EKSTERN RAPPORT NR. 6 / 2025

Sikkerhet for skybasert OT i kritisk infrastruktur

SKREVET AV SINTEF

NVE Ekstern rapport nr. 6/2025
Sikkerhet for skybasert OT i kritisk infrastruktur

Utgitt av:	Norges vassdrags- og energidirektorat
Redaktør:	Linn Barstad
Forfattere:	Karin Bernsmed, Lars Flå, Maren Istad og Martin Gilje Jaatun / SINTEF
Omslagsbilde:	Tistedalsfoss 1 kraftverk
Foto:	Unn Eide, NVE
ISBN:	978-82-410-2461-0
ISSN:	2535-8235
Saksnummer:	202504456

Sammendrag:

Denne rapporten beskriver hvordan sikkerheten til klasse 1 og 2 driftskontrollsystemer kan ivaretas når funksjoner kritiske for operasjonell driftskontroll er avhengig av eller er plassert i skyen. Basert på en litteraturstudie viser vi hvordan tre andre bransjer har begynt å ta i bruk skytjenester for IT/OT systemer, samt hvordan utviklingen i kraftbransjen utenfor Norge utvikler seg. Videre gjennomgås sikkerhetskrav fra gjeldende regelverk og relevante standarder som siden brukes for å tegne opp fire forskjellige tilnærminger til sikker bruk av skytjenester for norske driftskontrollsystemer.

Emneord:

Driftskontrollsystemer, skytjenester, IT, OT, kraftbransje, sikkerhetskrav, informasjonssikkerhet, skyløsninger, beskyttelse av driftskontrollsystem, driftssentral, lokalkontroll, kraftberedskapsforskriften, sikkerhetsanalyse, kritisk infrastruktur.

Norges vassdrags- og energidirektorat
Middelthuns gate 29
Postboks 5091 Majorstuen
0301 Oslo

Telefon: 22 95 95 95
E-post: nve@nve.no
Internett: www.nve.no

Februar 2025

Forord

Integrasjonen av informasjonsteknologi (IT) og operasjonell teknologi (OT) øker i alle bransjer, inkludert kraftsektoren. Det er et sterkt ønske og behov for å ta i bruk ny teknologi og nye løsninger. For å håndtere dagens og fremtidens utfordringer må kraftsektoren kunne ta i bruk teknologiske løsninger som kan forbedre effektiviteten og robustheten i deres systemer. Dette er avgjørende for å møte de økende kravene til det grønne skiftet og energieffektivitet. Bruk av skytjenester i IT og i OT er en naturlig del av dette behovet i kraftsektoren.

Formålet med rapporten er å se på hvordan NVE kan legge til rette for bruk av ny teknologi, uten at risikoen for kraftforsyningen øker. Rapporten bygger på hvordan skytjenester for OT/IT-systemer vurderes brukt i andre sektorer.

Rapporten presenter en grundig gjennomgang av gjeldene sikkerhetskrav i norsk lovgivning, samt internasjonale standarder, og skisserer ulike tilnærminger for bruk av skytjenester i driftskontrollsystemer. Funnene viser at skytjenester kan være en sikker og hensiktsmessig løsning, forutsatt at de stilles gode krav og at disse oppfylles av leverandørene. Rapporten peker også på en rekke utfordringer og forutsetninger som må være på plass for sikker bruk av skytjenester.

Vi vil takke Sintef for deres grundige arbeid med utarbeidelsen av denne rapporten. Dette gir et godt grunnlag for å forstå utfordringene på dette området, og for videre utvikling av kraftberedskapsforskriften.

Oslo, februar 2025

Christian Damslora
fungerende seksjonssjef
seksjon for digital sikkerhet i kraftforsyningen
Tilsyns- og beredskapsavdelingen

Dokumentet sendes uten underskrift. Det er godkjent i henhold til interne rutiner.

Rapport

Sikkerhet for skybasert OT i kritisk infrastruktur

Forfattere:
Karin Bernsmed, Martin Gilje Jaatun, Maren Istad, Lars Flå

Rapportnummer:
2024: 01266 - Åpen

Oppdragsgiver:
Norges vassdrags- og energidirektorat (NVE)

SINTEF Digital
Postadresse:
Postboks 4760 Torgarden
7465 Trondheim

Sentralbord: 40005100

info@sintef.no

Foretaksregister:
NO 919 303 808 MVA

Rapport

Sikkerhet for skybasert OT i kritisk infrastruktur

EMNEORD
Sikkerhet
IT/OT
Skytjenester

VERSJON
1.2

DATO
2024-12-09

FORFATTER(E)
Karin Bernsmed, Martin Gilje Jaatun, Maren Istad, Lars Flå

OPPDRAGSGIVER(E)
Norges vassdrags- og energidirektorat (NVE)

OPPDRAGSGIVERS REFERANSE
202409285

PROSJEKTNUMMER
102031735

ANTALL SIDER OG VEDLEGG
55

SAMMENDRAG
Den norske kraftsektoren har kommet langt når det gjelder digitalisering. Denne rapporten beskriver hvordan sikkerheten for klasse 1 og 2 driftskontrollsystemer kan ivaretas når funksjoner kritiske for operasjonell driftskontroll er avhengig av eller er plassert i skyen. Basert på en litteraturstudie viser vi hvordan tre andre bransjer har begynt å ta i bruk skytjenester for IT/OT systemer, samt hvordan utviklingen i kraftbransjen utenfor Norge arter seg. Videre gjennomgår vi sikkerhetskrav fra gjeldende norsk regelverk og relevante standarder som siden brukes for å tegne opp fire forskjellige tilnærminger til sikker bruk av skytjenester for driftskontrollsystemer. Rapportens konklusjon er skytjenester generelt sett er tilstrekkelig sikre for bruk i driftskontrollsystemer, gitt at leverandøren er villig og i stand til å oppfylle en rekke nødvendige sikkerhetskrav, men at det i dag ikke er mulig å ta i bruk slike løsninger i klasse 1 og 2 driftskontrollsystemer pga. gjeldende regelverk.

UTARBEIDET AV
Karin Bernsmed

SIGNATUR

KONTROLLERT AV
Vahiny Gnanasekaran

SIGNATUR

GODKJENT AV
Andrea Neverdal Skytterholm

SIGNATUR

RAPPORT NR.
2024: 01266

ISBN
978-82-14-07119-1

GRADERING
Åpen

GRADERING DENNE SIDE
Åpen

Historikk

VERSJON	DATO	VERSJONSBESKRIVELSE
1.0	2024-11-08	Første versjon sendt til kunde for gjennomlesing
1.1	2024-11-22	Endelig versjon
1.2	2024-12-09	Oppdatering etter tilbakemelding på presentasjon

Innholdsfortegnelse

1 Introduksjon 5

2 Bakgrunn 6

2.1 Dagens driftskontroll 6

2.2 Skytjenester i et driftskontrollperspektiv 8

2.3 Utfordringer med skyløsninger 9

3 Relevante sikkerhetskrav 12

3.1 Sikkerhetskrav fra Kraftberedskapsforskriften 12

3.1.1 Kapittel 6: Informasjonssikkerhet 12

3.1.2 Kapittel 7: Beskyttelse av driftskontrollsystem 13

3.1.3 Oppsummering av kravene 24

3.2 Andre lovverk og standarder 25

3.2.1 EU-direktivet NIS 2 25

3.2.2 IEC 62443 25

3.2.3 IEC 62351 26

3.3 Retningslinjer for god praksis 26

4 Litteraturstudie 28

4.1 Akademisk litteratur 28

4.2 Grålitteratur 30

5 Bruk av skybaserte tjenester for driftskontroll i andre sammenhenger 34

5.1 Case: Skykontroll av produksjonsprosess 34

5.2 Case: Skykontroll av sementproduksjon 35

5.3 Case: Skykontroll av jernbane 36

5.4 Case fra kraftsektoren utenfor Norge 37

6 Referansearkitektur 39

6.1 Dagens situasjon 39

6.2 Eksempel: Historian i skyen 42

6.2.1 Sikkerhetsanalyse 42

6.2.2 Designkriterier 43

6.3 Eksempel: Reservedriftssentral i skyen 44

6.3.1 Sikkerhetsanalyse 44

6.3.2 Designkriterier 45

6.4 Eksempel: Skybasert driftssentral 46

6.4.1 Sikkerhetsanalyse 47

6.4.2 Designkriterier 47

6.5 Eksempel: Skybasert lokalkontroll 48

6.5.1 Sikkerhetsanalyse 48
6.5.2 Designkriterier 49

7 Konklusjon og videre arbeid.....50

8 Referanser 51

1 Introduksjon

Kraftsektoren har kommet langt når det gjelder digitalisering, sammen med mange andre sektorer i Norge. Samtidig står bransjen ovenfor et alvorlig trusselbilde drevet av ressurssterke aktører med politiske, militære og økonomiske interesser. Kraftforsyningen er en av Norges mest samfunnskritiske infrastrukturer, og digitale angrep mot deres IT/OT- systemer kan potensielt forårsake mye skade.

Målsetningen med denne rapporten er å beskrive hvordan sikkerheten til klasse 1 og 2 driftskontrollsystemer kan ivaretas når funksjoner kritiske for operasjonell driftskontroll er avhengig av eller er plassert i skyen. Målgruppen for kravene som fremstilles i rapporten er dermed nettselskaper, siden de typisk eier driftskontrollsystemer av klasse 1 og 2. Rapporten inneholder:

- En overordnet oversikt over dagens driftskontroll, en introduksjon til skytjenester i et driftskontrollperspektiv og en gjennomgang av relevante utfordringer ved bruk av skytjenester (kap. 2)
- En analyse av kravene i kraftberedskapsforskriften og av krav fra andre relevante lovverk og standarder (kap. 3).
- En litteraturstudie om bruk av skyløsninger i kommersielle fabrikker, prosessindustri, annen kritisk infrastruktur utenfor kraftsektoren og i kraftsektoren utenfor Norge, komplettert med en oversikt over andre kilder relevante for skybasert driftskontroll (kap. 4).
- Beskrivelser av fire caser, en fra hver av de ovenfornevnte sektorene (kap. 5).
- Referansearkitekturer for sikre skybaserte klasse 1 og klasse 2 driftskontrollsystemer, inkludert sikkerhetsanalyse og designkriterier (kap. 6).
- Konklusjon og våre anbefalinger for videreføring av resultatene i denne rapporten (kap. 7).

Resultatene fra prosjektet vil kunne hjelpe NVE å evaluere om sikkerhetskravene i energiloven og kraftberedskapsforskriften er riktige og fornuftige, og med å legge til rette for at norske virksomheter skal kunne ta i bruk ny teknologi uten at risikoen i kraftforsyningen øker.

I denne rapporten bruker vi begrepet «sikkerhet» i betydningen «informasjonssikkerhet» (på engelsk «security» eller «cyber security») med mindre annet er angitt.

2 Bakgrunn

Før vi går inn på spesifikke krav rettet mot sikre, skybaserte driftskontrollsystem, vil det være nyttig med en gjennomgang av noen begreper. I seksjon 2.1 gir vi en oversikt over dagens driftskontroll, inkludert definisjonen av klasse 1 og 2 driftskontrollsystemer, som er temaet i denne rapporten. I seksjon 2.2 gjennomgår vi skytjenester, begreper og teknologier som kan bli relevante å ta i bruk. Til sist i seksjon 2.3 sammenfatter vi noen av utfordringene ved bruk av skyløsninger som vil bli spesielt relevante, sett fra et driftskontrollperspektiv.

2.1 Dagens driftskontroll

Kraftberedskapsforskriften (KBF) [1] er fastsatt av NVE med hjemmel i energiloven. I paragraf § 5-2 av KBF står det: «*Ved klassifisering av anlegg, system eller annet som har vesentlig betydning for drift eller gjenoppretting av eller sikkerhet i produksjon, omforming, overføring eller fordeling av elektrisk energi eller fjernvarme benyttes klasse 1 til 3. Klasse 3 benyttes der betydningen for kraftforsyningen er størst.*» Denne rapporten omhandler klasse 1 og 2 driftskontrollsystemer, som omtalt i punkt h) i listene under. De er mindre viktige for kraftforsyningen sammenlignet med klasse 3, men det får likevel konsekvenser for sluttbrukere om anlegg i klasse 1 og 2 ikke fungerer.

Klasse 1 omfatter:

a. *Kraftstasjon med samlet installert generatorytelse på minst 50 MVA.*
b. *Transformatorstasjon med samlet hovedtransformatorytelse på minst 10 MVA.*
c. *Omformerstasjon med samlet installert ytelse for omforming på minst 10 MVA.*
d. *Selvstendig koblingsstasjon i kraftsystemet bygget for et spenningsnivå på minst 30 kV.*
e. *Kraftledning bygget for et spenningsnivå på minst 5 kV.*
f. *Fjernvarmesentral med samlet installert ytelse på minst 50 MW. I ytelsen skal medregnes effekt i ekstern varmeleveranse.*
g. *Transformatorstasjon til vindkraftanlegg med samlet installert ytelse på minst 75 MVA. Dersom transformatorstasjonen også transformerer til nettformål, klassifiseres den som transformatorstasjon etter bokstav b.*
h. *Driftskontrollsystem som styrer eller overvåker anlegg som omfattet av bokstav a til g.»*

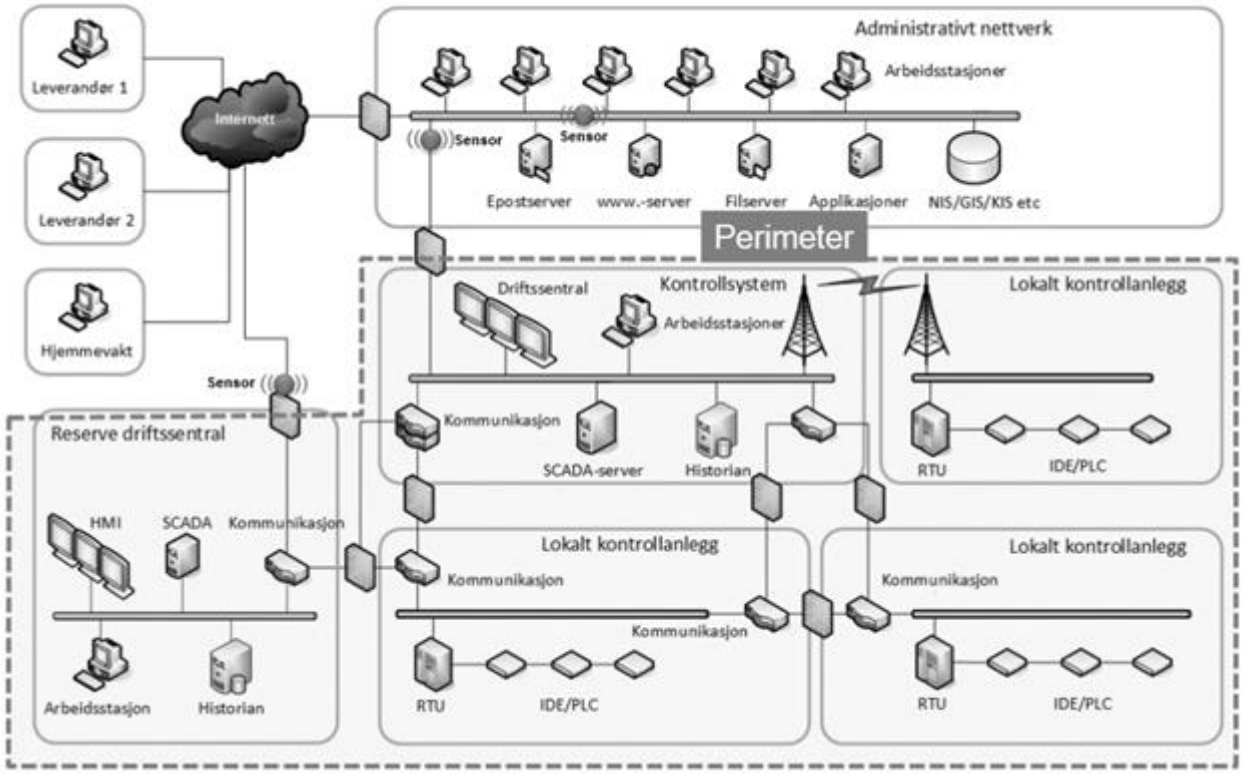
Klasse 2 omfatter:

a. *Kraftstasjon med samlet installert generatorytelse på minst 100 MVA og kraftstasjoner på minst 100 MVA plassert i dagen.*
b. *Transformatorstasjon med samlet hovedtransformatorytelse på minst 50 MVA og høyeste spenningsnivå på minst 30 kV.*
c. *Omformerstasjon med samlet installert ytelse for omforming på minst 50 MVA og høyeste spenningsnivå på minst 30 kV.*
d. *Selvstendig koblingsstasjon i kraftsystemet bygget for et spenningsnivå på minst 100 kV.*
e. *Kraftledning bygget for et spenningsnivå på minst 30 kV.*
f. *Fjernvarmesentral med samlet installert ytelse på minst 150 MW. I ytelsen skal medregnes effekt i ekstern varmeleveranse.*
g. *Transformatorstasjon til vindkraftanlegg med samlet installert ytelse på minst 500 MVA. Dersom transformatorstasjonen også transformerer til nettformål, klassifiseres den som transformatorstasjon etter bokstav b, men ikke lavere enn klasse 2.*
h. *Driftskontrollsystem som styrer eller overvåker kraftforsyningen til befolkning på minst 50 000, eller flere anlegg omfattet av bokstav a til g.*

KBF sier at klassifiserte anlegg skal sikres slik at risiko for skade, havari osv. er minst mulig. Kapittel 7 i KBF omhandler spesifikt beskyttelse av driftskontrollsystem. Som en del av dette omhandler kapittel 7-1 en generell plikt til å beskytte driftskontrollsystemet og gir også en definisjon av driftskontrollsystemer:

> *«Driftskontrollsystemer omfatter driftssentraler, utstyr, nettverk, datarom, sambandsanlegg og øvrige anlegg og rom, systemer og komponenter som ivaretar driftskontrollfunksjoner. Med anlegg forstås også tilhørende bygningstekniske konstruksjoner for driftskontrollfunksjoner.*
>
> *Driftskontrollfunksjoner er alle organisatoriske, administrative og tekniske tiltak for å overvåke, styre og beskytte anlegg i kraftforsyningen.»*

I veilederen til kraftberedskapsforskriften [2] er Figur 1 under brukt for å illustrere driftskontrollsystem og administrativt nettverk. Det som er innenfor stiplet linje regnes som driftskontrollsystem.



Figur 1: Driftskontrollsystem – alt innenfor stiplet linje regnes som driftskontrollsystem [2].

I denne rapporten er oppgaven å beskrive hvordan cybersikkerheten til klasse 1 og 2 driftskontrollsystemer kan ivaretas når funksjoner kritiske for operasjonell driftskontroll er avhengig av eller er plassert i skyen. For å gjøre dette vil vi i kapittel 6 av rapporten presentere en referansearkitektur, med tilhørende designkriterier, for vise hvordan man kan sikre skybaserte klasse 1 og klasse 2 driftskontrollsystemer. Ved utarbeidelsen av referansearkitekturen har vi derfor tatt utgangspunkt i de funksjoner som er innenfor den stiplede linjen i Figur 1, og i den tilsvarende definisjonen av «driftskontrollsystemer» fra kapittel 7-1 i KBF. Vi har valg å inkludere reserve driftssentral, selv om det er kun et krav for klasse 3 driftskontrollsystemer, da skyløsninger åpner helt nye muligheter mtp redundans.

2.2 Skytjenester i et driftskontrollperspektiv

Skytjenester (cloud computing) er en samlebetegnelse på alt fra dataprosessering og datalagring til programvare på servere som er tilgjengelig fra serverparker tilknyttet internett[1]. Skytjenester vil altså bringe internett inn i driftskontrollsystemet. USAs National Institute of Standards and Technology (NIST) beskriver tre typer av skytjenester [3]:

- Infrastructure-as-a-Service (IaaS). Virtuelle maskiner konfigureres over internett. Kundene må selve administrere operativsystem, programvare etc. på de virtuelle maskinene.
- Platform-as-a-Service (PaaS). Utviklingsmiljø (typisk for å lage nye tjenester) ferdig konfigurert og levert via internettet. Tilbyderen står for administrasjon av det underliggende operativsystemet.
- Software-as-a-Service (SaaS). Programvare tilbudt som webapplikasjoner.

I tillegg har nye typer av skytjenester blitt utviklet de siste årene. Spesielt relevant for denne rapporten er:

- Data-as-a-Service (DaaS). Kunden kjøper en ferdig database i en sky og mater inn egne data.
- SCADA-as-a-Service. Aktører som leverer industrielle kontrollsystemer, tilbyr egne skytjenester.

Det er vanlig med hybride løsninger, for eksempel SaaS leverandører som plasserer sine tjenester i infrastrukturen til en IaaS leverandør.

NIST beskriver videre fem egenskaper som karakteriserer skytjenester:

1. Selvbetjening for å tilpasse kapasitet.
2. Adkomst via nettverk.
3. Delte ressurser.
4. Rask kapasitetstilpassing.
5. Betaling for brukt kapasitet.

Fra et driftskontrollperspektiv, er alle disse fem egenskapene relevante. Som vil bli vist, tilbyr egenskapene 1, 4 og 5 muligheter å forenkle og forbedre implementasjonen av reservedriftssentralen. Samtidig vil egenskap 2 og 3 medføre økt sikkerhetsrisiko. Dette, og mye annet, vil bli gjennomgått i mer detalj senere i rapporten.

Det finnes ulike typer skyløsninger. Skyløsninger kan være offentlige (alle kan få tilgang mot betaling), private (en organisasjon oppretter en sky som en intern løsning), spleiselag (en samling organisasjoner oppretter en sky til felles bruk), og hybride (en privat sky betaler for ekstra kapasitet fra en offentlig sky). Fra et sikkerhetsperspektiv vil både type av skytjeneste, og valgt arkitektur for leveranse av skytjeneste, påvirke hvilken risiko skytjenesten medfører. Hvis en privat sky brukes, vil eieren av skytjenesten og eieren av driftskontrollsystemet være samme organisasjon, og da vil ikke bruken av sky medføre at data flyttes utenfor organisasjonen sin kontroll. Bruken av en privat skytjeneste trenger i slike tilfeller heller ikke å medføre eksponering mot Internett og dermed ikke forhøyet cyberrisiko. Situasjonen vil bli annerledes hvis en hybrid eller offentlig løsning benyttes. Det er vår oppfatning at private skytjenester vanligvis kun er aktuelt å ta i bruk av store aktører, og de store nettselskapene vil ofte ha driftskontrollsystemer i klasse 3, som er utenfor scope for denne rapporten. Hvis store nettselskaper driver slike private skytjenester, kan de også videreselge tjenester til mindre nettselskaper, men da holdes det hele innenfor sfæren av Kraftforsyningens beredskapsorganisasjon (KBO). Denne rapporten tar derfor ikke for seg private skyløsninger, hvis ikke noen annet sies. Isteden fokuserer vi på skytjenester som tilbys av eksterne leverandører, og hvor tjenestene er fysisk implementert utenfor systemeierens (nettselskapets) egne lokaler. Kort fortalt, når vi referer til skyløsninger og/eller skytjenester i denne rapporten så mener vi altså alltid **tjenester som tilgjengeliggjøres via internett**.

