Implementering av IEC 61508 og IEC 61511:

Oppfølging av pålitelighet i driftsfasen

Mary Ann Lundteigen (NTNU/SINTEF)

Agenda

SIS

Krav

Prosedyre

Konklusjoner

Formålet med presentasjonen:

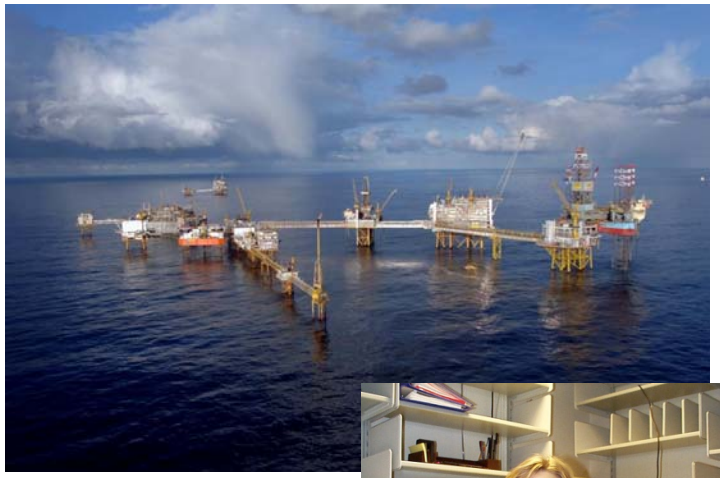
- Gi en kort introduksjon til instrumenterte sikkerhetssystemer (SIS)
- Beskrive krav til oppfølging av pålitelighet i driftsfasen:
  - Myndighetskrav
  - Krav i standardene IEC 61508 og IEC 61511
- Gjennomgå hovedpunkter i ei prosedyre for oppfølging i driftsfasen
  - Utviklet i et forskningsprosjekt i samarbeid med industrien

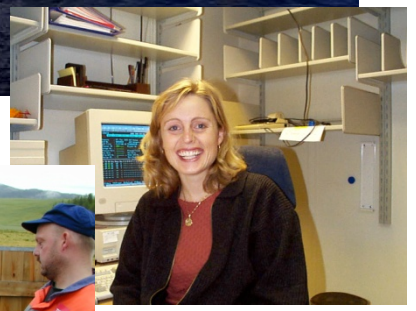
Hovedfokus er presentasjonen er olje og gassvirksomheten, men mye er relevant for andre industrisektorer også

To ord om meg selv

Agenda
SIS
Krav
Prosedyre
Konklusjoner

- Utdannet ved NTH, teknisk kybernetikk i 1993
- Industrierfaring fra Phillips Petroleum (Nå Conoco-Phillips), Nidar og SINTEF
- Jobbet med jernbane og offshore sikkerhetssystemer
- Tok doktorgraden ved NTNU i perioden 2005-2008
- …og er fortsatt ved NTNU



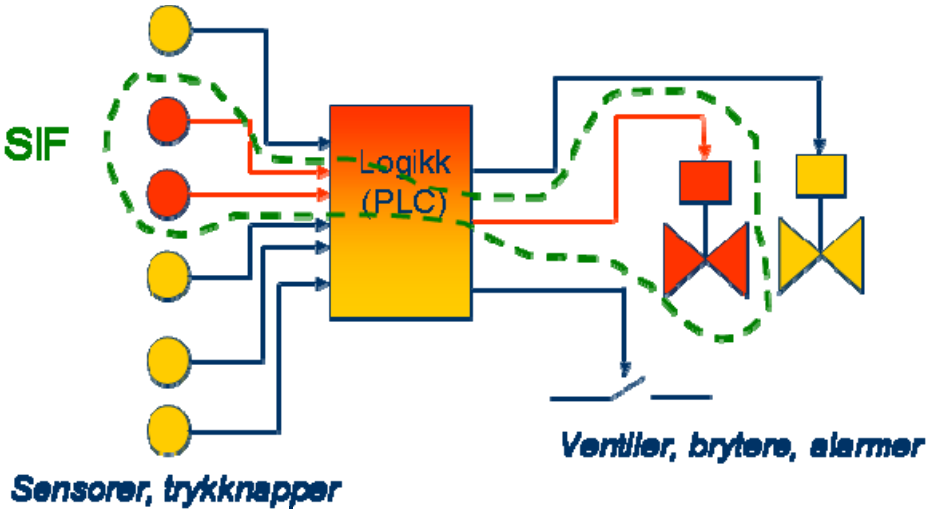


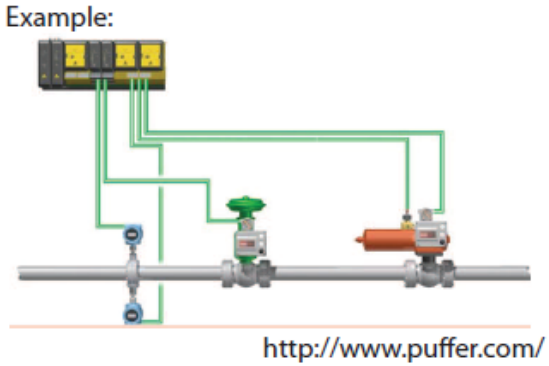
Instrumentert sikkerhetssystem (SIS)

