttes av 4G/LTE (og etter hvert 5G). Dette vil gi besparelser i mange tonn med kabel. Spesielt for gamle innretninger er det svært dyrt med ny kabling	-
5	Utvikling av "Carrier-grade" modem, i stedet for "Enterprise-grade"	Kan da i regelverk/standarder stille krav om "Carrier-grade". Selv om man har redundante modem, er dette viktig
6	Økt innføring av "roaming" og dermed tilgjengelighet	-

	for mobiltelefoner (firma og privat)	
7	Økt ønske om fjerntilgang til OT, som i gitte tilfeller kan avhjelpe en situasjon	Sikre at slik tilgang ikke kan misbrukes
8	Aktørbildet har endret seg ved at det tidligere var et tydelig skille mellom boreoperatør og kunde. Dette er nå mer uklart, og mange av kundens tidligere leverandører nærmer seg oss [teleoperatører]. Spesielt i forbindelse med mer fjernoperering	-
9	5G er mulig erstatning for Wifi. Økte behov som f.eks. bruk av hjelmkamera uten å måtte ha veldig mange aksesspunkter (kunne trenge igjennom stål)	-

Veiledninger

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

Veiledningene viser på enkelte områder til industristandarder, som en anbefalt måte å oppfylle forskriftens krav på. Veiledningene til forskriftene er ikke rettslig bindende, og aktørene kan derfor velge andre løsninger.

Dersom den ansvarlige aktøren velger å benytte den anbefalte løsningen, kan det normalt legges til grunn at forskriftenes krav er oppfylt. Hvis aktøren velger andre løsninger, som for eksempel andre standarder eller selskapsspesifikke prosedyrer, må de kunne dokumentere at den valgte løsningen er minst like god som, eller bedre enn, den anbefalte.

Les mer om dette regelverksprinsippet i rammeforskriften § 24 om bruk av anerkjente normer med veiledning."

www.ptil.no [51]

Rammeforskriften § 24 [50]:

I veiledningene til de utfyllende forskriftene brukes begrepene *bør og kan* når det henvises til anbefalte løsninger for å oppfylle forskriftens krav. I den sammenhengen menes følgende med disse begrepene.

Bør, betyr myndighetenes anbefalte måte å oppfylle funksjonskravet på. Alternative løsninger med dokumentert likeverdig funksjonalitet og kvalitet kan nyttes uten at dette må forelegges for myndighetene.

Kan, betyr en alternativ, likeverdig måte å oppfylle forskriftens krav, eksempelvis der det i veiledningen anbefales å bruke maritime normer som et alternativ til å følge en NORSOK-standard.

Spesifikke forslag til endringer diskutert i kapittel 2-4 er listet i tabell 5.2.

Tabell 5.2 Spesifikke forslag til endringer i regelverk og standarder

Nr.	Utfordring	Forslag
1	Det representative utvalget av DFU-er som inngår i beredskapsplanen kan bli for statisk i forhold til både teknologiutvikling og trusselbilde	Utdype, eksempelvis i veiledningen til aktivitets-forskriften § 73 Beredskapsetablering, at det representative utvalget av DFU-er bør gjenspeile situasjonen til enhver tid
2	I veiledning til IF § 18 står det: "*For å oppfylle kravet til utforming av interne kommunikasjons- og alarmsystemer som nevnt i første ledd, bør følgende standarder brukes: NORSOK S-001, kapittel 18 for*	Inkludere ekstern kommunikasjon i forskriftsteksten, både når det gjelder henvisning til NORSOK S-001 og NORSOK-standarder for telekom systemer

	allmenngyldige lyd- og lysalarmer, T-001 og T-100 for alarm- og kommunikasjonssystemer …" Dette dekker ikke ekstern kommunikasjon mellom innretningen og land	
3	NORSOK T-001:2010 og NORSOK T-100:2010 er utgått og erstattet av NORSOK T-101:2019	Erstatte henvisningen til de utgåtte NORSOK-standardene med NORSOK T-101:2019
4	Ny NORSOK-standard T-003:2019 for telekom systemer for flyttbare offshore installasjoner er ikke henvist til i regelverket	Vurdere å henvise til NORSOK T-003:2019 i regelverket
5	Veiledning til IF § 18 og NORSOK T-101:2019 (kap. 5.3.6) avviker med hensyn til kravet til minst to uavhengige varslingsveier til land. Veiledning til IF § 18 nevner ikke 4G/LTE, mens NORSOK T-101:2019 gjør det, og veiledning til IF §18 aksepterer at én av varslingsveiene erstattes med samband i den maritime tjenesten, mens NORSOK T-101:2019 kun aksepterer oppkoplet satellitt-tjeneste som back-up	Veiledning til IF § 18 og NORSOK T-101:2019 bør avstemmes. 4G/LTE kan inngå begge steder dersom man går via basestasjon på naboinnretning. Videre bør aksept av alternativ varslingsvei være lik begge steder, enten samband i den maritime tjenesten eller kun satellittforbindelse
6	IEC 62443, og en tilhørende retningslinje, er ikke henvist direkte til i regelverket.	Vurdere å inkludere (endelige deler av) IEC 62443, og en eventuell tilhørende retningslinje, direkte i veiledningen til Styringsforskriften § 5 Barrierer, på lik linje med IEC 61508/61511 og NOROG 070
7	NORSOK T-101:2019 (kap. 6.5.1) viser kun til DNVGL-RP-G108 direkte uten å vise til (endelige deler av) IEC 62443	Dersom DNVGL-RP-G108 anses som relevant å henvise til spesifikt for telekom systemer, dvs. dersom man ikke lager en felles standard for IKT-sikkerhet for alle relevante systemer, så bør også IEC 62443 henvises til i NORSOK T-101:2019 (kap. 6.5.1)
8	NORSOK T-003:2019 (kap. 8.1) henviser kun til NOG 104, og viser til at den skal følges, mens NORSOK T-101:2019 (kap. 6.5.1) viser til DNVGL-RP-G108, NOG 104, NEK IEC 27001 og NEK IEC 27002, og viser til at man her kan finne anbefalinger til beste praksis (ikke at de skal følges)	Samordne henvisningene til IKT-standarder og retningslinjer i de to NORSOK-standardene for telekom systemer
9	NORSOK T-003:2019 (kap. 8.2) spesifiserer krav til IKT-sikkerhet mer detaljert enn NORSOK T-101:2019 (kap. 6.5.2), eksempelvis viser sistnevnte til at fjerntilgang skal adresseres i sårbarhetsvurderingen, mens NORSOK T-003:2019 viser til at fjerntilgang skal begrenses til godkjente brukere og at all aktivitet skal logges	Samordne kravene til IKT-sikkerhet i de to NORSOK-standardene for telekom systemer, blant annet med hensyn til detaljeringsnivå[11]
10	NORSOK T-003:2019 refererer til NORSOK T-101:2019, men ikke motsatt	De to NORSOK-standardene for telekom systemer bør kryss-referere til hverandre
11	Fortolking av kravet om to uavhengige varslingsveier til land i IF § 18	Utdype hvordan kravet skal forstås ved bortfall, enten i veiledning til IF § 18 eller i fortolkning til IF § 18

[11] DNV GL mener at NORSOK T-101:2019 [27] ikke inneholder konkrete krav til IKT-sikkerhet, og at det burde etableres en NORSOK IKT-sikkerhetsstandard som også gjelder for telekom [37]. Dette peker mot at en samordning, dersom man ikke etablerer en egen IKT-sikkerhetsstandard, går i retning av de detaljerte kravene i NORSOK T-003:2019 [28]. Dette kan inkludere anbefaling til standard for sårbarhetsvurderinger, som DNV GL også etterlyser.

6 Anbefalinger

I dette kapitlet oppsummeres SINTEFs anbefalinger til tiltak for næringen og Petroleumstilsynet, samt behov for videre arbeid med kunnskapsinnhenting. Anbefalingene er hentet fra forslag i kapittel 2-5, og allokert til henholdsvis næringen og Petroleumstilsynet.

6.1 Næringen

Anbefalinger til tiltak for næringen er gitt i tabell 6.1.