[1] Datatilsynet: https://www.datatilsynet.no/personvern-pa-ulike-omrader/internett-og-apper/skytjenester/

For driftskontrollsystemer er det i tillegg relevant å se på hvilken type funksjoner som kan bli avhengig av eller plassert i skyen. Operasjonell driftskontroll er ikke eller i veldig liten grad (mer på uttestingsnivå) avhengig av data eller funksjoner som utføres i skyen i dag. Vi forutser derimot at dette vil endre seg. Eksempelvis kan et ønske om (og et eksternt press om) å drifte nettet mer dynamisk medføre at nettselskapene installerer nye sensorer på kraftledninger og kabler, og benytter data fra disse til å forutsi framtidig belastning. Slike prediksjoner legger deretter grunnlag for operasjonelle beslutninger i driftssentralen. Ettersom data fra slike sensorer kan ligge i skyen (eller ta veien om skyen) har man dermed en situasjon hvor operasjonelle beslutninger er avhengig av data eller analyser som ligger i eller utføres i skyen. Vi ser allerede i dag at noen nettselskaper benytter skyløsninger i forbindelse med både innhenting av sensordata fra eksterne leverandører og til å utføre dataanalyser, men det er ofte ikke data og analyser som (ennå) brukes i operativ drift. I NVE sitt veikart for oppfølging av IKT-sikkerhet i leverandørkjeden fra 2021 [4] rapporteres det av både selskaper og leverandører i kraftbransjen om bruk av skytjenester (SaaS-tjenester) blant annet på virksomhetsstyringssystem (ERP-system), fagapplikasjoner og andre administrative systemer, mens driftskontrollsystemer (SCADA-systemer) ennå ikke er løftet til sky på grunn av forskriftskrav.

Det er en rekke teknologier som kan bli relevante ved vurdering av bruk av skytjenester for driftskontrollsystemer. Spesielt for denne rapporten har vi:

- Node-RED[2]. Et grafisk programmeringsverktøy brukt til å koble sammen maskinvare, APIer, og internettbaserte tjenester. Node-RED bygger på Node.js, som er et åpent kryssplattform runtime-system for server- og nettverksapplikasjoner basert på JavaScript. Node-RED gjør det enkelt å lage datadrevne prosesser med minimal kode, men er ikke designet for å maksimere ytelsen.
- OPC UA[3]. En åpen, plattformuavhengig og serviceorientert kommunikasjonsarkitektur for kommunikasjon mellom industrielt utstyr og systemer. Den er basert på en klient-tjener-modell, men har i tillegg mulighet til «publiser/abonner». OPC UA har kapasitet til sanntidskontroll og har en lang fortid innen industrielle applikasjoner. Sikkerhet, i form av autentisering, kryptering og logging, er en del av arkitekturen.
- MQTT[4]. En lettvekts «publish/subscribe» protokoll for maskin-til-maskin-kommunikasjon. MQTT har blitt svært populært i IoT applikasjoner siden den krever mye mindre ressurser enn OPC UA.

Disse tre teknologiene brukes allerede i en eller flere av casene som presenteres i kapittel 5 i denne rapporten.

2.3 Utfordringer med skyløsninger

Generelt er bruk av skytjenester veldig sikkert i dag, uavhengig av type skytjeneste som brukes, tjenesteleverandør og hvilket land datasenteret er plassert i [5]. I mange tilfeller vil man få økt sikkerhet ved bruk av skytjenester sammenlignet med foregående løsning. Men det finnes fortsatt flere årsaker til at skyløsninger kan være problematiske, sett fra et driftskontrollperspektiv. Her går vi gjennom noen av de mest åpenbare utfordringene som kan oppstå hvis nettselskaper tar i bruk skyløsninger for driftskontrollsystemer, og som derfor er relevante for analysen i denne rapporten. Informasjonen er sammenstilt fra [6] og [7].

[2] https://nodered.org/
[3] https://opcfoundation.org/about/opc-technologies/opc-ua/
[4] https://mqtt.org/

Tjenesteutsetting av kontrollen til ekstern part. Tjenesteutsetting av funksjoner som brukes ved styring av et system til en ekstern part medfører at denne gis full kontroll over disse funksjonene. Den eksterne parten vil håndtere funksjonene og den infrastruktur hvor funksjonene (tjenestene) er installert i henhold til opprettede tilgjengelighetsavtaler (SLA) og driftsinstruksjoner. Det samme gjelder ved lagring av data**.** Når data lagres i et eksternt datasenter, medfører dette at eieren av dataene ikke lenger selv har full kontroll over hvem som har tilgang til dataene.
Det er viktig å merke seg at avgrensninger mellom funksjoner og data fra forskjellige kunder er kun tydeliggjort på logiske nivå i skytjenester, som medfører en risiko for f.eks. at dataene lekker ut ved feil i virtualiserings-programvaren eller om det er blitt gjort administrative feil ved oppsettet og konfigurasjonen av tjenesten. I tillegg vil driftspersonellet ved skyleverandøren sannsynligvis ha systemadministratortilgang til nettselskapene sine funksjoner og data. Selv om tilgangskontrollen er kontraktsfestet og korrekt implementert i skytjenesten, vil det medføre noe risiko å gi fra seg kontrollen av (deler av) et system.

Mister kontroll over systemets plassering og hvem man deler sky med. Ved bruk av skytjenester vil nettselskapets kontroll over systemets fysiske plassering reduseres. Tidligere ble det ofte ansett som et problem at kunder til skytjenester ikke hadde kontroll over hvor dataene var lagret, men i dag er de fleste leverandører kjent med utfordringene og kan tilby tilpassede løsninger, for eksempel at dataene lagres på europeisk eller norsk jord. Skytjenesteleverandøren kan for eksempel ta inn nye kunder som medfører at trusselbildet øker, eller leverandøren kan bli mål for inngripende fra myndigheter basert på andre kunder som bruker den samme plattformen eller datasenteret. Uansett vil det fortsatt medføre noe risiko å gi fra seg kontrollen av systemet sine omgivelse.

Sikre korrekt tilgangskontroll og logging. Både tilgangskontroll og logging vil bli mer komplekst når flere aktører er involvert. I en skytjeneste vil det være minst fire forskjellige aktører involvert: nettselskapet (som kjøper tjenesten), skytjenesteleverandøren (som eier tjenesten), driftspersonell (som ofte er tjenesteutsatt til en tredjepart) og kommunikasjonsleverandøren (som leverer forbindelsen til skytjenesten). Teknisk sett er det ikke noe problem å etablere en fungerende rollebasert tilgangskontroll med definerte sikkerhetstillatelser og spesifisert logging i en skytjeneste, men risikoen for menneskelige feil øker når kompleksiteten øker.

Utvidet angrepsflate. Ved flytting av deler av et system som tidligere vært lokalisert internt opp i skyen vil kommunikasjonskanalen mot skytjenesten bli et nytt angrepspunkt, med tilhørende risiko for eksempel for avlytting av kommunikasjon og tjenestenektangrep. I tillegg bruker mange skytjenesteleverandører webgrensesnitt for leveranse eller konfigurasjon av sine tjenester, og angrep på disse er ikke uvanlig. De store leverandørene er i seg selv ofte et attraktivt mål for potensielle angripere, hvilket medfører at trusselbildet mot de som bruker deres tjenester også øker.

Økt systemkompleksitet, sammensatte avhengigheter og uforutsette kaskadeeffekter. Ved bruk av skytjenester vil kompleksiteten av systemet øke. Virtualisering medfører innføring av et ekstra lag av programvare på logisk nivå som gjemmer den underliggende maskinvaren. Det blir vanskeligere, og i mange tilfeller umulig, å fremskaffe en detaljert oversikt over hvordan systemet er implementert, spesielt på et fysisk nivå. Dette betyr at nettselskapene vil bli avhengig av at skyleverandører informerer om endringer som skjer i deres systemer, for eksempel i den underliggende nettverkstopologien eller i selve oppsettet av tjenesten som kjøpes.

Likevel vil det være mange kunder som er avhengige av samme type skytjenester og -teknologier. Dette leder til en usynlig (for kjøperen av tjenesten/teknologien) reduksjon av redundans og kan medføre at to tilsynelatende redundante funksjoner feiler samtidig, på tross av at de fremstår som uavhengig i teorien.

Gjenbruk av teknologi er en fundamental egenskap ved skytjenester som følger av tilbydernes behov for en lik og effektiv tjenesteleveranse til mange forskjellige kunder med mulighet for oppskalering ved behov. I tillegg til minket redundans medfører dette at risikoen for uforutsette kaskadeeffekter av feil og angrep vil øke, når mange tjenester fra flere forskjellige sektorer er avhengige av en håndfull teknologier.

Hendelseshåndtering. Håndteringen av sikkerhetshendelser må forberedes nøye. Skytjenesteleverandøren har ikke kjennskap til lokale forhold og sannsynligvis ikke de samme bakgrunnskunnskapene om nettselskapenes systemer som nettselskapets ansatte. Det er viktig å merke seg at ved en hendelse vil skytjenesteleverandøren kun følge rutinene som er satt opp i de etablerte avtalene. Det er derfor svært viktig å sikre at rutinene fungerer i alle ledd i kjeden; deteksjon, varsling, iverksetting av strakstiltak for å begrense skade og etablering av permanente korrigerende tiltak for å hindre gjentagelse. Kostnadene og konsekvensene av et uforutsett feil eller et tilsiktet angrep kan ellers bli meget store, og håndteringen av disse blir vanskelige å forberede seg på. Videre kan det bli komplisert, kanskje umulig, å gjennomføre beredskapsøvelser som inkluderer skytjenesteleverandøren. Her vil det bli svært viktig å sikre seg at avtalen med leverandøren dekker alle situasjoner som kan oppstå på en tilfredsstillende måte.

Skyleverandørens stabilitet. Skyleverandørens stabilitet som bedrift, både finansielt og juridisk, må tas i betrakting fordi det kan påvirke tilgangen til både funksjonene og dataen som lagres i skyen. Det er svært viktig å sikre at nettselskapene sine beredskapsplaner er i stand til å håndtere alle typer avbrudd som kan skje, inkludert langvarige avbrudd som kan skje under en juridisk konflikt, som vil gå utover formuleringene i et «standard»-tilgjengelighetsavtale. Portabilitet av data og funksjoner som kjøres i skyen må derfor sikres og testes nøye, og interne beredskapsplaner bør dekke et scenario hvor skyleverandøren plutselig «forsvinner» fra markedet.

Kontroll av etterlevelse av avtaler. Det blir vanskeligere å kontrollere skytjenesteleverandørens etterlevelse av avtaler når nettselskapet ikke har tilgang til den underliggende plattformen.

I tillegg til disse utfordringene er NSM sine svar på «ofte stilte spørsmål om sky og tjenesteutsetting»[5] svært relevante å lese for en bedre forståelse av fordelene og ulempene med skyløsninger.

[5] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/sporsmal-om-sky-og-tjenesteutsetting/

3 Relevante sikkerhetskrav

Relevante sikkerhetskrav ved vurdering av skybasert driftskontroll finner vi først og fremst i Kraftberedskapsforskriften (KBF). I tillegg vil NIS 2 direktivet [8] bli relevant, samt de etablerte standardene IEC 62443 [9] og IEC 62351 [10].

Andre relevante lovverk og standarder (for eksempel CER-direktivet, Cybermotstandsdirektivet og Cybersikkerhetsloven) er ikke tatt med i analysen i denne rapporten.

3.1 Sikkerhetskrav fra Kraftberedskapsforskriften

Ved vurdering av bruk av skytjenester for funksjoner kritiske for operasjonell driftskontroll vil to kapitler fra Kraftberedskapsforskriften (KBF) bli spesielt relevante: «Kapittel 6: Informasjonssikkerhet» og «Kapittel 7: Beskyttelse av driftskontrollsystem». Siden kravene i kapittel 6 allerede er tatt i betraktning i rapporten «Sikkerhetsveileder for kraftsensitiv informasjon i skytjenester» [6], utgitt av Forum for informasjonssikkerhet i kraftforsyningen (FSK) i 2021, vil vi kun gi en kort sammenfatting her. Hovedfokus i resten av denne seksjonen er derfor kapittel 7 i KBF, hvor vi vil gi en første vurdering om hvorvidt/hvordan kravene vil være mulige å etterleve ved bruk av skyløsninger for driftskontrollsystemer.

3.1.1 Kapittel 6: Informasjonssikkerhet

Dette kapittelet omhandler informasjonssikkerhet av *kraftsensitiv informasjon*. I veilederen fra FSK [6] pekes fem paragrafer ut som spesielt relevante ved bruk av skytjenester: § 6-1 og § 6-2 som begge går på inkludert identifikasjon av kraftsensitiv informasjon, § 6-3 som går på systemer og rutiner for beskyttelse, avskjerming og tilgangskontroll av informasjonen, § 6-5 som går på anskaffelser av leverandører som vil prosessere informasjonen, og § 6-9 som går på sikring av selve systemene som vil prosessere informasjonen. Sistnevnte, § 6-9, Digitale informasjonssystemer, er basert på NSMs grunnprinsipper for IKT-sikkerhet og ekstra relevant for bruk av skytjenester. Som diskutert i veiledningen fra FSK, inneholder denne paragrafen flere underpunkter med krav på rutiner og prosesser som må kontraktsfestes ved bruk av skytjenester, spesielt c) Sikre og oppdage, d) Håndtere og gjenopprette og f) Sikkerhetsrevisjon. Veilederen fra FSK gir konkrete anbefalinger om hva som bør inngå i en kravliste som kan benyttes ved anskaffelser av skytjenester.

Det er vår oppfatning at kravene til informasjonssikkerhet i paragrafene § 6-1 til § 6-9 i kapittel 6 av KBF vil være mulige å oppfylle ved bruk av skytjenester for klasse 1 og 2 driftskontrollsystemer, gitt at den presenterte kravlisten i FSK sin veiledning oppfylles. Kravlisten fra FSK gjør ingen forskjell på driftskontrollsystemer klasse 1 eller 2, hvilket er forventet ettersom den kraftsensitive informasjonen relatert til alle de tre klassene har den samme kritikaliteten iht. KBF. Kravlisten er lang og utfordrende å oppfylle, men det er ifølge FSK mulig å benytte skytjenester for kraftsensitiv informasjon og samtidig oppfylle lovverket hvis kravlisten oppfylles.

Paragraf § 6-10 i kapittel 6 av KBF går spesielt på beskyttelse av brytefunksjonalitet i AMS. Siden AMS ikke en del av NVE sin definisjon av «driftskontrollsystem» er ikke kravene i denne paragrafen relevante for vår analyse. Men det er verdt å merke seg at dette er den eneste paragrafen i kapittel 6 som etablerer et spesifikt krav til den geografiske lokasjonen til leverandører som gis tilgang til informasjon. Tilsvarende krav på geografisk lokasjon kommer tilbake i kapittel 7 (§ 7-14 Særskilte krav til driftskontrollsystemer i klasse 2, bokstav k. Krav til leverandører), men gjelder da kun leveranser til driftskontrollsystemer fra utenlandske leverandører, ikke selve lokasjonen av informasjonen eller tjenestene som leveres.

3.1.2 Kapittel 7: Beskyttelse av driftskontrollsystem

Dette kapittelet omhandler *sikring av driftskontrollsystemet*, slik at det fungerer og gir korrekt informasjon selv ved langvarige og ekstraordinære hendelser. Kravene til sikring og beredskap er avhengig av driftskontrollsystemets klasse. I Tabell 1 under gjennomgår vi alle paragrafene i dette kapittelet og gir vår vurdering om hvorvidt og hvordan kravene i disse paragrafene kan oppfylles ved bruk av skyløsninger.

Tabell 1: Relevante krav fra Kraftberedskapsforskriften - kapittel 7.

Kraftberedskaps-forskriften	Vår vurdering ved bruk av skytjenester
§ 7-1 Generell plikt til å beskytte drifts-kontrollsystemet	Hensikten med dette kravet er å beskytte driftskontrollsystemet mot alle typer uønskede hendelser. Vår vurdering er at dette kan oppfylles ved bruk av skytjenester, men vil kreve at tiltakene kontraktfestes. En interessant del av kravet er at det spesifiserer at eksterne leverandører (som ikke er KBO-enheter) ikke får lov å «utføre driftskontrollfunksjoner». En skyleverandør har kontroll over tjenestene i egen infrastruktur og kan i teorien utføre driftskontroll, så det blir viktig å se til at det er kontraktsfestet at de ikke får lov til å gjøre dette. Vi anser at denne delen av kravet vil da være tilfreds-stilt. Kravet omfatter både fysisk og logisk sikring. Den logiske sikringen krever ende-til-ende kryptering, som er uproblematisk å ved bruk av skyløsning. Vedrøren-de fysisk sikring må dette, igjen, avtales mellom skyleverandøren og nett-selskap, og som da vil være mulig å oppfylle i en skyløsning.
§ 7-2 Interne sikkerhetsregler	Uproblematisk - det er ikke noe med skyløsninger som påvirker nettselskapenes mulighet å oppfylle dette kravet.
§ 7-3 Dokumentasjon	Dette krever at virksomheter til enhver tid har oppdatert dokumentasjon av driftskontrollsystemet. Kravet dekker både det logiske og det fysiske datanettverket som brukes, samt alt utstyr som brukes i driftskontrollsystemet. Den logiske delen av dokumentasjonen er uproblematisk, men dokumentasjon over det fysiske nettverket er sannsynligvis ikke mulig å kreve ved bruk av skyløsninger, i alle fall ikke hvis man bruker en av de store, kommersielle løsningene. Dette er en mulig «showstopper» for bruk av skyløsninger.

Kraftberedskaps-forskriften	Vår vurdering ved bruk av skytjenester
§ 7-4 Kontroll med brukertilgang	Dette kravet går på tilgangskontrollen til driftskontrollsystemer. Kravet dekker både den fysiske og logiske tilgangen til systemet. Den logiske delen av kravet er stort sett uproblematisk, så lenge man passer på at tilgangskontrollen blir korrekt kontraktfestet med skyleverandøren. Men det er noen interessante aspekter. Den første omhandler restriksjonene for «eksterne leverandører». I veiledningen fra NVE sies det at «*eksterne leverandører får ikke lov til å på egenhånd, og uten kontroll fra virksomheten, administrere beskyttelsestiltakene for driftskontrollsystemet*». Det er vår oppfatning at i en skyløsning vil leverandørens driftspersonell kunne sees på som rettmessige brukere og må derfor kunne unntas fra denne delen av kravet når det gjelder sikkerhetstiltakene i sine plattformer som beskytter tjenestene. Samtidig må det avtales nøyaktig hva de får lov til å gjøre på egenhånd når det gjelder nettselskapene sine tjenester. Den andre omhandler individuell tilgang. NVE sin veiledning spesifiserer personlige brukertilgang. Det blir derfor viktig å forby bruk av gruppetilgang og/eller felles påloggingsinformasjon i avtalen med skyleverandøren. Den tredje omhandler kravet på at virksomhetene skal kontrollere hvilken bruker som er eller har vært pålogget driftskontrollsystemet. Tilgang til logger, og nøyaktig hva som skal loggføres, må derfor avtales spesielt med skyleverandøren. Den fysiske delen av kravet vil kreve at nettselskapene til dels har kontroll over hvem som har tilgang til datasentret, samt muligheten å revidere hvem som har hatt tilgang. Dette er sannsynligvis ikke mulig å kreve ved bruk av skyløsninger, i hvert fall ikke hvis man bruker en av de store kommersielle løsningene. Dette er en mulig «showstopper».
§ 7-5 Kontroll ved endringer i driftskontrollsystemet	Dette krever kontrollordninger for vurdering, testing og godkjenning av endringer i systemet. Kravet dekker både logiske og fysiske endringer. Deler av kravet er sannsynligvis mulig å etterleve ved bruk av en skyløsning, gitt at man klarer å avtale at alle endringer varsles til nettselskapene og at de får mulighet til å godkjenne dem før de trer i kraft. Samtidig kan kravet om å få utføre tester før endringen trer i kraft bli vanskelig i praksis. Rent konkret, hvis man har et SCADA system som kjører i Azure, og leverandøren (Microsoft) varsler om at de vil oppdatere Azure, vil det sannsynligvis ikke være mulig å teste at SCADA fortsatt virker før oppdateringen er blitt gjennomført. Men dette gjelder logiske endringer – den delen av kravet som går på fysiske endringer vil sannsynligvis ikke være mulig å oppfylle i en skyløsning. Selv om endringer vil bli vanskelig å få testet ut i praksis, er det vår erfaring at endringer generelt forårsaker mindre problem for funksjoner som kjører i skyløsninger enn i typiske «on-premises» løsninger. Fortsatt, slik KBF er formulert i dag, er dette en mulig «showstopper».

