

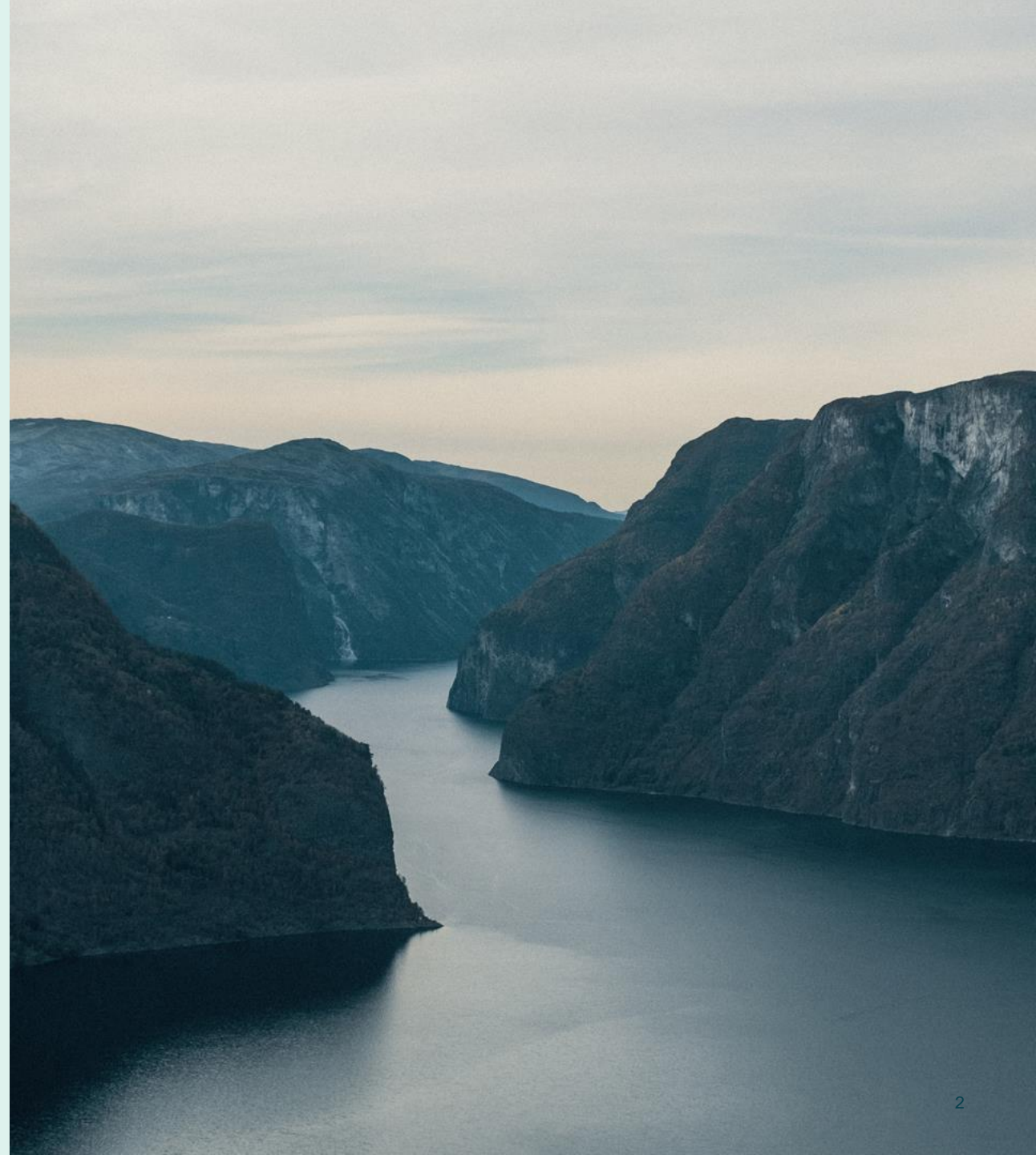


Hafslund
Eco

Sonemodell anno 2023

Vegard Mathisen

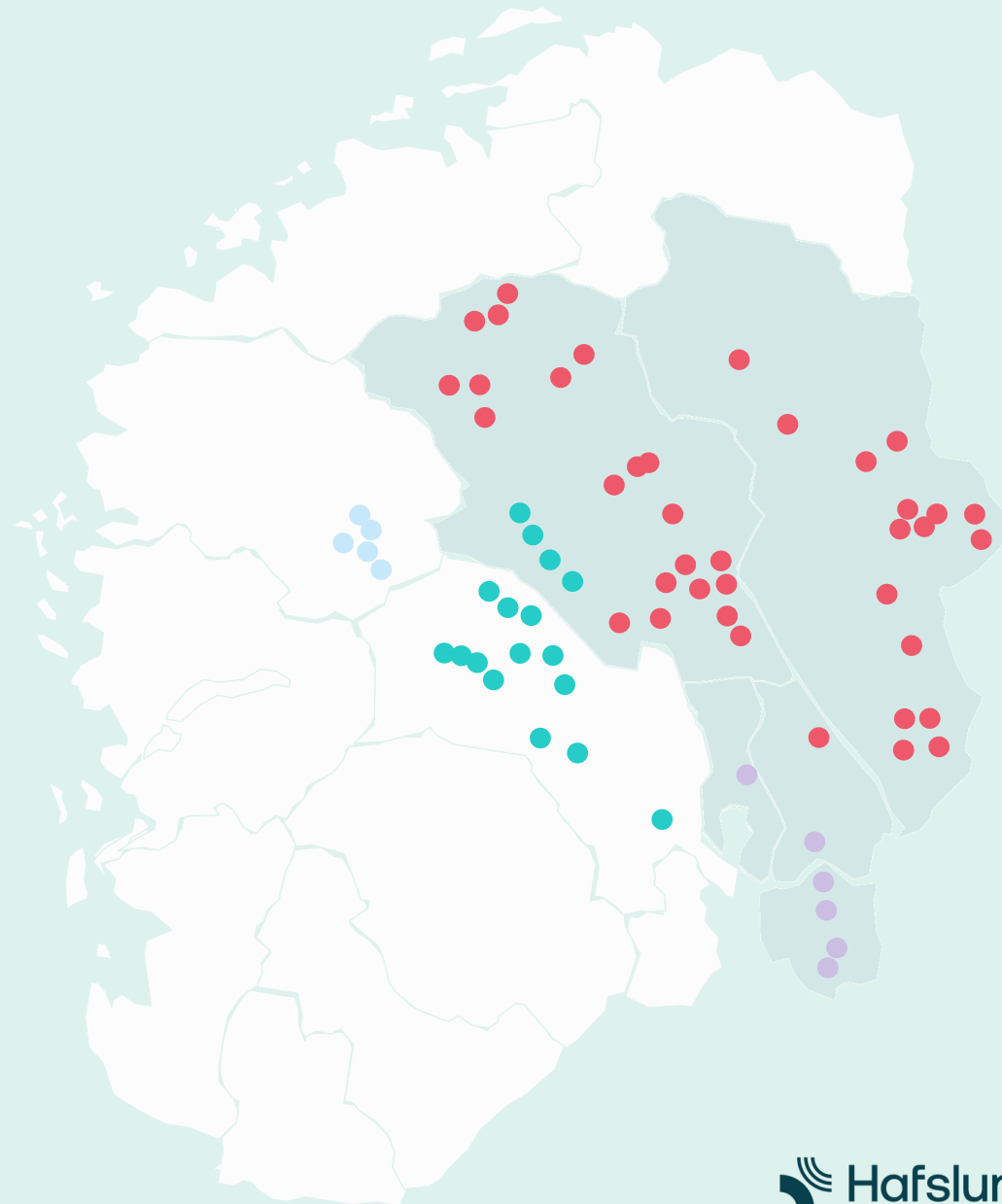
Sikkerhetsdesigner Hafslund Eco Vannkraft AS



Hafslund Eco Vannkraft opererer 82 kraftverk med produksjon på 21 TWh per år

- Kraftverksområde Aurland (3,3 TWh)
- Kraftverksområde Hallingdal og Valdres (5,3 TWh)
- Kraftverksområde Innlandet (8,0 TWh)
- Kraftverksområde Glomma (4,8 TWh)

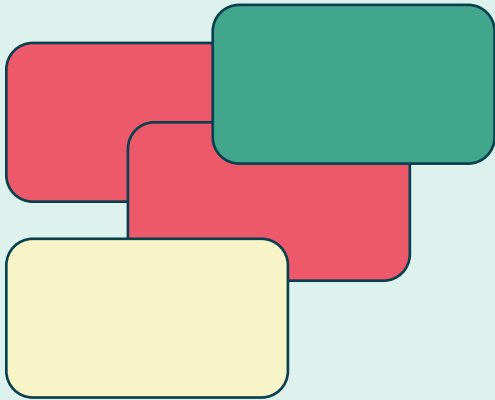
Det er nok til å forsyne over 2,6 millioner innbyggere med strøm.