Tabell 6.1 Oppsummering av SINTEFs anbefalinger til tiltak for næringen

Nr.	Utfordring	Anbefaling
1	Tilstrekkelig forståelse av betydningen av bortfall av ekstern kommunikasjon	Definere tap av ekstern kommunikasjon som en DFU (eventuelt også intern nødkommunikasjon)
2	(Som over)	Alternativt kan tap av ekstern (og eventuelt intern) nødkommunikasjon inngå i aksjonsplanene i beredskapsplanen som spesielle utfordringer (eskalering) for andre DFU-er
3	(Som over)	Et tredje alternativ er å definere en DFU som dekker flere sikkerhetssystemer ("sikkerhetssystemer midlertidig ute av drift"), hvor nødkommunikasjons-systemene inngår
4	Vite hvordan man skal håndtere bortfall av ekstern kommunikasjon (på den enkelte innretning) – øve tilstrekkelig	Øve på "tap av ekstern kommunikasjon" enten det er definert som en DFU eller ikke. Kan alternativt gjennomføres som skrivebordsøvelse
5	Vite hvordan man skal samhandle ved bortfall av ekstern kommunikasjon når det rammer mer enn en enkelt innretning – øve tilstrekkelig	Øvelsene bør også innbefatte gjensidig avhengige naboinnretninger, alle områderessurser, og ekstremtilfellet med et sentralt utfall av nettet som fører til at mye av petroleumsvirksomheten i Nordsjøen stopper opp
6	Nødvendig oppmerksomhet og oppfølging av alt telekom-utstyr som inngår i nødkommunikasjon	Sikre at alt telekom-utstyr som inngår i ekstern nødkommunikasjon defineres som barriereelementer
7	Tilstrekkelig oppmerksomhet og oppfølging av telekom-utstyr for ekstern kommunikasjon som ikke inngår i operatørenes barriere- og vedlikeholdsstyring	Sørge for god oppfølging av telekom-utstyr for ekstern kommunikasjon som ikke inngår i operatørenes barriere- og vedlikeholdsstyring, men som driftes og vedlikeholdes av teleoperatører
8	Manglende risiko- og sårbarhetsvurderinger av eksterne kommunikasjonsnettverk mellom innretning og land	Selskapene bør sørge for at risiko- og sårbarhets-vurderinger utføres, som innbefatter eksterne kommunikasjonsnettverk mellom innretning og land
9	Uautorisert fysisk tilgang til kritisk utstyr ombord	Påse etterlevelse av adgangskontroll gjennom informasjon om krav og viktighet, og oppfølging gjennom tilsyn
10	Mangelfull testing av reserveløsninger	Påse at reserveløsninger for ekstern kommunikasjon vedlikeholdes og testes regelmessig
11	Samordning og kommunikasjon så raskt som mulig etter at en feil har inntruffet, og ved planlagt utkopling. (Strømutkopling eller strømbrudd er vanlige årsaker til utfall av kommunikasjonssystemer)	Etablere rutiner for rask varsling til berørte nabo-innretninger og til berørte teleoperatører ved feil, og ved planlagt utkopling av kommunikasjonssystemer

12	NORSOK T-101:2019 (kap. 6.5.1) viser kun til DNVGL-RP-G108 direkte uten å vise til (endelige deler av) IEC 62443	Dersom DNVGL-RP-G108 anses som relevant å henvise til spesifikt for telekom systemer, dvs. dersom man ikke lager en felles standard for IKT-sikkerhet for alle relevante systemer, så bør også IEC 62443 henvises til i NORSOK T-101:2019 (kap. 6.5.1)
13	NORSOK T-003:2019 (kap. 8.1) henviser kun til NOG 104, og viser til at den skal følges, mens NORSOK T-101:2019 (kap. 6.5.1) viser til DNVGL-RP-G108, NOG 104, NEK IEC 27001 og NEK IEC 27002, og viser til at man her kan finne anbefalinger til beste praksis (ikke at de skal følges)	Samordne henvisningene til IKT-standarder og retningslinjer i de to NORSOK-standardene for telekom systemer
14	NORSOK T-003:2019 (kap. 8.2) spesifiserer krav til IKT-sikkerhet mer detaljert enn NORSOK T-101:2019 (kap. 6.5.2), eksempelvis viser sistnevnte til at fjerntilgang skal adresseres i sårbarhetsvurderingen, mens NORSOK T-003:2019 viser til at fjerntilgang skal begrenses til godkjente brukere og at all aktivitet skal logges	Samordne kravene til IKT-sikkerhet i de to NORSOK-standardene for telekom systemer, blant annet med hensyn til detaljeringsnivå
15	NORSOK T-003:2019 refererer til NORSOK T-101:2019, men ikke motsatt	De to NORSOK-standardene for telekom systemer bør kryss-referere til hverandre

6.2 Ptil

Anbefalinger til tiltak for Petroleumstilsynet er gitt i tabell 6.2.

Tabell 6.1 Oppsummering av SINTEFs anbefalinger til tiltak for Petroleumstilsynet

Nr.	Utfordring	Anbefaling
1	Det representative utvalget av DFU-er som inngår i beredskapsplanen kan bli for statisk i forhold til både teknologiutvikling og trusselbilde	Utdype, eksempelvis i veiledningen til aktivitets-forskriften § 73 Beredskapsetablering, at det representative utvalget av DFU-er bør gjenspeile situasjonen til enhver tid
2	Manglende risiko- og sårbarhetsvurderinger av eksterne kommunikasjonsnettverk mellom innretning og land	Ptil bør påse at selskapene utfører risiko- og sårbarhetsvurderinger, som innbefatter eksterne kommunikasjonsnettverk mellom innretning og land
3	I veiledning til IF § 18 står det: "*For å oppfylle kravet til utforming av interne kommunikasjons- og alarmsystemer som nevnt i første ledd, bør følgende standarder brukes: NORSOK S-001, kapittel 18 for allmenngyldige lyd- og lysalarmer, T-001 og T-100 for alarm- og kommunikasjonssystemer …*" Dette dekker ikke ekstern kommunikasjon mellom innretningen og land	Inkludere ekstern kommunikasjon i forskriftsteksten, både når det gjelder henvisning til NORSOK S-001 og NORSOK-standarder for telekom systemer
4	NORSOK T-001:2010 og NORSOK T-100:2010 er utgått og erstattet av NORSOK T-101:2019	Erstatte henvisningen til de utgåtte NORSOK-standardene med NORSOK T-101:2019
5	Ny NORSOK-standard T-003:2019 for telekom systemer for flyttbare offshore installasjoner er ikke henvist til i regelverket	Vurdere å henvise til NORSOK T-003:2019 i regelverket

6	Veiledning til IF § 18 og NORSOK T-101:2019 (kap. 5.3.6) avviker med hensyn til kravet til minst to uavhengige varslingsveier til land. Veiledning til IF § 18 nevner ikke 4G/LTE, mens NORSOK T-101:2019 gjør det, og veiledning til IF §18 aksepterer at én av varslingsveiene erstattes med samband i den maritime tjenesten, mens NORSOK T-101:2019 kun aksepterer oppkoplet satellitt-tjeneste som back-up	Veiledning til IF § 18 og NORSOK T-101:2019 bør avstemmes
7	IEC 62443, og en tilhørende retningslinje, er ikke henvist direkte til i regelverket.	Vurdere å inkludere (endelige deler av) IEC 62443, og en eventuell tilhørende retningslinje, direkte i veiledningen til Styringsforskriften § 5 Barrierer, på lik linje med IEC 61508/61511 og NOROG 070
8	Fortolking av kravet om to uavhengige varslingsveier til land i IF § 18	Utdype hvordan kravet skal forstås ved bortfall, enten i veiledning til IF § 18 eller i fortolkning til IF § 18
-	Innspill gitt under intervju	Se tabell 5.1

6.3 Behov for kunnskapsinnhenting

Formålet med denne rapporten har vært å gi næringen økt forståelse av rollen til og sårbarheten av kommunikasjonsnettverk, spesielt i beredskapssituasjoner når en definert fare- og ulykkessituasjon (DFU) har inntruffet. Dette er videre utdypet, gjennom spesifikke målsettinger, til å dekke ekstern nød-kommunikasjon mellom innretning og land.

Vi opplever at en av de største utfordringene er å ha oversikt over helheten, dvs. kommunikasjonen ende-til-ende fra varslingsansvarlig, kontrollromsoperatør eller beredskapsledelse til hovedredningssentral, 2. linje beredskap, osv., både med hensyn til telekommunikasjonsutstyret og aktørene som inngår. Dette forsterkes av manglende risiko- og sårbarhetsvurderinger. Disse ville i seg selv bidratt til å få bedre oversikt over systemer, utstyr og aktører som inngår.

