2021:00053 - Åpen

Rapport

Datakvalitet ved digitalisering i petroleumssektoren

IKT-sikkerhet – Robusthet i petroleumssektoren 2020

Forfattere
Thor Myklebust, Tor Onshus, Stefan Lindskog, Maria Vatshaug Ottermo, Mary Ann Lundteigen

SINTEF Digital
2021-02-22

SINTEF Digital

Postadresse:
Postboks 4760 Torgarden
7465 Trondheim

Sentralbord: 40005100

info@sintef.no

Foretaksregister:
NO 919 303 808 MVA

Rapport

Datakvalitet ved digitalisering i petroleumssektoren

IKT-sikkerhet – Robusthet i petroleumssektoren 2020

EMNEORD:
Data
Datakilder
Dataflyt
Sikkerhet
Cybersikkerhet
OT-system
IT-system
Standarder

VERSJON
1.1

DATO
2021-02-22

FORFATTER(E)
Thor Myklebust, Tor Onshus, Stefan Lindskog, Maria Vatshaug Ottermo, Mary Ann Lundteigen

OPPDRAGSGIVER(E)
Petroleumstilsynet

OPPDRAGSGIVERS REF.
Arne Halvor Embergsrud

PROSJEKTNR
102022556

ANTALL SIDER OG VEDLEGG:
63 (2 vedlegg)

SAMMENDRAG
Formålet med denne rapporten er å undersøke hvilke datakilder og data som benyttes i industrielle IKT-systemer og hvordan data behandles og prosesseres før de gjøres tilgjengelig i kontornettet. Styrker og sårbarheter knyttet til datakvalitet og sikring av data blir diskutert.

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

UTARBEIDET AV
Thor Myklebust

SIGNATUR
Thor Myklebust
Thor Myklebust (23. Feb. 2021 09:18 GMT+1)

KONTROLLERT AV
Lars Bodsberg

SIGNATUR

GODKJENT AV
Maria Bartnes

SIGNATUR

RAPPORTNR	ISBN	GRADERING	GRADERING DENNE SIDE
2021:00053	978-82-14-06477-3	Åpen	Åpen

MANAGEMENT SYSTEM CERTIFICATION
DNV·GL
ISO 9001 = ISO 14001
OHSAS 18001

Historikk

VERSJON	DATO	VERSJONSBESKRIVELSE
1.0	2021-01-29	Endelig rapport
1.1	2021-02-22	Endelig rapport med oppdatert forfatterliste

Innholdsfortegnelse

Sammendrag

Innledning

Formålet med denne rapporten er å undersøke hvilke datakilder og data som benyttes i industrielle IKT-systemer (OT-systemer) og hvordan data behandles og prosesseres før de gjøres tilgjengelig i kontornettet. Styrker og sårbarheter knyttet til datakvalitet og sikring av data blir diskutert. Vi har vektlagt tilgjengelighet og integritet av data og svakheter i OT-systemer som direkte kan påvirke funksjonell sikkerhet. Arbeidet er i hovedsak basert på dokumentgjennomgang og ni intervju med utvalgte oljeselskap, riggselskap og leverandører.

Datakilder og dataflyt

Vi har lagt vekt på å beskrive typiske SAS løsninger og hvordan dataflyt foregår fra sensor til skyen og helt ned til en håndholdt enhet som ett eksempel. Vi har laget flere figurer for å illustrere dette og inkludert Purdue modellen for å få dette illustrert i forhold til IKT-sikkerhet. Vi har også inkludert mulig kommunikasjon relatert til trådløst feltutstyr. I tillegg har vi beskrevet aktuelle protokoller som UPC UA, da de har blitt nevnt i alle intervjuene og IEC har nå en omfattende standard serie for OPC UA.

Krav til datakvalitet og sikring av data i OT-systemer i standarder og retningslinjer

I forhold til datakvalitet og sikring av data har vi beskrevet krav i aktuelle standarder for funksjonell sikkerhet som IEC 61508 og IEC 61511. For maskinsikkerhet har vi inkludert standardene ISO 13849 og IEC 62061. Hovedvekten har vi lagt på IEC 61508 og IEC 61511 og krav til data. Disse kravene er også ekstrahert og vist i vedlegg. I tillegg har vi beskrevet krav til IKT-sikkerhet basert på IEC 62443 serien. IEC 62443 serien er i sterk utvikling, så både nye oppdateringer av eksisterende standarder og helt nye standarder vil bli utgitt i nærmeste fremtid.

Styrker og sårbarheter knyttet til datakvalitet og sikring av data i OT-systemer

Vi har beskrevet terminologi da det er en stor utfordring for næringen at det ikke eksisterer gode internasjonale standarder og retningslinjer som definerer de aktuelle ord og uttrykkene. Det er derfor inkludert en omfattende oversikt over aktuelle definisjoner basert på flere ulike standarder og retningslinjer, inkludert forslag fra SINTEF til hvordan noen av dem kan defineres.

Videre har vi beskrevet hvordan data behandles og prosesseres. Her har vi spesielt inkludert ett eget avsnitt om tidsstempling da det ble nevnt som en spesiell utfordring under intervjuene.

Vasking har blitt beskrevet, men næringen antar i stor grad at det meste av vaskingen allerede er utført som del av SAS løsningene.

Kontekstualisering ansees som svært viktig av aktørene og det er beskrevet i et eget kapittel. Vi har også omtalt kvalitetssikring av data og noe informasjon rundt IKT-sikkerhet og data.

Anbefalinger

Det er gitt 10 anbefalinger til tiltak for næringen, hvorav seks retter seg mot endringer i standarder og veiledninger, og det er gitt seks anbefalinger til tiltak for Petroleumstilsynet, hvorav tre retter seg mot tilsyn og de øvrige mot forståelse av regelverket og kompetanseheving.

Vi ser behov for innhenting av mer kunnskap og erfaring relatert til datakvalitet. Dette gjelder bl.a. i forhold til dataflyt opp og ned mellom OT, IT og skyen. Både OT- og IT-personell bør inkluderes i dette arbeidet. I tillegg bør man se nærmere på hva som gjøres og hva som bør kreves i forbindelse med kunstig intelligens og maskinlæring.

Executive summary

Introduction

The purpose of this report is to investigate which data sources and data are used in industrial ICT systems (OT systems) and how data is addressed and processed before it is made available in the office network. Strengths and vulnerabilities related to data quality and data safety are discussed. We have emphasized the availability and integrity of data and weaknesses in OT systems that can directly affect functional safety. The work is mainly based on document review and nine interviews with selected oil companies, rig companies and suppliers.

Data sources and data flow

We have emphasized describing typical SAS solutions and how data flow takes place from sensors to the cloud and all the way down to a handheld device as one example. We have developed several figures to illustrate this and included the Purdue model to ensure that this is illustrated in relation to ICT security. We have also included possible communication related to wireless field equipment. In addition, we have described current protocols such as UPC UA, as they have been mentioned in all the interviews and IEC has issued a comprehensive standard series for OPC UA.

Data quality requirements and safety of data in the OT systems in standards and guidelines

In relation to data quality and data safety, we have described requirements in current standards for functional safety such as IEC 61508 and IEC 61511. For machine safety, we have included the standards ISO 13849 and IEC 62061. The main emphasis has been on IEC 61508 and IEC 61511 and requirements for data. These requirements are also extracted and shown in the appendix. In addition, we have described requirements for ICT security based on the IEC 62443 series. The IEC 62443 series is still being developed, so both updates of existing standards and completely new standards will be released in the near future.

Strengths and threats related to data quality and safety in OT systems

We have described terminology as terminology is a challenge for the industry. There are no complete international standard or guideline that define the relevant words and expressions. This report includes a comprehensive overview of current definitions based on several standards and guidelines, including some new proposals from SINTEF.

Furthermore, we have described how data is addressed and processed. Here we have especially included a separate section on time stamping as timestamping was mentioned as a special challenge during the interviews.

Data cleaning has been described, but the industry largely assumes that most of the data cleaning has already been done as part of the SAS solutions.

Contextualisation is considered very important by the actors and it is described in a separate chapter. We have also described quality assurance of data and some information related to ICT security and data.

Recommendations

Ten recommendations have been made for the industry, of which six are aimed at changes in standards and guidelines. Six recommendations are measures for the Petroleum Safety Authority Norway, three of which are aimed at supervision and the others are related to knowledge gap and improved understanding of the regulations.

It is important to acquire more knowledge and experience related to data quality. This applies in relation to data flow up and down between OT, IT and the cloud. Both OT and IT personnel should be included in this work. In addition, one should look more closely at current international work and possible application of artificial intelligence and machine learning.

1 Innledning

1.1 Bakgrunn

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

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

Datakvalitet – *denne rapporten*

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

Notat – IKT-sikkerhet i petroleumsindustrien

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

Veileder IKT-sikkerhet

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

Modellkontrollert operasjon

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

Premisser for digitalisering og integrasjon IT – OT

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

Kommunikasjonsnettverk

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

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

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

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

1.2 Mål og hensikt

Hovedmålet for denne rapporten er å gi næringen økt forståelse av datakvalitet og sikring av data fra de industrielle IKT-systemene på norsk sokkel, med vekt på data fra OT-system til tilgjengeliggjøring i kontormiljøet.

Følgende to målsettinger er definert:

1. Undersøke hvilke data og hvilke datakilder som benyttes i OT-system, og hvordan data behandles og prosesseres før de gjøres tilgjengelig i kontormiljøet.
2. Vurdere styrker og sårbarheter knyttet til datakvalitet og sikring av data i OT-systemer med spesiell vekt på følgende tema:

    a. Datakilder og dataflyt
    b. Sikring/beskyttelse av data, inkludert sårbarhet i forhold til IKT-trusler både for OT- og IT-systemer
    c. Vasking/prosessering/behandling av data
    d. Kontekstualisering
    e. Validering
    f. Kvalitetssikring

I denne rapporten bruker vi begrepet datakvalitet om å ha tilgang til riktige data når det er nødvendig. Vi har fokus på tilgjengelighet og integritet av data og svakheter i IKT-systemer som direkte kan påvirke datakvaliteten.

1.3 Begrensninger

Følgende begrensninger gjelder:

- Konfidensialitet av data og sikring av data mot forsettlige angrep fra ondsinnede individer eller grupper er ikke en vesentlig del av rapporten.
- Dagens løsninger er vektlagt fremfor nye teknologitrender.
- Utfordringer knyttet til ML (maskinlæring) og AI (kunstig intelligens) er ikke vurdert.
- Bruk av data i robotteknologi er ikke vurdert.
- Bruk av data i digital tvilling og modeller er ikke vurdert (Se egen rapport fra delprosjekt 6).

1.4 Begreper, definisjoner og forkortelser

Begreper, definisjoner og terminologi er beskrevet i kapittel 4.1 og vedlegg A. Relevante forkortelser er beskrevet i tabellen nedenfor.

Forkortelse	Beskrivelse
ALARP	As Low As Reasonably Practicable
AI	Aritificial intelligence - kunstig intelligens
API	Application Programming Interface
APIS	Application Programming Interface Specification
APS	Abandon Platform Shutdown
bara	Absolutt trykk målt med enheten bar
barg	Bar gauge - overtrykk, trykket over atmosfæretrykket
BPCS	Basis Process Control System
BOP	BlowOut Preventer - brønnsikringsventil
CAP	Critical Alarm Panel - kritisk alarm panel
CIA	Confidentiality, Integrity and Availability
C&E	Cause and Effect
CM	Condition Monitoring
CMMI-SVC	Capability Maturity Model® Integration – for Services
CPU	Control Proces Unit
CRC	Cyclic Redundancy Check
DMZ	DeMilitarized Zone
DSAL	Data Safety Assurance Level
DSMP	Data Safety Management Plan
ES	Engineering Station
ESD	Emergency ShutDown - nødavstengningssystem
ExS	Expert Station
FD	Fire Detector
F&G	Fire&Gas system - brann- og gassdeteksjonssystem
FTP	File Transfer Protocol
GD	Gas Detector
GPS	Global Positioning System
GW	Gateway
HART	Highway Addressable Remote Transducer
HAZOP	HAZard and OPerability Analysis
HMAC	Keyed-Hash Message Authentication Code
HMI	Human Machine Interface
HTTPS	Hypertext Transfer Protocol Secure
IACS	Industrial Automation and Control System
IEC	International Electrotechnical Commission
IMS	Information Management System
ISA	International Society of Automation
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
ISO	International Standardization Organization
IT	Informasjonsteknologi
KAP	Kritisk Aksjons Panel
ML	Maturity Level

Forkortelse	Beskrivelse
ML	Maskinlæring
MS	Maintenance Station
M+O	Monitoring and Optimization
NIST	National Institute of Standards and Technology
NOA	NAMUR Open Architecture
NOG	Norsk olje og gass
NORSOK	NORsk SOkkels Konkurranseposisjon
NOU	Norges Offentlige Utredninger
NSM	Nasjonal sikkerhetsmyndighet
NTP	Network Time Protocol
OPC	OPC Foundation (a non-profit industry association) formerly an acronym for “OLE for Process Control”.
OPC UA	Open Platform Communication Unified Architecture
ODR	Organisational Data Risk
OT	Operasjonell teknologi
PCS	Process Control - prosesskontrollsystem
PERA	Purdue Enterprise Reference Architecture (PERA). Også kalt ISA95 referansemodell
PES	Programmable Electronic System
PL	Performance Level
PLS	Programmerbar Logisk Styring
Profibus	Process Field Bus
PSD	Process ShutDown - rosessnedstengningssystem
PT	Pressure Transmitter
Ptil	Petroleumstilsynet
P&ID	Piping and Instrumentation Diagram
RA	Remote Access
SAP	Systems Applications and Products
SAS	Safety and Automation System – sikkerhets- og automasjonssystem
SIL	Safety Integrity Level
SIS	Sikkerhetsinstrumenterte systemer
SL	Security level
SRECS	Safety-Related Electrical Control Systems
SRP/CS	Safety-Related Parts of Control System
SCSC	Safety-Critical Systems Club
TCP	Transmission Control Protocol
TSN	Time Sensitive Networking
VPN	Virtual Private Network
UTC	Coordinated Universal Time - koordinert universaltid

1.5 Metode og gjennomføring

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

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

1.6 Rapportstruktur

Kapittel 2 gir eksempler på datakilder, dataflyt og protokoller for OT-systemer i petroleumsvirksomheten på norsk sokkel.

Kapittel 3 oppsummer relevante standarder og retningslinjer for datakvalitet og sikring av data i OT-systemer.

Kapittel 4 gir en vurdering av styrker og sårbarheter knyttet til datakvalitet og sikring av data i OT-systemer, inklusive vasking/prosessering/behandling av data, samt kontekstualisering, validering og kvalitetssikring. Dette kapitlet er basert på intervju med selskaper, gjennomgang av mottatt dokumentasjon fra selskaper, samt litteraturgjennomgang og SINTEFs erfaring og kompetanse innen OT-systemer.

Kapittel 5 oppsummerer SINTEFs anbefalinger til tiltak for næringen og Petroleumstilsynet (Ptil), samt behov for videre arbeid med kunnskapsinnhenting.

Det er 2 vedlegg (A-B), som gjengir utdrag av relevante krav i standarder og retningslinjer knyttet til datakvalitet og sikring av data i OT-systemer.

2 Datakilder og dataflyt i OT-systemer

Historisk har det i industrien vært et skille mellom administrative datasystemer (kontorstøttesystemer) som behandler data og informasjon (IT-og IKT-systemer) og datasystemer som kontrollerer drift og overvåker (OT-systemer) på bore- og produksjonsinnretninger. I Ptils regelverk brukes IKT-systemer om systemer som ivaretar behovet for innhenting, bearbeiding og formidling av data og informasjon (Ref SF §15). Industrielle IKT-systemer brukes generelt om OT-systemer som medfører 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).

OT-systemer på en innretning som tidligere var adskilt fra omverdenen, moderniseres og blir stadig mer komplekse og sammenkoblet med IT-systemer. Dette åpner opp for mer helhetlige løsninger, inkludert styring og overvåking fra land hvor OT-systemer har flere tilkoblingspunkter mot selskapets IT-systemer og forlengelser til eksterne nettverk som skyløsninger via internett. 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.

I det følgende gis først en overordnet beskrivelse av OT-systemer som i henhold til Ptils regelverk utfører sikkerhetsfunksjoner, det vil si kontroll og overvåkingssystemer og instrumenterte sikkerhetssystemer (SIS). Deretter gis det et typisk eksempel på både logisk og fysisk dataflyt mellom IT- og OT-systemer i henhold til Purdue-modellen. Det bemerkes at det kan være flere varianter av figurene for konkrete innretninger.

2.1 Data og datakilder

På en innretning finner man i hovedsak tre adskilte instrumenterte sikkerhetssystemer (SIS) i tillegg til kontrollsystemet. Disse fire går under fellesbetegnelsen SAS (Safety And Automation system):

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

Sikkerhetssystemene skal håndtere farlige hendelser på innretningen. Dette inkluderer å oppdage unormale tilstander, hindre at unormale tilstander utvikler seg til fare- og ulykkessituasjoner og begrense skade ved ulykker (jfr. § 8 i Iinnretningsforskriften [50]). Farlige hendelser kan være at prosesskontrollsystemet svikter, en gasslekkasje eller branntilløp oppstår, eller det oppstår andre hendelser der operatører vurderer det som tryggest å stenge ned. I tillegg er det krav om at ESD- og PSD-systemene er feil-sikre, det vil si at de skal gå til eller forbli i en sikker tilstand dersom det oppstår en feil (i ESD- eller PSD-systemet) som kan hindre systemet i å virke (jfr.§ 33 og 34 i innretningsforskriften). Det er videre krav til at sikkerhetssystemene (ESD, PSD og F&G) skal kunne utføre sine tiltenkte funksjoner uavhengig av andre systemer. Figur 1 viser hvordan de enkelte systemene i SAS henger sammen på en produksjonsinnretning.

I forbindelse med boring har man noen andre systemer og parametere i tillegg til de som er nevnt over, for eksempel:

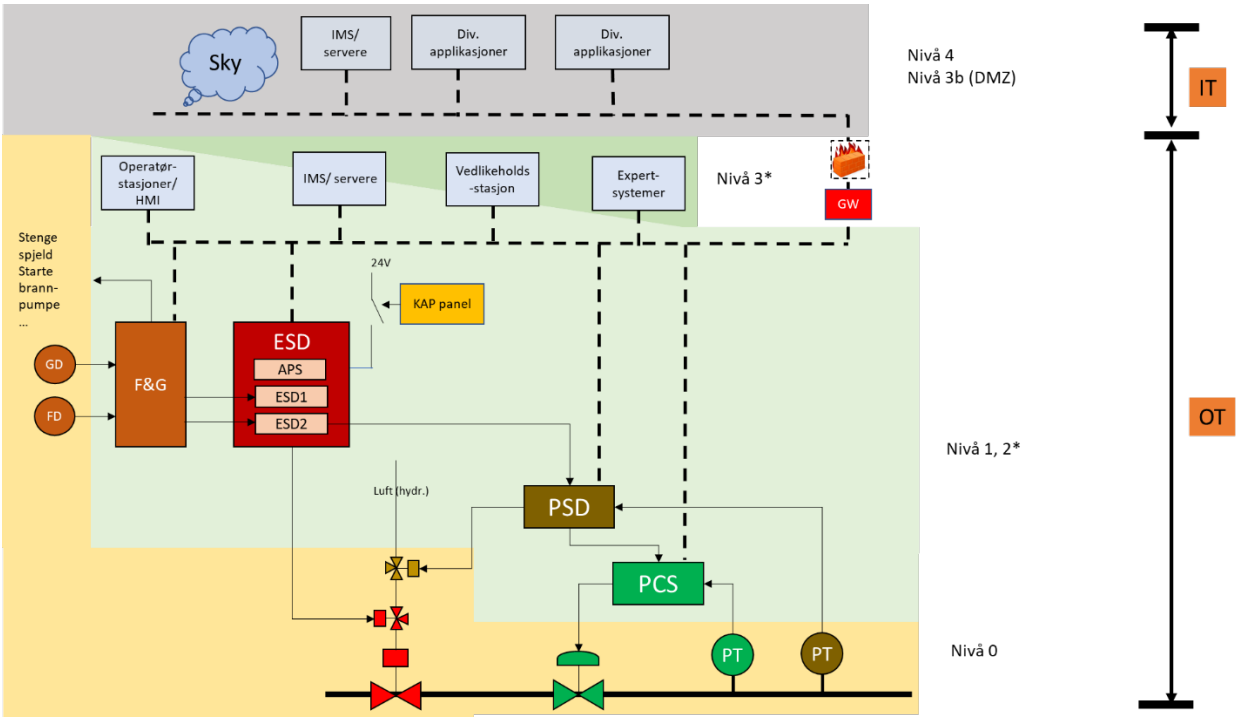
- Brønnsikringsventil (BOP)

- Strømning inn og ut 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 [54])
- Fiskal måling
- Styresystemer brukt ved boring
- Kritiske marine systemer som posisjonering-, ballast- og lense-systemer

Overvåknings, vedlikeholds og konfigurasjonssystemer for feltinstrumenter (se Figur 2) er ikke en del av OT, da de ikke direkte påvirker produksjonen. Se ID3 rapport [62] for flere detaljer.



