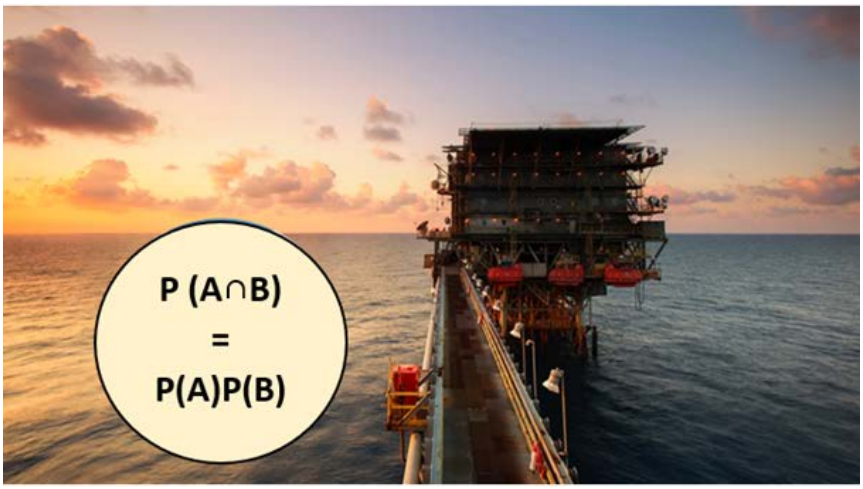


Rapport

IKT-sikkerhet og uavhengighet

Forfattere):
Tor Onshus, Lars Bodsberg, Stein Hauge, Martin Gilje Jaatun, Mary Ann Lundteigen, Thor Myklebust, Maria Vatshaug Ottermo, Stig Petersen, Egil Wille

Rapportnummer:
2021:01387 - Åpen

Oppdragsgiver:
Petroleumstilsynet

SINTEF Digital
Postadresse:
Postboks 4760 Torgarden
7465 Trondheim

Sentralbord: 40005100

info@sintef.no

Foretaksregister:
NO 919 303 808 MVA

Rapport

IKT-sikkerhet og uavhengighet

EMNEORD
Digitalisering
Sikkerhetssystemer
Cybersikkerhet
Regelverk

VERSJON
02

DATO
2021-12-17

FORFATTER(E)
Tor Onshus, Lars Bodsberg, Stein Hauge, Martin Gilje Jaatun, Mary Ann Lundteigen, Thor Myklebust, Maria Vatshaug Ottermo, Stig Petersen, Egil Wille

OPPDRAGSGIVER(E)
Petroleumstilsynet

OPPDRAGSGIVERS REFERANSE
Arne Halvor Embergsrud

PROSJEKTNUMMER
102025521

ANTALL SIDER
61

SAMMENDRAG
Petroleumstilsynets regelverk har krav om uavhengighet mellom systemer både i styringsforskriften og innretningsforskriften. Dessuten finnes det tilsvarende krav i for eksempel IEC 61508 og IEC 61511 som pekes på i veiledningene til forskriftene. Denne rapporten vurderer hvorvidt disse kravene blir utfordret med mulige framtidige tekniske løsninger og hvordan en kan bidra til at kravene oppfylles.

Vi har her fokus på storulykker og ikke avhengigheter som kan føre til tapt produksjon. Ved vurdering av IKT-sikkerhet i industrielle IKT-systemer (OT-systemer) er vårt fokus på tilsiktede hendelser og vi ser spesielt på tilgjengelighet og integritet.

UTARBEIDET AV
Tor Onshus

SIGNATUR
Tor Onshus
Tor Onshus (15. Dec. 2021 16:59 GMT+1)

KONTROLLERT AV
Knut Steinar Bjørkevoll

SIGNATUR
Knut S. Bjørkevoll
Knut S. Bjørkevoll (15. Dec. 2021 21:26 GMT+1)

GODKJENT AV
Anita Øren

SIGNATUR
Anita Øren
Anita Øren (16. Dec. 2021 09:14 GMT+1)

RAPPORT NR.
2021:01387

ISBN
978-82-14-07697-4

GRADERING
Åpen

GRADERING DENNE SIDE
Åpen

Historikk

VERSJON	DATO	VERSJONSBESKRIVELSE
01	2021-11-19	Utkast til Ptil for kommentarer
02	2021-12-13	Sluttrapport

Innholdsfortegnelse

Sammendrag **5**

Executive Summary **7**

1 Innledning **9**

1.1 Mål og hensikt 9

1.2 Begrensninger 9

1.3 Begreper, definisjoner og forkortelser 10

1.3.1 Begreper og definisjoner 10

1.3.2 Forkortelser 14

1.4 Rapportstruktur 15

2 Dagens status **16**

2.1 Bakgrunn for oppdraget 16

2.2 Hva menes med uavhengighet 16

2.3 Modellering og analyser av avhengigheter 17

2.4 Funksjonell sikkerhet og IKT-sikkerhet – utilsiktet og tilsiktet risikoelement 18

2.5 Dagens systemer og løsninger 19

3 Standarder og retningslinjer og krav til uavhengighet **23**

3.1 IEC 62443 23

3.2 IEC 61508 26

3.3 IEC 61511 26

3.4 NORSOK I-002 27

3.5 DNV-RP-G108 28

3.6 Norsk olje og gass 070, Appendix G 29

3.7 NSMs Grunnprinsipper for IKT-sikkerhet 29

4 Teknologiske trender, nye IKT-systemer og IIoT-løsninger **30**

4.1 Datadioder 30

4.2 Industri 4.0 31

4.2.1 Industri 4.0 og petroleumsindustrien 31

4.2.2 OPC UA 32

4.2.3 NAMUR Open Architecture 33

4.3 5G 34

4.3.1 Arkitektur og teknologi 34

4.3.2 Potensielle bruksområder for 5G 34

4.3.3 Integrasjon, driftsmodeller og uavhengighet 35

4.4 Kantenheter 37

4.5 Håndholdte enheter 39
4.6 Ekstern tilgang til OT-systemene 40

5 Tiltak for å motstå cyberangrep 42
5.1 Kommunikasjon for funksjonell sikkerhet 42
5.2 Kryptering 43
5.3 Digitale signaturer og meldingsautentiseringskoder (MAC) 44
5.4 Egenskaper til soner og tunneler 45
5.5 OPC UA 46
5.5.1 PubSub som innfallsvinkel til datadioder 46
5.6 Zero trust versus skallsikring 48

6 Mulige avhengigheter og negative påvirkninger 49
6.1 Hva legger vi i negativ påvirkning? 49
6.2 Nye avhengigheter og koblinger 49
6.3 I hvilken grad vil Ptils krav til uavhengighet være oppfylt? 50

7 Behov for endringer i Petroleumtilsynets regelverk 52
7.1 Bakgrunn 52
7.2 Diskusjon rundt mulige justeringer av regelverket 52
7.2.1 Forslag vedrørende Ptils Styringsforskrift § 5 Barrierer 53
7.2.2 Forslag vedrørende henvisninger i Ptils Innretningsforskrift §32-34 53
7.2.3 Forslag vedørende Ptils Barrierenotat 2017 54

8 Hovedkonklusjoner og anbefalinger 55
8.1 Anbefalinger til næringen 55
8.2 Anbefalinger til Ptil 57
8.3 Behov for kunnskapsinnhenting 58

Referanser 59

Sammendrag

Petroleumstilsynets regelverk har krav om uavhengighet mellom systemer både i styringsforskriften og innretningsforskriften. Dessuten finnes det tilsvarende krav i for eksempel IEC 61508 og IEC 61511 som refereres til i veiledningene til forskriftene. Denne rapporten vurderer hvorvidt disse kravene blir utfordret med mulige framtidige tekniske løsninger og hvordan en kan bidra til at kravene oppfylles. Vi har her fokus på avhengigheter relatert til storulykker og ikke avhengigheter som kan føre til tapt produksjon. Ved vurdering av IKT-sikkerhet i industrielle IKT-systemer (OT-systemer) er vårt fokus på tilsiktede hendelser, og vi ser spesielt på sikkerhet, tilgjengelighet og integritet.

Et hovedspørsmål som vi har forsøkt å finne svar på, er om kravene til uavhengighet er oppfylt i dag og hvordan utviklingen framover kan bli. Vi har inntrykk av at det mangler systematiske analyser med målrettete vurdereringer av avhengigheter og basert på det må en kunne si at uavhengighet ikke er godt nok dokumentert.

En ser at utviklingen med økt informasjonsoverføring fra hav til land og færre operatører på installasjonene fortsetter og at dette kanskje er en forutsetning for at olje og gassindustrien skal overleve. Det er også et generelt krav fra operatørselskaper at stort sett all informasjon skal hentes ut fra alle systemer på installasjonene så den kan analyseres på land. En viktig utfordring blir da sikring og beskyttelse av OT-systemer mot cyberangrep så disse ikke kan føre til negativ påvirkning og ulykker på innretninger.

En ser tilløp til at den lagdelte Purdue-modellen som blant annet skal beskytte OT-systemene mot uønsket påvirkning, brytes ned, og at en i stedet får en rekke forbindelser på kryss og tvers mellom systemene og mot omgivelsene. Hver forbindelse behøver ikke være et problem i seg selv, men sikring er ferskvare og mange forbindelser kombinert med felles komponenter og tjenester kan gi store utfordringer.

Å opprettholde uavhengighet vil også bero på hvordan man ivaretar IKT-sikkerhet og løsninger for IT/OT som har mange felles funksjoner og systemer som må sikres. Eksisterende instrumenterte sikkerhetssystemer (SIS) og prosesskontrollsystemer er ikke egnet/laget for å kunne beskytte mot uventet datatrafikk og ondsinnede handlinger. Hvis utviklingen med økt kompleksitet fortsetter, blir utfordringene med å sikre disse systemene stadig større, da antall angrepspunkter og feilmekanismer øker.

Dagens systemer for administrasjon av feltutstyr, 5G og nye kantenheter og IIoT-enheter kan (hvis en ikke iverksetter mottiltak) gis tilgang direkte ned i OT-systemene uten autentisering og arbeidstillatelser for å spare tid og byråkrati. Dette øker selvsagt effektiviteten, men kan også gi uønsket tilgang og påvirkning fra aktører med onde hensikter.

Det finnes mange standarder og initiativ for å sikre anleggene mot uønsket påvirkning via kommunikasjon, men feltet er fortsatt umodent. Likevel virker det som ulike deler av standardserien IEC 62443 "Security for industrial automation and control systems" blir brukt av de store aktørene. IEC 62443-serien er svært omfattende og inneholder en rekke (del)standarder, tekniske spesifikasjoner og tekniske rapporter. De ulike delene foreligger dessuten i varierende grad i oppdaterte eller offisielle versjoner, hvor for eksempel del 1-1 og 2-1 er over 10 år gamle. Det kan være utfordrende og ressurskrevende å skaffe seg oversikt, og for næringen som helhet vil det derfor vært en stor fordel med en oppdatert retningslinje for implementering av standarden.

Vi anbefaler at Petroleumstilsynet ser på hvorvidt styringsforskriftens §5 og innretningsforskriftens §§ 32-34 med tilhørende veiledninger, kan justeres for å sette økt søkelys på viktigheten av IKT-barrierer. Vi ser et fremtidig behov for at definisjonen av barrierer utvides fra å ha kontroll på energien til også å omfatte

informasjonsområdet, herunder at beskyttelse mot uønsket dataflyt og påfølgende negativ påvirkning behandles som en barrierefunksjon.

Til tross for at sentrale deler av IEC 62443 ikke foreligger i oppdaterte versjoner, anbefaler vi at Ptil henviser til (deler av) IEC 62443-serien i veiledningen til §§32-34 i innretningsforskriften. Spesielt delstandard 3-3 inneholder flere systemkrav (og delstandard 4-2 tilsvarende komponentkrav) som hvis implementert, kan bidra til uavhengighet.

Executive Summary

The Petroleum Safety Authority (PSA) Norway's management regulations and facilities regulations both have a requirement for independence between systems. In addition, there are similar requirements in e.g. IEC 61508 and IEC 61511 that are referred to in the guidelines to the regulations. This report assesses whether these requirements are challenged with possible future technical solutions and how these requirements can be met. We focus on major accident risk and not dependencies that can lead to lost production. When assessing industrial ICT systems (OT systems), our focus is on intentional acts and events, and we look specifically at functional safety (including availability and integrity).

Key questions are how the industry complies with the requirements for independence and how this may develop in the future. Our impression is that systematic analyses that assess dependencies are generally missing and based on this it is fair to conclude that independence is not sufficiently documented.

The development with reduced manning on the offshore facilities and increased information transfer from offshore to land continues and may also be a prerequisite for the future survival of the oil and gas industry. A general requirement from the operators has emerged that all relevant information from offshore located systems should be made available so that it can be analyzed on land. This represents a challenge to safety to avoid negative impacts and potential accidents on the facilities.

One sees that the layered Purdue model, which is intended, among other things, to protect the OT systems from unwanted influences, is undermined, and that many new connections between the OT systems and the surroundings arise. Each connection is not necessarily a problem, but in total they may represent a challenge to functional safety and security.

Maintaining independence will also depend on how ICT security is ensured, and solutions for IT/OT usually have many common functions and systems that need to be safeguarded. Existing instrumented safety systems (SIS) and process control systems must be protected from digital attacks, as they are often not suitably designed to protect against unexpected data traffic and malicious actions. If the development with increased complexity continues, the challenges of securing these systems will increase, as the number of attack points and error mechanisms increases.

Both today's systems for managing field equipment, 5G and new edge and IIoT devices can, unless protected against, be granted access directly into OT systems without authentication and work permits to save time and bureaucracy. This, of course, increases efficiency, but can also represent undesirable access and influence from actors with malicious intents.

There are many standards and initiatives dealing with the protection of OT systems against undesirable influence via communication, but the field remains immature. Nevertheless, it seems that different parts of the standard series IEC 62443 "Security for industrial automation and control systems" are used by major actors. The IEC 62443 series is very comprehensive and contains several parts, including technical specifications and technical reports. The different parts are to a varying degree updated or available in official versions, and e.g. substandard 1-1 and 2-1 are over 10 years old. It can be challenging and resource-demanding to obtain an overview, hence updated guidance on how to implement the standard will be of great benefit to the industry.

We recommend the PSA Norway to consider adjusting section 5 of the management regulations and section 32-34 of the facilities regulations with associated guidelines, to highlight the importance of ICT barriers. We see an emerging need for the definition of barriers to be expanded from controlling energy to also

encompass the information area, e.g. that protection against unwanted data flow and subsequent negative impacts is treated as a barrier function.

Even though key parts of IEC 62443 are not available in updated versions, we recommend that the PSA Norway refers to (parts of) the IEC 62443 series in the guidelines to sections 32 to 34 of the facility regulations. In particular, IEC 62443-3-3 contains several system requirements (and substandard 4-2 corresponding component requirements) that, if implemented, can contribute to independence.

1 Innledning

1.1 Mål og hensikt

Oppdragets overordnede mål er:

> Kartlegge og vurdere hvordan næringen ved design og levering av nye IKT-systemer og IIoT-løsninger ivaretar Petroleumstilsynets (Ptils) krav om at prosess-sikring- og sikkerhetssystemene skal utføre tiltenkte funksjoner uavhengig av andre systemer og ikke bli påvirket negativt.

Oppdragets delmål er:

a. Kartlegg hvordan prosessikring- og sikkerhetssystemene kan påvirkes negativt av hverandre og av andre IKT-systemer og IIoT-løsninger, inklusive koblinger til leverandørbaserte skyløsninger utenfor OT-domenet,
b. Vurder i hvilken grad Ptils krav til uavhengighet vil være oppfylt
c. Foreslå tiltak som kan sikre at prosessikring- og sikkerhetssystemene ikke påvirkes negativt av andre IKT-systemer og IIoT-løsninger
d. Vurder om det er behov for endringer i krav til uavhengighet i Ptils regelverk og hvilke standarder som vises til i Ptils veiledninger.

Dette prosjektet er sentrert rundt §§32-34 i Ptils Innretningsforskrift [43], der det står:

> *"Systemet [herunder brann&gass, nødavstengning og prosessikring] skal kunne utføre tiltenkte funksjoner uavhengig av andre systemer"*

og i veiledningene:

> *"Systemet kan ha grensesnitt mot andre systemer dersom det ikke kan bli negativt påvirket som følge av systemsvikt, feil eller enkelthendelser i disse systemene."*

Prosjektet inngår i satsingen på IKT-sikkerhet i petroleumssektoren (2018-2021), hvor DNV og SINTEF har utarbeidet en rekke rapporter for Ptil som undersøker ulike sider av temaet IKT-sikkerhet i industrielle systemer [41]. Både litteraturstudier, intervjuer med aktører i næringen og med representanter fra andre sektorer og myndigheter er benyttet.

1.2 Begrensninger

I oppdraget vektlegges analyse av de nye IKT-systemene og IIoT-løsningene som er i ferd med å tas i bruk eller som på kort sikt (typisk 5-års perspektiv) vil kunne anvendes i norsk petroleumsvirksomhet.

Vi vurderer spesielt følgende krav i Ptils Innretningsforskrift § 34 Prosessikringssystem [43]

> *"Prosessikringssystemet skal kunne utføre tiltenkte funksjoner uavhengig av andre systemer, dvs. at prosessikringssystemet kommer i tillegg til systemer for styring og kontroll og andre sikkerhetssystemer og at prosessikringssystemet kan ha grensesnitt mot andre systemer dersom det ikke kan bli negativt påvirket som følge av systemsvikt, feil eller enkelthendelser i disse systemene"*

Denne paragrafen stiller også krav om at prosessikringen skal utformes med to uavhengige sikringsnivåer for beskyttelse av utstyr, dvs. at sikringsnivåene skal beskyttes mot avhengige feil, slik at en enkelt feil ikke medfører at begge sikringsnivåene svikter, samt at prosessikringssystemet skal utformes slik at det går til eller forblir i en sikker tilstand dersom det oppstår en feil som kan hindre systemet i å virke.

Kravene som regelverket i dag setter til uavhengighet, er på et funksjonelt og forholdsvis overordnet nivå. Vi vurderer om disse uavhengighetskravene kan konkretiseres og operasjonaliseres. I prosjektet vurderer vi spesielt mulige funksjonelle tilleggskrav som kan utfylle nåværende regelverk.

Vi legger vekt på:

- Helhetlig tilnærming til Ptils innretningsforskriften § 32-34, inklusive krav om at innretningen skal utformes med to uavhengige sikringsnivåer ("ingen enkelt feil") og forbli i en sikker tilstand ved feil.
- Potensielle utfordringer knyttet til sikkerhet fremfor produksjonsregularitet.
- "Løfte blikket" – hva kommer rundt "svingen" av nye systemer/løsninger de kommende fem år.
- Gå i dybden på forhold knyttet til nye IKT-systemer/IIOT-løsninger (eg. OPC Unified Architecture, NAMUR Open Architecture, 5G) fremfor velkjente utfordringer i eksisterende systemer/løsninger.
    - Hvordan nye IKT-systemer kan påvirke uavhengighet? (F.eks. å oppnå uavhengighet med ulik lokalisering av utstyr og systemer tones ned.)
    - Hvordan kompensere når eksisterende beskyttelse i lagdelt struktur fjernes ved "åpne/flate løsninger" (F.eks. behov for kvantesikker kryptering er ikke viktig i dagens systemer.)
- Vurdering av produksjonsinnretninger til havs.
- Overordnede anbefalinger til regelverksutvikling fremfor konkrete forslag til tekst i regelverket.
- Utfordringer med å holde systemene atskilte ved flytting av deler av styring og kontroll inn til land (eller til en annen innretning).

Følgende to hovedtema behandles

1. Nye IKT-systemer og IIoT-løsninger. (Hva vil leveres de neste 5 år?)
2. Vurdering av "security". (Hvordan ivareta "security" i morgendagens IKT-systemer/løsninger?)

Med IKT-systemer og IIoT løsninger mener vi nye systemer/løsninger som kan tas i bruk de kommende fem år. Når ikke annet er spesielt nevnt, vil begrepet IKT-systemer omfatte både systemer og løsninger i denne rapporten.

1.3 Begreper, definisjoner og forkortelser

1.3.1 Begreper og definisjoner

I Tabell 1 er begrep i internasjonale standarder forsøkt tilpasset norske begrep. Det er spesielt begrepet sikkerhet som skaper utfordringer siden dette i daglig tale brukes om både de to engelske begrepene ”safety" og "security".

Tabell 1: Sentrale begreper og definisjoner som benyttes i rapporten

Begrep	Definisjon/beskrivelse	Referanse
Autentisering	Tiltak for å fastslå gyldigheten av en overføring, melding eller opphavsmann, eller et middel for å bekrefte en persons autorisasjon til å motta bestemte kategorier av informasjon	IEC 62443-1-1 [26]
Barriere	Tiltak som har til hensikt og funksjon enten å forhindre et konkret hendelsesforløp i å inntreffe, eller påvirke et hendelsesforløp i en tilsiktet retning ved å begrense skader og/eller tap. Funksjonen til disse barrierene ivaretas av tekniske, operasjonelle og organisatoriske elementer enkeltvis eller samlet	Ptil, Ord og uttrykk [46]
"Black channel"	Deler av kommunikasjonskanalen er ikke designet, utviklet eller validert i henhold til IEC 61508, bare endepunktene (sender og mottaker).	IEC 61784-3 [17]
Cybersikkerhet	Beskyttelse av IKT-systemer mot IKT-angrep som kan ramme IKT-systemers konfidensialitet, integritet og tilgjengelighet. (Merk: I noen standarder inkluderer begrepet også utilsiktede hendelser)	IEC 62443-1-2 [26]
Datadiode (eng: "Unidirectional gateway or data diode")	Nettverkskomponent som garanterer at når den er koblet mellom nettverk A og nettverk B, så kan data kun flyte fra A til B, men ikke fra B til A.	Jones et al [19]
Digital signatur	En mekanisme for å kunne verifisere avsender av en melding, samt avdekke om meldingen har blitt endret urettmessig etter sending fra avsender. Meldingen signeres vha. en privat nøkkel (kun kjent for avsender), men kan verifiseres av den korresponderende offentlige nøkkelen (kjent for alle). Brukes vanligvis med en PKI.	SINTEF [55]
Fare	Mulig forhold som kan føre til en uønsket hendelse	NS 5830:2012 [37]
Funksjonell sikkerhet (eng. "functional safety")	Vi har i denne rapporten tolket dette som beskyttelse av menneskers liv og helse, miljø og materielle verdier gjennom OT-systemer "Part of the overall safety relating to the process and the BPCS which depends on the correct functioning of the SIS and other protection layers"	IEC 61511-1 [16]
Hash	En kryptografisk sjekksum som genererer et resultat av fast lengde basert på en variabel datamengde som mates inn. Skal være beregningsmessig ugjennomførbart ("umulig") å finne enten a) et dataobjekt som kan generere et forhåndsoppgitt hashresultat (enveis-egenskapen), eller b) finne to dataobjekter som genererer samme hash (kollisjonsfrihet-egenskapen).	SINTEF [55]
IKT-system	Alle systemer som utfører sin funksjon gjennom å sende, motta, lagre, prosessere og konvertere informasjon fra andre systemer	Riksrevisjonen [49]
IKT-angrep	Handlinger som utføres for å skade eller påvirke et IKT-system.	Riksrevisjonen [49]