Vi har gitt anbefalinger om at risiko- og sårbarhetsvurderinger som innbefatter eksterne kommunikasjons-nettverk mellom innretning og land blir utført av selskapene og fulgt opp av myndighetene, men parallelt med dette er det behov for å innhente mer kunnskap om kommunikasjonen ende-til-ende. Dette gjelder spesielt der hvor kommunikasjonen går via kontornettverket (IP-telefoni), som er trenden, og hvor berørte komponenter i kontornettverket skal behandles som nødkommunikasjonsutstyr.

Nært opp til dette ligger også behov for mer kunnskap om håndtering av IKT-hendelser/cyberangrep hvor kontornettverket kan være angrepet samtidig som man på innretningen er avhengig av ekstern ekspertise (CSIRT – Cyber Security Incident Response Team), og hvor mange innretninger har ekstern nød-kommunikasjon via det samme kontornettverket.

Et tredje forhold hvor det er behov for videre kunnskapsinnhenting er hvordan man totalt sett øver på samt tester kommunikasjonsutstyr og reserveløsninger for ekstern nødkommunikasjon.

Referanser

[1] Petroleumstilsynet, IKT-sikkerhet – robusthet i petroleumssektoren, https://www.ptil.no/fagstoff/utforsk-fagstoff/prosjektrapporter/2020/ikt-sikkerhet--robusthet-i-petroleumssektoren/ (nedlastet 31.10.2020)

[2] Lov om elektronisk kommunikasjon (Ekomloven), 01.07.2020, https://lovdata.no/dokument/NL/lov/2003-07-04-83 (nedlastet 31.10.2020)

[3] NOU 2015: 13. Digital sårbarhet – sikkert samfunn. Departementenes sikkerhets- og serviceorganisasjon. https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/ (nedlastet 31.10.2020)

[4] Petroleumstilsynet, Veiledning til aktivitetsforskriften (18. desember 2019), https://www.ptil.no/contentassets/332166193108427e978accb21449436c/aktivitetsforskriften20_veiledning_n.pdf (nedlastet 31.10.2020)

[5] NORSOK Z-013:2010, Risk and emergency preparedness assessment. Edition 3, October 2010, https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=459004 (nedlastet 31.10.2020)

[6] Petroleumstilsynet, Fagstoff, Ord og uttrykk, https://www.ptil.no/fagstoff/ord-og-uttrykk/, (nedlastet 17.10.2020)

[7] Nasjonal sikkerhetsmyndighet (NSM), 2015. Helhetlig IKT-risikobilde 2015, https://nsm.no/getfile.php/133681-1592831865/Demo/Dokumenter/Rapporter/nsm_helhetlig_ikt_risikobilde_2015_lr.pdf (nedlastet 31.10.2020)

[8] NS 5814:2008. Krav til risikovurderinger. Standard Norge. https://www.standard.no/no/nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=337102 (nedlastet 31.10.2020)

[9] NS 5832:2014. Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger - Krav til sikringsrisikoanalyse, https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=718202 (nedlastet 31.10.2020)

[10] UNISDR: Terminology on Disaster Risk Reduction. United Nations International Strategy for Disaster Risk Reduction, Geneva, 2009. https://www.undrr.org/publication/2009-unisdr-terminology-disaster-risk-reduction (nedlastet 31.10.2020)

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

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

[13] Bodsberg, L., Grøtan, T.O., Gilje Jaatun, M., Onshus, T., Wærø, I., 2019. IKT-sikkerhet – Fjernarbeid og HMS, SINTEF 2019:00361. https://www.ptil.no/contentassets/92b2f32146e346acac52546c53b72a46/sluttrapport-ptil-ikt-sikkerhet---fjernarbeid-og-hms-med-underskrift-og-vedlegg.pdf (nedlastet 31.10.2020)

[14] Petroleumstilsynet, Veiledning til rammeforskriften (18. desember 2019), https://www.ptil.no/contentassets/332166193108427e978accb21449436c/rammeforskriften20_veiledning_n.pdf (nedlastet 31.10.2020)

[15] Petroleumstilsynet, Forskrift om utføring av aktiviteter i petroleumsvirksomheten (aktivitets-forskriften 18.12.2017),

https://www.ptil.no/contentassets/332166193108427e978accb21449436c/aktivitetsforskriften20_n.pdf (nedlastet 31.10.2020)

[16] Petroleumstilsynet, Forskrift om styring og opplysningsplikt i petroleumsvirksomheten og på enkelte landanlegg (styringsforskriften 18.12.2017), https://www.ptil.no/contentassets/332166193108427e978accb21449436c/styringsforskriften20_n.pdf (nedlastet 31.10.2020)

[17] Petroleumstilsynet, Veiledning til styringsforskriften (18. desember 2019), https://www.ptil.no/contentassets/332166193108427e978accb21449436c/styringsforskriften20_veiledning_n.pdf (nedlastet 31.10.2020)

[18] Nasjonal sikkerhetsmyndighet (NSM), 2020. Risiko 2020. https://nsm.no/aktuelt/risiko-2020 (nedlastet 31.10.2020)

[19] Røde Kors, 2020. Norges klima og beredskap. Er vi beredt? https://www.rodekors.no/globalassets/globalt/rapporter-program-avtaler/beredskap-og-hjelpekorps-arsrapporter/beredskapsrapport-2019/rodekors-klima-beredskap_nr5_rgb.pdf (nedlastet 31.10.2020)

[20] Øien, K., Bodsberg, L. and Jovanovic, A., 2018. Resilience assessment of smart critical infrastructures based on indicators. Safety and Reliability – Safe Societies in a Changing World – Haugen et al. (Eds). 2018 Taylor & Francis Group, London, ISBN 978-0-8153-8682-7.

[21] FFI-Rapport 19/00363: Brynhild Stavland, Janita Andreassen Bruvoll, Resiliens – hva er det og hvordan kan det integreres i risikostyring? Mars 2019, https://publications.ffi.no/nb/item/asset/dspace:6458/19-00363.pdf (nedlastet 31.10.2020)

[22] DNV GL, 2020. Resiliens mot cyberhendelser og kan blokkjede bidra? Rapport nr.: 2019-0825, Rev. 0. https://www.ptil.no/contentassets/fbde8c6d6b9d4ff7afb8188aadb96a62/dnv-gl---resiliens-mot-cyberhendelser-og-kan-blokkjede-bidra.pdf (nedlastet 31.10.2020)

[23] Petroleumstilsynet, Forskrift om tekniske og operasjonelle forhold på landanlegg i petroleumsvirksomheten med mer (teknisk og operasjonell forskrift, 18. desember 2019), https://www.ptil.no/contentassets/332166193108427e978accb21449436c/teknisk_og_operasjonell_forskrift20_n.pdf (nedlastet 31.10.2020)

[24] NORSOK T-001:2010, Telecom systems. Edition 4, February 2010, https://www.standard.no/no/nettbutikk/produktkatalogen/produktpresentasjon/?ProductID=443200 (nedlastet 31.10.2020)

[25] NORSOK T-100:2010, Telecom subsystems. Edition 4, February 2010, https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=443201 (nedlastet 31.10.2020)

[26] Petroleumstilsynet, Veiledning til innretningsforskriften (18. desember 2019), https://www.ptil.no/contentassets/332166193108427e978accb21449436c/innretningsforskriften20_veiledning_n.pdf (nedlastet 31.10.2020)

[27] NORSOK T-101:2019, Telekom systemer, https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=1094701 (nedlastet 31.10.2020)

[28] NORSOK T-003:2019, Telekom systemer for flyttbare offshore installasjoner, https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=1094702 (nedlastet 31.10.2020)

[29] NORSOK S-001:2018, Teknisk sikkerhet, Utgave 5, juni 2018, https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=981001 (nedlastet 31.10.2020)

[30] FOR-2004-02-16-401 Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften), https://lovdata.no/dokument/SF/forskrift/2004-02-16-401 (nedlastet 31.10.2020)

[31] FOR-2011-12-07-1206 Forskrift om autorisasjon for virksomhet som utfører installasjon og vedlikehold av elektronisk kommunikasjonsnett (autorisasjonsforskriften), https://lovdata.no/dokument/SF/forskrift/2011-12-07-1206 (nedlastet 31.10.2020)

[32] FOR-2014-07-01-955 Forskrift om radiokommunikasjonsutstyr for norske skip og flyttbare innretninger, https://lovdata.no/dokument/SF/forskrift/2014-07-01-955 (nedlastet 31.10.2020)