Figur 1: Prinsippskisse av sammenhengene i SAS

Felles for alle systemene i SAS er at de består av tre delsystemer:

1. Sensorer som konverterer fysiske verdier/tilstander til et målesignal
2. Kontrollere eller logiske enheter (også kalt PLSer – Programmerbar Logisk Styring)
3. Aktivert utstyr (som oftest ventiler og brytere) som griper inn for å håndtere den farlige hendelsen.

Kontrolleren består av følgende hovedkomponenter: inngangskort som mottar signalene fra sensorene, CPU(er) (Central Processing Unit) som utfører logiske operasjoner og utgangskort som setter verdier som sendes til utstyret som skal aktiveres. Her er også sensorer kalt feltinstrumenter, transmittere og detektorer,

avhengig av konteksten. En sensor kan også være en manuell bryter. Samlebetegnelsen feltutstyr brukes når vi mener både sensorer og aktivert utstyr.

PCS-systemet er det som holder prosessen innenfor sikre grenser og sørge for at den daglige driften går best mulig. Regulering og styring er stort sett realisert i dette systemet, men det kan som nevnt over finnes i andre enheter som ikke på samme måte er integrert i SAS.

PSD-systemet har i hovedoppgave å respondere på hendelser som oppstår i produksjonsprosessen. Systemet har egne sensorer for å måle trykk, temperatur, nivå, strømning m.m. og PSD-logikken (vist som firkant med «PSD») vil sammenligne måleverdi med grenseverdier og ta aksjon dersom grensen passeres. Typiske aksjoner i forbindelse med PSD vil være å stenge ventiler og stanse pumper og kompressorer.

F&G-deteksjonssystemet består av kontrollere som får signal fra brann- og gassdetektorer i prosessområder og branndetektorer i boligkvarter og verksteder. F&G-deteksjonssystemet vil sette i gang flere aksjoner, der noen er håndtert av systemet selv, eksempelvis å stenge spjeld i luftinntak og gi signal til slukkesystemer og brannpumper, mens andre aksjoner blir utført av ESD-systemet. Når ESD-systemet mottar signal fra F&G-deteksjonssystemet, så vil ESD-systemet fjerne tennkilder og seksjonere og trykkavlaste områder slik at tennsannsynligheten og eskaleringspotensialet reduseres.

ESD-systemet har i hovedoppgave å isolere tennkilder, seksjonere prosessen i henhold til definerte brannområder (ved å stenge ESD-ventiler), trykkavlaste prosessavsnitt enten manuelt eller automatisk ved å åpne ventiler til fakkel, stenge sikkerhetsventiler på brønner og også sikkerhetsventiler på havbunnen og på rørledninger inn til en innretning. Isolering av tennkilder består i å koble bort kraftforsyning. Hvordan dette skjer, avhenger av hvilket ESD-nivå som er initiert (se detaljer i NORSOK S-001 [53]). Valg av utstyr (ventiler og brytere) er vanligvis slik at de vil automatisk gå til sikker tilstand ved bortfall av kraft, enten elektrisk kraft eller luft/hydraulikk.

Kritisk Aksjons Panel (KAP) som inngår i ESD, er et operatør-brukergrensesnitt som stort sett er basert på lamper og trykknapper. Dersom operatørstasjonene går i «svart» eller ikke virker, så skal man kunne sikre innretningen ved å aktivere ESD, starte brannpumper og andre kritiske funksjoner direkte fra KAP. Fra KAP er det mulig å fjerne strømmen til ESD-systemet (som i praksis betyr at ESD-systemet aktiveres). Samtidig inneholder panelet et utvalg av andre funksjoner og visning av kritiske verdier. Det er krav om at innretningen skal kunne bringes til sikker tilstand uavhengig av de programmerbare systemene (jfr.§ 33 i innretningsforskriften).

Detaljerte eksempler på sikkerhetsfunksjoner som inngår i hver av de nevnte sikkerhetssystemene er beskrevet i Norsk Olje og Gass retningslinje 070 [55]. Samme dokument beskriver sentrale krav til design, dokumentasjon og oppfølging (i driftsfasen) for instrumenterte sikkerhetssystemer med utgangspunkt i standarder for funksjonell sikkerhet for prosessindustrien: IEC 61511 som er spesifikt rettet mot prosessindustrien og IEC 61508 som er standarden som produsenter av utstyr til instrumenterte sikkerhetssystemer benytter.

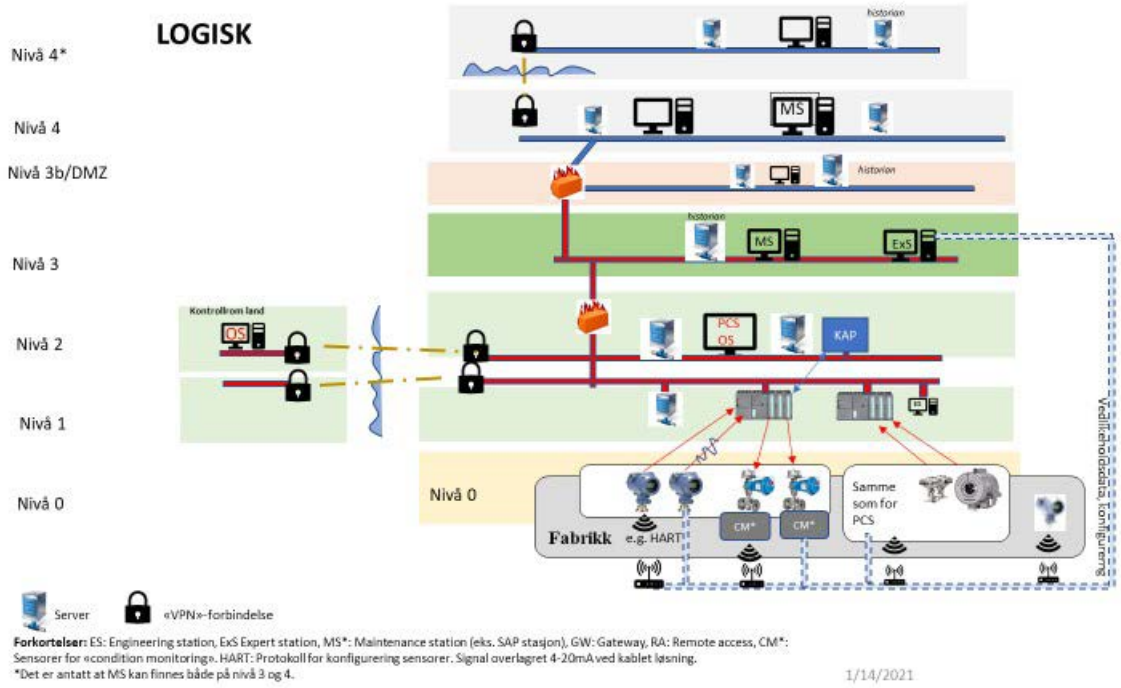
2.2 Dataflyt

2.2.1 Logisk dataflyt i henhold til Purdue-modellen

I **Figur 2** identifiseres 6 nivåer (nivå 0, 1, 2, 3, 3b og 4), disse er hentet fra Purdue-referansearkitektur [37] for OT/IT-systemer (også omtalt som ISA-95 referansemodell), med tilhørende detaljering i DNV-GL RP G108 [16] og ISA 84.00.009:2017 [37]. Det vi kan merke oss her er at det skilles mellom utstyr som plasseres i IT-

nettverk og utstyr plassert i OT-nettverk, og innenfor hver av disse nettverkene vil det være ulike delnettverk. Vi merker oss også at det skal være et tydelig skille mellom OT og IT med brannmur(er).

Med utgangspunkt i **Figur 2** nedenfor gis en overordnet forklaring av datakilder og logisk dataflyt mellom OT-systemer (operasjonell teknologi) og IT-systemer (i selskapets kontornettverk eller kontormiljø). Nivåene som er vist i figuren, blir forklart litt senere i dokumentet.



Figur 2: Illustrasjon av logisk dataflyt for produksjonsinnretninger i henhold til Purdue-modellen

I figuren er nivåene definert som følger:

- **Nivå 0:** Den fysiske prosessen og feltutstyret som inngår i styring og overvåkning. I noen kilder beskrives feltutstyr som nivå 1, men siden ISA TR 84.00.00.09:2017 og DNV-GL RP G108:2017 ganske entydig definerer feltutstyr som del av nivå 0, så velges dette.
- **Nivå 1:** Nettverk med kontrollere for prosesskontroll og sikkerhetssystemer og tilhørende servere for datautveksling. Engineering station (ES) kan være plassert her eller på nivå 2.
- **Nivå 2:** Nettverk med operatørstasjoner, ES, Information Management System (IMS) og servere for utveksling og presentasjon av data. En ES kan også være plassert i nivå 2 som et alternativ (eller tillegg) til ES plassert på nivå 1. En har her plassert KAP her sammen med operatørstasjonene, men deler av KAP (noen knapper og lamper) påvirker Nivå 1 direkte.
- **Nivå 3:** Teknisk nett med applikasjoner og servere for lagring av historiske/aggregerte data, inkludert tilhørende nettverk.*Det er ikke alltid et entydig og klart skille mellom hva som plasseres på nettverk i nivå 2 og i nivå 3. Et skille som kan benyttes er det som foreslås i ISA TR 84.00.09:2017 Her indikeres det at nivå 2 er «process control network» mens nivå 3 er et «process information network».*
- **Nivå 3b:** Demilitarisert sone (DeMilitarized Zone, DMZ) som styrer datatrafikk mellom nivå 4 og nivå 3. I prinsippet er det slik at de lavere nivåene kopierer informasjon til DMZ og nivåene lenger

opp henter fra DMZ. I prinsippet skal en aldri overføre noe uten at det mellomlagres i DMZ og hentes av en annen applikasjon fra andre siden.

- **Nivå 4**: Kontornettverk på innretningen og forlengelsen av dette til eksterne systemer via internett, slik som skyløsninger. Her plasseres utstyr som servere, PC-utstyr med tilhørende applikasjoner, slik som vedlikeholdssystem.
- **Nivå 4*:** Kontornett *på land* med mye av det samme utstyret (servere, PCer med ulike applikasjoner, som SAP vedlikeholdssystem) tilkoblet. I tillegg vil dette nettverket ha tilkobling mot eksterne systemer utenfor selskapet via brannmur. Dette kan inkludere applikasjoner i et nettverk hos leverandøren for å aksessere utstyr som står i OT-systemet. Det kan også gjelde skyløsninger som samler inn, analyserer og gir tilbake data og informasjon for beslutningsstøtte.

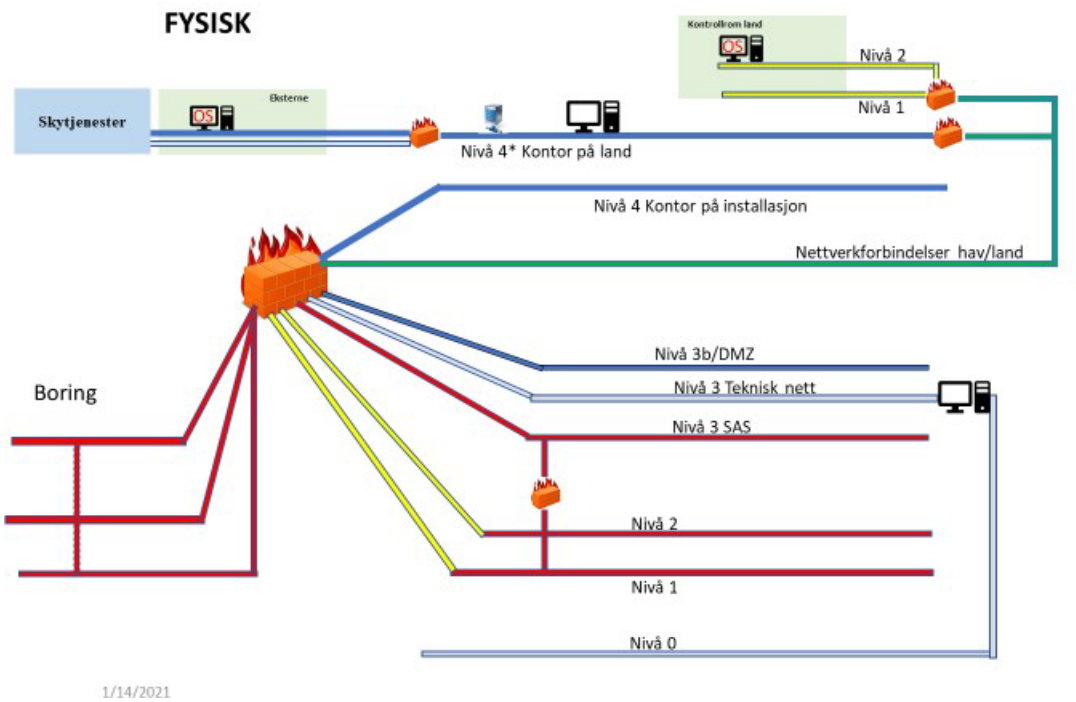
Datautvekslingen mellom ulike nivå i Purdue-modellen kan foregå på mange måter, men som oftest ved klienter og servere. Selv om en enhet er koblet til kontornettet kan den selvsagt stå fysisk i nærheten av enheter på andre nivå, men de er ikke koblet sammen. Eventuell kommunikasjon med OT-systemene uten å gå om DMZ er utfordrende og krever i tilfelle like bra beskyttelse som DMZ kan gi.

2.2.2 Fysisk realisering

Figur 3 illustrerer hvordan nettverkene kan være koblet opp rent fysisk. Merk at logisk dataflyt kan realiseres ved bruk av felles enhet med flere regelsett i stedet for flere brannmurer for å skille de forskjellige nettene. Det bemerkes at det kan være flere varianter av dette for konkrete innretninger. Noen kommentarer til Figur 3:

- Grønt farget nettverk er forbindelsen mellom land og innretning til havs med en brannmur i hver ende. Dette felles nettverket defineres hverken som kontornett eller del av OT.
- Brannmuren på innretningen til havs (den store brannmuren i figuren) styrer trafikk til alle nettverk på innretningen, både IT og OT, inkludert DMZ der dette eksisterer. Dette kan i praksis være fra én til mange fysiske enheter (men sees logisk som én funksjon).
- Kontrollrom på land definert som del av OT på nivå 2 og skilles fra kontornettet på nivå 4.

Avhengig av hvordan kontrollrom på land implementeres kan en også ha utstyr der som hører hjemme på nivå 1. Dette kan for eksempel være forlengelser av ESD, FG samt løsninger for å kompensere for at en ikke lenger kan oppfylle IF §33 «Fra bemannet kontrollsenter skal det være en manuell aktiveringsfunksjon som bringer innretningen til en sikker tilstand uavhengig av de programmerbare delene av systemet.»

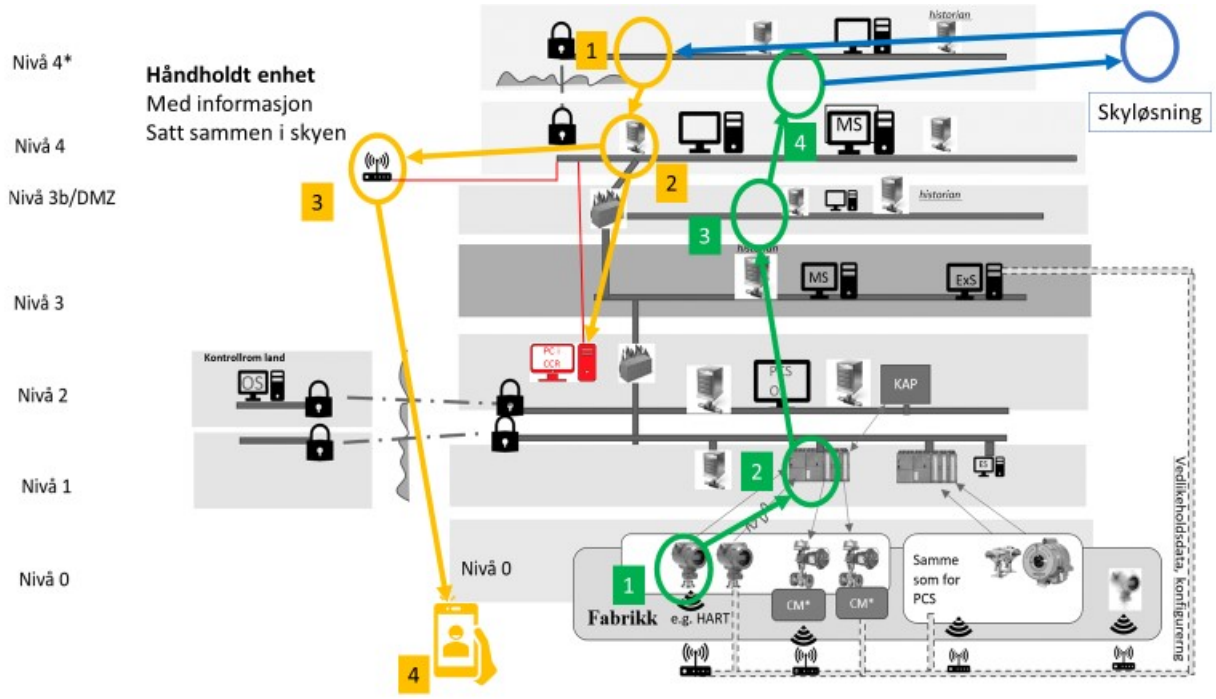


Figur 3: Illustrasjon av mulig fysisk struktur for å realisere logiske dataflyt

2.2.3 Logisk dataflyt ved bruk av håndholdte enheter

Håndholdte enheter er i dag ofte en del av IT-systemer på en innretning. I et fremtidsscenario vil informasjon presentert i håndholdte enheter kunne bli brukt som underlag for inngripen i prosessutstyr, 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 4 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).



Figur 4: Illustrasjon av logisk dataflyt ved bruk av håndholdte enheter

Noen kommentarer til figuren er gitt nedenfor.