Agenda

1. Sonemodell – hva og hvorfor?
2. Purdue, SANS ICS410, IEC 62443
3. IT? OT?
4. Løk og andre grønnsaker

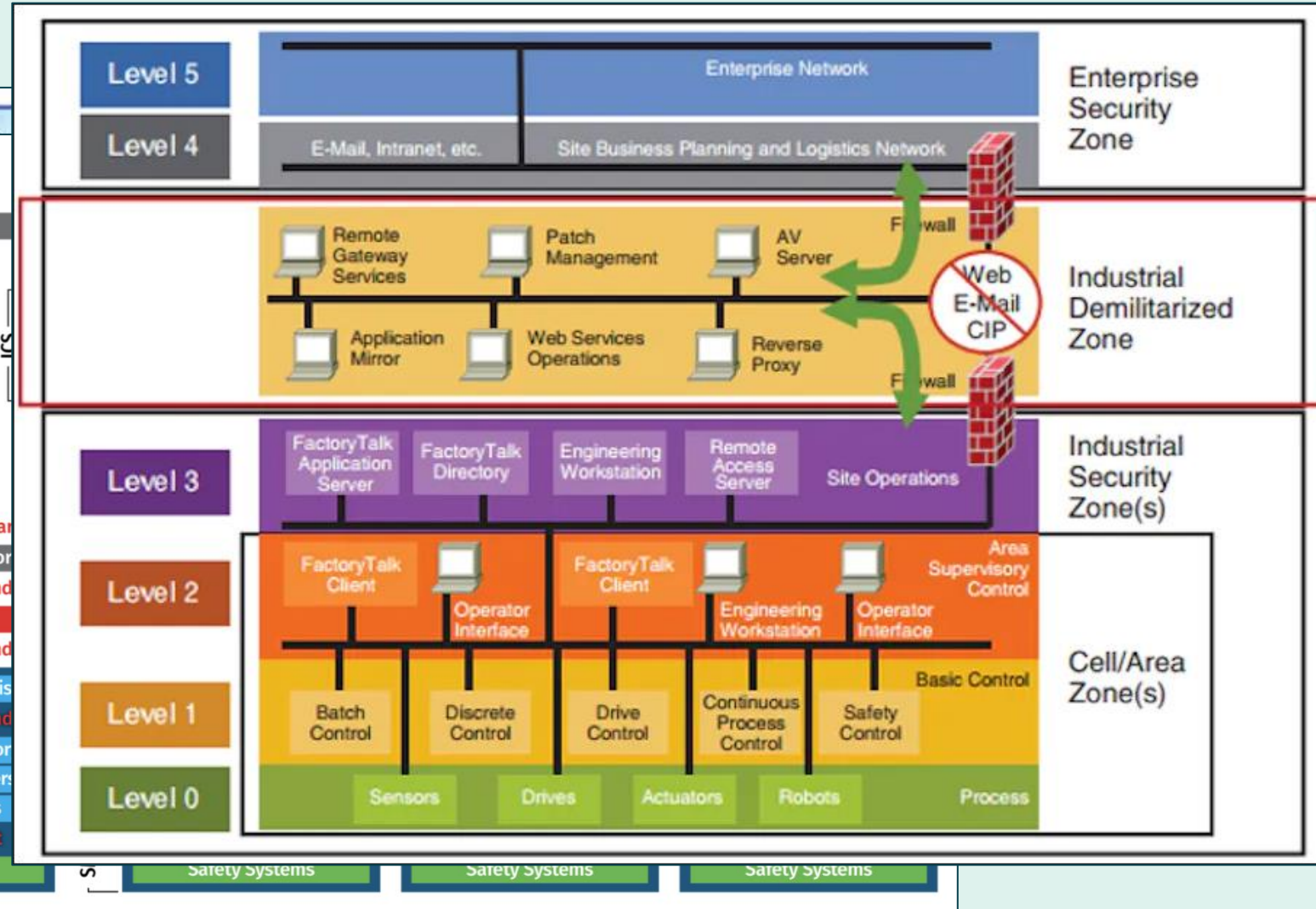
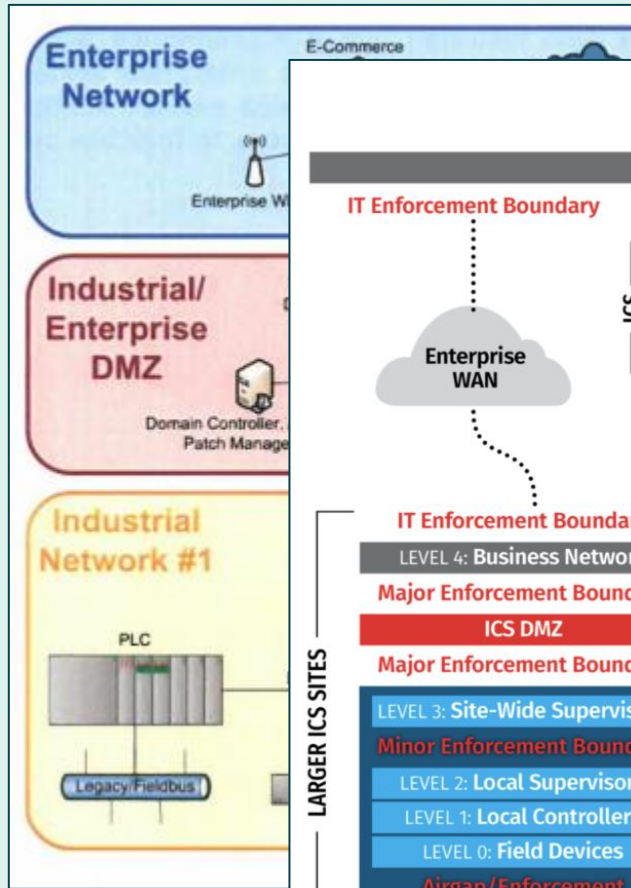
Sonemodell – Hva og hvorfor?



