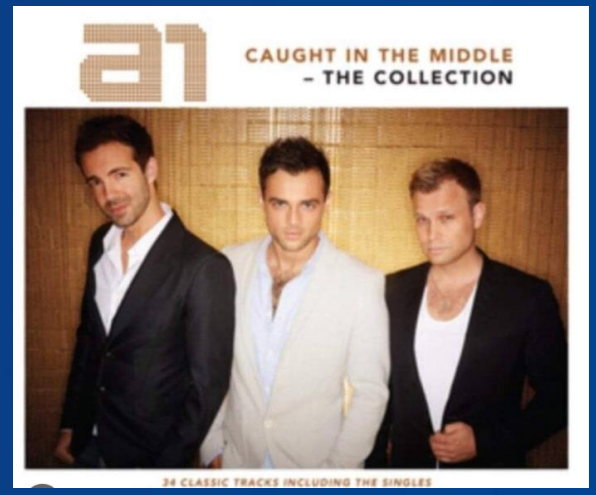
Cought in the middle: High-demand SIFs

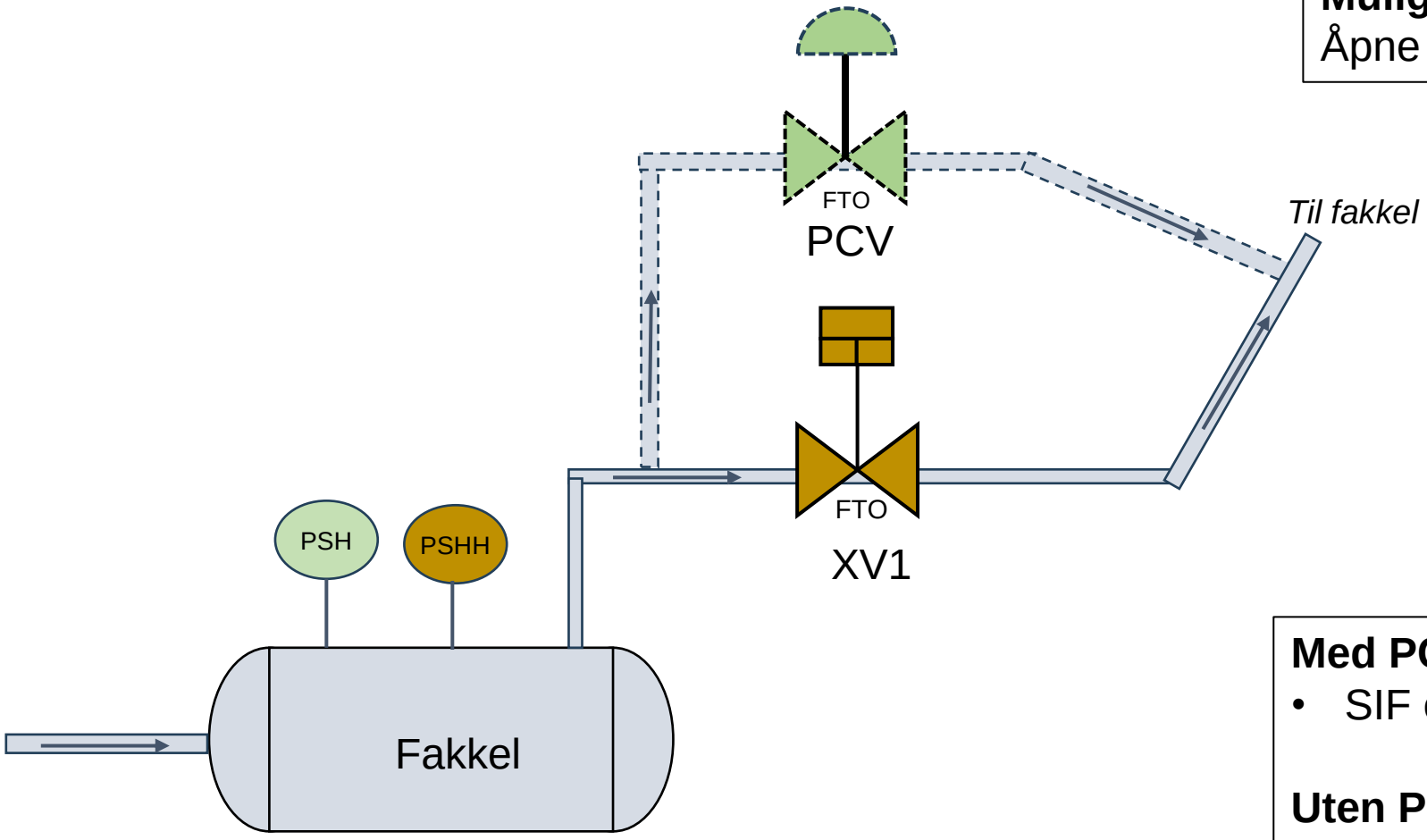


Mary Ann Lundteigen, institutt for teknisk kybernetikk
(mary.a.lundteigen@ntnu.no)

Praktisk eksempel

SIF:
Åpne XV1 hvis trykk = HH settpunkt

Mulig tilleggsfunksjon (PCS):
Åpne PCV hvis trykk= H settpunkt



Samme SIF, men ulik løsning og pålitelighetsmål?

