


Prosjekt:

# Fellesaktiviteter Nye sykehus

Tittel:

## Referansearkitektur - Operasjonell teknologi i Helse Sør-Øst

03	Godkjent versjon utgitt			05.05.25	YNGFLA	LIZTAN	ROGBJO
02	Utgitt for gjennomsyn			05.04.25	YNGFLA	LIZTAN	
01	Utgitt for gjennomsyn			05.03.25	YNGFLA	LIZTAN	
Rev.	Beskrivelse			Rev. Dato	Utarbeidet	Kontroll	Godkjent
Kontraktor/leverandørs logo:			Bygg nr:	Etasje nr.:	Systemgr.:	Antall sider:	
						Side 1 av 44	
Prosjekt:		Kontrakt nr:	Fag:	Dok.type:	Løpenr:	Rev.nr.:	Status:
HSØ		8250	F	RA	0013	01	G

Revisjonsendringer

Versjon	Endret av	Beskrivelse av endring	Dato
0.6	Tor Martin S. Skaar	Første høringsrunde.	2024-05-13
0.7	Tor Martin S. Skaar	Andre høringsrunde.	2024-09-13
0.8	Tor Martin S. Skaar	Endringer etter kommentarer og innspill.	2024-11-15
0.81	Yngve Flater-Sandberg	Omorganisering av kapitlene 1 og 2.	2025-01-08
0.9	Yngve Flater-Sandberg Henning Hogness	Godkjenning – ASR Infrastruktur og sky. Lagt til kap. 9.7.	2025-01-29
0.91	Iris Olsen Sandsengen	Lagt over i HSØ mal.	2025-03-03
1.0	Yngve Flater-Sandberg	Godkjenning – SPARK. Omklassifisert til referansearkitektur, endret ordlyd i hele dokumentet. Presisert områder i kap. 8.1. Fjernet kap. 9.7.	2025-03-20
1.1	Yngve Flater-Sandberg Henning Hogness	Innspill/kommentarer HSØ PO.	2025-04-02

Godkjenning

Godkjent av	Navn	Funksjon	Organisasjon	Dato
ASR Infrastruktur og sky				2025-01-15
SPARK				2025-02-03
RARK				2025-05-06

Kontaktpersoner:

ROLLE	NAVN	EPOST	TELEFON
PROSJEKTLEDER	Liz Tandberg	<a href="mailto:liztan@sykehuspartner.no">liztan@sykehuspartner.no</a>	+47 469 30 563
ARKITEKT	Yngve Flater-Sandberg	<a href="mailto:yngfla@sykehuspartner.no">yngfla@sykehuspartner.no</a>	+47 952 05 418

## Ordliste

<b>FORKORTEELSE</b>	<b>BESKRIVELSE</b>
<b>OT</b>	Operasjonell Teknologi
<b>IT</b>	Informasjonsteknologi
<b>SEGMENT</b>	Et segment i nettverket er en del av et nettverk der alle tilkoblede enheter kan snakke direkte med hverandre uten å måtte gå gjennom et filter eller en barriere.
<b>MTU</b>	Medisinteknisk Utstyr
<b>BTU</b>	Byggteknisk Utstyr
<b>BESKYTTELSE</b>	Handlingen eller tilstanden av å sikre noe eller noen mot fare, skade eller uønsket påvirkning. Innebærer å skape en barriere eller utføre tiltak som hindrer negative effekter fra å oppstå. Beskyttelse kan være fysisk (beskyttelse mot vær, vind, brann, hærverk, vold eller uautorisert tilgang), virtuell (beskyttelse som hindrer cybertrusler, hacking, uautorisert tilgang eller annen skadelig digital aktivitet) eller abstrakt (som juridisk beskyttelse av rettigheter).
<b>FAIL-SAFE</b>	Fail-safe er et designprinsipp som sikrer at en enhet eller et system vil innta en sikker tilstand ved en feil eller uforutsett hendelse.

## Innholdsfortegnelse

	Revisjonsendringer .....	2
	Godkjenning .....	2
	Kontaktpersoner: .....	2
	Ordliste 3	
	Figurliste .....	5
1	Innledning .....	6
1.1	Bakgrunn .....	6
1.2	Analyse av nåværende tilstand .....	6
1.3	Behov .....	6
1.4	Omfang .....	7
1.5	Utenfor omfang .....	7
1.6	Bruk .....	7
1.7	Forankring av arbeidet .....	7
1.8	Forvaltning av referansearkitekturen .....	8
1.9	Leseveiledning .....	8
2	Operasjonell Teknologi (OT) .....	9
2.1	Introduksjon .....	9
2.2	Definisjon .....	10
2.3	Funksjon .....	11
2.4	Profil .....	11
3	Prinsipper og føringer .....	14
3.1	OT prinsipper .....	14
3.2	Føringer .....	15
4	Prinsipp #1: Segmentering .....	18
4.1	OT referansemodell .....	18
4.2	IEC 62443: Zones and Conduits .....	19
4.3	Segmentering .....	20
4.4	Operasjonell Teknologi (OT) .....	21
4.5	Informasjonsteknologi (IT) .....	22
5	Prinsipp #2: Arkitekturmønstre og informasjonsflyt .....	22
5.1	Mønster 1: OT informasjonskilde til IT destinasjon .....	22
5.2	Mønster 2: IT informasjonskilde til OT destinasjon .....	23
5.3	Mønster 3: Distribusjonstjenester fra OT .....	24
5.4	Mønster 4: Distribusjonstjenester til OT .....	24
5.5	Mønster 5: Administrasjon av OT komponenter fra IT eller Eksternt .....	25
5.6	Mønster 6: OT produksjonssystem .....	26
6	Prinsipp #3: Regionale løsninger .....	27
6.1	Regional referansemodell .....	27
7	Prinsipp #4: Logging og overvåkning .....	28
8	Prinsipp #5: Risikobasert soneinndeling .....	28
8.1	Systemidentifikasjon .....	28
8.2	Modell for risikobasert soneinndeling .....	29
9	Forutsetninger .....	31
9.1	Sonemodell og segmentering .....	31
9.2	Sikkerhetsarkitektur .....	31
9.3	Digital motstandsdyktighet («resilience») .....	31
9.4	Lokal overlevelse .....	31
9.5	Designprinsipp (krig eller fredstid) .....	31
9.6	Kapabiliteter / innsatsfaktorer .....	32
10	Referanser .....	32

## Figurliste

Figur 1 - HSØ strategiske innsatsområder .....	8
Figur 2 - KIT og fokusområdet for OT .....	9
Figur 3 - Kategorisering av kritikalitet i Helse Sør-Øst .....	12
Figur 4 – OT referansemodell.....	18
Figur 5 - IEC 62443 Zones and Conduits.....	19
Figur 6 - Segmentering av IT OT komponenter og funksjoner .....	20
Figur 7 - OT referansemodell - Teknisk Sone.....	21
Figur 8 - Arkitekturmønster 1: OT til IT.....	23
Figur 9 - Arkitekturmønster 2: IT til OT.....	23
Figur 10 - Arkitekturmønster 3: Distribusjon fra OT .....	24
Figur 11 - Arkitekturmønster 4: Distribusjon til OT .....	25
Figur 12 - Arkitekturmønster 5: Administrasjon av OT komponenter .....	26
Figur 13 - Arkitekturmønster 6: OT produksjonssystem.....	27
Figur 14 - Regional referansemodell IT/OT .....	28
Figur 15 – Flytskjema risikobasert soneinndeling.....	30

# 1 Innledning

## 1.1 Bakgrunn

Sykehuspartner HF (SPHF), i samarbeid med Helse Sør-Øst (HSØ), har over lengere tid sett behov for å standardisere og sikre måten Medisinteknisk utstyr (MTU) (benevnt Medisinsk utstyr (MU) i lovverket) og Byggteknisk utstyr (BTU) behandles på. MTU er utstyr som brukes i pasientbehandling og er essensiell for at spesialisthelsetjenesten skal kunne utføre sin rolle. Det investeres store summer i denne type utstyr og utstyret er å finne på stort sett alle lokasjoner der Helse Sør-Øst utfører behandling. BTU er utstyr som installeres og blir brukt for overvåkning og styring av bygningsmassen og funksjoner knyttet til dette. Byggteknisk utstyr er kritisk for at sykehus eller andre behandlingsinstitusjoner kan brukes til tiltenkt formål.

Sykehuspartner HF utarbeider dette dokumentet som en referansearkitektur for området operasjonell teknologi. Operasjonell teknologi er et begrep som er brukt i forskjellige bransjer for å beskrive miljø som innehar utstyr som påvirker den fysiske verden, og i Helse Sør-Øst faller primært MTU og BTU under denne kategorien.

Sykehuspartner HF har som mål å tilby tjenester til helseforetakene som forbedrer anskaffelse, installasjon, sikkerhet, bruk, drift og forvaltning av denne type utstyr.

## 1.2 Analyse av nåværende tilstand

Denne referansearkitekturen tar utgangspunkt i at det ikke er implementert omfattende arbeid innen arkitektur og helhetlig design av miljø for operasjonell teknologi i Helse Sør-Øst, hverken innen MTU eller BTU. Det eksisterer diverse isolerte modeller, føringer og definisjoner på ulike nivå, men det er ikke utarbeidet en helhetlig arkitektur eller regionale føringer innenfor operasjonell teknologi.

Det nevnes kort arbeid som er gjort som er relevant eller har innvirkning på hvordan referansearkitekturen utformes:

- SIKT har en modell med ett MTU-segment per HF.
- Sykehuset i Østfold HF (SØHF) har en modifisert modell med mer granularitet.
- Akershus universitetssykehus HF (AHUS) har en modell som avviker fra resten av regionen, men denne skal avvikles gjennom migrering av AHUS til regional plattform.
- Oslo universitetssykehus HF (OUS) har en sonemodell som kan separere MTU, BTU og ATU i over 200 individuelt FW- og rutingsregulerte nettverkssegmenter, samt to mikrosegmenterte (NSX-T) hovedsoner på FW-nivå for servere, én for servere med akseptabelt OS/patch/securitynivå og én for servere under akseptabelt nivå. Begge disse serversonene er logisk segmentert for MTU, BTU og ATU.

## 1.3 Behov

Helsesektoren ser en teknologisk utvikling innenfor operasjonell teknologi på samme måte som andre sektorer. Utstyr og systemer blir stadig mer avansert og kommer nå klargjort for flere og flere integrasjoner mot andre systemer. Disse integrasjonene blir fort utnyttet og innlemmet i eksisterende og nye prosesser som igjen resulterer i et økt omfang av både kjente og ukjente avhengigheter. Uten klare føringer, prinsipper og modeller vil dette resultere i uoversiktlige miljø der konsekvensene av feil eller utfall er svært vanskelig å forutse.

Operasjonell teknologi har lenge eksistert hos helseforetakene, men da hovedsakelig betegnet som MTU og BTU med adskilte fagmiljø og organisatorisk separasjon. MTU og BTU har dog mange fellestrekk og har i stor grad like behov, både teknisk og ikke-teknisk.

## 1.4 Omfang

Dette dokumentet beskriver en overordnet teknologisk referansearkitektur for operasjonell teknologi i Helse Sør-Øst. Omfanget av denne referansearkitekturen er å beskrive infrastrukturmessige forhold som må legges til rette for at Sykehuspartner HF skal kunne levere og understøtte bruken av operasjonell teknologi i foretaksgruppen. Dette innebærer arkitekturprinsipper, føringer og referansemodeller for oppbygging av miljø for operasjonell teknologi. Sentrale begrep defineres og beskrives i kapittel 2.

Referansearkitekturen skal bidra med:

- Hjelp til formalisering og forankring av operasjonell teknologi for Helse Sør-Øst
- Definisjon av risikoprofiler for operasjonell teknologi
- Overordnede prinsipper og føringer for operasjonell teknologi
- Referansemodeller og føringer for miljø til bruk for operasjonell teknologi
- Føringer for informasjonsflyt mellom IT og operasjonell teknologi, samt internt innen operasjonell teknologi
- Føringer for plassering av server- og klientutstyr for å understøtte funksjonelle forhold

## 1.5 Utenfor omfang

Ikke-prioritert liste over identifiserte områder som ikke blir tatt med i denne versjonen av referansearkitekturen.