Kraftberedskaps-forskriften	Vår vurdering ved bruk av skytjenester
§ 7.6 Kontroll med utstyr i driftskontrollsystemet	Dette er et relativt bredt krav som tar for seg alt av utstyr som brukes i drifts-kontrollsystemet. Hensikten er å sørge for at det er et vanntett skille mellom OT/IT, gjennom krav på kontroll av tilgangen til OT-delen av systemet, kontroll av utstyret som brukes for å sikre tilgangen, samt kontroll av kommunikasjon-en med systemet. Det meste i dette kravet vil, på tilsvarende måte som tidligere krav i kapittel 7, være mulige å kontraktfeste med skyleverandøren. Dette inkluderer hindring av urettmessig tilgang til systemet og til utstyret som brukes for å beskytte systemet, og forbudet mot bruk av personlig utstyr i systemet. Kravet om trådbundet kommunikasjon i driftssentralen og datarommet er mulig å kontraktfeste, gitt at alle funksjonene i driftssentralen implementeres i det samme datasenteret. Den første delen av kravet som går på at «utstyr (…) ikke har blitt brukt (…) utenom driftskontrollsystemet», sammen med forbudet mot gjenbruk av utstyret til andre formål etterpå, vil bli vanskelige å oppfylle ved bruk av skyløsninger. Virtualisering og ressursdeling er en del av selve kjernekonseptet av «sky» og en gitt server i et datasenter vil normalt brukes til forskjellige formål. Selv om det er mulig å avtale at den fysiske serveren som kundens løsning kjører på skal kun brukes av kunden, vil denne delen av kravet ikke lenger kunne oppfylles hvis/når behovet for å migrere oppstår. Det å kreve å få bytte til ressurser som ikke er blitt brukt til noe annet formål tidligere, vil sannsynligvis være umulig. Hvis man skiller mellom logikk og fysikk, er det rent teoretisk relevant å ta i betraktning at på virtuelt maskinnivå vil det være en ren, blank versjon som starter opp, som ikke vil ha tilgang til den underliggende maskinvaren. Man kan da muligens argumentere at utstyret er «nytt» i den forstand at det ikke er mulighet for spredning av virus eller skadevare fra tidligere installasjoner, og at det videre ikke vil bli mulig å få tak i informasjon fra selve maskinvaren som har vært vert for driftskontrollen tidligere når tjenesten avsluttes. Slik KBF er formulert i dag, er denne delen av kravet en klar «showstopper».

Kraftberedskaps-forskriften	Vår vurdering ved bruk av skytjenester
§ 7-7 Håndtering av feil, sårbarheter og sikkerhetsbrudd	Dette er et relativt bredt krav med flere underpunkter med krav på rutiner og prosesser, hvorav de fleste må kontraktsfestes ved bruk av skytjenester. Sannsynligvis vil slike prosesser kunne håndteres bedre av en skyleverandør enn av mange av de mindre nettselskapene, siden de store tjenesteleverandørene vanligvis har bedre tilgang til «tilstrekkelig personell med nødvendig kompetanse». Skyleverandøren registrerer alle hendelser, men det må avtales spesielt hva som skal rapporteres videre. Nettselskapene må deretter selv ta ansvar for å varsle videre til beredskapsmyndigheten (KraftCERT). Håndteringen av feil og sårbarheter skal skje «uten unødig opphold». Siden dette kan tolkes på forskjellige måter, må det avtales prioriteter for forskjellige typer hendelser i avtalen med skyleverandøren. NVE sin veiledning til KBF anbefaler at virksomhetene har tilgang til et sikkerhetsoperasjonssenter (SOC), at KraftCERT gir råd i forbindelse med anskaffelsen av en slik tjeneste og påpeker at NSM har en godkjenningsordning for leverandører av sikkerhetstjenester. Hvis man tjenesteutsetter hele eller deler av driftskontrollsystemet til en skyleverandør, er det rimelig å anta at det må etableres en tilsvarende godkjenningsordning for skyleverandører, herunder hvordan skyleverandørene håndterer feil, sårbarheter og sikkerhetsbrudd.
§ 7-8 Beredskap ved svikt i driftskontroll-systemet	Dette kravet går i praksis på etableringen av en reservedriftssentral, slik illustrert i Figur 1 i kapittel 2.1 av denne rapporten. Det er vår vurdering at kravet er mulig å oppfylle ved en skyløsning, og at man i tillegg da kan få en mer robust løsning mhp. fortsatt driftskontroll ved svikt i deler av systemet. I kapittel 6 vil vi vise flere eksempler på løsninger hvor deler av driftskontroll-systemet er flyttet opp i skyen og forklare hvordan dette vil medføre økt tilgjengelighet og redundans i driften av strømnettet. Ved bruk av skyløsning må beredskapsplanen oppdateres for å reflektere hvordan skytjenestene vil håndteres og brukes ved svikt. Tiltakene for å sikre redundans må i tillegg avtales spesielt med skyleverandøren. Det blir for eksempel viktig å avtale geolokalisering og synkronisert back-up av reserve-løsninger, slik at en alvorlig hendelse (brann, oversvømmelser...) i datasenteret hvor tjenestene kjøres ikke vil påvirke hele driftskontrollsystemet. Små leverandører av skytjenester kan faktisk «forsvinne». Gitt at funksjonene i det skybaserte driftskontrollsystemet er såpass generisk implementert at de kan kjøres i et vilkårlig skysystem kan man i teorien tenke seg en «cold spare» ved en annen leverandør. Men det vil da bli en større forsinkelse hvis man trenger å ta den i bruk ved svikt i hovedsystemet. Teknisk sett er Docker *containers* et smart valg, da de vil være relativt enkelt å migrere til en annen leverandør. Det er dog vår oppfatning at det sannsynligvis ikke vil være nødvendig å ha redundans på leverandør-nivå for å møte dette kravet, men at det er viktigere at den leverandøren man velger er redundant internt, ved at leverandøren har flere datasentre på ulike fysiske lokasjoner, og kan tilby replikering mellom disse.

Kraftberedskaps-forskriften	Vår vurdering ved bruk av skytjenester
§ 7-9 Bemanning av driftssentral	Uproblematisk - det er ikke noe med skyløsninger som påvirker nettselskapenes mulighet å oppfylle dette kravet.
§ 7-10 Ekstern tilkobling til driftskontrollsystemet	Dette kravet dekker eksterne tilkoblinger til driftskontrollsystemet. Det er et interessant krav, fordi når funksjonene i driftskontrollsystemet flyttes til skyen vil alle tilkoblinger bli eksterne. Kravet vil da omfatte flere situasjoner enn de som er beskrevet i NVE sin veiledning til kraftberedskapsforskriften som nå kun dekker tilkoblinger fra brukere på hjemmekontor og fra brukere hos leverandører i dennes lokaler. Det er vår vurdering at kravet er mulig å oppfylle ved en skyløsning, men at det blir enda viktigere å etablere korrekt logisk tilgangskontroll. Nettselskapene må iverksette en mer omfattende tilgangskontroll for å sørge for at alle forskjellige typer av brukere er godkjent og har rette tilganger, oversikt over hvem som har tilgang, og sikre at det kun brukes unike innlogginger, ikke fellesbrukere. I prinsippet kan samme fremgangsmåte brukes for ansatte i nettselskapet som i dag brukes for tilkobling for eksterne.
§ 7-11 Systemredundans i driftskontrollsystemet	Dette kravet pålegger nettselskapene å vurdere behovet for redundans i drifts-kontrollsystemet, basert på en risikovurdering. Kravet er i utgangspunktet uproblematisk – det er ikke noe med skyløsninger som påvirker nettselskap-enes mulighet å oppfylle det, men risikovurderingen vil sannsynligvis få et mye større omfang ved bruk av skytjenester. Det fremstår for oss at kravet opprin-nelig er skrevet med tanke på fysiske feil i komponenter eller kabler, osv., men i en skyløsning vil det bli mer relevant å vurdere mulige logiske feil og angrep. Det er vår oppfatning at innføring av tiltak for økt redundans vil bli enklere i skytjenester – se vår vurdering av § 7-8 Beredskap ved svikt i driftskontroll-systemet.
§ 7-12 (Opphevet)	Opphevet – ikke vurdert.
§ 7-13 Beskyttelse mot elektromagnetisk puls og interferens	Dette kravet sier at nettselskapene må vurdere driftskontrollsystemets sårbarhet for elektromagnetisk puls (EMP) eller elektromagnetisk interferens (EMI). En slik vurdering vil ikke nettselskapene ha mulighet å gjennomføre på egen hånd ved bruk av skytjenester, men den må gjennomføres basert på informasjonen som kan fremskaffes fra skyleverandøren. I praksis vil resultatet bli avhengig av datasenteret som driftskontrollsystemet blir plassert i. Hvis datasenteret er sårbart for EMP/EMI kan noen (i teorien) enkelt slå ut drifts-kontrollsystemet. Skjermingstiltakene foreslått i NVE sin veiledning til kraftberedskapsforskriften vil ikke bli relevante ved bruk av skytjenester. Det er mer aktuelt med tiltak for økt redundans (slik beskrevet i vurderingen av § 7-8 Beredskap ved svik); slår man ut et datasenter, skal reserveløsningen finnes i et annet datasenter, på en annen geografisk lokasjon.

Kraftberedskaps-forskriften	Vår vurdering ved bruk av skytjenester
§ 7-14 Særskilte krav til driftskontroll-systemer i klasse 2: a) Sikkerhetskopier	Dette kravet er i utgangspunktet uproblematisk - det er ikke noe med sky-løsninger som påvirker nettselskapenes mulighet å oppfylle det. Merk at kravet ikke spesifiserer *hva* som må sikkerhetskopieres, og at det ved bruk av skyløsninger kan bli behov for sikkerhetskopiering av andre typer informasjon enn det kravet opprinnelig var ment å dekke.
§ 7-14 Særskilte krav til driftskontroll-systemer i klasse 2: b) Sikkerhetsrevisjon	Dette kravet vil bli en utfordring i en skyløsning, siden nettselskapene selv ikke vil få muligheten til å gå inn på datasenteret. Revisjonen vil da bestå av å gjennomgå en tredjepartsrapport som blir jevnlig produsert av et revisjonsfirma på oppdrag av skyleverandøren. For oss er det uklart om en slik rapport vil dekke dette kravet. Vi har derfor identifisert dette som en mulig «showstopper». I praksis vil nettselskapene bli avhengige av at revisjonsfirmaene, en tredjepart som de ikke har kontroll over, gjør jobben sin ordentlig og at rapporten dekker alle de pålagte beskyttelsesmekanismene.
§ 7-14 Særskilte krav til driftskontroll-systemer i klasse 2: c) Overvåkning og logging	Dette kravet er tilsynelatende uproblematisk – logging, overvåking og analyse inngår som standard i de aller fleste skyløsninger. Samtidig vil det kun være *skyløsningen* som overvåkes av skyleverandøren, noe som vil stille krav til nettselskapene selve å påse at både kommunikasjonsforbindelsene opp til skyen og det som skjer i de deler av driftskontrollsystemet som fortsatt er implementert lokalt logges og overvåkes. I tillegg vil det bli viktig å avtale spesielt om prosesser og tidsfrister for skyleverandøren sin varsling av relevante hendelser til nettselskapene, slik at de kan varsle videre til KraftCERT. Slik kravet er formulert nå vil det å overvåke, analyse og varsle om unormal datatrafikk blir spesielt vanskelig å imøtekomme, sannsynligvis en «show-stopper».
§ 7-14 Særskilte krav til driftskontroll-systemer i klasse 2: d) Utilgjengelig driftssentral	Dette kravet pålegger nettselskapene å kunne drifte systemet selv om driftssentralen blir utilgjengelig. I utgangspunktet er dette uproblematisk – se vår vurdering av § 7-8 Beredskap ved svikt i driftskontrollsystemet. I ytterste konsekvens dreier dette seg om behovet for å kunne utføre kontroll-funksjoner manuelt. Dersom man har et lokalt driftskontrollsystem med egen HMI, kan man fysisk dra til (f.eks.) transformatorstasjonen og bruke den lokale HMIen til å uføre kontrolloppgaver (f.eks. koble ut brytere). Man kan alter-nativt bruke kontrollpaneler med trykknapper på komponenter (IEDer). Siste instans kan være en fysisk knapp på bryteren. Denne siste utveien vil ikke påvirkes av om driftskontrollfunksjoner er plassert i skyen. Ved virtualisering av funksjoner (færre IEDer) og dermed mindre hardware, må antallet og funksjon av slike nødløsninger vurderes nøye.

Kraftberedskaps-forskriften	Vår vurdering ved bruk av skytjenester
§ 7-14 Særskilte krav til driftskontroll-systemer i klasse 2: **e) Bemanning**	Dette kravet er i utgangspunktet uproblematisk, men formuleringen om å «umiddelbart» oppdage og håndtere hendelser i driftskontrollsystemet vil være gjenstand for tolkning. Her må det gjøres en vurdering av hva som er godt nok og hva som sees som rimelig. På lik linje med § 7-7 Håndtering av feil, sårbarheter og sikkerhetsbrudd, må det avtales hva som skal varsles og hvor raskt. Mens det ofte er ønskelig å få varsel om hendelser raskt, kan man, hvis man avtaler altfor korte tidsfrister, risikere å kun få selve varselet uten av motparten har fått tid til å finne ut av hva det er (dvs. en større fare for at false-positives kommer igjennom). Det er i tillegg rom for tolkning av hva som dekkes av begrepet «ekstraordinære hendelser». En enkelt software-feil som rammer mange komponenter kan være en alvorlig hendelse sett fra nettselskapenes perspektiv, samtidig som dette typisk ikke betraktes som særlig alvorlig av skyleverandøren. Det må derfor avtales hva som defineres som «umiddelbart» og «ekstraordinært».

Kraftberedskaps-forskriften	Vår vurdering ved bruk av skytjenester
§ 7-14 Særskilte krav til driftskontroll-systemer i klasse 2: f) ekstern tilkobling	Dette kravet er et tilleggskrav til § 7-*10 Ekstern tilkobling til driftskontroll-systemet*, definert for klasse 2 driftskontrollsystemer. På lik linje med vår vurdering av § 7-10 anser vi at når funksjonene i driftskontrollsystemet flyttes til skyen vil alle tilkoblinger bli eksterne og dermed falle inn under dette kravet. Den første delen av kravet spesifiserer at driftssentralen skal være bemannet ved tilkobling fra leverandør. Her blir tolkningen av «bemannet» viktig. Mange vil trolig beholde en fysisk driftssentral, og muligens må det være en fysisk driftssentral for å oppfylle forskriften. Da forskriften er skrevet med tanke på at «alt er fysisk» vil nok digitalisering medføre behov for en oppdatering av forskriften. I dette tilfellet vil det ikke gi mye mening å tvinge nettselskapene å bemanne en lokal driftssentral når leverandører kobler opp seg mot funk-sjonene i skyen. Slik kravet er formulert i dag, kan det bli en «showstopper» for skyløsninger. En rimelig omformulering kunne være at leverandører ikke skal ha tilgang til driftskontrollsystemet med mindre ansatte fra nettselskapet er koblet opp og kan overvåke tilgangen. Kravet spesifiserer videre at nettselskapene må sørge for at ekstern tilkobling utføres fra et sted med tilstrekkelig sikre omgivelser, at tilkoblingen bare skal brukes når det er behov, at styring kun skal skje etter godkjennelse, osv. Ingenting av dette er noe hinder for bruk av skytjenester. Intensjonen med den første kravet er sannsynligvis at leverandører ikke skal ha mulighet å konfigurere driftskontrollsystemet uten overvåkning. I en fysisk driftssentral vil det da være naturlig å påse at det finnes ansatte på plass som observerer det som skjer. Det er et rimelig krav. Samtidig blir det blir stadig mindre meningsfullt med denne typen krav til fysisk tilstedeværelse når kraftnettet digitaliseres. Kanskje de deler av dette kravet, som ikke er helt uttalt, om å ha en fysisk driftssentral, kan fravikes for klasse 1 og 2 driftskontrollsystemer, eventuelt formuleres om slik at det legger bedre til rette for økt digitalisering.

Kraftberedskaps-forskriften	Vår vurdering ved bruk av skytjenester
§ 7-14 Særskilte krav til driftskontroll-systemer i klasse 2: g) Systemredundans	Dette kravet, som er et tilleggskrav til § 7-11, sier at samband i driftskontroll-systemet skal fungere uavhengig av funksjonssvikt i offentlige elektroniske kommunikasjonstjenester eller kommunikasjonsnett. Kravet spesifiserer videre at driftskontrollsystemet frem til anlegg i klasse 2 (og 3) skal være redundant frem til det lokale kontrollanlegget, og at redundante føringsveier og kompo-nenter i driftskontrollsystemet skal være fysisk adskilte og uavhengige. Dette gjelder altså helt ut til de fysiske enhetene, for eksempel fra kontrollrom og ut til vern, dvs. ikke bare internt i selve driftskontrollsentralen. Kravet er en utfordring, siden driftskontrollssystemet i skyen vil være avhengig av offentlige, elektroniske kommunikasjonstjenester eller kommunikasjonsnett. Hvis vi ser vekk fra sky og kun vurderer bruk av eksterne tjenester kan kravet møtes ved bruk av en dedikert kabel, eller fiber, som går ut til de eksterne tjenestene. I tillegg, siden det ikke er krav til trådbundet kommunikasjon, så kan den andre (redundante) forbindelsen settes opp som et privat 5G nett. Men det vil fortsatt være umulig å møte kravet hvis de eksterne tjenestene iverksettes i en offentlig sky, siden disse alltid vil kobles til via offentlige kommunikasjonsnett (som forklart i seksjon 2.2 er private skytjenester ikke aktuelt for analysen i denne rapporten). I NVE sin veiledning til KBF [2] spesifiseres det at NVE godtar at én sambands-vei i en redundant løsning går via offentlige elektroniske kommunikasjonsnett. Det betyr at man kan møte kravet gjennom for eksempel å bruke en vanlig offentlig linje ut av driftssentralen, og at man i tillegg har redundans gjennom en trådløs privat 5G løsning. Men dette vil ikke hjelpe skyløsninger å møte kravet, siden 5G forbindelsen ikke vil «rekke hele veien opp i skyen». Man kunne vurdere en endring av kravet til å gjelde at minst to uavhengige offentlige tilbydere skal brukes (per dags dato finnes det tre konkurrerende 5G operatører i Norge). Det er vår vurdering at dette kravet er en klar showstopper for klasse 2 driftskontrollsystemer i skyen. Vi anser i tillegg at kravet er uklart formulert og bør revideres. I dag er det ikke sett på som samfunnsøkonomisk og rasjonelt å sette opp dedikerte forbindelser over separat fiber. Det er i tillegg interessant at kravet sier at «redundante komponenter skal være fysisk adskilte». Dette betyr at det må brukes et separat datasenter for etablering av funksjoner i reserveløsninger. Dette må derfor avtales spesielt med skyleverandøren. Vi har dog ikke tatt med dette i oppsummeringen av hva som må avtales i seksjon 3.1.3, siden kravet som helhet uansett ikke er mulig å tilfredsstille, men det er selvfølgelig tatt med som «showstopper».

Kraftberedskaps-forskriften	Vår vurdering ved bruk av skytjenester
§ 7-14 Særskilte krav til driftskontroll-systemer i klasse 2: h) Særskilt om dublering	Dette kravet bygger videre på § 7-11 *Systemredundans i driftskontrollsystemet* gjennom å spesifisere at risikoen må kontrolleres når/om identiske teknologier og løsninger brukes i redundante løsninger. Bakgrunnen til dette kravet er sannsynligvis at man ønsker å unngå at flere fysiske komponenter feiler samtidig. Veiledningen til KBF fra NVE påpeker at dette også gjelder programvare, og gir spredning av skadevare til reservesystemet som et konkret eksempel. Dette er svært relevant ved bruk av skytjenester, og vil gjelde alle funksjoner som vurderes flyttes til skyen. For å tilfredsstille kravet må man bruke forskjellige skyteknologier, og sannsynligvis også forskjellige skyleverandører (fordi de vil tilby forskjellige plattformer). I teorien kan dette delvis oppfylles gjennom etablering av «Dockerized-løsninger», dvs. ferdigpakkede Docker images som kan kjøres både på for eksempel Azure og på Google Cloud. Men Docker er også en teknologi i seg selv, og bruken av Docker vil da bli en ny «single point of failure», som også burde dubleres. Vår vurdering er dog at det er noe rom for tolkning her, og at kravet ikke nødvendigvis må tolkes så strengt at det blir en showstopper. Merk at i vår vurdering av § 7-8 *Beredskap ved svikt i driftskontrollsystemet*, skrev vi at det sannsynligvis ikke er behov for redundans på leverandørnivå. Det utsagnet er ikke lenger gyldig hvis man skal møte dette kravet for klasse 2 driftskontrollsystemer.
§ 7-14 Særskilte krav til driftskontroll-systemer i klasse 2: i) Beskyttelse mot EMP og EMI	Dette kravet er en oppfølger til § 7-13 *Beskyttelse mot elektromagnetisk puls og interferens*, men går spesifikt på kommunikasjonen mellom driftssentral og de klasse 2 (og 3) anlegg som styres. Innføring av sikringstiltak vil bli vanskelig ved bruk av skyløsninger. De fleste (alle) av de foreslåtte tiltakene for beskyttelse i veiledningen til KBF er ikke mulige å benytte ved bruk av sky, og man må derfor satse på å møte kravet gjennom redundans i kommunikasjonen med skytjenestene, kombinert med økt beredskap for nedetid av skytjenestene. Vår vurdering er at dette er godt nok, da det påpekes spesifikt i veiledningen at beredskap er akseptabelt for sambandsvei til kraftforsyningsanlegg i klasse 2. Det bemerkes at deteksjon av slike hendelser må være en del av nettselskapet sin beredskapsplan, og at det må omfatte hele ende-til-ende kommunikasjonsforbindelsen mellom drifts-sentralen i skyen og lokale kontrollanlegg. Det er ikke noe som kan avtales med skyleverandøren, da den ikke kan ta ansvar for selve forbindelsen inn til tjenestene sine.