Dataflyt OPP til skyen

1. Informasjonen fra prosessen konverteres i transmitteren og overføres til PLS. Her er det mange mulige måter å overføre på, noen eksempler er:
    a. 4-20mA strømsløyfe
    b. Profibus digital kommunikasjon
    c. Profisafe hvis det er en sikkerhetsfunksjon
    d. Trådløse gassdetektorer
2. PLS som mottar verdien fra transmitteren og gjør den tilgjengelig for operatøren og lagrer den på DMZ.
3. Fra DMZ hentes data til kontornettet på innretningen
4. Fra kontornettet gjøres informasjonen tilgjengelig for skyløsningen (for mere informasjon se ID6 rapporten [65])

Dataflyt NED fra skyen

1. Kontornettet mottar informasjonen fra skyløsningen
2. Informasjonen på kontornetter gjøres også tilgjengelig på et trådløsnett på installasjonen
3. Trådløse aksesspunkt gjør at den håndholdte enheten kan kobles til kontornettet
4. Feltoperatøren kobler den trådløse enheten til trådløsnettet og henter informasjonen

En ser i Figur 4 at den håndholdte enheten er koblet til kontornettet på innretningen (Nivå 4) og at informasjonen kan betraktes på en PC koblet til kontornett, men fysisk plassert i kontrollrommet.

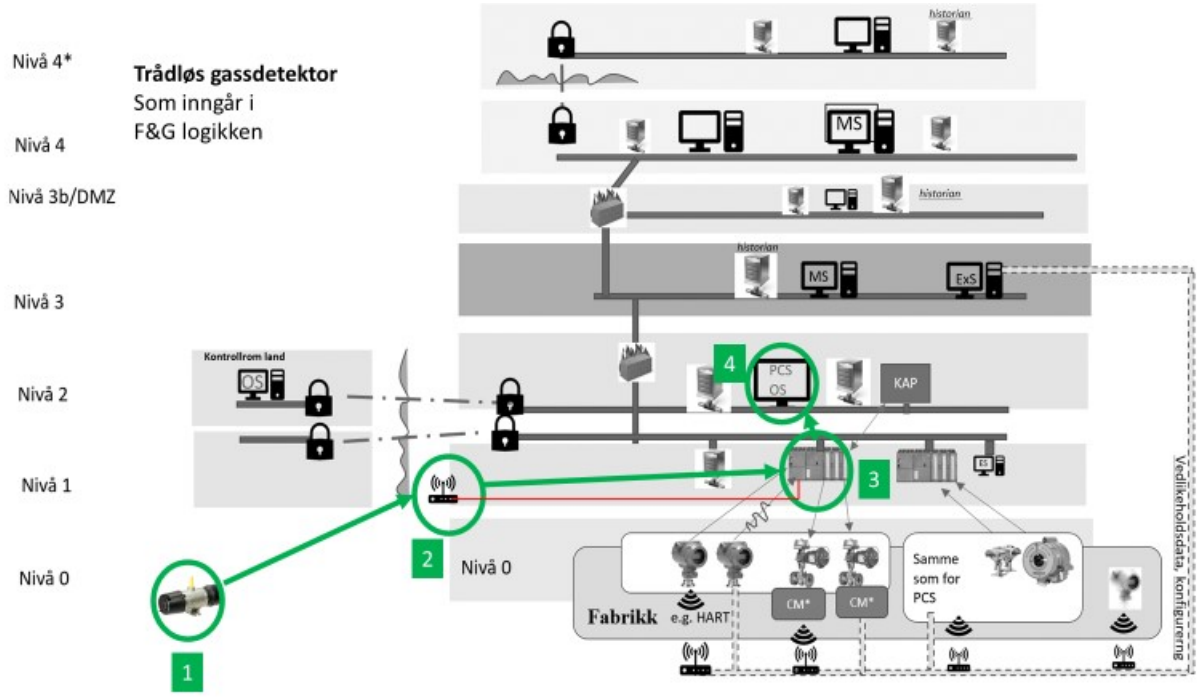
Hvis informasjonen på en eller annen måte føres gjennom DMZ enten for å sendes til den håndholdte enheten eller for å vises på de vanlige skjermene til operatørene, får en utfordringer med å sikre forbindelsen fra OT opp i skyen og tilbake til OT. Hvis en gjør det slik kan skyløsningen betraktes som en del av OT og må beskyttes deretter mot feil og negativ påvirkning.

Selv med den løsningen som vises i 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, se kapittel 5 i ID5-rapporten [64].

2.2.4 Logisk dataflyt ved bruk av trådløse sensorer

I Figur 5 har en vist en mulig tilkobling av en trådløs gassdetektor som inngår i C&E (Cause and Effect) i F&G. Det trådløse detektoren er koblet til F&G noden med et eget dedikert nett som ikke har noe felles med andre nett.

Trådløs instrumentering gir noen av de samme utfordringene som for håndholdte enheter. En ser at den her er koblet 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 kapittel 3.2.1).



Figur 5: Mulige kobling for trådløs gassdetektor

2.3 Rammeverk og protokoller

For å muliggjøre kommunikasjon og dataoverføring mellom to endepunkter, for eksempel to dataprogrammer eller et feltutstyr og en PLS, kreves det et konvensjonelt eller standardisert sett med regler som beskriver formater og fremgangsmåte for overføringen. Slike regler blir vanligvis referert til som protokoll. Protokoller er den kodingen (språket) som gjør at sender og mottaker kan forstå hverandre når informasjonen sendes over det fysiske nettet. Et eksempel på en protokoll som brukes på Internett er TCP (Transmission Control Protocol). I tillegg til protokoller er det også rammeverk. Det fins flere ulike alternative rammeverk for kommunikasjon innen OT-systemer, spesielt brukes OPC DA og OPC UA mye. ProfiSafe og Namur Open Architecture ble trukket fram i intervjurunden. Disse tre rammeverk er beskrevet mer detaljert nedenfor.

2.3.1 OPC UA

Oversikt over IEC OPC UA standarder:

IEC TR 62541-1:2020, Overview and concepts
IEC TR 62541-2:2020, Security Model
IEC 62541-3:2020, Address Space Model
IEC 62541-4:2020, Services
IEC 62541-5:2020, Information Model
IEC 62541-6:2020, Mappings
IEC 62541-7:2020, Profiles
IEC 62541-8:2020, Data Access
IEC 62541-9:2020, Alarms and Conditions
IEC 62541-10:2020, Programs
IEC 62541-11:2020, Historical Access
IEC 62541-13:2020, Aggregates
IEC 62541-14:2020, PubSub
IEC 62541-100:2015, Device interface
Kilde (lest 2020-12-08):
https://webstore.iec.ch/publication/68039

OPC UA (Open Platform Communication Unified Architecture) er en standard for industriell kommunikasjon og informasjonsmodellering som først ble publisert i 2008 [2] og som har blitt stadig mer tatt 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", også referert til som Purdue-modellen, se Figur 2. OPC UA har også blitt mer internasjonal i forbindelse med at IEC har utgitt en rekke OPC UA standarder, se faktaboks.

Det kan være verdt å merke seg at OPC UA er neste generasjon etter OPC Classic, som var den første versjonen av OPC. Mange installasjoner bruker fortsatt OPC Classic som ikke har de samme mulighetene som OPC UA. Hovedforskjellen mellom OPC Classic og OPC UA er at OPC Classic er implementert ved hjelp av Microsoft-produkter og programvare, som betyr at alle systemer som bruker OPC Classic også må være Microsoft-produkter. OPC UA derimot er mer serviceorientert og basert på en plattformuavhengig filosofi, som betyr at brukerne selv kan definere hvilket programmeringsspråk eller utviklingsmiljø de vil bruke.

OPC UA tilbyr en detaljert spesifikasjon av hvordan data skal presenteres og struktureres, samt tjenester for datautveksling i henhold til klient-server løsninger. OPC UA har også egenskaper ved protokollen (for eksempel kryptering) som beskytter mot uønsket påvirkning. Datautveksling mellom ulike nivå i Purdue-modellen foregår ved hjelp av klienter og servere. Serverne tilbyr data som skal utveksles og data transporteres ved forespørsel fra klienter.

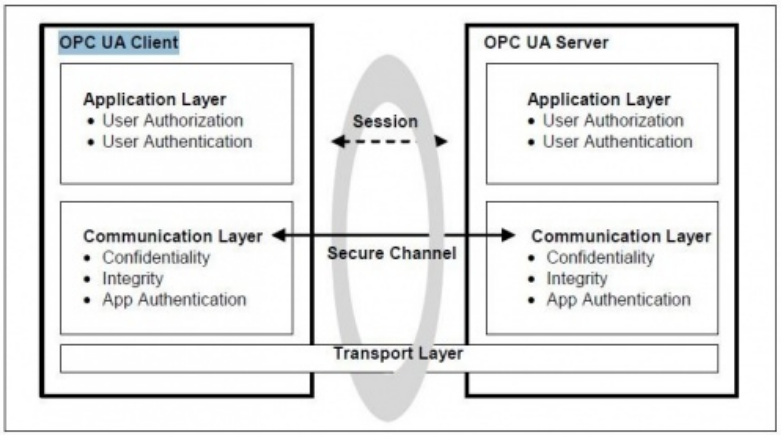
For å fasilitere utveksling av data definerer OPC UA flere muligheter knyttet til kommunikasjon og informasjonsmodellering.

Kommunikasjon
Kommunikasjonen i OPC UA er bygd opp av ulike lag; transportlag, kommunikasjonslag og applikasjonslag (se Figur 6). Transportlaget kommuniserer over TCP og støtter fire ulike format:

1. UA TCP er en enkel usikret protokoll for klient-server kommunikasjon. Den brukes typisk for kommunikasjon mellom feltutstyr hvor ytelse er essensielt, og kryptering mindre viktig. Det antas da at det er andre mekanismer som håndterer sikkerheten, for eksempel ved at de kjører i et isolert nettverk.
2. UA TCP Secured er lik UA TCP, men har i tillegg et enkelt krypteringslag på toppen. De fleste dedikerte OPC UA applikasjoner kommuniserer ved hjelp av dette formatet siden det er enkelt og har lav "overhead".
3. HTTPS brukes der hvor det er spesielle innstillinger i brannmurer som gjør det vanskelig å bruke UA TCP eller dersom en skal kommunisere med en OPC UA server som bruker et program som ikke er designet for OPC UA.
4. OPC UA over TSN (Time sensitive networking, IEEE 802.1 arbeidsgruppen) brukes typisk for lavnivå kommunikasjon og er en utvidelse av ethernet standarden. Den gir mulighet for å garantere at informasjon kommer frem over ethernet, som betyr at OPC UA kan brukes for utveksling av kritisk feltinformasjon da det også har god ytelse.

OPC UA støtter dessuten ulike dataformat.

Kommunikasjonslaget består av en sikker kanal som sikrer konfidensialitet og integritet for meldingene som sendes (end to end security). Her tilbys også autentisering av applikasjoner som skal kommunisere med hverandre. Både server og klient må ha et applikasjonssertifikat som utveksles når det opprettes en ny forbindelse. Applikasjonslaget brukes til å autentisere og autorisere brukere, slik at uautoriserte brukere ikke skal ha mulighet til å aksessere eller endre data i systemet.



Figur 6 OPC UA Klient- server kommunikasjon [2]

OPC UA har altså egenskaper ved protokollen som beskytter mot uønsket påvirkning. Konfidensialitet håndteres ved kryptering mellom server og klient. Integritet håndteres i to ulike deler av standarden. Den første er ved hjelp av kryptografiske sjekksummer, den andre er via signerte meldinger. OPC UA støtter dessuten andre former for autentisering, som for eksempel brukernavn, passord og to-faktor autentisering.

OPC UA spesifiserer et "Safety communication layer" (SCL) som muliggjør utveksling av sikkerhetsrelaterte (safety) data. En enhet som implementerer OPC UA Safety vil kunne oppfylle kravene for utveksling av data spesifisert i IEC 61508 [18] og IEC 61784-3 [19], se også kapittel 2.3.2. OPC UA Safety bruker et overvåkningsnummer, tidsavbrudd, et sett av ID-er og en syklisk redundanskode for å kunne detektere alle mulige kommunikasjonsfeil på OPC UA kommunikasjonskanalene. OPC UA Safety er en generell, applikasjonsavhengig løsning, hvor lengde og struktur på data som skal sendes defineres av applikasjonen selv [3].

Informasjonsmodellering
En informasjonsmodell er en konseptuell definisjon av informasjon som skal lagres eller utveksles. Informasjonsmodeller skiller seg fra datamodeller ved at informasjonsstrukturer kan beskrives uavhengig av enkeltapplikasjoner, implementasjonsteknologi eller hvordan dataene fysisk lagres eller aksesseres [4].

Når man har samlet mye data er de faktiske verdiene lite verdt i seg selv, med mindre de kan settes inn i en kontekst. For eksempel vil en sensor typisk ha mye mer informasjon enn bare en måleverdi og tagnummer tilknyttet seg, som grenseverdier, produsent, installasjonsdato, feildata, vedlikeholdsdata osv. En informasjonsmodell gir mulighet til å representere og bruke kompleks kontekstuell informasjon på en oversiktlig og entydig måte.

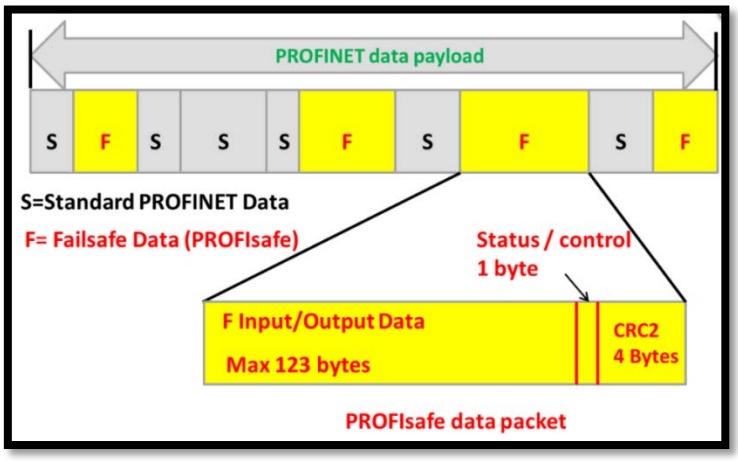
2.3.2 Profisafe

Profisafe og andre lignende protokoller (profiler) brukes der informasjon skal overføres på en eller annen form for nettverk i et sikkerhetssystem. Profisafe er f.eks. aktuelt når har en såkalt "black channel" løsning. PROFIsafe er en av fire sikkerhetsprotokoller som beskrives i IEC 61784-3:2016 standarden. De bygger på underliggende protokoller og overføres på samme nett/kabel som andre meldinger. I disse protokollene utvides nyttemeldingen med følgende:

- En CRC-kode som bare sender og mottaker klarer å danne (CRC har ingen IKT sikkerhet beskyttelse, og det er mulig å knekke koden)
- Sender og mottaker for meldingen
- Når neste melding skal komme til mottakeren
- Sekvensnummer på meldingen

Hensikten med dette er at det skal være svært vanskelig for uvedkommende å sende meldinger som påvirker sikkerhetsfunksjonene (safety), men det gir ingen beskyttelse mot at annen trafikk kan påvirke negativt. Det eneste profilen sørger for er at mottageren går til en forhåndsdefinert sikker tilstand hvis det oppdages noe feil på overføringen.

Figur 7 viser en PROFINET- datadel av en PROFINET-ramme med både standard data og F-data (Failsafe-data).



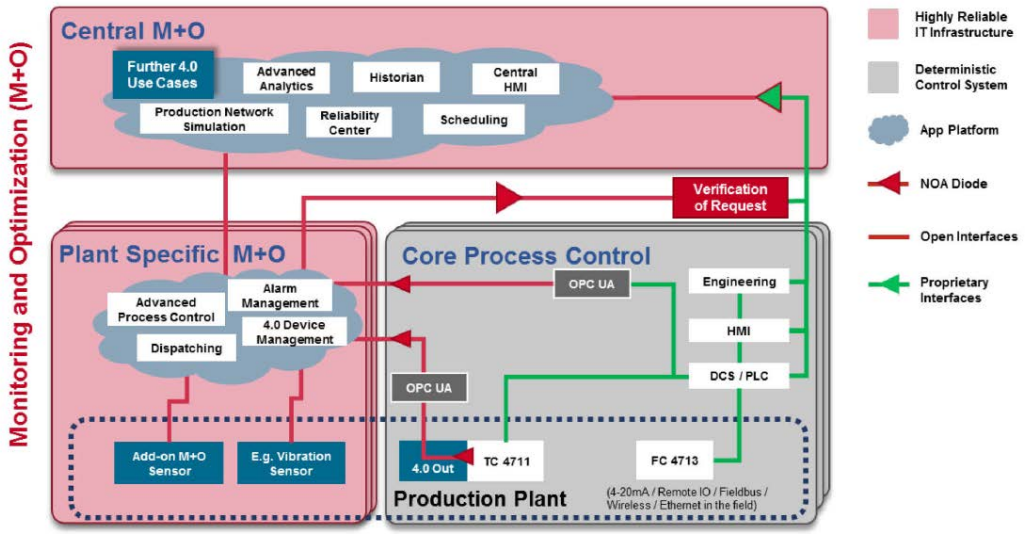
Figur 7: Profisafe med safety data og standard data

2.3.3 NAMUR Open Architecture, NE175

NAMUR er en internasjonal forening for automatiseringsteknologi og digitalisering i prosessindustrien. Kun ett firma fra Norge er medlem i denne organisasjonen (www.namur.net/en).

Denne anbefalingen fra NAMUR NE175:2020 definerer et åpent grensesnitt mellom OT- og IT-systemer og påstås å være spesielt nyttig i forbindelse med implementering av Industri 4.0 på eksisterende anlegg. Nøkkelord i denne sammenheng er Internet of Things (IoT), cloud computing, Big Data, 5G og allestedsnærværende mobile enheter. Hastigheten som nye innovasjoner blir implementert i OT henger etter moderne IT. Foreløpig oppleves dette som spesielt smertefullt, fordi IT-innovasjoner utvikler seg svært raskt.

Den grunnleggende ideen til NAMUR Open Architecture (NOA) er introduksjonen av et åpent grensesnitt mellom det eksisterende prosesskontrolldomenet og det mere nylig definerte overvåkings- og optimaliseringsdomenet (M + O) (se Figur 8).



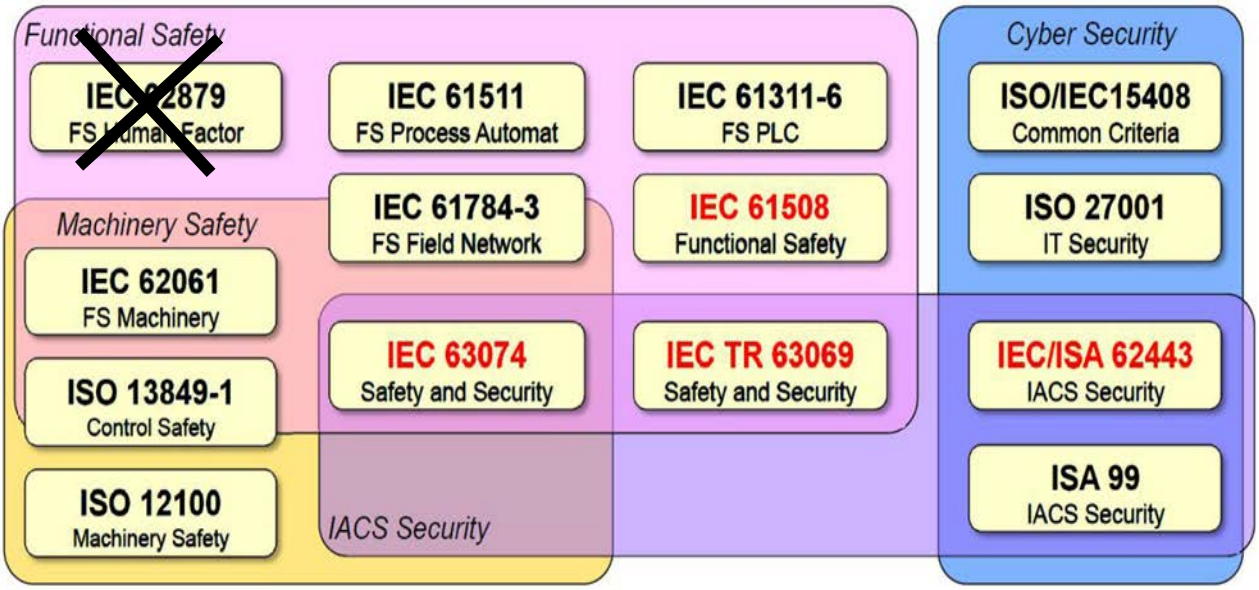
Figur 8**:** NOA arkitektur som viser bl.a. hvordan OPC UA- og NOA-diode (eksempel på datadiode) inkluderes, kilde NE 175:2020 [52]

3 Krav til datakvalitet og sikring av data i OT-systemer i standarder og retningslinjer

Funksjonell sikkerhet er aktiv sikring: Sikker tilstand oppnås som følge av aksjonene fra et sikkerhetssystem.