SIS:

Et system som er:

- basert på (blant annet) elektrisk, elektronisk, eller programmerbar elektronisk teknologi
- og som utfører **instrumenterte sikkerhetsfunksjoner** (SIF).





Noen eksempler på SIS

Olje og gass relaterte:

- Nødavstengningssystem (ESD/NAS)
- Brann- og gassdeteksjonssystem (F&G/B&G)
- Prosessnedstengningssystem (PSD/PAS)
- High Integrity Pressure Protection System (HIPPS)

Andre sektorer:

- Signalsystem for tog framføring
- Automatisk sikker lastindikator for kran
- Airbag og ABS bremser i bil

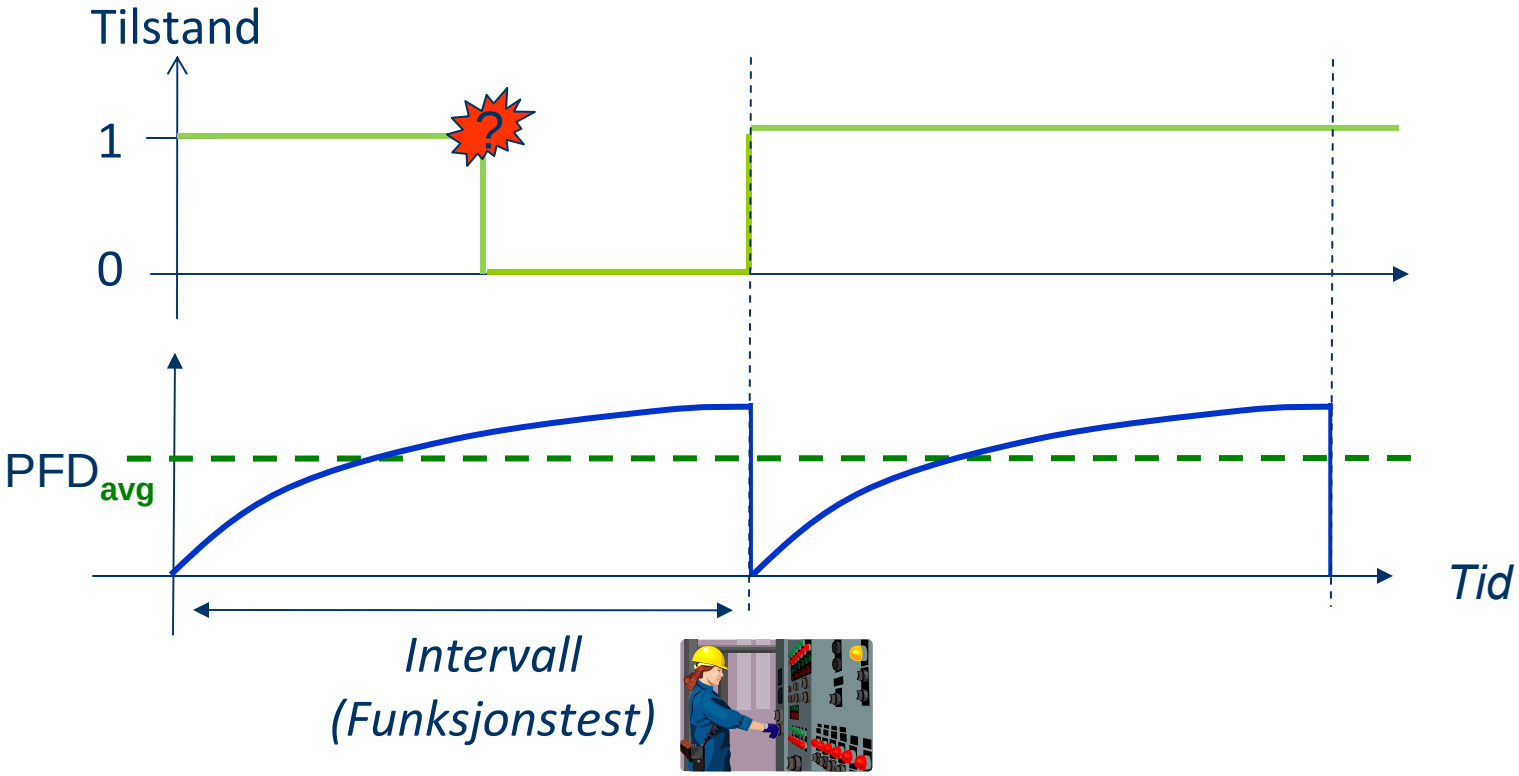
Noen SIS opereres sjelden (”low demand”), mens andre opereres ofte og noen ganger kontinuerlig (”High demand/continuous”).