- Systemer med forskjellig risikoprofil trenger forskjellige sikkerhetstiltak
- En sonemodell samler systemer med lik risikoprofil
- Vi ønsker ikke å gjøre en fullstendig RoS-analyse av hvert eneste system
- En sonemodell gir en strukturert samling av systemer med lik risikoprofil
- En sonemodell sier noe om hvordan systemene kan snakke sammen

IEC 62443, SANS ICS410, Purdue

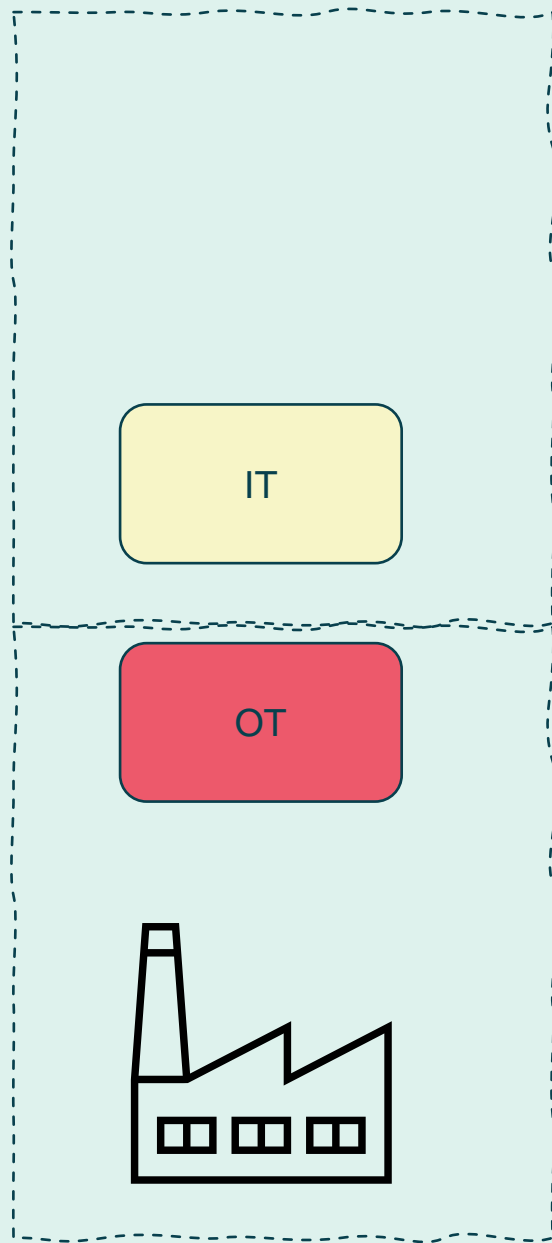
Noen har jo gjort dette før?