Kraftberedskaps-forskriften	Vår vurdering ved bruk av skytjenester
§ 7-14 Særskilte krav til driftskontroll-systemer i klasse 2: j) Sikker tidsreferanse	Kravet sier at driftskontrollsystem som er avhengig av eksakt tidsreferanse, skal ha sikre kilder for tidsangivelse. Veiledningen til KBF gir eksempel på behovet av nøyaktighet, basert på bruken av informasjon. I ECoDiS prosjektet[6] var sikker tidsreferanse et viktig tema. Digitalisering medfører høyere krav til tid og det bli viktig å ha tilgang til eksakte tidsangivelser. Det vil oppstå problemer hvis (når) man detekterer at det er feil i tidsangivelser. Konklusjonen fra prosjektet var at dette er en vanskelig problemstilling, og at en løsning kan være at «noen» tar rollen som «tidsleverandør». Det trenger nødvendigvis ikke være *rett* tid som leveres, men det må være *samme* tid som brukes av de forskjellige funksjonene. Sikker tidsreferanse vil sannsynligvis bli et enda større problem ved bruk av skytjenester. Det er p.t. uklart for oss om dagens skyleverandører har mulighet å operere med eksakte tidsreferanser.
§ 7-14 Særskilte krav til driftskontroll-systemer i klasse 2: k) Krav til leverandører	Kravet sier at det er kun norske, eller utenlandske leverandører fra land som er medlem i EFTA, EU eller NATO, som får lov til å levere driftskontrollsystemer av klasse 2 til nettselskapene. Det er spesifisert i NVE sin veiledning til KBF at kravet kun gjelder komplette leveranser av driftskontrollsystem. Dette vil stille et tilsvarende krav på skyleverandøren sitt land, gitt at hele driftskontrollsystemet flyttes ut i skyen. For SaaS løsninger vil dette bli spesielt relevant å følge opp, fordi de ofte implementeres i en infrastruktur (IaaS) fra en annen skyleverandør, som da også må oppfylle kravet. Ellers er vår vurdering at dette ikke er en showstopper for bruk av sky.
§ 7-16 Vern av kraftsystem i regional- og transmisjonsnett	Uproblematisk - det er ikke noe med skyløsninger som påvirker nettselskapenes mulighet å oppfylle dette kravet.
§ 7-17 Mobile radionett- driftsradio	Uproblematisk - det er ikke noe med skyløsninger som påvirker nettselskapenes mulighet å oppfylle dette kravet.

[6] ECoDiS - Engineering and Condition monitoring in Digital Substations
https://www.sintef.no/en/projects/2019/ecodis/

3.1.3 Oppsummering av kravene

Vår gjennomgang av kravene fra Kraftberedskapsforskriften kapittel 7 kan oppsummeres slik:

Følgende må avtales spesielt med skyleverandøren:

- Logiske sikkerhetstiltak i infrastrukturen som skytjenesten kjører i (§ 7-1).
- Fysisk sikring av datasenteret/ de datasentrene som skytjenestene kjører i (§ 7-1).
- Skyleverandøren har ikke lov å utføre operasjoner som er forbeholdt nettselskapene (f.eks. bruk av bryterfunksjon) (§ 7-1).
- Tilgang til komplett, oppdatert dokumentasjon over skytjenestene og den underliggende infrastrukturen (§ 7-3)
- Skyleverandøren må bruke personlige brukere ved administrasjon av tjenestene (§ 7-4).
- Det må spesifiseres hva skyleverandøren har mulighet å gjøre på egen hånd i systemet (§ 7-4).
- Tilgang til logger og spesifikasjon over hva som skal logges (§ 7-4).
- Skyleverandøren må varsle alle endringer i systemet og la kunden godkjenne dem (§ 7-5).
- Krav om nytt utstyr og forbud mot gjenbruk av utstyr (§ 7-6).
- Krav om trådbundet kommunikasjon mellom de tjenester som inngår i driftssentralen (§ 7-6).
- Håndteringen av feil, sårbarheter og sikkerhetsbrudd (§ 7-7).
- «Ekte» redundans i form av spredt geolokalisering og synkronisert back-up av tjenester (§ 7-8).
- Hva skal regnes som «umiddelbart» når det gjelder å oppdage og håndtere hendelser (§ 7-14: e)
- Bruk av forskjellig skyteknologier, og sannsynligvis også forskjellige skyleverandører, ved implementering av reserveløsninger (§ 7-14: h).

Vi har identifisert følgende som mulige «showstoppers» for bruk av skyløsninger for klasse 1 og 2 drifts-kontrollsystemer:

- Kravet om komplett dokumentasjon av de fysiske komponentene i systemet (§ 7-3).
- Kravet om å ha kontroll over hvem som har, og har hatt, fysisk tilgang til systemet (§ 7-4).
- Kravet om å teste alle endringer før de trer i kraft (og da spesielt fysiske endringer) (§ 7-5).
- Kravet om bruk av nytt utstyr og forbud mot gjenbruk av utstyr (§ 7-6).

I tillegg, for klasse 2 driftskontrollsystemer, har vi følgende mulige showstoppers:

- Kravet om sikkerhetsrevisjon (§ 7-14: b)
- Kravet om å overvåke all datatrafikk i nettverket (§ 7-14: c)
- Kravet om fysisk tilstedeværelse i driftssentral ved ekstern tilkobling (§ 7-14: f)
- Kravet om etablering av redundant føringsvei som ikke bruker offentlige nettverk (§ 7-14: g)
- Kravet om eksakte tidsangivelser (§ 7-14: j)

Følgende har vi identifisert som forbedringspotensial av lovverket:

- Definisjonen av «eksterne leverandører» (§ 7-4).
- Bedre (mer oppdatert) skille mellom fysiske og logiske sikkerhetsmekanismer.
- Akseptere alternative måter til fysiske sikkerhetstiltak, f.eks. virtualisering og/eller redundans.
- Utvid forklaringen av «ekstern tilkobling» (§ 7-4) til å også dekke egne ansatte på jobb.
- Eksplisitt angi at tredjepartsrevisjoner er akseptabelt ved sikkerhetsrevisjon (§ 7-14: b).
- Akseptere alternative måter til «bemanning» av driftssentralen ved tilkobling fra leverandør (§ 7-14: f)
- Akseptere redundante føringsveier over offentlige nett, eventuelt i kombinasjon med styrket krav på redundans (§ 7-14: g).

En observasjon fra gjennomgangen av kravene i KBF er at det framstår som at det er behovet for beskyttelse av fysiske komponenter som ligger bak de fleste av formuleringene i forskriften. Dette gjør det utfordrende å vurdere kravene i en kontekst hvor funksjoner er virtualiserte og befinner seg på en annen plass enn i den fysiske driftssentralen. Dette går utover vurderingen av skytjenester: det er vår oppfatning at ved digitalisering av kraftsystemer generelt vil mange av kravene rundt fysisk sikring bli irrelevante eller vanskelige å tilfredsstille.

En annen viktig observasjon fra gjennomgangen av kapittel 7 er at det ikke finnes noe krav om geografisk lokasjon av driftskontrollsystemet. Dette er som forventet, da forskriften er skrevet for dagens situasjon, men ved bruk av skytjenester er dette et viktig aspekt som bør tas med i vurderingen. I praksis er det sannsynlig at eksisterende krav til responstid (millisekunder) vil forutsette at skyløsningen fysisk befinner seg i Norge.

3.2 Andre lovverk og standarder

3.2.1 EU-direktivet NIS 2

EU direktivet NIS 2 [8] har som mål å opprettholde et høyt sikkerhetsnivå i nettverks- og informasjonssystemer på tvers av landene i Europa. De nye reglene stiller krav til sikkerheten i virksomheter i utvalgte sektorer med over 50 ansatte og en årlig omsetning/balanse på minst €10 millioner. Direktivet skal være implementert i nasjonal rett i EU-landene i oktober 2024 og vil dekke flere sektorer enn det opprinnelige direktivet («NIS-1»). Samfunnsviktige tjenestetilbydere innen energibransjen er allerede omfattet av kravene i NIS 1. Det samme gjelder digitale tjenestetilbydere, hvor tilbydere av skytjenester er inkludert.

Et EØS-notat utstedt i 2023[7] sammenfatter endringene i NIS 2. Notatet peker ut styrking av sikkerhetskravene fra NIS-1 som den viktigste endringen. Direktivet krever nå at tilbydere må iverksette hensiktsmessige og proporsjonale tekniske og organisatoriske tiltak for å håndtere risiko i nettverk og informasjonssystemer. Det oppstilles en risikostyringsmetode med en minimumsliste over grunnleggende sikkerhetselementer som må legges til grunn for sikkerhetsarbeidet, blant annet krav om at tilbydere håndterer cybersikkerhetsrisiko i forsyningskjeder og hos leverandører, planer for vedlikehold, overvåkning og testing samt bruk av krypto. Direktivet innfører også mer presise bestemmelser om prosessen for varsling av hendelser, hva det skal varsles om og når. I tillegg vil NIS 2 direktivet komme med nye krav på leverandørkjedesikkerhet og styrkede krav til beredskapsplaner.

Vår oppfattelse er at NIS 2 ikke vil forhindre bruk av skyløsninger i driftskontrollsystemer, men at de skjerpede kravene om varsling av hendelser, beredskapsplaner og leverandørkjedesikkerhet vil medføre strengere krav til de avtaler som nettselskapene må inngå med skyleverandørene. Samtidig er skyleverandørene selv omfattet av kravene i NIS 2, og det er all grunn til å tro at disse vil legge til rette for at både nye og eksisterende kunder kan bruke deres tjenester også etter at direktivet er innført[8].

3.2.2 IEC 62443

IEC 62443 [9] beskriver grunnleggende krav for å håndtere, minimere og/eller forhindre sikkerhetsrisikoer for komponentprodusenter, systemintegratorer og driftsansvarlige i industriell cybersikkerhet. Det er en «horisontal» standard som kan brukes i alle kritiske infrastrukturer, inkludert energi. Hensikten med standarden er å innlemme OT-systemer i cybersikkerhetsarbeidet. Dette gjøres gjennom å etablere et effektivt sikkerhetssystem som dekker hele verdikjeden, inkludert produsenter, installatører og operatører

[7] https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2021/feb/nis2-direktivet/id2846097/
[8] https://cloud.google.com/blog/products/identity-security/how-google-cloud-is-preparing-for-nis2-and-protecting-europe-from-cyber-threats

av prosesskontrollsystemer. På lik linje med andre sikkerhetsstandarder, for eksempel ISO/IEC 27005 [11], krever standarden en systematisk tilnærming av sikkerhetsarbeidet som inkluderer risikovurdering, etablering av sikkerhetspolitikker, og opplæring av ansatte. En fundamental del av IEC 62443, som er tatt i betraktning ved utarbeidelse av referansearkitekturen i denne rapporten, er oppdelingen av systemet som skal vurderes i forskjellige soner («zones») som kobles sammen på en sikker og kontrollert måte ved hjelp av kanaler («conduits»). Hensikten er å sikre kommunikasjonskanalene mellom de forskjellige deler av systemet, begrense tilgangen til systemet og minimere angrepsflaten til systemet.

The International Electrotechnical Commission (IEC) skriver i sitt nyhetsbrev *e-tech* at energisektoren bruker IEC 62443 standarden for å kontrollere cyberrisiko i bl.a. er distribusjonsnett, vannkraftanlegg og en rekke energilagringssystemer[9]. NVE sin veiledning til kraftberedskapsforskriften referer også til denne standarden som en del av forklaringen til den generelle plikten om å beskytte driftskontrollsystemet (§ 7-1).

3.2.3 IEC 62351

IEC 62351 [10] beskriver krav for sikker kommunikasjon ved bruk av IEC TC 57 protokollene, som går på informasjonsutveksling i kraftsystemer, inkludert driftskontrollsystemer/SCADA. Denne standarden er sett på som en viktig del i den pågående digitaliseringen av det norske kraftsystemet. Standarden muliggjør kryptering og integritetskontroll under overføring av data, og autentisering av endepunktene. For eksempel blir det mulig å autentisere kommunikasjonen mellom brukergrensesnitt (HMI) og SCADA, slik at SCADA ikke aksepterer kommandoer fra ondsinnet kode i operatørstasjonen. Det brukes vanligvis egen maskinvare for krypteringsfunksjonaliteten, slik at den ikke skal påvirke sanntidsegenskaper. I en rapport fra 2020 oppgir DNV-GL at det har begynt å komme flere typer industrielle komponenter innen kraftindustrien som støtter denne standarden [12]. Den samme rapporten beskriver utviklingen av kommunikasjon med vern som et konkret eksempel: «*De første digitale vern kommuniserte på lokalnett med proprietære protokoller, mens IEC 61850 standarden muliggjør i dag samtrafikk mellom vern fra forskjellige leverandører. Noen moderne vern støtter IEC 62351 standarden som bl.a. spesifiserer sikkerhetsprotokoller for bruk over IEC 61850*». En artikkel publisert nå i oktober 2024 viser at komponenter som er sertifisert i henhold til IEC 62351-3 har nå også begynt å komme på markedet[10].

IEC 62351 består av flere deler. Den tredje delen av standarden, IEC 62351-3, er spesielt relevant, da den spesifiserer hvordan TLS brukes for å sikre TCP/IP basert kommunikasjon mellom kontrollerende enheter og de enheter som kontrolleres. Dette er mulig å bruke for de forbindelser som er satt opp ved hjelp av IP-baserte protokoller, inkludert IEC 60870-5-104, DNP3/IEEE 1815 over LAN/WAN and MODBUS TCP/IP. Den siste delen, IEC/TR 62351-10 som er en teknisk rapport, er også relevant, da den inneholder en veiledende arkitektur for sikker utveksling av informasjon i kraftsystemer. Rapporten gir en oversikt over sikkerhetskravene til de forskjellige typer informasjon som brukes i driftskontrollsystemer og sammenligner disse med tilsvarende krav i vanlige IT/kontor systemer.

3.3 Retningslinjer for god praksis

I tillegg til etablerte standarder og lovverk, er **Purdue-modellen** [13] relevant for denne rapporten. Det er en veletablert arkitektur som organiserer industrielle kontrollsystemer i seks forskjellige hierarkiske nivåer. Nivåene strekker seg fra nivå 0 (prosess) opp til nivå 5 (*business enterprise* nettverk, koblet til internett). Hensikten med Purdue-modellen er å ivareta en tydelig arbeidsdeling i systemet, og dermed minimere risikoen for uautorisert tilgang og lateral bevegelse av trusler i systemet (lateral bevegelse er en teknikk cyberkriminelle benytter seg av for å bevege seg i et kompromittert nettverk). Purdue-modellen har flere

[9] https://etech.iec.ch/issue/2020-04/iec-62443-standards-a-cornerstone-of-industrial-cyber-security
[10] https://www.amnytt.no/plcnext-control-for-sikker-kommunikasjon-sertifisert-i-henhold-til-iec-61850-ed-2-1-og-iec-62351-3.6691535-304919.html

fellestrekk med sonemodellen i IEC 62443, men mens Purdue fokuserer på hierarki og er relativt streng med hvilken funksjonalitet og hvilke komponenter som hører hjemme på hvilket nivå, er sonemodellen i IEC 62443 mer fleksibel i definisjonen av kringvern («security perimeters») som isteden baseres på de unike sikkerhetskravene for hver sone. Vi har brukt Purdue-modellen i vår referansearkitektur i kapittel 6.

Det finnes også god praksis for sikkerhet i skytjenester fra Cloud Security Alliance[11] som med fordel kan vurderes hvis man skal migrere til skyen.

[11] https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4

4 Litteraturstudie

Litteraturstudien som ble gjennomført omfattet både akademisk artikler publisert i fagfellevurderte konferanser og tidsskrift, samt «grålitteratur» fra for eksempel bransjeorganisasjoner, offentlige instanser, forskningsinstitutt og konsulentselskap. Hovedfokus i studien var å finne litteratur som beskriver bruk av skyløsninger i OT/ICS for kommersielle fabrikker, prosessindustri, og kritisk infrastruktur utenfor kraftsektoren, og bruk av skyløsninger i OT/ICS i kraftsektoren utenfor Norge. I tillegg har vi vurdert og tatt i bruk noe litteratur som beskriver sikkerhetsutfordringer i skyløsninger generelt.

4.1 Akademisk litteratur

For å finne relevant akademisk litteratur brukte vi en forenklet utgave av retningslinjene for systematisk litteraturanalyse [14]. Først definerte vi kriterier for vurdering. Deretter bestemte vi hvilke databaser som skal gjennomsøkes og deretter formulerte vi en passende søkestreng. De resulterende artiklene ble deretter først vurdert basert på tittel, deretter på sammendrag, og til slutt på hele artikkelen.

I søket etter fagfellevurdert litteratur baserte vi oss på databasene Scopus[12], IEEE Explore[13] og ACM Digital Library[14]. I disse databasene søkte vi etter følgende ordkombinasjon i enten tittel eller sammendrag eller nøkkelord:

((cloud OR edge OR fog) **AND**
(factory OR production OR "smart grid" OR "power grid" OR utility OR industry OR maritime OR ship OR vessel OR chemical OR oil OR gas OR food OR beverage OR wastewater OR railway OR automotive) **AND**
(ics OR "industrial control system*" OR iacs OR "industrial automation and control system*" OR ot OR "Operations Technology" OR scada OR "supervisory control and data acquisition") **AND**
("use case" OR "case study"))

Søket ble begrenset til tidsrommet 2018 – 2024, og ble gjennomført i september 2024. I hvert av stegene ble artiklene vurdert opp mot følgende kriterier:

- Artikkelen beskriver et eller flere case, og casene er godt beskrevet og har et visst nivå av realisme (eks. inkluderer industrielt utstyr).
- Artikkelen omhandler både industrielle kontrollsystem og skyløsninger, og kontrollsystemet er tilkoblet sky.
- Artikkelen knyttes til en industri eller bransje hvor industrielle kontrollsystem er relevant (eks. prosessindustri eller strømnettet).

Dersom det ikke virket som om en artikkel ville være relevant på bakgrunn av feltene som ble vurdert i de ulike stegene ble artikkelen ekskludert. I tilfeller hvor det virket usikkert ble artikkelen tatt med i neste steg. Dette er illustrert i Figur 2.

[12] https://www.scopus.com/search/form.uri?display=basic#basic
[13] https://ieeexplore.ieee.org/Xplore/home.jsp
[14] https://dl.acm.org/

Figur 2: Søkestrategi i prosjektet.

Som vist i Figur 2 resulterte søket i 51 artikler, etter at duplikater var fjernet. Alle artiklene, med unntak av én, var indeksert i Scopus databasen. Etter å ha vurdert tittel og deretter sammendrag, ble 31 artikler ekskludert. Av de gjenværende 20 lyktes det ikke å fremskaffe teksten til tre av dem, mens ytterligere 11 ble vurdert som relevante, men mindre egnet for å beskrive caser. De gjenværende seks artiklene ble brukt for å utarbeide case-beskrivelsene som er presentert i kapittel 5 av denne rapporten. Vedlegg A inneholder en oversikt over de 20 artiklene som ble vurdert som relevante, hvor de seks artiklene som ble brukt i case-beskrivelsene er spesielt fremhevet.

På temaet **bruk av skyløsninger i OT/ICS for kommersielle fabrikker** framstod to artikler som spesielt relevante. Kučera et al. [15] beskriver tre caser innenfor produksjon, utviklet med utdanningsunderlag som formål. Casene er basert på et virtuelt produksjonsmiljø, virtuelle PLSer, Node-RED som middleware og Azure som skyløsning, med funksjonalitet for å samle data og å gripe inn i (den virtuelle) produksjons-prosessen. Fortoul-Diaz et al. [16] setter opp en testbed hvor en robotarm plukker biter fra et transport-bånd og bygger en brukerbestemt figur. En maskinlæringsmodell i Google Cloud Platform avgjør om bitene som leveres langs transportbåndet er tilstrekkelige for å fullføre figuren eller ikke, og underretter robot-armen om dette. Foruten disse to artiklene fant vi få gode eksempler fra produksjon og kommersielle fabrikker. Det virker derimot som om bruk av skyløsninger i produksjon er et aktuelt tema, Liu et al. [17] hevder for eksempel at det har blitt publisert mer enn 800 artikler innenfor tema «Cloud Manufacturing».

På temaet **bruk av skyløsninger i prosessindustri** framstod en artikkel omhandler bruk av skyløsninger og droner ved sementproduksjon skrevet av Salhaoui et al. i 2019 [24] som spesielt relevant. Det er en godt beskrevet case som valideres i et faktisk produksjonsmiljø.

På temaet **bruk av skyløsninger i OT/ICS i annen kritisk infrastruktur utenfor kraftsektoren**, fant vi ikke noen akademiske artikler i vårt søk som beskrev gode caser, unntatt de vi allerede har presentert. Vi har derfor valgt å ta med et eksempel på *skykontroll av jernbane* fra grålitteraturen i seksjon 4.2 som et interessant og relevant eksempel i denne kategorien.

På temaet **bruk av skyløsninger i OT/ICS fra kraftsektoren utenfor Norge** framstod en artikkel fra Khan et al. [18] som relevant. Forfatterne foreslår å bruke en gateway til å koble industrielt utstyr opp mot skyen, og demonstrerer denne tilnærmingen på PMU-er i et microgrid case. PMU-ene kobles opp mot AWS, hvor PDC og kontrollerer for microgrid kjøres på virtuelle maskiner. Case-beskrivelsen kompletteres med en artikkel publisert av Jelacic i 2020 [19] som beskriver en metode for risikovurdering av smartgrid OT tjenester til skyen og en artikkel publisert av Chehida et al. nå i 2024 [20] som gir et konkret eksempel på virtualiseringstrenden som allerede foregår i bransjen i dag.

4.2 Grålitteratur

Grålitteratur er ofte ikke indeksert i databaser på samme måte som akademisk litteratur, og vi har derfor ikke brukt samme fremgangsmåte som for akademisk litteratur. I stedet har vi tatt utgangspunkt i et sett med kjente aktører og publikasjoner og supplert dette med internettsøk. Vi har i tillegg sjekket litteraturlistene til de artiklene og rapportene som vi har funnet. En oversikt over grålitteraturen vi har vurdert finnes i Tabell 2.

Tabell 2: Oversikt over vurdert grålitteratur

Dokument	Vurdering
Sikkerhetsveileder for kraftsensitiv informasjon i skytjenester (utgitt av FSK – Forum for informasjonssikkerhet i kraftforsyningen) [21]	Veilederen beskriver godt utfordringer med forretningsmodellen til leverandører av skytjenester og oppfyllelse av krav i Energiloven og Kraftberedskapsforskriften knyttet til blant annet signering av taushetserklæringer, sikkerhetstesting og beredskap. Veilederen begrenser seg til skytjenester som behandler kraftsensitiv informasjon og problematiserer ikke eksponering av andre informasjonstyper mot skyen. Dette betyr at kun de kravene i energilovgivningen som regulerer behandlingen av kraftsensitiv informasjon diskuteres. Et interessant poeng i rapporten er at forfatterne påpeker at ved tjenesteutsetting må det tas hensyn til at det i ekstraordinære situasjoner må være mulig å utføre all drift fra norsk territorium, og at det må finnes planer og løsninger som ivaretar dette dersom tjenestene som settes ut i skytjeneste er nødvendig for drift. Dette inkluderer også de støttesystem som er nødvendige for drift over tid.
Navigating NERC CIP compliance in the cloud (utgitt av Microsoft)[15]	NERC CIP er North American Electric Reliability Corporation's Critical Infrastructure Protection, og fra januar 2024 tillates det å lagre "medium and high impact bulk cyber system information (BCSI)» i skyen, gitt at visse kriterier er oppfylt. Dette har ikke vært tillatt tidligere.
IKT-sikkerhet og uavhengighet utgitt av SINTEF Digital på oppdrag fra Petroleumstilsynet (nå Havtil) [22]	Rapporten omhandler primært hvordan uavhengighetskrav til trygghetssystemer utfordres av nye IKT-baserte løsninger som tas i bruk på sokkelen. En av problemstillingene er hvordan konsepter fra Industri 4.0 påvirker uavhengighet. Her er Namur Open Architecture nevnt som en løsning som muliggjør utveksling av informasjon mellom prosesskontrollanlegg og såkalte «monitorerings- og optimaliserings-soner» (M+O). Det er ikke angitt eksplisitt, men nøyere studier avdekker at deler av M+O typisk vil havne i skyen i mange tilfeller.