Begrep	Definisjon/beskrivelse	Referanse
IKT-hendelse	En hendelse som kan ramme IKT-systemers konfidensialitet, integritet og tilgjengelighet. IKT-hendelser omfatter både tilsiktede handlinger og utilsiktede hendelser	Riksrevisjonen [49]
IKT-hendelseshåndtering	Aktiviteter som utføres for å stanse eller begrense skade på IKT-systemer og nettverksressurser som er rammet av sikkerhetstruende hendelser eller handlinger, og for deretter å gjenopprette en sikker tilstand.	Riksrevisjonen [49]
IKT-sikkerhet	Beskyttelse av IKT-systemene, samvirket mellom systemene, tjenestene som leveres av systemene, eller informasjon som behandles i systemene	NOU 2018:14 [36]
Informasjonssikkerhet	Handler om å sikre at informasjon ikke blir kjent for uvedkommende (konfidensialitet), ikke blir endret utilsiktet eller av uvedkommende (integritet) og er tilgjengelig ved behov (tilgjengelighet). Termen informasjonssikkerhet brukes ofte synonymt med IKT-sikkerhet. Informasjonssikkerhet omfatter også informasjon som ikke utveksles og lagres i IKT-systemer eller elektronisk på annen måte.	Riksrevisjonen [49]
Industriell IKT-system (eng. "Industrial Automation and Control System – IACS")	Samling av personell, maskinvare, programvare, prosedyrer, prosesser og retningslinjer som kan påvirke sikker drift	IEC 62443-1-1 [26]
Integritet (av IKT-system)	At informasjonen som behandles i systemene, og tjenestene tilknyttet systemene ikke endres uautorisert	IEC 62443-3-1 [26]
Kommunikasjonskanal (eng. "Channel")	Spesifikk kommunikasjonsforbindelse i en kommunikasjonstunnel ("Conduit")	IEC 62443-1-1 [26]
Klient	Enhet eller applikasjon som mottar eller ber om tjenester eller informasjon fra en serverapplikasjon	IEC 62443-1-1 [26]
Konfidensialitet (av IKT-system)	At informasjonen kun er tilgjengelige for prosesser, enheter og personer som rettmessig skal ha tilgang.	IEC 62443-1-1 [26]
Meldingsautentiserings kode (MAC)	Kalles også en nøklet hashfunksjon, og brukes typisk mellom to parter som deler en hemmelig nøkkel, for å autentisere informasjon som utveksles mellom de to partene.	Cheswick [5]
Node	Enhet i et IKT-nettverk. Det kan være for eksempel en ruter, en server eller en svitsj	IEC 60050 [14]
Profil (feltbuss)	Definerer funksjonell sikkerhet for en gitt feltbussprotokoll. De fleste feltbusser har sin egen profil for funksjonell sikkerhet, f.eks. PROFISafe for PROFIBUS og PROFINET.	IEC 61784-3 [17]
"Protection profile"	Sett med sikkerhetskrav som er uavhengig av implementering og kan anvendes for evaluering av spesifikke brukerbehov.	IEC 62443-1-2 [26]
Proxy	Prosess som opptrer "på vegne av" en annen prosess, gjerne i en brannmur. Feks. hvis man har behov for å kontakte en epost-tjener på innsiden av en brannmur, vil man ofte koble seg opp mot en proxy på brannmuren som så vil videreformidle meldinger. En proxy vil typisk være enklere enn tjenesten den representerer, og følgelig enklere å evaluere/sikre.	FFI [11]
Risiko	Med risiko menes konsekvensene av virksomheten med tilhørende usikkerhet. Begrepet "konsekvensene" er her brukt som et samlebegrep for alle de konsekvensene som virksomheten potensielt kan gi. Begrepet er ikke kun avgrenset	Ptil, Ord og uttrykk [46]

Begrep	Definisjon/beskrivelse	Referanse
	til de endelige konsekvensene av virksomheten i form av eksempelvis skade på eller tap av menneskers liv og helse, miljø og materielle verdier, men inkluderer også tilstander og hendelser som kan gi eller føre til denne typen konsekvenser.	
Ruter	Funksjonell enhet som etablerer en sti gjennom ett eller flere datanettverk og videresender pakker	IEC 60050 [14]
"Safety"	Frihet fra uakseptabel risiko	IEC 62443-1-1 [26]
"Security"	Tiltak for å beskytte et system	IEC 62443-1-1 [26]
Server (tjener)	Funksjonell enhet som tilbyr tjenester til arbeidsstasjoner, til personlige datamaskiner eller til andre funksjonelle enheter i et datanettverk	IEC 60050 [14]
Sone (eng. "Zone")	Gruppering av logiske eller fysiske enheter ut ifra risiko, kritikalitet, funksjon, plassering, tilgang eller andre kriterier. Et system kan deles inn i flere soner.	IEC 62443-3-2 [26]
System til/under vurdering (eng. "System Under Consideration" - SUC)	Definert samling av IACS-komponenter (inkludert relevant nettverksinfrastruktur) som til sammen utgjør en automasjonsløsning. SUC består av en eller flere soner, samt relaterte tunneler. Alle enheter som inngår i SUC tilhører enten en sone eller en tunnel.	IEC 62443-3-2 [26]
Svitsj	Apparat som mottar signaler fra en rekke inngående linjer og sender dem videre etter bestemte regler. (Svitsjer i telefonnettet kalles vanligvis telefonsentraler)	IEC 60050 [14]
Sårbarhet	Et uttrykk for de problemer et system får med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet	NOU 2000:24 [35]
Sikringstiltak	Tiltak for å redusere risiko forbundet med tilsiktede uønskede handlinger	NS 5830:2012 [37]
Tilgjengelighet (av IKT-system)	IKT-systemets evne til å være i en tilstand til å utføre en nødvendig funksjon under gitte forhold i et gitt øyeblikk eller over et gitt tidsintervall, forutsatt at de nødvendige eksterne ressursene er til stede	IEC 62443-1-1 [34]
Trussel	Mulig uønsket handling som kan gi en negativ konsekvens for en entitets sikkerhet	NS 5830:2012 [37]
Tunnel (eng. "Conduit")	Logisk gruppering av kommunikasjonskanaler, med felles sikkerhetskrav, som forbinder to eller flere soner.	IEC 62443-1-1 [26]
Uønsket hendelse	Hendelse som kan usette en verdi for uønsket påvirkning og medføre en negativ konsekvens for den som eier, forvalter eller drar fordel av en materiell eller immateriell ressurs.	NS 5830:2012 [37]

1.3.2 Forkortelser

Forkortelser som er benyttet i rapporten, er vist i Tabell 2.

Tabell 2: Forkortelser som benyttes i rapporten

Forkortelse	Beskrivelse
AAS	Asset Administration Shell
BPCS/PCS	Basic Process Control System/Process Control System
EUC	Equipment under control
FR	Foundational Requirements
HMAC	Hash-Based Message Authentication Code - Meldingsautentiseringskode som er implementert ved hjelp av en kryptografisk hash-funksjon etter et bestemt mønster.
IACS	Industrial Automation and Control Systems – Industriell IKT-system
IEC	International Electrotechnical Commission
IKT	Informasjons- og kommunikasjonsteknologi
IIoT	Industrial Internet of Things
IoT	Internet of Things
IPL	Independent Protection Layers
IT	Informasjonsteknologi
LOPA	Layer of Protection Analysis
MAC	Meldingsautentiseringskode
ML	Maturity Level
MTP	Modular Type Package
NEK	Norsk elektroteknisk komite
NOA	Namur Open Architecture
NORSOK	Norsk Sokkels Konkurranseposisjon
NOU	Norges Offentlige Utredninger
NS	Norsk Standard
NSM	Nasjonal sikkerhetsmyndighet
OPA	Open Process Automation
OPC	Open Platform Communication
OPC UA	OPC Unified Architecture.
OT	Operasjonell teknologi
PCS	Process Control System
PKI	Public Key Intrastructure
PFD	Probability of Failure on Demand
Ptil	Petroleumstilsynet
RAMI 4.0	Reference Architectural Model Industrie 4.0
RE	Requirement Enhancement
SAS	Safety and Automation System – sikkerhets- og automasjonssystem
SIS	Sikkerhetsinstrumenterte systemer
SL	Security Level
SPR	Security Protection Rating
SR	System Requirement
UDP	User Datagram Protocol

1.4 Rapportstruktur

Kapittel 2 gir bakgrunn for oppdraget, hva som menes med uavhengighet og hvordan man kan modellere uavhengighet. I kapitlet illustreres sammenheng mellom funksjonell sikkerhet og IKT-sikkerhet og hvordan disse attributtene kan påvirkes av både utilsiktede og tilsiktede hendelser. Til slutt gis det eksempel på typiske sammenhenger mellom kontroll- og sikkerhetssystemer (OT-systemer) i petroleumsvirksomheten på norsk sokkel.

Kapittel 3 oppsummer krav til uavhengighet i relevante standarder og retningslinjer

Kapittel 4 gir en vurdering av mulige nye avhengigheter ved implementering av nye IKT-systemer og løsninger, inklusive økt bruk av 5G. Dette kapitlet er basert på intervju med selskaper, litteraturgjennomgang og SINTEFs erfaring og kompetanse innen OT-systemer.

Kapittel 5 gir en vurdering av mulige tiltak mot cyberangrep som kan påvirke kritiske funksjoner i OT-systemer

Kapittel 6 diskuterer hvordan nye løsninger kan medføre mulige avhengigheter og negative påvirkning og hvorvidt Ptil sine krav til uavhengighet kan sies å være oppfylt eller ikke.

Kapittel 7 diskuterer hvorvidt Ptil sitt regelverk bør oppdateres i forhold til oppdaterte standarder og retningslinjer for IKT-sikkerhet

Kapittel 8 oppsummerer SINTEFs anbefalinger til tiltak for næringen og Ptil, samt behov for videre arbeid med kunnskapsinnhenting.

2 Dagens status

2.1 Bakgrunn for oppdraget

Innretningers OT-systemer, som tidligere var adskilt fra omverdenen, moderniseres og blir stadig mer komplekse og sammenkoblet med IT-systemer. Dette åpner opp for mer helhetlige løsninger, inkludert styring og overvåking fra land hvor OT-systemer har flere tilkoblingspunkter mot selskapets IT-systemer og forlengelser til eksterne nettverk som skyløsninger via internett. Dette betyr at det tradisjonelle skillet mellom IT- systemer og OT-systemer utfordres. IT-utstyr blir i økende grad også brukt for å ivareta OT-funksjoner. Eksempler er overvåknings-, vedlikeholds- og konfigurasjonssystemer for feltinstrumenter som tradisjonelt har vært sett på som IT-systemer siden de ikke direkte påvirker produksjonen.

Den økte kompleksiteten i IKT-systemer medfører at nye avhengigheter introduseres, og at systemene derfor blir tettere koblet. Dette kan medføre at anleggene blir vanskeligere å forstå, operere og ikke minst å vedlikeholde, og at det i nødssituasjoner kan være vanskeligere for operatøren å skaffe seg oversikt over situasjonen.

2.2 Hva menes med uavhengighet

Rent matematisk kan en si at to hendelser A og B er uavhengige dersom $P(B|A) = P(B)$. Dette betyr at hendelse B har samme sannsynlighet for å inntreffe uavhengig av hvorvidt A inntreffer eller ikke (og motsatt). Dette innebærer også at sannsynligheten for at to uavhengige hendelser inntreffer samtidig, er gitt av produktet av sannsynlighetene; $P(A \cap B) = P(A) \times P(B)$. Hvis dette ikke er tilfelle, er de to hendelsene avhengige.

Når en beregner feilsannsynligheten for sikkerhetsfunksjoner (PFD) brukes β-faktoren for å angi graden av avhengighet.

Ulike former for avhengighet kan opptre, og i dette prosjektet tar vi utgangspunkt i følgende kvalitative klassifisering av avhengighet (ikke nødvendigvis gjensidig utelukkende).

1. *Funksjonell avhengighet*, dvs. et system er avhengig av et annet system for å fungere.
2. *Kaskadefeil*, dvs. at feil i ett system oppstår pga. feil i et annet system – kan knyttes til feil både i maskinvare og programvare.
3. *Felles komponenter*, dvs. at samme komponent eller modul inngår i flere systemer – kan også innbefatte felles programvare.
4. *Felles lokalisering* som gjør at systemene kan utsettes for felles påvirkning fra enten omgivelser (ytre påvirkning) eller operativt personell (menneskelig påvirkning).

Enkelte avhengigheter mellom systemer og komponenter kan være åpenbare, slik som at en pumpe trenger kjøling for å fungere, eller at en har felles ESD og PSD ventil, mens andre avhengigheter – for eksempel felles nettverk eller samme programvare - *kan* være mer krevende å avdekke.

Avhengigheter skapes gjerne som en følge av teknologiutvikling, operasjonelle og økonomiske vurderinger, økt standardisering i prosjektene og ved oppgraderinger av programvare. Noen eksempler på koblinger og avhengigheter som i dag er mer eller mindre vanlige i norsk petroleumsindustri:

- Avhengigheter mellom prosesskontroll- og prosess-nedstengningssystemet (felles operatør-stasjoner og felles kommunikasjonskanaler for kontrollsystemet og sikkerhetssystemene).

- Avhengigheter mellom sikkerhetssystemer og andre sikkerhetskritiske systemer og funksjoner, slik som for eksempel mellom sjøvanns- og brannvannsystemet, mellom ballastkontroll og nødballastering og mellom HVAC og brann- & gass-systemet.
- Felles komponenter slik som for eksempel brannmurer, nettverkskomponenter, operatørstasjoner / HMI, konfigurasjonsverktøy, klokkesystem og domenekontrollere.

Ut fra et sikkerhetsperspektiv er avhengigheter generelt uønsket, for eksempel mellom sikkerhetssystemer og kontrollsystemet, men det kan være store designmessige, økonomiske og/eller andre fordeler med slike løsninger.

2.3 Modellering og analyser av avhengigheter

Generelt har dagens pålitelighets- og risikoanalyser en forholdsvis grov tilnærming når det gjelder å modellere avhengigheter. Dette er litt nærmere diskutert for noen sentrale analyser.

Kvantitative risikoanalyser av typen TRA (Total Risiko Analyse) innbefatter ofte alle fysiske områder og sikkerhetsfunksjoner på en innretning og dekker de fleste hendelseskategorier som bidrar til storulykkesrisikoen. Av natur er derfor disse analysene forholdsvis grove og tar sjelden for seg detaljer knyttet til kompleksitet og koblinger mellom systemene. For eksempel er felles komponenter, felles påvirkninger, kaskadefeil eller operasjonelle avhengigheter i begrenset grad analysert. For hydrokarbonhendelser starter analysen normalt ved en lekkasje, noe som betyr at kontrollsystemet og prosess-nedstengningssystemet i liten grad er analysert. Det benyttes stort sett generiske data, som impliserer at en antar en gjennomsnittlig ytelse på tekniske systemer og personell. Analyse av bakenforliggende feilårsaker og sammenhenger er derfor ofte begrenset. Potensielle avhengigheter og sårbarheter i for eksempel brukergrensesnitt og nettverk fanges derfor sjelden opp i risikoanalyser (eller andre analyser). Det bør herunder bemerkes at de overordnede risikoanalysenes primærformål er å verifisere en akseptabel total risiko, samt gi innspill til design på et forholdsvis grovt nivå, og at det derfor ikke er gitt at disse analysene er egnet til å gå i den slags detalj som vil kreves for å analysere mulige avhengigheter og koblinger.

Pålitelighetsanalyser, herunder SIL analyser, fokuserer normalt på enkeltsystemer, og går derfor ofte i større detalj på disse enn det som er tilfelle i en TRA (hvor pålitelighet av sikkerhetssystemer ofte kommer frem som greinsannsynligheter i et hendelsetre). Siden pålitelighetsanalyser normalt ser på enkeltsystemer, ligger det imidlertid i deres natur at koblinger mot- og avhengigheter av andre systemer fort kan falle utenfor "scope". De samme argumentene gjelder i stor grad også for FMECA analyser (Feilmode, Effekt og Kritikalitets-Analyser). Ikke dermed sagt at det er stor variasjon mellom analysene, og at det selvfølgelig finnes unntak fra disse generelle betraktningene.

LOPA ("Layer of Protection Analysis") er blitt en populær metode for å fastsette krav til risikoreduksjon og ytelseskrav for ulike lag av beskyttelse (sikkerhetsfunksjoner). På Norsk sokkel brukes metodikken ofte som et alternativ eller supplement til Norsk olje og gass 070 sin retningslinje for bruk av IEC 61508 og 61511 [33] (med deterministiske minimums SIL krav). Enkelt forklart er stegene i LOPA som følger:

1. Identifiser uønskede hendelser
2. For en gitt hendelse; identifiser hvor ofte en har bruk for beskyttelse for å unngå denne (behovsrate)
3. Identifiser uavhengige lag av beskyttelse for å unngå uønsket hendelse (IPL = Independent Protection Layers)
4. Bestem kravene til risikoreduksjon for de ulike IPL-ene som gir beskyttelse

Normalt henter disse analysene sine inputparametere/tallverdier fra forhåndsdefinerte tabeller og multipliseres deretter feilsannsynligheten (PFD) for de enkelte uavhengige beskyttelsene sammen for å estimere ytelsen av alle identifiserte beskyttelseslag sett i sammenheng.

Siden selve LOPA metodikken i begrenset grad legger opp til særskilte vurderinger av mulige avhengigheter, vil kvaliteten av eventuelle slike vurderinger i stor grad være avhengig av kompetansen til LOPA-teamet og selvfølgelig av avsatt tids- og ressursbruk for analysene. Noen andre hovedutfordringer knyttet til oppfølging av LOPA analyser er:

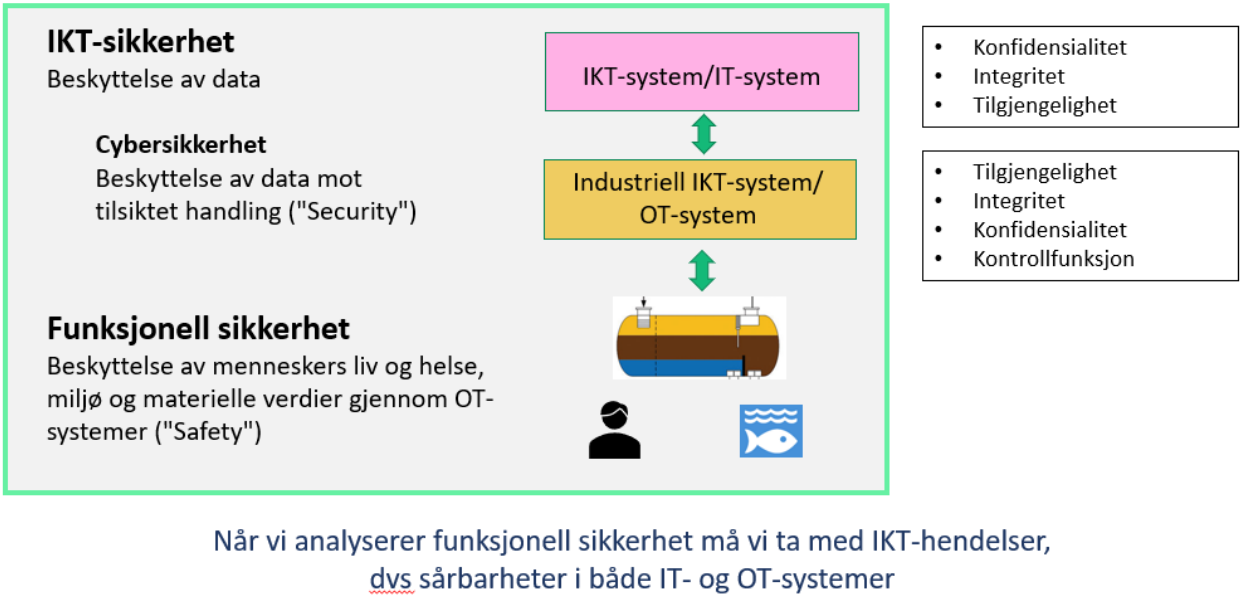
1. Det verifiseres ikke at behovsrate og pålitelighet av IPL-er har de verdier en henter fra tabellene
2. Det verifiseres ikke alltid i drift at IPL-ene blir vedlikeholdt slik at de opprettholder antatt ytelse gjennom hele levetiden
3. Det er svært krevende å verifisere at antagelser knyttet til godhet av manuell inngripen er oppfylt i drift
4. Det verifiseres ikke at beskyttelseslagene virkelig er uavhengige (at β=0)

Disse observasjonene støttes også av en artikkel skrevet av de som opprinnelig utviklet LOPA [3].

2.4 Funksjonell sikkerhet og IKT-sikkerhet – utilsiktet og tilsiktet risikoelement

Historisk sett har det i industrien vært et skille mellom administrative datasystemer (kontorstøttesystemer) som behandler data og informasjon (IT- og IKT-systemer) og datasystemer som overvåker og kontrollerer drift (OT-systemer) på produksjons- og boreinnretninger. I Ptils regelverk brukes IKT-systemer om systemer som ivaretar behovet for innhenting, bearbeiding og formidling av data og informasjon (Jf. styringsforskriften §15 [44]). Industrielle IKT-systemer brukes generelt om OT-systemer som kan styre endringer i fysisk utstyr og prosesser så som kontroll og overvåkingssystemer og sikkerhetssystemer. Ptils myndighetsområde i forhold til IKT-systemer er i hovedsak rettet mot industrielle IKT-systemer (OT-systemer), og spesielt systemer som har en barrierefunksjon (sikkerhetssystemer).

I Figur 1 er det forsøkt å vise hvorfor IKT-sikkerhet også er viktig for funksjonell sikkerhet og storulykker.

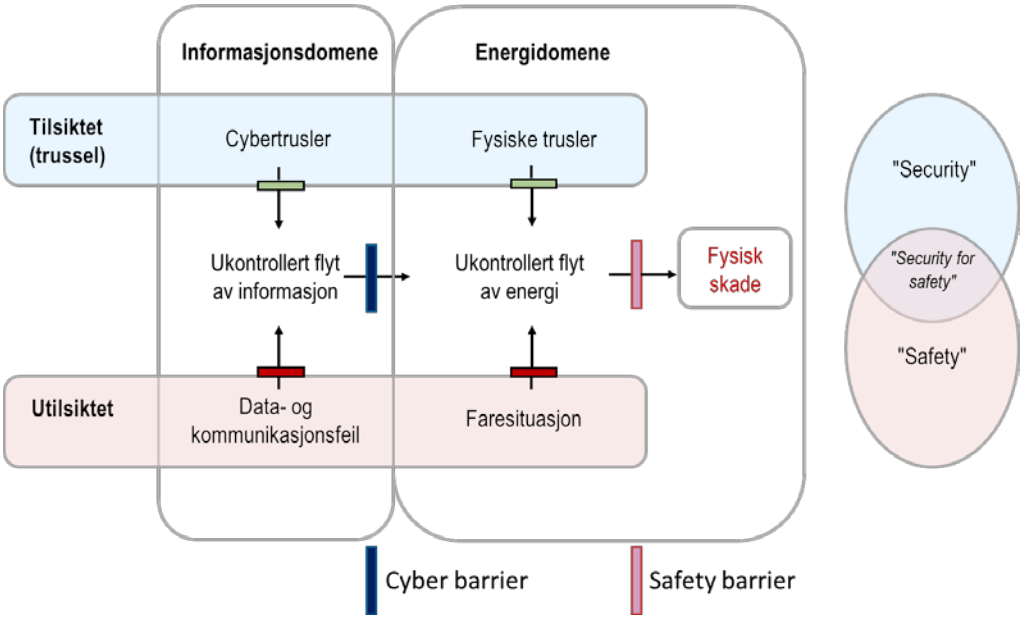


Figur 1 Funksjonell sikkerhet, cybersikkerhet og IKT-sikkerhet

Teknisk sikkerhet og herunder funksjonell sikkerhet har tradisjonelt vært knyttet til at en ønsker å beskytte mennesker og miljø mot ukontrollert flyt av energi som en følge av utilsiktede hendelser og feiltilstander. Teknisk sikkerhet omfatter mange ulike type tekniske barrierer, mens funksjonell sikkerhet normalt benyttes om barrierer som er implementert med elektriske/elektroniske og programmerbare systemer.

Figuren viser at funksjonell sikkerhet påvirkes av IKT-sikkerhet i både IT- og OT-system og at IKT-hendelser omfatter både tilsiktede handlinger og utilsiktede hendelser. Viktige attributter i IKT-system er konfidensialitet, integritet og tilgjengelighet. Konfidensialitet og beskyttelse av data og informasjon mot tilsiktede (ondsinnede) handlinger er ofte vektlagt i IT-systemer, mens tilgjengelighet knyttet til utilsiktede hendelser og feiltilstander er ofte vektlagt i OT-systemer.

Som en følge av nye koblinger og avhengigheter mellom ulike systemer vil energiområdet og informasjonsområde i økende grad gripe inn i hverandre. Dette er forsøkt illustrert i Figur 2 som viser hvordan tilsiktede og utilsiktede risikoelementer kan påvirke både informasjons- og energiområdet og hvordan disse to områdene påvirker hverandre. Dessuten illustrerer figuren tiltak (barrierer) som kan innføres for å hindre uønskede konsekvenser. Modellen er utgangspunktet for en ny metodikk kalt CyPHASS [12], [13] utviklet for å systematisk identifisere koblinger mellom potensielle ulykkessituasjoner og tap av kontroll med informasjonsdomenet.