High demand versus Low demand

System	Low D	High D
Nødavstengningssystem (ESD/NAS)	x	
Brann- og gassdeteksjonssystem (F&G/B&G)	x	
Prosessnedstengningssystem (PSD/PAS)	x	(x)
High Integrity Pressure Protection System (HIPPS)	x	
Signalsystem for tog framføring		x
Automatisk sikker lastindikator for kran	x	
Airbag (bil)	x	
Anti-lock braking system(ABS)		x
Isolering brønn (Del av workover control system)	x?	x?

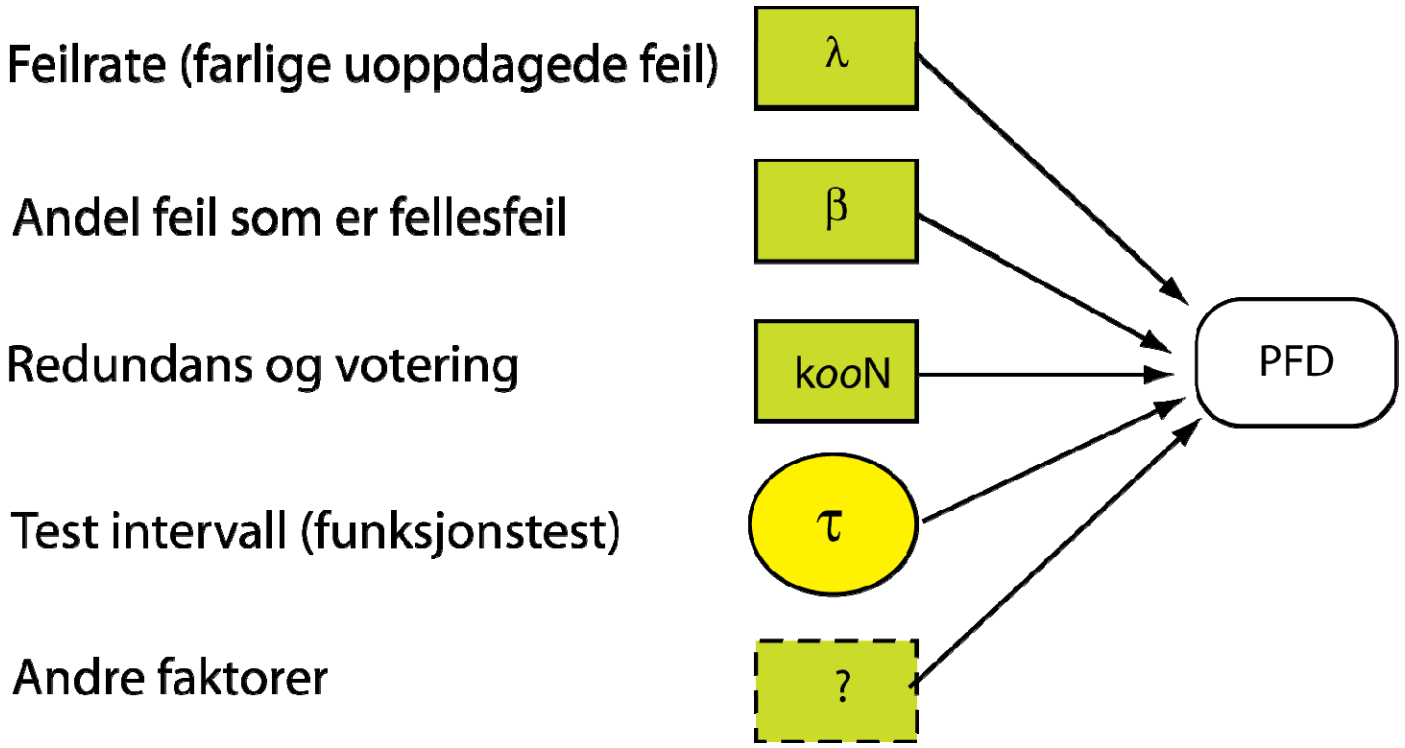
Metoden som presenteres i dag er tilpasset "low demand" systemer

Pålitelighet ("low demand")



- **Bekymring:**
  Uoppdagede farlige feil ("DU feil")
- **Pålitelighetsmål:**
  Probability of failure on demand (PFD)

PFD – når vi regner på det…



"En del faktorer påvirkes primært av beslutninger tatt i design. Feilratene er ukjente størrelser som må bestemmes i driftsfasen. Vår primære beslutnings"-parameter" for å oppnå ønsket pålitelighet er testintervallet."