Purdue-modellen

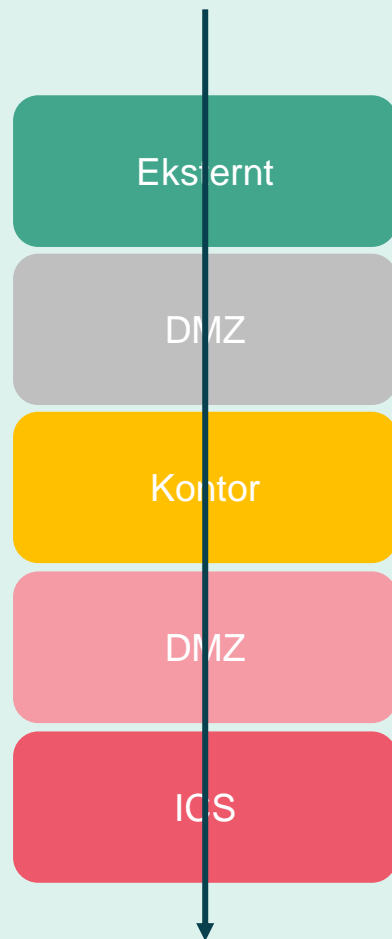


IT? OT?



Felles for disse?

Det som blir implementert er en serialisert infrastruktur

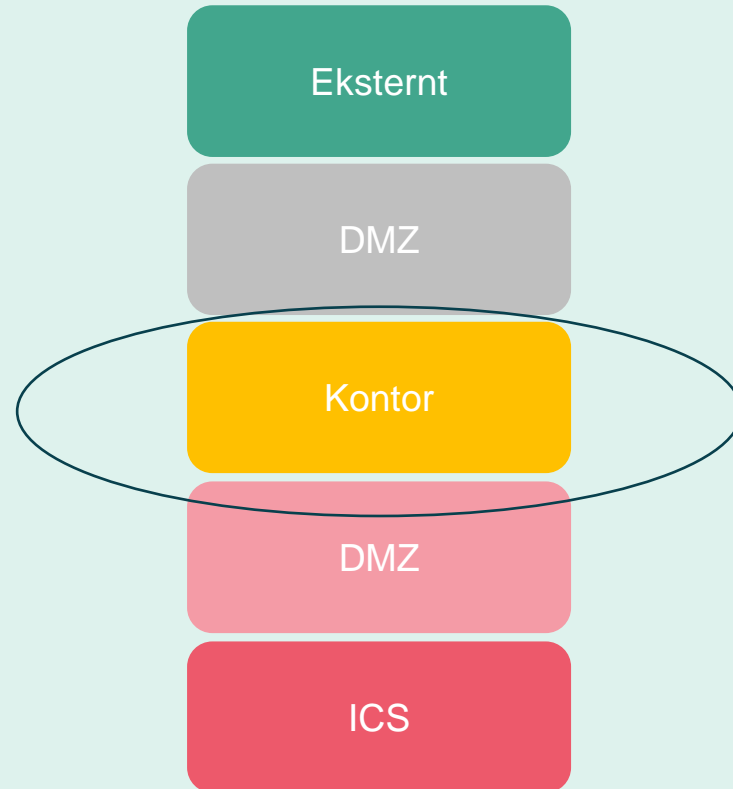


Hva skal jeg snakke om?