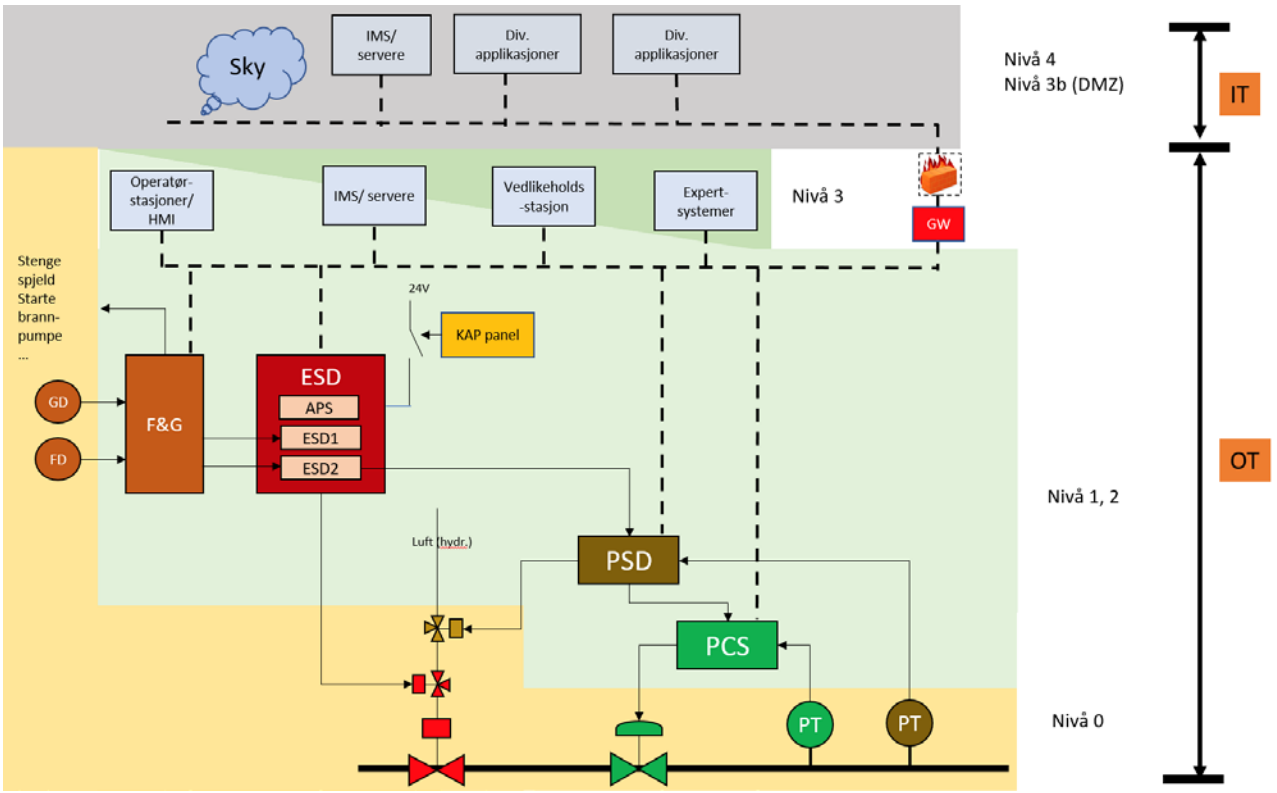


Figur 2 Utilsiktet og tilsiktede feil og hvordan de kan gi fysisk skade [Tilpasset fra [13]]

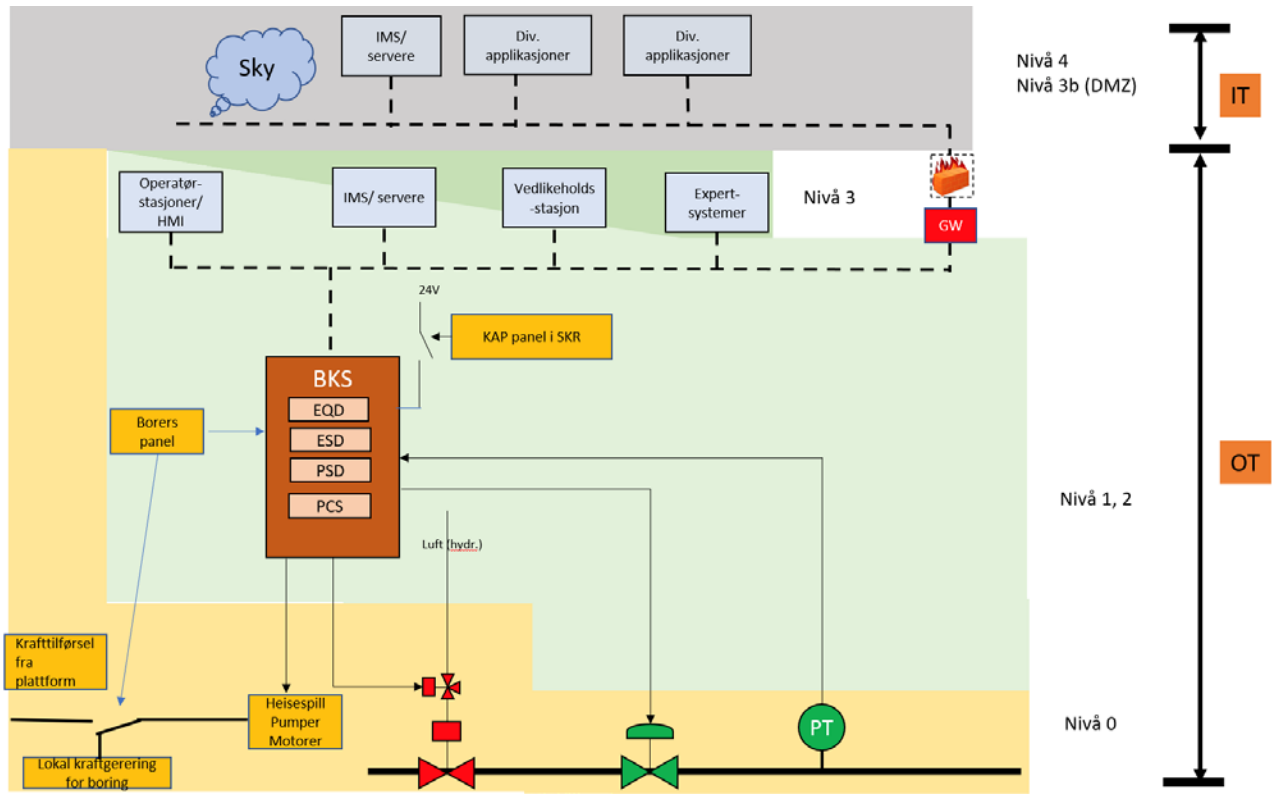
Det bør bemerkes at Ptil sitt regelverk og tradisjonell barrierestyring først og fremst har handlet om å ha kontroll på energien, og at informasjonsområdet har vært relevant i den grad det kan påvirke energiområdet negativt og ha potensiale til å medføre fysisk skade. Hvorvidt regelverket bør endres som en følge av tettere koblinger mellom de to områdene er nærmere diskutert i kapittel 7.

2.5 Dagens systemer og løsninger

Figur 3 og Figur 4 nedenfor viser typiske prinsippskisser for produksjonsinnretninger og borerigger samt eksempler på dataflyt mellom IT- og OT-systemer i henhold til Purdue-modellen som enkelte leverandører nå ønsker å utfordre. Det bemerkes at det kan være flere varianter av figurene for konkrete innretninger.



Figur 3 Prinsippskisse som viser sammenheng mellom industrielle IKT-systemer på produksjons-innretninger



Figur 4 Prinsippskisse som viser sammenheng mellom industrielle IKT-systemer på borerigger

På dagens innretninger finner man i hovedsak tre adskilte instrumenterte sikkerhetssystemer (SIS) i tillegg til kontrollsystemet. Disse fire systemene går under fellesbetegnelsen SAS ("Safety and Automation System"):

- Prosesskontrollsystem - "Process Control System" (PCS)
- Prosessnedstengningssystem - "Process ShutDown" (PSD)
- Brann- og gassdeteksjonssystem - "Fire and Gas" (F&G)
- Nødavstengningssystem - "Emergency ShutDown" (ESD)

I forbindelse med boring har en dessuten noen spesielle systemer og parametere utover de som er nevnt over, for eksempel:

- Utblåsningssikring (BOP)
- Sirkulasjon og vedlikehold av borevæske (Væskesøylen)
- Rotasjonshastighet for borekrona
- Trykk nede i brønnen

Utover SAS-løsningene, er det mange andre systemer som tilhører OT og som må håndteres på samme måte, uten at de er integrert i SAS. Noen eksempler kan være:

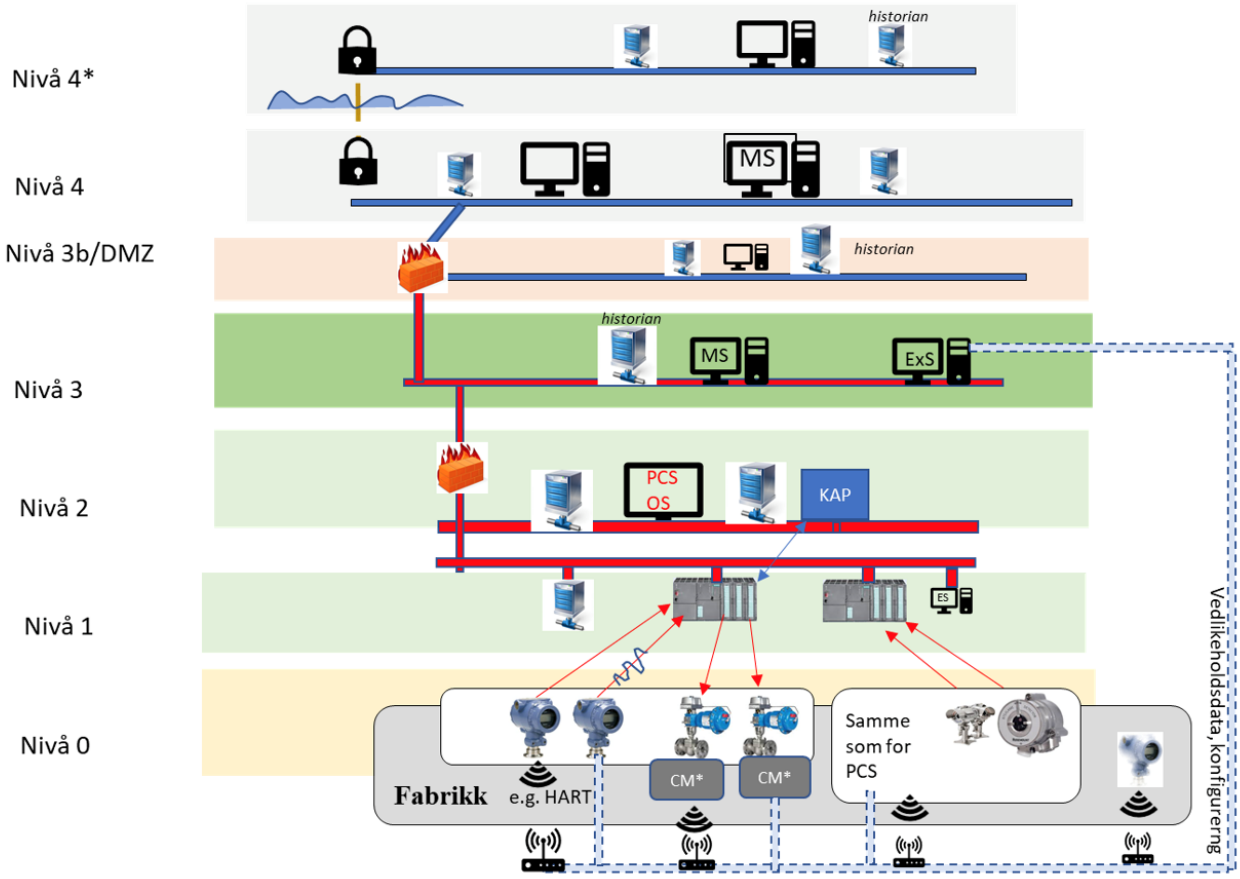
- Frittstående enheter uten kobling til SAS (Control Class 3, NORSOK I-002 [34])
- Fiskal måling
- Styresystemer brukt ved boring
- Kritiske marine systemer som posisjonering-, ballast- og lense-systemer

I henhold til definisjonen av IT/OT, vil overvåknings, vedlikeholds og konfigurasjonssystemer for felt-instrumenter ikke være en del av OT, da de ikke direkte påvirker prosess/produksjon.

Nivåinndeling for dagens løsninger og systemer er stort sett basert på prinsippene vist i Figur 5.

Grunnen til at en har denne lagdelingen med flere logiske nivå er blant annet at de systemene som i dag implementerer den (sikkerhets)funksjonaliteten som beskrevet over, ikke er laget for dagens trusselbilde og må beskyttes mot uønsket påvirkning utenfra.

Det finnes også løsninger der en forsøker å skille i et PCS-nett og et SIS-nett for å redusere muligheten for at feil på PCS siden skal påvirke SIS negativt. Dette kan begrense trafikken på SIS-nettet, men det er vanligvis fortsatt mange meldinger som må slippes gjennom, slik som til/fra det felles brukergrensesnittet og synkroniseringssignaler. I Norsk olje og gass 070, Appendix G finnes det en del betingelser for å kunne bruke et felles nett.



Figur 5 Prinsippskisse for dagens nivåinndeling for beskyttelse av OT-systemene

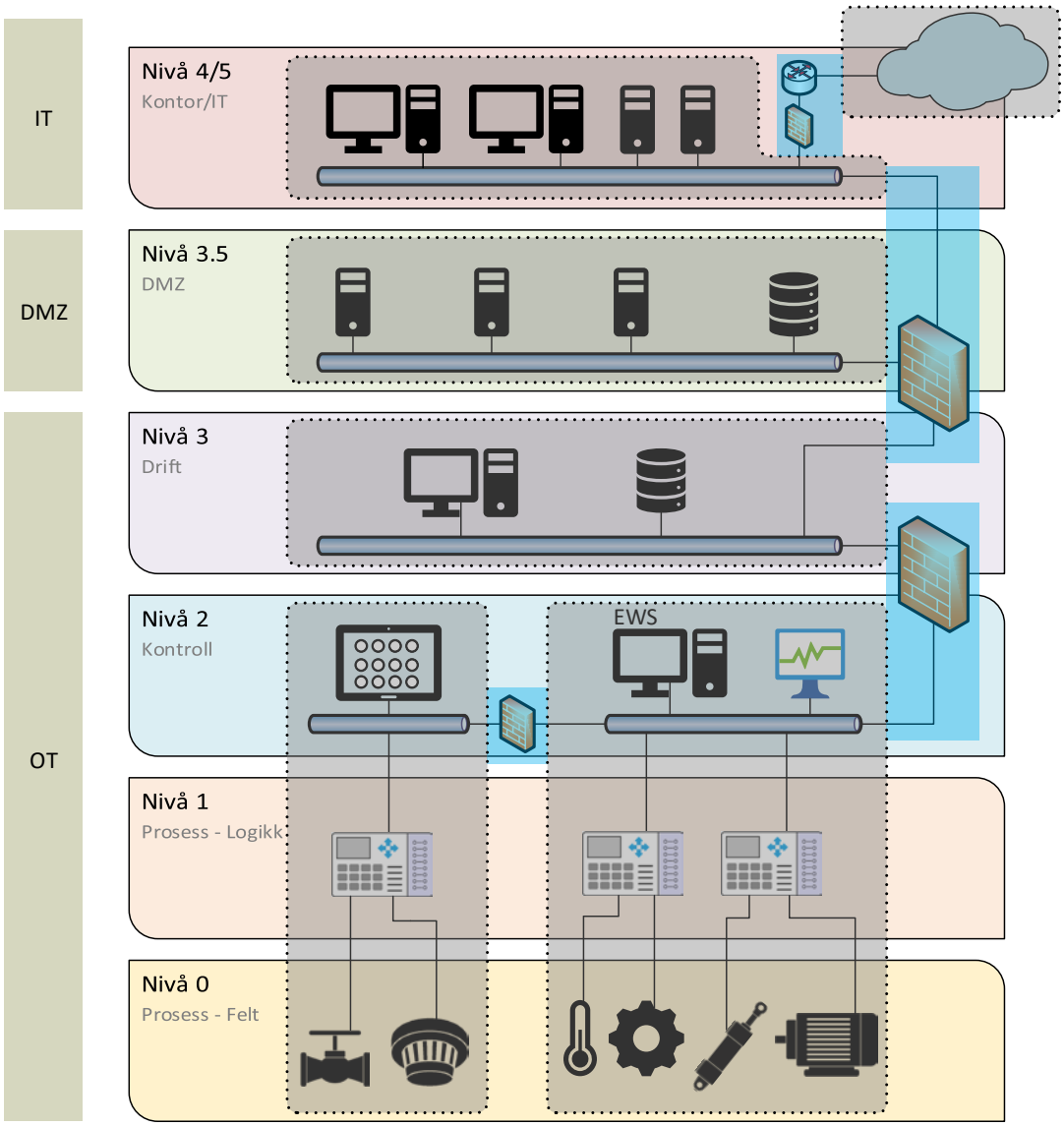
3 Standarder og retningslinjer og krav til uavhengighet

I det følgende diskuteres noen relevante standarder og retningslinjer, med vektlegging av krav til uavhengighet og forslag til løsninger utover det som står i Ptils regelverk.

3.1 IEC 62443

IEC 62443 [26] er en serie av standarder utviklet for å sikre industrielle kommunikasjonsnettverk og OT-systemer. 62443-serien blir av mange aktører ansett for å være et naturlig rammeverk å følge for å bygge og ivareta "security" i OT-systemer, og er blant annet sentral i DNVs klassenotasjon: Cyber Secure for maritime OT-systemer [8].

Et av de grunnleggende konseptene beskrevet i IEC 62443-3-2, er å dele systemer og nettverk inn i hensiktsmessige soner og tunneler ("zones" and "conduits"), for å gruppere funksjoner og enheter basert på kritikalitet, og for å avgrense/begrense konsekvensene av uønskede hendelser, se Figur 6. Videre vil soner og tunneler beskytte enheter og koblinger mellom dem mot uønsket påvirkning utenfra.



Figur 6 - Eksempel på nettverkstopologi med soner (grå) og tunneler (blå)

IEC 62443-serien legger opp til at man velger nettverkstopologi og sikkerhetsbarrierer basert på risikovurderinger, så graden av uavhengighet kan variere mellom forskjellige anvendelser/ tolkninger av 62443.

Et sentralt begrep i IEC 62443 er "Security Level" (SL). Konseptet fokuserer på at soner og tunneler skal graderes i ulike nivåer (SL1 - SL4), og er i IEC 62443-3-3 og IEC 62443-4-2 beskrevet som krav til henholdsvis systemer og komponenter som inngår i de ulike sonene. Basert på en risikovurdering representerer disse "security"-nivåene et rammeverk for å bestemme nødvendige beskyttelser og tiltak. Jo høyere SL, jo større vurdert risiko og jo høyere grad av beskyttelse skal en ha mot eventuelle ondsinnede angrep.

Hvor høy SL et system eller en komponent kan oppnå ("Security Level Capability") er avhengig av graden av oppfyllelse av syv typer grunnleggende krav ("Foundational Requirements" - FR). Disse kravtypene er [26]:

- FR1 – "Identification and Authentication Control"
- FR2 – "Use Control"
- FR3 – "System Integrity"
- FR4 – "Data Confidentiality"
- FR5 – "Restricted Data Flow"
- FR6 – "Timely Response to Events"
- FR7 – "Resource Availability"

For hver av de syv grunnleggende kravtypene beskriver standardens del 3-3 en rekke spesifikke systemkrav (SR – "System Requirement") og tilhørende kravtillegg (RE – "Requirement Enhancement") som må oppfylles for å oppnå et visst "security"-nivå (SL), og for å oppfylle for eksempel SL2, må alle krav som gir minimum nivå 2 oppfylles for alle de syv grunnleggende kravkategoriene (FR1 – FR7).

Dersom vi ser på de syv grunnleggende kravtypene (FR1 – FR7) som ligger til grunn for et gitt "security"-nivå (SL), er det FR5 "Restricted data flow" som har en mest tydelig kobling opp mot uavhengighet. I kapittel 9 av IEC 62443-3-3 er det gitt fire spesifikke krav (SR 5.1 – SR 5.4) med tillegg for "Restricted data flow". I tekstboksen på neste side er dette eksemplifisert gjennom krav SR 5.1. Som en ser av tekstboksen, må en for å oppnå for eksempel SL4, i tillegg til selve kravet også oppfylle de tre kravtilleggene.

Et annet sentralt begrep i IEC 62443 er "Maturity Level" (ML) eller modenhetsnivå. Mens SL primært omhandler teknologi, er ML mere knyttet til organisasjon, og dokumenter dennes modenhet når det gjelder å gjennomføre ulike operative og vedlikeholds-relaterte prosesser og rutiner og trekke læring ut av dette i ettertid.

Ved å kombinere SL og ML kan en oppnå en viss "Security Protection Rating" (SPR1 – SPR4) basert på regler nærmere beskrevet i standardens del 2-2. Per desember 2021 foreligger imidlertid denne delen av standarden kun i draft versjon.

Kort vurdering av IEC 62443-serien

IEC 62443-serien er svært omfattende og innholdsrik, og er velegnet for bruk i OT-miljøer. Den er internasjonal og godt kjent, og tilrettelegger dermed for felles forståelse og effektiv interaksjon mellom aktører. Et grunnleggende konsept er å dele systemer og nettverk inn i hensiktsmessige soner og tunneler. Filosofien med soner og tunneler bidrar til å understøtte uavhengighet, men det er få eller ingen spesifikke krav om full isolasjon/uavhengighet.

SR 5.1 – Network segmentation

Requirement

The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control systems networks from other control system networks

Requirement enhancements

RE 1 - Physical network segmentation

The control system shall provide the capability to physically segment control system networks from non-control system networks and to physically segment critical control system networks from non-critical control systems networks.

RE 2 - Independence from non-control system networks

The control system shall have the capability to provide network services to control system networks, critical or otherwise, without a connection to non-control system networks.

RE 3 – Logical and physical isolation of critical networks

The control system shall provide the capability to logically and physically isolate critical control system networks from non-critical control system networks.

Security levels

The requirements for the four SL levels relate to SR 5.1 – Network segmentation are:

- SL-C(RDF, control system) 1: SR 5.1
- SL-C(RDF, control system) 2: SR 5.1 (1)
- SL-C(RDF, control system) 3: SR 5.1 (1) (2)
- SL-C(RDF, control system) 4: SR 5.1 (1) (2) (3)

IEC *62443-3-3 (Chapter 9)*

En ulempe med denne serien er at den er krevende å sette seg inn i siden den inneholder en rekke (del)standarder, tekniske spesifikasjoner og tekniske rapporter. De ulike delene foreligger dessuten i varierende grad i oppdaterte eller offisielle versjoner, noe som gjør det ekstra utfordrende å få oversikt. Dette gjelder spesielt for mindre aktører, som kan oppleve at de må bruke store ressurser på å sette seg inn i standarder istedenfor å prioritere konkret sikkerhetsarbeid.

Delstandard 3-3 inneholder systemkrav som er knyttet opp mot "Security Level" (SL) (og disse systemkravene er i delstandard 4-2 gjenspeilet i form av komponentkrav). Hvilke av kravene som skal velges framkommer av en risikoanalyse og dessuten en vurdering fra de som skal drifte/eie systemene (gjennom å etablere en såkalt "profil" med krav). Anvendelse av, og evt. sertifisering i henhold til, IEC 62443 er ikke nødvendigvis nok til å hevde at et system er fullstendig uavhengig, men det er rimelig å forvente en betydelig grad av uavhengighet i systemer som innfrir strenge 62443-krav. Verdien av et sertifikat avhenger av hvilke krav som inngår i sertifiseringen, og det er opp til sertifiseringsorganene å definere gode kravspesifikasjoner.

Det er i kapittel 7 nærmere diskutert hvorvidt Ptil sitt regelverk bør referere til IEC 62443-serien.

3.2 IEC 61508

Tilsvarende som Ptil sitt regelverk krever også IEC 61508-1 (7.5.2.6, punkt d) [15] at PCS skal være uavhengig av SIS: *"The EUC control system shall be independent from E/E/PE safety-related systems and other risk reduction measures".* Betingelsene for uavhengighet detaljeres videre i en egen paragraf 7.6.2.7 gjengitt nedenfor.