Oppfølging i SIS i driftsfasen

Agenda
SIS
Krav
Prosedyre
Konklusjoner

Myndigheter gir overordnede krav:

- I Ptil's regelverk sies det blant annet:
  - *Innretningsforskriften §7:*
    Ytelseskrav til sikkerhetsfunksjoner skal etableres
  - *Styringsforskriften §18/Aktivitetsforskriften §44:*
    Data må samles inn og brukes for å vurdere ytelsen
- Ptil refererer til IEC 61508 og OLF 070 (retningslinje for bruk av IEC 61508 og IEC 61511)

IEC standarder for SIS

- IEC 61508 og IEC 61511 er to sentrale standarder i prosessindustrien:
  - IEC 61508:
    I hovedsak for nytt utstyr
  - IEC 61511:
    Sammenstilling av utstyr som er velprøvd eller "sertifisert" i hht. IEC 61508. Til bruk i prosessindustrien.

- OLF 070: Norsk retningslinje (på engelsk) for bruk av disse to IEC standardene *(Kan lastes ned fra www.olf.no under **HMS & drift)***
- IEC standardene skiller mellom **fire** pålitelighetsnivå (SIL 1 til SIL 4)
- For å oppnå et bestemt SIL nivå, stilles flere krav, deriblant krav til PFD

Krav til oppfølging av påliteligheten – IEC

Ved idriftssettelse:

- Testintervall skal være basert på PFD beregninger og valgt slik at SIL kravet er oppfylt

I driftsfasen skal det jevnlig vurderes *om*:

- Feilratene for *farlige (uoppdagede) feil ("DU feil")* er slik de var antatt i design
- Testintervall må justeres bakgrunn av driftserfaring:
  - Feil registrert ved test
  - Feil registrert under drift og ved reelle hendelser

Referanser: OLF 070 (kap 10.8) og IEC 61511(kap 5.2.5.3 og 16.3)

Hvordan overvåke påliteligheten av et SIS i drift?

Når skal test intervallet justeres?

Spørsmål som var sentrale i forskningsprosjekt "Styring og oppfølging av integriteten til SIS" ledet av SINTEF og med støtte fra PDS forum og forskningsrådet.

Hvordan overvåke påliteligheten av et SIS i drift?

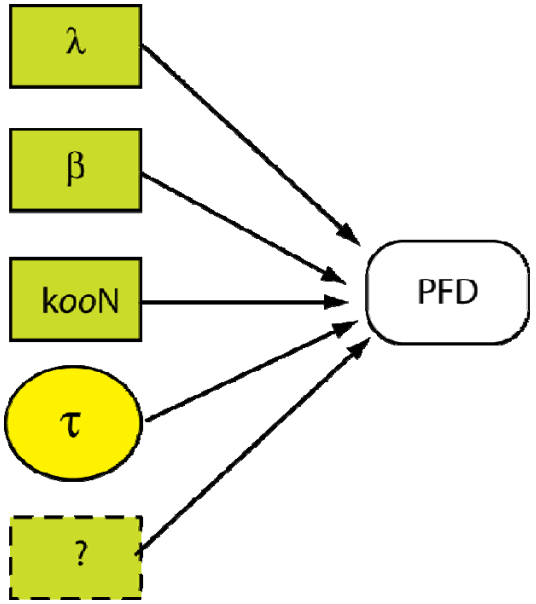
Viktig å kunne si noe om den **erfarte** PFD i forhold til **beregnet** PFD (i design)

Når skal test intervallet justeres?

Det kan vi - hvis vi kan si noe om den **erfarte feilraten** i forhold til den **antatte feilraten**

Antagelser

Påvirkes	Feilrate (farlige uoppdagede feil)	λ
Antas uendret	Andel feil som er fellesfeil	β
	Redundans og votering	kooN
Beslutnings parameter	Test intervall (funksjonstest)	τ
Antas uendret	Andre faktorer	?