Med PCV funksjon:
- SIF er **low-demand**

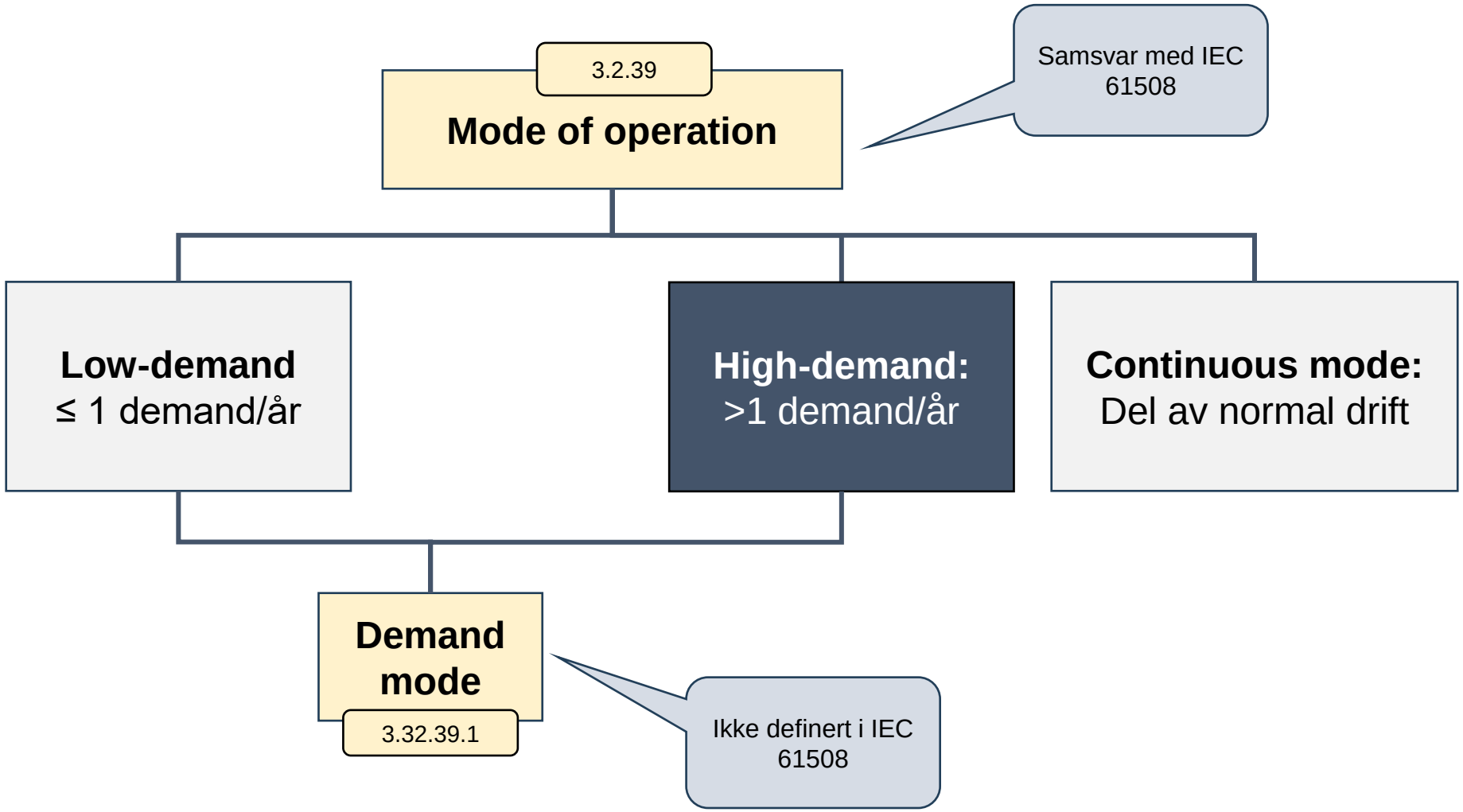
Uten PCV-funksjon:
- SIF blir **high-demand**

Trykk kan passere H (og event. HH) 2-3 ganger per år eller kanskje mye oftere (1 gang i uka)