[33] FOR-2019-05-14-604 Forskrift om luftfart med helikopter – bruk av offshore helikopterdekk, https://lovdata.no/dokument/SF/forskrift/2019-05-14-604 (nedlastet 31.10.2020)

[34] Meld. St. 38 (2016-2017), IKT-sikkerhet – Et felles ansvar, Justis- og beredskapsdepartementet, https://www.regjeringen.no/no/dokumenter/meld.-st.-38-20162017/id2555996/ (nedlastet 31.10.2020)

[35] Petroleumstilsynet, Forskrift om utforming og utrusting av innretninger med mer i petroleums-virksomheten (innretningsforskriften 18.12.2017), https://www.ptil.no/contentassets/332166193108427e978accb21449436c/innretningsforskriften20_n.pdf (nedlastet 31.10.2020)

[36] Petroleumstilsynet, Ansvar, kompetanse og vedlikehold av kommunikasjonssystemer. 06.02.2020, https://www.ptil.no/contentassets/94380bf6cc064ca8b3143ffd01059ab9/rapport-om-ansvar-kompetanse-og-vedlikehold-av-kommunikasjonssystemer.pdf (nedlastet 31.10.2020)

[37] DNV-GL, IKT-sikkerhet – robusthet i petroleumssektoren. Telekommunikasjon og protokoller. 24-02-2020, https://www.ptil.no/contentassets/fbde8c6d6b9d4ff7afb8188aadb96a62/dnv-gl---telekommunikasjon-og-protokoller.pdf (nedlastet 31.10.2020)

[38] NOU 2018: 14, IKT-sikkerhet i alle ledd — Organisering og regulering av nasjonal IKT-sikkerhet, Justis- og beredskapsdepartementet, https://www.regjeringen.no/no/dokumenter/nou-2018-14/id2621037/ (nedlastet 31.10.2020)

[39] NOROG 104. Norwegian Oil and Gas recommended guidelines on information security baseline requirements for process control, safety and support ICT systems. Rev. 06, 2016, https://www.norskoljeoggass.no/contentassets/15263fd7f781409286f319bbeb427d93/104-recommended-guidelines-on-security-baseline-requirements.pdf (nedlastet 31.10.2020)

[40] DNV GL rapport til Lysne-utvalget, https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/sved/5.pdf (nedlastet 31.10.2020)

[41] Nkom, EkomROS 2019: Den digitale grunnmuren. Risikovurdering av ekomsektoren. Juni 2019. https://www.nkom.no/rapporter-og-dokumenter/ekomros-2019 (nedlastet 31.10.2020)

[42] Nkom, EkomROS 2020: Den digitale grunnmuren satt på prøve. 13.10.2020. https://www.nkom.no/rapporter-og-dokumenter/ekomros2020 (nedlastet 31.10.2020)

[43] DNVGL-RP-G108. Cyber security in the oil and gas industry based on IEC 62443 (2017), www.dnvgl.com/oilgas/download/dnvgl-rp-g108-cyber-security-in-the-oil-and-gas-industry-based-on-IEC-62443.html (nedlastet 22.08.2020)

[44] NEK EN ISO/IEC 27001:2017, Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015), https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=882638 (nedlastet 31.10.2020)

[45] NEK EN ISO/IEC 27002:2017, Information technology - Security techniques - Code of practice for information security controls (ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015), https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=882614 (nedlastet 31.10.2020)

[46] NEK IEC 62443, https://www.nek.no/nek-iec-62443-en-baerebjelke-for-cybersikkerhet/ (nedlastet 31.10.2020)

[47] IEC 61508 Functional safety of electrical/electronic/programmable electronic safety related systems, https://www.iec.ch/functionalsafety/standards/page2.htm (nedlastet 22.08.2020)

[48] IEC 61511 Functional safety of safety instrumented systems for the process industry sector, https://webstore.iec.ch/publication/24241 (nedlastet 22.08.2020)

[49] Norwegian Oil and Gas. 070 Guidelines for the Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry (Recommended SIL requirements), 2018, Revision no.: 03, https://www.norskoljeoggass.no/contentassets/adc7e1512f90400cb7fe9f314600bed6/norwegian-oil-and-gas-guidelines-070-rev-3-june-2018.pdf (nedlastet 22.08.2020)

[50] Petroleumstilsynet, Forskrift om helse, miljø og sikkerhet i petroleumsvirksomheten og på enkelte landanlegg (rammeforskriften 26. april 2019), https://www.ptil.no/contentassets/332166193108427e978accb21449436c/rammeforskriften20_n.pdf (nedlastet 31.10.2020)

[51] Petroleumstilsynet, Om regelverket, https://www.ptil.no/regelverk/lover/om-regelverket/ (nedlastet 31.10.2020)

[52] IEC 60050-192:2015, International Electrotechnical Vocabulary (IEV) - Part 192: Dependability, https://www.standard.no/nettbutikk/produktkatalogen/produktpresentasjon/?ProductID=739134 (nedlastet 31.10.2020)

[53] Regjeringen.no, 2016. Grønne datasentre og mørk fiber: Regjeringen vil ha svar på om fibermarkedet fungerer godt nok, Samferdselsdepartementet, pressemelding 27.07.2016, Nr: 177/16, https://www.regjeringen.no/no/aktuelt/gronne-datasentre-og-mork-fiber-regjeringen-vil-ha-svar-pa-om-fibermarkedet-fungerer-godt-nok/id2508212/ (nedlastet 31.10.2020)

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

Vedlegg A: Krav til ekstern kommunikasjon i petroleumsregelverket (utdrag)

Tabell A.1 Krav til ekstern kommunikasjon i petroleumsregelverket (per 24.06.2020)

PARAGRAF - TEMA	KRAV
Aktivitetsforskriften [5] (med tilhørende veiledning [2])	
§ 21 Kompetanse (utdrag)	Den ansvarlige skal sikre at personellet til enhver tid har den kompetansen som er nødvendig for å kunne utføre aktivitetene i henhold til helse-, miljø- og sikkerhets-lovgivningen. I tillegg skal personellet **kunne håndtere fare- og ulykkessituasjoner**, jf. styringsforskriften § 14 og denne forskriften § 23. …
Veiledning til § 21 (utdrag)	… For å oppfylle kravet til kompetanse på området helse, arbeidsmiljø og sikkerhet bør … h) det ved bruk av kommunikasjonsutstyr sikres at **den kommunikasjonsansvarlige**, jf. § 80 andre ledd, har god erfaring som kommunikasjonsoperatør og gyldig GMDSS radio-operatørsertifikat (GOC eller ROC avhengig av radioutstyr om bord), samt nødvendig kompetanse på områder som beredskapsledelse, helikopterkommunikasjon, meteorologiske observasjoner og overvåking av sikkerhetssonene og havområdene rundt innretningen, … For **radiooperatører** som opererer maritimt radioutstyr, er kompetansekravene gitt i konsesjonsvilkår fastsatt av Samferdselsdepartementet.
§ 23 Trening og øvelser (utdrag)	Den ansvarlige skal sikre at det utføres nødvendig trening og nødvendige øvelser, slik at personellet **til enhver tid er i stand til å håndtere** operasjonelle forstyrrelser og **fare- og ulykkessituasjoner på en effektiv måte**. …
Veiledning til § 23 (utdrag)	For å oppfylle kravet til trening og øvelser bør … b) de som har beredskapsfunksjoner, trene på sine beredskapsoppgaver minst én gang i løpet av oppholdsperioden. …
§ 75 Beredskaps-organisasjon	Beredskapsorganisasjonen skal være robust slik at den kan **håndtere fare- og ulykkessituasjoner** på en effektiv måte. Ved akutt forurensning skal beredskapsorganisasjonen ivareta nødvendige funksjoner for å kunne utføre aksjoner mot akutt forurensning effektivt.
Veiledning til § 75 (utdrag)	Med beredskapsorganisasjonen som nevnt i første ledd, menes det personellet, deriblant en lege, som er knyttet direkte til enhetsressursene, områderessursene, de eksterne ressursene og de regionale ressursene. …
§ 80 Kommunikasjon	Det skal sikres at nødvendig intern og **ekstern varsling og kommunikasjon** blir ivaretatt til enhver tid under installering og drift, og **i fare- og ulykkessituasjoner**, jf. innretnings-forskriften § 18 og § 19. Det skal pekes ut en kommunikasjonsansvarlig om bord for kommunikasjonssystemene på bemannede innretninger.
Veiledning til § 80 (utdrag)	For å ivareta kommunikasjonen som nevnt i første ledd, bør blant annet … c) **direkte og kontinuerlig kommunikasjon** kunne opprettes og opprettholdes mellom kommunikasjonsoperatør, felt- og plattformledelse og interne og **eksterne beredskapsressurser i fare- og ulykkessituasjoner**, … Kravet til ekstern kommunikasjon som nevnt i første ledd, innebærer at bemannede innretninger har **døgnkontinuerlig telekommunikasjonstjeneste med vakt på VHF-kanal 70 (DSC) og kanal 16**. Tjenesten kan være opprettet på egen innretning eller som en del av en fellesløsning der flere innretninger ligger innenfor et nærmere definert område. … Med kommunikasjonsansvarlig som nevnt i andre ledd, menes en som har et særlig ansvar for å se til at driften av innretningens radiostasjon og bruken av de andre kommunikasjonssystemene er faglig forsvarlig til enhver tid.