> *The allocation shall proceed taking into account the possibility of common cause failures. If the EUC control system, E/E/PE safety-related systems and other risk reduction measures are to be treated as independent for the allocation, they shall:*
>
> - *be independent such that the likelihood of simultaneous failures between two or more of these different systems or measures is sufficiently low in relation to the required safety integrity;*
> - *be functionally diverse (i.e. use totally different approaches to achieve the same results);*
> - *be based on diverse technologies (i.e. use different types of equipment to achieve the same results);*
> - *not share common parts, services or support systems (for example power supplies) whose failure could result in a dangerous mode of failure of all systems;*
> - *not share common operational, maintenance or test procedures.*
>
> ***IEC 61508-1 (Chapter 7)***

Utover en definisjon av fellesfeil, inneholder ikke standarden en egen definisjon av uavhengighet, eller beskriver eksplisitt hvordan en skal bevise eller dokumentere uavhengighet. I vedlegg D i del 6 av standarden finnes det sjekklister og metodikk for å anslå β faktoren når en skal regne på redundante konfigurasjoner. Det laveste estimatet en kan få for logikk er β=0.5% (0.005), og det står at det vil være vanskelig å rettferdiggjøre en mindre verdi.

Kort vurdering av IEC 61508

IEC 62508-1 krever, tilsvarende som Ptil sin Innretningsforskrift (§§ 32-34), at kontrollsystemet skal være uavhengig av sikkerhetssystemene. Når uavhengighetskravet utdypes brukes blant annet formuleringen "sufficiently low" om sannsynligheten for samtidige feil, noe som har sin parallell i styringsforskriftens §5 om at barrierer skal være *tilstrekkelig* uavhengige. IEC 61508 utdyper imidlertid uavhengighetskravet noe ved å presisere at en skal unngå felles komponenter, hjelpesystemer og operasjons- og testprosedyrer.

3.3 IEC 61511

IEC 61511-1 [16] uttrykker kravet om uavhengighet mellom PCS og SIS litt annerledes enn det IEC 61508-1 gjør. I 11.2.4 er kravet formulert slik: "*If it is intended not to qualify the BPCS to the IEC 61511 series, then the SIS shall be designed to be separate and independent from the BPCS to the extent that the safety integrity of the SIS is not compromised*".

I en note til det samme kravet i IEC 61511 er det også pekt på at SIS og BPCS kan benytte samme fysiske utstyr dersom det kan vises at en feil på dette utstyret ikke kompromitterer sikkerhetsfunksjoner implementert i SIS.

Kort vurdering av IEC 61511

En rimelig tolkning av standarden er at SIS og PCS skal være uavhengige da PCS vanligvis ikke oppfyller kravene i IEC 61511. Noten er ganske lik det som står i veiledningen til innretningsforskriften og peker på at felles komponenter kan tillates dersom dette ikke svekker sikkerhetsfunksjonenes evne til å bli utført.

3.4 NORSOK I-002

En revidert versjon av NORSOK I-002 Industrial Automation and Control Systems ble utgitt oktober 2021 [34]. Den dekker funksjonelle og tekniske krav til design av industrielle automatiserings- og kontrollsystemer (IACS) for prosessanlegg i petroleumsvirksomheten.

Krav som er spesielt knyttet til Ptils krav om at prosess-sikring- og sikkerhetssystemene skal utføre tiltenkte funksjoner uavhengig av andre systemer og ikke bli påvirket negativt:

Network and system security design

The IACS network and system design process shall as a minimum follow the security risk assessment for system design as defined in NEK IEC 62443-3-2.

Operational and technical requirements relevant for the design are also important to be included in the design work.

The IACS network and system design shall comply to required security level – targets (SL-T) with relevant countermeasure resulting from NEK IEC 62443-3-2 security risk assessment.

The SL-T guides which requirements and enhancements in NEK IEC 62443-3-3 that is relevant to be evaluated to ensure relevant countermeasures.

The IACS shall have a system log monitoring solution for capture and storage of system logs from all networked devices.

NORSOK I-002

IACS network architecture design

Effort shall be made to use shared network within main IACS network infrastructures based on risk assessments. The following shall be maintained in the design:

- *system independency, reliability, availability, maintainability and performance;*
- *cyber security;*
- *network monitoring and management;*
- *frame prioritization.*

Separate network management solutions should be designed for:

- *general technical network and firewall equipment, including package control system network switches connected to the network;*
- *critical technical network and firewall equipment, including package control system edge network switches connected to the network;*
- *SAS network and firewall equipment*

The IACS networks shall:

- *have capacity to handle the data load for all operational modes;*
- *be scalable with respect to capability and capacity;*
- *support quality of service (QoS) functionality;*
- *prioritise IACS dependent data traffic over non-dependent data traffic;*
- *support virtual local area network (VLAN) functionality;*
- *protect networked devices from unwanted network traffic where relevant;*
- *be able to distribute time to networked devices;*
- *support end-to-end connectivity for management data where required.*

The IACS networks should be based on recognised open industry standards.

The IACS networked devices shall not be connected to different networks by-passing installed firewalls.

The IACS network internet protocol (IP) plan shall be pre-approved by company.

The high availability firewall solution shall be a redundant firewall cluster solution with state synchronisation that support deep package inspection and intrusion detection system

NORSOK I-002

Kort vurdering av NORSOK I-002
NORSOK I-002 fra 2021 legger opp til en slags skallsikring, der en har de strengeste kravene (SL4) for tilgang til anlegget, men lavere for eksempel for den sonen som inneholder SIS (SL1). Med lavere bemanning, bruk av kantenheter og IIoT må en antakelig gi tilgang til flere både personer og organisasjoner oftere og kanskje permanent gjennom tilgangssystemet.

Når en først har fått tilgang til anlegget og kanskje sonen, så kan en enklere utøve negativ påvirkning både tilsiktet og utilsiktet. Det er derfor ikke innlysende at streng skallsikring gir den beste beskyttelsen mot storulykker.

3.5 DNV-RP-G108

DNVs retningslinjer ("recommended practice") for "Cyber security in the oil and gas industry based on IEC 62443"[1] [9] gir aktører i bransjen råd om hvordan IEC 62443-standardene bør anvendes. Et sentralt konsept i DNV-RP-G108 (og i IEC 62443-serien) er å plassere innretningens systemer i hensiktsmessige soner, for å hindre problemer som eventuelt oppstår ett sted fra å spre seg til andre soner. Retningslinjene anerkjenner at noe kommunikasjon vil være nødvendig på tvers av soner, og slik kommunikasjon skal foregå gjennom tunneler, hvor det kreves egne barrierer (f.eks. brannmur). DNV-RP-G108 gir også konkrete råd for hvordan løsninger for fjerntilgang bør sikres.

Retningslinjene sier lite om konkrete uavhengighetskrav, men det er verdt å merke at soneinndeling i seg selv kan være et virkemiddel for å redusere avhengighet. DNV-RP-G108 nevner blant annet at to av karakteristikkene som bør dokumenteres for soner og tunneler er "assumptions and dependencies", og i så måte tvinges en viss bevissthet knyttet til avhengigheter frem.

Nye systemer med et større antall koblinger på tvers av soner vil helt klart "utfordre" soneinndelingskonseptet (på samme måte som for ISBR 4 i Norsk olje og gass 104). DNV-RP-G108 sier også at "*Wireless communication should be in one or more zones separated from wired communication*", noe som kan bli en utfordring dersom man etter hvert ser utstrakt bruk av trådløse enheter og 5G i samspill med kablede enheter.

Kort vurdering av DNV-RP-G108
DNV-RP-G108 har hentet ut de viktigste elementene for OT-systemer fra et utvalg av IEC 62443-standarder, og summerer opp dette på et håndterlig format for å gjøre sikkerhetsarbeidet enklere for aktører i petroleumssektoren.

DNV-RP-G108 er basert på del 2-1, 2-4, 3-2 og 3-3 av IEC 62443-serien, hvorav del 2-1, 2-4 og 3-3 er under revisjon/oppdatering (se også avsnitt 3.1). Selv om den har blitt godt mottatt i petroleumssektoren, er det utfordrende for myndighetene å vise til DNV-RP-G108, ettersom den til dels er basert på draft-versjoner fra IEC 62443-serien. En bør derfor være bevisst på hvilke versjoner fra IEC 62443-serien og hvilken versjon av DNV-RP-G108 (som planlegges oppdatert) som til enhver tid er gjeldende.

[1] DNV-RP-G108 september 2017-versjon revidert i oktober 2021 ifm. navnebytte fra DNV GL til DNV

3.6 Norsk olje og gass 070, Appendix G

Norsk olje og gass sin retningslinje 070 [33] omhandler implementering av IEC 61508 og IEC 61511 i Norsk petroleumsindustri og henvises til i Ptil sitt regelverk. I vedlegg G i denne retningslinjen er det gitt en del tekniske krav for kobling mellom systemer og vist en del løsninger som er akseptable forutsatt at en gjennomfører de tiltakene som er angitt. Det er dessuten gitt noen eksempler på løsninger som ikke er akseptable uansett tiltak.

Kort vurdering av Norsk olje og gass 070, Appendix G

Kravene og løsningene som er beskrevet i Appendix G, er forfattet tilbake i 2004 og passer ikke nødvendigvis med dagens løsninger og utfordringer. Det er derfor behov for en komplett gjennomgang og oppdatering av vedlegget. Se også kapittel 8.

3.7 NSMs Grunnprinsipper for IKT-sikkerhet

Nasjonal sikkerhetsmyndighet (NSM) har gitt ut dokumentet "Grunnprinsipper for IKT-sikkerhet" [38], som er et sett med grunnleggende prinsipper og konkrete tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. Grunnprinsippene er relevant for alle norske virksomheter.

Kort vurdering av NSMs grunnprinsipper

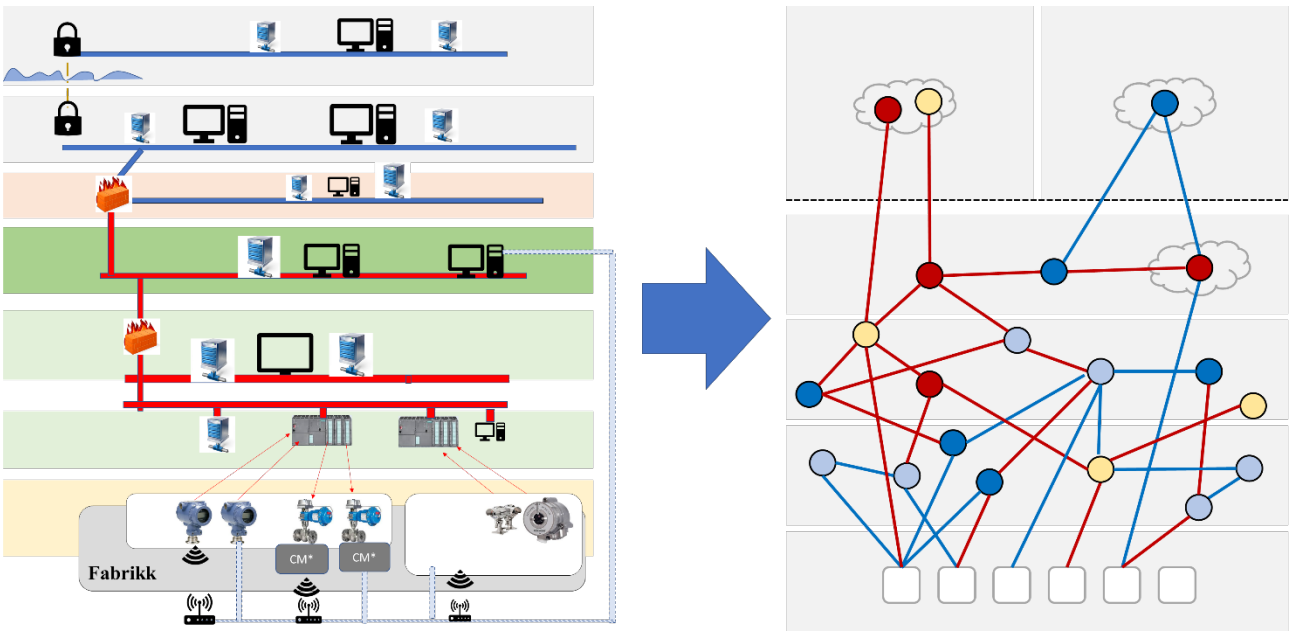
Grunnprinsippene er nyttige på et overordnet nivå, men sier ikke noe eksplisitt om uavhengighet mellom systemer. Anbefalingene/tiltakene som oppgis er primært egnet for å beskytte informasjonssystemer (IT), og ved eventuell anvendelse på (nåtidens) OT-systemer anbefales en noe justert fremgangsmåte [52].

4 Teknologiske trender, nye IKT-systemer og IIoT-løsninger

Vi vil i dette kapitelet se på teknologiske trender, teknologier og løsninger som kan medføre nye avhengigheter og mulige negative påvirkninger, blant annet som følge av at nye systemer kan kobles opp mot tekniske nettverk. Herunder diskuteres:

- Bruk av datadioder, se avsnitt 4.1
- Industri 4.0, herunder Namur Open Architecture (NOA) og OPC Unified Architecture (OPC UA), se avsnitt 4.2
- 5G teknologi og infrastruktur, se avsnitt 4.3
- Kantenheter, se avsnitt 4.4
- Håndholdte enheter, se avsnitt 4.5
- Ekstern tilkobling til OT-systemene, se avsnitt 4.6

En hovedutfordring med de nye løsningene er at tradisjonell lagdeling utfordres gjennom at data sendes på kryss og tvers mellom autonome komponenter, som beskrevet blant annet gjennom Industri 4.0. Dette er illustrert i Figur 7.



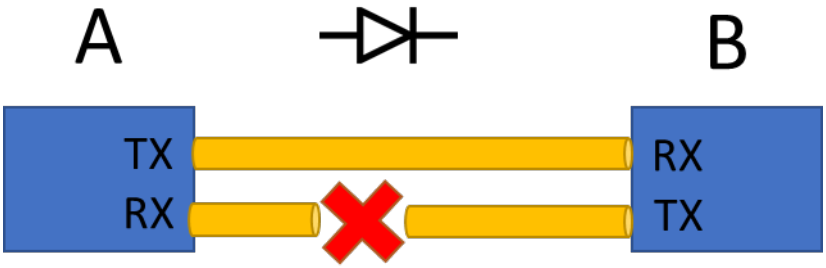
Figur 7 Fremtidig transisjon fra Purdue-modellen til åpen og flat struktur

4.1 Datadioder

Som forklart i definisjonene i avsnitt 1.3.1, er en datadiode en fysisk nettverkskomponent som når den forbinder nettverk A med nettverk B kan garantere at data kan flyte fra A til B, men ikke fra B til A. Det finnes en rekke forskjellige måter å implementere en datadiode på. Et tidlig forslag fra Kang og Moskowitz [20] involverte en tiltrodd prosess som skrev til en kommunikasjonsbuffer (dvs. en kø), og en annen tiltrodd prosess som leste fra andre enden av kommunikasjonsbufferen. Imidlertid ble mange slike datadioder konstruert for å sikre konfidensialitet i situasjoner hvor man skriver data fra et lavt graderingsnivå (f.eks. "Begrenset") til et høyere graderingsnivå (f.eks. "Hemmelig"). Dette er i tråd med Bell-LaPadula-modellen [2], men i vårt tilfelle er situasjonen omvendt: Vi ønsker å kommunisere data fra en høy-integritets-sone til

en sone med lavere integritetskrav; vi er ikke opptatt av konfidensialitet - det avgjørende er at utstyr i den sistnevnte sonen ikke kan påvirke utstyr i den førstnevnte (funksjonell uavhengighet).

Løsningen fra Kang og Moskwitz var ganske komplisert, og senere løsninger som eksemplifisert av Jones og Bowersox [19] var heller basert på bruk av en lysdiode og en fototransistor. I prinsippet er dette det samme som å ta et fiberoptisk grensesnitt hvor man fysisk fjerner returfiberen (se Figur 8). Det finnes et stort antall datadioder fra forskjellige leverandører som er sikkerhetsevaluert iht. Common Criteria på høyeste nivå [4].



Figur 8: Konseptuell beskrivelse av optisk datadiode

Som det framgår av Figur 8, er datadioden en tiltrekkende løsning på den måten at den fysisk kan garantere at A er uavhengig av B dersom datadioden representerer den eneste forbindelsen mellom de to. Imidlertid vil den kunne representere et problem dersom det skulle oppstå et behov for at A f.eks. må oppdateres eller rekonfigureres fra B. Da ville det være behov for å kunne omgå datadioden på en eller annen måte; på en innretning kan dette være at vedlikeholdspersonell fysisk reiser ut for å gjøre endringene, noe som ofte framstår som tungvint og kostbart. I praksis betyr dette at mange som tar i bruk datadioder samtidig lager seg "tilleggsløsninger" som gjøre det mulig å koble seg til A fra B (og andre steder); dette vil i så fall medføre at uavhengighetsgarantien som datadioden representerer ikke lenger vil være reell.

4.2 Industri 4.0

Begrepet *Industri 4.0* beskriver den fjerde industrielle revolusjonen, eller snarere en evolusjon der internett smelter sammen med produksjon og produkter. Tingenes internett (IoT -Internet of things) er en hoved-driver i denne utviklingen, som bringer den fysiske og den digitale verden sammen og har fire hovedbestanddeler: Tingene, nettforbindelsene, data og analyse [18].

I forbindelse med *Industri 4.0* [7]utforskes nye plattformer for sømløs sammenkobling av utstyr og deling av data. Industri 4.0 har sitt opphav innenfor tysk produksjonsindustri ("manufacturing"), men konseptet har fått fotfeste over hele verden som en del av den generelle digitaliseringstrenden.

4.2.1 Industri 4.0 og petroleumsindustrien

I første omgang har petroleumsindustrien vektlagt utvikling av skyløsninger der store datamengder fra innretninger samles og deles, men dette er gjort uten større endringer i underliggende nettverk og systemer i OT. Samtidig kommer nye initiativ som retter seg både mot utforming av OT-nettverk og utstyr, både fra tyske og globale organisasjoner. Dette inkluderer krav og løsninger for integrering og datautveksling mellom feltutstyr, kontrollere, operatørstasjoner, servere og klienter for ulike applikasjoner. Mens *RAMI 4.0* (*Reference Architecture Model Industrie 4.0*) gir de overordnede rammene for hvordan systemintegrasjonen

skal skje [47], er det flere konkurrerende plattformer som beskriver hvordan dette kan løses praktisk innenfor både OT og IT-nettverket:

- *Open Process Automation* (OPA) *Forum* [39] foreslår både krav og standardiserte løsninger for sømløs tilkobling og datautveksling på nivåene 0-2 i OT-nettverket, se Figur 5. Eksisterende systemleverandører kan koble seg til et OPA nettverk via et "OPA-grensesnitt" eller de kan utvikle kontrollere med full OPA funksjonalitet. Realisering er i hovedsak basert på kommunikasjonsprotokollen OPC UA. Det kan bemerkes at instrumenterte sikkerhetssystemer er utelatt fra OPA.
- *Modular Type Package* (MTP) [23] er en AutomationML-basert standard [1] for konfigurering for visning av utstyr på operatørskjerm, alarmhåndtering, diagnostikk, og måleverdier. Et utstyr med MTP grensesnitt kan automatisk innlemmes i anleggets OPC UA baserte informasjonsmodell og som operatørstasjonene vil hente informasjon fra.
- *Namur Open architecture* (NOA) er mer et konsept enn en løsning for utveksling av data mellom utstyr på nivå 1 og 2 i OT nettverket og systemer og applikasjoner på høyere nivå (OT, IT) og skyløsninger. Det kan derfor hevdes at NOA tar over der en OPA infrastruktur ender. NOA foreslår å benytte en egen kommunikasjonskanal som er uavhengig av OT-nettverket, med begrunnelse at dette er godt egnet for eksisterende anlegg ("brownfields") [24]. Namur er ytterligere omtalt i avsnitt 4.2.3 under.

Til sammen dekker OPA, MTP og NOA funksjoner som burde vært integrert. Dette er bakgrunnen for at tysk industri har utviklet *Asset Administration Shell* (AAS) [59][60]som er en praktisk tilnærming for dette. Enkelte operatørselskaper i Norge har pekt på AAS som svært interessant og har utfordret leverandørindustrien på hvordan AAS kan tas i bruk [28]. Petroleumsindustrien ser til blant annet tysk industri som er mer offensive på standardisering og digitalisering for "plug and play" løsninger.

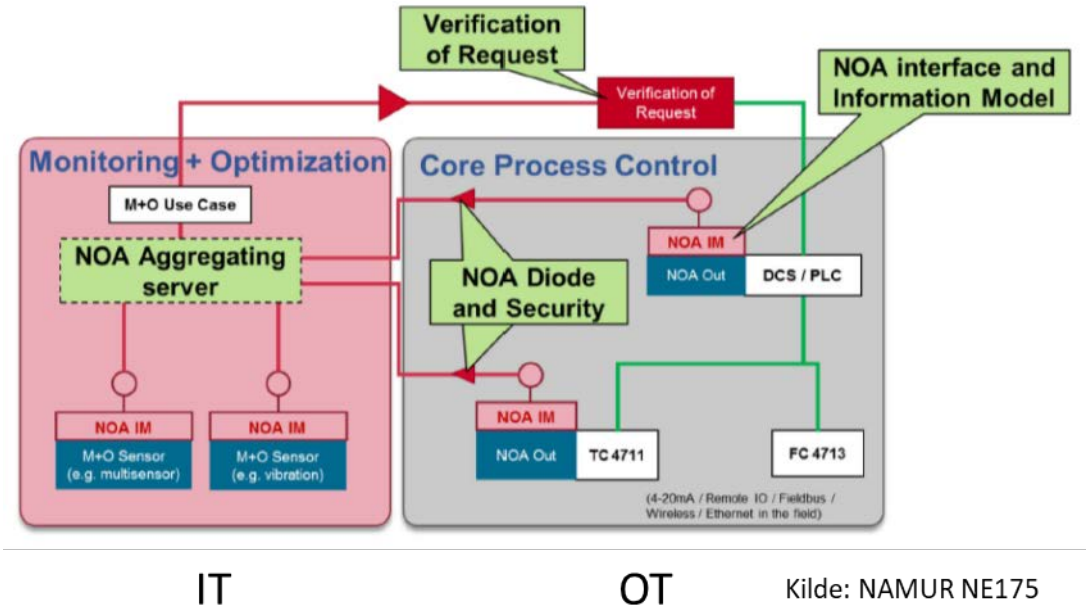
Oppsummert er det skapt store forventninger til gevinstene ved å bruke AAS til å realisere RAMI 4.0 (grunnsteinen i Industri 4.0). Dette reiser samtidig en bekymring for at de tradisjonelle skillene som er bygget inn i nettverk og mellom systemer kan bli visket ut. Det observeres også at både verktøy og kode, eksempelvis for AAS, publiseres og videreutvikles gjennom åpne nettsteder (github) som en slags bransjedugnad. Til tross for at de ulike plattformene (OPA, MTP, NOA, AAS) hevder å ivareta cybersikkerhet, så representerer løsningene også risiko for nye sårbarheter gjennom nye nettverksstrukturer og måter å utveksle data på [22].

4.2.2 OPC UA

OPC UA (Open Platform Communication Unified Architecture) er en standard for industriell kommunikasjon og informasjonsmodellering som først ble publisert i 2008 [39] og som har blitt tatt stadig mere i bruk de siste årene. OPC UA er som navnet tilsier en åpen standard, og hensikten med standarden er å sørge for sikker og plattformuavhengig utveksling av data på feltutstyrsnivå og mellom OT og IT. Å finne gode løsninger for dette blir mer og mer relevant ettersom stadig mer feltdata blir tilgjengelig. OPC UA er tatt i bruk av flere sektorer, og beskrives ofte som den protokollen som kan bringe data fra feltutstyret til kontornettverket og/eller sky. Prosessindustrien representerer ofte denne utvekslingen av data ved hjelp av "ISA-95 referansearkitekturen/ Purdue-modellen". OPC UA har også blitt mer internasjonal i forbindelse med at IEC har utgitt en rekke OPC UA standarder.