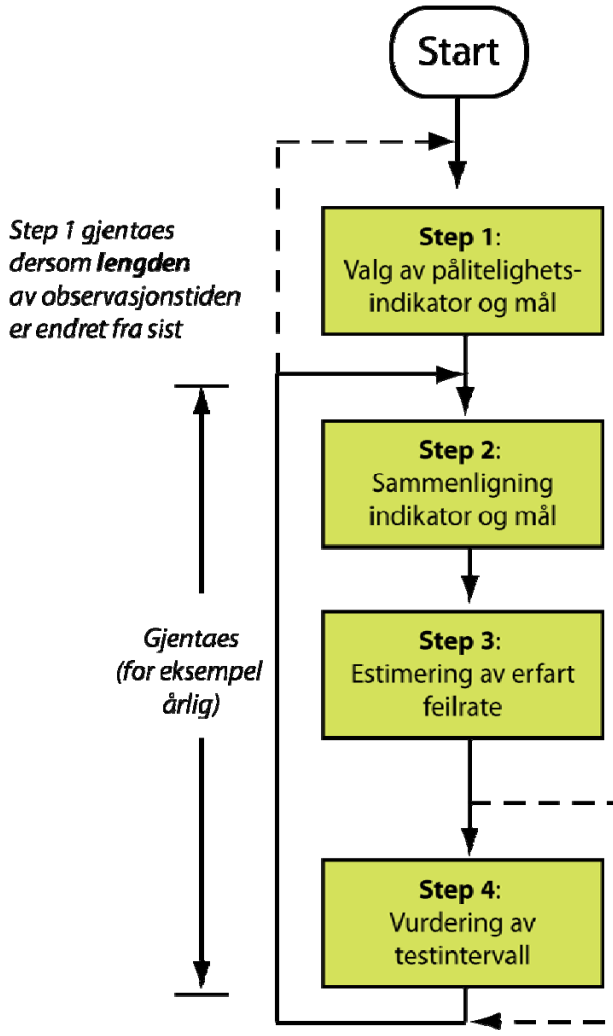
Under disse antagelsene vil $PFD_{op} \leq PFD_{des}$ dersom:

$$\lambda_{op} \cdot \tau_{op} \leq \lambda_{des} \cdot \tau_{des}$$

op= Operasjonell (driftsfasen), des = design

Ny prosedyre

Feilrater kan ikke måles eller observeres direkte, de må estimeres!



- **Indikator:**
  Antall feil x_1 i en periode t
- **Target (i samme periode):**

