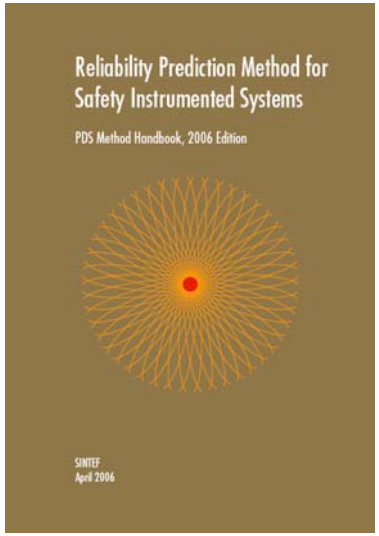
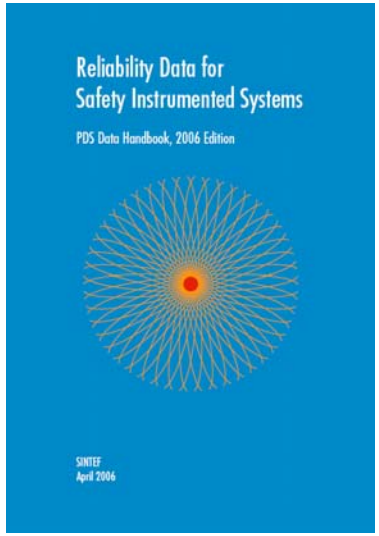
# Revidert PDS metode og håndbøker




PDS forum møte 5. april 2006

Stein Hauge og Knut Øien, SINTEF

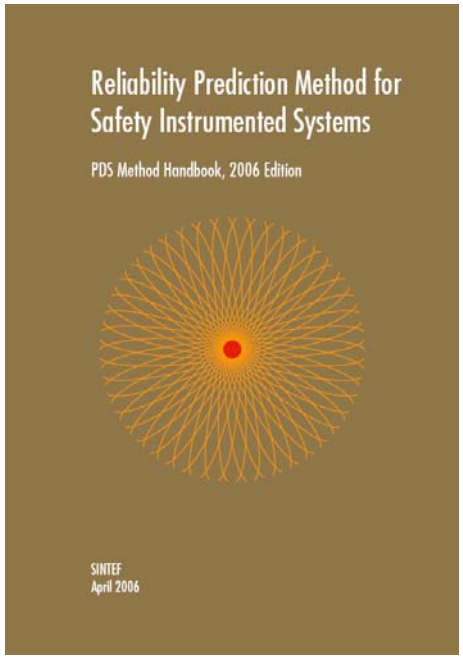
# Innhold

1. PDS metoden – ny revisjon av metodehåndboka

2. Ny revisjon av PDS datahåndboka

3. Applikasjonsspesifikke modeller
   - Systematiske feil
   - Fellesfeil
   - Testuavhengige feil

# Del 1
# PDS metoden – ny revisjon av metodehåndboka



# Hva er PDS metoden?

- PDS metoden brukes for å kvantifisere sikkerhets- og pålitelighetsmål knyttet til instrumenterte sikkerhetssystemer
- Metoden gir også formler for å beregne tapt produksjon som en følge av feil (tripp) av sikkerhetssystemene
- Den siste oppdateringen av metoden har hovedsakelig fokusert på sikkerhets- / pålitelighetsaspekter