- Internet of Medical Things (IoMT) – IoT/IoMT må ha en egen arkitektur. IoT er i utgangspunktet så forskjellig fra operasjonell teknologi at det ikke gir mening å ta dette med i denne referansearkitekturen. En teknologiarkitektur for IoMT må settes sammen under flere overordnede teknologiske domenearkitekturer da IoMT ikke er et eget teknologiområde, men mer et sammensatt bruk av flere. For IoT er det utarbeidet en egen referansearkitektur (2020).
- Digital hjemmeoppfølging (DHO) – faller teknologisk sett primært under IoMT.

## 1.6 Bruk

Referansearkitekturen gjelder for alle OT-leveranser i Helse Sør-Øst, som klinisk, forskning og bygg aktiviteter. Tiltent bruk av dokumentet er som følger:

- Til bruk av Helse Sør-Øst og helseforetakene for å forankre teknisk og organisatoriske behov
- Til bruk av domenearkitekter for å beskrive en fremtidig tilstand i forbindelse med operasjonell teknologi i helseregionen
- Til bruk av arkitekter for å utarbeide underordnede sammensatte arkitekturer innenfor hensiktsmessige adskilte områder
- Til bruk av prosjekter for å forankre behov og beslutninger

## 1.7 Forankring av arbeidet

I Sykehuspartner HF's Utviklingsplan frem til 2028 forventes det at Sykehuspartner HF:

- kan understøtte økt endringstakt,
- kan akselerere den digitale transformasjonen som helseforetakene står i,

- tilrettelegger for samhandling og gode arbeidsprosesser gjennom effektive, arbeidsbesparende og brukervennlige digitale løsninger, samt deling av informasjoner mellom systemer, og
- bidrar til at helse- og styringsdata kan nyttiggjøres i utviklingen av helsetjenesten.

Det er derfor viktig at Sykehuspartner HF tilrettelegger for og utvikler evnen til å understøtte alle former for tjenester som tilbys pasienter i helsesektoren. Dette gjelder også for operasjonell teknologi, som er en kritisk komponent i behandlingsporteføljen til helseforetakene så vel som kontroll, drift og forvaltning av tekniske komponenter i bygningsmassen.



Figur 1 - HSØ strategiske innsatsområder

## 1.8 Forvaltning av referansearkitekturen

Referansearkitekturen, som beskrevet i dette dokumentet, forvaltes av Sykehuspartner HF's virksomhetsområde Teknologi- og arkitekturstyring (TAS).

Denne referansearkitekturen skal revideres minimum hvert 5. år, men kan i de første leveårene se en hyppigere endringstakt.

## 1.9 Leseveiledning

For å kunne lese og forstå innholdet i dette dokumentet må man ha grunnleggende IT-kompetanse og ha et overordnet forhold til hva operasjonell teknologi er. Det er en fordel å ha evnen til å kunne lese og forstå modeller, føringer og prinsipper på et overordnet nivå og hva dette innebærer for videre arbeide med konkretisering av arkitekturbeskrivelser innenfor definerte områder.

De sentrale kapitlene for definisjon, prinsipp og føringer er:

*Kapittel 2* definerer og beskriver sentrale begreper innen operasjonell teknologi.

*Kapittel 3* gir en oversikt over definerte prinsipper og føringer.

*Kapitlene 4 til 8* utdyper hvert enkelt prinsipp.

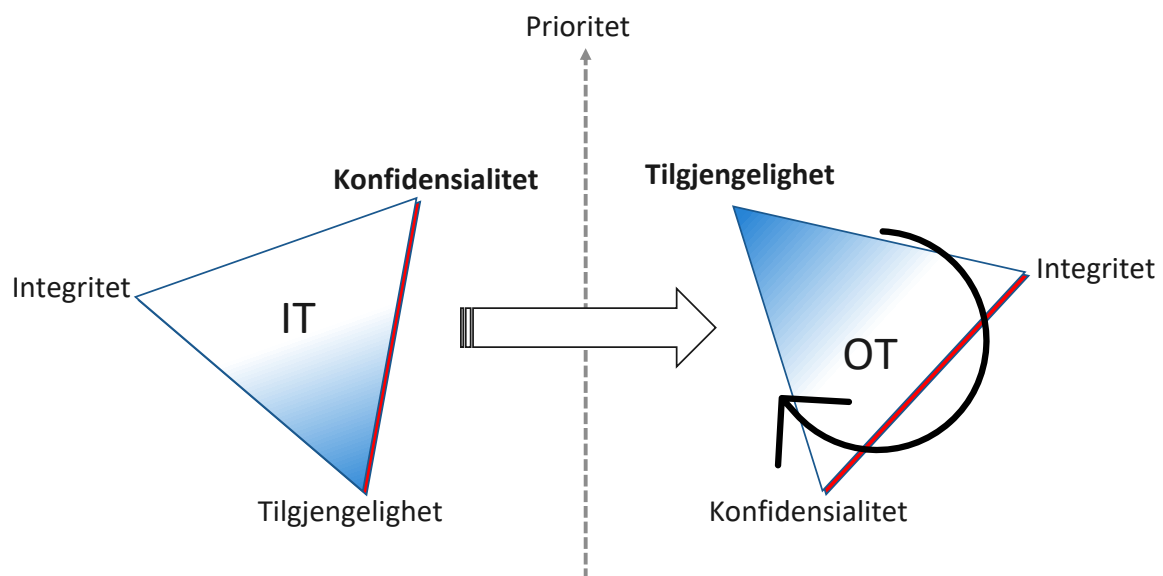


## 2 Operasjonell Teknologi (OT)

### 2.1 Introduksjon

Operasjonell Teknologi (OT) har siden første definisjon av Gartner i 2006 gjennomgått en rekke endringer og tilpasninger til forskjellige sektorer og industrier. Det er dog en enighet om at operasjonell teknologi er, på en eller annen måte, bruk av teknologi for å påvirke eller observere den fysiske verden. For å sikre at Helse Sør-Østs forståelse og bruk av begrepet OT samsvarer med det andre bransjer legger til grunn, benyttes definisjonen fra USAs *National Institute for Standards and Technology (NIST) Special Publication (SP) 800-82r3 – Guide to Operational Technology (OT) security*. Denne definisjonen er bred nok til å omfavne de områdene som er identifisert og den anerkjenner at OT også inkluderer omkringliggende systemer, prosesser og hendelser.

I kort beskriver OT en spesifikk bruk av teknologi der fysisk funksjon og teknologiens tilgjengelighet (les evnen til å kontrollere tingen) er betraktet som den viktigste forutsetningen for suksess. Resten av dokumentet bygger videre på forutsetningen om at i OT beskyttes enhetens og systemets evne til å opprettholde og utføre tiltenkt fysisk funksjon, i motsetning til informasjonsteknologi (IT), der systemets evne til å behandle digital informasjon og beskytte konfidensialiteten er det viktigste. Figur 2 illustrerer denne dreiningen i hvilket sikkerhetsaspekt som er prioritert innen IT og OT.



Figur 2 - KIT og fokusområdet for OT

Innen tradisjonell IT, og beskyttelsen av komponenter og miljø, er det primære fokuset konfidensialitet. Det er hovedsakelig informasjon som skal beskyttes og dersom det er fare for at informasjon kommer på avveie vil det settes inn tiltak for å forhindre dette. **Informasjon** beskyttes ved å, til enhver tid, forsøke å forhindre brudd på konfidensialitet.

For operasjonell teknologi er det *kontroll* som er høyst prioritert, og derfor er tilgjengelighet den viktigste egenskapen, tett etterfulgt av integritet og konfidensialitet. Dersom man mister evnen til å kontrollere utstyret eller prosessen, kan konsekvensene bli betydelige ved at de direkte påvirker fysiske miljøer, og kan i verste fall forårsake skade på eiendeler, miljøkatastrofer eller tap av liv. Innenfor OT beskyttes utstyrets **funksjon**, der det til enhver tid forsøkes å legge til rette for at utstyret skal kunne utføre sin *essensielle funksjon* (beskrives i kapittel 2.3).

Referansearkitekturen etablerer regler og identifiserer attributter som beskriver hvilke deler av Helse Sør-Østs infrastruktur og komponenter som vil bli inkludert av denne definisjonen.

## 2.2 Definisjon

I NIST SP 800-82r3 er definisjonen av Operasjonell Teknologi (OT) slik:

***Et bredt spekter av programmerbare systemer og enheter som observerer og/eller påvirker fysiske miljøer (eller administrerer enheter som gjør dette). Disse systemene og enhetene oppdager eller direkte forårsaker en endring gjennom overvåkning og/eller kontroll av enheter, prosesser og hendelser.<sup>1</sup>***

For spesialisthelsetjenesten betyr dette at operasjonell teknologi hovedsakelig omfatter programvare og applikasjon, komponenter, utstyr, enheter m.m. i kategorien Medisinteknisk Utstyr (MTU) og Byggteknisk Utstyr (BTU), men det kan også være andre områder som naturlig faller under denne definisjonen i fremtiden.

For å gjenspeile definisjonen, og for å kunne klassifisere og ilegge riktige attributter til forskjellige deler av operasjonell teknologi, defineres enheter og systemer som følger:

### ***Enhet (OT enhet)***

*Dette er enheten, utstyret, komponenten eller maskinen som direkte påvirker eller observerer den fysiske (virkelige) verden.*

### ***System (OT system)***

*Dette er samlingen av enhet(er), programvare, applikasjon og/eller funksjon som i sin helhet representerer systemets evne til å utføre en gitt funksjon. Et system må bestå av minst en enhet. Et system kan være en del av et annet system, og et system kan bestå av eller inneholde flere systemer.*

### 2.2.1 OT-enheter i HSØ

Ut fra denne definisjonen og sammen med andre identifiserte behov, defineres et sett med attributter som må være til stede for at en **enhet** skal kunne klassifiseres som OT:

1. *Enheten* må ha en identitet.
2. *Enheten* må direkte kunne påvirke (forårsake en endring) eller tolke (gjennom observasjon og analyse) den fysiske (virkelige) verden.
3. *Enheten* kan være maskinvare og programvare.
4. *Enhetens* behov for beskyttelse er primært knyttet til tingens evne til å utføre en tiltenkt fysisk funksjon, både maskinvare og programvare inkludert i enheten.
5. *Enheten* må kunne kommunisere med andre via bransjestandard digitale kommunikasjonsløsninger.
6. *Enheten* må kunne konfigureres, via
  - a. et innebygget brukergrensesnitt, via
  - b. et administrativt fjernstyringsverktøy, eller via
  - c. elektriske innganger.

<sup>1</sup> Original engelsk tekst finnes her: <https://csrc.nist.gov/pubs/sp/800/82/r3/ipd>

## 2.2.2 OT-enheter og -systemer i HSØ

En enhet eller et system er i Helse Sør-Øst betraktet som OT dersom det faller inn under én eller flere av følgende påstander:

1. *Enheten* er et MTU, et BTU, eller noe annet som observerer eller direkte påvirker fysiske miljøer,
2. Det er et *system* som direkte eller indirekte støtter *enhets* primære funksjon og det er et *system* der funksjonalitet må opprettholdes i en beredskapssituasjon, eller
3. Det er et *system* som gir tilgang til sanntid eller nær-sanntids OT-informasjon/data og
  - brukes i aktiv pasientbehandling, eller
  - informasjonen er kritisk for styring av en prosess, og som
  - ikke er betraktet som et arkivverktøy/oppslagsverk.
4. Det er et *system* som brukes for å administrere/styre *enheter* som beskrevet i pkt. 1-3

## 2.3 Funksjon

**Normalfunksjon** er en eller flere funksjoner i et system, som er tatt i bruk, og er derfor betraktet som systemets normale og forventede virkemåte.

**Essensiell funksjon** er en eller flere funksjoner som et system må tilby for at systemet skal betraktes som funksjonelt på et absolutt minimumsnivå.

## 2.4 Profil

Enheter og systemer innenfor operasjonell teknologi vil ha et beskyttelsesbehov som er forskjellig fra tilsvarende enheter og systemer innenfor informasjonsteknologi. Behovet for beskyttelse er sterkt knyttet til enheten og systemets funksjon innenfor byggteknisk og klinisk virksomhet.