Tema som belyses

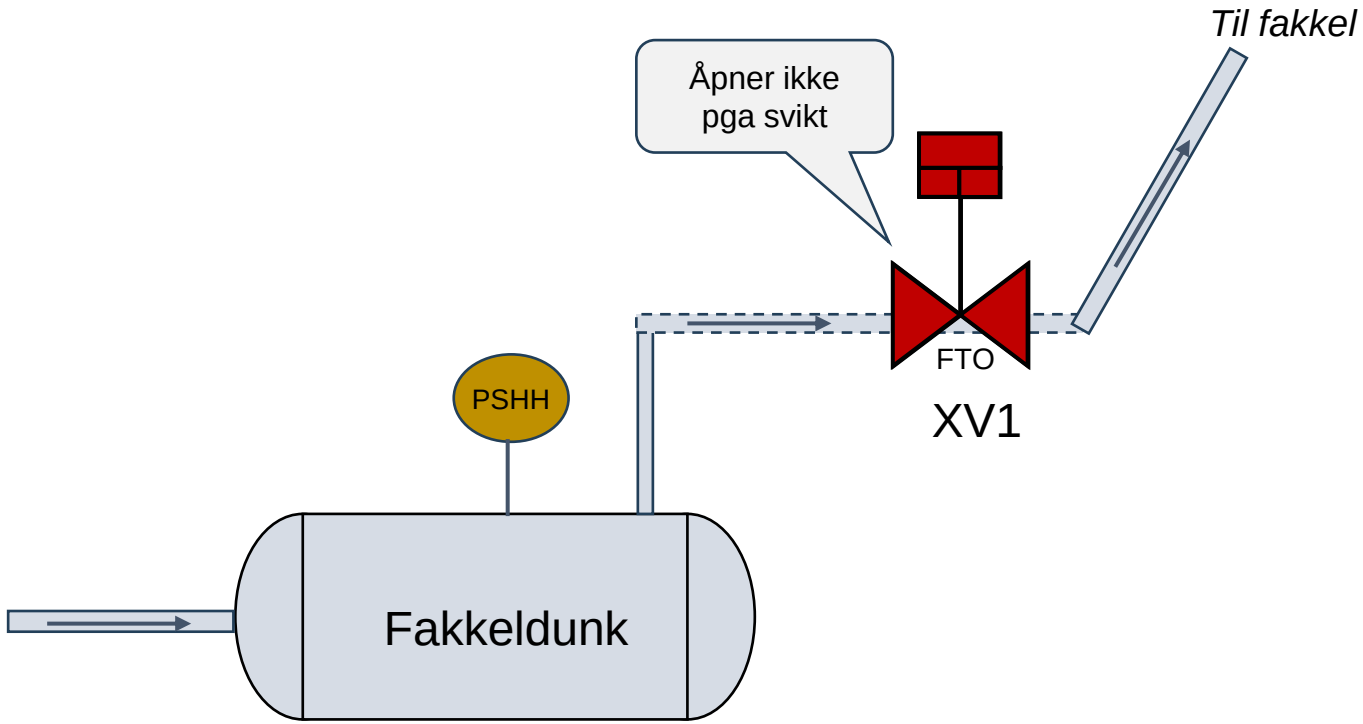
- Hva sier IEC 61511 om high-demand?
- Kan PFD brukes for high-demand? Når?
- Er det egne designkrav til high-demand?
- Kan vi foreslå noen kriterier der en SIF er en mild variant av high-demand?

Hva sier IEC 61511 om high demand?



*IEC 61511-1 (2016), kapittel 3.2.39 og 3.2.39.1

Hva kjennetegner de tre mode of operation?

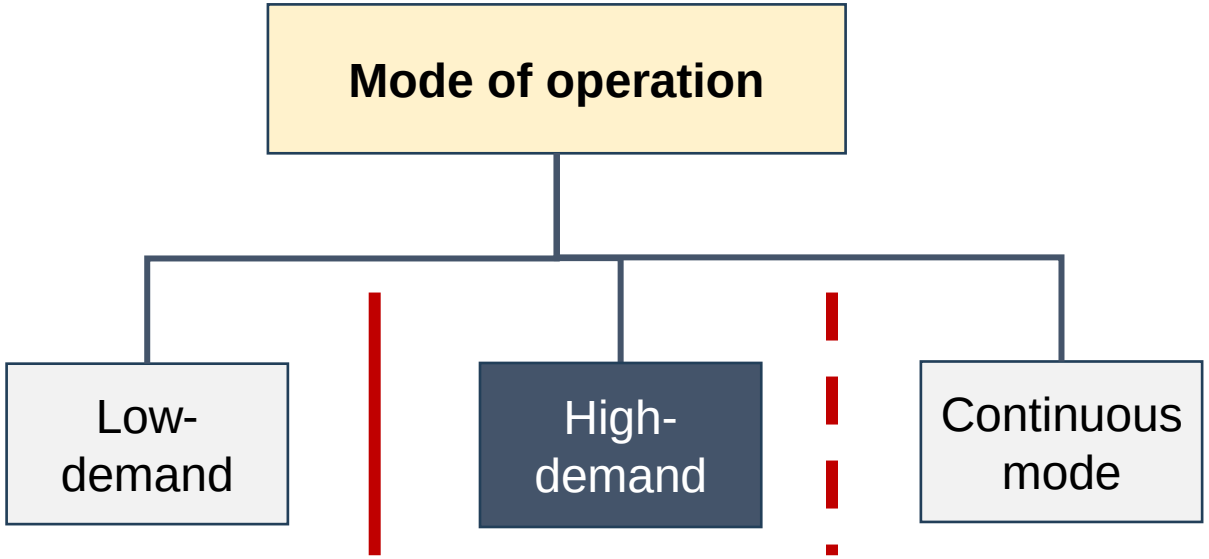


Low demand:
- XV1 svikt sannsynligvis avdekket på test og ikke under demand
- Kan repareres i tide

High demand:
- XV1 svikt *kan* avdekkes på test heller enn demand hvis testing er ofte nok
- Kan repareres i tide

Kontinuerlig:
- XV1 svikt får umiddelbar konsekvens
- Ikke anledning til å reparere i tide