ISO og IEC har utgitt flere standarder innen funksjonell sikkerhet og IKT sikkerhet (se Figur 9). Selv om menneskelige faktorer er viktig, har IEC i år besluttet å ikke fullføre arbeidet med å utgi IEC 62879 som omhandlet dette. Det pågår imidlertid et arbeid med menneskelige faktorer som del av neste utgave av IEC 61508.

I figuren nedenfor er de relevante standardene listet. I forbindelse med dette prosjektet har vi fokusert på følgende standarder for funksjonell sikkerhet: IEC 61508 (generisk), IEC 61511 (prosessindustri), IEC 62061 (maskin) og ISO 13849-1 (maskin).



Figur 9: Functional safety standards and the relation to security standards. ISA99 utvikler også andre dokumenter enn ISA/IEC 62443 serien [67]

Ingen av disse standardene inkluderer relevante krav i forhold til ML/AI og data. Det er på gang initiativ for å utarbeide standarder som kobler funksjonell sikkerhet og ML/AI.

I tabellen nedenfor har vi rangert de mest aktuelle standardene for funksjonell sikkerhet i forhold til de aktuelle data temaene i denne rapporten.

Svak: Ikke tilstrekkelig for å forhindre datautfordringer
Middels: Tilstrekkelig for systemer som ikke har komplekse datasystemer
God: Tilstrekkelig for dagens systemer, men ikke tilstrekkelig for moderne systemer som inneholder ML/AI

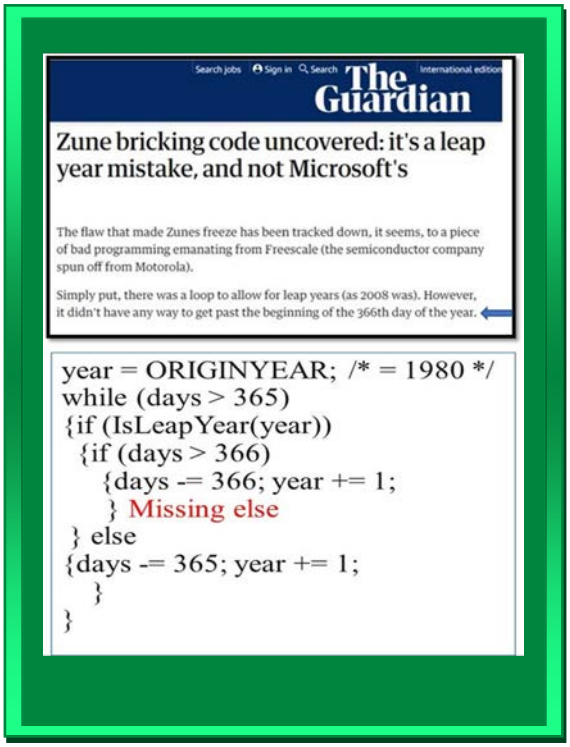
Tabell 1: Vurdering av standarder innen funksjonell sikkerhet

Tema	IEC 61508-3:2010	IEC 61511:2016	IEC 62061:2005 ISO 13849-1:2015
Datakilder	Svak Brukes kun på det enkelte produkt eller det enkelte system (SIS), ser ikke helheten utenfor dette systemet	Middels Dette er en generell standard for prosessindustrien. Hvis man i tillegg bruker NOROG 070 så kan dette løftes til "God"	Svak Brukes kun på den enkelte maskin eller det enkelte system (SRECS eller SRP/CS), ser ikke helheten utenfor dette systemet
Dataflyt	Middels Middels ift. det enkelte produkt eller det enkelte system (SIS), ser ikke helheten utenfor dette systemet	God De systemene som ikke har fulgt siste utgave av IEC 61508 kan karakteriseres som "middels"	Middels Brukes kun på den enkelte maskin eller det enkelte system (SRECS eller SRP/CS), ser ikke helheten utenfor dette systemet
Sikring/-beskyttelse av data, inkludert sårbarhet i forhold til IKT-trusler	Svak ift. IKT sikkerhet. Ny utgave av standard vil trolig kun referere til IEC 62443 serien, men dette er ett ømtålig tema i IEC 61508 komiteen	Middels IEC 61511:2016 har strengere krav til IKT sikkerhet enn IEC 61508, men hvis systemet kun tilfredsstiller 2003 versjonen av IEC 61511 så er det i kategorien "svak".	Svak Inkluderer ikke eksplisitte krav til IKT sikkerhet
Vasking av data	Svak Behandler ikke dette temaet konkret	Svak Behandler ikke dette temaet konkret, men er en nødvendig aktivitet for at SAS systemet skal fungere som tiltenkt.	Svak Behandler ikke dette temaet konkret
Prosessering/be-handling av data	Middels Standarden har noen krav til dette, se vedlegg A.2, men det er enighet i komiteen at forhold relatert til data må bedres så det er bestemt at man skal referere til SCSC veiledningen [59].	Middels Standarden har noen krav til dette, se vedlegg I.A.1.a)(1)B.1	Middels Standardene har noen krav relatert til dette
Kontekstu-alisering	Svak da dette er en generisk standard	Middels Dette er en generell standard for prosessindustrien. Hvis man i tillegg bruker NOROG 070 så kan dette løftes til "God" for allerede installerte systemer	Middels Dette er generelle standarder for maskiner.
Validering	Middels Standarden har noen krav til dette, se vedlegg A.2,	Middels Standarden har noen krav til dette, se vedlegg A.1,	Svak De sier lite i forhold til validering av data, selv om det fins en egen ISO 13849-2:2012 for validering
Kvalitetssikring	Middels Standarden har noen krav til dette, se vedlegg A.2,	Middels Standarden har noen krav til dette, se vedlegg A.1,	Middels Standardene har noen krav relatert til dette

3.1 Standarder for funksjonell sikkerhet

Nedenfor har vi beskrevet krav i de ulike standardene i forhold til data.

3.1.1 IEC 61508 og krav til data



IEC 61508 er den generiske standarden som definerer SIL (Safety Integrity Level). IEC 61508 bruker SIL 1-4 (Safety Integrity Level) for å beskrive hvilken risikoreduksjon en funksjon kan gi. Det er kvantitative krav til maskinvaren og krav til arbeidsmetodikken og metoder for utvikling av programvare.

Det finnes flere sektorstandarder som IEC 61511 (prosessindustri) og IEC 62061 (maskinsikkerhet), se nedenfor.

Diagnostics coverage/diagnosedekning (DC) er etablert for hovedsakelig å ta vare på tilfeldige feil, mens data defineres som del av programvare i IEC 61508:2010, altså del av systematiske feil.

IEC 61508 har definert data som del av programvare. Ellers er det få aktuelle definisjoner relatert til data i denne standarden.

I denne standarden forbindes data ofte med konfigurering og testdata, men også ved krav til grensesnitt mellom programvare og eksterne system. Ved slike grensesnitt skal de følgende ytelseskarakteristikkene bli vurdert:

A: Nødvendigheten av konsistens når det kommer til datadefinisjoner
B: Ugyldig, utenfor området eller verdier som oppgir feil tid
C: Responstid og gjennomføring, inkluder maksimal belastning
D: Beste tilfelle og verste tilfelle av utføringstid, og deadlock (vranglås)
E: Overflod (overflow) og for liten datalagringskapasitet

Programvaredesignet skal inkludere, i samsvar med kravene til SIL, selv-monitorering av kontrollstrømmen og datastrømmer.

Standarden inkluderer krav relatert til verifisering av data, se vedlegg, der vi har oppsummert eksplisitte krav til data.

Angående verifisering av tidsytelser så skal forutsigbarhet for atferd i tidsdomenet verifiseres. Tidsadferd kan inkludere: ytelse, ressurser, responstid, lengste utføringstid, dead-lock free (vranglås fri), kjøretid/run-time systemer.

Annex G i SCSC guiden presenterer "Veiledning for å skreddersy livssyklus assosiert med datadrevne systemer".

3.1.2 IEC 61511 og krav til data

IEC 61511 er en sektorstandard for prosessindustri som bygger på den generiske IEC 61508 standarden og bruker SIL på samme måte. IEC 61511 har definert data som del av programvare. Ellers er det få aktuelle definisjoner relatert til data i denne standarden, men flere krav, se I.A.1.a)(1)B.1 i denne rapporten.

Standarden har krav om at utstyr som kan konfigureres via nettet eller med for eksempel trådløs HART skal låses slik at det ikke er mulig å endre etter at det er satt i drift. Utstyret har derfor en fysisk bryter som må slås over for å kunne endre innholdet.

IEC 61511:2016 utgaven av standard serien inkluderer flere krav relatert til data, se vedlegg 1, der vi har oppsummert eksplisitte krav til data.

3.1.3 IEC 62061/ISO13849 og krav til data

Disse standardene gjelder for maskiner på land og på faste installasjoner, og skal sørge for at mennesker ikke blir skadet av de bevegelige delene på maskinene. Da disse standardene er harmoniserte, vil en ved å oppfylle disse standardene oppfylle kravene i maskinforskriften innenfor området.

IEC 62061 er en sektorstandard som bygger på IEC 61508 og bruker derfor SIL for å angi mulig risikoreduksjon. ISO 130849 har sitt opphav fra EN 954-1 som del av EU maskindirektivet og har definert ytelsesnivå PL a-e (Performance Level). IEC TR 62061:2010 beskriver sammenhengen mellom SIL og PL.

IEC 62061:2005 og ISO 13869-1:2015 har ikke eksplisitt definert data som del av programvare. Ellers er det få aktuelle definisjoner relatert til data i disse standardene.

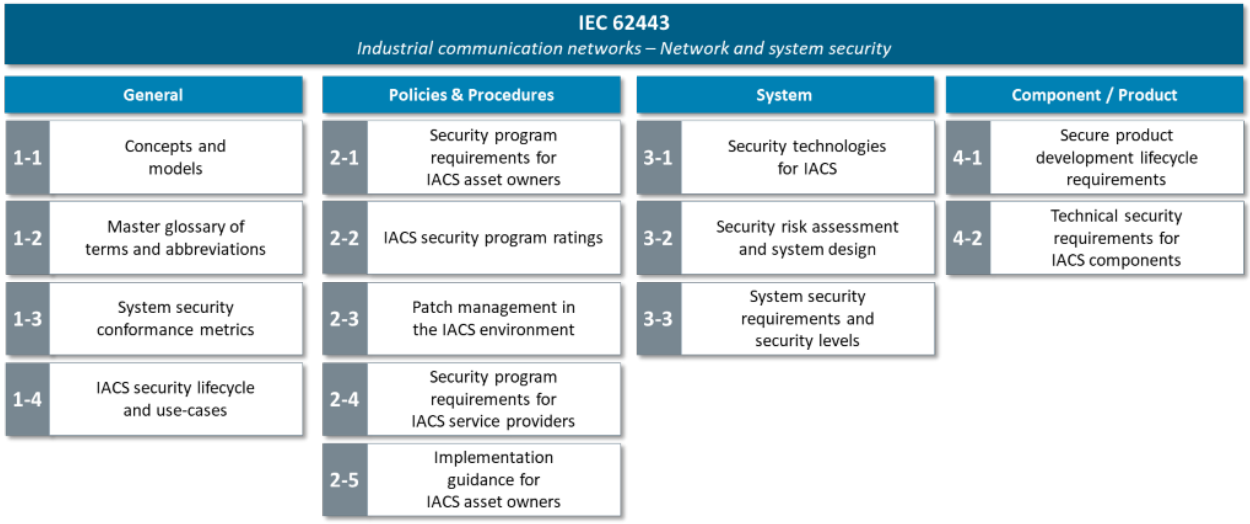
En bør også være klar over at det ikke er noe krav om skille mellom PCS og SIS i maskinstandardene, de opererer med begreper som de sikkerhetskritiske delene (Safety Critical Parts of Control System).

3.2 IKT-sikkerhetsstandarder og retningslinjer

Det finnes en rekke standarder, retningslinjer, anbefalinger og veiledninger for hvordan IKT-sikkerhet skal implementeres i OT-systemer. Den viktigste standarden er uten tvil IEC 62443 [5-12]. Noen eksempler på retningslinjer, rammeverk, anbefalinger og veiledninger er NIST Framework for Improving Critical Infrastructure Cybersecurity [13], NIST 800-82 [14], NOROG 104 [15] DNVGL-RP-G108 [16] og NSMs NSM grunnprinsippene for IKT-sikkerhet [47]. Flere av disse refererer til IEC 62443-standarder. Vi har derfor valgt å ta IEC 62443 som utgangspunkt i den videre beskrivelsen av IKT-sikkerhet i forhold til data.

3.2.1 IEC 62443

IEC 62443 er en internasjonal standard for IKT-sikkerhet i OT-systemer eller «Industrial Automation and Control System» som systemene kalles i standarden. Standarden ble utviklet av ISA99-komiteen og vedtatt av International Electrotechnical Commission (IEC). IEC 62443 består av en rekke deler. Disse er illustrert i Figur 10. IEC 62443 inneholder spesifiserte krav til både datakonfidensialitet og dataintegritet. Kravet om å sikre/beskytte data i forhold til IKT-trusler kan derfor anses å være godt. Merk at alle delene ennå ikke har blitt en standard, men er under utvikling. Andre deler blir nå oppdatert.



Figur 10: ISA/IEC 62443 standard serien

Et sentralt sikkerhetskonsept i IEC 62443 er forsvar i dybden («defense in depth») [5], som betyr at sikkerheten til et system ikke må avhenge av en individuell sikkerhetsmekanisme. I stedet bør flere komplementære mekanismer brukes. Noen eksempler på mekanismer som kan brukes sammen er brannmur, innbrudds-deteksjonssystem (IDS), virtuelt privat nettverk (VPN) og fysisk beskyttelse.

IEC 62443-1-1 [5] beskriver syv grunnleggende IKT-sikkerhetskrav i et OT-system. Kravene er:

1. Adgangskontroll (access control)
2. Brukerkontroll (user control)
3. Dataintegritet (data integrity)
4. Datakonfidensialitet (data confidentiality)
5. Begrenset dataflyt (restricted data flow)
6. Rettidig respons på hendelsen (timely response to event)
7. Ressurstilgjengelighet (resource availability)

IEC 62443-2-4 [8] spesifiserer at sensitive data må beskyttes med tanke på konfidensialitet og integritet. Dette gjelder både lagrede data og data som sendes i OT-systemet. Standarden angir imidlertid ikke på hvilken måte dette skal gjøres. En måte er å bruke skallbeskyttelse. En annen er å bruke kryptografi i form av nøkkelbasert meldingsautentiseringskode («Keyed-Hash Message Authentication Code (HMAC)») og kryptering av data. Standarden sier at det må være støtte for kryptografi..

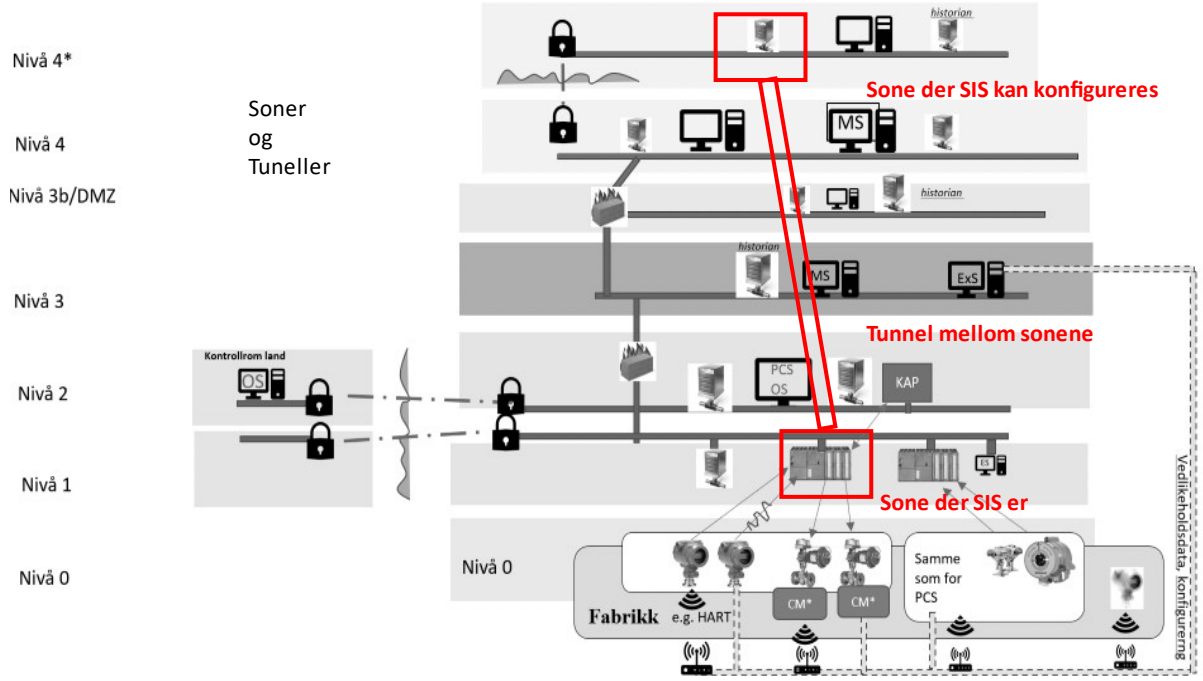
Ved hjelp av HMAC-er kan dataintegritet oppnås. De kan beskytte mot både uautorisert modifikasjoner og fabrikasjon av data. Slike HMAC-er knyttet til data når de lagres eller sendes. HMAC-en blir senere brukt til å bekrefte at dataene ikke har blitt endret eller opprettet ved en feiltakelse eller av en ondsinnet angriper. Det finnes forskjellige typer og versjoner av HMAC-er. Noen av disse anses som sikre eller sikre nok til å brukes i et produksjonssystem, mens andre anses som usikre. Anbefalingen i DNVGL-RP-G108 [16] fra september 2017 er å bruke algoritmen SHA-224 eller bedre. Med algoritmen SHA-224 eller bedre oppnås en tilstrekkelig god beskyttelse av dataintegritet akkurat nå, men også her gjelder det å følge med utviklingen.

Kryptering kan brukes for å oppfylle kravet om datakonfidensialitet. Også her er det anbefalinger i DNVGL-RP-G108 [16] om hvilke algoritmer som skal brukes, samt delvis hvor det kan brukes. Den nåværende

anbefalingen er å bruke AES 128 eller bedre for symmetrisk kryptering og RSA 2048 eller bedre for asymmetrisk kryptering. Selv disse anbefalingene kan anses å gi tilstrekkelig god beskyttelse av datakonfidensialitet akkurat nå, men hva som skjer vet bare den som følger med.

Standardserien opererer blant annet med sikkerhetsnivåer [10, 12]. Hvor bra beskyttelsen er angis i SL 1-4 (SL, Security Level). Dessuten er sentrale begreper soner (zones) og tunneller (conduits) og kan brukes til for eksempel å dele OT og SAS i to soner, de som har med sikkerhet (safety) og de som har styring og regulering. Koblingene mellom de forskjellige sonene defineres da som tunnel. Både soner og tunneler skal basert på risikovurderingen gis et SL.