[15] Microsoft: Navigating NERC CIP compliance in the cloud, 2024 https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-product-and-services/industry/pdf/Microsoft-P-U-NERC-CIP-compliance-2024.pdf

Dokument	Vurdering
Datakvalitet ved digitalisering i petroleumssektoren utgitt av SINTEF Digital på oppdrag fra Petroleumstilsynet (nå Havtil) [23]	Formålet med 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. Skyløsninger blir diskutert blant annet i forbindelse med analyse av data og rask kommunikasjon med trådløse håndholdte/felt enheter. Denne utfordringen er formulert i rapporten: *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.* Anbefaling fra rapporten til Havtil: *Forsterke tilsyn med operatørers kvalitetssikring av IT-leverandører og krav til dataflyt fra skyen ned til OT-systemer (påseplikt).* Dette er relevante problemstillinger fra petroleumssektoren.
Premisser for digitalisering og integrasjon IT-OT utgitt av SINTEF Digital på oppdrag fra Ptil (nå Havtil) [24]	En av målsetningene for rapporten er å vurdere konsekvensen ved økt digitalisering i OT-systemer, og da særlig bruk av skytjenester. Rapporten fokuserer spesielt på samling av store mengder data fra prosesskontrollsystemer ved hjelp av bl.a. distribuerte sensorer, og overføring av disse dataene til skybaserte analysesystemer, hvorpå resultater (f.eks. optimaliseringsbeslutninger) sendes tilbake til prosesskontrollsystemene. Rapporten dokumenterer ikke at de skybaserte løsningene er planlagt slik at de skal kontrollere prosesskontrollsystemene direkte (snarere at operatører får informasjonen på annet vis, og gjør manuelle kontrolloperasjoner), men mange av de nye aktørene som er intervjuet signalerer at dette er noe de kunne sett fordelen av. Rapporten påpeker også at det er en forskjell mellom petroleumsbransjen og kraftbransjen (HMS versus leveransesikkerhet), og at i sistnevnte er det lettere å gå til sikker tilstand.
NE 175 *NAMUR Open Architecture - NOA Concept*. Utgitt av NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V., juli 2020	Introduserer M+O (Monitoring and Optimization) konseptet, som dreier seg om å a) overføre sensorinformasjon fra prosesskontrollnettverket til et eksternt M+O-system, og b) introdusere ytterligere sensorer som ikke er direkte en del av prosesskontrollsystemet, og følgelig ikke har så stringente sikkerhetskrav. Rapporten beskriver både en lokal M+O, og en sentralisert M+O som kan aggregere data fra flere lokale anlegg. Ettersom M+O ligger utenfor prosesskontrollsystemet, legges det opp til at det også kan implementeres som en skytjeneste.
Good practices for security of Internet of things in the context of smart manufacturing utgitt av ENISA (European Union Agency for Network and Information Security – nå European Union Agency for Cybersecurity) [25]	Rapporten inneholder et høynivå referansemodell basert på Purdue og lister opp mange trusler og mottiltak. Rapporten er opptatt av skytjenester og tilhørende trusler ved bruk av slike tjenester.

Dokument	Vurdering
Towards secure convergence of Cloud and IoT utgitt av ENISA (European Union Agency for Network and Information Security – nå European Union Agency for Cybersecurity) [26]	Rapporten gir oversikt over sikkerhetsproblemer for IoT-utviklere og IoT-integratorer som bruker skyløsninger.
BES Operations in the Cloud utgitt av NERC[16]	Dette white paperet er veldig relevant og tar for seg bulk energy system (BES) og potensiell bruk av sky, samtidig som man har krav på høy sikkerhet og pålitelighet.
Informasjonssikkerhet og sky-baserte tjenester for vannbransjen (238-2018) utgitt av Norsk Vann [5]	Rapporten inneholder en egen sjekkliste som kan brukes av vann- og avløpsvirksomheter som ønsker å bruke skytjenester i forbindelse med drift av sin infrastruktur. Det er viktig for bransjen å beskytte både abonnentene (persondata) og selve infrastrukturen. Mye av innholdet er relevant i dag, men ettersom det er gått 6 år vil det være nødvendig å lese rapporten med et kritisk blikk.
Sett krav til IKT-sikkerhet i anbud og kontrakter utgitt av NVE, skrevet av SINTEF [27]	Rapporten går gjennom tidligere NVE-rapporter og akademisk litteratur for å finne anbefalinger til sikkerhetsrelevante krav som nettselskap kan stille til sine leverandører. Det er få anbefalinger som går direkte på skytjenester, men vi kan trekke fram relevante betraktninger rundt geografisk plassering av servere og personell, eierskap til data, og separasjon mellom kunder.
Experiences and recommendation from the ECoDiS-project utgitt av Statnett med mange forfattere, blant annet SINTEF Energi og NVE [28]	Denne rapporten gir erfaringer og anbefalinger fra et forskningsprosjekt om digital transformatorstasjon. En transformatorstasjon er en viktig del av kraftsystemet og digitalisering av disse har mange fordeler og ulemper. Kapittel 4.10 om tilstandsovervåkning av primærkomponenter inneholder en figur (Figur 17) som viser et eksempel på hvordan data kan samles inn og sendes videre vha. ulike protokoller og nettverk. Dette er en av flere alternativer, men illustrerer utfordring med digitalisering, kommunikasjonsløsninger og behov for å skille data for drift og mer «uviktig» informasjon til overvåkning. Skyløsninger er også vist i figuren, men da helt på siden av driftskontrollsystemet, om en mulighet for dataanalyse for andre formål enn drift.
Train2Cloud. Whitepaper utgitt av Siemens Mobility [17]	White paperet beskriver en teknisk løsning for å plassere kontrollfunksjoner til et Communications-Based Train Control system i en skyløsning. Artikkelen ligger til grunn for caset «Skykontroll av jernbane» presentert i kapittel 5.3 av denne rapporten.

[16] NERC; BES operations in the cloud: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/SITES_WhitePaper_BES_Ops_in_Cloud.pdf , 2023

[17] https://www.mobility.siemens.com/global/en/portfolio/digital-solutions-software/infrastructure/infrastructure-in-the-cloud/train2cloud.html

Dokument	Vurdering
NCS3 - Molntjänster inom industriella informations- och styrsystem - En översikt av säkerhetsaspekter. Rapport utgitt av svenske Totalförsvarets Forskningsinstitut (FOI). [7]	Studien kartlegger sikkerhetsaspekter som vil bli relevante ved bruk av skytjenester for industrielle kontrollsystemer. Betraktningene i denne studien er svært relevante for sikkerhetsanalysen i vår rapport og har blitt tatt med i listen av utfordringer presentert i kapittel 2.3 av denne rapporten.

5 Bruk av skybaserte tjenester for driftskontroll i andre sammenhenger

Dette kapittelet presenterer eksempler på bruk av skyløsninger i fire forskjellige caser.

5.1 Case: Skykontroll av produksjonsprosess

Det utvalgte caset på temaet kommersielle fabrikker er **kontroll av produksjonsprosesser**. Vi bruker to forskjellige artikler for å beskrive caset.

Artikkelen «*Educational Case Studies for Pilot Engineer 4.0 Programme: Monitoring and Control of Discrete-Event Systems Using OPC UA and Cloud Applications*» skrevet av Kučera m.fl i 2022 [15] omhandler digitalisering av kontroll av diskrete systemer, som er typisk brukt i produksjonsprosesser. Forfatterne presenterer to eksempler på bruk av skyløsninger, som inkluderer forskjellige applikasjonssystemer, mellomvare og protokoller, og som alle er basert på et fiktivt produksjonsmiljø satt opp i Factory IO. Teknologier som benyttes er OpenPLC/Codesys, utviklingsverktøyet Node-RED, kommunikasjonsstandarden OPC Unified Architecture (OPC UA), og to forskjellige skyløsninger fra Microsoft Azure. I begge eksemplene brukes MQTT-protokollen for å kommunisere data til og fra skyløsningene. I det første eksemplet bruker forfatterne skytjenesten Azure IoT Central aPaaS for å lage et «dashboard» til overvåking og «*emergency intervention*» av produksjonsprosessen. I det andre eksemplet bruker de skytjenesten Azure Virtual Machine IaaS for å rulle ut en egen instans av Node-RED hvor de etablerer «dashboardet». Begge eksemplene er veldig forenklet og tiltenkt utdanningsformål, men er likevel svært interessante fordi de inkluderer en komplett teknologioversikt og eksperimentell «testbed» som dekker hele kjeden fra produksjonsmiljø til overvåkning og kontroll fra grensesnitt i skyen.

Den andre relevante artikkelen på samme tema er «*A Smart Factory Architecture Based on Industry 4.0 Technologies: Open-Source Software Implementation*» skrevet av Fortoul-Diaz m.fl. i 2023 [16]. I denne artikkelen etablerer forfatterne en enkel use case med et transportbånd og en robot. Skyfunksjonalitet benyttes for å bestemme om roboten vil klare å samle delene eller ikke. I den foreslåtte arkitekturen er funksjoner for dataanalyse og læring gjennom maskinlæring flyttet ut i en skyløsning. Også her det vist hvordan et enkelt SCADA-system kan etableres i skyen ved bruk av utviklingsverktøyet Node-RED og MQTT-protokollen for å kommunisere med de lokale delene av produksjonssystemet.

Styrkene ved begge disse artiklene er at selve teknologien er beskrevet forholdsvis detaljert, og særlig gjelder dette for Kučera et al. [15]. Den største svakheten er ingen av casene er særlig industrinære. Kučera et al. benytter seg av et fullstendig virtuelt miljø, riktignok ved bruk av gode virtualiseringsmiljøer, inkludert factory IO[18], mens Fortoul-Diaz et al. bruker et test-bed med få fysiske komponenter (robot og transportbånd).

Cybersikkerhet er et tema i begge de overnevnte artiklene. Fortoul-Diaz peker på behovet for å autentisere de ulike del-elementene som kommuniserer i arkitekturen og sikre både informasjonen som sendes og selve forbindelsene som brukes for kommunikasjonen. I den foreslåtte arkitekturen etablerer de SSH-forbindelser for å sikre MQTT kommunikasjonen som skjer mellom skyen og de lokale tjenestene og mellom skyen og produksjonsmiljøet. De bruker i tillegg HPPTS (TLS) for å sikre kommunikasjonen mellom funksjonen for dataanalyse og læring i skyen og de lokale tjenestene. Autentiseringen oppgis å skje enten gjennom offentlig nøkkelkryptografi, eller gjennom brukernavn og passord. Kučera er dessverre ikke like detaljert i sin beskrivelse av hvordan sikkerhet er ivaretatt, men skriver at årsaken til at de valgte OPC UA, istedenfor OpenPLC, i det tredje eksempel for å kommunisere med skytjenesten Azure IoT Central aPaaS, er behovet for å sikre kommunikasjonsforbindelsen til skyen.

[18] https://factoryio.com/

5.2 Case: Skykontroll av sementproduksjon

Det utvalgte caset på temaet prosessindustri er **sementproduksjon**. Beskrivelsen er basert på artikkelen «*Smart Industrial IoT Monitoring and Control System Based on UAV and Cloud Computing Applied to a Concrete Plant*» skrevet av Salhaoui et al. i 2019 [29].

Dette caset omhandler bruk av skyløsninger og droner (eng: *Unmanned Aerial Vehicle* – UAV) ved sementproduksjon. Sement er avhengig av en riktig sammensetning av innsatsfaktorer for å oppnå påkrevd kvalitet. I caset som beskrives i artikkelen vil det «ordinære» kontrollsystemet, dersom det oppdager avvik i måleverdier, kunne sende ut en drone utstyrt med et kamera. Dronen filmer så transportbåndene som brukes til å frakte innsatsfaktorene som inngår i produksjonene, og sender bildene til en skytjeneste. I skytjenesten analyseres bildene, og resultatet sendes tilbake til kontrollsystemet med det mål om at det kan utføre korrigerende aksjoner. Systemet valideres i en virkelig sementfabrikk, men er ikke i bruk i daglig drift.

I sentrum av systemet finner vi en IoT Gateway, som knytter kontrollsystemet, skyen og dronen sammen. Siden IoT Gateway er plassert lokalt er denne referert til som «fog computing» i artikkelen. Logikken i IoT Gateway er implementert hovedsakelig ved bruk av Node-RED. I det implementerte systemet bruker gatewayen OPC UA for å kommunisere med kontrollsystemet, men forfatterne peker ut at det vil være mulig å bruke MTQQ som et alternativ. Kontrollsystemet består av PLSer og sensorer. Til tross for at kontrollsystemet kan motta nødvendig data fra skyen for å tilpasse produksjonsprosessen fremgår det ikke klart om nødvendige aktuatorer er tilkoblet. Skyløsningen er levert av IBM og driftet fra Dallas, USA. Sementfabrikken og øvrig utstyr er lokalisert i Spania. En PLS opptrer som OPC UA server som kommuniserer med en OPC UA klient plassert i IoT gateway. Kommunikasjonen mellom IoT Gateway og sky foregår over internettet, mens kommunikasjon mellom IoT Gateway og dronen benytter seg av WiFi.

Forfatterne av artikkelen undersøkte også nettverks- og prosesseringsforsinkelser knyttet til bruk av drone, sky og IoT Gateway. For dette formålet ble IoT Gateway satt opp på ulike typer maskinvare: Siemens Gateway, Raspberry Pi, og en standard PC. Jevnt over introduserte Siemens Gateway betydelig mer forsinkelser enn de to andre maskinvarene, og belastningen på CPUen under lagring av bilder fra dronen var høyere og i nærheten av 100% for denne maskinvaren. Avhengig av hvilken maskinvare som brukes lå nettverksforsinkelsen fra drone, via sky, og til kontrollsystem i området mellom 1 og 3 sekunder.

Forfatterne påpeker behovet av cybersikkerhet for å sende data mellom de forskjellige delene på en sikker måte. Det er ikke gitt noen detaljer om hvordan, eller hvor, sikkerhet er tatt tilvære i caset, men vi antar at siden de bruker OPC UA kan vi anta at autentisering, kryptering og logging av kommunikasjonen er satt opp og brukt i undersøkelsene.

Styrkene ved denne casen er at den er godt beskrevet. For eksempel gjøres det målinger av forsinkelser i nettverk og i ulike implementasjoner av IoT Gateway. Det er også en styrke at den valideres i et faktisk produksjonsmiljø. Svakheten ved casen er at selv om den valideres i et produksjonsmiljø er det ikke noe som tyder på at den brukes i daglig drift.

5.3 Case: Skykontroll av jernbane

Dette caset er hentet fra Siemens Mobility sitt whitepaper «*Train2Cloud*»[19], hvor Siemens beskriver en teknisk løsning for å plassere kontrollfunksjoner til et *Communications-Based Train Control System* i en skyløsning.

Løsningen hevdes å legge til rette for at funksjonalitet flyttes fra utstyr plassert på tog og langs skinnegangen til et skymiljø, on-prem hos operatøren eller hos en tredjepartstilbyder. To mulige scenarioer presenteres: ett hvor de eksisterende kontrollenhetene som i dag er installerte langs sporet er virtualiserte og flyttet opp i en skyløsning, og et mer fremtidsrettet scenario hvor i tillegg selve funksjonene for å kontrollere trekk, brems og åpning/lukking av dørene på toget er flyttet opp i skyen. De konkrete funksjonene som nevnes i Siemens sitt system er *Automatic Train Supervision, Wayside Control Unit* og *Interlocking*. Disse funksjonene later til å være implementert i en Infrastructure-as-a-Service modell, hvor den nevnte funksjonaliteten kjører på en proprietær plattform, som i sin tur kjører i et Linux operativsystem spesielt konfigurert for formålet. I artikkelen sies det at operativsystemet, i tillegg til «generell IT sikkerhet» (det er uklart for oss hva dette er), tilbyr sikkerhetsovervåking og sikker fjernoppdatering av programvare/ data i plattformen. Operativsystemet hevdes dermed å kunne oppfylle Security Level 3. Systemet som helhet hevdes å kunne støtte sikkerhetsfunksjoner helt opp til Safety Integrity Level (SIL) 4 (definert i standarden IEC 61508 [30]). Kommunikasjonen mellom tog og sky, samt sky og feltutstyr er beregnet til å foregå over 5G, eventuelt supplert med andre teknologier, for eksempel i tunneler.

Styrken ved dette caset er at slike ting som konkrete funksjoner og arkitektur i skyen (IaaS, Spesielt konfigurert Linux OS, plattform kjørende i nevnte OS) beskrives. Ettersom dette er noe som presenteres av Siemens antar vi også at teknologien er av en viss modenhet, blant annet hevdes det at SIL 4 funksjoner kan flyttes opp i skyen, og at Linux OS-et kan oppfylle Security Level 3. I artikkelen oppgir Siemens at det er deres nye DS3 (*distributed smart safe system*) *safety platform*[20] som er sertifisert til SIL4 som muliggjør flyttingen av kontrollfunksjoner til skyen.

Svakheten ved caset er at konteksten er merkbart annerledes enn kraftbransjen. Tog er mobile og i den eksisterende standarden IEEE 1474.1[21] er begrepet «*Communications-Based Train Control systems* (CBTC)» allerede definert. Dette trådløse, kommunikasjonsbaserte signalsystemet er blitt en bransjestandard som nå implementeres rundt om i verden, inklusiv i Norge[22]. Systemet, som er halvautomatisert, medfører at de fysiske signalene (grønt/rødt) ute i sporet fjernes, og at togføreren i stedet får informasjon inn på et display i førerrommet. Det er da systemet som styrer pådrag og brems, slik at hastighet mellom stasjoner og stoppmønster blir automatisert. Siden mye av kontrollfunksjonaliteten i CBTC er implementert i et sentralisert system er det derfor allerede «tilrettelagt» for å virtualisere funksjonaliteten og tilby den som en skytjeneste. Delsystemene *Automatic Train Supervision, Wayside Control Unit* og *Interlocking* i caset er alle en del av dette systemet. En annen svakhet er at kilden til casen er utelukkende basert på et whitepaper fra en industriell aktør, og at det derfor i ytterste fall kan være snakk om kun en salgspitch.

[19] https://www.mobility.siemens.com/global/en/portfolio/digital-solutions-software/infrastructure/infrastructure-in-the-cloud/train2cloud.html
[20] https://www.mobility.siemens.com/global/en/portfolio/digital-solutions-software/infrastructure/signaling-x/ds3.html
[21] https://standards.ieee.org/ieee/1474.1/6959/
[22] https://www.sporveien.no/prosjekter-og-arbeid/nytt-signalsystem-cbtc-for-t-banen/

5.4 Case fra kraftsektoren utenfor Norge

Det pågår en diskusjon både i Norge og internasjonalt om bruk av skyløsninger i kraftsektoren. En viktig endring for aktørene i kraftsektoren er at driftskontrollssystem tidligere er levert av en håndfull store aktører som er godt kjent i bransjen og som gjerne både leverer hardware og software (noen ganger i ulike deler av samme konsern). Det er leverandører som man er kjent med og ofte har hatt samarbeid med i årtier og som kjenner bransjen godt, inkludert de strenge kravene som må oppfylles for å ha høy forsyningssikkerhet. Når man snakker om bruk av sky og skytjenester kommer det andre store aktører på banen, som Microsoft, som også er kjente, men ikke som leverandører knyttet til driftskontrollsystemer. Sikkerhetsveilederen [21] beskriver godt utfordringer med forretningsmodellen til leverandører av skytjenester og oppfyllelse av krav i Energiloven og Kraftberedskapsforskriften knyttet til blant annet signering av taushetserklæringer, sikkerhetstesting og beredskap. Men denne veilederen sier eksplisitt at den ikke dekker problemstillinger knyttet til bruk av skytjenester i driftskontrollsystemer.

Internasjonalt tillot NERC CIP (*North American Electric Reliability Corporation's Critical Infrastructure Protection*) fra januar 2024 lagring av "*medium and high impact bulk cyber system information* (BCSI)» i skyen, gitt at visse kriterier er oppfylt. Dette er beskrevet i revisjoner av standardene CIP-004-7[23] og CIP-011-3[24] (CIP betyr *Critical Infrastructure Protection*). Lagring av denne typen informasjon i skyen har ikke vært tillatt tidligere. Dermed er det en endring på gang internasjonalt, som er interessant å følge fra Norge. Det er ikke så lett å sammenligne BCSI og kraftsensitiv informasjon, men det er forfatternes mening at kraftsensitiv informasjon omfatter mer informasjon enn BCSI, men det er fremdeles interessant å se på endringene i NERC CIP.

I litteraturen er det kun funnet teoretiske studier og forsøk i testbed av migrasjon av driftskontrollsystem til skyen, men ingen faktiske eksempler på at dette er utført og i bruk. Vi har funnet to forskjellige artikler som begge beskriver svært relevante case fra kraftsektoren utenfor Norge. Den første artikkelen; «*A Seamless Cloud Migration Approach to Secure Distributed Legacy Industrial SCADA Systems*» skrevet av Khan m. fl. i 2020 [18], foreslår en strategi for å migrere eksisterende kontrollsystem til skyen og presenterer en referansearkitektur for dette formål. Referansearkitekturen viser hvordan såkalte «*cloud connectivity kit*» kan festes til industrielt utstyr og brukes for å etablere en kryptert VPN-tunnel til en plattform i skyen. Forfatterne viser siden hvordan referansearkitekturen kan brukes i en case fra kraftsektoren. Caset er et microgrid, det er en geografisk avgrenset del av nettet med både produksjon og forbruk, som kan være tilkoblet hovedstrømnettet eller fungere som en egen enhet frakoblet hovedstrømnettet (være en «øy» som er produserer energi som dekker eget forbruk). Et microgrid må være synkront med hovedstrømnettet når det er tilkoblet dette og det må synkroniseres med hovedstrømnettet når det skal kobles sammen. Overgangsfasen mellom å være en «øy» og tilkoblet hovedstrømnettet er en utfordring. Da må mange parametere overvåkes og synkroniseres for å få en overgang som ikke gir avbrudd hos sluttkunder. Dette må skje i sanntid. I artikkelen er et oppsett for synkronisering av microgrid med hovedstrømnettet testet i et fysisk smart grid testbed. Testen i lab er vellykket og viser at det foreslåtte konseptet fungerer i praksis. Spesielt interessant er at testen viser at kommunikasjonsforsinkelsen mellom funksjonene i skyen og «on-premises» delen i labben er svært lav og ikke har noen negativ innvirkning på sanntidsfunksjoner. Forfatterne mener at dette viser at konseptet vil fungere i andre industrielle kontrollsystemer som også har strenge krav på høy data rate og lav forsinkelse.