Beskyttelsesbehovet fokuserer på:

- Sikring i form av evnen til kontinuerlig kontroll av en funksjonell prosess.
- Kontinuitet i form av at når ting er påbegynt, så må det ha evnen til å fullføre oppgaven.
- Sikre utstyrets evne til å opprettholde forutsigbar integritet i output.
- Sikre utstyrets evne til å utføre essensiell funksjon.

En OT-profil kartlegger forskjellige dimensjoner innenfor krav til en funksjon. Elementer som kan inngå er:

1. Kritikalitetsklasse (se kapittel 2.4.1)
2. Konsekvensklasse (se kapittel 2.4.2)
3. Hvordan løses redundans?
  - a. Duplisering
  - b. Erstatningsfunksjon
  - c. Ingen
4. Informasjonsklasse
  - a. Inneholder systemet informasjon som må hensyntas?
5. Miljøklasse
  - a. Produksjon eller ikke-produksjonsmiljø?
6. Robusthet
  - a. Er enheten eller systemet i seg selv robust?
  - b. Hvor mye kan enheten eller systemet beskytte seg selv (egenbeskyttelse)?
7. Essensiell funksjon (hva er utstyrets essensielle funksjon?) og normalfunksjon

- a. Tidskritikalitet
  - b. Hva er konsekvensene (for gruppe mennesker eller individer)
  - c. Teknologiske avhengigheter
  - d. Ikke-teknologiske avhengigheter
8. Behov for support (24/7, 8-16)
  9. Grad av tilgang for utedkommende

OT profilen og tilhørende risikoprofil foreslås beskrevet i eget policydokument NO-xx [må utarbeides], tilsvarende det som finnes for informasjonsklassifisering i NO-53.

## 2.4.1 Om Kritikalitet

Kritikalitetstabellen i «Bilag 5 – Tjenestenivå med standardiserte kompensasjoner»<sup>2</sup> (Figur 3) brukes i HSØ for å sette en tjenestes kritikalitetsnivå. Tjenester vil være klassifisert etter hvor kritiske tjenestene er, det vil si etter hvilke konsekvenser nedetid vil medføre. Sykehuspartner leverer drift, beredskap og feilretting for å understøtte disse klassene.

Kritikalitet	Kriterier
1	<b>MEGET KRITISK:</b> Tjenester hvor stopp er eller kan være livstruende for pasienter, kan medføre feilmedisinering, eller er kritisk for virksomhetens drift.
2	<b>KRITISK:</b> Tjenester hvor stopp får alvorlige konsekvenser, som eksempelvis: <ul style="list-style-type: none"><li>• kan medføre at pasientgrupper/publikum taper tillit til Kunden</li><li>• kan medføre betydelig merarbeid for personell</li><li>• kan medføre tapt effektivitet</li></ul>
3	<b>MINDRE KRITISK:</b> Tjenester hvor stopp har mindre konsekvenser hos Kunden, som eksempelvis: <ul style="list-style-type: none"><li>• ikke medfører tapt tillit hos Kunden</li><li>• kan medføre økonomiske konsekvenser ved lengre nedetid</li><li>• kan medføre noe merarbeid for personell</li></ul>

Figur 3 - Kategorisering av kritikalitet i Helse Sør-Øst

Mye av OT vil ofte havne i kategorien kritikalitet 1 – Meget Kritisk, men det er ikke noe direkte sammenheng som sier at dersom det er OT, så er det Meget Kritisk. Det er heller ikke gitt at dersom systemer er Meget Kritiske, så er det OT.

Kritikalitetsklasser sier noe om hvilke konsekvenser nedetid vil medføre. Resultatet av at en tjeneste blir klassifisert som en kritikalitetsklasse gir føringer for hvilke sikkerhetstiltak som skal benyttes.

Denne grupperingen brukes som et av underlagene til å foreslå enhetens eller systemets OT profil, som benyttes for å klargjøre enhetens og systemets skjermingsbehov og innplassering i HSØ infrastruktur.

## 2.4.2 Om Konsekvensklasser

Som vist i kapittel 2.4.1, er kritikalitetsklasser laget for å si noe om en tjenestens (applikasjonens) viktighetsgrad for helseregionen. Kritikalitetsklasser mangler dog evnen til å kunne si noe om viktigheten på enheter og systemer i liten skala, for eksempel et enkelt MTU eller en byggnær-funksjon.

<sup>2</sup> [https://sykehuspartner.fisp.no/Delte%20dokumenter/Tjenesteavtalen\\_Bilag%205%20-%20Tjenesteniv%C3%A5%20med%20standardiserte%20kompensasjoner\\_20210101%20med%20synlige%20endringer.docx](https://sykehuspartner.fisp.no/Delte%20dokumenter/Tjenesteavtalen_Bilag%205%20-%20Tjenesteniv%C3%A5%20med%20standardiserte%20kompensasjoner_20210101%20med%20synlige%20endringer.docx)

OT konsekvensklasser introduseres for å bidra til riktig profilering av enheter og systemer basert på enheten og systemets tiltenkte funksjon. Dette gjøres for å kunne implementere tilstrekkelig og riktig beskyttelse av enheten og systemet i lokal størrelsesorden og for å sikre utstyrets evne til å utføre essensiell funksjon.

Referansearkitekturen foreslår å operere med fire OT-konsekvensklasser som beskrevet i tabellen under.

KLASSE	KONSEKVENNS
1	OT laget for å direkte kontrollere en funksjon av kritisk betydning for Helse, Miljø og Sikkerhet. Bortfall eller feil på funksjonen resulterer direkte i en «hendelse» som kan forårsake umiddelbar fare for <ol style="list-style-type: none"><li>tap av menneskeliv,</li><li>avbrutt behandling,</li><li>feilmedisinering,</li><li>negativ påvirkning på miljø og sikkerhet</li></ol>
2	OT som utfører en funksjon som understøtter prosesser og der bortfall eller feil på funksjonen forårsaker en <ol style="list-style-type: none"><li>forsinkelse i pasientbehandlingen</li><li>reduksjon av kvalitet i pasientbehandlingen</li><li>reduksjon av kapasitet for pasientbehandling</li><li>nedsatt evne til å varsle om unormale og uønskede hendelser</li><li>reduksjon av byggeteknisk funksjon</li><li>nedsatt evne til å ivareta hensiktsmessig tilgangskontroll</li></ol>
3	OT som er designet for å observere og analysere den virkelige verden, for så å representere den i form av et digitalt format. Resultatet fra funksjonen må verifiseres av en tredjepart (fagekspert). Feil eller bortfall av funksjonen kan resultere i <ol style="list-style-type: none"><li>manglende underlag for beslutning</li><li>forsinket eller feil beslutning</li><li>ineffektive prosesser</li></ol>
4	Øvrig - feil signal eller bortfall av funksjonen har ingen umiddelbare kritiske konsekvenser.

Denne grupperingen brukes som et av underlagene til å foreslå enhetens eller systemets OT profil.

## 3 Prinsipper og føringer

Det skal bygges en helhetlig arkitektur for OT i Helse Sør-Øst ved å følge et sett med prinsipper og føringer beskrevet i dette kapittelet.

### 3.1 OT prinsipper

<b>Prinsipp nr.</b>	<b>1</b>
<b>Navn</b>	<b>Segmentering</b>
<b>Beskrivelse</b>	Kommunikasjon og trafikkflyt internt i OT, samt mellom OT og IT, skal følge de retningslinjene beskrevet i denne referansearkitekturen, mer spesifikt referansemodellen som beskrevet i kapittel 4.
<b>Rasjonale</b>	Det bygges et eget miljø tilpasset OT for å kunne oppnå tilstrekkelig beskyttelse av tjenester, systemer, applikasjoner, komponenter og utstyr.
<b>Implikasjon</b>	Infrastrukturen får et eksplisitt og definert skille mellom IT og OT. Dette gir mulighet for å beskytte Operasjonell Teknologi bedre og gir en forutsigbarhet i forhold til plassering av leveranser.

<b>Prinsipp nr.</b>	<b>2</b>
<b>Navn</b>	<b>Arkitekturmønstre</b>
<b>Beskrivelse</b>	OT-løsninger skal følge et av arkitekturmønstrene som er definert i dette dokumentet (se kapittel 5). Løsninger som ikke lar seg tilpasse til et av arkitekturmønstrene skal registreres som avvik.
<b>Rasjonale</b>	Det er definert opp et sett med arkitekturmønstre for å kunne standardisere på hvordan systemer og løsninger blir bygget. Dette vil gi forutsigbarhet ved behov for drift, support, kompetanse og maskinvare for å understøtte våre leveranser. Dette vil også bidra til en bedre måte å skalere opp sikkerhetsarbeidet for å opprettholde sikkerheten og dekke beskyttelsesbehovet til løsningene.
<b>Implikasjon</b>	Arkitektur og design av løsninger vil måtte forholde seg til disse arkitekturmønstrene når nye løsninger skal realiseres. Dette gir mulighet for å lage standard- og mønsterdesign som kan gjenbrukes som «byggeklosser». Etablering og behov for sikkerhetsovervåkning vil bli mer forutsigbart og den totale sikkerheten i helseregionen vil øke som et resultat av at man i en mye større grad vet hva som skal beskyttes og hvordan dette kan utføres.

<b>Prinsipp nr.</b>	<b>3</b>
<b>Navn</b>	<b>Regional løsning</b>
<b>Beskrivelse</b>	Det skal benyttes standardiserte plattformer og løsninger for å kunne bygge likt der det lar seg gjøre, men som ved behov også muliggjør og understøtter lokal tilpasning, utvikling og innovasjon.
<b>Rasjonale</b>	For å kunne oppnå stordriftsfordeler og kunne dra effekt av standardisering er det en ambisjon om å gjøre like ting likt. Prinsippet om regional løsning betyr at man i større grad skal gjøre anskaffelser og tilrettelegge for å gjenbruke løsninger og systemer i hele regionen.
<b>Implikasjon</b>	Sykehuspartner HF vil kunne optimalisere leveranse, drift og forvaltning av løsninger da man i en større grad vil kunne gjenbruke deler av, eller komplette leveranser til to eller flere helseforetak.

<b>Prinsipp nr.</b>	<b>4</b>
<b>Navn</b>	<b>Logging og overvåkning</b>
<b>Beskrivelse</b>	Kontinuerlig overvåkning av nettverkstrafikk, samt logging av aktiviteter for å kunne avdekke og analysere sikkerhetshendelser.
<b>Rasjonale</b>	For å kunne levere på kravene som dataansvarlig og som infrastrukturleverandør til foretaksgruppen, må Sykehuspartner HF, til enhver tid, kunne si noe om status i infrastrukturen og på de tjenestene Sykehuspartner HF har ansvaret for.
<b>Implikasjon</b>	Sykehuspartner HF vil få tilstrekkelig innsyn i infrastrukturen til å oppdage hendelser (sikkerhet, driftsmessig eller andre) som har et mulig negativt utfall. Sammen med de andre prinsippene vil man også ha gode muligheter til å begrense spredning og omfang og konsekvenser av hendelsen.

<b>Prinsipp nr.</b>	<b>5</b>
<b>Navn</b>	<b>Risikobasert soneinndeling</b>
<b>Beskrivelse</b>	«IEC 62443-3-2 - Security risk assessment for system design» følges for å dele et system inn i hensiktsmessige soner.
<b>Rasjonale</b>	Sykehuspartner HF skal ha en risikostyrt tilnærming til sikkerhet. Sykehuspartner HFs miljøer og infrastruktur deles opp ved å basere seg på prosesser for å identifisere behov for sikkerhet og isolasjon ved å bruke en anerkjent standard og godt etablerte prosesser.

<b>Prinsipp nr.</b>	<b>5</b>
<b>Implikasjon</b>	Soneinndeling vil som et resultat av dette prinsippet bli forutsigbart, dokumenterbart og funksjonelt. Vi vil kunne garantere for at beskyttelses- og sikkerhetsbehovene er ivaretatt og er tilstrekkelig i forhold til dokumenterte prosesser. Dette vil bidra til riktig bruk av midler og innsats for å få tilstrekkelig beskyttelse av tjenester og systemer.

## 3.2 Føringer

### 3.2.1 Kommunikasjon med andre miljø

Kommunikasjon inn og ut fra OT-miljøer skal ha et dokumentert behov og ha tilstrekkelig overvåkning og beskyttelse.

### 3.2.2 Leverandøraksess (fjerntilgang)

Fjerntilgang for leverandører skal følge gjeldende krav og føringer for fjerntilgang. Leverandørers løsninger for fjerntilgang (e.g. VPN) må bruke Helse Sør-Østs infrastruktur for å nå systemet eller tjenesten.