Innretningsforskriften [IF] (med tilhørende veiledning [7])	
§ 18 Systemer for intern og ekstern kommunikasjon (utdrag)	Midlertidig og permanent bemannede innretninger skal utstyres med kommunikasjonssystemer som **til enhver tid gjør det mulig å kommunisere** internt på innretningen, og **mellom innretningen** og skip, luftfartøy **og land**. … Det skal være etablert **minst to uavhengige varslingsveier til land**, fortrinnsvis ved hjelp av faste samband.
Veiledning til § 18 (utdrag)	For å oppfylle kravet til utforming av interne kommunikasjons- og alarmsystemer som nevnt i første ledd, bør følgende standarder brukes: NORSOK S-001, kapittel 18 for allmenngyldige lyd- og lysalarmer, T-001 og T-100 for alarm- og kommunikasjonssystemer … [1)] 1) Merk at NORSOK T-001 og T100 er erstattet av **NORSOK T101:2019 (en)**. Kravet om minst to uavhengige varslingsveier som nevnt i andre ledd, innebærer at **alternative varslingsveier (sekundære) skal være uavhengig av den primære varslingsveien** med hensyn til kraftforsyning og tilgjengelighet under fare- og ulykkessituasjoner, deriblant være motstandsdyktig mot de dimensjonerende etablerte ulykkeslastene i et definert tidsrom. Det bør brukes faste samband som **fiberkabel-, radiolinje- eller satellittsystemer** dersom innretningens posisjon gjør dette mulig. Hvis to uavhengige varslingsveier via faste samband ikke lar seg realisere, kan én av varslingsveiene erstattes med samband i den maritime mobile tjenesten.
§ 19 Kommunikasjons-utstyr	**Utstyr for ekstern kommunikasjon skal velges ut fra** operasjonelle behov, type aktivitet og **definerte fare- og ulykkessituasjoner**, jf. styringsforskriften § 17. Kommunikasjonsutstyr og tilhørende kraftforsyning skal utformes og beskyttes slik at funksjonen **opprettholdes ved fare- og ulykkessituasjoner**.
Veiledning til § 19 (utdrag)	Ved valg av utstyr som nevnt i første ledd, bør **midlertidige og permanent bemannede innretninger** utrustes med følgende utstyr: a) To separate fastmonterte maritime VHF-radioer med DSC, b) Radiofyr for helikopternavigasjon, c) To separate fastmonterte aeromobile VHF-radioer samt bærbare aeromobile VHF-radioer, d) Én NAVTEX mottaker, alternativt annen akseptert ordning for mottak av maritime sikkerhetsmeldinger (MSI=Maritime Safety Information). Ved valg av utstyr som nevnt i første ledd, bør *evakuerings- og redningsmidler* utrustes med følgende utstyr godkjent i samsvar med internasjonale og nasjonale standarder for slik bruk: a) **Livbåter:** én fastmontert VHF-radio og én RADAR-SART eller AIS-SART, b) **Flåter:** et nødvendig antall bærbare VHF-radiosett og RADAR-SART eller AIS-SART som er plassert slik at de er lett tilgjengelig for å kunne tas med i flåter, for eksempel i container for redningsstrømper, c) **Mann-over-bord-båter (MOB-båter):** vanntett VHF som opprettholder kommunikasjon under de forholdene som MOB-båten skal operere under, og som ikke hindrer mannskapet i å bruke begge hender til manøvrering av båt, eller deltakelse i redningsoperasjoner. Fastmontert VHF eventuelt som ekstra VHF. Med beskyttelse som nevnt i andre ledd, menes det blant annet at **utstyret må være plassert slik at kommunikasjonen ikke blir forstyrret**. De to maritime VHF-radioene med DSC bør plasseres i ulike rom slik at begge ikke blir satt ut av funksjon av en og samme hendelse. Dette gjelder også de fastmonterte aeromobile radioene. VHF-stasjon i livbåter bør utformes og plasseres slik at den kan brukes samtidig som båtene manøvreres med motoren på fullt turtall.
§ 59 Helseavdeling (utdrag)	… Fra helseavdelingen skal det være mulig å ha **telefonkontakt med lege i land**. … Kommunikasjonsteknisk utstyr skal være **sikret mot strømbrudd**.

	For å opprettholde livsviktige funksjoner ved strømbrudd skal helseavdelingen ha tilfredsstillende arbeidslys og minst to strømuttak for nødkraft, jf. § 38.
Veiledning til § 59	(Ikke relevant)
§ 77 EMC	Apparater og faste installasjoner som omfattes av forskrift om EØS-krav til elektromagnetisk kompatibilitet **(EMC) for utstyr til elektronisk kommunikasjon** skal være i samsvar med kravene i den forskriften, også når slikt utstyr brukes i petroleumsvirksomheten.
Veiledning til § 77	Denne paragrafen viderefører tidligere innarbeiding i petroleumsvirksomheten av rådsdirektiv 89/336/EØF, 92/31/EØF og 2004/108/EF (elektromagnetisk kompatibilitet – EMC).

Vedlegg B: Krav til ekstern kommunikasjon utenfor petroleumsregelverket (utdrag)

Tabell B.1 Krav til ekstern kommunikasjon utenfor petroleumsregelverket (per 24.06.2020)

PARAGRAF - TEMA	KRAV
FOR-2004-02-16-401 Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste [11]	
Kapittel 8. Sikkerhet og beredskap	
§ 8-2. Beredskapsplaner og øvelser m.m.	Tilbyder skal **utarbeide og vedlikeholde planer og gjennomføre tiltak** for å opprettholde forsvarlig sikkerhet i elektronisk kommunikasjonsnett for å: 1. sikre tilfredsstillende tjenestetilbud og utførelse av egne beredskapsoppgaver, 2. utførelse av pliktene som følger av § 8-4 første ledd. Tilbyder skal på forespørsel fra Nasjonal kommunikasjonsmyndighet utlevere **planer** etter første ledd, samt **risiko- og sårbarhetsvurderinger** som ligger til grunn for planer og tiltak. Nasjonal kommunikasjonsmyndighet fører tilsyn med planene og kan sette krav til form og innhold. Tilbyder skal på forespørsel delta i **beredskapsøvelser** arrangert av myndigheten.
§ 8-4. Prioritering av tjenestetilbud	Ved driftsstans skal tilbyder ved gjenoppretting prioritere hensynet til sluttbrukere med ansvar for borgernes liv og helse foran kommersielle hensyn. Myndigheten kan i særlige tilfeller så langt det er nødvendig for å sikre offentlige interesser, pålegge tilbyder å gi **prioritet til viktige samfunnsaktører** ved gjenoppretting etter driftsstans.
§ 8-5. Varsel (utdrag)	Tilbyder skal **varsle** Nasjonal kommunikasjonsmyndighet **om hendelser** som vesentlig kan redusere eller har redusert tilgjengeligheten til elektroniske kommunikasjonstjenester. …
FOR-2014-07-01-955 Forskrift om radiokommunikasjonsutstyr for norske skip og flyttbare innretninger [13]	
Hoveddel	
§ 2. Krav om radio-kommunikasjonsutstyr for lasteskip og passasjerskip	Den internasjonale konvensjonen om sikkerhet for menneskeliv til sjøs 1974 (**SOLAS**) konsolidert utgave 2014 kapittel IV, som endret ved resolusjon MSC.436(99), **gjelder som forskrift**.
§ 7. Krav om radio-kommunikasjonsutstyr på flyttbare innretninger	Flyttbare innretninger skal **følge kravene for lasteskip** i § 2.
§ 10. Krav til dobbelt sett utstyr og vedlikehold av radioutstyr	Skip og flyttbare innretninger i radiodekningsområdene A3 eller A4 skal ha **dobbelt sett radioutstyr**. På flyttbar boreinnretning skal radioutstyret som kreves med hjemmel i første punktum plasseres med størst mulig avstand fra det primære radioutstyret som kreves etter § 7.
Vedlegg: SOLAS 74	
Kapittel IV Radiokommunikasjon	
Del A generelle bestemmelser: Regel 4 Funksjonskrav (utdrag)	1 Ethvert skip, mens det er underveis, skal kunne: .1 sende **skip-til-land nødmeldinger** ved hjelp av **minst to atskilte og uavhengige midler**, der hvert av midlene bruker forskjellig radiokommunikasjonstjeneste, unntatt som fastsatt i regel 8 nr. 1.1 og regel 10 nr. 1.4.3, …