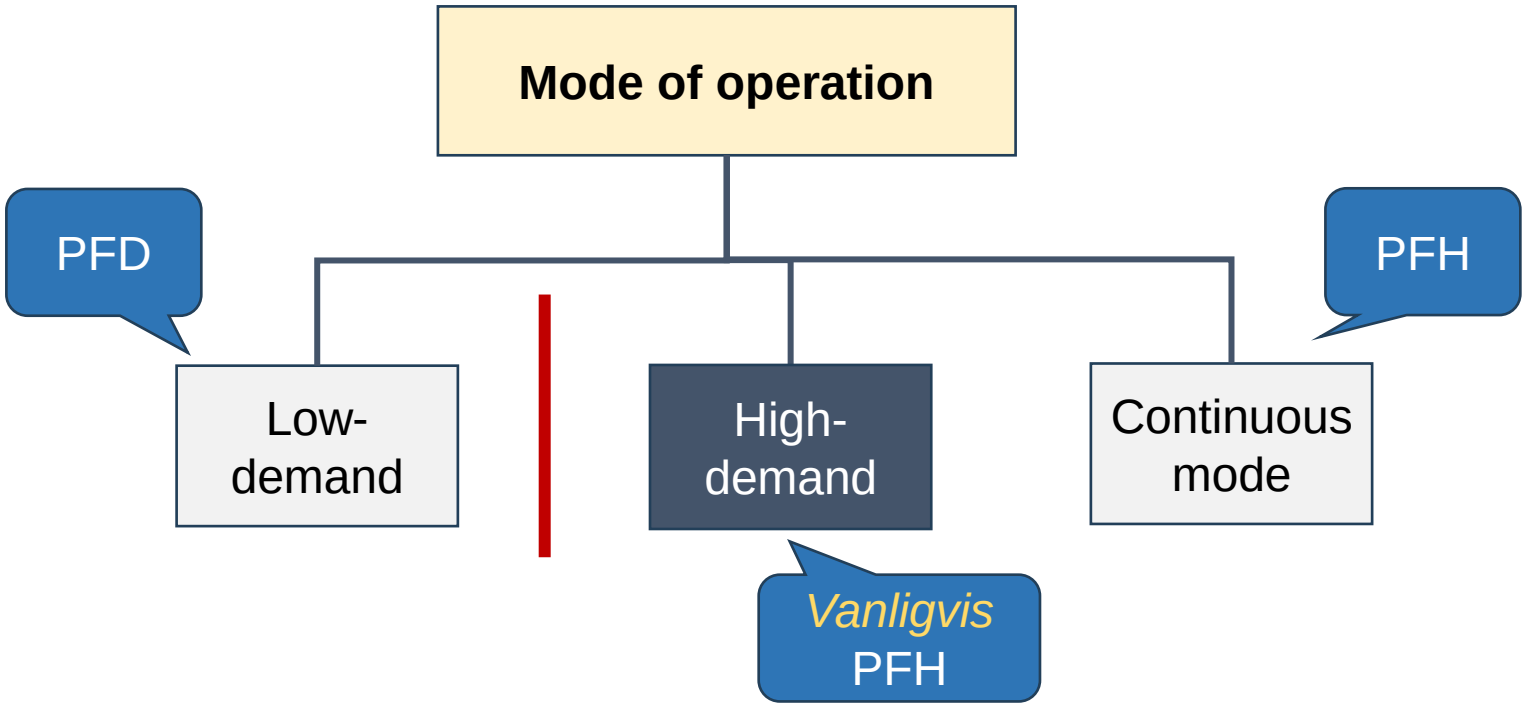
Hvor går skillet mellom low demand og high demand?



Gammelt IEC 61508 tilleggskriterium:
Oftere enn 2 ganger per test intervall

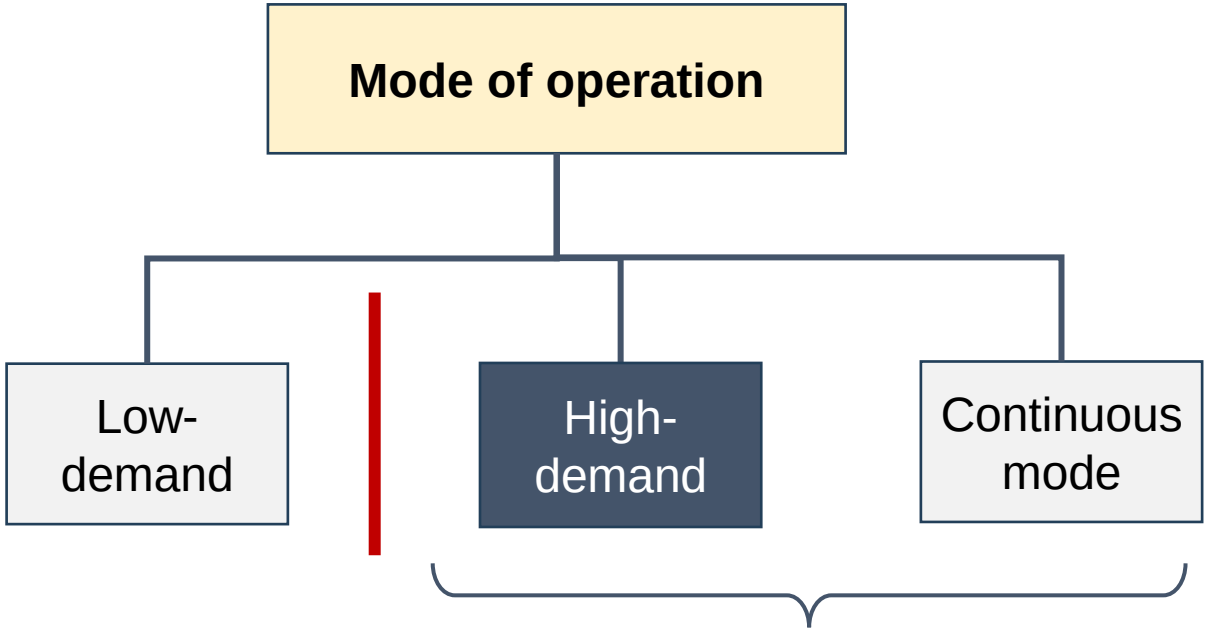
*IEC 61511-1 (2016), kapittel 3.2.39 og 3.2.39.1