### 3.2.3 Trygghetsfunksjoner («safety»)

Miljøparametere (sikkerhetskontroller, brannmurer, agenter, etc.) som innføres må ikke gå på bekostning av utstyrets evne til å utføre trygghetskritiske funksjoner, jf. Safety Instrumented Function (SIF)<sup>3</sup>.

### 3.2.4 “Break-the-glass” prosedyrer

Det skal foreligge prosedyrer og retningslinjer for å få tilgang til, og kontroll på, utstyret ved en ekstraordinær hendelse som forhindrer normal tilgang og kontroll av utstyret. Det skal også etableres en prosess som går gjennom og verifiserer at denne tilgangen blir brukt etter hensiktene. Denne definisjonen er også ofte omtalt som «Firecall»-metode.

### 3.2.5 “Fail-safe” (“fail-to-safe”) konfigurasjon

Utstyret og systemet skal ha mulighet for å konfigureres opp på en slik måte at dersom utstyret eller systemet opplever en feilsituasjon og som følger av dette ikke kan utføre tiltenkt funksjon, så skal utstyret eller systemet opphøre funksjonen på en slik måte at sikkerhet (trygghet) er ivaretatt.

### 3.2.6 Oppdage nettverksinntrenging («Network Intrusion Detection»)

Sykehuspartner HF skal ha mulighet for overvåkning av nettverksaktivitet helt ut til kant og ha mulighet til å oppdage og varsle om unormale tilstander og hendelser.

### 3.2.7 Nettverksisolasjon

Sykehuspartner HF skal ha mulighet for å isolere et enkelt segment for å forhindre at sårbarheter kan utnyttes på tvers av segmenter eller mot sentrale applikasjoner.

Sykehuspartner HF skal ha mulighet til enkelt å isolere OT fra IT på en måte som opprettholder OT systemers evne til å utføre essensiell funksjon.

<sup>3</sup> Safety Instrumented Function (SIF) er et beskyttelseslag som har som formål å oppnå eller vedlikeholde en trygg tilstand til en prosess eller et system dersom en spesifikk farlig hendelse oppstår. Denne funksjonen er ofte implementert i et Safety Instrumented System (SIS) som vanligvis inneholder flere SIF. SIS er ofte implementert ved å bruke egne kontroller for styring av prosesser slik at det ikke er avhengig av det primære kontrollsystemet.

### 3.2.8 Sikkerhetsmonitorering

Sykehuspartner HF skal ha mulighet til å overvåke, med det formål om å detektere skadevare og tegn på kompromittering, på utstyr, infrastruktur, applikasjon og system i OT. Disse skal, så langt det lar seg gjøre, sende sikkerhetslogger til regionalt loggmottak for analyse.

Sykehuspartner HF's organ for sikkerhetsovervåkning, CERT, skal kunne detektere trusler og hendelser ved bruk av flere deteksjonsmekanismer, e.g. signaturbasert, anomali/oppførselsdeteksjon o.l., slik at man kan oppdage både kjente trusler og skadevarer så vel som hendelser basert på bruk av legitime verktøy og funksjoner («living of the land»).

Sikkerhetsovervåkning skal kunne utføres helhetlig, på tvers av IT og OT. Dette for å kunne oppdage trusler på tvers av miljøene.

### 3.2.9 Statusmonitorering

Sykehuspartner HF skal ha oversikt over en enhets nåværende funksjonelle status. Funksjonell status kan bl.a. være:

- PÅ/AV
- RUN/IDLE/WAITING
- ERROR

#### 3.2.10 Enhetsregister («Asset inventory»)

Sykehuspartner HF skal ha detaljert og oppdatert oversikt over alle komponenter som er tilkoblet OT-infrastrukturen.

#### 3.2.11 Nettverksaksesskontroll («Network Access Control»)

Nettverket skal kunne identifisere, autentisere og autorisere komponenter. Dette kreves der dette ikke går på bekostning av komponentens primærfunksjon eller evne til å utføre essensiell funksjon.

#### 3.2.12 Kommunikasjon

Kommunikasjon i OT skal bruke bransjestandardprotokoller.

#### 3.2.13 Kryptering

Kryptering av trafikk og data i OT skal følge Helse Sør-Østs retningslinjer for kryptering med unntak av de tilfellene der det går på bekostning av komponentens evne til å utføre sin primærfunksjon eller dette strider med juridiske forhold.

Krav til kryptering av trafikk og data innenfor avgrensede nettverkssegmenter, system eller miljø kan sløyfes dersom det eksisterer juridiske eller funksjonsmessige grunner til dette.

#### 3.2.14 Erstatningsutstyr

Utstyr som understøtter en komponent eller et system skal enten bygges med tilstrekkelig redundans eller at utstyret kan byttes med reservedel som er tilgjengelig lokalt.



### **3.2.15      Kontaktpunkt**

Sammen med utstyret skal det alltid foreligge eller henvises til informasjon om utstyrets eier, samt utstyrets kontaktpunkt ved feil.

### **3.2.16      Dataeksport**

Sykehuspartner HF legger til rette for at data og informasjon som sier noe om enheten og systemets tilstand skal kunne sendes til leverandør/produsent for behandling uavhengig av plassering av utstyret.

### **3.2.17      Data og kontrollplan**

Det skal, i hensiktsmessig grad, skilles på data og kontrollplan for enheter og systemer.

### **3.2.18      Støtte for essensiell funksjon**

*Essensiell funksjon* representerer utstyrets evne til å opprettholde et sett med minimumsfunksjoner under og etter en utnyttelse av en svakhet. «Opprettholde» betyr her at utstyret skal gå over i en trygg tilstand, enten ved å stoppe funksjonen helt eller ved å utføre en minimumsfunksjon innenfor pre-definerte trygge rammer. Innføring av sikkerhetstiltak skal ikke negativt påvirke utstyrets evne til å opprettholde essensiell funksjon. Se også føringer i kapitlene 3.2.3 og 3.2.5.

### **3.2.19      Kompenserende tiltak**

Dersom enhetens tekniske kapabiliteter ikke er tilstrekkelig for å oppnå ønsket sikkerhetsnivå, bør det innføres kompenserende tiltak utenfor utstyret.

## 4 Prinsipp #1: Segmentering

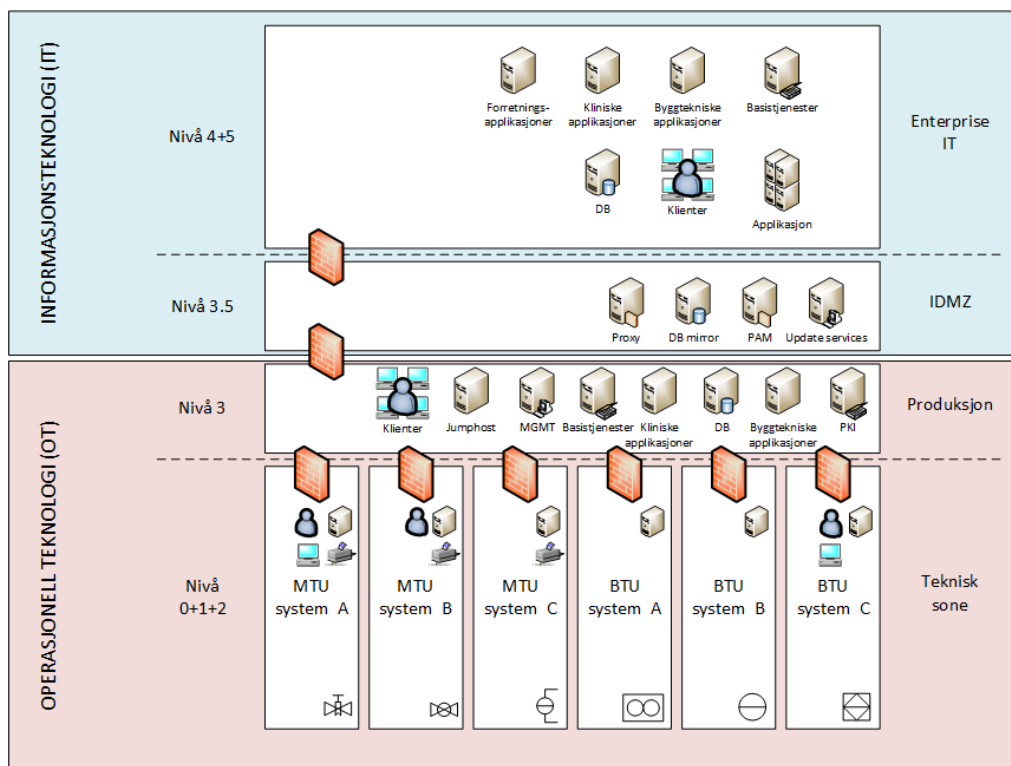
Sykehuspartner HF's OT prinsipp #1 handler om segmentering. Formålet med å segmentere OT-miljø i forskjellige soner er bl.a. for å redusere risiko for spredning av skadevare på tvers av infrastrukturen, en større forutsigbarhet i form av enklere leveranser og oppbygging av infrastruktur som understøtter mønsterdesign og mønstre for informasjonsflyt, samt klare grensesnitt mellom funksjonelle deler av Helse Sør-Østs infrastruktur.

### 4.1 OT referansemodell

Helse Sør-Øst følger den overordnede modellen definert i *Purdue Enterprise Reference Model (PERA)* med tillegg av en *Industrial Demilitarized Zone (IDMZ)*. Dette er samme referansemodell som brukes av den internasjonale standarden for industriell cybersikkerhet; IEC 62443 og det Amerikanske rammeverket NIST SP 800-82r3 Guide to Operational Technology (OT) Security.

Denne referansemodellen brukes til å bygge et grunnlag for stabil, sikker og forutsigbar drift av OT-systemer. Ekspisitt i denne modellen ligger det et sterkt definert grensesnitt mellom IT og OT. Dette må opprettholdes på tvers av teknologiske og ikke-teknologiske domener for å kunne understøtte stabil drift i fredstid, så vel som i krise, konflikt og krig.

Modellen deler virksomheten opp i to miljø: Informasjonsteknologi (IT) og Operasjonell Teknologi (OT). Innenfor hver av disse er det delt opp i forskjellige nivå basert på en funksjonell tilnærming. Se figur 4.



Figur 4 – OT referansemodell

Overordnet beskrivelse av nivåene 0-5:

- **Nivå 0, 1 og 2** defineres av den funksjonelle løsningen og er der selve OT-enhetene, inkludert tilhørende lokale systemer, er plassert. Nivå 0 og 1 er ofte omtalt som «Feltnivå».
- **Nivå 3** definerer nivået for systemer og tjenester som enten *understøtter behov definert av systemer i tekniske soner* eller er *sentrale komponenter som deles av flere tekniske løsninger*. Dette er en felles

sone for alt av støttesystemer i underliggende nivå. Her finner vi toppnivåsystemer, felleskomponenter som basistjenester, samt at OT plattformtjenester (PaaS) realiseres i denne sonen.

- **Nivå 3.5** er en sone for kontroll av informasjonsflyt mellom IT og OT. Denne sonen inneholder systemer og tjenester som muliggjør sikker kommunikasjon mellom enheter, systemer og tjenester i IT og OT. Denne sonen skal ikke inneha tjenester eller funksjonalitet som forhindrer produksjon (påvirker essensiell funksjon) dersom den blir utilgjengelig. Sonen skal heller ikke inneholde løsninger for permanent lagring av data. Data som befinner seg i denne sonen vil alltid være midlertidig (mellomlagret, bufret, etc.).
- **Nivå 4 og 5** definerer normale IT soner. Det tas i utgangspunktet ikke hensyn til opprinnelig forskjell på nivå 4 og 5 fra PERA, men beholder definisjonen her av kompatibilitetshensyn og mulig fremtidig bruk.