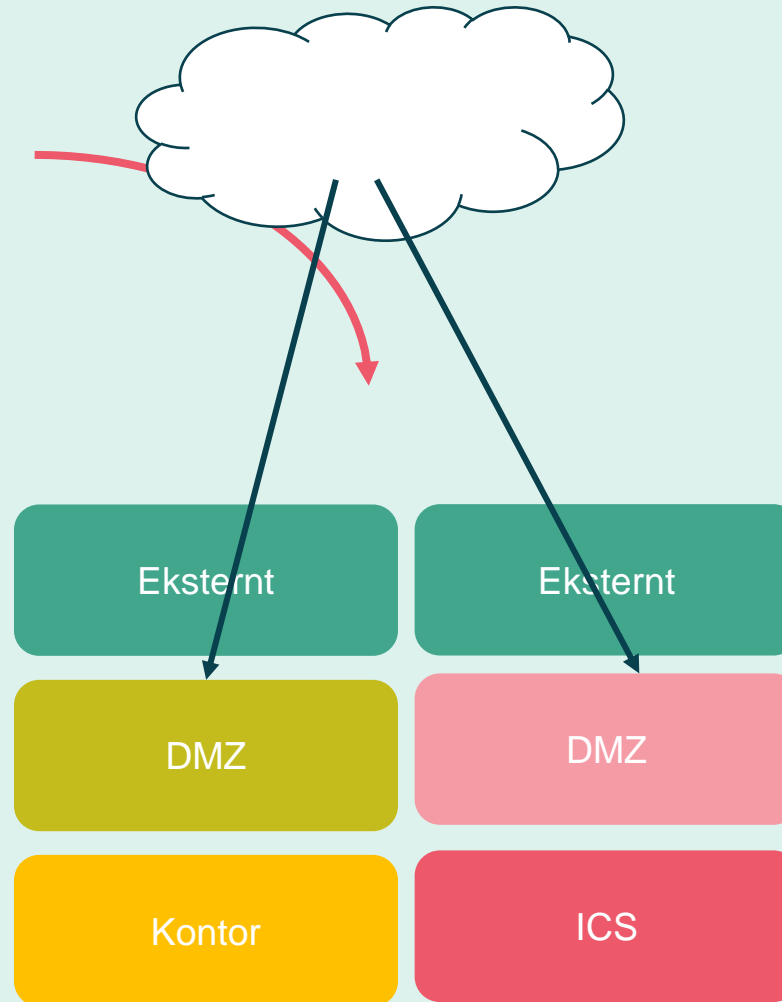
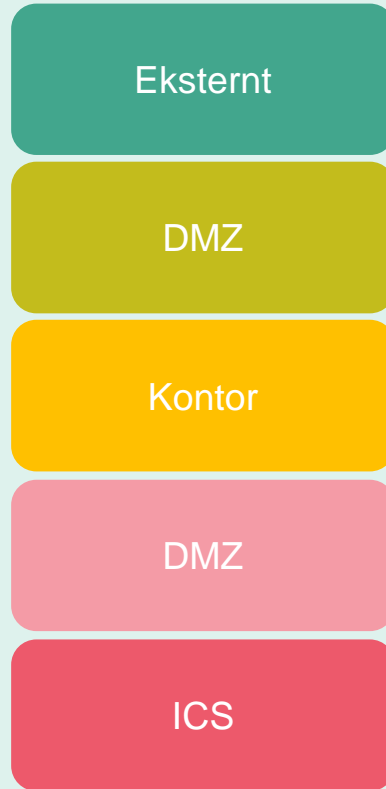
- Skille mellom IT og OT
- Serialisert lagmodell

Hvorfor er en serialisert infrastruktur dumt?