**Metoden fokuserer altså på den kvantitative delen av IEC 61508 / 61511**

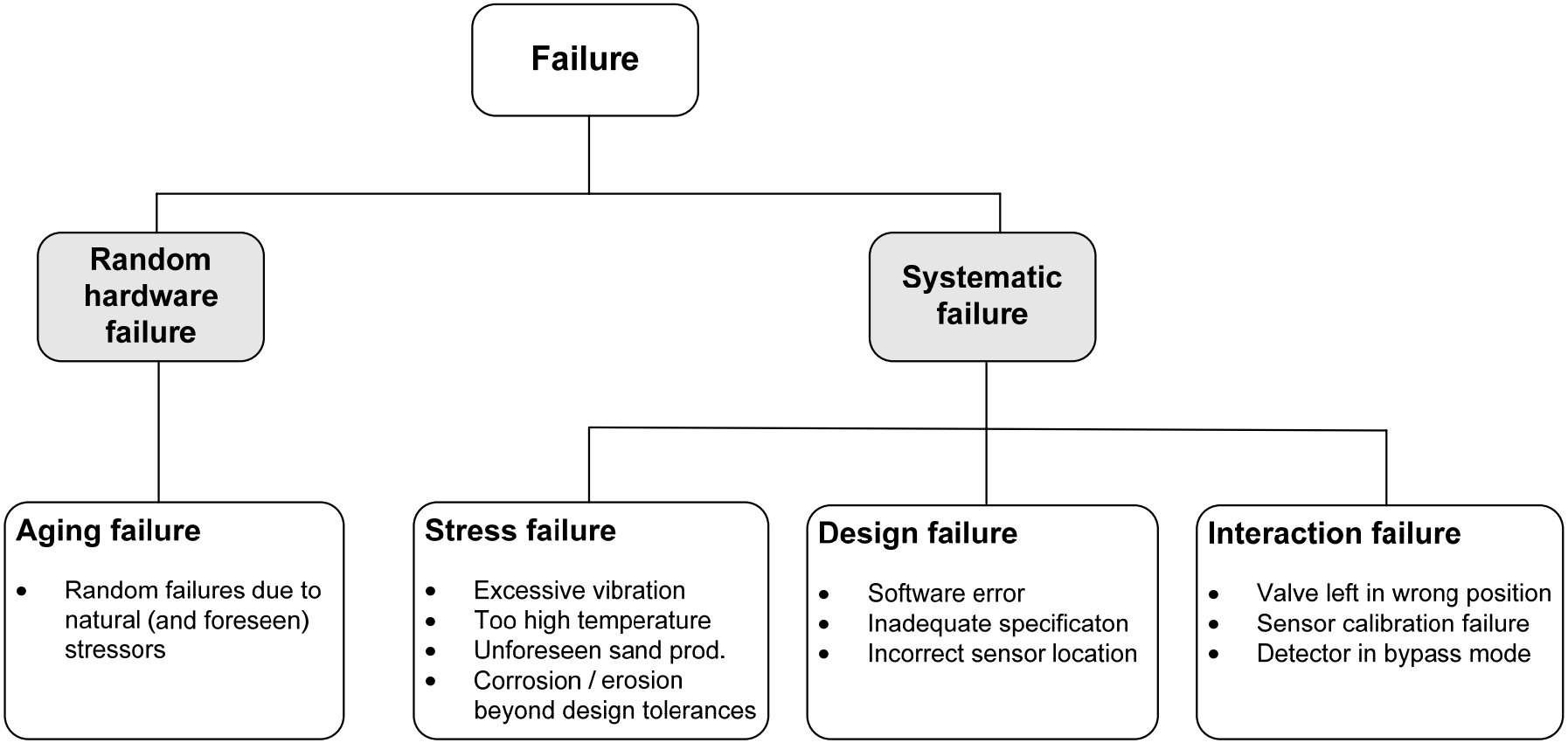
# Viktige egenskaper ved PDS-metoden

- Presenterer forholdsvis enkle beregningsformler med tilhørende (tilpassede) erfaringsdata
- Inkluderer hele "sløyfa" (sensor, logisk enhet, ventil)
- Inkluderer ”alle” realistiske feilårsaker og feilmoder
- Tallfester også systematiske feil
- Tar høyde for ulike typer testing og deteksjonsmåter
- Tallfester både "Fail-to-operate" og "Spurious operation”

# Hva er nytt i PDS metoden?

- Revidert feiltaksonomi - stressfeil (utover designspesifikasjon) defineres som en type systematisk feil
- Revidert tilnærming til modellering av systematiske feil
- Farlige udetekterbare feil ($\lambda_{DU}$) er delt opp i bidrag fra tilfeldige hardware feil og fra systematiske feil ($\lambda_{DU-RH}$ og $\lambda_{DU-S}$)
- Sikkerhetsutilgjengelighet knyttet til reparasjon og testing/vedlikehold er samlet i ett felles begrep; DTU
- Forenklet fellesfeilmodell hvor $\beta$ og $\beta_{SF}$ er slått sammen til en felles $\beta$
- Nye modeller for å beregne applikasjonsspesifikk $\lambda_{DU-S}$, $\beta$ og $P_{TIF}$

# Ny taksonomi for feilårsaker



# Systematiske feil – IEC 61508 vs. PDS

## IEC 61508

failure related in a deterministic way to a certain cause, which can only be eliminated by modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