Hva har det å si for hvordan vi «regner på» SIL?



*IEC 61511-1 (2016), kapittel 3.2.39 og 3.2.39.1

Hvordan påvirker high-demand teknisk løsning?



For SIL 2 kreves **feiltoleranse på 1** (i motsetning til 0 for low-demand

IEC 61508-2: Også tilleggskrav ifbm klassifisering av DD feil for PFH og SFF beregninger hvis HFT=0.

*IEC 61511-1 (2016), kapittel 11.4.5

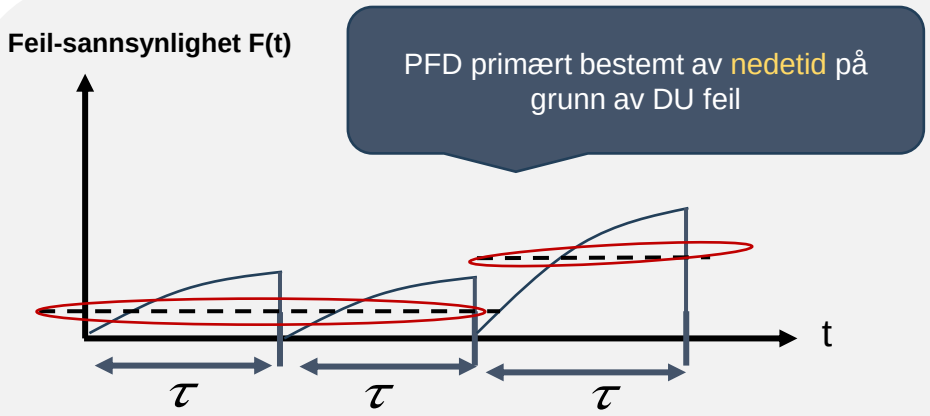
Spørsmål som vil bli (forsøkt) belyst

1. ***Når*** kan man bruke PFD for en high-demand funksjon?

2. Uavhengig av PFD eller PFH – hvordan **følger vi opp high-demand**?

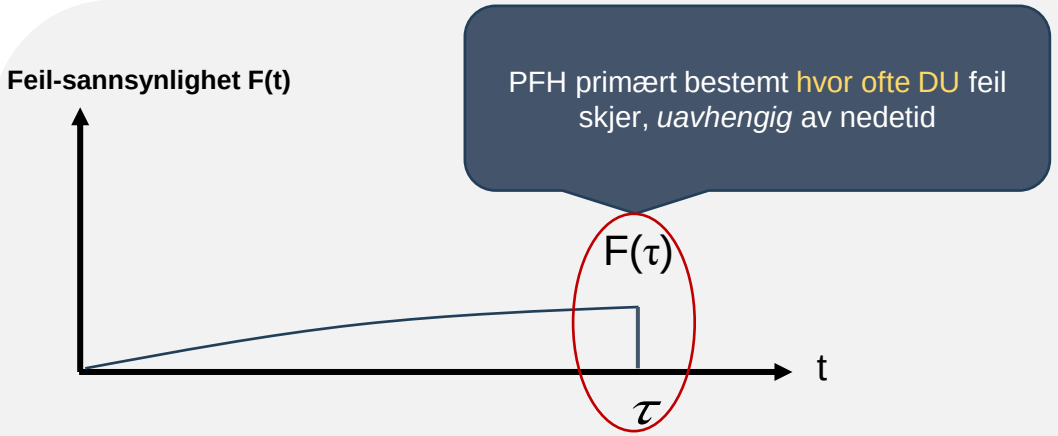
1. Når kan PFD brukes for high demand SIFer?

- … men aller først – hva var nå forskjellen på PFD og PFH?



$$PFD = \frac{1}{\tau}\int_0^{\tau} F(t)dt \approx \frac{\lambda_{DU}\tau}{2}$$ (for et en enkeltkomponent)

$$\text{PFD} \approx \frac{(\lambda_{DU}\tau)^2}{3}$$ (for 1oo2 uten fellesfeil)



$$PFH = \frac{F(\tau)}{\tau} \approx \lambda_{DU} + \lambda_{DD}$$ (for en enkelt-komponent)

$$PFH = \frac{F(\tau)}{\tau} \approx 2\lambda_{DU}^2\,\tau$$ (for 1oo2 uten fellesfeil)

Merk at:

- τ for PFD er test intervall der man antar så godt som nytt etter test.
- τ for PFH er **egentlig** et tidsrom der man ikke forventer mer enn **en** SIF svikt (som av og til strekkes litt vel langt) og hvor systemet i etterkant er så godt som nytt.