I Figur 11 er det vist et tenkt eksempel der en oppretter en sone rundt SIS og en der en kan konfigurere disse systemene (ESD, F&G og PSD) på land. Sonene og forbindelsen er da beskyttet med tilstrekkelig SL.



Figur 11: Mulige soner og kanaler for å beskytte SIS ved fjernkonfigurering

I IEC 62443-3-3:2013 stilles det egne krav til det som er definert som «essential functions». Dette omfatter typisk de instrumenterte sikkerhetssystemene, enkelte kritiske støttesystemer og et utvalg av kritiske kontrollfunksjoner. To krav som blir gjeldende ved security level (SL) 3 (IEC 62443-4-2) er å ha funksjonalitet for å ivareta «island mode» og «fail-close». Det betyr at systemet skal kunne stenge sonegrensene for å hindre kommunikasjon og at dette skal kunne skje når det oppdages feil.

Det kan være relevant å undersøke hvordan dette faktisk lar seg realisere innenfor nåværende nettverksarkitektur, systemer og plassering av brannmurer og andre enheter som kan stoppe og åpne opp for trafikk mellom ulike soner. For eksempel vil en sone rundt SIS som vist i Figur 11 føre til at operatøren mister kontroll og må i et slik tilfelle mest sannsynlig føre til full nedstengning i «island mode».

3.3 Veileder datakvalitet

Innledning
The Data Safety Initiative Group har utviklet en veileder **[59]** som tar sikte på å:

- Beskrive datasikkerhetsproblemet (safety).
- Oppgi metoder for å identifisere og analysere risikonivåer
- Anbefale metoder og tilnærminger for å evaluere og behandle disse risikoene.

Dokumentet er skrevet for de fleste domener og er derfor på mange måter for generelt og må tilpasses til de enkelte domene og prosjekter. Målgruppen for dokumentet dekker alle de som har en interesse for, eller et ansvar for, sikkerhetsrelaterte (safety) data innen systemer, inkludert ledere, utviklere, sikkerhetsingeniører, assurandører (inkludert uavhengige sikkerhets-assessorer), myndigheter og operatører.

Definisjoner og terminologi
Retningslinjen lister syv basisdefinisjoner: Datagjenstand, dataeier, dataegenskap, bedømmelse av safety data, data safety krav (DSAL), og datainteressent. I tillegg har de oppgitt 42 definisjoner i et vedlegg.

Følgende uttrykk ble brukt av flere av de firmaene vi intervjuet: Data lineage, data ingestion og data cleaning. Definisjon for disse er oppgitt i vedlegg A.

Data sikkerhetsplan (safety)
Retningslinjen inkluderer beskrivelse av en datasikkerhetsplan (DSMP - Data Safety Management Plan) med forslag til innhold som kan utfylle selskapers sikkerhetsstyringsplan (SMP – Safety Management Plan). De foreslår at planen inkluderer følgende hovedkapittel: Introduksjon, konsekvensanalyse av bestemt DSAL og ODR (Organisational Data Risk), omfanget av kategorier av safety data, analyse av datakrav, styring av datarisiko, argumenter for bruk av data, nødvendige analyser og verifiseringer, og dokumenter som må utarbeides.

DSAL (Data Safety Assurance Level)
Retningslinjen definerer fem nivå (Data Safety Assurance Level - DSAL 0-4) for å angi hvor omfattende sikringen må være for få risikoen redusert til et akseptabelt nivå. Tabell 2 viser at en mulig feil med katastrofal konsekvens og høy sannsynlighet vil få DSAL4-nivå.

Tabell 2: DSAL for ulike risikonivå

Alvorlighet	Sannsynlighet		
	Høy	Medium	Lav
Liten	DSAL1	DSAL0	DSAL0
Moderat	DSAL2	DSAL1	DSAL0
Signifikant	DSAL3	DSAL2	DSAL1
Stor	DSAL4	DSAL3	DSAL2
Katastrofal	DSAL4	DSAL4	DSAL3

Datasikkerhetskultur (safety)
Organisasjonenes forhold til datarisiko er viktig. Derfor inkluderer retningslinjen et eget avsnitt om ODR og de har eget spørreskjema for å bedømme organisasjonens modenhet i å håndtere datasikkerhetsrisiko (safety). Spørsmålene er rettet mot å etablere graden av bevissthet om datasikkerhet og tilhørende ledelsesprosesser i organisasjonen. Det er imidlertid ikke alltid enkelt å måle nivået av bevissthet om prosesser og konsepter i en organisasjon. Spørreskjemaet må tilpasses organisasjonen som helhet, eller et bestemt prosjekt, tjeneste eller aktivitet. I spørreskjemaet er fokuset på et personlig syn i stedet for et prosjekt eller selskapssyn, så spørreskjemaet vil bli utfylt av alle, eller en betydelig undergruppe av ansatte. Svar kan samles for å gi en samlet verdi på datasikkerhetskultur. Et sentralt aspekt ved denne tilnærmingen er at det med jevne mellomrom kan gjentas for å vurdere trender. For eksempel, hvis totalpoengene synker, kan dette tyde på at videre opplæring og orienteringer vil være nødvendig.

Dataegenskaper
Dataegenskaper brukes til å fastslå hvilke aspekter av dataene (f.eks. aktualitet, nøyaktighet) som må ivaretas for at systemet fungerer på en sikker måte. I forhold til safety så har man erfaring med at det er kombinasjonen av datakategorier med aktuelle dataegenskaper som er viktig når man utfører sikkerhetsanalyser. Det fins mange ulike dataegenskaper og det er ikke lett å bestemme alle de aktuelle egenskapene data kan ha. I Figur 12 har vi derfor vist 22 ulike egenskaper som data kan ha, se også vedlegg I.A.1.a)(1)B.5. 20 av disse egenskapene er hentet fra SCSC-guide, mens vi har lagt til to egenskaper: Testbarhet og analyserbarhet, se vedlegg B.5.

Figur 12: Ulike dataegenskaper

Data HAZOP stikkord

Data HAZOP stikkord:

"Integrity, completeness, consistency, continuity, format, accuracy, resolution, traceability, timeliness, verifiability, availability, fidelity/representation, priority, sequencing, intended destination/usage, accessibility, suppression, history, lifetime, disposability/deletability.

SCSC Guide v3.2

HAZOP (Hazard and operability analysis) er en mye brukt metode for å identifisere farlige hendelser og det eksisterer en IEC standard for dette, IEC 61882:2016 "Hazard and operability studies (HAZOP studies) – Application guide". HAZOP er også nevnt i NORSOK S001:2018 "Teknisk sikkerhet".

HAZOP involverer vanligvis et tverrfaglig team som samarbeider om å identifisere potensielle farer og driftsproblemer. Struktur og fullstendighet støttes gjennom bruk av stikkord, for eksempel for å vurdere mulige konsekvenser hvis programvarekomponenter utfører funksjoner for tidlig, sent eller ikke i det hele tatt. Disse stikkordene er ment å stimulere kreativ tenking og diskusjon.

Når man utfører HAZOP. så er det viktig å først ha etablert gode stikkord. Dette har man gjort i SCSC-guiden [59] for data safety og de ulike ordene er vist i faktaboksen. Disse stikkordene som f.eks. integritet, kan medføre feil, delvis tap eller tap av integritet og så videre. Listen er ikke uttømmende. Andre stikkord kan være nyttige for bestemte systemer som kan brukes for å sikre datasikkerheten. I tillegg har retningslinjen inkludert et vedlegg som konkretiserer og forklarer HAZOP i praksis. Uansett så må man tilpasse stikkordene til de enkelte domer, prosjekt og system som man analyserer.

Man må lære av data HAZOP analyse, datakultur undersøkelser og bruke dette ovenfor både OT- og IT-miljøene.

3.4 Utfordringer knyttet til standarder og retningslinjer

Funksjonell sikkerhet

IEC 61511 bedret de datarelaterte kravene fra 2003-utgaven til 2016-utgaven. Flere av dagens systemer har blitt utviklet i henhold til 2003-utgaven og noen av systemene er også eldre enn dette. IEC 61511-1:2016 inneholder en del krav til data, slik at følger man den fullt ut med hensyn til data burde løsningen være god, men dette handler også om data fokus og data kultur som nevnt i SCSC-guiden. Datakulturen både hos leverandører og operatører har ikke blitt undersøkt som del av dette prosjektet.

IEC 61508:2010 inneholder en del krav til data, men det er bred enighet i IEC 61508 komiteen at dette må bedres. Det er derfor bestemt at man skal referere til SCSC-guiden [59] i neste versjon av IEC 61508.
Veilederen NOROG 070:2020 for anvendelse av IEC 61508 og IEC 61511 inkluderer ikke veiledning som er relevant i forhold til data utfordringer.

Siden data har vært lite behandlet i dagens safety standarder, vil SCSC-guiden kunne være til stor hjelp, men den må tilpasses aktuelt domene, prosjekt og system.

IKT-sikkerhet

I intervjuene kom det frem at OT-systemene ofte består av en blanding av gammelt og nytt utstyr. Den største IKT-sikkerhetsutfordringene i OT-systemer er derfor å kunne håndtere både gammelt og nytt utstyr på en sikker måte. Da det eldre utstyret ble utviklet, ble det ikke tatt hensyn til at OT-systemene en dag ville være koblet til IT-systemene. En god fysisk skallbeskyttelse var da fullt tilstrekkelig og eldre utstyr har derfor ikke støtte for kryptografi. Dette betyr at verken HMAC-er eller datakryptering brukes i eldre utstyr, noe som igjen betyr at dataintegritet og datakonfidensialitet er avhengig av skallbeskyttelse. Dette betyr videre at kravene til støtte for kryptografi i standarden IEC 62443 ikke er oppfylt.

SIL, SL, ML og i fremtiden også DSAL

Første utgave av IEC 61508 ble utgitt i 2000 og første utgave av IEC 61511 ble utgitt i 2003, slik at SIL har vært kjent i lang tid. I tillegg har dette blitt klargjort i NOROG 070:2020 som nå eksisterer i fjerde utgave. I de siste årene har man gradvis tatt i bruk IEC 62443-standardene etter hvert som de har blitt utgitt.

IEC 62443 inkluderer security level (SL) og maturity level (ML) for å ivareta krav til hhv. tekniske og organisatoriske forhold. Det å forholde seg til både safety og security standarder er utfordrende. IEC 62443 er fortsatt i sterk utvikling så det å tilfredsstille disse vil være en utfordring i lang tid fremover. Ptil krever ikke at man følger IEC 62443 serien i sine veiledninger siden mange av standardene i serien fortsatt ikke er offentlige. I praksis er den på vei til å bli et bransjekrav både innen petroleumssektoren og andre domener.

SCSC-guiden introduserer også DSAL. Det vil medføre at utfordringene blir enda større. Man bør derfor først undersøke hvor viktig dette er ved f.eks. å utføre noen aktuelle data HAZOP og datakulturundersøkelser, se kap 3.3. I tillegg må dette vurdere i forhold til bruk av data og om det blir aktuelt å benytte f.eks. håndholdt utstyr, slik som beskrevet i kapittel 2.2. DNVGL nevner også organisasjonskultur som viktig element i DNVGL-rp-0497 [57].

Modenhetsnivåer i IEC 62443-serien er basert på CMMI-SVC modellen [66]. Disse nivåene definerer forhold som kreves for å oppfylle kravene som er definert i standardene IEC 62443 2-4 og IEC 62443 4-1. Hvert nivå er gradvis mere avansert enn det forrige nivået. Leverandørene og operatørene er pålagt å identifisere modenhetsnivået knyttet til gjennomføringen av hvert krav.

4 Styrker og sårbarheter knyttet til datakvalitet og sikring av data i OT- systemer

Med sårbarhet mener vi manglende evne hos OT-systemet til å fungere når det utsettes for en uønsket hendelse. Sårbarheter i OT-systemer kan bidra til at personell tar feil beslutninger. Sårbarheter omfatter både data og programvare og det vil være en innbyrdes avhengighet mellom data og programvare. Sentrale spørsmål er:

- Kan data påvirke programvaren slik at sikker drift av OT-systemer settes i fare? Et eksempel kan være et system som blir matet med data utenfor det forventede området.
- Kan programvaren påvirke data slik at sikker drift av OT-systemer settes i fare? Et eksempel kan være forsinkelse av kritisk data på grunn av bufring.

I dette kapitlet vurderes styrker og sårbarheter knyttet til datakvalitet og sikring av data i OT-systemer er hovedsakelig basert på synspunkter som har kommet frem i intervju med ni bedrifter. Kapitlet bygger på den overordnede beskrivelsen av datakilder og dataflyt i OT-systemer i kapittel 2, samt krav til datakvalitet og sikring av data i OT-systemer i standarder og retningslinjer i kapittel 3.

Utfordringer som ble trukket frem under intervju, var hovedsakelig knyttet til tidsstempling, gamle system og generelt at det ikke har vært så mye fokus på data relatert til funksjonell sikkerhet.

4.1 Terminologi

Det er ikke etablert en helhetlig og omforent terminologi for datakvalitet i OT-systemer. Selv standarder som ISO 8000 for datakvalitet og SCSC-guiden [59] mangler definisjon for flere sentrale ord og uttrykk. Ptil har heller ingen konkrete definisjoner relatert til data i sine liste for "ord og uttrykk". Relevante IEC-standarder for funksjonell sikkerhet og IKT-sikkerhet inkluderer ikke relevante definisjoner for datakvalitet, men IEC 61508 vil referere til SCSC-guiden i neste utgave av standarden.

Gjennom våre intervju har vi opplevd at OT- og IT-personell i de ulike selskapene har benyttet forskjellige ord og uttrykk for datakvalitet. Fagmiljøene innen OT og IT baserer seg på ulike standarder og retningslinjer som ikke benytter samme definisjoner.

De mest brukte uttrykkene i forbindelse med intervjuene er:

1. Data vasking (cleaning)
2. Data avstamming (lineage)
3. Data innføring (ingestion)

Disse uttrykkene er ikke definert i noen av de aktuelle standardene eller retningslinjene. Data vask er definert noe spesielt i ISO 5127:2017 "Information and documentation — Foundation and vocabulary", se Vedlegg A.

Det er også en utfordring at data berører terminologi overfor minst 4 fagmiljø:

1. Funksjonell sikkerhet (safety)
2. Cybersecurity
3. Informasjonsteknologi
4. Operasjon

I vedlegg A har vi listet all de aktuelle definisjonene for denne rapporten, samt ulike definisjoner på samme ord og uttrykk.

4.2 Behandling av data

4.2.1 Prosessering

Våre intervju indikerer at operatørselskaper ikke har vektlagt egen oppfølging av prosessering og behandling av data i sine OT-systemer og de har primært stolt på at dette er ivaretatt av OT-leverandører. Det meste av prosessering og behandling av data fra/til feltutstyr er utført før det kommer til IMF-(Information management system) systemet. Noen OT-systemer har kvalitetsflagg som gir informasjon om bl.a. datakilden og alarmstatus (kvitert eller ikke kvitert alarm).

Hittil har konvertering av måleenheter til en felles enhet som for eksempel trykk (Pascal, bara og barg), vært del av dataprosessering i OT-systemer. En informant sa at temperatur har blitt angitt på hele 19 ulike måter! Med økt bruk av skyløsninger, maskinlæring og kunstig intelligens vil data fra/til feltutstyr i økt grad kunne bli prosessert i IT-systemer.

Etter SINTEFs vurdering er det er en styrke at OT-data hittil har vært prosessert mest mulig i OT-systemet, spesielt siden SIS-systemene er utviklet basert på egne standarder innen funksjonell sikkerhet som stiller ekstra høye krav til pålitelighet. PCS-systemene vil også være prosessert i stor grad da man må sørge for at HMI krav er fulgt og at dette skal være konsistent, forståelig og brukervennlig for operatørene.
Relevante IKT sikkerhets standarder som f.eks. IEC 62443-serien var umodne når dagens OT-system system ble utviklet.

4.2.2 Tidsstempling (timestamp)

Bruk av tidsstempling innebærer at det til hver operasjon i OT-systemet knyttes et tidsstempel slik at operasjoner i og mellom OT-systemer gjennomføres i riktig sekvens. Systemer som kjører WinX i bunn, bruker gjerne Network Time Protocol (NTP) for distribusjon av tidsinformasjon mellom noder fra en server som tjener som, eller er dedikert tidsserver. Tidsserver mottar tid fra enten GPS-klokke, eller annen pålitelige kilde. Utveksling av dato og tidsinformasjon er standardisert i ISO 8601-1:2019 [44].

Det var kun i noen intervju at informanter sa at tidsstempling er en utfordring ved for eksempel beslutningsstøtte. Noen utfordringer som ble trukket frem:

- Produksjonsprosessen krever høy tidsoppløsning,
- Dataene er ikke alltid synkronisert
- Noen bruker egen klokke
- Tidsstempling ifm gamle systemer
- Drift av tidsstempling, den kan være på flere sekunder
- Kø på overføringen av data
- Sekvensen av hendelser
- Synkronisering
- Strenge krav til responstid i NORSOK, se faktaboks
- Sommertid

10 Process safety system
10.4 Functional requirements
10.4.5 Response time
" The maximum response time of a process safety function to reach safe state on demand in actual operation shall be defined according to process dynamic behaviour. Typical response times that shall be complied with unless faster responses are required from dynamic analysis:
-— Time from signal from sensor to start of PSD execution, e.g. de-energised solenoid valve, should be less than 2 seconds.
— PSD valve travel time (in service) should not exceed 2 seconds/inch (valve size. 1 inch=2,54 cm) to reach safe state.
For valves 8 inch or less, a typical travel time should be set to 15 seconds.
— New valves should have a design margin to allow for degradation during service life, typically 1 second/inch."

NORSOK S001:2018

OPC-UA inkluderer tid og kvalitet, men det blir ikke bedre enn det selve applikasjonen er. Dette er en av grunnene til at man ønsker direkte tilgang til sensorene siden man dermed får tilgang til bl.a. bedre tidsdata, men man ser at dette kan medføre bl.a. utfordringer ift IKT-sikkerhet.

Også når man overvåker og vurderer IKT-sikkerhet, er nøyaktig tidsstempling på tvers av systemer svært viktig, da det er viktig å ha informasjon om korrekte tidssekvenser både før og etter en hendelse eller ett angrep.

4.2.3 Vasking

Med vasking av data menes prosessen med å forbedre datakvalitet. Dette kan gjøres ved å fjerne eller modifisere data som er feil, ufullstendige, irrelevante, dupliserte, eller data som har ugyldige verdier, uhåndterlige variabelnavn, tall som tekst, upraktisk struktur eller feil format. Selv om vasking ikke er nevnt konkret i sikkerhetsstandardene IEC 61508 og IEC 61511, vil man i praksis inkludere vanlige krav til datakvalitet ved utforming av OT-systemer.

De fleste operatørselskapene som ble intervjuet, forventer at tilstrekkelig vasking er utført av leverandørene av SAS-systemene. Det vil si at informasjon fra Historian/IMS eller lignende systemer har allerede blitt vasket. I tillegg kan operatørselskap utføre noen egne sjekker ift. F.eks. spesielle verdier og kontekstualisering av informasjonen.

4.3 Kontekstualisering

For at informasjon skal ha verdi må den fortolkes, gis en mening og settes i en gitt kontekst (sammenhengen man bruker data i). Dette inkluderer flere forhold som:

- Systemkontekst (sammenheng) og hvordan systemet (f.eks. OT-system) skal brukes
- Aktuelle interessenter. F.eks. operatører, leverandører etc.
- Identifisere aktuelle data gjenstander (artefacts). F.eks. Sensor data: overvåkings-data, temperatur data etc.
- Grensesnitt, f.eks. fra transmitter til PLS, eller fra OT- til IT-systemet

I petroleumsvirksomheten brukes tag hierarki og P&ID (piping og instrumenterings diagram). For å beskrive utstyr og forstå oppgaver i OT-systemer. Hvis man har en digital tvilling, så knyttes denne informasjonen ofte også mot 3D-modell og teknisk dokumentasjon.