4.2.3 NAMUR Open Architecture

NAMUR Open Architecture (NOA) er et rammeverk som skal forenkle innføring av prinsipper og løsninger relatert til Industri 4.0, digitalisering og industriell IoT i prosessindustri. NOA beskriver hvordan informasjonsutveksling mellom prosesskontrollsystemer og det nye området "Monitoring and Optimization" (M+O)" kan utføres med åpne grensesnitt basert på datadioder (se avsnitt 4.1) for ivaretakelse av tilstrekkelig informasjonssikkerhet (se Figur 9).



Figur 9 Informasjonsutveksling mellom IT og OT med NOA

NOA er tiltenkt eksisterende prosessanlegg ("brownfield) hvor det med tanke på kostnader og kompleksitet er urealistisk å forandre på grunnprinsippene rundt automasjonspyramiden og Purdue-modellens laginndeling. NOA skal dermed ivareta integriteten til prosesskontrollsystemer (OT) samtidig som data og informasjon fra kontrollere og I/O-enheter gjøres tilgjengelig for videre analyse og behandling i IT-domenet (M+O). Et konsept kalt "NOA dioder" skal i denne sammenhengen sørge for enveiskommunikasjon med tilstrekkelige mekanismer for informasjonssikkerhet. NOA definerer også en løsning for hvordan man kan kommunisere f.eks. nye settpunkt for prosesskontroll fra M+O og tilbake til OT-systemene, men detaljer rundt hvordan dette skal implementeres er per november 2021 ikke ferdig spesifisert.

En viktig begrensning med NOA er at kommunikasjon til og fra instrumenterte sikkerhetssystemer ikke er en del av standarden. Det uttrykkes eksplisitt at konseptene i NOA ikke skal brukes til dette formålet. Bevisstgjøring i petroleumsindustrien rundt akkurat dette blir viktig for å ivareta uavhengighet ved og redusere risikoen for at NOA i fremtiden blir brukt for å hente ut informasjon fra systemer som ivaretar funksjonell sikkerhet.

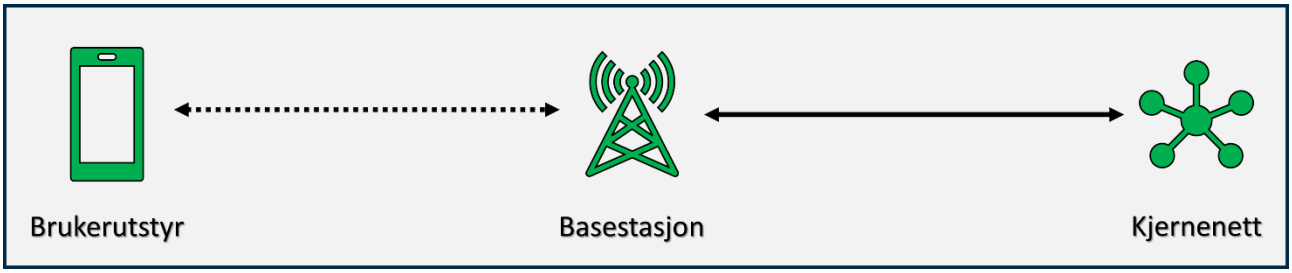
4.3 5G

5G er den nyeste generasjonen av mobilnettverk, som i motsetning til tidligere generasjoner er spesielt laget for anvendelser utover tradisjonell mobiltelefoni og mobilt bredbånd. Med egenskaper som høy datakapasitet, høy pålitelighet og lav forsinkelse er 5G tiltenkt brukt innen blant annet industri, energi, helse og transport.

Nytt med 5G er også muligheten for å opprette private nettverk, som ikke opereres eller driftes av de tradisjonelle mobiloperatørene. Dette er essensielt for anvendelser med strenge krav til ytelse og sikring av data, som for eksempel industrielle kontroll- og sikkerhetssystemer. En forutsetning for private 5G-nett er imidlertid tilgang til frekvensressurser. I Norge er Nasjonal kommunikasjonsmyndighet (Nkom) i ferd med å ferdigstille et nytt regulativ for private frekvenser for industri og næringsliv i 3,8-4,2 GHz båndet, som i løpet av 2022 skal åpne for lokale, geografisk avgrensede frekvenstillatelser på fastlandet. Det er forventet at et tilsvarende regelverk også blir gjeldende på norsk sokkel.

4.3.1 Arkitektur og teknologi

Mobilnettet til en mobiloperatør tilbyr trådløs tilkopling til mobile enheter (brukerutstyr), som tradisjonelt sett har vært en mobiltelefon. Den trådløse dekningen kommer fra et nettverk av basestasjoner, hvor hver basestasjon har en rekkevidde på opptil noen titalls kilometer. For å gi nasjonal dekning er det dermed behov for tusenvis av basestasjoner. Dette nettverket av basestasjoner overvåkes og styres fra et sentralisert kjernenett, som også tar seg av konfigurering, autentisering, ruting, abonnementer, fakturering m.m. En forenklet oversikt over komponentene i et mobilnett er presentert i Figur 10.



Figur 10 Komponenter i et mobilnettverk

Teknologi og komponenter for basestasjoner og kjernenett er i hovedsak utviklet av infrastrukturtilbyderne Ericsson, Huawei og Nokia, som er underleverandører til de store mobiloperatørene.

4.3.2 Potensielle bruksområder for 5G

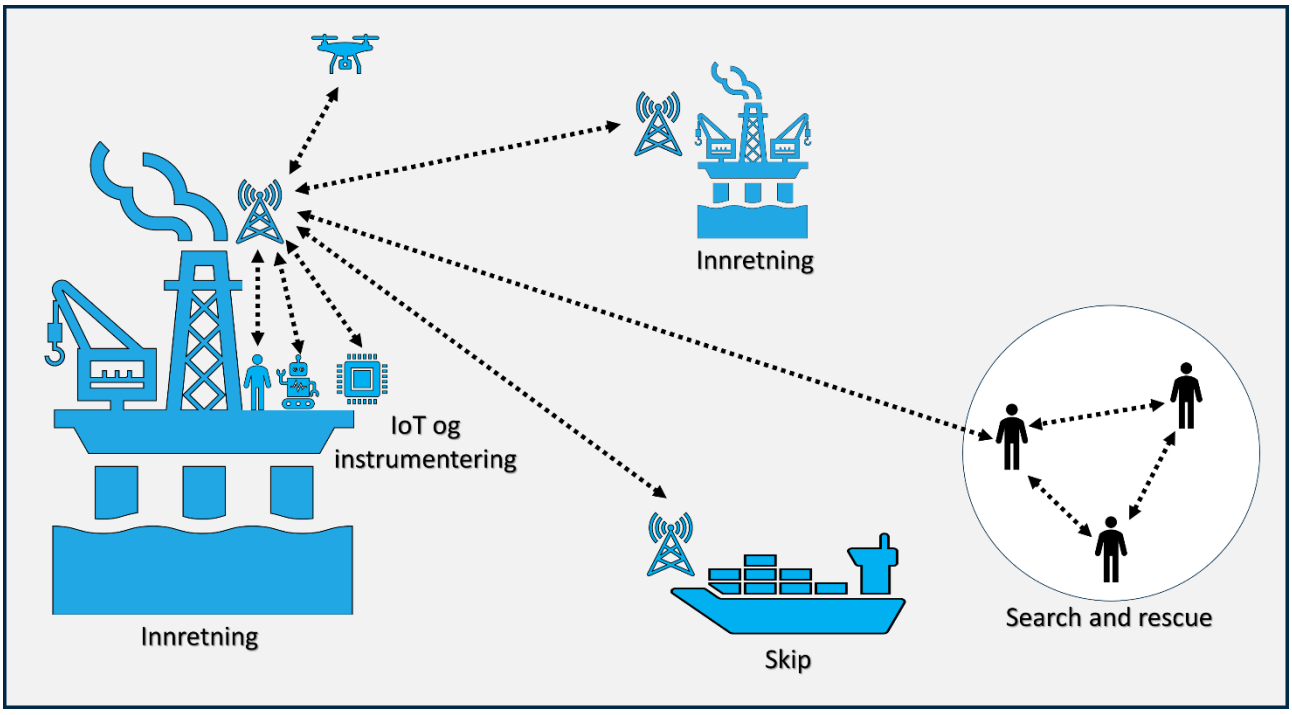
5G er en samling av flere radioløsninger og nettverksteknologier med ulike egenskaper, som kan tilpasses og konfigureres til forskjellige anvendelser. Denne fleksibiliteten, kombinert med andre nyvinninger, gjør at 5G kan tilby:

- Trådløs kommunikasjon med høy pålitelighet og lav forsinkelse til industriell bruk.
- Trådløse sensorer med lang batterilevetid og rekkevidde for IoT.
- Lokal databehandling, slik at operasjonskritiske data kan behandles raskt og trygt.
- Garantert kapasitet og kvalitet gjennom segregering og virtualisering av ulike tjenester.

Disse egenskapene gjør at bruksområdene for 5G på innretninger er mange, inkludert:

- Tradisjonelle IT-anvendelser som digital feltarbeider, audio/video, AR/VR (augmented reality / virtual reality), o.l.
- Sensorer for monitorering og optimalisering for nye konsepter som IoT/digitalisering/NOA
- Trådløs instrumentering for prosesskontroll og funksjonell sikkerhet
- Styringssignaler og sensordata for droner og roboter
- Områdedekning for skip, borerigger og evt. andre innretninger innen rekkevidde
- Nødkommunikasjon og neste generasjon nødnett

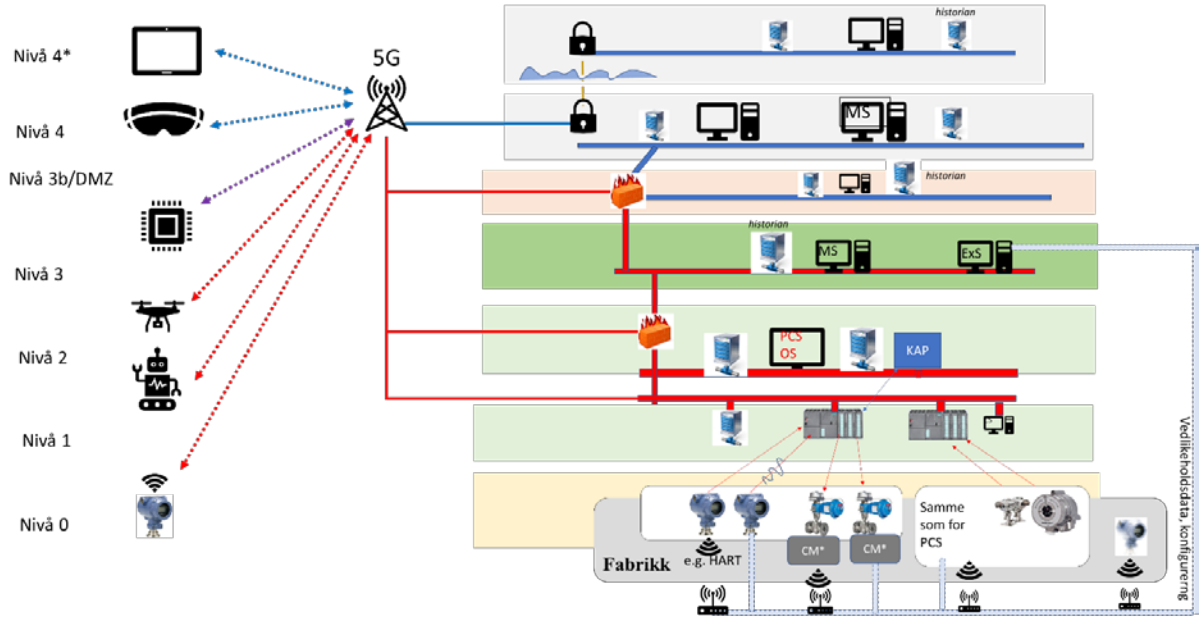
Mulighetsrommet for 5G er illustrert i Figur 11. Isolert sett er kanskje ikke 5G nødvendigvis den beste løsningen for hver enkelt av disse anvendelsene, men den store forretningsmessige gevinsten med 5G på en innretning ligger i at man kan bruke en felles teknologiplattform og fysisk infrastruktur på tvers av mange bruksområder.



Figur 11 Identifiserte bruksområder for 5G

4.3.3 Integrasjon, driftsmodeller og uavhengighet

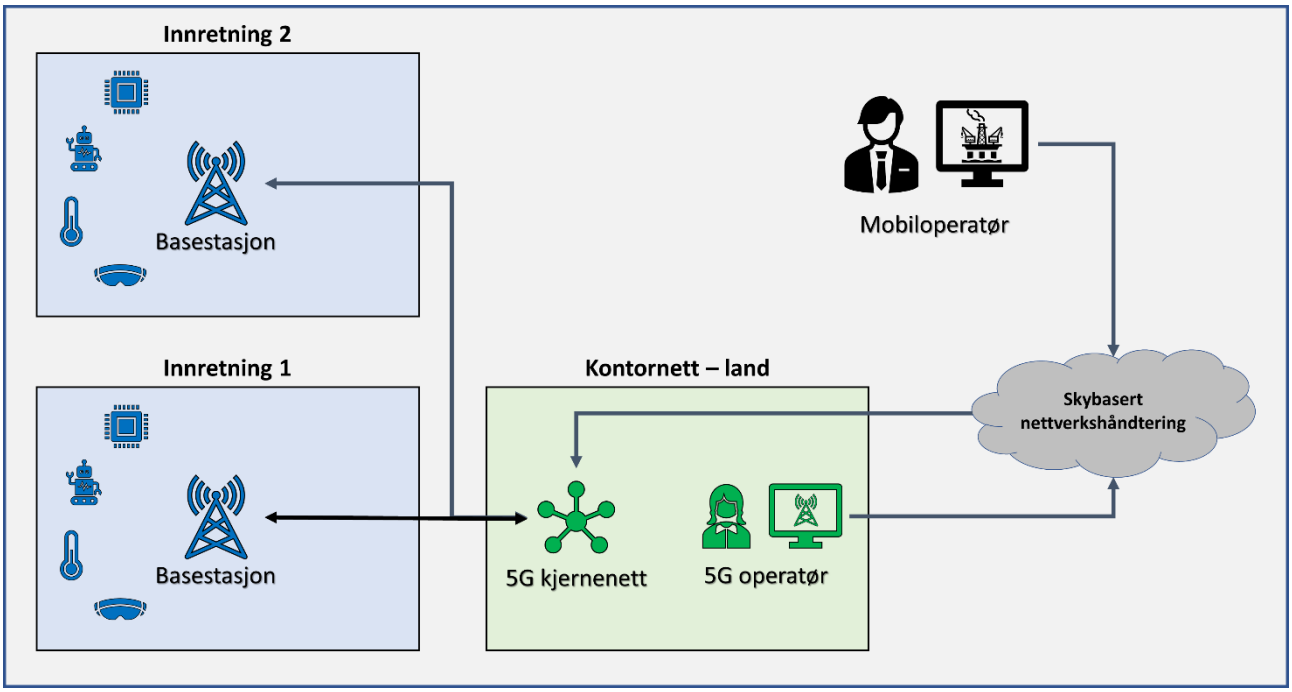
Som nevnt i forrige avsnitt er den store forretningsmessige gevinsten med 5G at man kan bruke en felles fysisk infrastruktur på tvers av mange bruksområder. Denne styrken utgjør samtidig en risiko og sårbarhet, ved at innretninger nå har tilgang til en infrastruktur som kan brukes på tvers av IT, OT og IoT. Ved å bruke virtualisering og logisk separasjon av ulike anvendelser (også kalt skivedeling, eller "network slicing"), kan 5G gi en systemarkitektur hvor basestasjoner videreformidler data fra brukerutstyr til applikasjoner på flere nivåer i Purdue-modellen. En basestasjon kan dermed bli en felles fysisk komponent som benyttes til både IT og OT, inkludert systemer for funksjonell sikkerhet. Dette er illustrert i Figur 12.



Figur 12 Integrasjon av 5G med Purdue-modellen

En annen utfordring med 5G på innretninger er relatert til verdikjeder og driftsmodeller. I skrivende stund er det en gjennomgående trend for industriell 5G at mobiloperatørene vil være involvert i drift og vedlikehold av 5G nettverk og infrastruktur, primært gjennom skybaserte løsninger. Dette gjelder både om man benytter offentlig infrastruktur fra nasjonale operatørselskap, eller om man anskaffer utstyr fra en infrastrukturleverandør (e.g. Nokia eller Ericsson). En mulig (og sannsynlig) driftsmodell for 5G er skissert i Figur 13. Her installerer et tenkt operatørselskap 5G basestasjoner på to innretninger offshore, med et sentralisert kjernenett på land. Operatørselskapet har tilgang til enkel overvåkning og styring av 5G-nettverket via en skytjenste. Via den samme skytjenesten har også mobiloperatøren en mye mer detaljert tilgang til oppsett, konfigurering, dataflyt og status til 5G-nettet, inkludert endringsmuligheter til oppsettet av basestasjonene på innretningene.

En videre utfordring relatert til bruk av 5G på innretninger ligger i det forventede globale omfanget 5G kommer til å få i årene fremover. Som nevnt innledningsvis er det tenkt at 5G skal brukes til anvendelser innenfor mange domener, som f.eks. kritisk infrastruktur, transport, logistikk, industri, helse, militært/forsvar og nødnett. Dette fører til at man for de nasjonale nettene til teleoperatørene får en felles fysisk infrastruktur som betjener mange samfunnsfunksjoner. Videre vil man med private 5G-nett bruke samme felles teknologiplattform til å betjene et enda større utvalg av driftskritiske anvendelser innenfor industri og næringsliv. Samtidig har 5G også komplekse verdikjeder med nye aktører, hvorav flere må forventes å ha begrenset domenekunnskap og forståelse for f.eks. industrielle krav og operasjonsmodeller. I sum fører dette til en dramatisk endring i risiko- og sårbarhetsbildet, hvor eventuelle angrep fra aktører med ondsinnede intensjoner kan få store konsekvenser på samfunnsnivå.



Figur 13 Mulig driftsmodell for 5G

Oppsummert gir 5G nye muligheter til kostnadsbesparelser og effektivisering av drift og operasjoner på tvers av IT, OT og IoT, og det er forventet at mange innretninger vil få 5G infrastruktur i tiden fremover. Derimot bringer teknologien også med seg en del utfordringer innenfor tre kategorier:

- 5G basestasjoner vil bli en felles infrastruktur som brukes til anvendelser på flere nivåer i Purdue-modellen samtidig
- Forretningsmodellene for 5G innebærer skybaserte løsninger hvor teleoperatører har full tilgang til konfigurasjon og oppsett av infrastruktur på innretninger
- 5G vil være en felles infrastruktur og felles teknologiplattform som skal brukes innenfor industri, transport, helse, forsvar, nødnett, m.m., noe som gjør det til et veldig attraktivt mål for ondsinnede aktører.

Hvorvidt 5G har tilstrekkelig med beskyttelsesmekanismer (e.g. skivedeling, virtualisering, kryptering) for å ivareta uavhengighetsprinsippet er en problemstilling som bør undersøkes videre.

4.4 Kantenheter

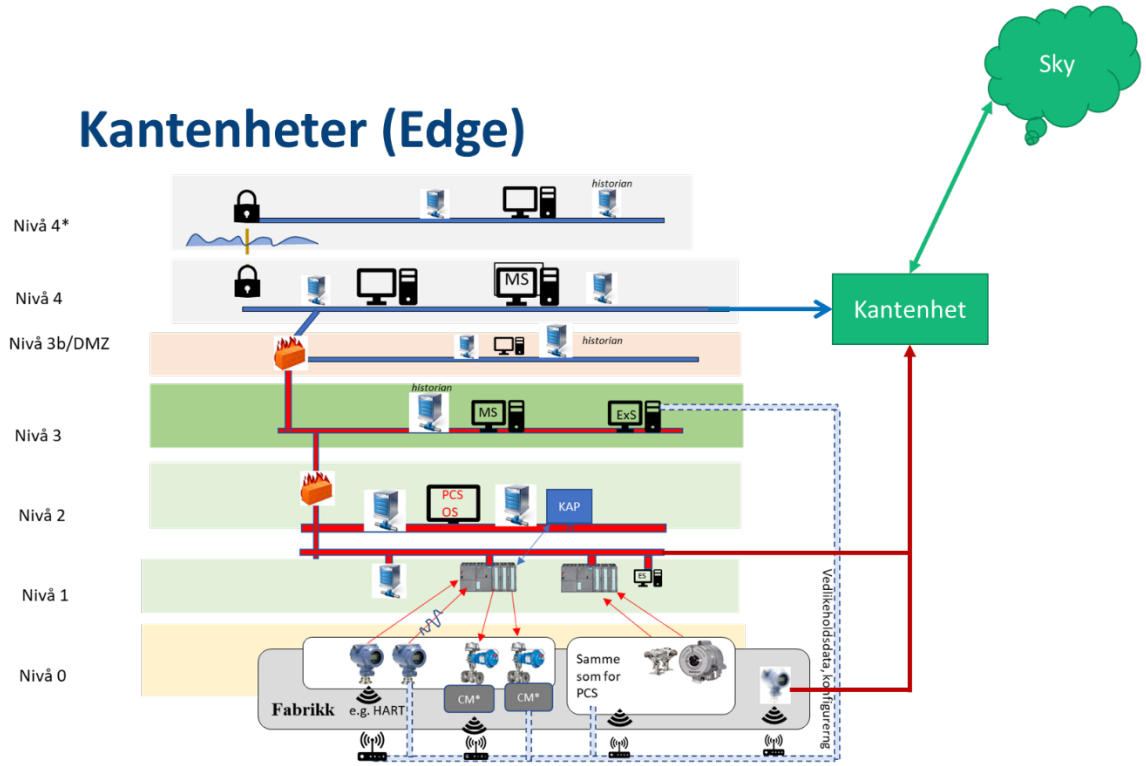
Kantenheter (Edge) ser ut til å bli brukt mer og mer for å hente ut data fra OT-systemene. Det finnes ikke noen entydig definisjon, annet enn at de brukes på kanten av det som ellers finnes av IT/OT. Teknologien og protokoller er heller ikke entydige, men avhenger av leverandør og hvem som skal hente ut data. Det er flere grunner til at disse enhetene blir brukt:

- En kan miste informasjon på veien gjennom lagene i Purdue-modellen fordi en her kan ønske å redusere båndbredde og lagringsbehov, for eksempel:
    - Midlinger for et tidsintervall
    - Sender ikke over alle verdier

- Oppdatering av verdier bare når de har endret seg en gitt verdi i forhold til siste som ble sendt

- En ønsker å hente annen informasjon enn det som er tilgjengelig og monterer IIoT enheter som kan hente ut annen informasjon

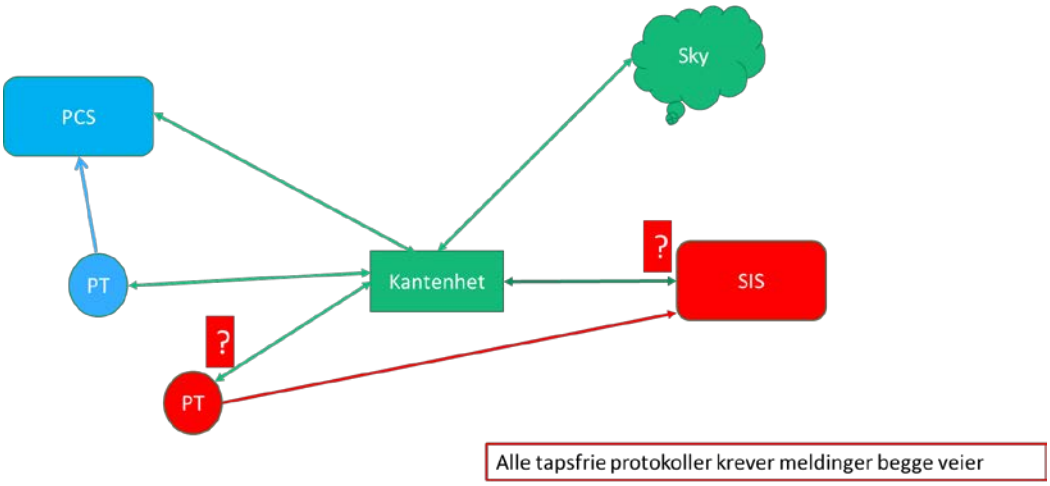
I Figur 14 er prinsippet for en mulig tilkobling av en kantenhet vist. Denne løsningen ser i første omgang tilforlatelig ut, men en må huske på at for å realisere en tapsfri overføring må en bruke en protokoll som har meldinger begge veier. En må enten forespørre om verdier, eller kvittere på mottatt og dette krever god beskyttelse for å hindre at det blir med noe annet på disse meldingene.