1. Når kan PFD brukes for high-demand SIFer?

Forsøkes belyst ved å sammenligne **HR** for et 1oo1 system når demand raten λ_{de} varierer:

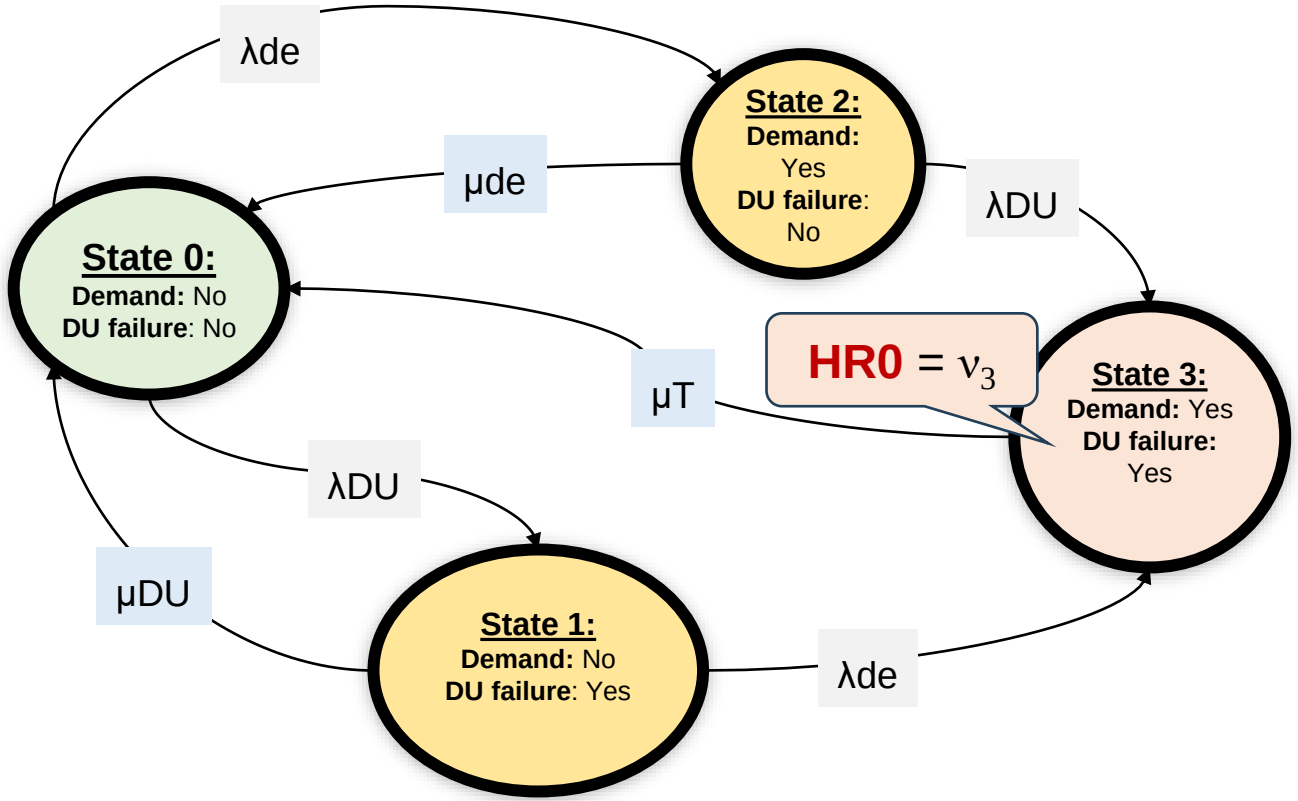
	Hvordan HR bestemmes	Metode	Hva vi bruker som «fasit»
HR1	λ_{de}* PFD= λ_{de}* λ_{DU}*τ/2	Håndregning	
HR2	PFH=λ_{DU}	Håndregning	
HR0	Beregner HR som inkluderer demand rate, varighet av demand i tillegg til DU feil.	Markov analyse	X

HR: Hazard rate – hvor ofte en farlig hendelse skjer som følge av SIF svikt

Beregning av **HR0** vha Markov analyse

State	Description
0	No demand, No DU failure
1	No Demand, DU failure
2	Demand , No DU failure
3	Hazardous state (HE): Demand and DU failure

Parameter	Description	Value
λde	Demand rate	Between 1E-6 -1 E-3 (per time)
λDU	DU failure rate	1E-6 per hour
μDU	2/τ which is the mean time to restore one DU failure, where τ is the test interval	2/8760, 8760=1 year
μde	Restoration after a demand	1/24 per hour
μT	Restoration after a hazardous event	1/24 per hour (Kan økes mye uten at det får betydning)



$$\text{Transisjonsmatrise} = \begin{bmatrix} -(\lambda_{DU}+\lambda_{de}) & \lambda_{DU} & \lambda_{de} & 0 \\ \mu_{DU} & -(\mu_{DU}+\lambda_{de}) & 0 & \lambda_{de} \\ \mu_{de} & 0 & -(\mu_{de}+\lambda_{DU}) & \lambda_{DU} \\ \mu_{T} & 0 & 0 & -\mu_{T} \end{bmatrix}$$