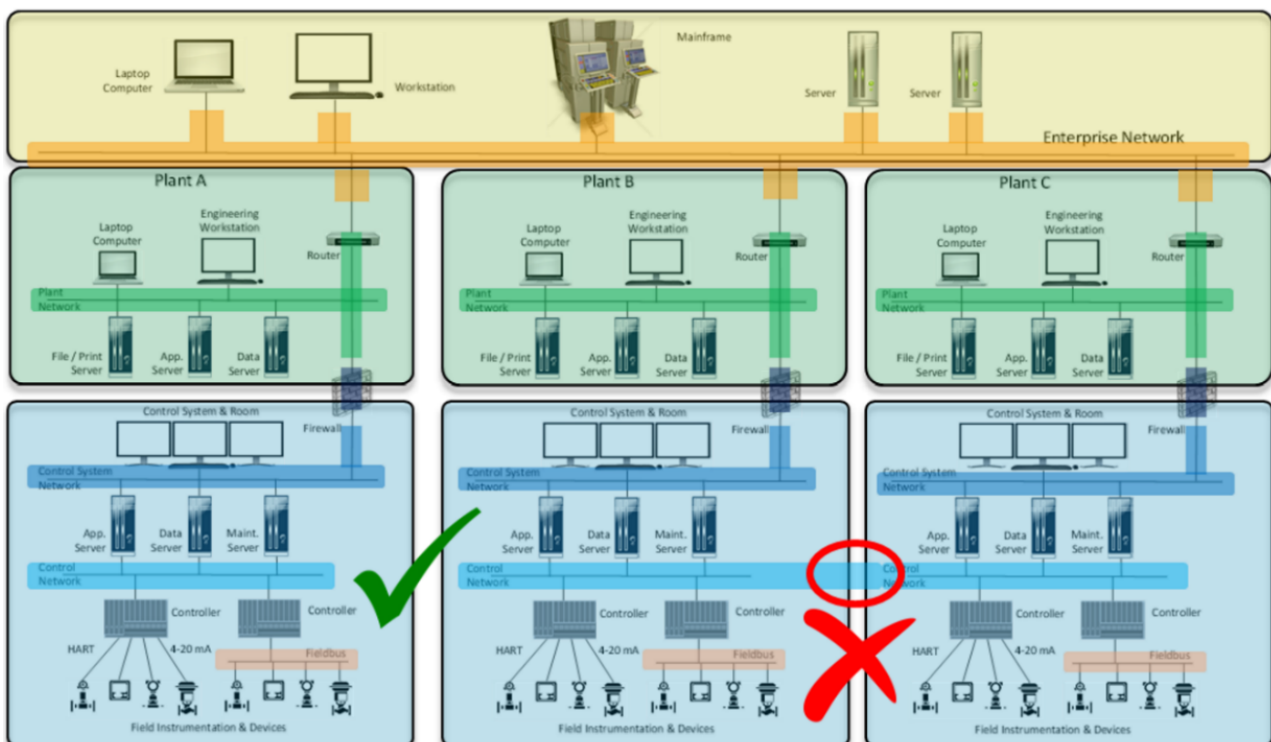
Nivåene beskrives videre i kapitlene 4.4 (OT) og 4.5 (IT).

## 4.2 IEC 62443: Zones and Conduits

IEC623443-1-4s definisjon av *Zones and Conduits* benyttes. Konseptet “IEC 623443 Zones and Conduits” – se Figur 5, benyttes ikke bare for å beskrive sonene i Helse Sør-Østs modell, men den beskriver også kommunikasjonsobjekter mellom disse. Et slik kommunikasjonsobjekt kalles «Conduit» og er en abstrakt virtuell definisjon av en kommunikasjonskanal. En slik kommunikasjonskanal har to primære bruksområder der den beskriver:

1. en kommunikasjonskanal mellom utstyr med samme krav til sikkerhet
  - a. vert til vertskommunikasjon i samme nettverkssegment
  - b. vert til infrastrukturkommunikasjon i samme nettverkssegment
2. en kommunikasjonskanal mellom **to** komponenter som representerer forskjellige sikkerhetsnivå
  - a. brannmur til brannmurkommunikasjon

En viktig egenskap til modellen (som visualisert i Figur 5) er at kommunikasjon mellom soner går via høyere nivå.



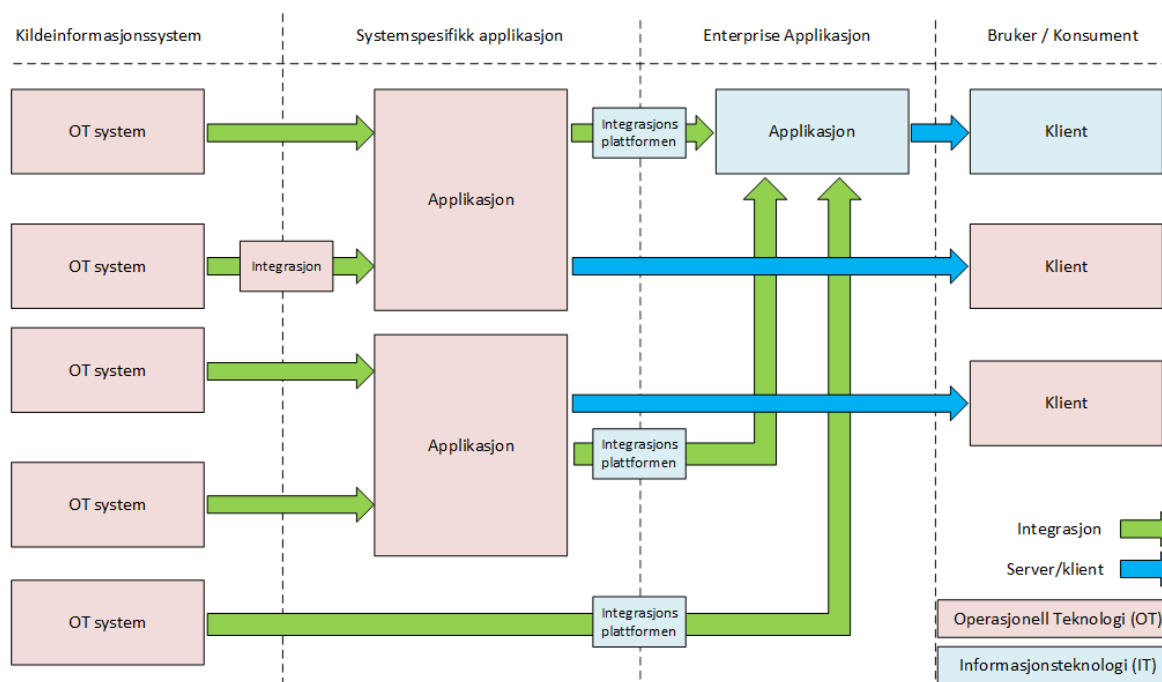
Figur 5 - IEC 62443 Zones and Conduits

## 4.3 Segmentering

Det opprettes et klart skille mellom IT og OT for å oppnå tilstrekkelig:

- **beskyttelse** (beskytte informasjon og funksjon, samt forhindre at en kompromittering i et miljø påvirker et annet, på kort sikt),
- **forutsigbarhet** (oppførsel til systemer og tjenester er kjent gitt endrede forutsetninger i miljø), og
- **operasjonelle behov** (patch management, life-cycle management, driftsmodell, service-partner, etc.)

Denne segmenteringen omhandler infrastruktur, identitetstjenester, dokumentasjon, støttesystemer, overvåkning, prosesser, rutiner og andre behov som identifiseres som nødvendige for å understøtte produksjonen. Et eksempel på dette er vist i Figur 6 og er videre forklart i kapitlene 4.3.1 og 4.3.2.



Figur 6 viser sammenhengen mellom kilde, mellomvare og klient. For å øke motstandsdyktighet og robusthet muliggjøres bruk av systemspesifikk applikasjon via dedikerte klienter lokalisert i OT-miljøet. Disse klientene beskyttes og følger samme overordnede livssyklusstyring som kildesystemene. Dette forsikrer at kritiske systemer og funksjonalitet kan benyttes selv om nødvendigheten for isolasjon av OT-miljøet oppstår som følge av en utilsiktet eller bevisst handling.

### 4.3.1 Klientutstyr

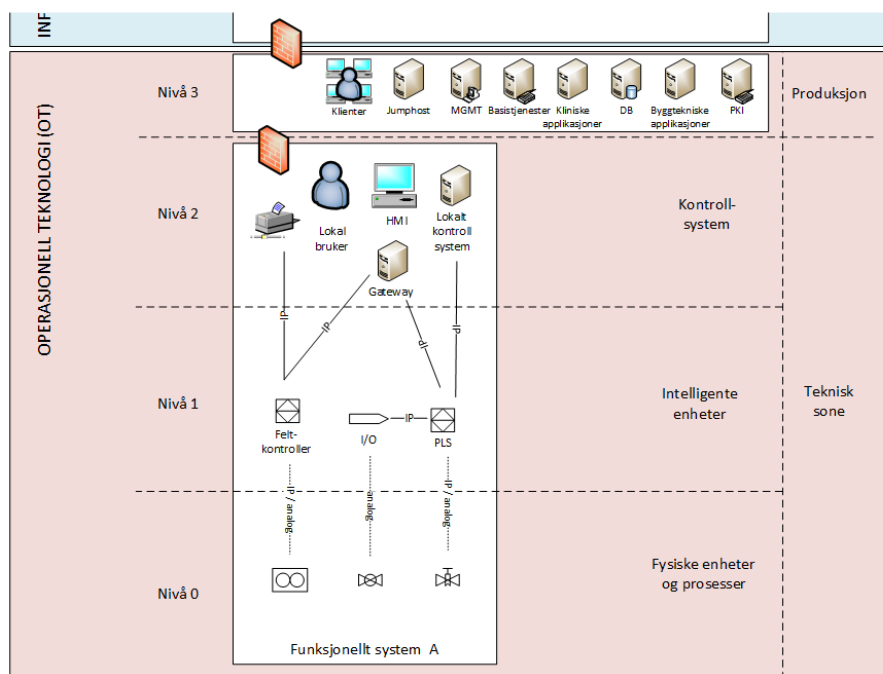
Plassering av klientutstyr må vurderes i hvert enkelt tilfelle, og dette må samsvare med bruksbehov, integrasjonsbehov, beredskapsbehov og funksjonelle behov. Som en generell føring skal en klient stå i det segmentet der det blir minst mulig forhindret i å utføre tiltenkt oppgave skulle det oppstå behov for å isolere IT fra OT.

### 4.3.2 Server/tjenerutstyr/applikasjon

Plassering av tjenere (maskinvare og/eller plattform for å kjøre applikasjoner) må gjøres i henhold til tiltenkt funksjon og behov for kommunikasjon med kildeinformasjonssystemer. Et kildeinformasjonssystem kan være selve medisinske utstyret (MTUet), et styringssystem til f.eks. heis eller ventilasjon, eller andre typer operasjonell teknologi som brukes for å tolke eller styre funksjoner i den fysiske verden.

## 4.4 Operasjonell Teknologi (OT)

OT-delen av infrastrukturen er hovedsakelig delt opp i to typer soner; en **produksjonssone** (nivå 3) og en eller flere **tekniske soner** (nivå 0 – 2), se figur 7.



Figur 7 - OT referansemodell - Teknisk Sone

### 4.4.1 Produksjon

Produksjonssonen (nivå 3) inneholder komponenter, systemer, applikasjoner og tjenester som understøtter egen og tekniske soners behov. Dette er bl.a. nettverkstekniske komponenter og basiskapabiliteter (DNS, DHCP, NAC, NTP, etc.), applikasjons- og tilgangsløsninger, identitetsløsninger og arbeidsflater for brukere som jobber mot OT systemer. Denne sonen kan også inneholde produksjonssystemer og toppnivåsystemer.

### 4.4.2 Teknisk sone

En Teknisk Sone (også kjent som *area/cell* fra PERA, se Figur 7) inneholder de lokale OT-enhetene og -systemene som er involvert i realiseringen av en funksjon.

I nivå 0 finnes sensorer, aktuatorer, ventiler, motorer eller andre enheter som forårsaker en endring eller direkte leser og tolker den fysiske verden.

I nivå 1 finnes lokale kontrollkomponenter som direkte kontrollerer utstyr i nivå 0 og er med på å bygge opp et system. Et system er en samling av enheter og systemkomponenter som samlet sett er i stand til å utføre en eller flere spesifikke oppgaver. Enhetene her, ofte kalt intelligente enheter, har ofte mulighet for Ethernet og IP-basert kommunikasjon. Nivå 0 og 1 blir ofte samlet omtalt som et «felt» eller «feltnivå».