De forskjellige bedriftene utvikler ulike systemer som gjerne er basert på programvaren Python. Power BI brukes for analyse og visualisering av kontekst og informasjonsflyt. Verktøy for forståelse av data og visualisering er viktig for dataanalytikere og teknisk orienterte forretningsbrukere. Fokuset for disse verktøyene er ikke først og fremst rapportering og overvåking, men heller ad hoc-analyse av flere datakilder. Disse verktøyene gir dataanalytikere en intuitiv måte å sile gjennom store datamengder for å avsløre mønstre og avvik som er skjult i dataene. De erstatter i økende grad de tradisjonelle radene og kolonnene med tradisjonelle datapresentasjoner med grafiske bilder og diagrammer. I forhold til IKT sikkerhet er det viktig å ha god kontekst informasjon både før og etter f.eks. en IKT-sikkerhet hendelse. Dette for tidlig å få ett godt bilde av hvordan hendelsen har vært. Dette er informasjon som analytikerne bruker når de vurderer hva som har skjedd og hva som må foretas for å rette på IKT-sikkerheten.

4.4 Validering av data

Ifølge intervjuene valideres data for SAS-systemer i stor grad basert på standardene IEC 61508 og IEC 61511. Det er en styrke, spesielt for de systemene som er utviklet i henhold til siste utgave av IEC 61511 som ble utgitt i 2016. Aktuell validering ifm IEC 61508-3 og IEC 61511-1 er nevnt i vedlegg A. IEC standardene har mere fokus på validering av design enn av validering som foretas under drift. Validering har også en sterk tilknytning til kontekst. Se også figur i Vedlegg B.4 for å klargjøre hva som menes med validering ("getting the right system and the right data"). Det er verdt å merke seg at SRS i forbindelse med IEC standardene hovedsakelig er utviklet med tanke på utvikling av SIS og SAS systemer og ikke i forhold til aktuelt bruk av IT-personell som for eksempel data analytikere. Dermed kan det være aktuelt å vurdere om SRS bør tilpasses tiltenkt bruk for IT-personell.

SCSC-guiden [59] er noe svak ift validering og inkluderer ikke validering som ett eget tema. Aktører som ikke er involvert i utvikling av produkter og system (SIS og SAS) i henhold til disse standardene utfører ikke validering av data i særlig grad.

Eksempler på validering som oppgis i intervju er:

- Sjekk av nye data mot gamle data og trender
- Vedlikeholdsdata valideres manuelt av prosesspersonell og teknisk personell

Her kan man ha sårbarheter siden IKT-sikkerhetsstandarder var umodne når dagens OT-systemer ble utviklet.

4.5 Kvalitetssikring

Med kvalitetssikring av data mener vi nivå av tillit til at dataene som leveres, oppfyller krav fra brukeren. Disse kravene kan inkludere nivåer av nøyaktighet, oppløsning, sporbarhet, rettidighet, fullstendighet og format.

De fleste firmaene mener: *"at dette hovedsakelig er tilfredsstilt ved at OT-utstyret tilfredsstiller standarder som IEC 61508 og IEC 61511"*. Begge disse standardene inkluderer "data" i definisjonen for programvare.

Et applikasjonsprogrammeringsgrensesnitt (API) er et sett med subrutine definisjoner, kommunikasjons protokoller og er et verktøy for å utvikle programvare. Generelt er API et sett med klart definerte kommunikasjonsmetoder mellom ulike komponenter. Et godt API gjør det lettere å utvikle et dataprogram ved å tilby de aktuelle byggesteinene, som deretter settes sammen av programmereren. Når man lager API spesifikasjoner så inkluderer man også kvalitetssikring. En API-spesifikasjon kan ha mange former, men inkluderer ofte spesifikasjoner for blant annet rutiner, datastrukturer, objektklasser og variabler.
Det foregår også en del manuell mapping/dekoding. Noen informanter mener det er for mange mappinger som foretas. Dette bør forenkles og normaliseres. I tillegg ønsket man forenklede modeller og at man setter dette i

riktig kontekst overfor brukerne. I tillegg bemerker man at mapping tar for lang tid. De intervjuede selskapene ser for seg at AI kan være aktuelt for å lage en bedre løsning for dette. Mapping template mates inn i f.eks. API spesifikasjon som da bygger opp modellen. Modellen som da etableres blir kvalitetssikret. Det er en egen IEC OPC UA standard for mapping [26].

En styrke med OPC UA er at den inkluderer egen standard for IKT sikkerhet IEC TR 62541-2:2020, mens OPC UA ikke inneholder egen IEC standard for safety.

4.6 Sikring og sårbarhet av data relatert til IKT-trusler

Innen OT-systemene er tilgang til riktige data sentralt for å opprettholde produksjon og stenge ned produksjon på en sikker måte ved en uønsket hendelse. Krav til høy tilgjengelighet og integritet er dermed viktigere enn kravet om konfidensialitet [5]. Sikring av data i OT-systemene kan være fysisk (gjennom f.eks. adgangskontroll) og/eller logisk (gjennom f.eks. brannmurer som skiller OT-systemer fra IT-systemene og skyen). Når data sendes ut i IT-systemene og muligens lenger ut i skyen, blir det økte utfordringer med sikring av data.
|
En viktig sårbarhet i dagens OT-systemer er at de ofte inneholder eldre utstyr som ikke har innebygd støtte før kryptografi. Dette betyr at høy dataintegritet avhenger av god skallbeskyttelse. HMAC-er, som har muligheten til å verifisere at data er autentiske og ikke har blitt endret, brukes vanligvis ikke i OT-systemer.

DNVGL-RP-G108 [16] inneholder følgende anbefaling:

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

IEC 62443 inkluderer 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, ...) vil ikke kunne oppdage innbruddsforsøk. Nettverksovervåking blir da også vanskeligere.

En annen utfordring er at kryptering/dekryptering krever ressurser og vil gå på bekostning av responstid og mulighetene for utveksling av informasjon mellom de enkelte systemer samt at operatørgrensesnittet også kan bli langsommere. Det kan hende at skallsikring i form av soner og tuneller ihht. IEC 62443 er en bedre løsning for OT-systemer.

Det finnes SIL 4 sertifiserte hardwirede 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.

4.7 Eksempler på hendelser knyttet til datakvalitet

Under intervjuene har man ikke referert til konkrete hendelser relatert til data.

Nedenfor har vi beskrevet to ulykker hvor datakvalitet har vært et problem, og hvordan lignende datautfordringer kan være en utfordring for Petroleumsnæringen.

Tabell 3: To ulykker relatert til datautfordringer, basert på beskrivelser i SCSC-guiden [59]

Tittel	Sammendrag og aktuelle dataegnskaper	Aktuell problemstilling for Petroleumsnæringen
Boeing 737 Max 8 ulykke i 2018 og 2019	Ved to anledninger var det en enkelt feil i "Angle-of-Attack-sensor" som gjentatte ganger satte nesen til flyet ned og førte til at flyet gikk i sjøen/ bakken • Integritet • Kompletthet • Nøyaktighet • Tilgjengelighet • Verifiserbarhet • Nøyaktig/representasjon	• Er det tilstrekkelig redundans på aktuelle systemer? • Data integritet generelt. DSAL (Data Safety Assurance Levels) er ikke del av nåværende utgave av hverken IEC 61508 eller IEC 61511. SCSC-guide [59] blir referert i neste utgave av IEC 61508 • Kompletthet. Ifm intervjuene kom det frem at man ikke alltid fikk data til riktig tid, manglet data eller de inkluderte ikke tidsstempling • Tilgjengelighet generelt og til riktig tid. Dette inkluderer også tilgang til aktuelle prosedyrer • Ikke alt er like lett å verifisere og ofte kun ved bestemte tidsrom • Sikkerhetskultur • Programvare overstyrer systemet basert på informasjon fra sensor(er)
A400M kraftmoment kalibrerings parameter innen luftfart i 2015	A software update apparently wiped the engine torque control parameters. Aircraft crash; four fatalities. • Fullstendighet	• Utfordringer ifm oppdatering av dreiemoment til motorer • Data og parametre ifm oppdatering av programvare generelt. o Denne utfordringen vil også øke både pga hyppigere forbedringer pga automatisering/Industri4.0 og fordi flere og flere produkter og utstyr inkluderer programvare som kan oppdateres • Se også: Software is both code and data [61]

5 Anbefalinger

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

5.1 Næringen

Anbefalinger til tiltak for næringen er gitt i Tabell 4.

Tabell 4: Oppsummering av anbefalinger til tiltak for næringen

Nr.	Utfordring	Anbefaling
1	Håndtering av gammelt utstyr og bakover-kompatibilitet for systemer.	Forbedre aktuelle veiledninger (f.eks. NOROG 070) basert på internasjonale standarder.
2	Dataplan (jfr SCSC-Guide [59]) eksisterer ikke eller er ikke kjent i organisasjonene. Det er heller ikke nevnt i aktuelle standarder som IEC 61508 og IEC 61511.	Etablere mal for dataplan for sikkerhetsdelen (safety) med tilhørende veiledning. Utføre data HAZOP-analyser og vektlegge bevisstgjøring og kultur for oppfølging av datakvalitet (ref SCSC-guide og DNVGL-RP-0497). Gjelder både for OT- og IT-systemer. Forbedre aktuelle veiledninger (f.eks. NOROG 070) basert på internasjonale standarder og tilpasse bruk av SCSC-guide til næringen.
3	Terminologi for datakvalitet generelt og mange nye uttrykk som mangler gode norske oversettelser. SCSC-guide [59] er for generisk til at den vil bli anvendt og forstått på samme måte av de ulike fagekspertene i IT og OT.	Klargjøre terminologi for datakvalitet for bedre kommunikasjonen mellom IT- og OT-personell. Forbedre aktuelle veiledninger (f.eks. NOROG 070) basert på internasjonale standarder og tilpasse bruk av SCSC-guide til næringen.
4	Kvalitetssikring av dataflyt fra IT-systemer tilbake til håndholdt feltutstyr.	Forbedre aktuelle veiledninger (f.eks. NOROG 070) basert på internasjonale standarder.
5	Beskyttelse mot cyberangrep i dataflyt fra IT-systemer til OT-systemer.	Forbedre aktuelle veiledninger (f.eks. NOROG 070) basert på internasjonale standarder.
6	Krav om kryptering og HMAC-er innen OT-systemer.	Vurdere hvordan kryptering og/eller HMAC-er kan brukes i deler av OT og i forhold til IT. Alternativt om skallsikring med soner og tuneller enklere gir tilsvarende sikring.
7	Manglende forståelse av økt IKT-sårbarhet ved å tillate lesing av data fra OT-systemer.	Legge vekt på økt forståelse av IKT-sårbarheter som introduseres ved lesetilgang lavere ned i systemet.
8	Svært rask teknologiutvikling innen tilrettelegging og bruk av data, samtidig som angripernes verktøy også utvikles raskt.	Legge vekt på kontinuerlig trusselvurdering og iverksetting av tiltak mot nye sårbarheter ved nye digitale løsninger.
9	Manglende kompetanse og forståelse innen kvalitetssikring av data hos mindre leverandører.	Forbedre aktuelle veiledninger (f.eks. NOROG 070) basert på internasjonale standarder.
10	IT-personell arbeider i større grad med forhold som kan påvirke OT, og IT-personell får større ansvar	Forbedre kompetanse om OT-systemer hos IT-personell.

5.2 Ptil

Anbefalinger til tiltak for Petroleumstilsynet er gitt i Tabell 5.

Tabell 5: Oppsummering av anbefalinger til tiltak for Petroleumstilsynet

Nr.	Utfordring	Anbefaling
1	Næringen ønsker tydeligere veiledning for fastsettelse av interne krav til dataflyt fra skyen ned til OT-systemer. Generelt er det krevende å bevise uavhengighet og at dataflyt ikke påvirker OT-systemer negativt.	Forsterke tilsyn med operatørers kvalitetssikring av IT-leverandører og krav til dataflyt fra skyen ned til OT-systemer (påseplikt).
2	Behov for bedre bevisstgjøring både hos OT- og IT-personell om IKT-sikkerhet.	Forsterke Ptils rolle i deling av kunnskap og erfaring om IKT-sikkerhet og oppfølging av kompetansekrav til aktuelt IT- og OT-personell
3	Små leverandører mangler kompetanse og ressurser for oppfølging av IKT-sikkerhet i den raske datautviklingen.	Forsterke Ptils rolle i deling av kunnskap og erfaring om IKT-sikkerhet blant små leverandører, inklusive tilsyn av operatørers kvalitetssikring av leverandører (påseplikt).
4	Næringen legger ikke tilstrekkelig vekt på å inkludere IKT-sikkerhetstiltak i design. Dette har nok også med at hele IEC 62443 serien ikke har vært ferdig. I tillegg er det viktig at det settes krav til dette ved kontraktsinngåelse.	Spesielt følge opp IKT-sikkerhet under design, inklusive tilsyn av operatørers kvalitetssikring av leverandører (påseplikt).
5	Norske selskaper som har et internasjonalt marked, må forholde seg til flere nasjonale standarder. Dette er en generell utfordring og ikke spesielt ift data	I størst mulig grad vise til internasjonale standarder fremfor nasjonale standarder i veiledninger.
6	Terminologi for datakvalitet generelt er en utfordring. Det eksisterer mange nye data uttrykk for bransjen som mangler gode norske oversettelser	Inkludere relevante terminologi for datakvalitet i Ptils ordliste: Ord og uttrykk" www.ptil.no/fagstoff/ord-og-uttrykk/

5.3 Behov for kunnskapsinnhenting.

Maskinlæring (ML) og kunstig intelligens (AI) er ikke inkludert som del av datautfordringene i denne rapporten. SCSC-guiden [59] inkluderer relevant informasjon om maskinlæring og DNVGL RP-0510 [56] inkluderer relevant informasjon i forhold til datadrevne algoritmer. Det er behov for mer kunnskap om hva andre domener gjør innen bruk av ML og AI og hvordan Ptil og Næringen skal forholde seg til pågående standardiseringsarbeid i IEC og ISO.

Gjennom våre intervju har vi opplevd at OT- og IT-personell i de ulike selskapene har benyttet forskjellige ord og uttrykk for datakvalitet. Fagmiljøene innen OT og IT baserer seg på ulike standarder og retningslinjer som ikke benytter samme definisjoner. Selv standarder som ISO 8000 [43] for datakvalitet og SCSC-guiden mangler definisjon for flere sentrale ord og uttrykk. Ptil har heller ingen konkrete definisjoner relatert til data i sine liste for "ord og uttrykk" [58]. Når IT- og OT-systemer blir mer integrerte, er det et stort behov for å etablere en helhetlig og omforent terminologi for datakvalitet som kan bidra til bedre forståelse og samarbeid på tvers av fagmiljøene innen IT og OT.

I et fremtidsscenario vil informasjon presentert i f.eks. håndholdte enheter kunne bli brukt som underlag for inngripen i prosessutstyr, for eksempel til å sjekke trykket og forholdene i en del av prosessen før et mannhull

åpnes for intern inspeksjon og jobbing. Det er behov for økt kunnskap om datakvalitet og styrker og sårbarheter knyttet til bruk av håndholdte enheter i felt. 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. Trådløst feltutstyr gir samme utfordringer som for håndholdte enheter.

Hvordan skal en konfigurere SIS fra land, finnes det utstyr for dette og hvordan skal en skal sørge for tilstrekkelig beskyttelse av soner og tuneller i slike konfigurasjoner (ref. IEC 62443 serien).

Relevante standarder innen IKT-sikkerhet og funksjonell sikkerhet krever at det gjennomføres en risikovurdering for å bestemme integritetsnivå (SIL og DSAL). Det er behov for økt kunnskap om hva som vil være formålstjenlige risikovurderinger for beskyttelse av OT-systemer i petroleumsvirksomheten. En kunne undersøke om det kan være mulig å lage en lignende retningslinje som NOG 070 [55] (eller bedre NOG 070 ift datakvalitet) for implementering av IEC 61508 [18] og 61511 [21] og derigjennom komme fram til et omforente beskyttelsesnivå for de enkelte enheter i OT-systemer i petroleumsvirksomheten.

Løsningen til NAMUR [52] for å beskytte OT-løsninger bør vurderes av oljenæringen. Spesielt er det viktig om denne tilnærmingen kan være fornuftig for eksisterende installasjoner i stedet for å skifte utstyr for å kunne oppfylle kravene som er gitt i for eksempel IEC 62443-serien.

Referanser

[1] Petroleumstilsynet, IKT-sikkerhet – robusthet i petroleumssektoren, www.ptil.no/fagstoff/utforsk-fagstoff/prosjektrapporter/2020/ikt-sikkerhet--robusthet-i-petroleumssektoren/, 27. juni 2020

[2] OPC UA Foundation, https://opcfoundation.org/about/opc-technologies/opc-ua/, 04.11.2020

[3] OPC 10000, OPC UA Online Reference, Online versions of OPC UA specifications and information models, https://reference.opcfoundation.org/v104/, 04.11.2020

[4] Y. Tina Lee (1999), Information modeling from design to implementation, National Institute of Standards and Technology.

[5] ISA/IEC-62443-1-1: 2009 – Security for industrial automation and control systems: Terminology, concepts and models.

[6] ISA/IEC-62443-2-1 Edition 2:2018 – Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program.

[7] ISA/IEC-62443-2-3:2015– Security for industrial automation and control systems –Part 2-3: Patch management in the IACS environment.

[8] ISA/IEC-62443-2-4:2017 – Security for industrial automation and control systems –Part 2-4: Security program requirements for IACS service providers.

[9] ISA/IEC-62443-3-2:2018 – Security for industrial automation and control systems – Part 3-2: Security risk assessment and system design.

[10] ISA/IEC-62443-3-3:2013 – Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels.

[11] ISA/IEC-62443-4-1:2018 – Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements.

[12] ISA/IEC-62443-4-2:2019 – Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components.

[13] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 16. april 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[14] NIST 800-82, Guide to Industrial Control Systems (ICS) Security, Revision 2, mai 2015.

[15] Norsk olje og gass, 104 Anbefalte retningslinjer krav til informasjonssikkerhetsnivå i IKT-baserte prosesskontroll-, sikkerhets- og støttesystemer, Revisjon 6, 5. desember, 2016. www.norskoljeoggass.no/arbeidsliv/retningslinjer/integrerte-operasjoner/104-anbefalte-retningslinjer-krav-til-informasjonssikkerhetsniva-i-ikt-baserte-prosesskontroll--sikkerhets--og-stottesystemer-ny-revisjon-pr-05.12.2016/.

[16] DNVGL-RP-G108:2017, Cyber security in the oil and gas industry based on IEC 62443, september 2017. http://rules.dnvgl.com/docs/pdf/dnvgl/rp/2017-09/dnvgl-rp-g108.pdf.