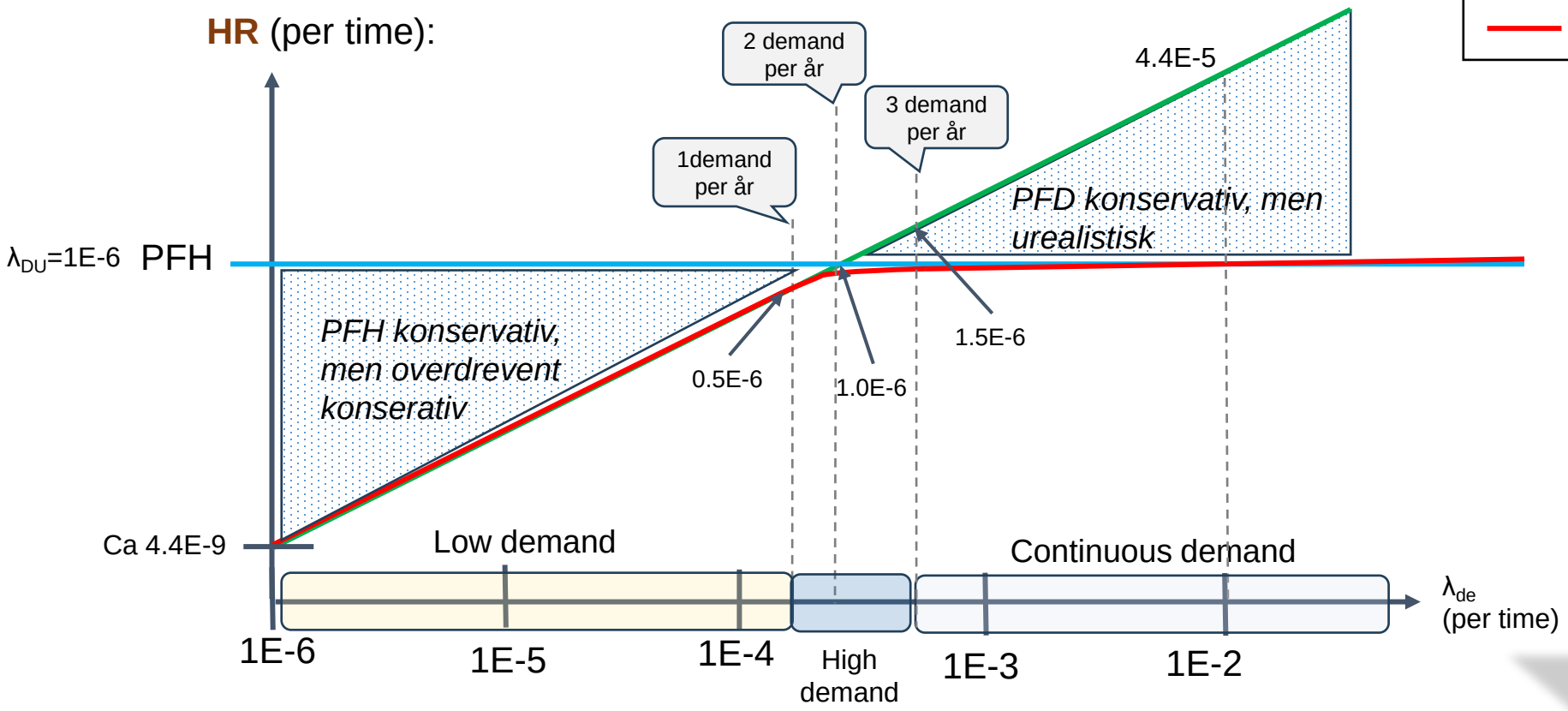
Resultater Markov analyse (rød kurve)

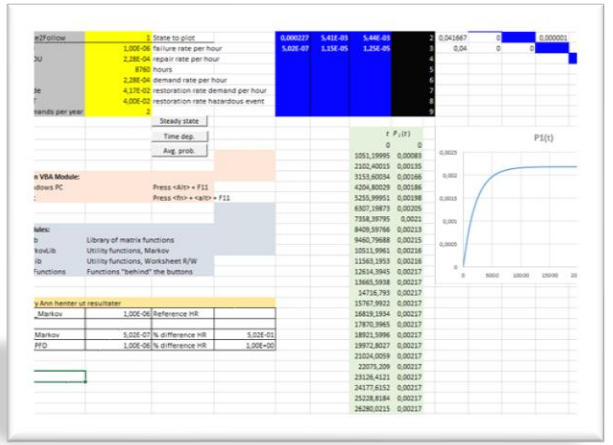
$HR1 = \lambda_{de} \cdot \frac{\lambda_{DU}\tau}{2}$