I nivå 2 finnes lokale kontrollsystem som administrerer og kontrollerer en eller flere systemer og enheter. Her er det også komponenter for integrasjon, brukergrensesnitt, terminaler, skrivere eller andre lokale støttekomponenter. Her finnes ofte IP-basert kommunikasjon og bruk av både IT- og OT-protokoller.

## 4.5 Informasjonsteknologi (IT)

Grensesnittet mot IT er via komponenter og funksjoner i den industrielle demilitariserte sonen (se kapittel 4.5.1). For Operasjonell Teknologi representerer IT forretningssiden av virksomheten, ofte er dette forholdet slik at IT forteller OT hva, når og hvor mye som skal produseres, og OT utfører dette.

### 4.5.1 Industriell Demilitarized Zone (IDMZ)

Den Industrielle Demilitariserte Sonen (IDMZ) er effektivt sett OTs perimetersikring. Men, i tillegg til å beskytte OT, er den designet til å være en «enabler» for kommunikasjon mellom OT-systemer og forretningssystemer i IT. Sonen tilgjengeliggjør informasjon og data fra OT til IT uten fare for eksponering av kritiske komponenter mot usikre miljø. Sonen er også en kritisk komponent i forbindelse med realisering av sikker leverandøraksess.

Sonen er i utgangspunktet en del av IT-miljøet. Dvs. at komponentene her betraktes som IT-komponenter, ikke OT. Det er et poeng at dette miljøet mottar oppdateringer og oppgraderes på lik linje med IT slik at komponentene her har best mulig forutsetning til å beskytte seg selv og kommunikasjon mot OT.

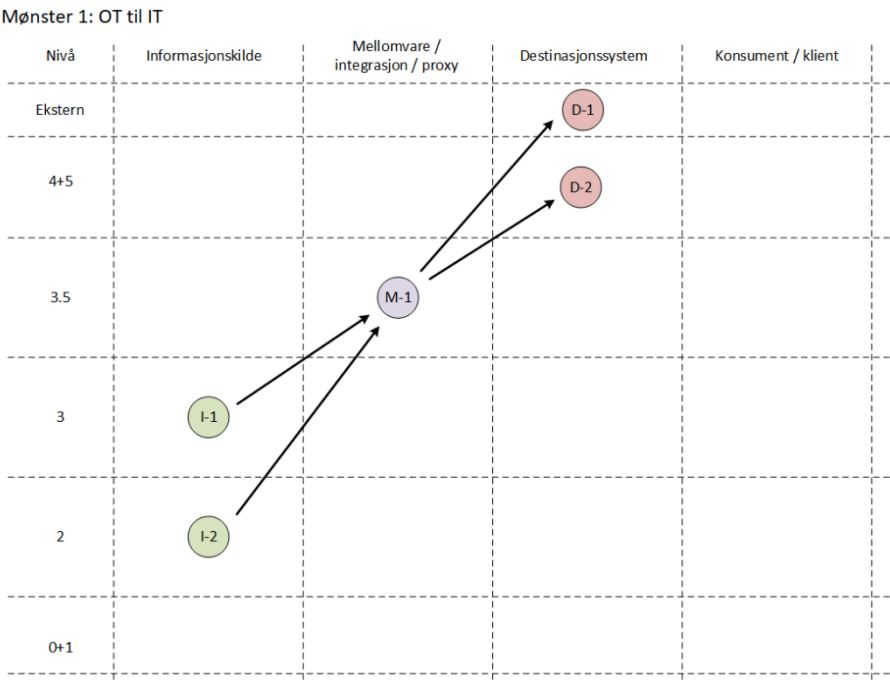
## 5 Prinsipp #2: Arkitekturmønstre og informasjonsflyt

Sykehuspartner HF har definert et sett med mønstre for plassering av komponenter sammen med informasjonsflyt. Disse mønstrene forholder seg ikke til hvordan underliggende integrasjoner og kommunikasjonsflyt konfigureres, men utelukkende til hvordan hovedkomponenter skal plasseres og hvordan informasjonen skal flyte mellom dem. Løsninger som ikke lar seg tilpasse til et av arkitekturmønstrene skal registreres som avvik og alternative sikkerhetstiltak må benyttes.

### 5.1 Mønster 1: OT informasjonskilde til IT destinasjon

Mønster 1 (Figur 8) tar for seg følgende use-cases:

- Som kliniker trenger jeg at mitt behandlingsapparat (MTU) kan sende data/informasjon til et sentralt pasientjournalssystem.
- Som driftstekniker ønsker jeg å kunne se status og statistikk fra mine lokale byggtekniske systemer i min leverandørs skytjeneste.



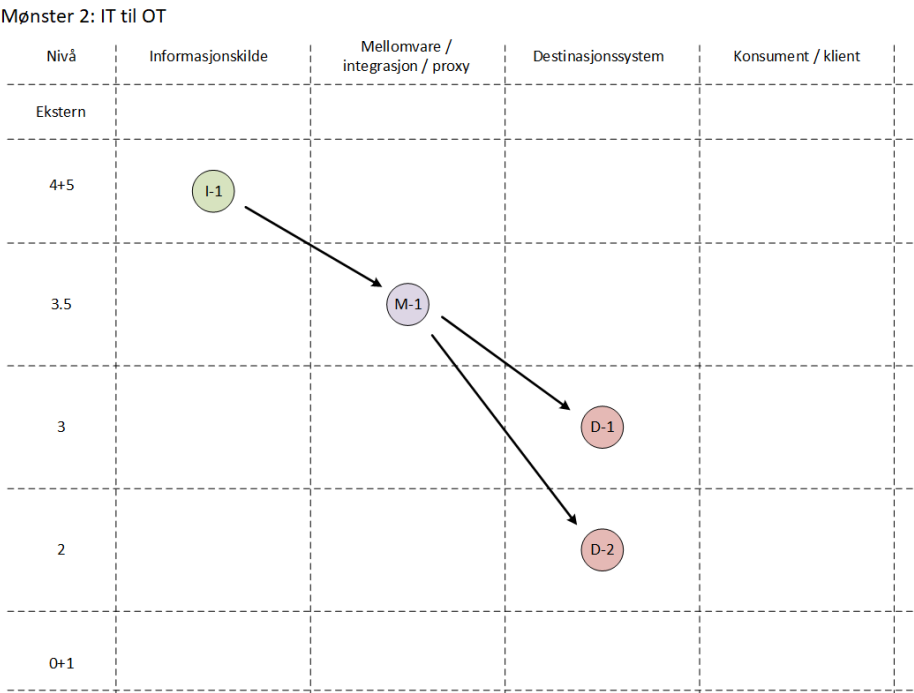
Figur 8 - Arkitekturmønster 1: OT til IT

Dette mønsteret representerer de behovene der et kildesystem i OT (**I-1** og/eller **I-2**) skal flytte data fra seg og inn til et destinasjonssystem i IT (**D-1** og/eller **D-2**). For at dette skal gjøres sikkert, skal dataen innom en aktiv komponent på veien (filsluse, proxy, ...), her representert som **M-1**.

## 5.2 Mønster 2: IT informasjonskilde til OT destinasjon

Mønster 2 (Figur 9) tar for seg følgende use-cases:

- Som kliniker har jeg behov for å flytte en arbeidsliste til et MTU.



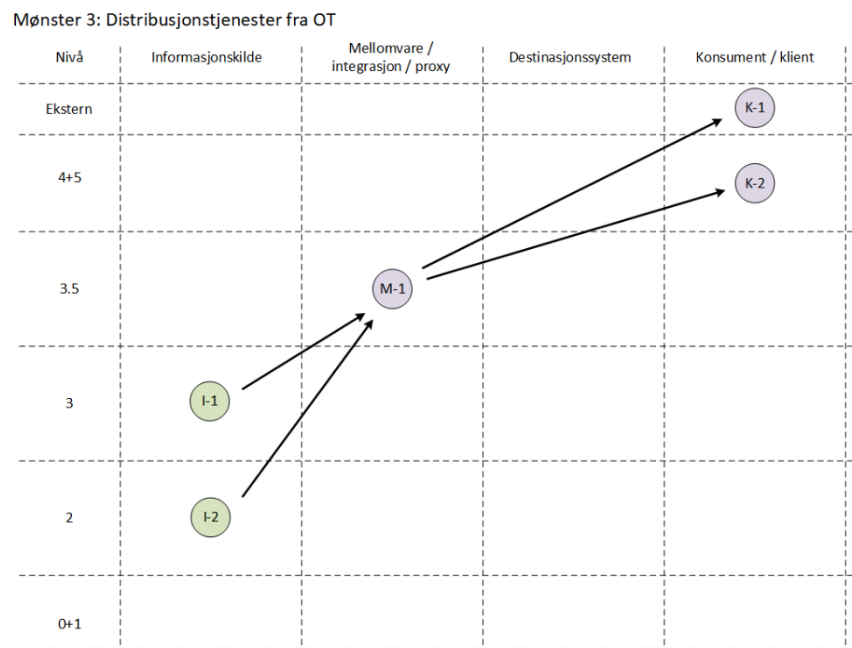
Figur 9 - Arkitekturmønster 2: IT til OT

Dette mønsteret er ment å dekke de behov som kommer av at informasjon lokalisert på en informasjonskilde i IT (**I-1**) skal flyttes til et destinasjonssystem i OT. Dette gjøres ved at informasjonen går gjennom en aktiv komponent på veien (proxy, filsluse, ...), representert av **M-1** i IDMZ. Destinasjonssystemene **D-1** og **D-2** er systemer for permanent lagring av informasjonen.

### 5.3 Mønster 3: Distribusjonstjenester fra OT

Mønster 3 (Figur 10) tar for seg følgende use-cases:

- Som driftsleverandør trenger jeg å få overført data fra utstyret jeg har driftsansvar for til mine egne systemer for analyse.



Figur 10 - Arkitekturmønster 3: Distribusjon fra OT

Dette mønsteret er ment å dekke de kriterier som kommer av behovet for å overføre informasjon fra OT til IT eller eksternt. Dette kan være logg-filer, datastrømmer eller lignende fra kildesystemene **I-1** og **I-2**. Data- og informasjonsstrømmen må innom en aktiv komponent på veien, her representert av **M-1** i IDMZ. Klientene **K-1** og **K-2** kan være interne systemer i IT eller leverandørsystemer lokalisert eksternt.

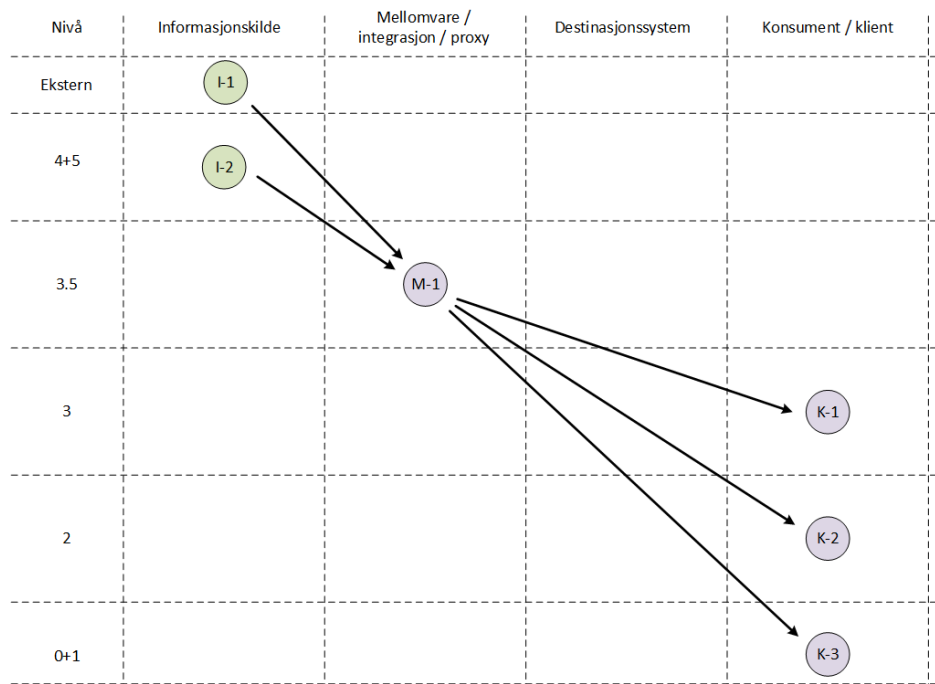
### 5.4 Mønster 4: Distribusjonstjenester til OT

Mønster 4 (Figur 11) tar for seg følgende use-cases:

- Som driftspersonell, må jeg kunne distribuere nye antivirus-signaturfiler fra internett til servere og annet utstyr lokalisert i OT.
- Som driftsleverandør, må jeg kunne overføre oppdateringsfiler fra min arbeidsstasjon til et sted som er tilgjengelig for målsystemet som det skal arbeides på.
- Som kliniker, må jeg kunne sende en bestilling fra EPJ eller et annet toppsystem til et behandlingsapparat (MTU).