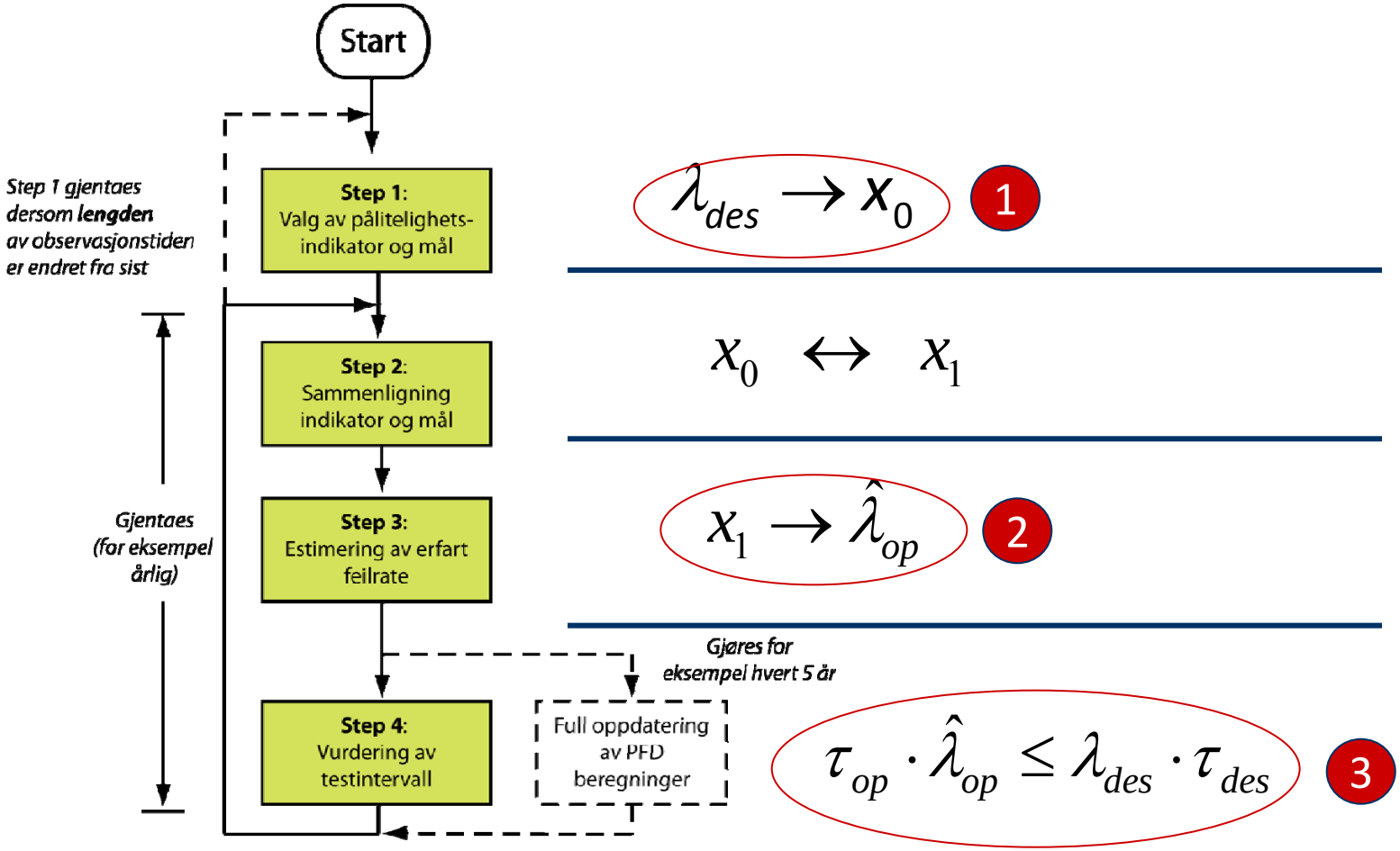
$$\lambda_{des} \rightarrow x_0$$

$$x_0 \leftrightarrow x_1$$

$$x_1 \rightarrow \hat{\lambda}_{op}$$

$$\tau_{op} \cdot \hat{\lambda}_{op} \leq \lambda_{des} \cdot \tau_{des}$$

Ny prosedyre



Ny prosedyre - forklaring

1 $\lambda_{des} \rightarrow x_0$

- Antar at antall feil X(t) i en periode t (målt fra driftsstart) kan modelleres som en Poisson prosess med rate λ_{des}

  Dette betyr at:

  $x_0 = E(X(t)) = \lambda_{des} \cdot t$

Kommentar: Perioden t løper her fra tidspunktet systemet ble idriftssatt.

Ny prosedyre - forklaring

2 $x_1 \rightarrow \hat{\lambda}_{op}$

- Alternativ 1: Kan også her anta at antall feil $X_1(t)$ opptrer som en Poisson prosess.

$$\hat{\lambda}_{op} = \frac{x_1}{t}$$

- **Men**, hvis vi har få hendelser (<2) vil alternativ 1 ha stor usikkerhet.
  Alternativ 2:
  Bayesiansk tilnærming. Feil-raten Λ er gammafordelt med parametre α og γ

$$\gamma = \frac{\lambda_{des}}{\left(\lambda_{cons} - \lambda_{des}\right)^2}$$

og $\alpha = \gamma \cdot \lambda_{des}$

På bakgrunn av ny informasjon:

$$\hat{\lambda}_{op} = \frac{\alpha + x_1}{\gamma + t},$$

Ny prosedyre - forklaring

3 $\tau_{op} \cdot \hat{\lambda}_{op} \leq \lambda_{des} \cdot \tau_{des}$

Tre trinn:

1. Beregn først et foreløpig nytt testintervall (τ_{op}*):

$$\tau_{op}^{*} \leq \frac{\lambda_{des} \cdot \tau_{des}}{\hat{\lambda}_{op}}$$

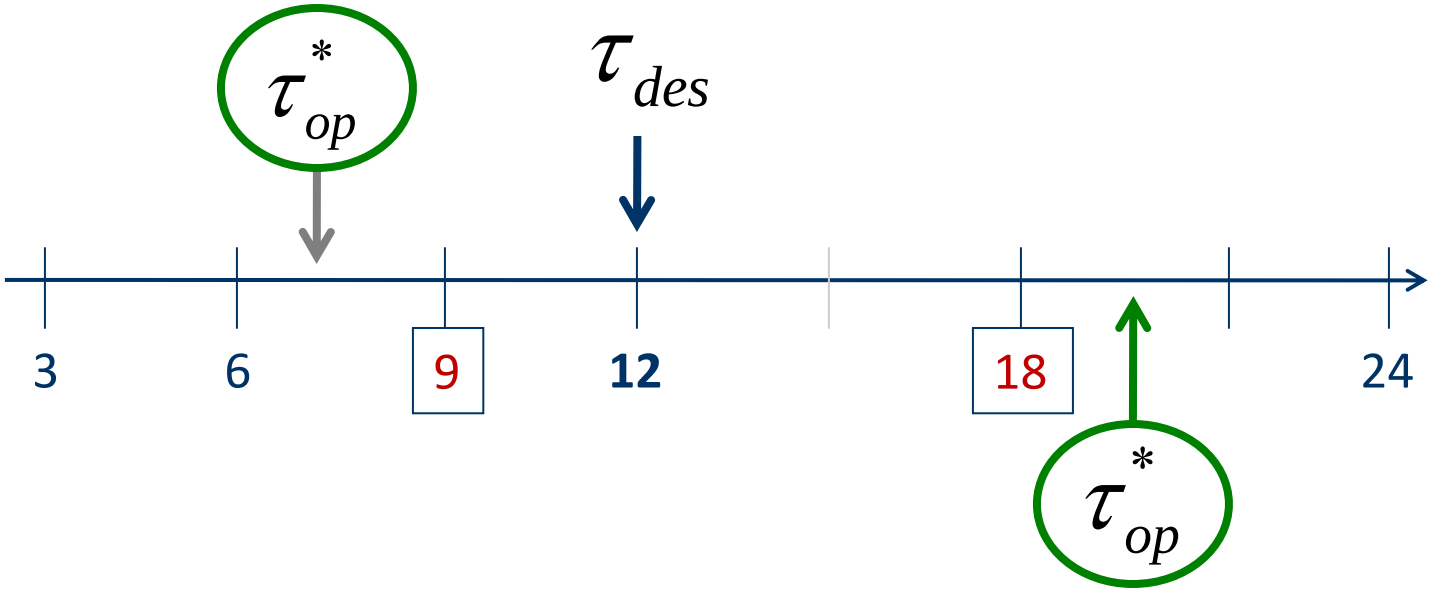
2. Bruk deretter følgende regler for nytt testintervall τ_{op} :

   - Velg blant forhåndsdefinerte intervaller
   - Tillat aldri ***mer*** en dobling eller halvering (på en gang)
   - Dobling og halvering tillates hvis tilleggskriterier er oppfylt

3. Før endelig beslutning tas, må ei sjekkliste gjennomgås

Visualisering

Antagelse: $\tau_{des} = 12$ måneder



Ved dobling eller halvering: 90% konfidensintervall for den *erfarte* feilraten tas også med i vurderingen.

Sjekkliste

Stol ikke på beregninger alene, gå også igjennom følgende sjekkliste:

- Kvalitet, relevans og konfidens (tillit) til innsamlede data
- Kvalitet på funksjonstester (blir virkelig alle feil avdekket?)
- (Antall driftstimer)
- Type feil? Er det for eksempel mange feil som har ***samme*** årsak?
- Ved forslag til å øke testintervallet:
  - Praktiske hensyn dersom testintervallet endres (er det andre grunner til å beholde testintervallet – for eksempel driftshensyn)?
- Har leverandøren anbefalinger som gjør at foreslått endring bør re-vurderes?
- Er det noen sekundære (følge-) effekter som en bør tenke på dersom testintervallet økes eller reduseres (økt slitasje, mer sannsynlig for gjengroing osv)

Eksempel

- **En DU feil** har blitt registrert I løpet av **tre års drift** for **35** blow-down ventiler. Akkumulert driftstid er $9.2 \cdot 10^5$ timer.
- Feilraten som ble antatt i design er **$2.9.10^{-6}$ feil/time** og et testintervall på **12** måneder ble valgt for å oppfylle SIL kravet.
- Spørsmål:
  a) Hvordan samsvarer erfart pålitelighet med forventet?
  b) Og bør testintervallet endres?

Svar på a) - Forventet versus erfart pålitelighet:

- Antall forventede feil i perioden er $2.9.10^{-6}$ feil/time $\cdot$ 3 $\cdot$ 8760 (timer per år) = 2.7 feil
- Dette betyr at påliteligheten ser ut til å være bedre enn forventet etter 3 år.

Men er påliteligheten så god at testintervallet kan endres? -> b)

Eksempel

Svar på b) – Kan testintervallet reduseres?

- Fordi det er registrert en DU feil, anbefales bayesiansk metode for beregning av erfart feilrate
- Konservativ feilrate antas 2 ganger design feilrate

$$\gamma = \frac{\lambda_{des}}{\left(2\cdot\lambda_{des} - \lambda_{des}\right)^2} \approx 3.5\cdot 10^5 \text{ timer}$$

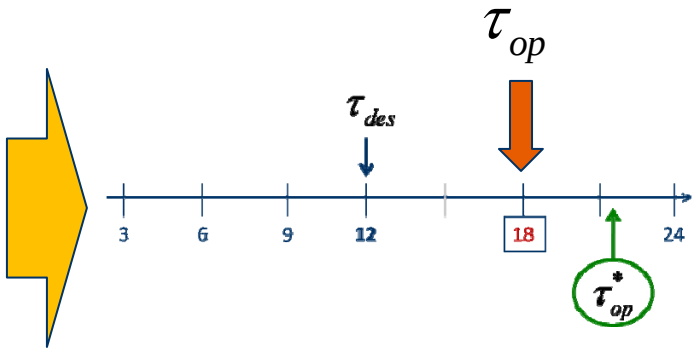
$$\text{og } \alpha = \gamma\cdot\lambda_{des} = 1 \text{ (feil)}$$

$$\rightarrow \hat{\lambda}_{op} = \frac{1+1}{3.5\cdot 10^5 + 9.2\cdot 10^5} \approx 1.6\cdot 10^{-6} \text{ feil/time}$$