Vedlegg C: Krav til ekstern kommunikasjon i relevante standarder (utdrag)

Her er det tatt med relevante standarder som det er referert til i petroleumsregelverket. Dette er NORSOK T-101:2019 *Telekom systemer* [9], NORSOK T-003:2019 *Telekom systemer for flyttbare offshore installasjoner* [10], og NORSOK S-001:2018 *Teknisk sikkerhet* [6]. (Uoffisiell oversettelse).

Vedlegg C.1: NORSOK T-101:2019 Telekom systemer

Tabell C.1 Krav til ekstern kommunikasjon i NORSOK T-101:2019

AVSNITT OG TEMA	KRAV
NORSOK T-101:2019 (en) Telekom systemer [9]	
DEL 1 Generell telekom	
5. Generelle krav	
5.3.2 Nød-kommunikasjons-systemer (utdrag)	Følgende telekommunikasjonssystemer skal være tilgjengelig og i drift under en fare eller nødsituasjon (se NORSOK S-001): … – Ekstern nødkommunikasjon slik som: o Radio (GMDSS) o Maritim VHF-radio o Aeronautisk VHF-radio o Telefoner i SKR/BS (prioritert tilgang og/eller hot line) o Kommunikasjon til land / andre innretninger o Infrastruktur for de ovenfornevnte systemer. … Når et datanettverk benyttes for tilkobling til nødkommunikasjonssystemer så skal alle deler av datanettverkene som er nødvendige for å opprettholde funksjonen designes i henhold til kravene til nødkommunikasjonssystemer.
5.3.6 Hoved-kommunikasjon til land / andre innretninger (utdrag)	Det skal minimum være to uavhengige faste kommunikasjonsforbindelser til driftssenteret på land, enten direkte eller via andre faste innretninger. Kommunikasjonsforbindelsene skal være designet for høy pålitelighet og høy kapasitet for å tillate nødkommunikasjon, daglig drift og integrerte operasjoner. Aktuelle systemer er: – Fiberoptisk kabel; – Radioforbindelse; – Satellittforbindelse; – 4G/LTE. … I tillegg til permanente kommunikasjonsforbindelser kan oppkoblede satellitt-tjenester benyttes for back-up. …
5.4.6 Antennetårn og antenner (utdrag)	Et antennetårn skal installeres på toppen av innretningen for antenner for VHF og UHF mobile radiosystemer, radioforbindelser, radar, osv. … Redundante antenner for nødkommunikasjonssystemer skal være adskilt fra hovedantennene for å unngå samtidig hindring eller mekanisk skade som resulterer i totaltap av kommunikasjon.

6. Systemkrav	
6.4 Pålitelighet (utdrag)	… For å unngå totaltap av funksjon for et telekommunikasjonssystem gjelder følgende: – Nødkommunikasjonssystemer (jf. avsnitt 5.3.2) eller kritiske moduler i disse systemene skal være redundante; … – Avbruddssikker kraftforsyning (UPS) skal distribueres dobbel-redundant. …
6.5 IKT-sikkerhet 6.5.1 Generelt (utdrag)	IKT-sikkerhet skal opprettholdes under hele levetiden til telekom-systemer. Anbefalinger til beste praksis kan man finne i følgende publikasjoner: DNVGL-RP-G108, NOG 104, NEK IEC 27001 og NEK IEC 27002. …
6.5.2 Sårbarhets-vurdering	En sårbarhetsvurdering skal gjennomføres for hvert telekom-system for å identifisere sikringsrisikoer og avhjelpende tiltak. Sårbarheter er svakheter i systemet og i prosedyrer som kan utnyttes av en trussel-agent. Resultatet av sårbarhetsvurderingen bør være en liste over sårbarheter sammen med tilhørende avhjelpende tiltak nødvendig for å begrense sannsynligheten for utnyttelse av disse sårbarhetene. Følgende tema bør som et minimum adresseres i sårbarhetsvurderingen: – Fysisk beskyttelse av maskinvare; – Ubrukte fysiske porter; – Adgangsmetoder; – Brukeradministrasjon og passord policy; – Oppgraderingsstyring; – Sikkerhetskopiering og nød-gjenoppretting; – Skadevare-beskyttelse; – Fjerntilgang. Resultatet av sårbarhetsvurderingen kan inneholde kritisk informasjon og skal behandles deretter.
6.13 Generelle funksjonskrav 6.13.4 Alarmgrensesnitt (utdrag)	… Kritisk alarm: Store deler av nødkommunikasjonssystemene ute av drift. … Kritiske alarmer skal også være fast koplet ("hardwired") direkte fra alle nødkommunikasjonssystemer til SAS for visning i SKR. …
6.15 PC-er, servere og brytere	PC-er, servere og brytere som er brukt som en del av telekom-systemene skal ha en pålitelighet som svarer til systemene de er brukt i.
DEL 2 Systemdesign	
Kapittel 9-31	Her inngår krav til en rekke telekom-systemer, hvorav noen er relevant for ekstern kommunikasjon / nødkommunikasjon. De mest relevante systemene som inngår, er: – System 21 – Telefonsystem (PABX); – System 23 – Datanettverksutstyr; – System 24 – Data- og telefonkabelnettverk; – System 31 – Radioforbindelser; – System 39 – Fiberoptiske kabelforbindelser; – System 41 – Påbudte og generelle radiosystemer; – System 46 – Tilgangskontrollsystem; – System 82 – Telekom strømforsyning; – System 84 – Telekom monitoreringssystem; Relevante krav for disse systemene er vist nedenfor.