Den andre artikkelen er «Security Risk Assessment-based Cloud Migration Methodology for Smart Grid OT Services» skrevet av Jelacic m.fl. i 2020 [19]. Forfatterne foreslår en metode for å risikovurdere migrasjon

[23] https://www.nerc.com/pa/stand/prjct2014xxcrtclinfraprtctnvr5rvns/cip-004-7_clean.pdf
[24] https://www.nerc.com/pa/Stand/Project201902BCSIAccessManagement/CIP-011-3_Clean.pdf

til sky av sensitive smart grid OT-tjenester, og illustrerer metoden på to caser; en mindre DSO (*Distribution System Operator*) med begrensede ressurser, en større DSO med flere ressurser, men også mer komplekse systemer. Artikkelen er teoretiske studier med fokus på informasjonssikkerhet og rapporterer ikke om virkelig utførte migrasjoner til sky. Det er likevel en interessant artikkel fordi den også foreslår systemarkitektur spesifikt for smartgrids iht. en IEC 62443 modell med sikkerhetssoner.

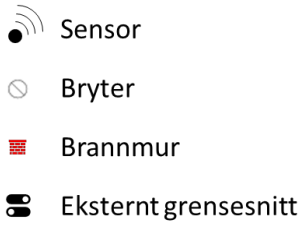
Som sagt, så er svakheten med begge artiklene at det er hhv. teoretisk og testbed, og dermed ikke eksempler på reelle case i energisektoren. De er likevel interessante fordi de gir eksempler på systemarkitektur og testene gjort i lab gir indikasjon på lav forsinkelse, en viktig parameter, da man er avhengig av sanntid for mange funksjoner i strømnettet. Det er lite rom for tidsforsinkelser.

Strømnettet har fysisk stor utstrekning (via kraftledninger og kabler) og viktig «noder» i strømnettet er transformatorstasjoner, hvor spenning blir transformert opp eller ned og strømmen kan endre retning eller skrus av (brytere). Mange funksjoner kan styres fra en sentral driftssentral, men bryting av strøm pga. feil i nettet gjøres lokalt vha. vern, se Figur 1 i kapittel 6.1, som viser driftskontrollsystem og lokalt driftskontrollsystem. Chehida et al. [20] foreslår en tilnærming til det å dynamisk allokere et sett med kontrollfunksjoner til servere. Bakteppet er det franske transmisjonsselskapets ønske om å virtualisere vernfunksjoner som tidligere ble implementert av IEDer på servere. Man gjør derimot ikke bruk av sky, men heller servere plassert i nettstasjonen (omtalt som edge). Det pågår en virtualiseringstrend i bransjen som ikke nødvendigvis innebærer bruk av sky, men fra leverandørsiden er dette gjerne foreslått som en del av løsningen. Det kan dermed være at «skytrenden» starter ute i nettet, i transformatorstasjoner, og senere kommer til de sentrale driftskontrollsystemene.

6 Referansearkitektur

For å kunne analysere hvordan sikkerheten til klasse 1 og 2 driftskontrollsystemer kan ivaretas når funksjoner kritiske for operasjonell driftskontroll er avhengige av eller plassert i skyen, bruker vi en referansearkitektur. Dette er en overordnet og generisk systembeskrivelse, som består av en figur med tilhørende forklarende tekst. Referansearkitekturen vil først illustrere dagens situasjon hvor alle funksjonene i driftskontrollsystemet er plassert «on-premises». I de etterfølgende figurene vil varierende grad av funksjoner være skilt ut fra de gjenværende funksjonene i driftskontrollsystemet og plassert i en eller flere skyløsninger. Beskrivelsene og visualiseringene av systemet i figurene holdes på et overordnet nivå, samtidig som de vil være tilstrekkelig detaljert for å kunne brukes til å analysere relevante svakheter, sårbarheter og trusler forbundet med skyløsningene.

Referansearkitekturen tar utgangspunkt i figuren i starten av kapittel 7 i NVE sin veiledning til kraftberedskapsforskriften [2], som gir en grafisk oversikt over hva som inngår i definisjonen av begrepet «driftskontrollsystem». Vi har i tillegg brukt en tilpasset variant av Purdue-modellen (se seksjon 3.3) som er vanlig å bruke i industrielle kontrollsystemer for å oppnå sikkerhet gjennom å segmentere systemet i forskjellige soner. Nomenklaturen vi har brukt for å illustrere viktige elementer i referansearkitekturen er vist i Figur 3.

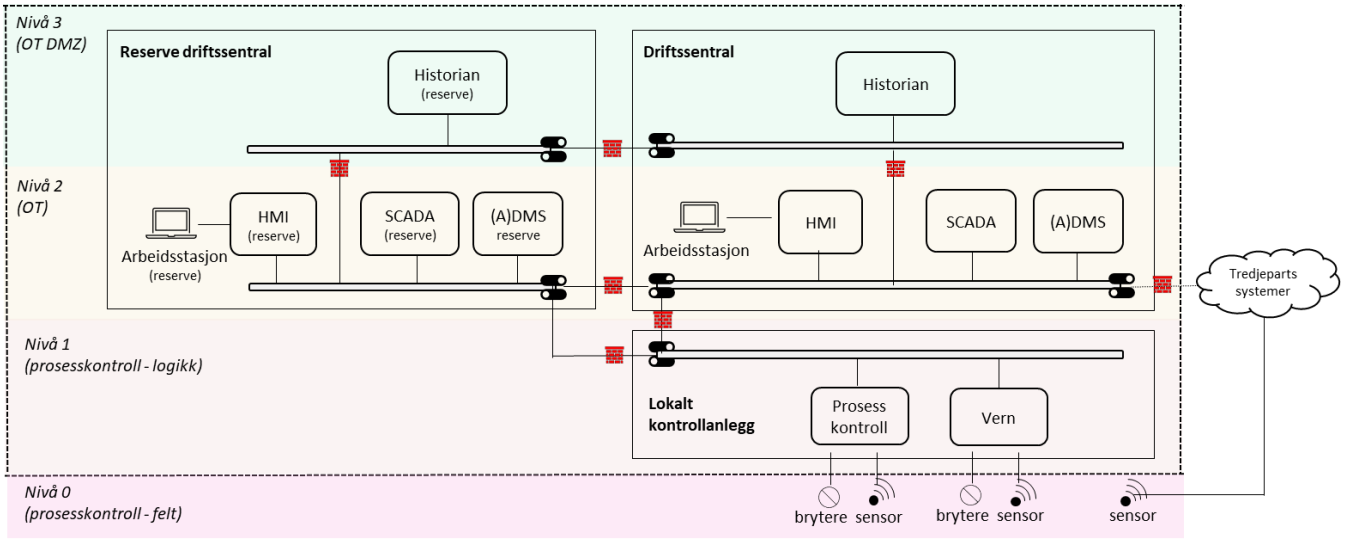


Figur 3: Nomenklatur brukt i referansearkitekturen.

Hovedfokus i referansearkitekturen er å vise hvilke funksjoner som inngår i et driftskontrollsystem, og hvordan disse funksjonene er koblet sammen, både med hverandre og med eksterne funksjoner eller systemer. Merk at vår definisjon av funksjon i referansearkitekturen er en *del av systemet som er mulig å skille ut logisk fra resten av systemet, og* som derfor er mulig å virtualisere og/eller implementere som en skytjeneste. Dette betyr at, for eksempel, fysiske brytere, kabler, operatører av utstyr og arbeidsstasjoner ikke vil defineres som funksjoner i referansearkitekturen, men at programvare som styrer brytere, selve transporten av data i nettverket og grensesnittene (HMI) som brukes av operatørene kan defineres som funksjoner, hvis hensiktsmessig.

6.1 Dagens situasjon

Referansearkitekturen som illustrerer nåværende driftskontrollsystemer, er gjengitt i Figur 4. Legg merke til at vi har tatt med reserve driftssentral som en del av arkitekturen, til tross for at det ikke er krav om dette for klasse 1 eller 2 driftskontrollsystemer i KBF. Imidlertid er det krav om at virksomheter med klasse 2 driftskontrollsystemer skal ha «planer for alternativ drift dersom driftssentralen blir utilgjengelig over lengre tid», og en reserve driftssentral kan være en av flere måter å møte dette kravet på.



Figur 4: Dagens situasjon. Alt innenfor stiplet linje regnes som driftskontrollsystem.

Følgende funksjoner er tatt med i arkitekturen:

HMI (Human Machine Interface). Tilsvarende operatørpanel på norsk. Det er et fysisk grensesnitt mellom menneske og maskin, typisk en dataskjerm som viser et systembilde med brytere og sensorer, med tastatur og mus for å gjøre endringer. Kan implementeres og tilbys som en skytjeneste til nettselskapene, typisk i form av en SaaS som aksesseres gjennom et webgrensesnitt fra en lokal arbeidsstasjon. I en driftssentral vil en slik arbeidsstasjon typisk være installert i nivå 2 (OT).

SCADA (Supervisory control and data acquisition). Den befinner seg i grenseland mellom den fysiske og den digitale verden. SCADA består av en samling maskinvare (PLSer, servere, switcher) og en programvarepakke som står for kontroll og datainnsamling. PLS er Programmerbar Logisk Styring (eller PLC – eng. *Programmable Logical Controller*). SCADA-systemet i nettet omfatter sensorer og aktuatorer som muliggjør fjernovervåkning og -styring [31]. Den kan implementeres og tilbys som en skytjeneste til nettselskapene, forslagsvis i form av en SaaS som aksesseres fra en lokal HMI installert i nivå 2 (OT), eller som en SCADA-as-a-service (HMI funksjonen vil inngå som en del av løsningen).

Historian[25] samler og lagrer data fra SCADA, og kan implementeres og tilbys som en skytjeneste til nettselskapene, typisk i form av en SaaS.

(A)DMS DMS (Distribution Management Systems) brukes for å overvåke og kontrollere et distribusjons-nett. Systemene samler inn, organiserer og visualiserer sanntidsinformasjon på tvers i hele nettet og har støtte for å gjennomføre analyser, predikere forbruk og optimalisere nettnytte. DMS er avhengig av data fra andre systemer, herunder SCADA og NIS/GIS. De siste årene har det også blitt økt fokus på integrerte løsninger som tilbyr SCADA og DMS-funksjonalitet i samme system - med tett integrasjon mot NIS/GIS. Slike løsninger kalles ofte ADMS (Advanced Distribution Management Systems). DMS benyttes uteluk-kende av nettselskaper [32].

Prosesskontroll. I denne rapporten kaller vi eksempelvis brytere og trinnkoblere for prosesskontroll for å illustrere alt som kan styres fra driftssentral og/eller lokalt kontrollanlegg. Brytere kan åpnes og lukkes og dermed kan strømnettet kobles om, mens en trinnkobler endrer trinn i transformator for å opprettholde

[25] https://www.scadainfo.com/scada-historian/

en gitt spenning ved endring i belastningen. Lengre ned i rapporten presenterer vi et eksempel på at lokalt kontrollanlegg virtualiseres og benytter skytjeneste.

Vern. Et vern utløses/aktiveres ved en feil i kraftsystemet. Det kan eksempelvis være en kortslutnings-strøm som etter en definert tidsperiode utløser vernet som kan bety at en bryter åpnes for å beskytte systemet mot kortslutningsstrømmen. I vår forenkling i Figur 4 er prosesskontroll og vern del av lokalt kontrollanlegg. På samme måte som med prosesskontroll, presenterer vi lengre ned i rapporten et eksempel på at lokalt kontrollanlegg virtualiseres og benytter skytjenester.

Alle funksjonene er representert som bokser i figuren. Grensesnitt mot eksterne systemer er illustrert med svitsjesymboler. Brannvegger er illustrert med røde firkanter. I henhold til tilsvarende figur i veiledningen til Kraftberedskapsforskriften så er alt innenfor de stiplede linje regnet som driftskontrollsystem. Merk at i denne arkitekturen er forbindelsene mellom kontrollsystemet og reserve driftssentralen illustrert som to separate logiske forbindelser; en på nivå 3 og en annen på nivå 2. Disse kan i praksis opprettes ved hjelp av en enkelt fysisk forbindelse, beskyttet av en brannmur (slik det er illustrert i tilsvarende figur i veiledningen til KBF). Merk at alle funksjonene vil inneholde kraftsensitiv informasjon.

I referansearkitekturen har vi kun tatt med nivå 0-3 fra Purdue modellen, siden det er disse nivåene som bygger opp et driftskontrollsystem. Arkitekturen vil enkelt kunne utvides til å inkludere flere av lagene fra Purdue, hvis det er behov for dette. I tidligere publiserte referansemodeller for kontrollsystemer varierer det hvorvidt Historian ansees høre hjemme i nivå 2 (slik som illustrert av DNV [33]) eller i nivå 3 (slik som antydet av ENISA [25] og [19]). Vi har valgt å plassere den i nivå 3, fordi OT-DMZ[26] er en naturlig plass for en slik database som har naturlige koblinger inn i både OT- og IT-nettverkene i et kraftsystem.

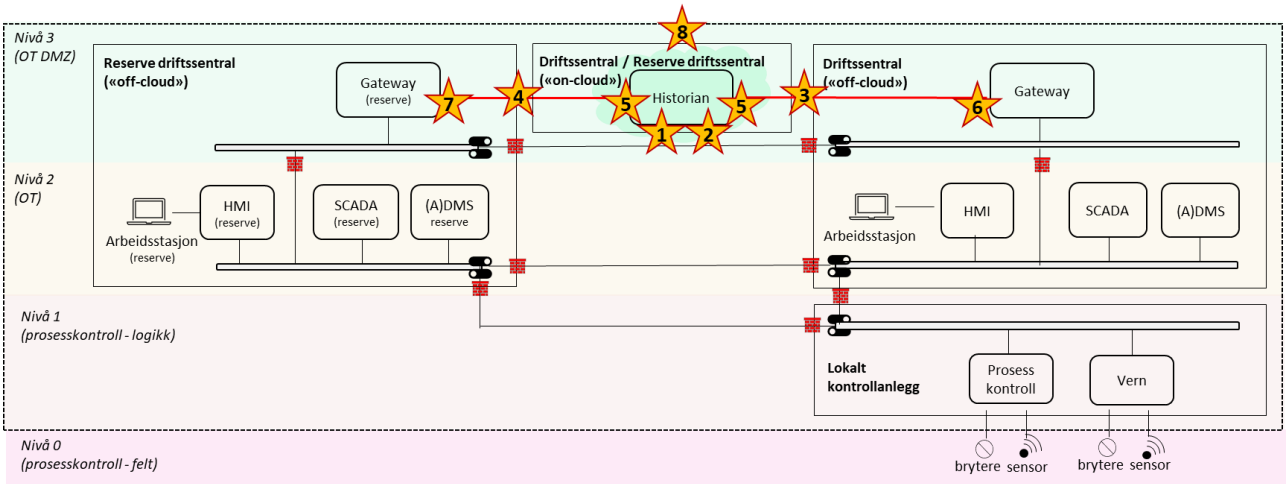
I tillegg til funksjonene i selve driftskontrollsystemet, inneholder Figur 4 en sky med navnet «Tredjeparts systemer». Dette utgjør typisk sensorer levert av en ekstern aktør med egen infrastruktur. De står da for all kommunikasjon selv, uten integrert tilknytning til driftskontrollsystemet. Eksempler kan være temperatur- eller vibrasjonssensorer fra Disruptive Technologies[27] som installeres i en nettstasjon, eller neuronene fra Heimdall Power[28] som monteres på høyspentledninger for å vurdere hvor hardt det er forsvarlig å belaste ledningen. Alle data samles inn av leverandøren i deres skyløsning, og leveres til kunden (nettselskap eller Statnett) i aggregert form. Det er ingen direkte kobling til kundens SCADA system, men når selskapet begynner å bruke resultatene fra slike tredjepartssystemer i sin daglige drift, så åpner det en ny angrepsflate. Hvis f.eks. Heimdall Cloud har feil data (som følge av ekstern manipulering av en trusselaktør) som blir brukt som grunnlag for å gjøre beslutninger i driften av et nett, kan dette medføre uønskede konsekvenser [34]. Dette til tross for at Heimdall ikke gjør noe i SCADA selv, men de *leverer data inn i SCADA som brukes i driften* (ved bruk av «custom SCADA connectors»). Dette er helt nytt. Bransjen er vant til å ta data fra sensoren selv, men her får man en indirekte leveranse av data fra sensoren. Tredjepartssystemer er ikke tatt med i våre analyser av skybasert driftskontroll (seksjon 6.2-6.5), men er tatt med i illustrasjonen av dagens situasjon for å vise at dagens driftskontrollsystemer i mange tilfeller allerede bruker skybaserte tjenester.

Vi vil nå vise tre forskjellige varianter av den samme referansearkitekturen som i Figur 4, men hvor varierende grad av funksjoner er skilt ut og plassert i en eller flere skyløsninger.

[26] Vi kan også nevne at de lærde strides om hvilket Purdue-nivå som utgjør DMZ – noen sier nivå 3 [25], mens andre legger til et ekstra nivå 3.5 [22].
[27] https://www.disruptive-technologies.com/
[28] https://heimdallpower.com/

6.2 Eksempel: Historian i skyen

I det første eksemplet har vi illustrert hvordan «Historian» funksjonen kan implementeres som en skytjeneste (Figur 5). I dette eksemplet vil begge funksjonene som tidligere ble brukt i driftssentralen og i reservedriftssentralen bli erstattet med en skyløsning. Denne vil sannsynligvis bli tilbudt som en SaaS løsning («Historian-as-a-Service»). Den nye skytjenesten vil da formelt bli en del av nivå 3 (OT DMZ), i både driftssentralen og i reservedriftssentralen. Løsningen vil trenge ny funksjonalitet i form av datakommunikasjonsenheter («gateways») for å koble de interne nettverkene til skyløsningen på en sikker måte. Merk at de to nye nettverksforbindelsene mellom driftssentralen og skyløsningen og mellom reservedriftssentralen og skyløsningen (illustrert med rødt i figuren) vil gå over Internett, samtidig som de formelt sett vil bli en del av selve driftskontrollsystemet.



Figur 5: Historian i skyen. Alt innenfor stiplet linje regnes som driftskontrollsystem. Relevante sikkerhetstrusler mot de nye delene av arkitekturen er illustrert med stjerner.

En åpenbar fordel med denne løsningen er økt tilgjengelighet av data fra Historian, sammenlignet med dagens situasjon. Replikering vil enkelt kunne håndteres av skyleverandøren. Back-up vil forbedres sammenlignet med dagens situasjon, siden det er enkelt å opprette en varm kopi (duplikat) av Historian-funksjonen i skyen som kan ta over umiddelbart hvis den primære tjenesten feiler. Synking mellom Historian servere henholdsvis i driftssentralen og reservedriftssentralen vil da ikke lenger være nødvendig.

6.2.1 Sikkerhetsanalyse

Fra et sikkerhetsperspektiv vil samspillet mellom driftssentralen og skyløsningen, samt mellom reserve driftssentralen og skyløsningen (begge illustrert med rødt i figuren over), og tilsvarende grensesnitt, bli spesielt viktig. Relevante (nye) sikkerhetstrusler som vil oppstå er

1. Brudd på konfidensialitet av informasjon som lagres av den skybaserte Historian.
2. Uautorisert endring av informasjon som lagres av den skybaserte Historian.
3. Tjenestenektangrep mot kommunikasjonsforbindelsen mellom den skybaserte Historian og driftssentralen.
4. Tjenestenektangrep mot kommunikasjonsforbindelsen mellom den skybaserte Historian og reservedriftssentralen.
5. Tjenestenektangrep mot grensesnittet til den skybaserte Historian.
6. Tjenestenektangrep mot det nye grensesnittet i driftssentralen.
7. Tjenestenektangrep mot det nye grensesnittet i reservedriftssentralen.
8. Tjenestenektangrep mot skytjenesteleverandøren sin plattform.

Disse er markert med tilsvarende stjerner i Figur 5.

Historian lagrer en historisk oversikt over SCADA-operasjoner, og er i utgangspunktet en enveis-tjeneste, i den forstand at det ikke er noe behov for å kommunisere tilbake til SCADA. Imidlertid er jo forutsetningen at noen har behov for disse dataene på et senere tidspunkt, og slikt sett kan en angriper potensielt ha et ønske om å kompromittere de lagrede dataene i skyen. Tilgjengelighet av tjenesten er mindre kritisk, ut over muligheten til å faktisk få overført historiske data. Selv om Historian formelt sett er en del av driftskontrollsystemet, vil bortfall av denne ikke ha en umiddelbar effekt på driften i seg selv.