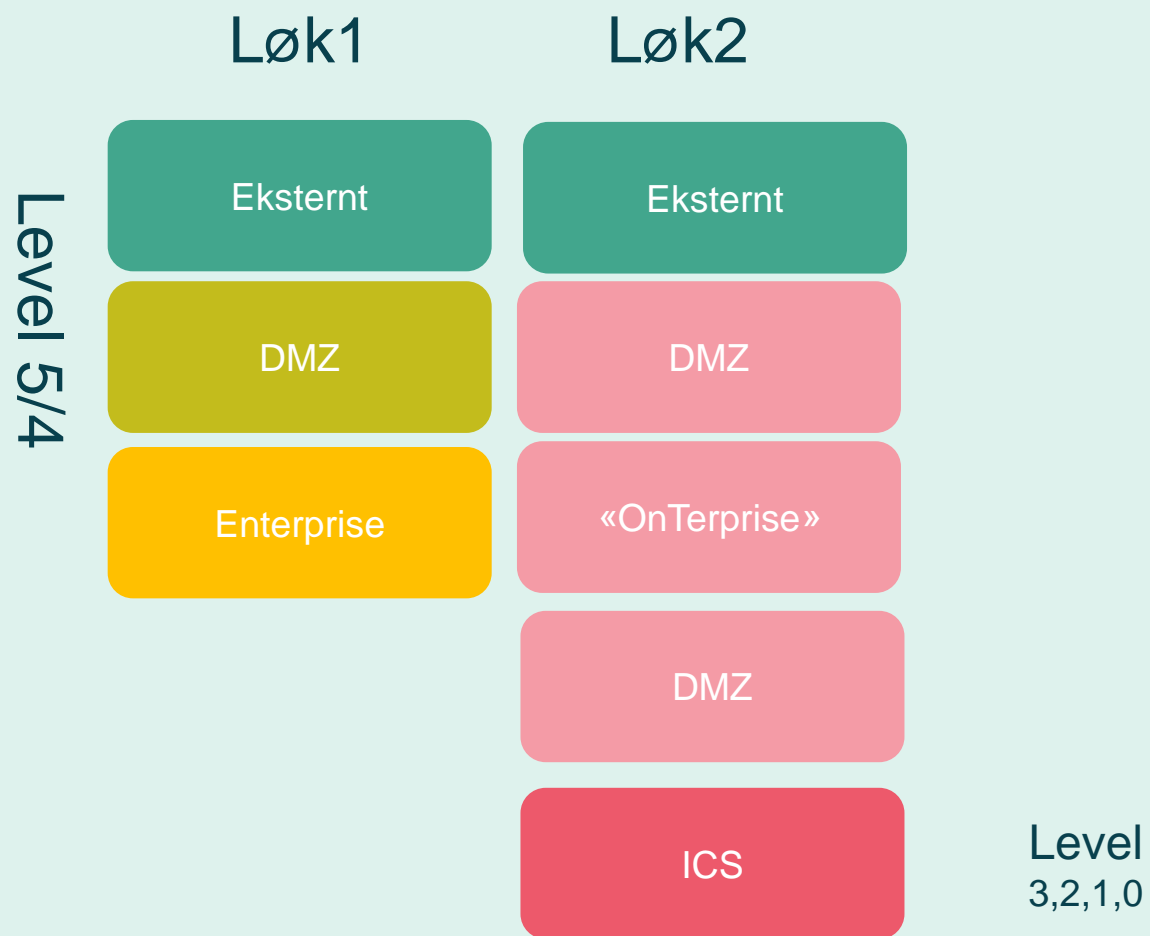
- Stadig flere konsumenter flytter ut til nivå 5 (skya)
- Hvorfor involvere andre deler av organisasjonen på veien?
- Vi ønsker oss autonomitet



Løk er bra, men ...



... men flere løk er enda bedre!



Begreper

Sikkerhetsdomene

- Samling av systemer på samme sikkerhetsnivå innenfor en organisatorisk inndeling
- Tilsvarende «Zone» i 62443
- Kommunikasjon mellom sikkerhetsdomener er «ekstern kommunikasjon»
- I motsetning til 62443, så vil vi ha lag inni hver «sone»