Figur 14 Tilkobling av kantenhet for uthenting av informasjon

I Figur 15 er bruk av kantenheter ytterligere problematisert, der en ser på mulig negativ påvirkning av sikkerhetssystemer.

Det er spesielt der en henter ut informasjon fra enheter som inngår i sikkerhetsfunksjoner det er kritisk at en beskytter seg mot "blindpassasjerer". For å unngå problemer med driften må en nok også beskytte PCS. Slike beskyttelser kan være krevende spesielt for "billige" enheter der en ikke har nok regnekraft og batterikapasitet, spesielt i trådløse enheter, men også for eksempel i en trykktransmitter. Som del av OPC UA finnes det mulige løsninger, se avsnitt 4.2.2.



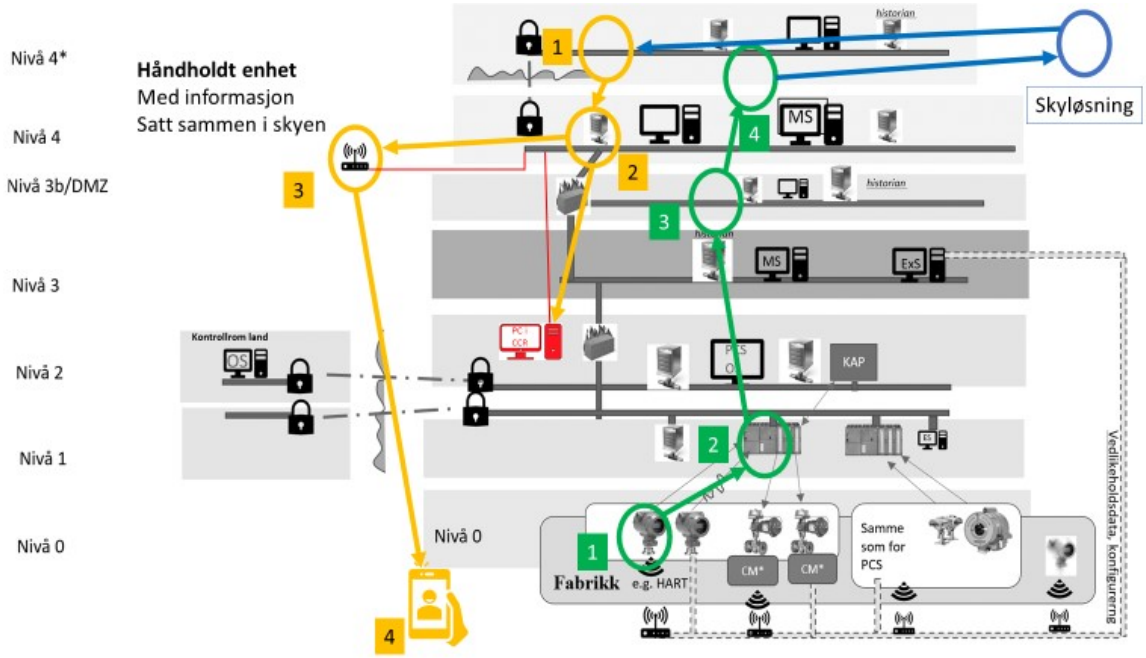
Figur 15 Mulige negative påvirkning av SIS fra kantenhet

4.5 Håndholdte enheter

Håndholdte enheter er et eksempel på nye IKT-systemer som kan tilkobles tekniske nettverk. Informasjon som kan presenteres i håndholdte enheter vil også *kunne bli* brukt som underlag for arbeid i prosessanlegget, for eksempel til å sjekke trykket og forholdene i en del av prosessen før et mannhull åpnes for intern inspeksjon og jobbing. Selv om alle formaliteter som arbeidstillatelse osv. er i orden, kan en tenke seg at en farlig situasjon vil kunne oppstå hvis den håndholdte enheten feilaktig viser at trykket er evakuert, og operatør åpner mannhullet fordi han stoler på denne informasjonen.

Figur 16 illustrerer mulig dataflyt for verdier fra en transmitter og opp til skyen (grønn), der informasjonen fra forskjellige kilder kobles sammen og føres ned til en håndholdt enhet på innretningen (gul). Hvis informasjonen fra skyen på en eller annen måte føres gjennom DMZ enten for å sendes til den håndholdte enheten eller for å vises på de vanlige skjermene til operatørene, får en utfordringer med å sikre forbindelsen fra OT opp i skyen og tilbake til OT. Hvis en gjør det slik kan skyløsningen betraktes som en del av OT og må dermed beskyttes mot feil og negativ påvirkning. Selv med den løsningen som vises i Figur 16 har en utfordringer med at enten feltoperatør eller de i kontrollrommet kan ta beslutninger basert på informasjon generert og sendt fra skyen. Hvis en ikke klarer å sikre kvaliteten og forbindelsen til og fra skyen tilstrekkelig, må en via prosedyrer styre hvilke beslutninger som kan tas basert på denne informasjonen. Også innen boring kan en ha lignende problemstillinger.

Trådløs instrumentering gir noen av de samme utfordringene som for håndholdte enheter. En trådløs detektor kan være koblet til F&G noden med et eget dedikert nett som ikke har noe felles med andre nett slik at informasjonen ikke må føres ned gjennom DMZ. At detektoren benytter en protokoll basert på samme prinsipper som PROFIsafe gir ikke tilfredsstillende løsning for å beskytte en slik penetrering av DMZ, se avsnitt 5.1.



Figur 16 Illustrasjon av logisk dataflyt ved bruk av håndholdte enheter

4.6 Ekstern tilgang til OT-systemene

Datakvalitet og sikring av data er spesielt viktig ved ekstern tilkobling og tilgang til IT- og OT-systemene. Ekstern tilkobling til IT-systemer har lenge vært mulig. Det nye er at også OT-systemer, som tidligere var avskjermet fra kontornettet, nå blir tilgjengelige fra eksterne steder via forbindelser over internett. Motivasjonen for denne utviklingen er å redusere kostnader gjennom effektivisering og flytting av personell til land, og også å kunne gi bedre beslutningsstøtte til drifts- og vedlikeholdspersonell, for eksempel ved at leverandører eller andre eksperter får tilgang til systemene fra land. Ved å flytte personell på land kan det dessuten argumenteres for at risikoen knyttet til farlige hendelser vil reduseres pga. redusert eksponering (konsekvens), slik at en også oppnår en sikkerhetsgevinst. Imidlertid vil automatiserte og fjernstyrte systemer tilføre nye risikoelementer, og en bevissthet om dette er avgjørende.

Det pågår en kontinuerlig utvikling av teknologier for å sikre dataflyt ved fjerntilkobling til OT-systemer, fra en situasjon der alle har tilgang til alt i et flatt teknisk nett, til en situasjon hvor det brukes en eller annen form for datafiltreringsfunksjon for å styre tilgangen til ulike delsystemer. For eksempel har VPN-teknologi eksistert siden 1990-tallet med protokoller som SSL og IPSec. Men uten kryptering vil VLAN til skjerming av de instrumenterte sikkerhetssystemene (som beskrevet i Appendix G.3 i Norsk olje og gass 070), utgjøre kun "tagging" av trafikk, og ikke gi noe sikkerhet mot en angriper som har tilgang til det tekniske nettet.

Typiske krav til fjerntilgang er at alle forbindelser er autorisert, autentisert, kryptert og dokumentert.

Noen praksiser som er felles for IT-sikkerhet ved autentisering for eksterne brukere:

- Autentiser alle eksterne brukere på passende nivå for å identifisere en ekstern interaktiv bruker
- Logg og gjennomgå alle tilgangsforsøk til kritiske systemer
- Deaktiver tilgangskontoen i en viss tid etter mislykkede forsøk på ekstern pålogging
- Krev re-autentisering etter ekstern systeminaktivitet

- Autentiseringsnivået som kreves, bør være proporsjonalt med risikoen for at systemet får tilgang

Dokumentasjon for hver tilkobling innebærer beskrivelse av:

- formålet,
- fjerntilgangsapplikasjonen som skal brukes,
- krypterings- og autentiseringsteknologier som brukes,
- hvordan tilkoblingen vil bli etablert (for eksempel via Internett gjennom et virtuelt privat nettverk (VPN) gjennom en DMZ) med instruksjoner etter behov,
- omstendighetene som krever tilknytningen,
- hvor lang tid forbindelsen må være åpen, inkludert forventede inaktivitetsperioder, og
- plasseringen og identiteten til den eksterne klientenheten, applikasjonen og brukeren.

Beste praksis for fjerntilkobling er beskrevet blant annet i IEC 62443-serien, sammen med Norsk olje og gass 070 og DNV-RP-G108. Andre relevante dokumenter er NIST SP 800-46 og NIST SP 800-82.

5 Tiltak for å motstå cyberangrep

Dersom et system A kan utsettes for cyberangrep fra eller via et system B, vil dette være en trussel mot uavhengigheten til system A. Følgelig vil et system måtte beskyttes mot cyberangrep for å virkelig være uavhengig. I denne sammenhengen er vi mest opptatt av cyberangrep som kan påvirke *integritet* og *tilgjengelighet* av systemer og data, og som i ytterste konsekvens kan påvirke uavhengighet[2]. Når det gjelder data, vil vi oftest løse dette ved hjelp av byggesteinene kryptering, meldingsautentisering og/eller digitale signaturer. Det er også vanlig å dele inn i ulike soner, som da gjerne forutsetter at man bruker forskjellige former for tunneler for kommunikasjon mellom sonene. Et spesialtilfelle er bruk av datadioder for å sikre at kommunikasjon kan gå fra en sone til en annen, men ikke tilbake igjen (se 4.1). Disse temaene beskrives i mer detalj i de følgende underavsnittene.

Også programvare kan utsettes for angrep, og et vellykket angrep kan gjøre en aktør i stand til å endre oppførselen til et system og dermed kunne påvirke dets uavhengighet [6]. For egenutviklet programvare er det viktig å følge god praksis for programvaresikkerhet for å sørge for at programvaren gjør det den er ment å gjøre, også når den utsettes for ondsinnet påvirkning. Dette bør selvfølgelig også tilstrebes for programvare fra ekstern leverandør, men det har man gjerne mindre kontroll over. Dermed vil det ofte være nødvendig også å bruke nettverksmekanismer som begrenser hvilke aktører som er i stand til å (forsøke å) kommunisere med programvare som kan påvirke funksjonell sikkerhet.

5.1 Kommunikasjon for funksjonell sikkerhet

IEC 61508 sier at når en instrumentert sikkerhetsfunksjon (SIF) er avhengig av kommunikasjon, skal kommunikasjonssystemet ansees som en komponent i SIF'en. Funksjonelt sikker (safe) kommunikasjon kan da oppnås ved en av to metoder:

1. Hele kommunikasjonskanalen (inklusive endepunktene) designes, utvikles og valideres i henhold til IEC 61508 og *enten* IEC 61784-3 *eller* EN 50159.
2. Deler av kommunikasjonskanalen er ikke designet, utviklet eller validert i henhold til IEC 61508, bare endepunktene (sender og mottaker). I så fall skal nødvendige tiltak for sikker feilhåndtering av kommunikasjonssystemet som helhet allikevel implementeres i henhold til enten IEC 61784-3 eller EN 50159.

Metode I kalles for "white channeling", og krever at det utvikles et eget, dedikert kommunikasjonssystem utelukkende for sikker (safe) kommunikasjon. Dette er i de fleste tilfeller veldig tids- og kostnadskrevende, og er dermed ikke så utbredt. Metode II kalles for "black channeling", og involverer å legge sikkerhetsfunksjoner på endepunktene i kommunikasjonen, for å unngå kvalifisering av hele kommunikasjonssystemet.

IEC 61784-3 for industrielle kommunikasjonsnettverk definerer prinsipper for overføring av sikkerhetsrelaterte meldinger mellom deltagere i et distribuert feltbussnettverk i henhold til krav for black channel i IEC 61508. IEC 61784-3 beskriver også ett sett med profiler for sikker (safe) kommunikasjon for et utvalg feltbuss-standarder:

- Profil 1: Funksjonell sikkerhet med FOUNDATION Fieldbus
- Profil 2: Funksjonell sikkerhet med CIP (Common Industrial Protocol)
- Profil 3: Funksjonell sikkerhet med PROFIBUS og PROFINET

[2] Det kan også være gode grunner for å være opptatt av konfidensialitet, men det er ikke vårt fokus i dette dokumentet.

- Profil 6: Funksjonell sikkerhet med INTERBUS
- Profil 8: Funksjonell sikkerhet med CC-Link
- Profil 12: Funksjonell sikkerhet med EtherCAT
- Profil 13: Funksjonell sikkerhet med Ethernet POWERLINK
- Profil 14: Funksjonell sikkerhet med EPA (Enhanced Performance Architecture)

Hver av disse profilene er spesifisert under IEC 61784-3-x, f.eks. adresserer IEC 61784-3-3 funksjonell sikkerhet for PROFIBUS og PROFINET – en profil som kalles PROFISafe. Profilene for sikker (safe) kommunikasjon bygger på de underliggende protokollene og overføres på samme nett/kabel som andre meldinger. Nyttemeldingen utvides derimot med følgende informasjon:

- En sikkerhetskode ("safety"-kode) som skal kunne detektere utilsiktede feil av tilfeldig og systematisk karakter i meldinger
- Unik identifikasjon for sender og mottaker for meldingen
- Sekvensnummer på meldingen
- Når neste melding skal komme til mottakeren

Selv om profilene i IEC 61784-3 tar for seg diverse feilmodi for kommunikasjonskanaler, er standarden noe mangelfull når det gjelder dekning av informasjonssikkerhet. Det refereres til IEC 61784-4 for feltbussrelatert "security", og til IEC 62433 for generell "security", men uten noe videre forklaring på eller krav til hvordan det skal implementeres. Det er dermed dessverre ikke vanskelig for uvedkommende å manipulere meldinger uten at det kan oppdages av mekanismene i disse profilene; dette kan påvirke sikkerhets-funksjonene ("safety"), og det gis heller ingen beskyttelse mot at annen trafikk kan påvirke negativt. Det eneste disse profilene sørger for er at mottageren går til en forhåndsdefinert sikker tilstand hvis det oppdages noe feil på overføringen.

En ser en utvikling mot tettere integrasjon mellom prosesskontroll og sikkerhetssystemer, og ikke minst det at flere ulike industrielle IKT-systemer og IIoT-løsninger blir koblet opp mot tekniske nettverk. Da bør det stilles krav til at selv om løsningen er sertifisert i henhold til IEC 61784-3 må den også ha tilstrekkelige mekanismer for informasjonssikkerhet. Beskyttelse mot uautorisert tilgang kan da gjøres på to måter:

- Kryptering av innholdet i meldinger som sendes til og fra SIF
- Plassering av hele SIF innenfor en sone som definert i IEC 62443

Av disse to fremgangsmåtene vil den første kreve en endring i kommunikasjonselementer i SIF'en, med påfølgende tid- og kostnadskrevende resertifisering. Med den andre fremgangsmåten unngår man endring av SIF ved å forhindre uautorisert tilgang til kommunikasjonskanalen ved hjelp av soner og tunneler som definert i IEC 62443.

5.2 Kryptering

En viktig sårbarhet i dagens OT-systemer er at de ofte inneholder eldre utstyr som ikke har innebygd støtte for kryptografi. Dette betyr at høy integritet avhenger av god skallbeskyttelse. Digitale signaturer eller meldingsautentiseringskoder (MAC – se avsnitt 5.3), som gir muligheten til å verifisere at data er autentiske og ikke har blitt endret, brukes vanligvis ikke i OT-systemer. DNV-RP-G108 [9] inneholder følgende anbefaling:

- Symmetrisk kryptering: AES 128 eller bedre
- Asymmetrisk kryptering: RSA 2048 eller bedre
- Hash: SHA-224 eller bedre

Det har tidligere vært en utbredt misforståelse at kryptering av en kommunikasjonskanal (for eksempel i form av et Virtuelt Privat Nettverk) gjør det umulig å manipulere med dataene som overføres uten at det kan detekteres av mottakeren. I de senere år har IT-bransjen imidlertid måtte ta inn over seg at slike garantier kun kan gis dersom man benytter seg av en av de nærmere definerte protokollene for autentisert kryptering, for eksempel AES-GCM [57] eller AES-CCM [29].

Dersom kvantedatamaskiner blir tilgjengelige på kort sikt, vil det medføre dramatiske endringer i hvilke algoritmer og nøkkellengder som gir tilstrekkelig nivå av sikkerhet [58]. Skal man ta høyde for dette kan det blant annet få følgende konsekvenser:

- Dagens offentlig-nøkkel-algoritmer som baserer seg på diskret logaritme eller faktorisering av store tall (Diffie-Hellman, RSA eller ECC er de vanligste eksemplene) må byttes ut med kvante-sikre alternativer
- Nøkkellengden til symmetriske krypteringsalgoritmer (AES) må dobles -> 256 bit eller mer
- Lengden på hasher må dobles (SHA3-384 eller SHA3-512)

Per i dag er det ingen konsensus omkring hvilken offentlig-nøkkel-algoritme man bør velge, men det arbeides med ulike alternativer [56] . Autentisert kryptering later ikke til å være en problemstilling som får mye oppmerksomhet i bransjen, og heller ikke kvantesikker kryptering later til å være noe bransjen bekymrer seg om.

Avhengig av valg av profil i IEC 62443 kan det påløpe krav til kryptering, og OPC UA kan også inkludere kryptering. Det er også ulemper ved å bruke krypterte meldinger innen OT på grunn av at signaturbaserte IDS-er (Snort, Suricata, Bro, ...) ikke vil kunne oppdage innbruddsforsøk. Nettverksovervåking blir da også vanskeligere. For enkeltapplikasjoner går det an å vurdere proxy-løsninger som dekrypterer trafikken som går inn/ut av bestemte soner.

Det er i liten grad implementert kryptering mellom enheter i OT på norske innretninger, delvis fordi utstyret som brukes i dag sjelden støtter kryptering av trafikken, og delvis fordi kryptering/dekryptering krever ressurser og vil kunne gå på bekostning av responstid og mulighetene for utveksling av informasjon mellom de enkelte systemer, samt at operatørgrensesnittet også kan bli langsommere. Skallsikring i form av soner og tunneler i henhold til IEC 62443 kan på kort sikt representere en bedre løsning for OT-systemer.

Det finnes SIL 4 sertifiserte trådbundne sikkerhetssystemer i henhold til IEC 61508, der logikken ikke kan påvirkes via IKT-systemer. Logikken er da ikke sårbar for IKT-trusler, og informasjon og status kan for eksempel hentes ut med OPC (men OPC delen har ennå ikke blitt sertifisert i henhold til aktuelle IEC 62443 standarder). Dette betyr at logikken ikke trenger beskyttelse mot IKT-trusler, mens informasjonen på OPC har samme utfordring som annen programvarebasert infrastruktur.

5.3 Digitale signaturer og meldingsautentiseringskoder (MAC)

En digital signatur er avhengig av offentlige og private (dvs. asymmetriske) nøkler, noe som vanligvis innebærer en "Public Key Infrastructure" (PKI). Hvis A skal signere en melding, må A bruke sin private nøkkel; deretter kan enhver som får meldingen verifisere at meldingen kommer fra A og ikke har blitt modifisert

underveis ved å bruke As offentlige nøkkel. Den konseptuelt enkleste måten å implementere en digital signatur på er å ta en kryptografisk hash av meldingen, og kryptere resultatet med As private RSA-nøkkel. Mottakeren kan da gjøre samme hash-operasjonen på meldingen, dekryptere signaturen med As offentlige nøkkel, og sammenligne de to resultatene. Dersom de er like, er signaturen gyldig.

En meldingsautentiseringskode (MAC) kalles også en nøklet hashfunksjon, og brukes typisk mellom to parter som deler en hemmelig (symmetrisk) nøkkel, for å autentisere informasjon som utveksles mellom de to partene. Algoritmen mates med den hemmelige nøkkelen og en melding (en datamengde av variabel størrelse), og produserer en verdi (MAC) som kobles til meldingen som skal beskyttes. Hvis integriteten til meldingen senere må sjekkes, kan man anvende MAC-funksjonen på meldingen og sammenligne resultatet med den tilhørende MAC-verdien. En angriper som endrer på meldingen, vil ikke være i stand til å lage en ny korrekt MAC uten å kjenne den hemmelige nøkkelen.

En vanlig måte å implementere en MAC på er ved hjelp av en kryptografisk hash-funksjon etter et bestemt mønster. Dette kalles da for HMAC.

5.4 Egenskaper til soner og tunneler

Konseptet med soner og tunneler som illustrert i Figur 6, pekes ofte på som løsningen for å beskytte seg mot uønsket påvirkning utenfra, men disse konseptene garanterer ikke for uavhengighet, blant annet fordi omfanget av foreslåtte tiltak vil avhenge av applikasjon, fastsatt SL ("Security Level", se avsnitt 3.1), hvilke krav som faktisk er implementert og det faktum at alle systemer/komponenter innenfor en sone ikke nødvendigvis kan implementeres med gitte SL-krav for sonen.

Krav til implementering av soner og tunneler er gitt i ulike deler av IEC 62443 standardserien. Nedenfor er gitt noen problemstillinger som det er mulig å løse hvis en har implementert relevante tiltak:

1. En tunnel mellom to soner *kan* lages så den beskytter mot uønsket påvirkning også gjennom tunnelen, men dette er ikke en del av de kravene som følger direkte av nivå (SL) og andre krav til tunneler og soner i IEC 62443. En slik beskyttelse må enten realiseres i tunnelen eller hos mottakeren hvis en ikke skal kunne påvirke SIS fra andre systemer. (IEC 62443-2-4, SP.05.02). Dette betyr at krav av den typen som står i Norsk olje og gass 070 fortsatt er nødvendige, se avsnitt 3.7 i denne rapporten.

2. Det er i IEC 62443 mulighet for at sikkerhetssystemene (SIS) kan være logisk eller fysisk adskilt i soner som er forskjellig fra de som inneholder de systemene som ikke er sikkerhetssystemer (PCS). Hvis de ikke kan adskilles, må begge være i den samme sikkerhetsrelaterte sonen. (IEC 62443-3-2 avsnitt 4.4.4). For enheter i samme sone gir ikke standarden noen beskyttelse eller uavhengighet.

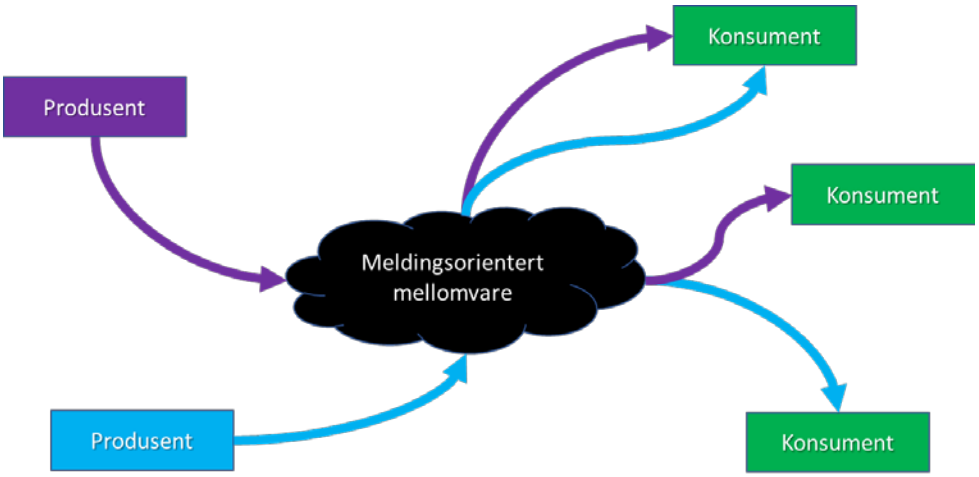
3. En kan hindre konfigurering av SIS ved fjernaksess. Dette skal også verifiseres av en uavhengig tredjepart. (IEC 62443-2-4, SP.05.09)

De tiltakene som en finner i 62443-2-4 er beskrevet som muligheter (eller "capabilities") som en leverandør skal kunne tilby en anleggseier, og er ikke eksplisitt koblet til "security"-nivå (SL). Kravene i IEC 62443-3-3 (til systemer) og IEC 62443-4-2 (til komponenter) er derimot knyttet opp mot fastsatt SL som igjen skal framkomme som et resultat av risikovurderinger. Som diskutert i avsnitt 3.1 er det imidlertid anleggseier som til syvende og sist bestemmer hvilke krav som faktisk skal gjennomføres, typisk ved å etablere en "profil". Det er derfor vesentlig at denne profilen innbefatter de kravene som en mener er viktige for å gi mest mulig uavhengighet.