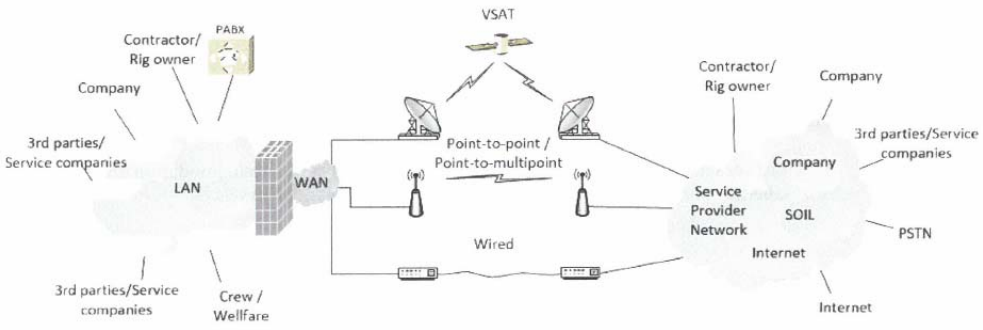
Kapittel 10 System 21 – Telefonsystem (PABX)	
10.1 Generelt	Telefonsystemet skal tilby interne og eksterne koblede telefontjenester inkludert nødkommunikasjon.
10.3 Ytelse	Systemet skal utformes som et nødkommunikasjonssystem som implementerer alle kravene gitt i punkt 5.3.2 og 6.4.
10.6 Vedlikeholdskrav	Telefonsentralen skal støtte ekstern tilgang for vedlikeholds- og supportformål. Midlertidig softphone-funksjonalitet skal være tilgjengelig for ekstern testing av systemet.
Kapittel 11 System 23 – Datanettverksutstyr	
11.1 Generelt	Datanettverkene bør deles inn i flere nettverk (f.eks. kontordatanettverk, teknisk nettverk og kritisk / PCSS-nettverk) og integreres som en del av LAN / WAN-infrastrukturen.
11.2 Systemdesign	Kritiske datanettverk med ekstern kommunikasjon til andre installasjoner eller til land skal ha: – redundans med fysisk atskilt ruting og ingen enkeltfeil-punkter; – deterministisk og tilkoblingsorientert ytelse med rask beskyttelsesbryter (50ms); – driftsadministrasjon og vedlikehold med proaktiv overvåking for rask feilsøking og forutsigbar nettverksytelse. Et styringssystem for overvåking og lagring av kritiske konfigurasjonsfiler skal implementeres. Datanettverket inkluderer: – data- og telefonnettkabler i henhold til spesifikasjonene i kapittel 12; – nettverksutstyr (f.eks. brytere, rutere, brannmurer osv.) for LAN / WAN; – trådløst nettverksutstyr for trådløst lokalnettverk (hvis aktuelt). Når et datanettverk brukes til å levere viktig PABX-kommunikasjon, skal alle deler av systemet som kreves for å opprettholde funksjonen være utformet i samsvar med kravene til nødkommunikasjonssystemer i punkt 5.3.2. Kryssing mellom ulike datanettverk skal bare være mulig gjennom informasjonssikkerhets-portaler (brannmur), og ingen klienter skal være koblet til flere forskjellige nettverk. Fysisk tilgang til sensitivt utstyr skal være begrenset.
11.3 Utstyr	Følgende designprinsipper gjelder: – grensesnitt til WAN skal være dobbelt / redundant; – grensesnitt (forbindelser) mellom rutere, brannmurer og kjernebrytere skal være dobbelt / redundant; – servere og andre viktige datamaskiner bør ha redundante nettverkstilkoblinger; – redundante strømforsyninger skal brukes til rutere, brannmurer og kjernebrytere; – redundant UPS tilførsel skal brukes til å drive utstyret.
Kapittel 12 System 24 – Data- og telefonkabelnettverk	
12.1 Generelt	Datanettverket bør deles inn i flere nettverk i henhold til kapittel 11.
12.2 Produkt og tjenester	Kabelsystemet består av: – telekommunikasjonsuttak; – fordeler (se NEK EN 50173 [13], etasjefordeler); – sentralfordeler eller hovedfordelingsramme (se NEK EN 50173 [13], bygningsfordeler); – horisontal kabling, fra telekommunikasjonsuttak i arbeidsområdet til fordeleren; – kabling til nettverksstammen, fra hovedfordelingsramme til etasjefordeleren (se NEK EN 50173 [13], kabling til nettverksstammen i bygning).

Kapittel 13 System 31 – Radioforbindelser	
13.1 Generelt	Radioforbindelser kan installeres for punkt-til-punkt kommunikasjon mellom to offshore-innretninger eller mellom en offshore-innretning og land. En radioforbindelses-overføring kan være en del av en offshore-innretnings hoved-infrastrukturforbindelse til land eller et supplement til optisk fiberforbindelse for å oppnå redundans i utstyr og / eller ruting. Dersom en radioforbindelses-overføring er del av en offshore-innretnings hoved-kommunikasjonsforbindelse til land, skal det designes med utstyrsredundans for kritiske deler.
13.2 Systemdesign	For en radioforbindelse som er en del av installasjonens infrastruktur til land, eller brukes til annen kritisk kommunikasjon, skal romdiversitet brukes hvis det er en risiko for flerveisfading.
13.3 Tekniske krav 13.3.1 Konfigurering 13.3.2 Grensesnitt	Utstyrsredundans og flerkanals-konfigurasjon: – for en radioforbindelse som er en del av installasjonens infrastruktur til land, eller brukes til annen kritisk kommunikasjon, skal forbindelsen være konfigurert med redundans av utstyr. I radiolink-terminologi blir dette vanligvis referert til som en konfigurasjon med beskyttelse. Nettverks-grensesnittkrav: – strømforsyning: o utstyret skal drives fra to uavhengige strømforsyninger o en kildeoverføringsmekanisme skal opprettholde uavbrutt drift hvis en av de to forsyningene svikter
Kapittel 15 System 39 – Fiberoptiske kabelforbindelser	
15.1 Generelt	Undersjøiske fiberkabler kan brukes til å koble en offshoreinnretning til land eller til en nærliggende innretning for å gi kommunikasjon med høy kapasitet og lav latens til innretningen. Et undersjøisk fiberkabelsystem kan enten være dedikert for en offshoreinnretning, eller en del av et nett som eies og drives av et partnerskap eller eneeier.
15.2 Ytelseskrav 15.2.1 Subsea fiberkabler	Den undersjøiske fiberkabelen skal være egnet for nedgraving eller overflatelegging og skal ha muligheter for lokalisering av feil. Hvis en offshoreinnretning har mer enn en fiberoptisk forbindelse til land, skal de forskjellige undersjøiske fiberkabelsegmentene være fysisk atskilt for å sikre at ingen enkeltfeil vil føre til tap av kommunikasjon til innretningen. Landingsstasjonene for undersjøisk fiberkabel på land skal være geografisk adskilt for ikke å bli påvirket av lokale strømbrudd eller lokale skader på landingsstasjonen eller på digital linjeseksjon (DLS). Det undersjøiske fiberoptiske nettverket skal ha et linjeovervåkingssystem for å overvåke statusen til undervannsanlegget for degradering og følgende feil: kabel, forgrenings-enheter, repeatere.
15.3 Tilgjengelighet og overlevelsesevne	Hvis det er en del av et omfattende nettverk, skal ikke det undersjøiske fibernettverket ha enkeltfeil-punkt som vil føre til at flere ressurser mister tilkoblingen.
Kapittel 16 System 41 – Påbudte og generelle radiosystemer	
16.1 Generelt	Følgende utstyr er dekket: – utstyr for GMDSS radiokrav; – utstyr for ytterligere maritim kommunikasjon; – utstyr for aeromobile kommunikasjon; – utstyr for aeromobile navigasjonshjelpemidler – NDB; – utstyr for kran-kommunikasjon.

Kapittel 20 System 46 – Tilgangskontrollsystem	
20.1 Generelt	Systemet kan brukes på innretninger for å styre tilgangskontroll til begrensede områder ved å kontrollere elektromekaniske dørlåser og solenoider for pneumatisk betjente dører. Systemet kan være koblet sammen med andre systemer, for eksempel sikkerhets- og automatiseringssystem (SAS) og personalregistreringssystem.
20.2 Systembeskrivelse	Hovedformålet med systemet er å administrere tilgangskontroll til begrensede områder som LER (lokalt utstyrsrom), TER (telekom-utstyrsrom), sykestua og elektriske bryterrom. Systemet skal ha et dedikert kommunikasjonsnettverk for kommunikasjon innenfor komponenter i tilgangskontrollsystemet. Det skal være muligheter for nødåpning, for eksempel ved å knuse sikkerhetsglass og global nødåpning fra SKR.
20.4 Lokalisering av utstyr	Utforming av feltutstyr skal være slik at lokale kontrollere osv. er innenfor beskyttet område. Pneumatiske dørkontrollsystemer bør utformes slik at låsefunksjoner ikke lett kan deaktiveres.
Kapittel 29 System 82 – Telekom strømforsyning	
29.1 Generelt	Avbruddsfri strømforsyning (UPS) skal leveres for alle telekommunikasjonssystemer som kreves i en farlig situasjon eller i en nødsituasjon, bortsett fra bærbart håndholdt utstyr.
Kapittel 31 System 84 – Telekom monitoreringssystem	
31.1 Generelt	Systemet brukes til overvåking av telekommunikasjonssystemer på offshore-innretninger. Overvåking av kritiske kommunikasjonsforbindelser til eksterne operasjonssentre skal inkluderes hvis det ikke overvåkes andre steder. For innretninger med vanligvis ingen telekommunikasjonsspesialister ombord, skal muligheter for fjerndiagnostikk være tilgjengelig.
DEL 3 Telekom på enklere innretninger	
Kapittel 32	Telekom og IT-systemer på enklere innretninger uten overnatting. Dette dekker krav til enkle ubemannede innretninger.