Mønster 4: Distribusjonstjenester til OT



Figur 11 - Arkitekturmønster 4: Distribusjon til OT

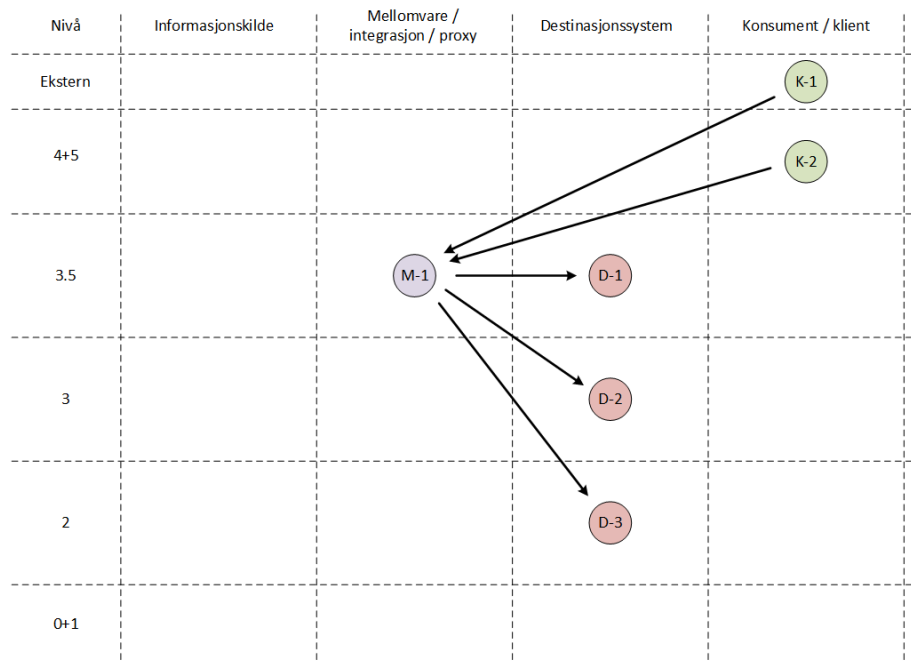
Dette mønsteret er tenkt å dekke de kriterier som kommer av behovet for å tilgjengeliggjøre filer og/eller andre ressurser fra IT eller ekstern inn til OT. **I-1** og **I-2** representerer her kildesystemet der filene eller ressursene er lagret. Filene og/eller ressursene kan da overføres via en «filsluse», proxy eller annen lignende komponent (**M-1**) i IDMZ. Klientsystemene kan være i nivå 3 (**K-1**), 2 (**K-2**) eller helt nede i nivå 1 og 0 (**K-3**).

## 5.5 Mønster 5: Administrasjon av OT komponenter fra IT eller Eksternt

Mønster 5 (Figur 12) tar for seg følgende use-cases:

- Som driftspersonell, må jeg kunne logge på et målsystem for å endre på innstillinger og gjøre generelt vedlikehold.
- Som applikasjonsansvarlig, må jeg kunne utføre administrative oppgaver på min applikasjon.

Mønster 5: Administrasjon av OT



Figur 12 - Arkitekturmønster 5: Administrasjon av OT komponenter

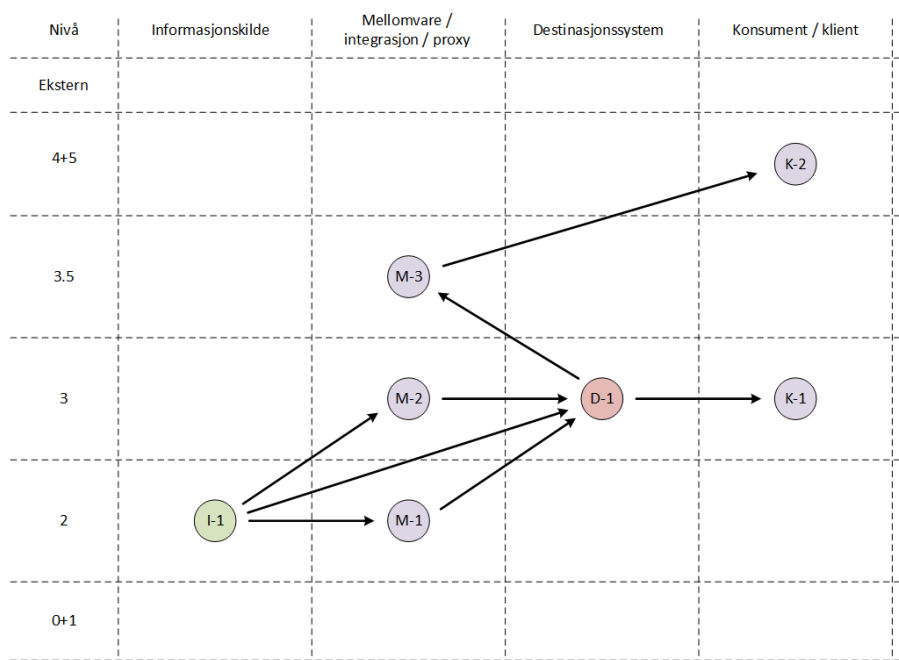
Dette mønsteret er tenkt å dekke de kriterier som kommer av behovet for administrasjon av OT-komponenter fra utenfor OT-miljøet. **M-1** kan være en Privilege Access Management (PAM) eller annen form for «remote desktop»-løsning. Klientene (**K-1**, **K-2**) dekker både interne og eksterne driftsleverandører. Destinasjonssystemene (**D-1**, **D-2** og **D-3**) kan være systemer så vel som enkeltstående komponenter eller applikasjoner.

## 5.6 Mønster 6: OT produksjonssystem

Mønster 6 (Figur 13) tar for seg følgende use-cases:

- Som produktansvarlig, trenger jeg et system som kan fungere uavhengig av tilstanden til IT-systemer og evnen til å kommunisere med sentrale datasenter og eksterne plattformer.

Mønster 6: OT produksjonssystem



Figur 13 - Arkitekturmønster 6: OT produksjonssystem

Dette mønsteret er tenkt å dekke de kriterier som kommer av behovet for *lokal overlevelse* (se også kapittel 9.4). Her er informasjonskilde (I-1) og desinasjonssystemet (D-1) lokalisert inne i miljøet for Operasjonell Teknologi og har ikke avhengigheter til IT. Klienter (K-1) er plassert i OT slik at systemene kan brukes uavhengig av tilstand til ordinær klientplattform. Det er mulig å nå D-1 fra klienter i IT (K-2) via Privilege Access Management (PAM) eller en annen form for «remote desktop»-løsning (M-3).

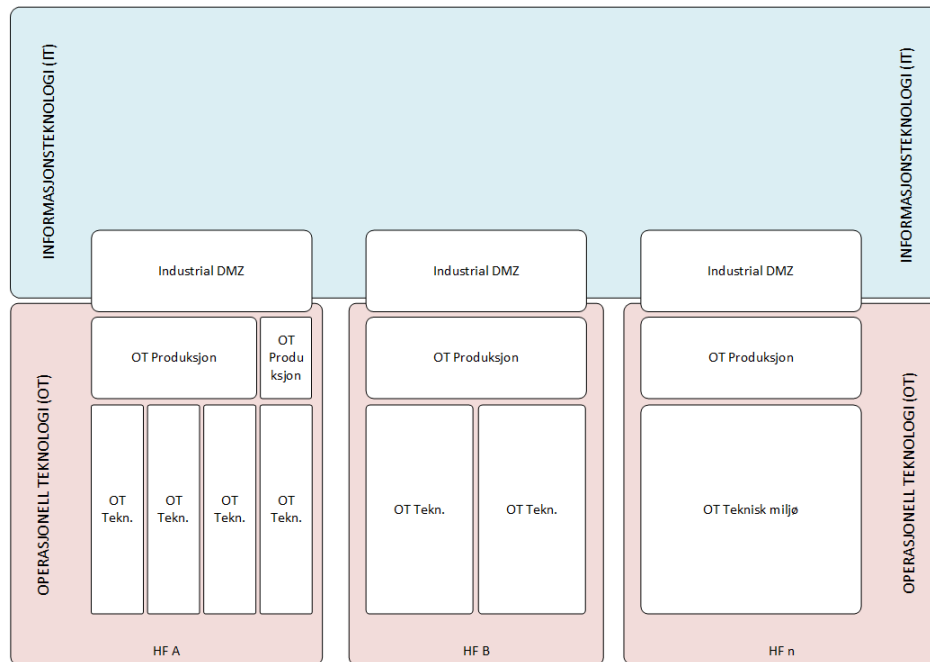
## 6 Prinsipp #3: Regionale løsninger

Prinsippet for regionale løsninger er ment for å kunne dra nytte av stordriftsfordeler og hente gevinster ved å gjenbruke design og arkitekturelementer på tvers av regionen. Intensjonen her er å planlegge løsninger på en slik måte at man skal kunne gjenbruke deler av, eller komplette løsninger flere ganger dersom behovet er likt eller tilnærmet likt på tvers av helseforetak.

*NB: Formålet med dette prinsippet er ikke «sentralisering», i den forstand at alt skal sentraliseres i en eller flere sentrale lokasjoner.*

### 6.1 Regional referansemodell

Figur 14 viser modellen for hele regionen. Hvert helseforetak (HF) har minimum et dedikert miljø for operasjonell teknologi for helseforetaket, vist i Figur 14 som HF A, HF B og HF n. Basistjenester med riktig grad av lokal overlevelse bygges for å understøtte lokal drift av OT-komponenter og -tjenester, selv om helseforetaket blir infrastrukturemessig isolert fra resten av helseregionen. Basistjenester plasseres i et eget OT-produksjonssegment i hvert HF slik at vi sikrer at disse tjenestene tilgjengeliggjøres for hele det dedikerte miljøet. Opprettelse av flere dedikerte OT-miljø og størrelsen på disse følger denne referansearkitekturens foreslåtte områder (beskrives i kapittel 8.1), og kan segmenteres ytterligere ved å gjennomføre en risikobasert soneinndeling som beskrives i kapittel 8.2.



Figur 14 - Regional referansemodell IT/OT

## 7 Prinsipp #4: Logging og overvåkning

Sykehuspartner skal bygge infrastruktur som muliggjør overvåkning av tilkoblede OT-enheter og OT-systemer. Det skal derfor

- defineres sentrale punkter for nettverkstrafikkovervåkning
- være tilgjengeliggjorte punkt for innsamling av logger
- være policykrav om å sende inn logger
- legges til rette for bruk av bransjestandard kommunikasjon for logging
- brukes definerte kommunikasjonsmønster

## 8 Prinsipp #5: Risikobasert soneinndeling

For å standardisere måten infrastrukturen segmenteres i helseregionen brukes en risikobasert soneinndeling. Denne skal ta utgangspunkt i «IEC 62443-3-2:2020 Security risk assessment for system design».

### 8.1 Systemidentifikasjon

IEC 62443-3-2 arbeidsflyt for å etablere «zones and conduits» starter med å identifisere systemet «System under Consideration» (SuC). Hele arbeidsflyten illustreres i neste kapittel. I Helse Sør-Øst brukes begrepet «område» og velger å definere hvert område som en frittstående SuC. Denne referansearkitekturen foreslår områder som beskrevet i tabellen under.