Betyr at

$$\tau_{op}^{*} = \frac{2.9\cdot 10^{-6}\cdot 12}{1.6\cdot 10^{-6}} \approx 22 \text{ mnd}$$

Svar: Nytt intervall er 18 mnd



Konklusjon

- Påliteligheten til instrumenterte sikkerhetssystemer må overvåkes i driftfasen
- Prosedyren som er foreslått sier noe om hvordan ***en del av*** kravene til pålitelighet kan følges opp
- Den erfarte PFD kan brukes som beslutningstøtte når det gjelder valg av testintervall
- **Ikke** bruk PFD for mer enn den er verdt!

Takk for oppmerksomheten!

Ta gjerne kontakt med meg -
mary.a.lundteigen@ntnu.no
for mer diskusjon og synspunkter!

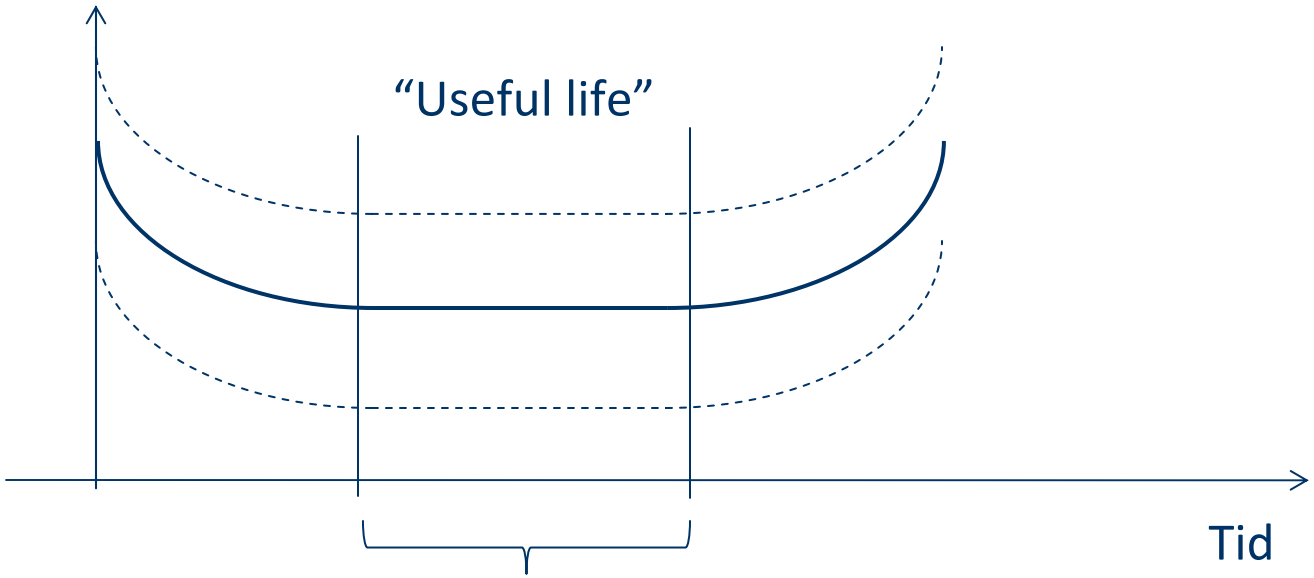
…eller besøk www.sintef.no/pds
for dette prosjektet og annen info om PDS.

RAMS aktiviteter på NTNU finner dere på:
www.ntnu.no/ross/rams

Rapport om oppfølging av SIS (fritt tilgjengelig)

SINTEF A8788 Guidelines for follow-up of Safety Instrumented Systems (SIS) in the operating phase (2008):
http://www.sintef.no/Teknologi-og-samfunn/Sikkerhet/Rapporter--Reports/

Feilrate (ROCOF)



"Feilraten antas å være konstant, men vi vet ikke hvilken verdi den har. I design, gjør vi antagelser om denne verdien basert på historiske data og ekspertvurdering. I driftsfasen samler vi inn data for å for finne den "sanne" verdien. Den "sanne" verdien vil påvirkes av drift, vedlikehold, og miljøbetingelser."

ROCOF: Rate of occurrence of failures