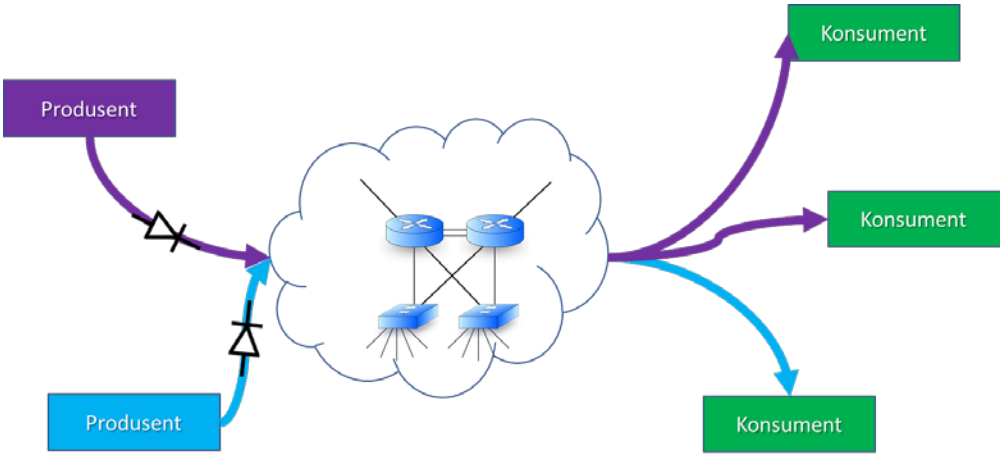
5.5 OPC UA

5.5.1 PubSub som innfallsvinkel til datadioder

Publish-Subscribe (PubSub) beskrives i OPC UA part 14 [40]. Modellen kan illustreres overordnet som i Figur **17**; man har en eller flere enheter som publiserer data, og en eller flere enheter som abonnerer på data. Dette skjer via en "mellomvare" som kan implementeres på forskjellige måter. I utgangspunktet kan alle enhetene være "normale" OPC UA enheter som kommuniserer på vanlig vis, men ett eksplisitt alternativ er å bruke UDP datagram uten kvittering. I dette tilfellet vil det være mulig å plassere en "unidirectional gateway" (dvs. datadiode – se avsnitt 4.1) mellom produsenten og konsumenten (se Figur **18**).

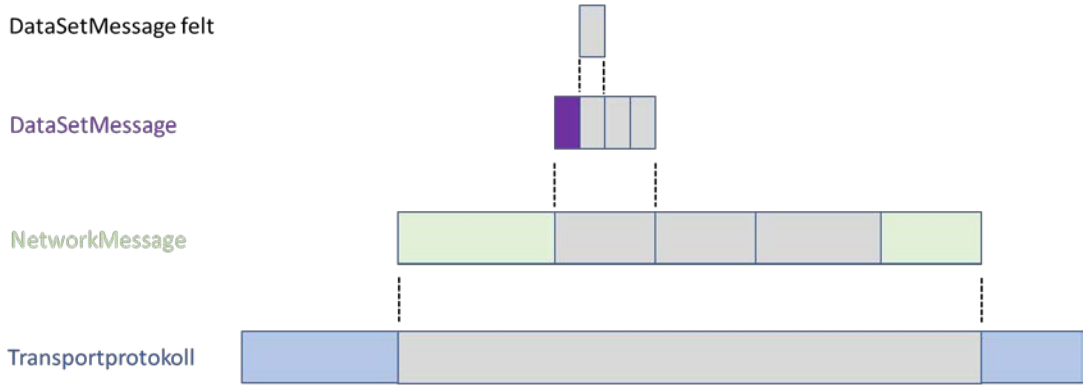


Figur 17: OPC UA PubSub modell



Figur 18: PubSub uten aktiv megler, med datadioder

PubSub har støtte for signering[3] eller signering og kryptering. Meldingsformatet illustreres i Figur **19**. Individuelle dataelementer grupperes i en "DataSetMessage", og flere av disse kan igjen grupperes i en "NetworkMessage", som til slutt utgjør nyttelasten i en transportprotokoll-melding (i vårt tilfelle UDP). Hvis man har flere som abonnerer, kan man bruke UDP multicast-adresser, men for vårt formål antas det at UDP unicast-adresser vil være tilstrekkelig.



Figur 19: PubSub meldingsformat

Datafeltet i "DataSetMessage" (det lilla feltet i **Figur 19**) består av informasjonen angitt i Tabell 3. De viktigste her er en ID som identifiserer avsenderen, et sekvensnummer, og et tidsstempel.

Tabell 3: Datafelt i DataSetMessage

Felt	Forklaring
DataSetWriterId	Identifies the *DataSetWriter* and indirectly the *PublishedDataSet.*
Sequence number	A number that is incremented for each *DataSetMessage*. Can be used to verify the ordering and to detect missing messages
Timestamp	A timestamp describing when the data in this *DataSetMessage* was obtained.
Version	Version information about the configuration of the *DataSetMetaData.*
Status	Status information about the data in this *DataSetMessage.*
Keep alive	When no *DataSetMessages* are sent for a configured time period, a keep alive *DataSetMessage* is sent to signal the *Subscribers* that the *Publisher* is still alive.

UDP gir i utgangspunktet ingen garantier om tidsriktighet, leveringskvittering, rekkefølge eller beskyttelse mot duplikater. Ved bruk av datadiode vil det ikke være mulig å be om retransmittering av manglende pakker, men det åpnes for å sende flere kopier av samme pakke; dette må man da evt. konfigurere dersom man har en kommunikasjonskanal med for stort pakketap. Sekvensnummeret gjør det da mulig å forkaste pakkene som er duplikater [40]. Hvis en benytter UDP må nok konsumentene tilpasses slik at de kan virke selv om enkelte pakker ikke kommer fram.

[3] Mulig at de her mener MAC snarere enn digital signatur, ettersom de også nevner at dette krever at produsent (*publisher*) og konsument (*subscriber*) deler en hemmelig nøkkel.

5.6 Zero trust versus skallsikring

I dataalderens spede begynnelse var datamaskiner monolittiske kolosser som fylte hele rom, og den eneste formen for kommunikasjon ble gjort i form av stabler med hullkort som ble båret inn og ut. Verden gikk imidlertid videre, og datanettverk så dagens lys. På et tidspunkt begynte man å knytte sammen datamaskiner fra forskjellige organisasjoner, og da Internett ble allemannseie på slutten av 90-tallet, kunne enhver koble seg opp til et hvilket som helst datasystem. Dette viste seg å også legge veien åpen for angripere, og mange organisasjoner fant ut at det var for vanskelig å sikre hver enkelt maskin. Dermed ble det duket for skallsikring av lokalnettverk i form av en brannmur; for å sitere Cheswick: "*et hardt skall rundt en seig kjerne*" [5].

I senere år har skallsikring med brannmurer i IT-nettverk vist seg å være utfordrende, delvis fordi en rekke tjenester nå krever at det lages "hull" i brannmuren for at de skal fungere, og delvis fordi det i dag er så mange mobile enheter som tas med inn i bedriftsnettverk, og fordi bruken av nettsky har tiltatt i stor grad. Dermed har en ny trend som nærmest bringer oss tilbake til utgangspunktet blitt populær: tillitsfri databehandling (*zero trust computing*) [21],[31]. Konseptet er at man ikke lenger skal ta utgangspunkt i skallsikring der alle enheter på innsiden av brannmuren er tiltrodd, men i stedet kreve at alle enheter skal autentisere seg overfor enhver annen enhet de skal interagere med. Videre må da også alle enheter være autorisert for at de skal få lov til å interagere med en gitt enhet.

Tillitsfri databehandling forutsetter at man har mekanismer for nøkkeldistribusjon og nøkkeladministrasjon på plass; det involverer gjerne en PKI, selv om det også finnes andre måter å gjøre det på. Dette betyr også at man er avhengig av bruk av kryptografiske mekanismer i OT-nettverk som skal bruke dette.

6 Mulige avhengigheter og negative påvirkninger

Vi vil i dette kapitlet si litt generelt om hvordan nye løsninger kan medføre mulige avhengigheter og negative påvirkning og dessuten reflektere litt rundt hvorvidt Ptil sine krav til uavhengighet kan sies å være oppfylt eller ikke. Mulige tiltak for å begrense de nye avhengighetene er sammenfattet i avsnitt 8.

6.1 Hva legger vi i negativ påvirkning?

Med "negativ påvirkning" tenker vi her at en feil eller hendelse i et system eller en tilhørende komponent, kan svekke eller forhindre sikkerhetsfunksjonen til et annet system eller en komponent i et annet system (såkalte farlige feil). Dette kan for eksempel skyldes felles komponenter, en funksjonell eller fysisk avhengighet, eller felles ytre påvirkninger (se avsnitt 2.2).

Negativ påvirkning kan også knyttes til feil eller hendelser som påvirker andre systemers eller komponenters *produksjonsevne* (men ikke forhindrer selve sikkerhetsfunksjonen). For eksempel at en ventil i produksjonslinjen klapper igjen som følge av en svikt i hydraulikksystemet (såkalte sikre feil). Dette er også negativ påvirkning, både med hensyn til regularitet og ut ifra det faktum at nedstengninger og oppstarter i seg selv representerer en risiko. Vårt primærfokus i denne rapporten er imidlertid sikkerhetskritiske (farlige) feil.

Et sentralt spørsmål blir da hvorvidt prosess-sikringssystemet (PSD) eller øvrige sikkerhetssystemer som ESD og brann & gass systemet kan påvirkes negativt som følge av feil i andre systemer. Er det for eksempel slik at de kan påvirke hverandre negativt, kan de påvirkes negativt av kontrollsystemet, eller kan de påvirkes negativt av andre IKT-systemer og IIoT-løsninger, inklusive koblinger til leverandørbaserte skyløsninger utenfor OT-domenet?

6.2 Nye avhengigheter og koblinger

Selv i lagdelte løsninger som følger Purdue-modellen, med beskyttelse av OT-systemene mot uønsket påvirkning, har en utfordringer når det gjelder koblinger mellom de forskjellige systemene. Dette kan være signaler som bevisst overføres, eller koblinger for eksempel via operatørgrensesnittet. Det er svært utfordrende å vise at enhver feil som kan opptre i et system ikke kan påvirke et annet negativt.

Noen opererer med et eget sikkerhetsnett som skiller SIS fra de andre, men i og med at en har bevisste koblinger over dette skillet og felles operatørgrensesnitt, blir skillet i de verste tilfellene ikke mer enn en reduksjon av belastningen på sikkerhetsnettet.

Soner og tunneler i henhold til 62443 kan gi beskyttelse mot uønsket ekstern påvirkning, men det garanterer ikke full uavhengighet. Innenfor en sone har en samme utfordringer som for dagens løsninger, og gjennom tunneler kan en i prinsippet få negativ påvirkning ved at feilaktig verdi overføres. Så lenge verdien er innenfor lovlige grenser vil den kunne påvirke negativt. Dette er sammenlignbart med at 4-20mA er innenfor lovlig grense, men uansett kan 16mA føre til at SIS ikke får 8mA som skulle ha resultert i en sikker aksjon.

Uavhengigheten som oppstår når man segmenterer nettverk for å skille forskjellige systemer fra hverandre, svekkes når det opprettes en rekke koblinger mellom sonene. Definisjonen/avgrensningen av et system blir uklar når forskjellige funksjoner legges i forskjellige soner. Ifølge DNVs RP-G108 skal forskjellige systemer segmenteres i forskjellige soner, så lenge de ikke har funksjonelle eller operasjonelle avhengigheter som krever at de er i samme sone. Denne tilnærmingen blir utfordret av de nye løsningene som har blitt skissert, med flere/mange koblinger på tvers av soner. Eksempel på dette er 5G basestasjoner som vil bli benyttet på

tvers av alle lagene i Purdue-modellen, og fremtidig utflating av automasjonspyramiden hvor alle kan kommunisere med alle, som definert av OPC UA.

Ved fjerntilkobling (eller andre koblinger på tvers av soner) er det ikke lenger en tydelig sammenheng mellom system og sone. Man kan hevde at et system strekker seg over flere soner, ettersom dets funksjoner befinner seg i flere forskjellige soner, men dette er ikke i tråd med anbefalingen om å ha forskjellige systemer i forskjellige soner.

Nyere teknologi som kantenheter og IIoT enheter har utfordringer hvis informasjon skal hentes fra enheter som er en del av sikkerhetssystemene så lenge de bruker en tapsfri protokoll som må sende enten forespørsler eller kvitteringer til enheten. Her er det også viktig å merke seg at NOA som definerer hvordan man kan hente informasjon fra OT til IT ved hjelp av datadioder, ikke innebefatter sikkerhetssystemer.

Hvis en ser på OT-systemene som en enhet kan det være en god del felles komponenter, selv om dette selvsagt kan variere mellom innretninger. Om disse ikke er kritiske per i dag, må en vurdere om de etter hvert kan bli det og spesielt om de kan benyttes som angrepspunkter. Noen eksempler på slike kan være:

- Brannmurer og andre nettverkskomponenter
- Menneske-maskin-grensesnitt
- Konfigurasjonsverktøy
- Klokkesystem
- Systemer for administrasjon av feltutstyr
- Domenekontrollere
- Backup-systemer
- Active directory
- 5G
- Maskin- og programvare (hypervisor) for virtualisering
- Systemer for autentisering
- Nøkkeladministrasjon (aktuelt for all autentisering/kryptering, også for Zero Trust)

Det er vanskelig å si noe generisk om hvor og hvordan disse enhetene brukes i dag, men hvis en skal vurdere angrepspunkter og avhengigheter må disse tas med. Hvis en vil redusere disse mulighetene, må i det minste IT og OT skal ha egne funksjoner. En må heller ikke glemme de mulige avhengighetene som kan finnes allerede i dagens løsninger med felles nettverk og signaler mellom enheter både innen SIS og mellom SIS og PCS.

En ser i en del av initiativene for å integrere informasjon fra IT/OT-systemene i skyløsninger eller annet, at nivåene i Purdue-modellen er under press og at det åpnes opp for at kantenheter, IIoT og andre kan høste informasjon og bringe den ut. Selv om hver enkelt forbindelse virker bra sikret, er det store antallet av forbindelser en utfordring da sikringen er ferskvare og må oppdateres og vedlikeholdes. Nye utfordringer relatert til skyløsninger blir også innført ved 5G, hvor mobiloperatører kan få tilgang til konfigurasjon og oppsett av 5G infrastruktur på innretninger via skybaserte tjenester.

6.3 I hvilken grad vil Ptils krav til uavhengighet være oppfylt?

Vi kan først konkludere med at det er vanskelig å gi et definitivt svar på om kravene til uavhengighet er oppfylt. Ptil sitt generelle krav (styringsforskriften §5) om at det skal være "*tilstrekkelig uavhengighet mellom barrierene*" er subjektivt og derfor vanskelig å verifisere, utover det som sies i veiledningen om at "*flere*

viktige barrierer ikke skal kunne svekkes eller settes ut av funksjon samtidig, blant annet som følge av en enkelt feil eller en enkelt hendelse". Dette utdypes videre i innretningsforskriftens §§ 32-34 som krever at henholdsvis brann- og gassdeteksjonssystemet, nødavstengningssystemet og prosessikringssystemet skal utføre tiltenkte funksjoner uavhengig av andre systemer, og ikke bli negativt påvirket av feil i disse systemene.

Sistnevnte krav er mer håndfaste og følgende observasjoner og kommentarer kan knyttes til dem:

- Som diskutert i avsnitt 2.3 inneholder dagens risiko- og pålitelighetsanalyser i begrenset grad detaljerte vurderinger av koblinger og avhengigheter mellom systemer
- Som en følge av økt kompleksitet og flere koblinger er det svært utfordrende å vise at enhver feil som kan opptre i et system ikke kan påvirke et annet system negativt
- Leverandørene synes generelt ikke å ha standarddokumentasjon som viser at deres løsning gir full uavhengighet og/eller ikke påvirker andre systemer negativt
- Operatørene har heller ikke noe slik dokumentasjon

Dersom en skal forsøke seg på et svar på spørsmålet i overskriften må det derfor bli: Det kan hende at kravene om uavhengighet er oppfylt, men det finnes ikke dokumentasjon som viser det.

Denne diskusjonen kan også knyttes til Ptil sin nye definisjon av risikobegrepet som i veiledning til rammeforskriften §11 sier at "*med risiko menes konsekvensene av virksomheten med tilhørende usikkerhet*". I presiseringen om "tilhørende usikkerhet" ligger det at graden av kompleksitet i - og kunnskap om fenomenene, systemene og operasjonene en står overfor skal vektlegges i risikostyringen.

Siden dagens risiko- og pålitelighetsanalyser i begrenset grad tar for seg eller studerer det relativt komplekse fenomenet avhengighet, og dokumentasjon av uavhengighet er til dels fraværende, kan en konkludere med av usikkerheten, og dermed risikoen, knyttet til mulige ukjente avhengigheter er betydelig.

7 Behov for endringer i Petroleumtilsynets regelverk

7.1 Bakgrunn

I Stortingsmelding 38 (2016-17) om IKT-sikkerhet tas det - basert på anbefalinger fra Lysne utvalget (2015) – til orde for at

> "*det bør foreligge krav fra tilsynsmyndigheten (Ptil) om at det skal være etablert barrierer mot digitale sårbarheter*" (avsnitt 13.2).

Det sies videre at

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

Som diskutert i avsnitt 2.4 har Ptil sitt regelverk og tradisjonell barrierestyring først og fremst handlet om å ha kontroll på energien, mens informasjonsområdet kun har vært relevant i den grad det kan påvirke energiområdet negativt og ha potensial til å medføre fysisk skade. Som et resultat av tettere koblinger og nye digitale avhengigheter som diskutert i denne rapporten, er det derfor på sin plass å spørre hvorvidt regelverket i enda større grad bør presisere behovet for å etablere barrierer mot digitale sårbarheter som kan medføre uønsket informasjonsflyt, utover det som en rent umiddelbart kan identifisere at kan påvirke energiområdet.

Det er også rimelig å spørre hvorvidt Ptil sitt regelverk bør oppdateres i forhold til hvilke standarder og retningslinjer knyttet til IKT-sikkerhet som refereres.

7.2 Diskusjon rundt mulige justeringer av regelverket

Regelverket for petroleumsvirksomheten bygger på en del fundamentale prinsipper, som skal sikre en god sikkerhets- og risikostyring. Sentralt her står en tenkning som i stor grad vektlegger funksjonskrav – hva en ønsker oppnådd – framfor detaljkrav som spesifiserer hvilke løsninger og tiltak som må velges [48]. Det er her naturlig å ta tak i funksjonskravet om *tilstrekkelig uavhengighet* i den videre diskusjonen om behov for eventuelle endringer og presiseringer i regelverket for å sikre at IKT-sikkerhet blir tatt høyde for ved valg av løsninger for å oppfylle av dette kravet.

Styringsforskriftens §5 innleder med kravet om å etablere nødvendige barrierer som vil ha en direkte rolle i å unngå eller redusere faren for ulykker og begrense skader. I praksis leses denne forskriften i betydning av barrierer som kan kontrollere eller redusere energi. Med digitale angrep kan tap av kontroll med informasjon og data medføre hendelser som svekker de tradisjonelle barrierene. Barrierer som har til hensikt å forhindre tap av kontroll med informasjon og data vil fremover få en økt betydning for sikkerhet i industrielle anlegg. SINTEF mener derfor at regelverket kan være mer eksplisitte når det gjelder å presisere behovet for IKT-barrierer, herunder en barrierefunksjon som hindrer uønsket informasjonsflyt, og hvordan disse er koblet til ytelsen av barrierer som beskytter tap av kontroll med energi.

I innretningsforskriftens §32 til 34 presiseres krav til at sentrale sikkerhetssystemer skal utføre tiltenkte funksjoner uavhengig av andre systemer. I forbindelse med veiledningen til disse paragrafene kan det vurderes å utvide perspektivet for hva som må vurderes i kravet om uavhengighet: I tillegg til krav til (tilstrekkelig) uavhengighet i den tekniske utformingen og oppfølgingen av PCS og SIS, vil det være viktig å stille krav om tilstrekkelig uavhengighet mellom IKT-hendelser og mulige svekkelser av PCS og SIS som

barrierer. I veiledningen kan det eksempelvis pekes på betydningen av IKT-barrierer ("counter measures") som tiltak for å opprettholde uavhengighet mellom barrierefunksjoner.

Under er noen mulige tilnærminger kort diskutert.

7.2.1 Forslag vedrørende Ptils Styringsforskrift § 5 Barrierer

Styringsforskriftens §5 dekker på en tilstrekkelig måte de overordnede kravene til barrierer. Én mulighet for å fremheve informasjonsområdet ytterligere kan da være å eksemplifisere utdypningen av barrierefunksjonsbegrepet i veiledningen som følger:

> *Eksempler på barrierefunksjoner er det å forhindre lekkasje, forhindre antenning, redusere brannbelastning, forhindre uønsket informasjonsflyt, sikre forsvarlig evakuering og forhindre hørselsskade*

Selv om en nok kan argumentere med at fenomenet uavhengighet er bakt inn i begrepene pålitelighet og integritet, kan på den annen side industriens mangelfulle fokus på å verifisere uavhengighet kanskje berettige at eksemplifisering av ytelse utvides:

> *Med ytelse menes verifiserbare krav til blant annet kapasitet, pålitelighet, tilgjengelighet, uavhengighet, effektivitet, evne til å motstå laster, integritet og robusthet.*

Ytterligere utdypninger av barrierefunksjonen *forhindre uønsket informasjonsflyt* og krav til uavhengighet kan for eksempel innarbeides i neste oppdatering av Ptil sitt barrierenotat [45], se avsnitt 7.2.3 under. Det kan også vurderes om hvorvidt et økt fokus på IKT-barrierer kan oppnås gjennom justeringer av andre paragrafer som styringsforskriftens §§ 15-16.

7.2.2 Forslag vedrørende henvisninger i Ptils innretningsforskrift §32-34

Basert på diskusjoner med industrien og SINTEFs forståelse av relevante standarder knyttet til IKT-sikkerhet, anbefaler vi at Ptil vurderer å henvise til IEC 62443-serien (se avsnitt 3.1) i veiledningen til §32 til 34 i innretningsforskriften. Denne standarden er allerede mye brukt, også internasjonalt[4], og den inneholder flere krav, som hvis implementert, kan bidra til uavhengighet. Allerede i dag har enkelte norske operatører utviklet en "profil" som inneholder utvalgte IEC 623443 krav som de benytter i sine prosjekter, og det kan for eksempel være aktuelt for Ptil gjennom målrettede tilsyn å se nærmere på hvorvidt disse kravene er oppfylt.

Som diskutert i avsnitt 3.1 foreligger de ulike delene av IEC 62443-serien i varierende grad i oppdaterte eller offisielle versjoner, og dette må i så fall vurderes spesielt dersom standarden eller utvalgte deler av den skal henvises til. I forhold til fastsettelse av "security"-nivå (SL) og tilhørende tekniske systemkrav er delstandard 3-2 og 3-3 spesielt aktuelle. Disse er begge utgitt i offisielle versjoner fra henholdsvis 2020 og 2013, men sistnevnte er åpnet for revisjon.

[4] USA synes imidlertid å forholde seg primært til NIST 800-82, som tematisk er lik IEC 62443-serien, men på enkelte områder har en noen annen tilnærming [54]

7.2.3 Forslag vedørende Ptils Barrierenotat 2017

Ptil sitt barrierenotat beskriver prinsipper for barrierestyring i petroleumsvirksomheten i Norge. Notatet utdyper og eksemplifiserer regelverkets intensjoner knyttet til barrierstyring og inneholder en rekke eksempler på barrierefunksjoner og ytelseskrav, herunder et vedlegg (7.1) som tar for seg fysisk sikring (hindre uautorisert tilgang).

Tatt i betraktning de fremtidige utfordringer som beskrevet i denne rapporten, og i forlengelsen av anbefalingen over om ta inn IKT-barrierer, og herunder definere "forhindre uønsket informasjonsflyt" som en egen barrierefunksjon, er det rimelig at også barrierenotatet oppdateres tilsvarende.