Område	Beskrivelse	Delområder
--------	-------------	------------

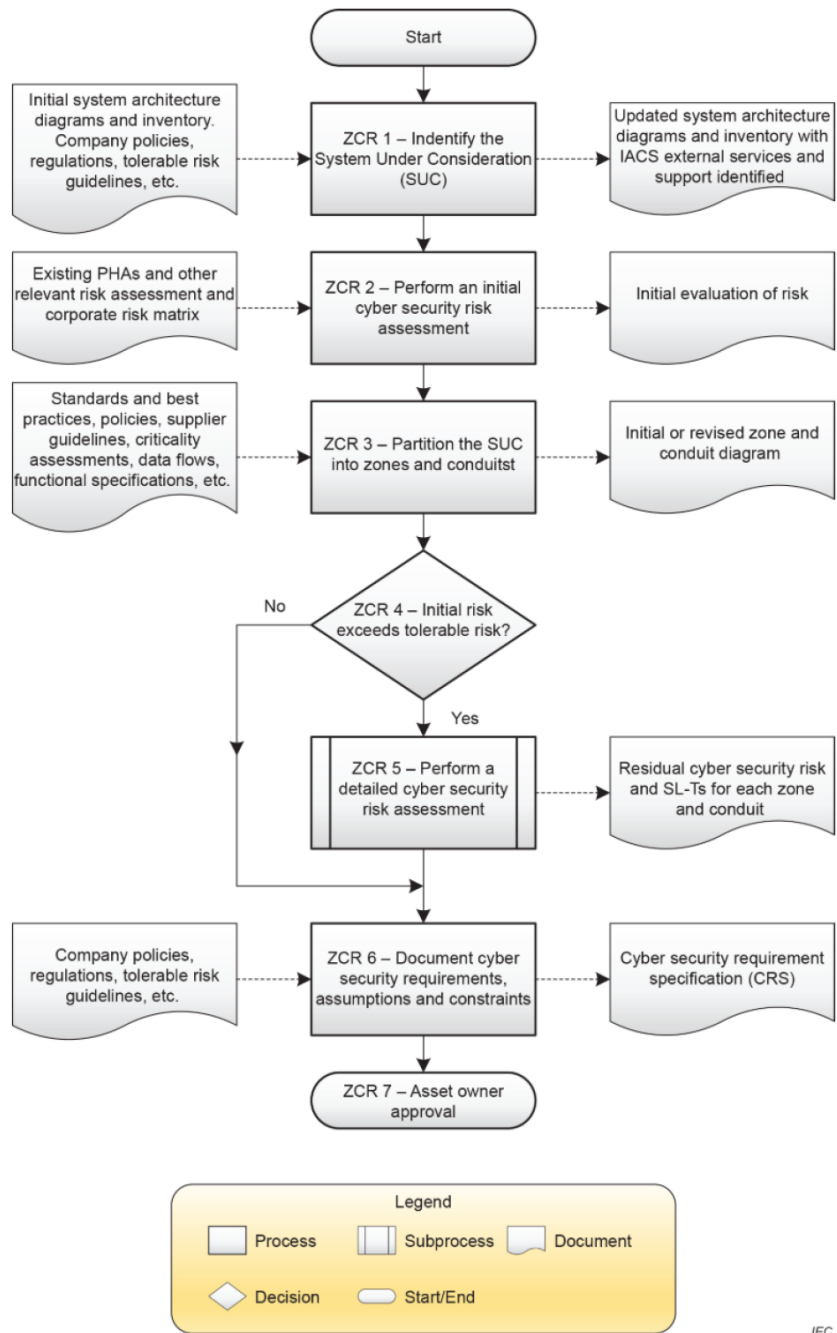
<b>Smarte bygg</b>	Smarte Bygg beskriver Helse Sør-Østs område for byggautomasjon og integrasjon av byggetekniske komponenter for å møte fremtidens behov og krav til energibesparelse, datadeling, kontroll, sikkerhet og optimalisering av kritiske og ikke-kritiske tekniske komponenter i bygningsmassen.	<ul style="list-style-type: none"> <li>• SD-anlegg</li> <li>• Brannvarsling</li> <li>• Tøy og avfallssug</li> <li>• Tøyautomater</li> <li>• Heis</li> <li>• Adgangskontroll</li> <li>• Varme og Ventilasjon (HVAC)</li> <li>• Solskjerming</li> <li>• Energigjenvinning</li> <li>• Vann og avløp</li> <li>• Nødstrøm</li> </ul>
<b>Laboratoriesystemer</b>	Systemer for bruk i lab.	<ul style="list-style-type: none"> <li>• Kjølelager</li> <li>• Analysemaskiner</li> </ul>
<b>Radiologi</b>	Systemer for bruk i digital bildediagnostikk.	<ul style="list-style-type: none"> <li>• Røntgen</li> <li>• CT</li> <li>• MR</li> <li>• Ultralyd</li> </ul>
<b>Prehospital</b>	Systemer for bruk i ambulanser og andre mobile installasjoner.	<ul style="list-style-type: none"> <li>• Medisinsk utstyr</li> <li>• Sambandsløsninger</li> <li>• Flåtestyring</li> <li>• «Asset management»</li> </ul>
<b>IoMT</b>	Internet of Medical Things beskriver området der Helse Sør-Øst drar nytte av personlige helseenheter (PHD), MTU, mm. for støtte i diagnose, behandling og oppfølging.	<ul style="list-style-type: none"> <li>• «Mobile Device Management»-systemer</li> <li>• Sambandsløsninger</li> <li>• Medisinsk utstyr</li> <li>• PoC Gateway</li> </ul>
<b>Digitale Helse-tjenester</b>	Systemer for e-helse/telemedisin.	<ul style="list-style-type: none"> <li>• Digital Hjemmeoppfølging</li> <li>• Hjemmesykehus</li> <li>• Velferdsteknologi</li> <li>• Sambandsløsninger</li> <li>• PH Gateway</li> <li>• Datalake/storage</li> <li>• Datadeling</li> </ul>
<b>Lokale IKT systemer</b>	Systemer for bruk av lokal behandlingsinstitusjon med krav til lokal overlevelse	<ul style="list-style-type: none"> <li>• Videoovervåkning og sikkerhetssystemer</li> <li>• IT-systemer</li> <li>• OT-systemer</li> </ul>
<b>Regionale IKT systemer</b>	Systemer for bruk av behandlingsinstitusjoner og pasienter i helseregionen	<ul style="list-style-type: none"> <li>• IT-systemer</li> <li>• OT-systemer</li> </ul>
<b>Nasjonale IKT systemer</b>	Systemer for bruk og eksponering til befolkningen i nasjonen Norge.	
<b>Forskning</b>	Systemer, tjenester, applikasjoner og infrastruktur for bruk i forskning	<ul style="list-style-type: none"> <li>• Informasjonsanalyse</li> <li>• Utstyrtesting</li> <li>• Kunstig Intelligens</li> </ul>

## 8.2 Modell for risikobasert soneinndeling

Vi bruker modellen for risikobasert soneinndeling av områder som beskrevet i «IEC 62443-3-2 security risk assessment for system design». Modellen tar for seg tre områder:

1. **Sikkerhetssoner** – brukes for å dele et system opp i flere individuelle soner der alle medlemmene av sonen har like krav til sikkerhet og deler samme risikoprofil.
2. **Kanaler** – brukes for å forbinde soner sammen og kontrollere dataflyten mellom disse.
3. **Risikovurderinger** – brukes for å fastslå hvilke sikkerhetssoner som trengs og hvilket sikkerhetsnivå disse skal tilordnes.

Hele prosessen starter med identifisering av et «System under Consideration (SuC)», og ender opp med et «zones and conduit»-diagram som, for hele SuC, beskriver sikkerhetssonene med tilordnet sikkerhetsnivå (SL-T). Figur 15 viser flytskjema som representerer denne prosessen - «IEC 62443-3-2 - Workflow diagram outlining the primary steps required to establish zones and conduits, as well as to assess risk.»



IEC

Figur 15 – Flytskjema risikobasert soneinndeling

## 9 Forutsetninger

Kapittelet beskriver forutsetninger som må være til stede for å realisere en målarkitektur som følger prinsipper og føringer beskrevet i denne referansearkitekturen.

### 9.1 Sonemodell og segmentering

For at Sykehuspartner HF skal kunne representere miljøene og muliggjøre fremtidige tjenesteleveranser må

- Sykehuspartner HF opprette en regional sonemodell for Helse Sør-Øst som også understøtter behovene innenfor Operasjonell Teknologi (OT).
- Helse Sør-Øst tar i bruk OT referansemodellen, som beskrevet i dette dokumentet (kapittel 4.1), i hele regionen.

### 9.2 Sikkerhetsarkitektur

Sykehuspartner HF må utarbeide en overordnet sikkerhetsarkitektur som legger føringer for hvilke sikkerhetstiltak som skal utarbeides hvor og til hvilken grad. Det må også defineres overordnede prinsipper som skal følges ved utarbeiding av domenespesifikke målarkitekturer.

### 9.3 Digital motstandsdyktighet («resillience»)

Sykehuspartner HF må ta stilling til hvor motstandsdyktig/robust Helse Sør-Østs miljøer skal være. Referansearkitektur for OT tilrettelegger for å møte helseforetakenes evne til å levere på sitt oppdrag.

### 9.4 Lokal overlevelse

Sykehuspartner HF og helseregionen må ta stilling til definisjonen av «lokal overlevelse». Dette for at man skal kunne designe og implementere teknologi og løsninger som understøtter og muliggjør dette behovet. I dag eksisterer det ingen god omforent definisjon av «lokal overlevelse», noe som resulterer i at alle finner på og tilpasser denne definisjonen til isolerte behov.

Lokal overlevelse må defineres ut ifra løsningens funksjon i forhold til Helse Sør-Øst og helseforetakenes samfunnsoppdrag. Det betyr at lokal overlevelse må defineres basert på en løsning eller et systems funksjon, essensiell og normal. Gjennom disse begrepene kan det finnes arkitekturmønstre som møter behovet for kostoptimalisering gjennom sentralisering vurdert opp mot samfunnsoppdraget og løsningens/systemets funksjon.

### 9.5 Designprinsipper (krig eller fredstid)

Sykehuspartner HF og helseregionen må beslutte om prinsipper for design av systemer skal understøtte overlevelse i krig eller i fredstid. Dette er essensielt for å kunne bygge og drifte infrastruktur og tjenester som er tilpasset den geopolitiske sikkerhetssituasjonen og Sykehuspartner HFs evne til å levere på en grunnleggende nasjonal funksjon skulle driftssituasjonen forverres.

## 9.6 Kapabiliteter / innsatsfaktorer

Sykehuspartner HF oppretter tjenester som understøtter OT-miljøene. Dette er essensielt for fremtidig utvikling og måloppnåelse. Tjenesteforslag (ikke i prioritert rekkefølge):

- Basis nettverkstjenester (NTP, DNS, DHCP, domenetjenester, ...)
- Identitetstjenester (identifisering, autentisering, autorisering og accounting)
- Overvåkningstjenester og skadevaredeteksjon
- Asset management / asset inventory / tilstandsrapportering
- Sikkerhetskopiering og gjenoppretting
- Sertifikattjenester (PKI)
- Backup og gjenoppretting
- Integrasjonstjenester
- Alarmering
- Filslusetjenester
- Livssyklusstyring
- Fjernaksess
- Lagringstjenester

## 10 Referanser

Referanse	Kommentar
Sykehuspartner Utviklingsplan 2024 – 2028	<a href="https://sykehuspartner.fisp.no/Delte%20dokumenter/Sykehuspartner%20Utviklingsplan%202024%20-%202028_uu.pdf">https://sykehuspartner.fisp.no/Delte%20dokumenter/Sykehuspartner%20Utviklingsplan%202024%20-%202028_uu.pdf</a>
NEK IEC TR 62443-3-1:2009	<a href="https://online.standard.no/nb/nek-iec-tr-62443-3-1-2009">https://online.standard.no/nb/nek-iec-tr-62443-3-1-2009</a>
NEK IEC 62443-3-2:2020	<a href="https://online.standard.no/nb/nek-iec-62443-3-2-2020">https://online.standard.no/nb/nek-iec-62443-3-2-2020</a>
NEK EN IEC 62443-3-3:2019	<a href="https://online.standard.no/nb/nek-en-iec-62443-3-3-2019">https://online.standard.no/nb/nek-en-iec-62443-3-3-2019</a>
NIST SP 800-82r3	<a href="https://csrc.nist.gov/pubs/sp/800/82/r3/final">https://csrc.nist.gov/pubs/sp/800/82/r3/final</a>
Målbilde HSØ IKT rom v1.1	
Målarkitektur Nettverk v1.0	
Målarkitektur Felles plattform v1.0	