$HR2 = PFH = \lambda_{DU}$

Håndregnet

$HR0 = \upsilon_3$ fra Markovmodell





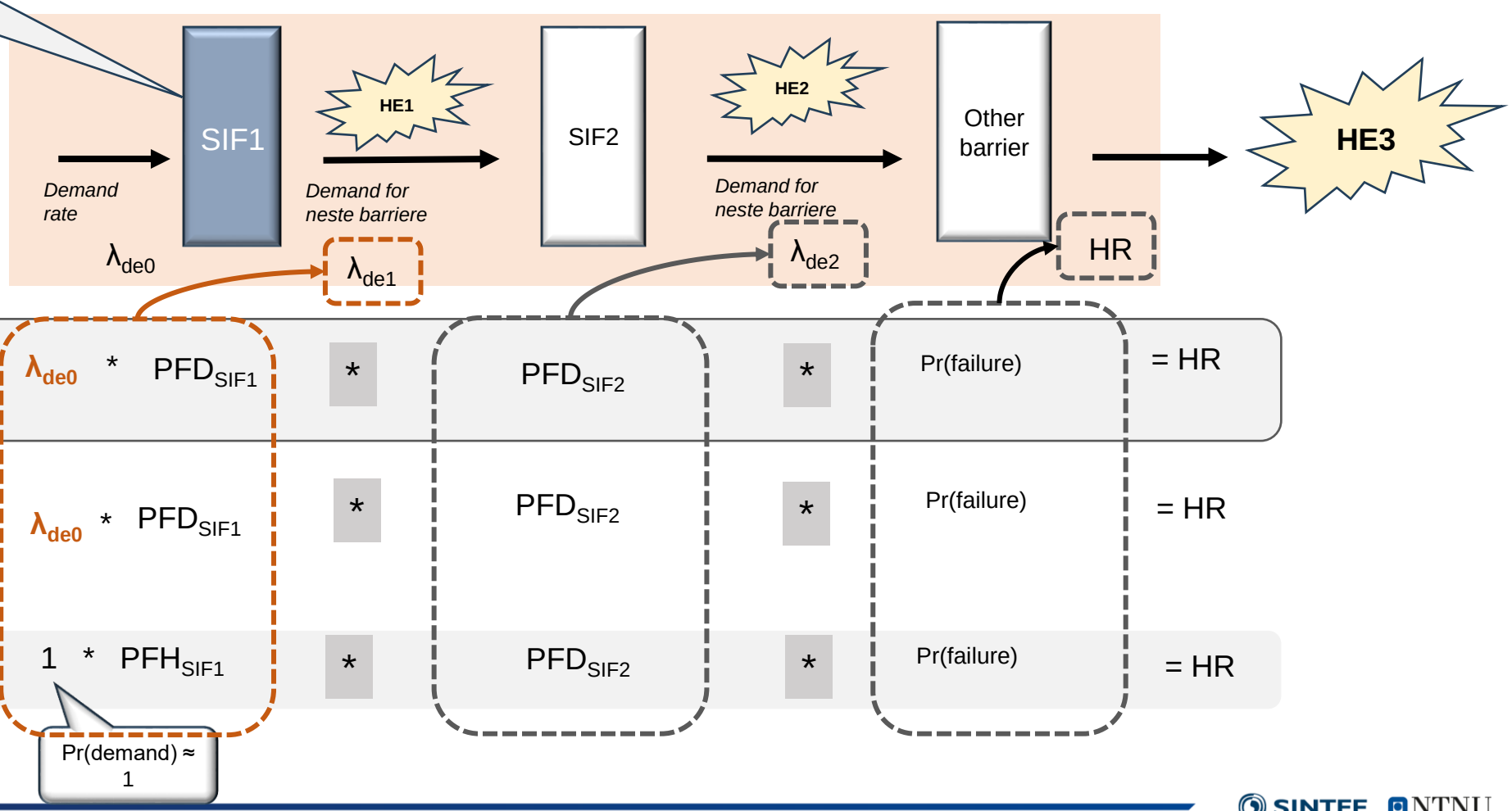
HR: Hazard rate

Eksempler på praktiske kriterier for high-demand

- **PFD** kan benyttes for en SIF som er high-demand dersom:
  - Demand raten i gjennomsnitt er **≤ 2-3 demands per år**
  - SIF testes minst like ofte som demand raten, alternativ med testintervallet angitt av SIL kravet hvis dette blir lavere
  - Eventuelt godta resultater av reelle aktiveringer i beregning av PFD? («Tørke støv» av PDS metoden appendiks E)
- **Feiltoleranse** bestemmes utfra kriteriene for **high-demand**, ikke for low-demand

Implikasjoner hvis flere barrierer

Antagelse: High demand vil bare bli aktuelt for «first in line» barriere ved flere barrierer



Eksempler på kriterier:

$\lambda_{de0} < 1/år$

$Max(\lambda_{de0} \leq 2\text{-}3\ /år, \lambda_{de0} \leq 2/\tau)$

$\lambda_{de0} > 2\text{-}3/år$

Spørsmål til diskusjon

- Er det mange situasjoner der SIFer blir high-demand*?
- Finnes det noen kontinuerlige SIFer*?
- Hva gjør man i dag (når high demand)
- I hvilken grad følger man opp andre (design) krav som følger av at SIFer blir high demand?
- Hvilke synspunkter har man på forslaget til kriterier?

*Andre eksempler enn sikkerhetsfunksjoner og styresystem for maskiner

Fortsatt «cought in the middle»?: High-demand SIFs

Synspunkter, spørsmål?

- Mary Ann Lundteigen, institutt for teknisk kybernetikk
- (mary.a.lundteigen@ntnu.no)