[17] IEC TR 62541-2:2016, Overview and concepts

[18] IEC 61508:2010-serien

[19] IEC 61784-3: 2016 Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions

[20] IEC 61511:2003-serien

[21] IEC 61511:2016-serien

[22] IEC TR 62541-2:2020, Security Model

[23] IEC 62541-3:2020, Address Space Model

[24] IEC 62541-4:2020, Services

[25] IEC 62541-5:2020, Information Model

[26] IEC 62541-6:2020, Mappings

[27] IEC 62541-7:2020, Profiles

[28] IEC 62541-8:2020, Data Access

[29] IEC 62541-9:2020, Alarms and Conditions

[30] IEC 62541-10:2020, Programs

[31] IEC 62541-11:2020, Historical Access

[32] IEC 62541-13:2020, Aggregates
[33] IEC 62541-14:2020, PubSUb
[34] IEC 62541-100:2015, Device interface
[35] IEC 61784-3:2016 Industrial communication networks – Profiles – Part3: Functional safety fieldbuses – General rules and profile definitions
[36] IEC 60050, se også www.electropedia.org/
[37] ISA-TR84.00.09-2017 Cybersecurity Related to the Functional Safety Lifecycle
[38] ISA TR84.00.09 draft 2020-11. revision 3 working file currently defines OT.
[39] IEC 62061:2005
[40] ISO 13849-1:2015
[41] ISO 13849-2:2015
[42] ISO 5127:2017 Information and documentation — Foundation and vocabulary, see also www.iso.org/obp/ui
[43] ISO 8000-2:2020 Data quality — Part 2: Vocabulary
[44] ISO 8601-1:2019, Date and time – Representations for information interchange – Part 1: Basic rules
[45] EN 50159:2010 Railway applications – Communication, signalling and processing systems – Safety-related communication in transmission systems
[46] EN TS 50701: draft 2020
[47] Nasjonal sikkerhetsmyndighet, NSMs grunnprinsipper for IKT-sikkerhet, versjon 2.0, april 2020.
[48] Zimmermann et al.,. (2019). Skill-based Engineering and Control on Field-Device-Level with OPC UA. 10.1109/ETFA.2019.8869473
[49] Rapport fra ekspertgruppen for Datadeling i næringslivet, april 2020. www.regjeringen.no/contentassets/c98cce6745b0486c948c269dc80335c8/rapport-fra-datadelingsutvalget2.pdf
[50] IF: Innretningsforskriften
[51] NOU 2015: 13
[52] NE 175:2020 NAMUR Open Architecture – NOA Concept
[53] NORSOK S-001 Technical safety
[54] NORSOK I-002 Safety and automation system (SAS)
[55] NOROG 070:2020 Norwegian oil and gas application of IEC 61508 and IEC 61511 in the Norwegian petroleum industry (Recommended SIL requirements)
[56] DNVGL-RP-0510:2020 Framework for assurance of data-driven algorithms and models
[57] DNVGL-RP-0497:2017 Data quality assessment framework
[58] Ptil 2020-11-10: www.ptil.no/fagstoff/ord-og-uttrykk/
[59] SCSC-127E Data safety Guidance version 3.2, DSIWG 2020, https://scsc.uk/scsc-127E
[60] J. Inge. Improving the analysis of data in safety-related systems, 2008
[61] A. Nanda, S. Mani, S. Sinha, M. J. Harrold and A. Orso, Regression testing in the presence of non-code changes. Fourth IEEE International Conference on Software Testing, Verification and Validation 2011
[62] SINTEF 2021:00054 Regulering av IKT-sikkerhet i petroleumssektoren
[63] SINTEF 2021:00055 Grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer
[64] SINTEF 2021:00056 Bruk av modeller i boring
[65] SINTEF 2021:00057 Premisser for digitalisering og integrasjon IT-OT
[66] CMMI-SVC, https://cmmiinstitute.com/
[67] Kanamaru, Hiroo (2017), "Bridging Functional Safety and Cyber Security of SIS/SCS", In Proceedings of the SICE Annual Conference 2017, Kanazawa, Japan

A Vedlegg A Data definisjoner og terminologi

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

IT og OT blir mere og mere integrert, det medfører at de må kunne kommunisere bedre sammen, det er derfor tatt med flere definisjoner fra IT, OT og de aktuelle domenene data, safety og IKT sikkerhet (security).

Begrep	Definisjon/beskrivelse	Referanse
Absolutt tidsstempel Engelsk: Absolute time stamp	3.1.1.1 absolute time stamp time stamp referenced to a global time which is common for a group of devices using a fieldbus [IEC 62280-2, modified]	IEC 61784-3:2016
Relativt Tidsstempel Engelsk: Relative time stamp	3.1.1.27 relative time stamp time stamp referenced to the local clock of an entity NOTE In general, there is no relationship to clocks of other entities. [IEC 62280-2, modified]	IEC 61784-3:2016
Tidsstempel Engelsk: Time stamp	3.1.1.43 time information included in a message	IEC 61784-3:2016
Barriere *	Tiltak som har til hensikt og funksjon enten å forhindre et konkret hendelsesforløp i å inntreffe, eller påvirke et hendelsesforløp i en tilsiktet retning ved å begrense skader og/eller tap. Funksjonen til disse barrierene ivaretas av tekniske, operasjonelle og organisatoriske elementer enkeltvis eller samlet	Ptil 2020-11-10 [58]
Black channel	black channel defined communication system containing one or more elements without evidence of design or validation according to IEC 61508 Note 1 to entry: This definition expands the usual meaning of channel to include the system that contains the channel.	IEC 61784-3:2016
Tunnel Engelsk: Conduit	3.2.27 conduit logical grouping of communication assets that protects the security of the channels it contains NOTE This is analogous to the way that a physical conduit protects cables from physical damage.	IEC TS 62443-1-1:2009
Cyclic Redundancy Check CRC	<Value> redundant data derived from , and stored or transmitted together with , a block of data in order to detect data corruption <method> procedure used to calculate the redundant data Note 1 to entry: Terms "CRC code" and "CRC signature'', and labels such as CRC1 , CRC2, may also be used in this standard to refer to the redundant data.	IEC 61784-3:2016
Datablanding Engelsk: Data blending	SINTEF definisjon som er tilpasset dette prosjektet: Man blander data fra ulike kilder og samler dem i ett brukbart og standardisert oppsett	Denne rapporten
Data diode	Boundary device which ensures that data between two separate networks is only transmitted in one direction. Note 1 to entry: data diode can be either of the physical or logical type (firewall)	EN TS 50701: Draft 2020

Begrep	Definisjon/beskrivelse	Referanse
Data avstamning Engelsk: Data lineage	SINTEF definisjon som er tilpasset dette prosjektet:	Denne rapporten
Data fare Engelsk: Data hazard	Use of data in the context of a system that could lead to an accident.	SCSC Data guide [59]
Fare Engelsk: Hazard	Potential source of harm NOTE The term includes danger to persons arising within a short time scale (for example, fire and explosion) and also those that have a long-term effect on a person's health (for example, release of a toxic substance).	IEC 61508-4:2010
Fare Engelsk: Hazard	Potential source of harm Note 1 to entry: The term includes danger to persons arising within a short time scale (e.g., fire and explosion) and also those that have a long-term effect on a person's health (e.g., release of a toxic substance or radioactivity).	IEC 61511-1:2016
Data egenskap	En karakteristikk som kan bli fremvist ved en data gjenstand	SCSC Data guide [59]
Data eier	Personen eller organisasjonen som har ansvaret for en spesiell data gjenstand eller samlingen av data gjenstander	SCSC Data guide [59]
Datagjenstand Engelsk: Data artefact	Ett objekt (item) eller samling av objekt som gir et nyttig perspektiv på data generert, behandlet eller konsumert av et system	SCSC Data guide [59]
Datainnføring Engelsk: Data ingestion	SINTEF definisjon som er tilpasset dette prosjektet:	Denne rapporten
Datavasking Engelsk: Data cleaning	SINTEF definisjon som er tilpasset dette prosjektet: Data vask er prosessen med å forberede data for analyse ved å fjerne eller modifisere data som er feil, ufullstendig, irrelevant, duplisert eller feil formatert.	Denne rapporten
Datavasking Data cleaning	Process used to improve data quality by detecting and correcting (or removing) defects and errors in data	ISO 5127:2017
Data Safety Requirement	A requirement to implement an approach specifically designed to achieve, maintain or demonstrate a Data Property (or Properties) for a given Data Artefact (or Artefacts).	SCSC Data guide [59]
Data Safety Assurance Level (DSAL)	An indication of the level of rigour with which relevant Data Properties should be demonstrated for appropriate Data Artefacts.	SCSC Data guide [59]
Datakvalitet	degree to which a set of inherent characteristics of data fulfils requirements	ISO 8000-2:2020
Datakvalitet	A degree or level of confidence that the data provided meet the requirements of the user. These requirements include levels of accuracy, resolution, assurance level, traceability, timeliness, completeness, and format.	SCSC Data guide [59] and RTCA/DO-200A

Begrep	Definisjon/beskrivelse	Referanse
Datakvalitet	Process by which the Electronic Chart Systems (ECS) Database is produced, the source materials, the resolution and reproduction accuracy of chart features, and the correctness and completeness of data.	SCSC Data guide [59] and ISO 19379:2003
Datakvalitet	A degree or level of confidence that the data provided meets the requirements of the data user in terms of accuracy, resolution and integrity.	SCSC Data guide [59] and EU 73/2010
Dataintegritet Engelsk: Data integrity	Property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner NOTE This term deals with constancy of and confidence in data values, not with the information that the values represent or the trustworthiness of the source of the values.	IEC 62443-1-1:2009
Data integrity assurance	5.4.7 Data integrity assurance The safety-related application process shall not trust the data integrity assurance methods if they are not designed from the point of view of functional safety. Therefore, redundant data is included in a message to permit data corruptions to be detected by redundancy checks. NOTE Communication systems used for safety-related applications can use methods such as cryptography to ensure data integrity, as an alternative to typical methods such as CRCs. If a hash function is used, it shall not include error correction mechanisms.	IEC 61784-3:2016
Data konfidensialitet Engelsk: Data confidentiality	Property that information is not made available or disclosed to any unauthorized system entity, including unauthorized individuals, entities, or processes	IEC 62443-1-1:2009
Assessering av safety data Engelsk: Data safety assessment	The process of explicitly considering data as part of a system safety assessment, via the means of Data Artefacts, Data Properties and Data Safety Assurance Levels.	SCSC Data guide [59]
Data validering	The activity whereby a data element is checked as having a value that is fully applicable to the identity given to the data element, or a set of data elements that is checked as being acceptable for their purpose.	SCSC Data guide [59] and RTCA/DO-200A
Data verifisering	Evaluation of the output of an aeronautical data process to ensure correctness and consistency with respect to the inputs and applicable data standards, rules and conventions used in that process.	SCSC Data guide [59] and EU 73/2010
Diagnostics coverage (DC)	fraction of dangerous failures rates detected by diagnostics. Diagnostics coverage does not include any faults detected by proof tests Note 1 to entry: Diagnostics coverage is typically applied to SIS devices or SIS subsystems. E.g., the diagnostics coverage is typically determined for a sensor, final element or a logic solver.	IEC 61511-1:2016
Eksplisitt data	Data som er overført	IEC 61784-3:2016

Begrep	Definisjon/beskrivelse	Referanse
Funksjonell sikkerhet	3.1.12 Functional safety part of the overall safety relating to the EUC and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures	IEC 61508-4:2010
Funksjonell sikkerhet	3.2.23 Functional safety 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 61511-1:2016
Funksjonell sikkerhet	IEC 62061:2005 3.2.9 functional safety part of the safety of the machine and the machine control system which depends on the correct functioning of the SRECS, other technology safety-related systems and external risk reduction facilities [IEC 61508-4, 3.1.9 modified] NOTE 1 This standard only considers the functional safety that depends on the correct functioning of the SRECS in machinery applications.	IEC 62061:2005
Hash	(mathematical) function that maps values from a (possibly very) large set of values into a (usually) smaller range of values Note 1 to entry: Hash functions can be used to detect data corruption. Note 2 to entry: Common hash functions include parity, checksum or CRC. [IEC TR 62210:2003, 4.1.12, modified - addition of "usually" and notes]	IEC 61784-3:2016
Implisitte data	Tilleggsdata som ikke overføres, men som er kjent for sender og mottager	IEC 61784-3:2016
IT-protokoll	Et sett med regler som beskriver formater og fremgangsmåte som kreves for å få datautstyr til å kommunisere.	Store Norske Leksikon
Kanal Engelsk: Channel	3.3.6 channel element or group of elements that independently implement an element safety function EXAMPLE A two-channel (or dual-channel) configuration is one with two channels that independently perform the same function. NOTE The term can be used to describe a complete system, or a portion of a system (for example, sensors or final elements).	IEC 61508-4:2010

Begrep	Definisjon/beskrivelse	Referanse
Kanal Engelsk: Channel	3.2.5 channel device or group of devices that independently perform(s) a specified function Note 1 to entry: The devices within a channel could include input/output (I/O) devices, logic solvers, sensors, and final elements. Note 2 to entry: A dual channel (i.e., a two-channel) configuration is one with two channels that independently perform the same function. Channels may be identical or diverse. Note 3 to entry: The term can be used to describe a complete system or a portion of a system (e.g., sensors or final elements). Note 4 to entry: Channel describes SIS hardware architectural features often used to meet hardware fault tolerance requirements.	IEC 61511:2016
Kanal Engelsk: Channel	3.2.20 channel specific communication link established within a communication conduit (see 3.2.27 conduit)	IEC TS 62443-1-1:2009
Klient	Klient/tjener-teknologi, prinsipp for å oppnå effektive nettverkssystemer ved å fordele arbeidet mellom applikasjoner (programvare) på brukernes lokale datamaskiner og en sentral vertsmaskin. Den lokale programvaren kalles klient, mens programmet på sentralmaskinen, som vanligvis betjener et større antall klienter, kalles tjener (engelsk server)	SNL (Store Norske Leksikon)
Klient	Client software application that sends Messages to OPC UA Servers conforming to the Services specified in the IEC 62541 series of standards	IEC TR 62541-1:2016
Kvalitet Engelsk: Quality	degree to which a set of inherent characteristics of an object fulfils requirements Note 1 to entry: The term “quality” can be used with adjectives such as poor, good or excellent. Note 2 to entry: “Inherent”, as opposed to “assigned”, means existing in the object.	ISO 9000:2015
Mapping	Specification on how to implement an OPC UA feature with a specific technology. Note1 to entry: For example, the OPC UA binary encoding is a mapping that specifies how to serialize OPC UA data structures as sequences of bytes	IEC 62541-6:2020
Masqueraded message	3.1.30 masqueraded message type of inserted message in which a non-authentic message is designed to appear to be authentic	EN 50159:2010
Metadata	data defining and describing other data	ISO 8000-2:2020

Begrep	Definisjon/beskrivelse	Referanse
Metadata	Data that represents information about data itself. Note that one should distinguish between “Structural Meta-data”, which is data about the design and specification of data structures (and is more properly called “data about the containers of data”) and “Descriptive Meta-data”, which is about individual instances of application data,the data content.	SCSC Data guide [59] and J. Inge [60]
NOA	NAMUR Open Architecture	NE 175:2020
NOA diode	The name “NOA Diode” is descriptive for one-directional data flow but does not define a technical solution.	NE 175:2020
Node	En node er i IKT-sammenheng betegnelsen på en enhet i et nettverk. Det kan være for eksempel en ruter, en server eller en svitsj.	NOU2015: 13 [51]
Node	Node fundamental component of an AddressSpace	IEC TR 62541-1:2016
Operasjonell Teknologi	Teknologi som støtter, kontrollerer og overvåker industriell produksjon, kontroll- og sikkerhetsfunksjoner	Denne rapporten
Operasjonell Teknologi	Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise and the applicable procedures performed by personnel (e.g. engineering, operations, maintenance) to operate and maintain with the purpose of safe and secure operation. Note: In the context of process plants, the enterprise is considered the IACS network inclusive of IACS networking devices (e.g. firewalls, switches, routers, etc.), all controls and smart instrumentation down to level 0 in the reference architecture and those responsible for its management, operation, engineering support and maintenance.	ISA TR84.00.09 [37]
Profil	Specific set of capabilities to which a Server may claim conformance Note 1 to entry: Each Server may claim conformance to more than one Profile. Note 2 to entry: The set of capabilities are defined in IEC 62541-7.	IEC TR 62541-1:2016
Profinet	Profinet er en industristandardstandard for datakommunikasjon over Industrial Ethernet, designet for å samle inn data fra og kontrollere utstyr i industrielle systemer, med en spesiell styrke i å levere data når man har strenge tidskrav	Denne rapporten
Påseplikt, operatørens	Operatøren skal påse at alle som utfører arbeid for seg, enten personlig, ved ansatte, ved entreprenører eller underentreprenører, etterlever krav som er gitt i helse-, miljø- og sikkerhetslovgivningen. Påseplikten gjelder også for rettighetshavere. Arbeidstakerne har plikt til å medvirke etter arbeidsmiljøloven § 2-3	Ptil ord og uttrykk [58]

Begrep	Definisjon/beskrivelse	Referanse
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 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.	Ptil ord og uttrykk [58]
Risiko	Risk: <safety> combination of the probability of occurrence of harm and the severity of that harm Note 1 to entry: For more discussion on this concept see Annex A of IEC 61508-5 :2010. [IEC 61508-4:2010, 3.1.6, modified - The domain has been added between angle brackets.]	IEC TR 63069:2019
Risiko	Risk: <security> expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence [IEC TS 62443-1-1 :2009, 3.2.87, modified - The domain has been added between angle brackets.]	IEC TR 63069:2019
Ruter	Funksjonell enhet som etablerer en sti gjennom ett eller flere datanettverk og videresender pakker	IEC 60050, www.electropedia.org
Safety data	3.1.41 safety data data transmitted across a safety network using a safety protocol Note 1 to entry: The Safety Communication Layer does not ensure safety of the data itself, only that the data is transmitted safely.	IEC 61784-3:2016
Server (tjener)	Funksjonell enhet som tilbyr tjenester til arbeidsstasjoner, til personlige datamaskiner eller til andre funksjonelle enheter i et datanettverk	IEC 60050, www.electropedia.org
Server	Software application that implements and exposes the Services specified in the IEC 62541 series of standards	IEC TR 62541-1:2016
Sikkerhet Engelsk: Safety	Sikkerhet mot ulykker.	Denne rapporten
Sikkerhet Engelsk: Security	Sikkerhet mot (forsettlig) inntrenging. I denne rapporten bruker vi IKT-sikkerhet som et synonym for "security".	Denne rapporten
Sikring	Sørge for at konfidensialitet, integritet, og/eller tilgjengelighet av informasjon ivaretas	Denne rapporten
Svitsj	En svitsj er et apparat som mottar signaler fra en rekke inngående linjer og sender dem videre etter bestemte regler. (Svitsjer i telefonnettet kalles vanligvis telefonsentraler)	NOU2015: 13 [51]
Interessent Engelsk: Stakeholder	An individual or organisation that has some relationship to the system, possibly including a power of veto.	SCSC Data guide [59]
Tilgjengelighet Engelsk: Availability	Tilgjengelighet er forebygging av uautorisert tilbakeholdelse av informasjon eller ressurser.	Denne rapporten

Begrep	Definisjon/beskrivelse	Referanse
Timeliness	3.1.58 timeliness state in which information is available at the right time according to requirements	EN 50159:2010
Transmitter	Transmitter, apparat (sender), som via radiobølger overfører informasjon fra ett medium til en mottaker; radiosender som overfører analoge eller digitale signaler til en mottaker. Kan være radio, telefoni eller f.eks. måleverdier	SNL (Store Norske Leksikon)
Trussel Engelsk: Threat	Potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm	IEC TS 62443-1-1:2009
Verifisering	confirmation, through the provision of objective evidence, that specified requirements have been fulfilled Note 1 to entry: The objective evidence needed for a verification can be the result of an inspection or of other forms of determination such as performing alternative calculations or reviewing documents. Note 2 to entry: The activities carried out for verification are sometimes called a qualification process. Note 3 to entry: The word “verified” is used to designate the corresponding status.	ISO 9000:2015
Validering	Confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled Note 1 to entry: In the IEC 61511 series this means demonstrating that the SIF(s) and SIS after installation meet the SRS in all respects.	IEC 61511-1:2016
Validering	confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled Note 1 to entry: The objective evidence needed for a validation is the result of a test or other form of determination such as performing alternative calculations or reviewing documents. Note 2 to entry: The word “validated” is used to designate the corresponding status. Note 3 to entry: The use conditions for validation can be real or simulated.	ISO 9000:2015