6.2.2 Designkriterier

For å ivareta cybersikkerheten i den foreslåtte løsningen i eksemplet «Historian i skyen» må følgende være på plass:

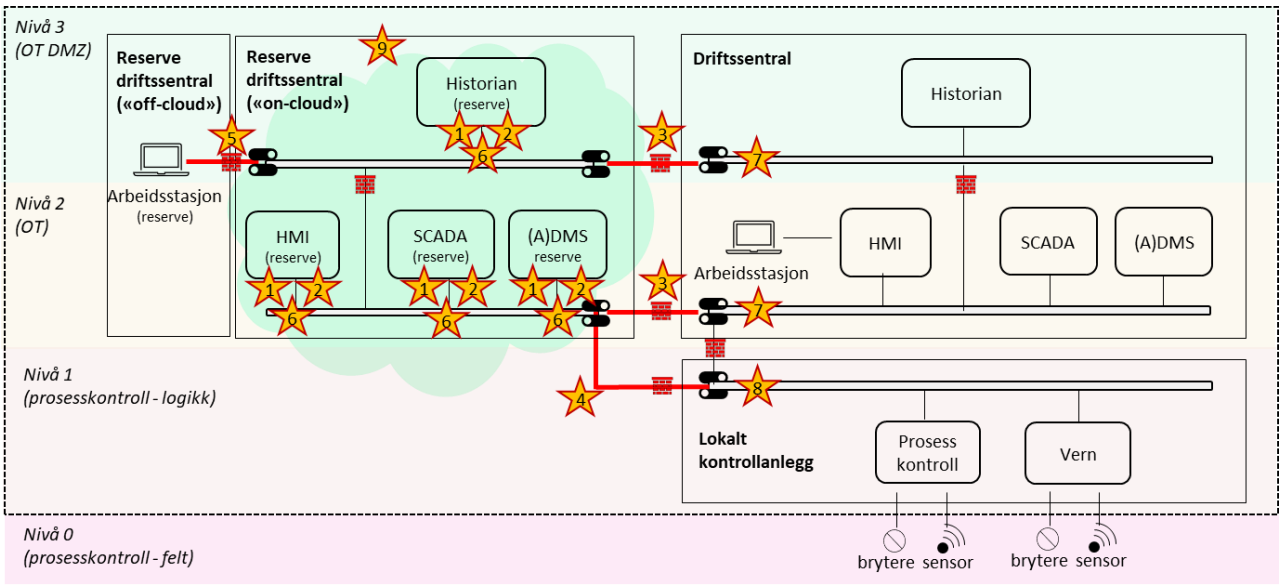
- Etablere en «gateway» for gjensidig autentisering og kryptering av kommunikasjons-forbindelsen fra driftssentralen til den skybaserte Historian.
- Etablere en «gateway» for gjensidig autentisering og kryptering av kommunikasjons-forbindelsen fra reservedriftssentralen til den skybaserte Historian.
- Tilgangskontroll på den skybaserte Historian som sikrer at kun autoriserte enheter får anledning til å sende data til den.
- Selve forbindelsen fra driftssentralen til den skybaserte Historian må sikres, og det må verifiseres at den har tilstrekkelig tilgjengelighet og pålitelighet.

Merk at for å tilfredsstille kravene i KBF Kapittel 7, må kulepunktene identifisert i seksjon 3.1.3 i denne rapporten avtales spesielt med skyleverandøren.

6.3 Eksempel: Reservedriftssentral i skyen

I det andre eksemplet har vi illustrert hvordan reservedriftssentralen kan implementeres som en sky-tjeneste (Figur 6). Selv om det eksplisitte kravet om å ha en reservedriftssentral kun gjelder for klasse 3 driftskontrollsystemer (KBF § 7-15 a), anser vi at å etablere en reservedriftssentral i skyen er en hensikts-messig tilnærming til «planer for alternativ drift» som det heter i § 7-14 d. I dette eksemplet vil alle funk-sjonene i reservedriftssentralen bli erstattet med en skyløsning. Unntaket er arbeidsstasjonen, som er en fysisk komponent. Løsningen vil trenge ny funksjonalitet i form av flere nye datakommunikasjonsenheter («gateways») mot skyløsningen: en for å holde Historian reserven synkronisert, en annen for å holde SCADA reserven og de andre enhetene på nivå 2 synkronisert, og sannsynligvis også en tredje som brukes for å koble over skyløsningen til de lokale kontrollanleggene hvis driftssentralen går ned. For å ikke gjøre figuren for komplisert, er disse datakommunikasjonsenhetene utelatt fra figuren.

De nye nettverksforbindelsene i denne løsningen er illustrert med rødt i figuren. Merk at de fire nye nett-verksforbindelsene vil gå over Internett, samtidig som de formelt sett vil bli en del av selve driftskontroll-systemet.



Figur 6: Reservedriftssentral i skyen. Alt innenfor stiplet linje regnes som driftskontrollsystem. Relevante sikkerhetstrusler mot de nye delene av arkitekturen er illustrert med stjerner.

I denne løsningen vil driftssentralen brukes som vanlig, fram til noe skjer. Skifter da til reserveløsningen i skyen. Åpenbare fordeler med en slik løsning er den økte graden av tilgjengelighet og redundans som følger med bruken av sky. En skybasert reservedriftssentral vil til enhver tid være klar til bruk og den kan fungere helt uavhengig av den ordinære driftssentralen. Merk at i en slik løsning kan arbeidsstasjonen i reserveløsningen (i teorien) plasseres hvor som helst - dette vil være en konfigurasjonspolicy sak som er avhengig av kravene til «driftssentral» i KBF.

6.3.1 Sikkerhetsanalyse

Fra et sikkerhetsperspektiv vil samspillet mellom driftssentralen og reservedriftssentralen i skyen, mellom reservedriftssentralen i skyen og lokalt kontrollanlegg, samt mellom arbeidsstasjonen i reserveløsningen og reservedriftssentralen i skyen (illustrert med rødt i figuren over), og tilsvarende grensesnitt, bli spesielt viktig. Relevante (nye) sikkerhetstrusler som vil oppstå er

1. Brudd på konfidensialitet av informasjon som lagres av funksjonene i den skybaserte reserve-driftssentralen (Historian, SCADA (A)DMS og HMI).

2. Uautorisert endring av informasjon som lagres av funksjonene i den skybaserte reserve-driftssentralen (Historian, SCADA (A)DMS og HMI).
3. Tjenestenektangrep mot kommunikasjonsforbindelsen(e) mellom driftssentralen og reserve-driftssentralen i skyen (på nivå 2 og 3).
4. Tjenestenektangrep mot kommunikasjonsforbindelsene mellom reservedriftssentralen i skyen og lokalt kontrollanlegg.
5. Tjenestenektangrep mot kommunikasjonsforbindelsene mellom reservedriftssentralen i skyen og arbeidsstasjonen i reserveløsningen
6. Tjenestenektangrep mot grensesnittene i funksjonene i den skybaserte reservedriftssentralen.
7. Tjenestenektangrep mot de nye datakommunikasjonsenhetene («gateways») i driftssentralen som brukes mot reservedriftssentralen i skyen.
8. Tjenestenektangrep mot de nye datakommunikasjonsenhetene («gateways») i lokalt kontrollanlegg som brukes av reservedriftssentralen i skyen
9. Tjenestenektangrep mot skytjenesteleverandøren sin plattform.

Disse er markert med tilsvarende stjerner i Figur 6.

To viktige sikkerhetsrelaterte aspekter ved denne løsningen er tilgjengelighet og tilgangskontroll. Arbeids-stasjonen kan i prinsippet stå hvor som helst (hos hjemmevakten, på et kontor). Tilgangskontroll fra arbeidsstasjonen vil konfigureres i skyløsningen, for eksempel kan man bestemme at alle ansatte skal få tilgang hjemmefra, eller at tilgang kun tillates fra et spesifikt reservekontor. Vedrørende tilgjengelighet er det viktig å hensynta sanntidskrav, spesielt hva som kan aksepteres med tanke på tidsforsinkelse for en endring i skyen på SCADA serveren, til det faktisk skjer noe i det lokale prosessanlegget.

Et annet aspekt er overgangen fra normal drift til bruk av reservedriftssentral. Så lenge driftssentralen fungerer som vanlig skal det ikke være mulig å bruke reserveløsningen og det trengs en egen form for autentisering for å bruke reservedriftssentral; altså en rutine for «active changeover» og avslutning av bruk når normal driftssentral er operativ igjen.

Når kontrollsystemet er nede, vil de lokale kontrollanleggene styres fra skyen. Denne situasjonen er tilsvarende som i NVE sin figur i kapittel 7 av veiledningen til kraftberedskapsforskriften, hvor lokale kontrollanlegg kan styres via trådløs forbindelse. Samme nivå av sikkerhet må kunne oppnås på forbind-elsene mellom skytjenesten og de lokalkontrollsystemene som det som kreves på (den trådløse) forbind-elsen mellom driftssentralen og lokalkontrollanleggene i dag.

6.3.2 Designkriterier

For å ivareta cybersikkerheten i den foreslåtte løsningen i eksemplet «reservedriftssentral i skyen» må følgende være på plass:

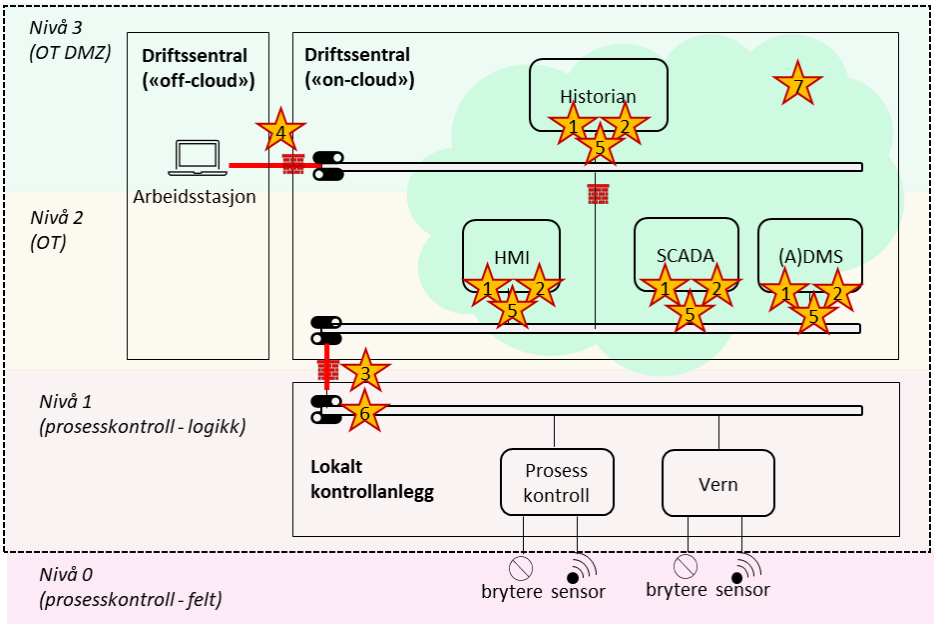
- Etablere en «gateway» for gjensidig autentisering og kryptering av kommunikasjons-forbindelsen fra driftssentralen til reservedriftssentral i skyen på nivå 3
- Etablere en «gateway» for gjensidig autentisering og kryptering av kommunikasjons-forbindelsen fra driftssentralen til reservedriftssentral i skyen på nivå 2
- Etablere en «gateway» for gjensidig autentisering og kryptering av kommunikasjons-forbindelsen fra lokale kontrollanlegg til reservedriftssentral i skyen
- En avklaring hva som er tillatt mtp. fjerntilgang fra hjemmekontor og en tilsvarende konfigurasjon av både skytjenesten + de godkjente arbeidsstasjonene.
- Konfigurere oppsettet av reservedriftssentralen i skyen slik at den ikke kan brukes når driftssentralen er operativ.

- Selve forbindelsen fra driftssentralen til reservedriftssentral, og fra lokale driftsanlegg til reservedriftssentral, må sikres, og det må verifiseres at den har tilstrekkelig tilgjengelighet og pålitelighet.

Merk at for å tilfredsstille kravene i KBF Kapittel 7, må kulepunktene identifisert i seksjon 3.1.3 av denne rapporten avtales spesielt med skyleverandøren.

6.4 Eksempel: Skybasert driftssentral

I det tredje eksemplet har vi illustrert hvordan driftssentralen kan implementeres som en skytjeneste (Figur 7). I dette eksemplet vil alle funksjonene i driftssentralen bli erstattet med en skyløsning, unntatt arbeidsstasjonen, som er en fysisk komponent. Løsningen vil trenge ny funksjonalitet i form av «gateways» mot skyløsningen som må installeres i hvert av de lokale kontrollanleggene. Disse er ikke tatt med i figuren under. Fra et sikkerhetsperspektiv vil to nye kommunikasjonsforbindelsene (illustrert med rødt i figuren) bli viktige å beskytte. Merk at de to nye forbindelsene vil gå over Internett, samtidig som de formelt sett vil bli en del av selve driftskontrollsystemet.



Figur 7: Skybasert driftssentral. Alt innenfor stiplet linje regnes som driftskontrollsystem. Relevante sikkerhetstrusler mot de nye delene av arkitekturen er illustrert med stjerner.

En åpenbar fordel med denne løsningen er at det ikke lenger, teknisk sett, er behov for en reserveløsning for funksjonene i driftssentralen, siden replikering er en del av selve kjernekonseptet av skytjenester. I praksis vil dette bli avhengig av hvordan kravene i Kraftberedskapsforskriften tolkes.

Et annet aspekt er det som gjenstår av den fysiske delen av driftssentralen (illustrert som «off-cloud» i bildet). Vår oppfatning er at det vil sannsynligvis fortsatt eksistere et fysisk beskyttet rom for arbeidsstasjonen med adgangskontroll («bomberom») fordi nettselskapene har etablert slike og antageligvis vil ønske å fortsette med en slik løsning for driftspersonell, i tillegg til at noen har klasse 3 anlegg og dermed må ha et slikt beskyttet rom. For å tilfredsstille kravene i KBF for klasse 2, må det fortsatt finnes noe slags reserveløsning også for denne delen, som kan brukes hvis det fysiske rommet blir utilgjengelig (§ 7.14.d). Men merk at KFB har ikke noe eksplisitt krav på et slikt rom for klasse 1 og 2 driftskontrollsystemer (kun for klasse 3); forskriften sier kun at det må finnes «*planer for alternativ drift*», hvilket ikke nødvendigvis betyr at den lokale arbeidsstasjonen må plasseres i en fysisk reservedriftssentral.

6.4.1 Sikkerhetsanalyse

Fra et sikkerhetsperspektiv vil de to nye forbindelsene mellom driftssentralen i skyen og lokalt kontrollanlegg, samt mellom driftssentralen i skyen og den lokale arbeidsstasjonen (illustrert med rødt i figuren over), og tilsvarende grensesnitt, bli spesielt viktig. Relevante (nye) sikkerhetstrusler som vil oppstå er

1. Brudd på konfidensialitet av informasjon som lagres av funksjonene i den skybaserte driftssentralen (Historian, SCADA (A)DMS og HMI).
2. Uautorisert endring av informasjon som lagres av funksjonene i den skybaserte driftssentralen (Historian, SCADA (A)DMS og HMI).
3. Tjenestenektangrep mot kommunikasjonsforbindelsen mellom driftssentralen i skyen og lokalt kontrollanlegg.
4. Tjenestenektangrep mot kommunikasjonsforbindelsen mellom driftssentralen i skyen og den lokale arbeidsstasjonen.
5. Tjenestenektangrep mot grensesnittene i funksjonene i driftssentralen i skyen.
6. Tjenestenektangrep mot det nye grensesnittet i lokalt kontrollanlegg som brukes mot driftssentralen i skyen.
7. Tjenestenektangrep mot skytjenesteleverandøren sin plattform.

Disse er markert med tilsvarende stjerner i Figur 7.

Dette eksemplet er det mest radikale, da hele driftssentralen er lagt i en skyløsning. Det er trolig at man vil nærme seg en slik løsning gradvis, blant annet ved å beholde en fysisk arbeidsstasjon. Skyløsninger bringer med seg mange fordeler, men også noen utfordringer som nevnt i trussel-listen over. Det er også problematisk å tilfredsstille alle kravene i KBF.

Tidskrav rundt skybasert driftssentral kan bli en utfordring. Det kan bli avhengig av hvor du er i landet, og hvor lang den fysiske avstanden til de aktuelle datasentrene vil være.

6.4.2 Designkriterier

For å ivareta cybersikkerheten i den foreslåtte løsningen i eksemplet «skybasert driftssentral» må følgende være på plass:

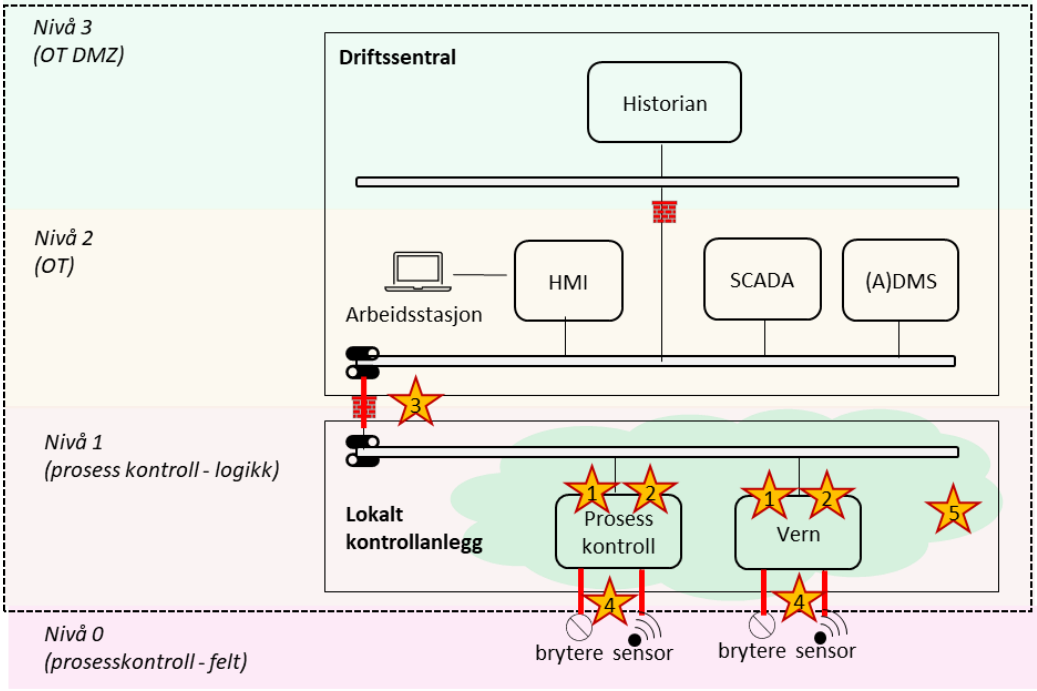
- Etablere en «gateway» for gjensidig autentisering og kryptering av kommunikasjonsforbindelsen fra lokale kontrollanlegg til driftssentral i skyen
- En avklaring hva som er tillatt mht. fjerntilgang fra hjemmekontor og en tilsvarende konfigurasjon av både skytjenesten + arbeidsstasjonene.
- Tilgangskontroll på den skybaserte driftssentralen som sikrer at kun autoriserte enheter får anledning til å sende data til den.
- Selve forbindelsen fra den skybaserte driftssentralen til lokale kontrollanlegg og til arbeidsstasjonen i «off-cloud» driftssentral må sikres, og det må verifiseres at den har tilstrekkelig tilgjengelighet og pålitelighet.

Merk at for å tilfredsstille kravene i KBF Kapittel 7, må kulepunktene identifisert i seksjon 3.1.3 av denne rapporten avtales spesielt med skyleverandøren.

6.5 Eksempel: Skybasert lokalkontroll

I det siste eksemplet har vi illustrert hvordan funksjoner i et lokalt kontrollanlegg kan implementeres som skytjenester (Figur 8). Dette er et interessant eksempel, fordi det skjer mye arbeid på virtualisering i nett-selskapene allerede, som legger til rette for bruk av skytjenester. Generelt ser vi også en trend hvor leverandørene er pådrivere for virtualisering i lokale kontrollanlegg. Dette caset er beskrevet som neste steg for vern og kontroll i ECoDiS prosjektet, et case hvor det blir mindre og mindre hardware, og mer virtualisering [28].

I et slikt eksempel ser vi for oss at man vil fortsette som i dag med å bruke SCADA-funksjonalitet (etc.) i et fysisk kontrollsystem, men at ett eller flere nettselskaper har valgt å virtualisere funksjoner, og etablert disse som skytjenester. Alle funksjoner i det lokale kontrollanlegget som legges i skyen (i dette eksemplet: prosesskontroll og vern) må da oppfylle kravene til klasse 1 og/eller 2 fra KBF. Merk at i et slikt eksempel vil SCADA gi kommando *via skyen* ut til brytere i det fysiske strømnettet. Fra et sikkerhetsperspektiv vil da samspillet mellom det lokale kontrollanlegget og SCADA (illustrert med rødt i figuren under), og tilsvarende grensesnitt, bli spesielt relevant å analysere.



Figur 8: Skybasert lokalkontroll. Alt innenfor stiplet linje regnes som driftskontrollsystem. Relevante sikkerhetstrusler mot de nye delene av arkitekturen er illustrert med stjerner.

De fysiske forbindelsene mellom prosesskontroll/vern og bryterne/sensorene i nettet vil bli erstattet med en nettverksforbindelse til skyen. For eldre utsyr vil dette kreve et slags «cloud connectivity kit», slik som forklart av Khan [18] (dette er ikke tatt med i figuren). Dette ligger på linje med digitalisering av det fysiske utstyret ute i stasjonene, som vist i ECoDiS prosjektet som neste steg for vern og kontroll [28]. I ECoDiS handler det om virtualisering og ikke sky, men virtualisering legger godt til rette for bruk av sky, så det er mulig at eksemplet i dette delkapitlet blir en første test på bruk av sky som del av driftskontrollsystem.

6.5.1 Sikkerhetsanalyse

Fra et sikkerhetsperspektiv vil de nye forbindelsene mellom driftssentralen og de lokale skybaserte kontrollanleggene, samt forbindelsene mellom prosesskontroll/vern og brytere/sensorer (illustrert med

rødt i figuren over), og tilsvarende grensesnitt, bli spesielt viktige. Relevante (nye) sikkerhetstrusler som vil oppstå er:

1. Brudd på konfidensialitet av informasjon som lagres av funksjonene i de skybaserte funksjonene for prosesskontroll og vern.
2. Uautorisert endring av informasjon som lagres av funksjonene i de skybaserte funksjonene for prosesskontroll og vern.
3. Tjenestenektangrep mot kommunikasjonsforbindelsen mellom driftssentralen og prosesskontroll/vern som er plassert i skyen.
4. Tjenestenektangrep mot kommunikasjonsforbindelsen mellom brytere/sensorer og prosesskontroll/vern som er plassert i skyen.
5. Tjenestenektangrep mot skytjenesteleverandøren sin plattform.

Disse er markert med tilsvarende stjerner i Figur 8.