Sikkerhetsnivå

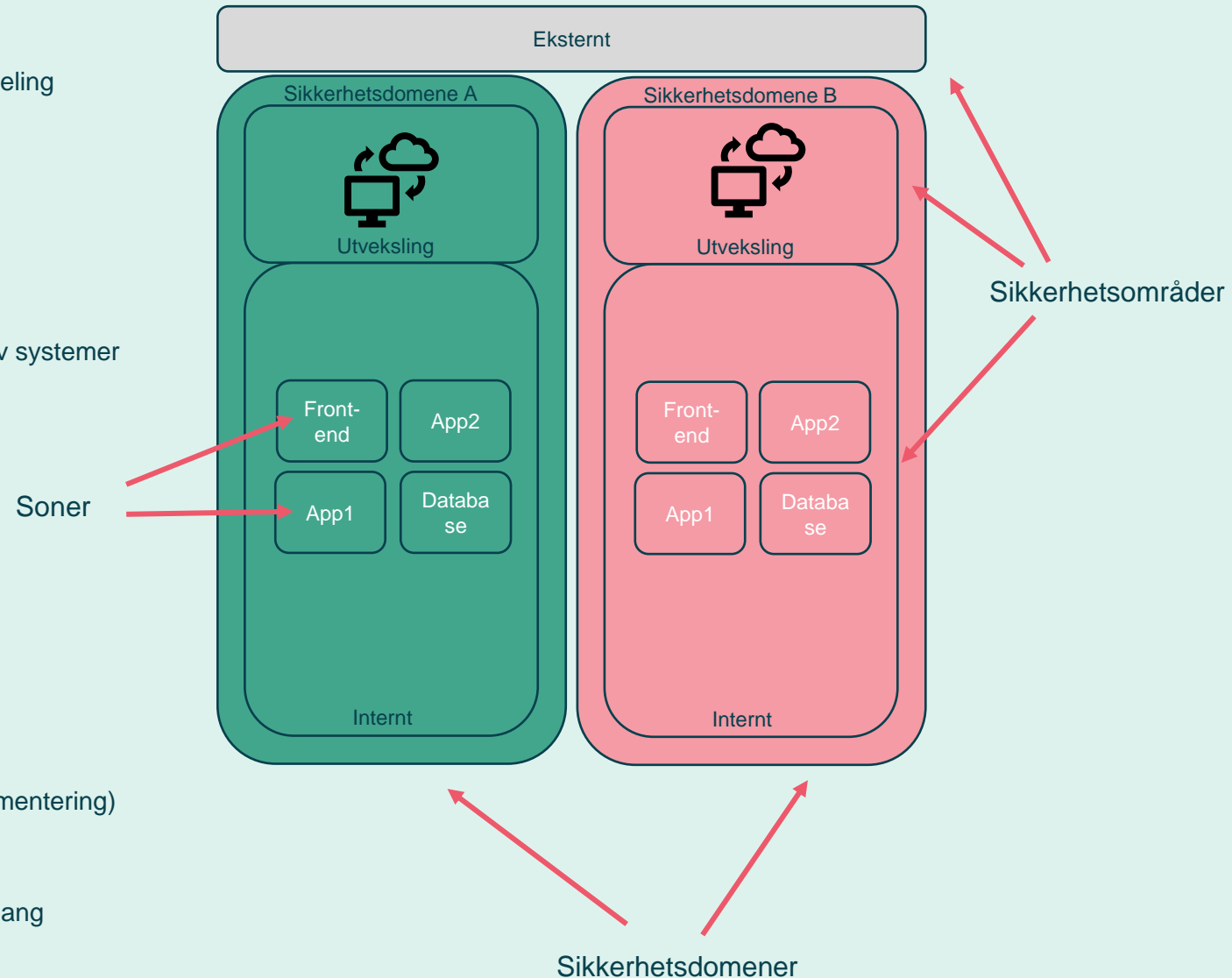
- Definerte sikkerhetsegenskaper for å oppnå akseptabel risiko for en kategori av systemer
- Tilsvarende «Security Level» i 62443
- «Grønt», «Gult», «Rødt» og «Mørkerødt»

Sikkerhetsområde

- Inndeling etter hvor god fysisk kontroll HEV har på systemene
- «Eksternt», «Utveksling» og «Internt»

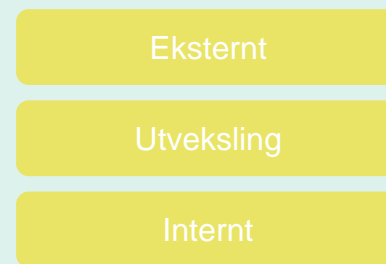
Sikkerhetssone

- Segment/lag innenfor et sikkerhetsdomene
- Segmentet kan enten omfavne en (mikro-segmentering) eller flere (makro-segmentering) komponenter
- Tilgangshåndheving mellom soner
- Internt i soner er det kun herding av komponentene i sonen som hindrer full tilgang



Sikkerhetsnivå

Sikkerhetsområder



Egenskaper

- Autonomitet
- Isolasjon
- Strukturere tiltak etter verdivurdering



Fordeler/Ulemper

- Sterkere egenskaper for isolering og autonomitet
- Redusert skadeomfang ved hendelser
- Differensierte sikkerhetstiltak basert på beskyttelsesbehov (kosteffektive tiltak)
- Identitet
- Økt administrasjon
- Økt kompleksitet
- Økte kostnader

Q & A