Vedlegg C.2: NORSOK T-003:2019 Telekom systemer for flyttbare offshore installasjoner

Tabell C.2 Krav til ekstern kommunikasjon i NORSOK T-003:2019

AVSNITT OG TEMA	KRAV
NORSOK T-003:2019 (en) Telekom systemer for flyttbare offshore installasjoner [10]	
5. Generelle krav og betingelser	
5. Generelle krav og betingelser (utdrag)	Den mobile offshore-enheten skal utstyres med egnet utrustning som vist i figur 1 for data- og telekommunikasjonstjenester mellom den mobile offshore-enheten og selskapets kommunikasjonsnettverk.  Figur 1 Prinsipp-skisse Som et generelt prinsipp skal kontraktøren være ansvarlig for data-, telekom-, og nettverksinfrastruktur på den mobile offshore-enheten. Eksterne kommunikasjons-forbindelser kan bli skaffet og operert av andre. Når en radioforbindelse benyttes, skal selskapet skaffe radioforbindelsesutstyr og frekvenser. Stemme, data og nettverksutstyr (f.eks. sentrale og distribuerte brytere, media-omformere, rutere, PABX) skal skaffes, opereres og vedlikeholdes av kontraktør. …
6. Generelle funksjonskrav	
6.1 Krav til kraft-forsyning	Telekom, data og tilhørende utstyr skal forsynes med kraft fra en UPS-kilde eller kilder. UPS-en som forsyner nødkommunikasjonssystem og støttesystemer som er designet for å operere under en fare eller nødsituasjon skal ha kapasitet til minimum 2 timers drift. Telekom, data og tilhørende utstyr skal være individuelt kontrollert av den mobile offshore-enhetens nedstengningssystem.
8. IKT-sikkerhet	
8.1 Generelt	Hensikten er å levere sikre nettverksløsninger til alle partene på den mobile offshore-enheten og være i stand til å kontrollere og overvåke trafikken. Kravene i NOG 104 skal følges.
8.2 Krav	Fjerntilgang/fjernkommunikasjon skal skaffes og følgende gjelder: – Ingen VPN (virtuelle private nettverk) tunneler tillatt for prosesskontroll og støtte-systemer (PCSS) på riggen; – Segmenterte nettverk for PCSS/IKT-infrastrukturen, og kontroll av alle

	kommunikasjonsveier; – Fjerntilgang: o Begrenses til godkjente brukere; o All aktivitet logges; – Sikker filoverføring: o Kun overføring til den mobile offshore-enheten av filer sjekket for skadevare og ondsinnet kode; – Tidsbegrenset tilgang basert på input fra godkjent arbeidstillatelse; – To-faktor-autentisering påkrevd for fjerntilgang; – Kun personlige brukerkontoer tillatt for autentisering til fjerntilgangsløsningen; – Sikker overføring av alle permanente datastrømmer fra mobil offshore-enhet til land; – Ingen standard/fabrikksatte passord eller IP-adresser tillatt på utstyr installert på den mobile offshore-enheten; – Passord skal revideres og fornyes periodisk. Generell sikring skal besørges som følger: – Alle PCSS/IKT-nettverk skal være logisk separert og avgrenset med en brannmur; – Et innholds-filter for all gjestetrafikk skal benyttes, og skal konfigureres for å begrense tilgang; – Alle endringer skal være i henhold til en endringsledelsesprosess: o Dette kan basere seg på et IT-infrastruktur-bibliotek (ITIL) eller lignende; – Alle stativ som inneholder nettverks-utstyr, skal sikres: o Kun autorisert personell skal ha adgang; – Alle nettverk eksponert for SOIL og Internett, skal være beskyttet med inntrengnings-deteksjons-systemer for logging av all nettverksaktivitet; – Alle PCSS nettverk skal konfigureres med nivå 2 sikring, for å forhindre oppkobling av uautorisert utstyr: o Dette kan gjøres med bryterport-konfigurering som kun tillater forhånds-godkjente MAC (medie-tilgangs-kontroll) adresser eller sertifikat-baserte løsninger.
10. Kommunikasjonsforbindelser	
10.1 Generelt	Foretrukket kommunikasjon fra den mobile offshore-enheten skal være høy-kapasitets forbindelser. VSAT kan benyttes som back-up eller som hoved-kommunikasjon dersom høy-kapasitets forbindelse ikke er tilgjengelig.
10.2 Krav (utdrag)	… Satellitt: … – Den mobile offshore-enheten skal forberedes for to forskjellige satellitt-antenne-plasseringer som sikrer dekning for enhver orientering av den mobile offshore-enheten. – …
11. Fjernnett (WAN)	
11.1 Generelt	WAN er tilkoplingen fra den mobile offshore-enheten til land.
11.4 Ekstranett-tjenester	Brannvegger, tilgangs-lister og/eller separate ruting-domener skal benyttes for ekstranett-tjenester.
12. Privat automatisk utveksling (PABX)	
12.1 Generelt	Telefonutvekslingen skal sørge for intern og ekstern tale-tjeneste.

12.2 Krav (utdrag)	Følgende krav gjelder: … – Automatiske oppkoplinger (dvs. et anrop til et pre-definert nummer eller automatisk satt opp videreforbindelse når telefonen tas opp eller en direkte-anrops-knapp trykkes inn, som gir køfrie linjer) bør være tilgjengelig; – Grensesnitt mellom nettverk og PABX bør være digital; – PABX skal være fjern-konfigurerbar; – I nødsituasjoner bør omdirigering av telefonnummer til alternative lokasjoner være mulig.
14. Ultrahøy frekvens (UHF) radio	
14.2 Krav (utdrag)	Følgende krav gjelder: … – UHF frekvenser er lisensiert av NKOM, og skal kun benyttes i det geografiske området som lisensen er gitt for.

Vedlegg C.3: NORSOK S-001:2018 Teknisk sikkerhet

Tabell C.3 Krav til ekstern kommunikasjon NORSOK S-001:2018

AVSNITT OG TEMA	KRAV
NORSOK S-001:2018 (en) Teknisk sikkerhet [6]	
18 Personvarsling (PA), alarm og nødkommunikasjon	
18.1 Rolle (utdrag)	PAGA (personvarsling og generell alarm), alarm og kommunikasjonssystemer for bruk i nødsituasjoner (inntil evakuering fra innretningen) skal: – Advare, informere og veilede personell så raskt som mulig i tilfelle av en fare eller nødsituasjon; …
18.2 Grensesnitt (utdrag)	PAGA, alarm og kommunikasjonssystem for bruk til nødkommunikasjon har grensesnitt mot følgende sikkerhets-system/funksjoner: – Planløsning (layout); – Nødavstengning (ESD); – Gassdeteksjon; – Branndeteksjon; – Menneske-maskin grensesnitt (HMI) for SKR-systemer; – Nødkraft og belysning; – Rømning og evakuering; – Rednings- og sikkerhetsutstyr. …
18.3 Nødvendige hjelpe-system	PAGA, alarm og nødkommunikasjonssystemene er avhengige av nødkraftsystemer (dedikert telekom batteriforsyning og/eller innretningens UPS-system). Batterier kan benyttes for satellitt-telefoner og håndholdt utstyr dersom en ordning med ladning er tilfredsstillende administrert, f.eks. forebyggende vedlikeholdsrutiner.
18.4 Funksjonskrav 18.4.4 Ekstern nød-kommunikasjon (utdrag)	Installasjonen skal ha nødvendig utstyr for kommunikasjon med eksterne beredskaps-ressurser. Kommunikasjonssystemene skal tillate kommunikasjon med installasjoner, helikoptre, livbåter, MOB-båter, redningsflåter, fartøyer og land. … Utstyr for ekstern kommunikasjon skal gis strøm fra dedikert batteriforsyning og/eller fra innretningens UPS-system.
18.4.5 Telekom-system i en nødsituasjon	Telekom-systemer som kreves for å forbli aktive i en nødsituasjon, skal ikke gi ytterligere farer. Antenner som er plassert i ikke-farlige, naturlig ventilerte områder skal leveres i samsvar med følgende krav: – Eksplosjonsbeskyttelse (elektriske tilkoblinger) egnet for bruk i sone 2, og – (1) den maksimale overføringseffekten er 6 W eller mindre, eller (2) antennen er i samsvar med krav om sikker avstand for å unngå induksjon og gnister i tilstøtende strukturer, f.eks., for veiledning se CENELEC CLC/TR 50427.
18.5 Overlevelseskrav (utdrag)	Sentralt utstyrsrom og batterier skal være plassert i samsvar med kravene i 5.4.1 angående plassering av sikkerhetssystemer. … Kabling av feltutstyr skal føres slik at sannsynligheten for skade på grunn av eksterne ulykkeslaster og samtidig tap av feltutstyr i flere områder minimeres. Brannsikre kabler skal benyttes.

Teknologi for et bedre samfunn

www.sintef.no