Dette eksemplet kan sees som en mindre risikabel migrasjon til sky-basert drift enn å plassere selve kontrollsystemet helt, eller delvis, i skyen. Hvis et enkelt sky-basert lokalt kontrollanlegg detter ut, vil det ikke bli kritisk for Norge på samme måte som hvis et sky-basert kontrollsystem går ned. Merk at hvis flere lokale aktører går for en slik løsning, og de velger den samme skyløsningen og/eller den samme skyleverandøren, vil det ha større påvirkning hvis noe i løsningen går galt fordi alle som bruker den samme tjenesten og /eller leverandøren sannsynligvis vil bli rammet samtidig. Det vil da bli enda viktigere hvilke valg som gjøres for å oppnå redundans av de funksjoner og samband som brukes i løsningen. Som nevnt over, vil kravet om at minst en av de redundante forbindelsene ikke skal gå over offentlige kommunikasjonsnettverk være vanskelig å tilfredsstille for en skyløsning.

Tidskrav rundt skybasert lokalkontroll kan bli en utfordring. Det kan bli avhengig av hvor du er i landet, og hvor lang den fysiske avstanden til de aktuelle datasentrene vil være.

6.5.2 Designkriterier

For å ivareta cybersikkerheten i den foreslåtte løsningen i eksemplet «skybasert lokalkontroll» må følgende være på plass:

- Etablere en «gateway» for gjensidig autentisering og kryptering av kommunikasjonsforbindelsen fra driftssentralen til den skybaserte lokalkontrollen.
- Etablere en «gateway» på nivå 0 for gjensidig autentisering og kryptering av kommunikasjonsforbindelsene fra den skybaserte lokalkontrollen mot brytere, og fra sensorer til den skybaserte lokalkontrollen (for eksempel gjennom et «Cloud Connectivity Kit», som foreslått av Khan [18]).
- I den grad det er mulig bør man bruke moderne protokoller som tilbyr innebygget sikkerhet for kommunikasjon med brytere og sensorer, ikke protokoller som sender informasjon i klartekst.
- Tilgangskontroll på den skybaserte lokalkontrollen som sikrer at kun autoriserte enheter får anledning til å sende data til den.
- Selve forbindelsen fra den skybaserte lokalkontrollen til og fra brytere og sensorer, samt til driftssentralen, må sikres, og det må verifiseres at den har tilstrekkelig tilgjengelighet og pålitelighet.

Merk at for å tilfredsstille kravene i KBF Kapittel 7, må kulepunktene identifisert i seksjon 3.1.3 av denne rapporten avtales spesielt med skyleverandøren.

7 Konklusjon og videre arbeid

Skytjenester kan forenkle digitaliseringen av kraftsektoren, men det er flere utfordringer som må løses før potensialet kan bli utnyttet. De mest grunnleggende utfordringene er å forstå hvorvidt skybasert driftskontroll kan være sikkert nok, og hvilke tilpasninger som må gjøres for å overholde relevante myndighetskrav. I denne rapporten har vi vist hvordan skytjenester for OT/IT systemer vurderes brukt i tre andre sektorer; kommersielle fabrikker, prosessindustrien og jernbane. Vi har også diskutert hvordan utviklingen i kraftsektoren utenfor Norge arter seg. Casene presentert i denne rapporten viser hvordan skytjenester kan tas i bruk som en del av i driftskontrollsystemer, hvilke teknologier som kan vurderes brukt, og hvordan disse kan sikres. Vi har videre gjennomgått relevante krav fra Kraftberedskapsforskriften som vil komme til anvendelse ved vurdering av bruk av skytjenester for driftskontrollsystemer av klasse 1 og 2. For å illustrere hvordan kraftsektoren gradvis kan nærme seg skyløsninger, har vi tegnet opp fire forskjellige referansearkitekturer som tar i bruk skytjenester for deler av driftskontrollsystemer.

Vår oppfatning er at det ikke nødvendigvis er sikkerhetsmessige forhold ved skyløsninger i seg selv som forhindrer bruk av slike tjenester i driftskontrollsystemer. Skyløsninger er generelt svært sikre i dag, og for enkelte (mindre) aktører som sliter med IT kompetanse vil tjenesteutsetting gjennom skydrift sannsynligvis medføre økt sikkerhet, sammenlignet med dagens situasjon. Samtidig ser vi at nåsituasjonen for sikkerhet i kraftsektoren gjør det utfordrende å ta i bruk skytjenester, fordi aspekter som allerede ofte oppleves som vanskelige i bransjen, inkludert risikostyring, overvåking og logging, hendelseshåndtering og gjennomføring av sikkerhetsrevisjoner [35], er utfordringer som også er tilknyttet bruk av skytjenester og som da risikerer å bli enda vanskeligere å håndtere. Vi mener fortsatt at bruk av skytjenester som en del av driftskontrollsystemer kan være sikkert nok, gitt at nettselskapene klarer å stille de riktige kravene ved anskaffelsesprosessen, at skyleverandørene i neste steg klarer å oppfylle disse kravene, og at nettselskapene håndterer oppfølging og eventuelle skifter av leverandører. Det vil også være nødvendig for nettselskapene å påse at koblingen(e) mellom deres fysiske infrastruktur (driftskontrollsystem) og skyløsningen konfigureres på en sikker måte, med de nødvendige fysiske grensesnittskomponenter osv. En forutsetning for å bruke skyløsninger slik vi har skissert, er at det er mulig å få en tilstrekkelig sikker og stabil kommunikasjonsforbindelse mellom skyen og lokale elementer, og at fysiske begrensninger ikke medfører for store forsinkelser i kommunikasjonen for den aktuelle bruken. Hvis det gjøres riktig, kan tjenesteutsettelse i form av skytjenester bli et løft for hele bransjen.

Vår gjennomgang av relevante sikkerhetskrav i denne rapporten viser at gjeldende myndighetskrav medfører at det i dag ikke er mulig for norske nettselskaper å flytte driftskontrollsystemer av klasse 1 eller 2 opp i skyen. Årsaken er først og fremst enkelte spesifikke ordlyder i noen av paragrafene i Kraftberedskapsforskriftens kapittel 7 som gjør det umulig å tilfredsstille kravene som i dag er grunnleggende for god sikkerhet i næringen. Dog fremstår det for oss som om mange av kravene i forskriften er formulert med tanke på fysisk sikring, og ikke tar i betraktning at logisk sikring i mange tilfeller kan gi tilsvarende god nok beskyttelse. Det er vår oppfatning at det vil kun trenges mindre endringer av enkelte paragrafer i forskriften for å bedre legge til rette for digitalisering, virtualisering og bruk av skytjenester, uten å måtte kompromisse med sikkerheten av driftskontrollsystemene.

Veien fremover bør inkludere en etablering av en godkjenningsordning av skyleverandører som har tillatelse til å levere tjenester for norske driftskontrollsystemer, fortrinnsvis i regi av Nasjonal Sikkerhetsmyndighet (NSM). Det å ha en knippe leverandører å velge mellom, som på forhånd har dokumentert at de kan tilfredsstille de nødvendige kravene, vil gjøre det enklere for nettselskapene å ta i bruk skyløsninger på en sikker måte. I lys av dagens utfordrende geopolitiske situasjon mener vi at de godkjente leverandørene bør være norske – norsk kritisk infrastruktur bør kjøres i Norge!

8 Referanser

[1] *Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften)*. 2019. Accessed: Jan. 25, 2023. [Online]. Available: https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157

[2] 'Veiledning til kraftberedskapsforskriften'. NVE. [Online]. Available: https://www.nve.no/energi/tilsyn/kraftforsyningsberedskap-og-kbo/veiledning-til-kraftberedskapsforskriften/

[3] P. Mell and T. Grance, 'The NIST Definition of Cloud Computing', NIST Special Publication 800–145, Sep. 2011. [Online]. Available: https://www.nist.gov/publications/nist-definition-cloud-computing

[4] K. Haver, A.-K. Valdal, T. Vernholt, and H. S. Wiencke, 'Veikart for NVEs oppfølging av IKT-sikkerhet i leverandørkjeden', Proactima, 1074197-RE-01, Dec. 2021. [Online]. Available: https://www.nve.no/media/13231/1074197-re-01-veikart-for-nves-oppf%C3%B8lging-av-ikt-sikkerhet-i-leverand%C3%B8rkjeden-endelig-rapport.pdf

[5] J. Røstum and M. G. Jaatun, 'Informasjonssikkerhet og skybaserte tjenester for vannbransjen (kun digital) | Norsk Vanns Kompetanseweb', Norsk Vann, A 238/2018. Accessed: Oct. 27, 2024. [Online]. Available: https://va-kompetanse.no/butikk/a-238-informasjonssikkerhet-og-skybaserte-tjenester-for-vannbransjen-kun-digital/

[6] T. Zuo, J. Sherman, M. Hamin, and S. Scott, 'Critical Infrastructure and the Cloud: POLICY FOR EMERGING RISK', Atlantic Council, Jul. 2023. [Online]. Available: https://dfrlab.org/wp-content/uploads/sites/3/2023/07/critical_infra_and_the_cloud.pdf

[7] A. G. Hunstad and M. Karresand, 'Molntjänster inom industriella informations-och styrsystem', 2018, Accessed: Oct. 27, 2024. [Online]. Available: https://www.msb.se/siteassets/dokument/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/industriella-informations--och-styrsystem/molntjanster-inom-ics.pdf

[8] *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)*, vol. 333. 2022. Accessed: Nov. 07, 2024. [Online]. Available: http://data.europa.eu/eli/dir/2022/2555/oj/eng

[9] IEC, 'IEC 62443: Industrial communication networks - Network and system security'. IEC. [Online]. Available: https://www.iec.ch/blog/understanding-iec-62443

[10] *Power systems management and associated information exchange – Data and communications security*, IEC 62351, 2018.

[11] *Information technology — Security techniques — Information security risk management*, 27005:2022, 2022. Accessed: Nov. 04, 2022. [Online]. Available: https://www.iso.org/standard/80585.html

[12] P. B. Kristoffersen and K. Omberg, 'Cyber security SIS og egensikre komponenter, kommunikasjonsprotokoller', DNV-GL, 2019–0826, Jan. 2019. Accessed: Nov. 04, 2024. [Online]. Available: https://kudos.dfo.no/dokument/31086/-20220504092757

[13] T. J. Williams, 'The Purdue enterprise reference architecture', *Comput. Ind.*, vol. 24, no. 2–3, pp. 141–158, 1994.

[14] B. A. Kitchenham, 'Systematic review in software engineering: where we are and where we should be going.', in *Systematic review in software engineering: where we are and where we should be going.*, ACM, 2012.

[15] E. Kučera, O. Haffner, P. Drahoš, and J. Cigánek, 'Educational Case Studies for Pilot Engineer 4.0 Programme: Monitoring and Control of Discrete-Event Systems Using OPC UA and Cloud Applications', *Appl. Sci.*, vol. 12, no. 17, 2022.

[16] J. A. Fortoul-Diaz, L. A. Carrillo-Martinez, A. Centeno-Tellez, F. Cortes-Santacruz, I. Olmos-Pineda, and F.-Q. Roberto Rafael, 'A Smart Factory Architecture Based on Industry 4.0 Technologies: Open-Source Software Implementation', *IEEE Access*, vol. 11, pp. 101727–101749, 2023.

[17] Y. Liu, L. Wang, and X. Vincent Wang, 'Cloud manufacturing: latest advancements and future trends', *Procedia Manuf.*, vol. 25, pp. 62–73, Jan. 2018, doi: 10.1016/j.promfg.2018.06.058.
[18] R. Khan, K. McLaughlin, B. Kang, D. Laverty, and S. Sezer, 'A Seamless Cloud Migration Approach to Secure Distributed Legacy Industrial SCADA Systems', presented at the 2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), IEEE, 2020.
[19] B. Jelacic, I. Lendak, S. Stoja, M. Stanojevic, and D. Rosic, 'Security risk assessment-based cloud migration methodology for smart grid OT services', *Acta Polytech. Hung.*, vol. 17, no. 5, pp. 113–134, 2020.
[20] S. Chehida, K. Fellah, E. Rutten, G. Giraud, and S. Mocanu, 'Model-based Self-adaptive Management in a Smart Grid Substation', in *2023 IEEE 28th International Conference on Emerging Technologies and Factory Automation (ETFA)*, IEEE, 2023, pp. 1–8. Accessed: Oct. 27, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10275470/
[21] FSK, 'Sikkerhetsveileder for Kraftsensitiv Informasjon i Skytjenester', Forum for informasjonssikkerhet i kraftforsyningen, Oct. 2021. [Online]. Available: https://fsk-forum.no/wp-content/uploads/2021/11/FSK-Veilder-for-skytjenester-Final-PDF.pdf
[22] T. Onshus *et al.*, 'IKT-sikkerhet og uavhengighet', 2021:01387, 2021. Accessed: Oct. 27, 2024. [Online]. Available: https://kudos.dfo.no/documents/31285/files/27707.pdf
[23] T. Myklebust, T. Onshus, S. Lindskog, M. V. Ottermo, and M. A. Lundteigen, 'Datakvalitet ved digitalisering i petroleumssektoren', SINTEF Digital, 2021:00053, 2021. Accessed: Oct. 27, 2024. [Online]. Available: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2826975
[24] G. K. Hanssen, T. Onshus, M. G. Jaatun, T. Myklebust, M. Ottermo, and M. A. Lundteigen, 'Premisser for digitalisering og integrasjon IT-OT', SINTEF, 2021. Accessed: Dec. 16, 2022. [Online]. Available: https://www.ptil.no/globalassets/fagstoff/prosjektrapporter/ikt-sikkerhet/id6-premisser-for-digitalisering-og-integrasjon-it-ot_sintef-rapportnr-2021-00057-feb--signert.pdf
[25] ENISA, 'Good Practices for Security of Internet of Things in the context of Smart Manufacturing', Nov. 2018. [Online]. Available: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot/
[26] Christina Skouloudi and Gema Fernández, 'Towards secure convergence of Cloud and IoT', ENISA, Report/Study, Sep. 2018. Accessed: Nov. 07, 2024. [Online]. Available: https://www.enisa.europa.eu/publications/towards-secure-convergence-of-cloud-and-iot
[27] M. G. Jaatun and H. Sæle, 'Sett krav til IKT-sikkerhet i anbud og kontrakter', NVE, NVE Eksternrapport 5/2023, Mar. 2023. [Online]. Available: https://publikasjoner.nve.no/eksternrapport/2023/eksternrapport2023_05.pdf
[28] Kjartan Andersland *et al.*, 'Experiences and recommendations from the ECoDiS project', Statnett, IFS 4035877. Accessed: Oct. 27, 2024. [Online]. Available: https://www.statnett.no/globalassets/her-er-vare-prosjekter/region-ost/nettplan-stor-oslo/liasen-transformatorstasjon/ecodis_recommendations-report_june-2024.pdf
[29] M. Salhaoui, A. Guerrero-González, M. Arioua, F. J. Ortiz, A. El Oualkadi, and C. L. Torregrosa, 'Smart Industrial IoT Monitoring and Control System Based on UAV and Cloud Computing Applied to a Concrete Plant', *Sensors*, vol. 19, no. 15, 2019.
[30] *Functional Safety of Electrical/Electronic/Programmable Electronic Safety- Related Systems*, IEC 61508-1:2010, 2010. Accessed: Jul. 11, 2022. [Online]. Available: https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=429346
[31] C. Frøystad, M. G. Jaatun, K. Bernsmed, and M. Moe, 'Risiko- og sårbarhetsanalyse for økt integrasjon av AMS-DMS-SCADA', 2018, Accessed: Oct. 27, 2024. [Online]. Available: https://nve.brage.unit.no/nve-xmlui/bitstream/handle/11250/2633171/eksternrapport2018_15.pdf?sequence=1

[32] Kristine Fiksen *et al.*, 'IKT-systemers rolle og betydning for strukturen i kraftbransjen', NVE, Konsulentrapport utarbeidet for NVE 32–2016. [Online]. Available: https://publikasjoner.nve.no/rapport/2016/rapport2016_32.pdf
[33] DNV, 'Cyber security for power grid protection devices', DNV-RP-0575, Aug. 2021. Accessed: Oct. 27, 2024. [Online]. Available: https://www.dnv.com/cybersecurity/recommended-practices/dnv-rp-0575-cyber-security-for-power-grid-protection-devices/
[34] G. K. Hanssen and M. G. Jaatun, 'Agile Approaches in Critical Infrastructures', presented at the XP 2024, 2024. Accessed: Oct. 27, 2024. [Online]. Available: https://jaatun.no/papers/2024/agile-critical.pdf
[35] Iselin Paulsen, 'Økt motstandskraft og konkurransedyktige virksomheter', Jun. 2024. Accessed: Nov. 04, 2024. [Online]. Available: https://www.cisco.com/c/dam/global/no_no/assets/pdfs/final_05-06-24_rapport-om-okt-motstandskraft.pdf

A Oversikt over akademisk litteratur fra søk

I det følgende presenteres listen med de 20 akademiske artikler fra litteratursøket beskrevet i kapittel 4.1, som ble vurdert som muligens relevante etter vurdering av tittel og sammendrag. Kolonnen "Brukt?" angir om artikkelen er en av de 6 artikler som ble tatt med i beskrivelsen av de fire casene i denne rapporten.

Nr	Tittel	Forfatter(e)	År	Domene	Brukt?
1	Recognizing Value in an Open-Architecture Digital Water System: San Jacinto River Authority's Approach to Becoming a Smart Water Utility	Dent, Shawn; Meeks, Chris; Shindewolf, Aaron; Victor, Meera; Mishra, Pierre	2023	Vann	Nei
2	Model-based Self-adaptive Management in a Smart Grid Substation	Chehida, Salim; Fellah, Karim; Rutten, Eric; Giraud, Guillaume; Mocanu, Stéphane	2023	Smart grid	Ja
3	Educational Case Studies for Pilot Engineer 4.0 Programme: Monitoring and Control of Discrete-Event Systems Using OPC UA and Cloud Applications	Kučera, Erik; Haffner, Oto; Drahoš, Peter; Cigánek, Ján	2022	Produksjon	Ja
4	Lab-Scale Smart Factory Implementation Using ROS	Abdelatti, Marwan; Sodhi, Manbir	2023	Ingen	Nei
5	Security risk assessment-based cloud migration methodology for smart grid OT services	Jelacic, Bojan; Lendak, Imre; Stoja, Sebastijan; Stanojevic, Marina; Rosic, Daniela	2020	Smart grid	Ja
6	A Case Study on Managing the Complexity of Service Failure Modes in IoT Systems	Klabes, Sebastian; Zeller, Marc	2021	Jernbane	Nei
7	Smart manufacturing: State-of-The-Art review in context of conventional & modern manufacturing process modeling, monitoring & control	Mehta, Parikshit; Rao, Prahalada; Wu, Zhenhua David; Jovanović, Vukica; Wodo, Olga; Kuttolamadom, Mathew	2018	Produksjon	Nei
8	Smart industrial iot monitoring and control system based on UAV and cloud computing applied to a concrete plant	Salhaoui, Marouane; Guerrero-González, Antonio; Arioua, Mounir; Ortiz, Francisco J.; El Oualkadi, Ahmed; Torregrosa, Carlos Luis	2019	Sement-produksjon	Ja
9	A Smart Factory Architecture Based on Industry 4.0 Technologies: Open-Source Software Implementation	Fortoul-Diaz, Jesus Anselmo; Carrillo-Martinez, Luis Antonio; Centeno-Tellez, Adolfo; Cortes-Santacruz, Froylan; Olmos-Pineda, Ivan; Flores-Quintero, Roberto Rafael	2023	Produksjon	Ja

Nr	Tittel	Forfatter(e)	År	Domene	Brukt?
10	Development Process for Information Security Concepts in IIoT-Based Manufacturing	Koch, Julian; Eggers, Kolja; Rath, Jan-Erik; Schüppstuhl, Thorsten	2023	Produksjon	Nei
11	Transforming Legacy Production Operations into Smart Asset Operations in Ecuador	Ruiz, Yeniffer Lopez; Carrera, Julia Marlene; Tagarot, Gary Nelson; Gey, Gian Marcio; Davalos, Daniel; Segovia, Ruben Dario; Campana, Danny Rafael; De Jesus Gonzalez, Dario; Azancot, Annalyn Josefina; Briones, Cesar; Pastrana, Wilmar Andrés	2022	Olje og gass	Nei
12	Towards Consolidating Industrial Use Cases on a Common Fog Computing Platform	Denzler, Patrick; Ruh, Jan; Kadar, Marine; Avasalcai, Cosmin; Kastner, Wolfgang	2020	Ingen	Nei
13	CPGrid-OT: Cyber-Power Data Generation Using Real-Time Reconfigurable Testbed for Resiliency	Mustafa, Hussain M; Basumallik, Sagnik; Kidder, Samuel; Srivastava, Anurag	2023	Smart grid	Nei
14	From digital shop floor to real-time reporting: An IIoT based educational use case	Mayer, Barbara; Tantscher, Dominik; Bischof, Christian	2020	Produksjon	Nei
15	A seamless cloud migration approach to secure distributed legacy industrial SCADA systems	Khan, Rafiullah; McLaughlin, Kieran; Kang, Boojoong; Laverty, David; Sezer, Sakir	2020	Smart Grid	Ja
16	Energy consumption analysis in wastewater treatment plants using simulation and SCADA system: Case study in northern Taiwan	Sean, Wu-Yang; Chu, Ya-Yun; Mallu, Lili Lorensia; Chen, Jian-Gu; Liu, Han-Yang	2020	Vann	Nei
17	OPTIMIZING THE COMBUSTIBLE CONSUMPTION USING THE IoT CONCEPT FOR FOUNDRY FURNACES	Florea, B.; Marcu, D.F.; Semenescu, A.; Ioana, A.; Ciurdas, M.; Iacob, G.; Niculescu, F.; Iorga, M.; Hristache, F.	2023	Produksjon	Nei
18	Findings from a Mobile Worker Augmented Reality Enabled Continuous Manufacturing Skid Project	Esko, Iiro; Nachenberg, Andrew; Kelsey, Katelyn; Grossman, Leon	2021	Produksjon	Nei
19	How Different Monitoring Approaches Impact the P-F Model – A Case Study	Hickey, Daryl; Smith, Mikael; Simmonds, Ben; Dinwoodie, Iain	2022	Produksjon	Nei
20	A data-analytic framework to monitor product density of four-effect falling-film evaporator for skimmed milk production	Wagh, Nivedita; Agashe, Sudhir D.	2023	Energi	Nei

NVE

Norges vassdrags- og energidirektorat

Middelthuns gate 29
Postboks 5091 Majorstuen
0301 Oslo
Telefon: (+47) 22 95 95 95