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

B Vedlegg B Krav til datakvalitet i relevante standarder og retningslinjer

B.1 IEC 61511-1:2016

AVSNITT OG TEMA	KRAV
IEC 61511-1:2016	
Kap.nr – kapittel tittel – Under titler	
3.2.54 programmable electronic system PES	3.2 Terms and definitions Data highways is mentioned as part of the definition of a PES
7.2.2 (ingen tittel)	7 Verification 7.2 Requirements Where the verification includes testing, the verification planning shall also address the following: • test cases and test data (these will be specific scenarios with the associated data) At some periodic interval (determined by the user), the frequency of testing shall be re-evaluated based on various factors including historical test data, plant experience and hardware degradation.
10.3.5 (ingen tittel)	10 SIS safety requirements specification (SRS) 10.3 SIS safety requirements I forbindelse med krav til anvendelsesprogram, skal man vurdere følgende: • application program self-monitoring (e.g., application driven watch-dogs and data range validation) the requirements for communication interfaces, including measures to limit their use and the validity of data and commands both received and transmitted
11.4.9 (ingen tittel) 11.9.3 (ingen tittel) 11.9.4 (ingen tittel)	11 SIS design and engineering 11.4 Hardware fault tolerance Reliability data in relation to requirements and confidence limit
11.5.2.2 (ingen tittel)	11 SIS design and engineering 11.5 Requirements for selection of devices 11.5.2 General requirements Failure rate data requirements and suitability
11.5.3.1 (ingen tittel)	11 SIS design and engineering 11.5 Requirements for selection of devices 11.5.3 Requirements for the selection of devices based on prior use Appropriate evidence related to Prior use data
11.7.3.2 (ingen tittel)	11 SIS design and engineering 11.7 Interfaces data necessary to troubleshoot the SIS

AVSNITT OG TEMA	KRAV
IEC 61511-1:2016	
Kap.nr – kapittel tittel – Under titler	
11.9.3 (uten tittel) 11.9.4 (uten tittel)	11 SIS design and engineering 11.9 Quantification of random failure Vendor data based on returns can be restricted to a population where there is full knowledge of the operational environment and fully recorded in accordance with IEC 60300-3-2:2004 or ISO 14224:2006. The user can also record the operational environment for the SIF and be able to demonstrate that the vendor's operational environment data matches the environment of the SIF. The reliability data uncertainties shall be assessed and taken into account when calculating the failure measure.
12.3.4	12 SIS application program development 12..3 Application program design The application program design and its decomposition into modules if applicable, shall address how the requirements are to be implemented, including the following as appropriate: • definition of input and output interfaces, including tag listings and the associated data types • details of the data exchanged between the SIS application program and the operator interfaces • details of the data exchanged between the SIS application program and the BPCS and peripherals such as printers, data storage, etc. a detailed description of any application level diagnostics that may be implemented such as external watch dogs, application data integrity checking, sensor validation to meet the required SIL
12.4.2 (ingen tittel)	12 SIS application program development 12.4 Application program implementation The following information shall be contained in the application program or related documentation: • j) a description of the program structure, including a description of the order of the logical processing of data with respect to the input/output sub-systems and any limitations imposed by scan times • k) If required by the SRS, the means by which: o the correctness of field data is ensured, (e.g., comparison between analog sensors to improve the diagnostic coverage); o • the correctness of data sent over a communication link is ensured (e.g., when communicating from an HMI, before implementation of a command an 'ack' or 'acknowledge' is transmitted); communications are made secure (e.g., cyber security measures);
12.5.3 (uten tittel)	12 SIS application program development 12.5 Requirements for application program verification (review and testing) The application program, including its decomposition into modules if appropriate, shall be verified through review, analysis, simulation and testing techniques using written procedures and test specifications, that shall be carried out to confirm that the application program functions meet the SRS and that unintended functions are not executed and that there are no unintended side effects with respect to the SIF. The following shall be addressed: internal data flow checks to confirm that the logic solver is not just apparently working, but is working as expected

AVSNITT OG TEMA	KRAV
IEC 61511-1:2016	
Kap.nr – kapittel tittel – Under titler	
12.5.4 (uten tittel)	12 SIS application program development 12.5 Requirements for application program verification (review and testing) The mapping of the I/O data to the application program, including data type and range, shall be verified.
13.2.2 (uten tittel)	13 Factory acceptance test (FAT) 13.2 Recommendations FAT planen skal spesifisere følgende: • Test cases, test description and test data • Internal data flow checks can be carried out to that the SIS is processing input data and generating output response as specified. Recording of tests conducted, data, results and observations whilst the tests are being conducted.
15.2.4 (uten tittel)	15 SIS safety validation 15.2 Requirements The validation of the SIS and its associated SIF(s) shall be carried out in accordance with the SIS validation planning. Validation activities shall include, but not be limited to, the following: the SIS properly communicates (where required) with the BPCS or any other system or network, including during abnormal conditions such as a data overload
15.2.6 (uten tittel)	15 SIS safety validation 15.2 Requirements 15.2.6 The results from the validation plan activities shall represent and cover the entire SIS validation process. SIS validation documentation shall be produced which provides: tools and equipment used, along with their calibration data
16.2.2 (uten tittel)	16 SIS operation and maintenance 16.2 Requirements Operation and maintenance procedures shall be developed in accordance with the relevant safety planning and shall provide the following: f) procedures for collecting data related to the demand rate and SIS reliability parameters;
16.3.1.5 (uten tittel)	16 SIS operation and maintenance 16.3 Proof testing and inspection At some periodic interval (determined by the user), the frequency of testing shall be re-evaluated based on various factors including historical test data, plant experience and hardware degradation.

B.2 IEC 61508-3:2010

AVSNITT OG TEMA	KRAV
IEC 61508-3:2010 Software	
Kap.nr – kapittel tittel – Kontekst titler	
6.2.3 (uten tittel)	6 Additional requirements for management of safety-related software 6.2 Requirements SW Configuration management shall: e) ensure that appropriate methods are implemented to load valid software elements and data correctly into the run-time system; g) formally document the release of safety-related software. Master copies of the software and all associated documentation and version of data in service shall be kept to permit maintenance and modification throughout the operational lifetime of the released software.
7.1.2.4 (uten tittel)	7 Software safety lifecycle requirements 7.1.2 Requirements NOTE 2 See Annex G for the characteristics of data-driven systems (e.g. full variability / limited variability programming languages, extent of data configuration) that may be relevant when customising the software safety lifecycle.
7.2.2.11 (uten tittel)	7 Software safety lifecycle requirements 7.2 Software safety requirements specification 7.2.2 Requirements Where software safety requirements are expressed or implemented by configuration data, the data shall be: a) consistent with the system safety requirements; b) expressed in terms of the permitted range and authorized combinations of its operational parameters; c) defined in a manner which is compatible with the underlying software (for example sequence of execution, run time, data structures, etc.). NOTE 1 This requirement on application data is particularly relevant to data-driven applications. These are characterized as follows: the source code is pre-existing and the primary objective of the development activity is to provide assurance that the configuration data correctly states the behaviour required from the application. There may be complex dependencies between data items, and the validity of data may change over time. NOTE 2 See Annex G for guidance on data-driven systems.
7.2.2.12 (uten tittel)	7 Software safety lifecycle requirements 7.2 Software safety requirements specification 7.2.2 Requirements Where data defines the interface between software and external systems, the following performance characteristics shall be considered in addition to 7.4.11 of IEC 61508-2: a.a) the need for consistency in terms of data definitions; b. b) invalid, out of range or untimely values; c. c) response time and throughput, including maximum loading conditions; d. d) best case and worst case execution time, and deadlock;

AVSNITT OG TEMA	KRAV
IEC 61508-3:2010 Software	
Kap.nr – kapittel tittel – Kontekst titler	
	e.e) overflow and underflow of data storage capacity.
7.4.1.3 (uten tittel)	7 Software safety lifecycle requirements 7.4 Software design and development 7.4.1 Objectives The third objective of the requirements of this subclause is to select a suitable set of tools, including languages and compilers, run-time system interfaces, user interfaces, and data formats and representations for the required safety integrity level, over the whole safety lifecycle of the software which assists verification, validation, assessment and modification.
7.4.1.6 (uten tittel)	7 Software safety lifecycle requirements 7.4 Software design and development 7.4.1 Objectives The sixth objective of the requirements of this subclause is to ensure, in so far as it is appropriate, that configuration of PE systems by data fulfils the specified requirements for the software systematic capability.
7.4.2.2 (uten tittel)	7 Software safety lifecycle requirements 7.4 Software design and development 7.4.2 Requirements In accordance with the required safety integrity level and the specific technical requirements of the safety function, the design method chosen shall possess features that facilitate: a) abstraction, modularity and other features which control complexity; b) the expression of: 1) functionality; 2) information flow between elements; 3) sequencing and time related information; 4) timing constraints; 5) concurrency and synchronized access to shared resources; 6) data structures and their properties;
7.4.2.7 (uten tittel)	7 Software safety lifecycle requirements 7.4 Software design and development 7.4.2 General requirements The software design shall include, commensurate with the required safety integrity level, self-monitoring of control flow and data flow. On failure detection, appropriate actions shall be taken.

AVSNITT OG TEMA	KRAV
IEC 61508-3:2010 Software	
Kap.nr – kapittel tittel – Kontekst titler	
7.4.2.14 (uten tittel)	7 Software safety lifecycle requirements 7.4 Software design and development 7.4.2 General requirements This Subclause 7.4.2 shall, in so far as it is appropriate, apply to data and data generation languages. NOTE See Annex G for guidance on data-driven systems. a) Where a PE system consists of pre-existing functionality that is configured by data to meet specific application requirements, the design of the application software shall be commensurate with the degree of application configurability, pre-delivered existing functionality and complexity of the PE safety-related system. b) Where the safety-related functionality of a PE system is determined significantly or predominantly by configuration data, appropriate techniques and measures shall be used to prevent the introduction of faults during the design, production, loading and modification of the configuration data and to ensure that the configuration data correctly states the application logic. c) The specification of data structures shall be: 1) consistent with the functional requirements of the system, including the application data; 2) complete; 3) self consistent; 4) such that the data structures are protected against alteration or corruption. d) Where a PE System consists of pre-existing functionality that is configured by data to meet specific application requirements, the configuration process itself shall be documented appropriately.
7.4.3	7 Software safety lifecycle requirements 7.4 Software design and development 7.4.3 Requirements for software architecture design NOTE 1 The software architecture defines the major elements and subsystems of the software, how they are interconnected, and how the required attributes, particularly safety integrity, will be achieved. It also defines the overall behaviour of the software, and how software elements interface and interact. Examples of major software elements include operating systems, databases, EUC input/output subsystems, communication subsystems, application program(s), programming and diagnostic tools, etc.
7.4.3.2 (uten tittel)	7 Software safety lifecycle requirements 7.4 Software design and development 7.4.3 Requirements for software architecture design e) select the design features to be used for maintaining the safety integrity of all data. Such data may include plant input-output data, communications data, operator interface data, maintenance data and internal database data;
7.4.4.2 (uten tittel)	7 Software safety lifecycle requirements 7.4 Software design and development 7.4.4 Requirements for support tools, including programming languages Software off-line support tools shall be selected as a coherent part of the software development activities. a.f) application data tools that produce or maintain data which are required to define parameters and to instantiate system functions. Such data includes function parameters, instrument ranges, alarm and trip levels, output states to be adopted at failure, geographical layout.

AVSNITT OG TEMA	KRAV
IEC 61508-3:2010 Software	
Kap.nr – kapittel tittel – Kontekst titler	
7.4.5	7 Software safety lifecycle requirements 7.4 Software design and development 7.4.5 Requirements for detailed design and development – software system design Requirements for detailed design and development – software system design a.However it is still good practice to design the software in a structured way, including organising the software into a modular structure that separates out (as far as possible) safety-related parts; including range checking and other features that provide protection against data input mistakes; using previously verified software modules; and providing a design that facilitates future software modifications.
7.4.8.2 (uten tittel)	7 Software safety lifecycle requirements 7.4 Software design and development 7.4.8 Requirements for software integration testing The software system integration test specification shall state the following: a.a) the division of the software into manageable integration sets; b. b) test cases and test data;
7.5.2.2 (uten tittel)	7 Software safety lifecycle requirements 7.5 Programmable electronics integration (hardware and software) 7.5.2 Requirements The software/PE integration test specification (hardware and software) shall state the following: a.a) the split of the system into integration levels; b. b) test cases and test data;
7.7.2.5 (uten tittel)	7 Software safety lifecycle requirements 7.7 Software aspects of system safety validation 7.7.2 Requirements For each safety function, software safety validation shall document the following results: d) tools and equipment used together with calibration data;
7.8.2.9 (uten tittel)	7 Software safety lifecycle requirements 7.8 Software modification 7.8.2 Requirements Information on the details of all modifications shall be documented. The documentation shall include the re-verification and re-validation of data and results.
7.9.2.7 (uten tittel)	7 Software safety lifecycle requirements 7.9 Software verification 7.9.2 Requirements Subject to the choice of software development lifecycle (see 7.1), the following verification activities shall be performed: a) verification of software safety requirements; b) verification of software architecture; c) verification of software system design; d) verification of software module design; e) verification of code; f) verification of data;

AVSNITT OG TEMA	KRAV
IEC 61508-3:2010 Software	
Kap.nr – kapittel tittel – Kontekst titler	
7.9.2.13 (uten tittel)	7 Software safety lifecycle requirements 7.9 Software verification 7.9.2 Requirements Verification of data. a) The data structures shall be verified. b) The application data shall be verified for: 1) consistency with the data structures; 2) completeness against the application requirements; 3) compatibility with the underlying system software (for example, sequence of execution, run-time, etc.); and 4) correctness of the data values. c) All operational parameters shall be verified against the application requirements. d) All plant interfaces and associated software (i.e. sensors and actuators and off-line interfaces: see 7.2.2.12) shall be verified for: 1) detection of anticipated interface failures; 2) tolerance to anticipated interface failures. e) All communication interfaces and associated software shall be verified for an adequate level of: 1) failure detection; 2) protection against corruption; 3) data validation.
Annex A (normative) Guide to the selection of techniques and measures	Relevant Techniques and measures mentioned related to data are: • Data recording and analysis • Data flow diagrams • Forward traceability between the software design specification and the software verification (including data verification) plan • Data flow analysis
Annex G (informative) Guidance for tailoring lifecycles associated with data driven systems	Mainly guidance related to configuration data

B.3 ISO 13849-1:2015

Diagnostikk er kun skikkelig nevnt i HW del av IEC 61508-2:2010 std serien
ISO 13849 henviser bl.a. til IEC 61508-2:2010 i forbindelse med DC. Altså del av tilfeldige feil og ikke systematiske feil. For tilfeldige feil er både IEC 61508 og ISO 13849-1 bra med tanke på data. Her finner man også nødvendig veiledning i både NOROG 070 og PDS håndbøkene.

Nedenfor har vi vist utdrag fra eksempler på DC hentet fra ISO 13849-1:2015 Annex E (informativ) "Estimates for diagnsotic coverage (DC) for functions and modules", tabell E1 "Examples of diagnostic coverage (DC)". Viser kun dette for "Input device":

Measure	DC
Input device	
Cyclic test stimulus by dynamic change of the input signals	90%
Plausibility check, e.g. sue of normally open and normally closed mechanically linked contacts	99%
Cross monitoring of inputs without dynamic test	0% to 99% depending on how often a signal change is done by the application
Cross monitoring of input signals with dynamic test if short circuits are not detectable (for multiple I/O)	90%
Cross monitoring of input signals and intermediate results within the logic (L), and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)	99%
Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90% to 99% depending on the application
Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99%
Fault detection by the process	0% to 99% depending on the application; this measure alone is not sufficient for the required performance level
Monitoring some characteristics of the sensor (response time, range of analogue signals, e.g. electrical resistance, capacitance)	60%

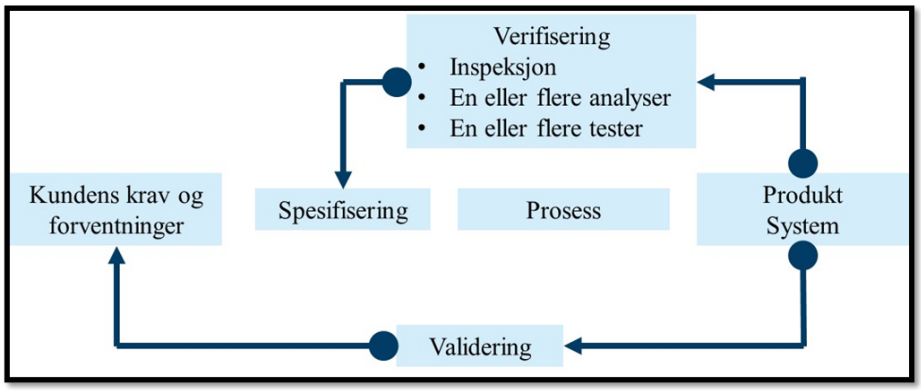
B.4 Data Safety Guidance (v3.2), The Data Safety Initiative Working Group (DSIWG), SCSC-127

Data har mange egenskaper. De 22 ulike egenskapene i Data Safety Guidance er listet nedenfor med tilhørende beskrivelse og kommentarer (20 av disse egenskapene er hentet fra SCSC -guide, mens vi har lagt til to egenskaper: Testbarhet og analyserbarhet).

De første 2 kolonnene er direkte kopi fra SCSC Guide med unntak av:

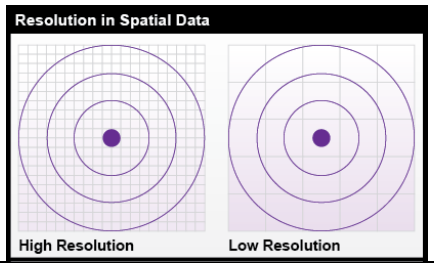
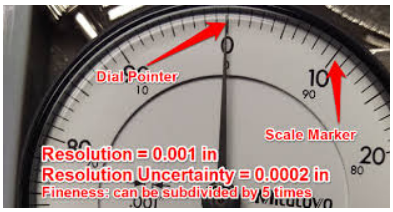
- Lagt inn to tilleggsegenskaper: Testability (testbarhet) og analysability (analyserbarhet)

Sammenhengen mellom testing, analyse, verifisering og validering er vist i Figur B.1



Figur B.1: Sammenhengen mellom testing, analyse, verifisering og validering

Tabell B.1 Data egenskaper (tabell 5 i SCSC Guide [59])

Data egenskap	Beskrivelse	Kommentarer
Integrity	The data is correct, true and unaltered	
Completeness	The data has nothing missing or lost	
Consistency	The data adheres to a common world view (e.g., units)	
Continuity	The data is continuous and regular without gaps or breaks	
Format	The data is represented in a way which is readable by those that need to use it	
Accuracy	The data has sufficient detail for its intended use	
Resolution	The smallest difference between two adjacent values that can be represented in a data storage, display or transfer system 	Oppløsning til ett måleinstrument 
Traceability	The data can be linked back to its source or derivation	Sporbarhetskrav er noe svak i IEC 61508-3:2010 og blir bedret i utgave 3
Timeliness	The data is as up to date as required	
Verifiability	The data can be checked and its properties demonstrated to be correct	Se figuren ovenfor
Testability	The data can be tested and its properties demonstrated to be correct	Se figuren ovenfor
Analysability	The data can be analysed and its properties demonstrated to be correct	Se figuren ovenfor
Availability	The data is accessible and usable when an authorised entity demands access	
Fidelity / Representation	How well the data maps to the real world entity it is trying to model	
Priority	The data is presented / transmitted / made available in the order required	
Sequencing	The data is preserved in the order required	
Intended Destination / Usage	The data is only sent to those that should have access to it	
Accessibility	The data is visible only to those that should see it	
Suppression	The data is intended never to be used again	
History	The data has an audit trail of changes	
Lifetime	When does the safety-related data expire	
Disposability / Deletability	The data can be permanently removed when required	

Teknologi for et bedre samfunn

www.sintef.no