8 Hovedkonklusjoner og anbefalinger

I dette kapitlet oppsummeres SINTEFs forslag til tiltak for henholdsvis næringen og for Ptil, samt behov for videre arbeid med kunnskapsinnhenting.

8.1 Anbefalinger til næringen

Anbefalinger til tiltak for næringen er gitt i Tabell 4.

Tabell 4: Oppsummering av anbefalinger til tiltak for næringen

Nr.	Utfordring	Anbefaling	Ref.
Dagens løsninger			
1.	Selv i dagens løsninger kan det være mange felles funksjoner og systemer. Noen eksempler kan være domenekontrollere, backup-systemer, autentisering og «active directory».	Unngå eller redusere bruken av systemer og komponenter som er felles for SIS og andre IT/OT-systemer og der det ikke kan unngås, etabler multiple barrierer for å forebygge angrep mot felles løsninger.	6.2
2.	Dagens SIS og PCS systemer har begrenset beskyttelse mot digitale angrep.	Selv om en har en rekke tiltak, er det behov for ytterligere tiltak. En må sørge for at disse systemene beskyttes mot angrep på andre måter.	2.5
3.	Effekten av å bruke adskilte nettverk for SIS og PCS kan være begrenset, da det er mange meldinger som må gå mellom disse nettverkene. Eksempler kan være synkronisering av PCS ved nedstengning og tilbakemeldinger på endebrytere.	En bør ikke stole på at adskilte nettverk gir full uavhengighet, men innføre/beholde andre tiltak for å unngå avhengigheter og uønsket påvirkning.	2.5
4.	Datadioder er nyttige for å hindre påvirkning av senderen, men de åpnes ofte opp for konfigurering og annen trafikk. Dette fører til komplisert konfigurering og stadige endringer.	Sørge for at andre metoder brukes hvis en må midlertidig inn i OT komponenter utenfra, slik at datadiodene ikke må gjennomhulles av denne type kommunikasjon.	4.1
5.	Sikkerhetsprofiler som PROFIsafe gir dårlig beskyttelse mot angrep.	Sørge for at slik kommunikasjon er ytterligere beskyttet mot uønsket påvirkning vha. tilleggsmekanismer når den kan være tilgjengelig utenfra (soner og tunneler e.l.).	5.1
6.	Uavhengighetskravene i Appendix G i Norsk olje og gas 070 er ikke tilstrekkelig kjent blant de som jobber med IKT-sikkerhet hos leverandørene.	Denne gruppen bør også gjøres bedre kjent med disse kravene.	3.7
7.	Appendix G i Norsk olje og gass 070 er til dels mangelfull når det gjelder beskyttelse mot påvirkning fra andre systemer, fjerntilgang og henting av informasjon til for eksempel skyløsninger.	I forbindelse med en fremtidig oppdatering av Norsk olje og gass 070 bør Appendix G revideres, herunder bedre hensynta risikomomenter knyttet til IKT-sikkerhet og nye løsninger for å dele data mellom OT- og IT-nivå.	3.7 4.6
8.	Det er utfordrende å oppfylle kravene om uavhengighet mellom PCS og SIS som er en forutsetning i både IEC 61508 og IEC 61511 for å kunne oppfylle SIL.	Sørge for at kravet er oppfylt også etter at OT-systemene er satt i drift og nødvendig utveksling av signaler er implementert.	3.2

Nr.	Utfordring	Anbefaling	Ref.
9.	Analyser og dokumentasjon av at dagens løsninger er uavhengige, er mangelfulle og analysemetodene som anvendes er ikke nødvendigvis utviklet for dette formålet, herunder at IKT-sikkerhet og funksjonell sikkerhet i begrenset grad blir vurdert i sammenheng.	Gjennomføre mer detaljerte og målrettede analyser som ser spesielt på koblinger og mulige avhengigheter mellom systemer også i forhold til IKT-trusler.	2.3
10.	Flere leverandører har begynt å sertifisere sine løsninger og arbeidsmetoder, men det er uklart hva dette gir av gevinst.	Vurdere om/hvordan sertifisering av utstyr og arbeidsmetodikker vil være et kostnadseffektivt tiltak.	3.1
Nye løsninger			
11.	Mange initiativer som jobber med digitalisering, ser ut til å medføre at lagene i Purdue-modellen forsvinner.	Sørge for at beskyttelsen som lagene i Purdue-modellen skulle gi, blir ivaretatt på andre måter.	4
12.	Økt kompleksitet i nettverkene, flere enheter og flere koblinger gir flere mulige avhengigheter. Flere enheter og flere koblinger gir flere angrepsveier.	Redusere kompleksitet og antall koblinger og ha streng kontroll på de som må finnes så de ikke kan påvirke OT-systemene negativt.	6.3
13.	Lokale 5G-systemer på installasjonene kan bli brukt for å hente ut data fra enheter på alle nivåer i Purdue-modellen. Telekom firmaene må utvikle kunnskap om kravene til uavhengighet.	Hvis en innfører 5G som kommunikasjonsmedium, må en sørge for at bruk av felles sentrale komponenter ikke kan føre til uønskede hendelser og avhengigheter.	4.3
14.	Selv med lokale 5G systemer på installasjonene, kan telekom firmaer få tilgang til kritisk felles infrastruktur på installasjonen for vedlikehold og konfigurering.	Sørge for at bruk av 5G ikke gir felles maskin- og programvare som kan benyttes som springbrett og ødelegge uavhengigheten for eksempel mellom SIS og PCS.	4.3
15.	5G vil i fremtiden representere en global teknologiplattform som brukes innenfor industri, energi, helse, forsvar, transport, m.m. Dette gjør 5G spesielt attraktivt for ondsinnede aktører.	Utarbeide retningslinjer for forsvarlig drift og vedlikehold av 5G nett med tanke på IKT-sikkerhet – gjerne i samarbeid med andre bransjer med tilsvarende behov.	4.3
16.	Kantenheter (Edge) og annet som brukes for å høste data fra OT, bruker som regel protokoller som enten gir forespørsler eller kvitteringer inn i OT-systemene. De meldingene som går inn i systemene, kan utnyttes til å påvirke OT-systemene negativt.	Benytte for eksempel datadioder eller OPC UA sin PubSub for å hindre meldinger inn til OT-systemene.	5.5
17.	Håndholdte enheter tas i bruk i første omgang for å gi informasjon til feltoperatørene. Dette kan lett endre seg til at den håndholdte enheten også kan sende informasjon til OT. Operatørene kan feilaktig stole på informasjonen fra de håndholdte enhetene.	Sørge for at informasjon på håndholdte enheter ikke brukes til sikkerhetskritiske operasjoner og at informasjon fra dem ikke påvirker OT-systemene.	4.5

Nr.	Utfordring	Anbefaling	Ref.
Standarder og retningslinjer			
18.	Bruk av IEC 62443 garanterer ikke uavhengighet, men kan bidra til dette hvis de rette kravene identifiseres og implementeres	Utvikle "profiler" basert på kravene i IEC 62433 som dokumenter og begrunner valg av relevante krav som bidrar til uavhengighet.	3.1 5.4
19.	Namur Open Architecture (NOA) betraktes av mange som et lovende initiativ for å hente ut informasjon fra eksisterende anlegg, men det står eksplisitt at NOA ikke skal brukes mot SIS ("out of scope").	Sørge for at bare akseptable løsninger brukes for kobling mot SIS.	4.2.3
20.	For lave krav (SL-nivå) knyttet til SIS er utfordrende. Med lavere bemanning, bruk av kantenheter og IIoT må en trolig gi flere personer og organisasjoner tilgang oftere og kanskje permanent gjennom tilgangssystemet.	Vurdere om SIS-sonen bør ha høyere beskyttelse så den også er godt beskyttet både mot utilsiktet og tilsiktet påvirkning fra det/de som bevisst slippes gjennom inn i IT/OT-systemene.	3.4

8.2 Anbefalinger til Ptil

Anbefalinger til tiltak for Ptil er gitt i Tabell 5.

Tabell 5: Oppsummering av anbefalinger til tiltak for Ptil

Nr.	Utfordring	Anbefaling	Ref.
1.	Analyser og dokumentasjon av at dagens løsninger er uavhengige, er mangelfulle.	Behold kravene om uavhengighet, men klargjør hva som kreves for å dokumentere at de er oppfylt. Vurder å presisere at krav til ytelse for barrierer også skal inkludere krav til uavhengighet fra andre systemer.	6.3 7.2
2.	Det er utfordrende å finne krav eller veiledning i dagens regelverk som presiserer behovet for å etablere barrierer knyttet til IKT-sikkerhet.	Vurder hvorvidt tekst i styringsforskriftens §5 og/eller innretningsforskriftens §§ 32-34 med tilhørende veiledninger kan justeres for å sette økt søkelys på behovet for barrierer knyttet til IKT-sikkerhet, herunder at beskyttelse mot uønsket dataflyt og påfølgende negativ påvirkning må behandles som en barrierefunksjon. Se videre på om dette krever justering av flere paragrafer i forskriften (som styringsforskriftens §§ 15-16).	7.2
3.	Ptil sitt barrierenotat omtaler fysisk sikring, men har begrenset fokus på IKT-sikkerhet.	Vurder å inkludere ny(e) barrierefunksjon(er) i neste oppdatering av barrierenotatet.	7.2.3
4.	Regelverkets referanser til standarder for industriell IKT-sikkerhet framstår som mangelfulle.	Det anbefales at Ptil vurderer å henvise til deler av IEC 62443-serien for industriell IKT-sikkerhet. Denne standarden er allerede mye brukt, også internasjonalt, og spesielt delstandard 3-3 inneholder flere systemkrav som hvis de implementeres kan bidra til uavhengighet.	3.1 7.2.2
5.	Til tross for at operatører allerede i dag bruker IEC 62443 i nye prosjekter er det ikke gitt at alle kravene som kan gi økt uavhengighet inkluderes.	Vurder å gjøre operatørenes kravprofiler og deres oppfyllelse av utvalgte krav gjenstand for tilsyn.	3.1 7.2.2

Nr.	Utfordring	Anbefaling	Ref.
6.	Det er ikke identifisert analyser eller dokumentasjon hos leverandørene som viser at de har uavhengighet mellom for eksempel PCS og SIS.	Utfør tilsyn der en går i dybden på uavhengighet og etterspør analyser og annet som dokumenterer hvorvidt kravene for eksempel i innretningsforskriften er oppfylt.	2.3 6.3

8.3 Behov for kunnskapsinnhenting

Anbefalinger om fremtidig behov for kunnskapsinnhenting og videre forskning og utvikling på området er gitt i Tabell 6.

Tabell 6: Anbefalinger knyttet til behovet for kunnskapsinnhenting

Nr.	Anbefaling
1.	Det er ikke innlysende hvordan en skal analysere og dokumentere at kravene om uavhengighet er oppfylt. En bør derfor se videre på egnet analysemetodikk, for eksempel gjennom å hente ideer fra andre industrier (som kjernekraftindustrien og luftfart).
2.	Innføring av 5G på innretninger byr på et sett av utfordringer som ikke nødvendigvis er åpenbare, siden 5G er en ny teknologi med nye verdikjeder og forretningsmodeller. Her er det et åpenbart kunnskapsbehov, og ikke minst et behov for kunnskapsspredning til bransjen – helst i **forkant** av fremtidige 5G-utrullinger.
3	Som diskutert i denne rapporten inneholder Ptils regelverk og relevante standarder og rapporter i begrenset grad konkrete råd om hvordan en på best mulig måte oppnår uavhengighet mellom systemer, herunder både IT- og OT-systemer. Det er derfor behov for spesifikke retningslinjer, også knyttet til hvordan en kan unngå at digitale angrep (via åpne plattformer) kan føre til avhengigheter. Som en del av dette ser vi også et behov for en komplett gjennomgang og oppdatering av Appendix G i Norsk olje og gass retningslinje 070.
4.	Det er behov for å utvikle prinsipper for barrierstyring i forhold til cyberangrep – jf. pågående SINTEF-prosjekt: "Cybersecurity Barrier Management"
5.	Det er behov for å utvikle metoder og retningslinjer for praktisk bruk av datadioder, for eksempel knyttet til oppdateringer og rekonfigureringer.
6.	LOPA metodikken blir stadig mer utbredt og forutsetter, som en basisantagelse, uavhengighet mellom de ulike beskyttelseslagene. Det bør vurderes hvorvidt LOPA metodikken kan forbedres gjennom å utvikle og inkludere en systematisk gjennomgang av mulige avhengigheter mellom beskyttelseslagene som en del av metoden.

Referanser

[1] AutomationML, What is AutomationML? https://www.automationml.org/about-automationml/automationml/ (nedlastet 10.11.2021)

[2] Bell, D. E. Bell (2005). Looking back at the Bell-La Padula model. *21st Annual Computer Security Applications Conference (ACSAC'05)* pp. 15 pp.-351. https://ieeexplore.ieee.org/document/1565261

[3] Bridges, W. and A. M. Dowell (2021). More issues with layer of protection analysis—From the originators. *17th Global Congress on Process Safety, April 18–23.* https://doi.org/10.1002/prs.12295

[4] Bundesamt fur Sicherheit in der Informationstechnik, Deutches IT-Sicherheitszertifikat, Arbit Data Diode 10 GbE, v1.00, Common Criteria Part 3 conformant EAL 7 augmented by ALCFLR.1. https://www.commoncriteriaportal.org/files/epfiles/1096c_pdf.pdf. (nedlastet 10.11.2021)

[5] Cheswick, B. (1990). The design of a secure internet gateway. *USENIX Summer Conference Proceedings*.https://cheswick.com/ches/papers/gateway.pdfhttps://cheswick.com/ches/papers/gateway.pdf

[6] Cruzes, D. S., M. G. Jaatun, I. A Tøndel, K. Bernsmed (2020). Sju steg til bedre programvaresikkerhet, Computerworld Norge. https://www.cw.no/debatt-sikkerhet-sintef-digital/sju-steg-til-bedre-programvaresikkerhet/402011

[7] DIN. Industy 4.0 – Success with standards. https://www.din.de/en/innovation-and-research/industry-4-0 (nedlastet 10.11.2021)

[8] DNV. Cyber Secure class notation. https://www.dnv.com/services/cyber-secure-class-notation-124600 (nedlastet 10.11.2021)

[9] DNV-RP-G108 (2021). Cyber security in the oil and gas industry based on IEC 62443. https://www.dnv.com/cybersecurity/recommended-practices/dnv-rp-g108-cyber-security-in-the-oil-and-gas-industry-based-on-IEC-62443.html

[10] Dragos. TRISIS Malware - Analysis of Safety System Targeted Malware. https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf (nedlastet 10.11.2021)

[11] FFI (2002). Firewall Technology. Publication-2002/01741 https://www.researchgate.net/publication/289377757_Firewall_Technology

[12] Guzman, N. H. C., I. Kozine, and M. A. Lundteigen (2021). An integrated safety and security analysis for cyber-physical harm scenarios. *Safety Science, Volume 144.* https://doi.org/10.1016/j.ssci.2021.105458

[13] Guzman, N. H. C., D. K. M. Kufoalor, I. Kozine, and M. A. Lundteigen (2021). Combined Safety and Security Risk Analysis using the UFoI-E method: A Case Study of an Autonomous Surface Vessel, In M. Beer & E. Zio (Eds.), *29th European Safety and Reliability Conference (ESREL)*. http://rpsonline.com.sg/proceedings/9789811127243/html/0208.xml

[14] IEC 60050. Vocabulary, https://www.standard.no/nettbutikk/sokeresultater/?search=60050

[15] IEC 61508. Functional safety of electrical/electronic/programmable electronic safety-related systems.https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=265022. (nedlastet 10.11.2021)

[16] IEC 61511. Functional safety - Safety instrumented systems for the process industry sector. https://www.standard.no/nettbutikk/sokeresultater/?search=61511 (nedlastet 10.11.2021)

[17] IEC 61784-3 (2021). Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions, https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=1341211

[18] IKT Norge. Industri 4.0 – digitalisering av tradisjonell industri, https://www.ikt-norge.no/tema/industri-4-0-digitalisering-av-tradisjonell-industri/ (nedlastet 10.11.2021)

[19] Jones, D. W, and T. C. Bowersox. (2006) Secure Data Export and Auditing using Data Diodes, USENIX Electronic Voting Technology Workshop (EVT '06).

https://www.usenix.org/legacy/events/evt06/tech/full_papers/jones/jones_html/. (nedlastet 12.11.2021)
[20] Kang M.H. and I.S. Moskowitz (1993) A pump for rapid, reliable, secure communication. In *Proceedings of the 1st ACM Conference on Computer and Communications Security*. pp. 119-129. https://dl.acm.org/doi/pdf/10.1145/168588.168604
[21] Køien, G.M. (2021). Zero-Trust Principles for Legacy Components. *Wireless Pers Commun 121.* pp. 1169–1186. https://doi.org/10.1007/s11277-021-09055-1
[22] Ma, Z., A. Hudic, A. Shaaban, and S. Plosz (2017). Security Viewpoint in a Reference Architecture Model for Cyber-Physical Production Systems. *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pp. 153-159, https://doi.org/10.1109/EuroSPW.2017.65
[23] NAMUR, Automation Modular Plants, https://www.namur.net/en/focus-topics/automation-modular-plants.html (nedlastet 10.11.2021)
[24] NAMUR, NAMUR Open Architecture, https://www.namur.net/en/focus-topics/namur-open-architecture/ (nedlastet 10.11.2021)
[25] National Cyber Security Centre. Device Security Guidance. https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device
[26] NEK 820 (2021). Cybersikkerhet for industrielle automatiserings- og kontrollsystemer. https://www.nek.no/produkter/nek-820/
[27] NEK CLC/TS 50701 (2021). Railway Applications – Cybersecurity. https://www.standard.no/nettbutikk/sokeresultater/?search=50701
[28] NFEA Webinar (2020), Digitalization of Automation Systems Part 1, https://nfea.no/arrangementer/digitalization-of-automation-systems-2020/
[29] NIST (2007). Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. Special Publication 800-38D. https://doi.org/10.6028/NIST.SP.800-38D
[30] NIST (2018). Framework for Improving Critical Infrastructure Version. 1.1. https://doi.org/10.6028/NIST.CSWP.04162018
[31] NIST (2020). Zero Trust Architecture. Special publication 800-207. https://doi.org/10.6028/NIST.SP.800-207
[32] Norsk olje og gass (2013). 104 Recommended guidelines for information security baseline requirements for process control, safety and support ICT systems. https://norskoljeoggass.no/en/working-conditions/retningslinjer/integrated-operations/104-recommended-guideline/
[33] Norsk olje og gass (2020). 070 Guidelines for the Application of IEC 61508 and IEC 61511 in the petroleum activities on the continental shelf (Recommended SIL requirements). https://norskoljeoggass.no/en/working-conditions/retningslinjer/health-working-environment-safety/technical-safety/070-guidelines/
[34] NORSOK I-002 (2021). Industrielle automasjons- og kontrollsystemer. https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=1382300
[35] NOU 2000:24 (2000). Et sårbart samfunn – Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet. https://www.regjeringen.no/no/dokumenter/nou-2000-24/id143248/
[36] NOU 2018:14 (2018). IKT-sikkerhet i alle led, Organisering og regulering av nasjonal IKT-sikkerhet. https://www.regjeringen.no/no/dokumenter/nou-2018-14/id2621037/
[37] NS 5830 (2012). Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger - Terminologi, https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=532802
[38] NSM (2020). NSMs Grunnprinsipper for IKT-sikkerhet (v2.0) https://nsm.no/getfile.php/133735-1592917067/Demo/Dokumenter/Veiledere/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf

[39] OPC Foundation. Unified Architecture (UA), https://opcfoundation.org/about/opc-technologies/opc-ua/ (nedlastet 04.11.2021)
[40] OPC Foundation (2018). OPC 10000-14: OPC Unified Architecture Part 14: PubSub. Release 1.04. https://reference.opcfoundation.org/Core/docs/Part14/
[41] Open Process Automation Forum, https://www.opengroup.org/forum/open-process-automation-forum. (nedlastet 10.11.2021)
[42] Petroleumstilsynet. IKT-sikkerhet i industrielle systemer. https://www.ptil.no/fagstoff/utforsk-fagstoff/fagartikler/2021/ikt-sikkerhet-i-industrielle-systemer/ (nedlastet 10.11.2021)
[43] Petroleumstilsynet. Innretningsforskriften. https://www.ptil.no/regelverk/alle-forskrifter/?forskrift=634 (nedlastet 10.11.2021)
[44] Petroleumstilsynet. Styringsforskriften. https://www.ptil.no/regelverk/alle-forskrifter/?forskrift=611 (nedlastet 10.11.2021)
[45] Petroleumstilsynet (2017). Prinsipper for barrierestyring i petroleumsvirksomheten. Barrierenotat 2017. https://www.ptil.no/fagstoff/utforsk-fagstoff/fagartikler/2017/barrierenotat/
[46] Petroleumstilsynet. Ord og uttrykk, https://www.ptil.no/fagstoff/ord-og-uttrykk/ (nedlastet 10.11.2021)
[47] Plattform Industrie 4.0, Reference Architectural Model Industrie 4.0 (RAMI4.0) - An Introduction, https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/rami40-an-introduction.html. (nedlastet 10.11.2021)
[48] Proactima (2020). Bruk av risikoakseptkriterier - en evaluering. Rapportnr 1073586-RE-01 https://www.ptil.no/contentassets/4deea346d8cb4008a2eef488f85313ae/bruk-av-risikoakseptkriterier---en-evaluering.pdf
[49] Riksrevisjonen (2021). Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen, Dokument 3:7 (2020-2021), https://www.riksrevisjonen.no/globalassets/rapporter/no-2020-2021/nves-arbeid-med-ikt-sikkerhet-i-kraftforsyningen.pdf
[50] Security Compass, Building a Cybersecurity Program for Industrial Control Systems, https://resources.securitycompass.com/blog/cybersecurity-for-industrial-control-systems (nedlastet 10.11.2021)
[51] SINTEF (2006). Uavhengighet av sikkerhetssystemer offshore - status og utfordringer. Rapport STF50 A06011. https://sintef.brage.unit.no/sintef-xmlui/handle/11250/2375920
[52] SINTEF (2021). Grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer. Rapport 2021:00055 https://www.ptil.no/globalassets/fagstoff/prosjektrapporter/ikt-sikkerhet/id4-grunnprinsipper-for-ikt-sikkerhet_sintef-rapportnr-2021-00055-feb---signert.pdf
[53] SINTEF (2021) Regulering av IKT-sikkerhet i petroleumssektoren. Rapport 2021:00054, https://www.ptil.no/globalassets/fagstoff/prosjektrapporter/ikt-sikkerhet/id3-regulering-av-ikt-sikkerhet.pdf
[54] SINTEF INFOSEC (2018). Digitale signaturer. https://infosec.sintef.no/informasjonssikkerhet/2018/10/digitale-signaturer/
[55] SINTEF INFOSEC (2018). Kryptografiske hash-funksjoner. https://infosec.sintef.no/informasjonssikkerhet/2018/10/kryptografiske-hash-funksjoner/
[56] Strand, M. (2021). A Status Update on Quantum Safe Cryptography. *2021 International Conference on Military Communication and Information Systems (ICMCIS).* pp. 1-7. https://ieeexplore.ieee.org/abstract/document/9486413
[57] The Internet Society (2003). Counter with CBC-MAC (CCM). IETF Request for Comments: 3610 https://tools.ietf.org/html/rfc3610
[58] Vasileios, M., K. Vishi, M. D. Zych, and A. Jøsang (2018): The Impact of Quantum Computing on Present Cryptography. *International Journal of Advanced Computer Science and Applications, Vol. 9.*

No. 3. https://thesai.org/Downloads/Volume9No3/Paper_54-The_Impact_of_Quantum_Computing.pdf

[59] Wagner, C. et al. (2017). The role of the Industry 4.0 asset administration shell and the digital twin during the life cycle of a plant, *22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA).* pp. 1-8. https://doi.org/10.1109/ETFA.2017.8247583

[60] Ye, X. and S. H. Hong (2019). Toward Industry 4.0 Components: Insights Into and Implementation of Asset Administration Shells. *IEEE Industrial Electronics Magazine, vol. 13, no. 1*, pp. 13-25. https://doi.org/10.1109/MIE.2019.2893397