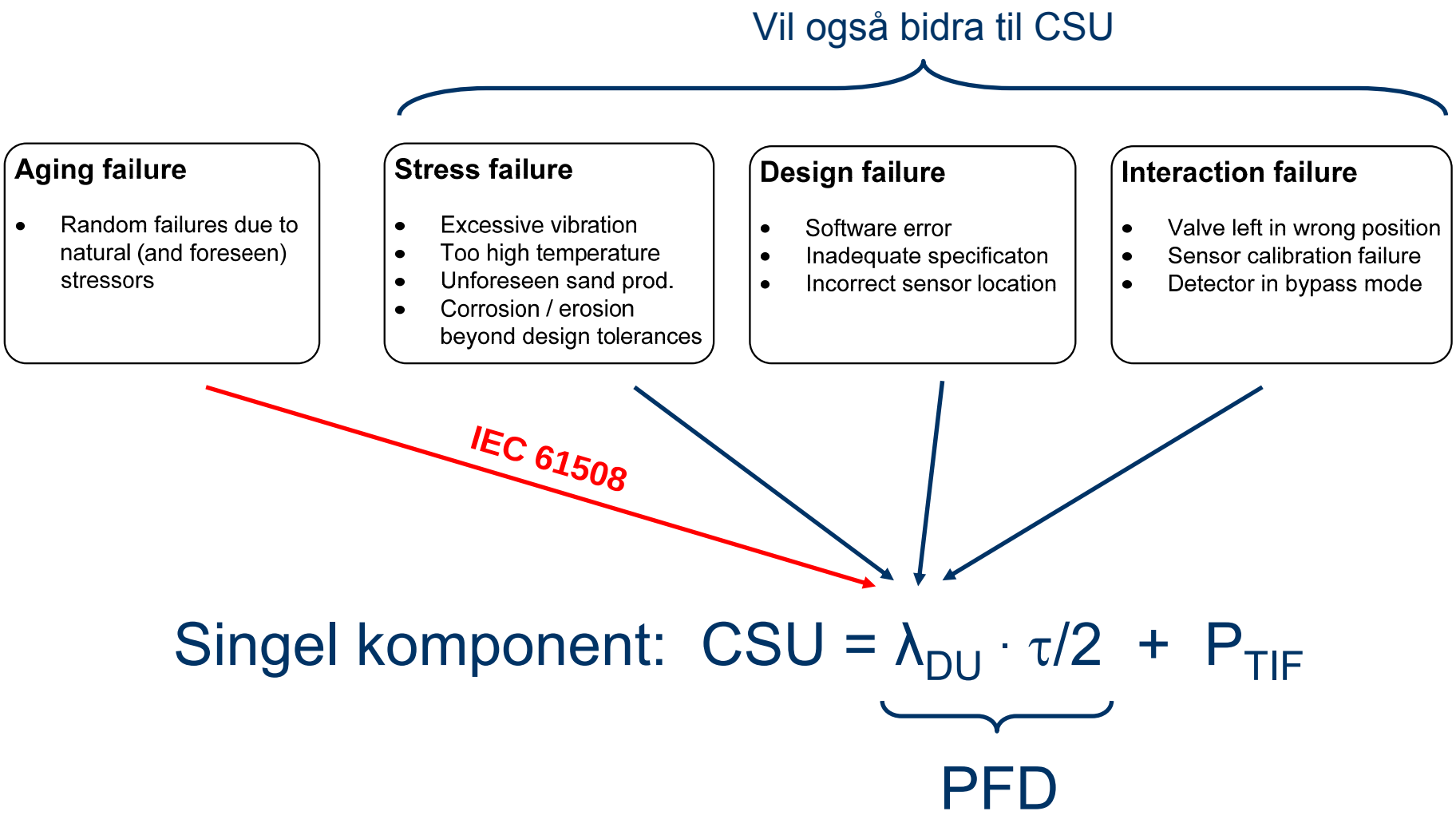
## PDS

failures that can be related to a particular cause other than natural degradation (aging). The failure can normally be eliminated by a modification, either of e.g. the design or manufacturing process, the operating procedures or documentation…….

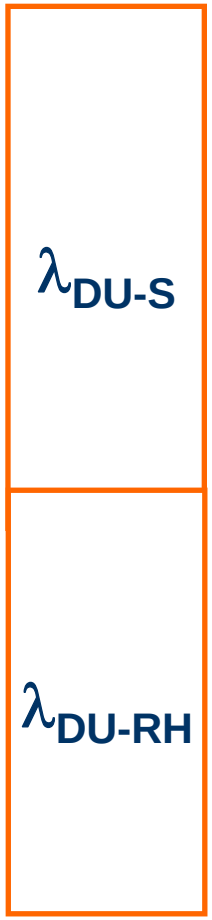
# Hvorfor kvantifisere også de systematiske feilene?

- Systematiske feil er ofte en hovedbidragsyter inn mot feilsannsynligheten til utstyret
- Når vi gjør pålitelighetsberegninger ønsker vi gjerne å predikere hvordan utstyret faktisk kommer til å oppføre seg “i felt”
- Tilsvarende i QRA er det viktig å bruke realistiske feilsannsynligheter for å reflektere den faktiske risikoen
- Feilrater gitt i ulike datakilder og håndbøker er basert på operasjonell erfaring og inkluderer derfor også systematiske feil. Med andre ord ”regner vi allerede med” de systematiske feilene!
- Når vi innfører tiltak for å redusere systematiske feil, ønsker vi (ideelt sett) å kunne kvantifisere effekten av disse, også for singel systemer.

# Kvantifisering av feilsannsynlighet - CSU



# $\lambda_{DU}$ vil bestå av "to deler"




Bidrag fra systematiske feil, dvs. feil i utstyret knyttet til feil bruk, feil vedlikehold, eller "galt" miljø. Kan også inneholde designfeil.

- Inkluderes ikke i $\lambda_{DU}$ ved streng fortolkning av IEC
- Kan påvirkes gjennom ulike tiltak fra operatøren
- Typisk kilde for fellesfeil

Bidrag fra tilfeldige hardware feil, dvs. feil i utstyret som skyldes naturlig aldring.

- Tilsvarer $\lambda_{DU}$ i streng IEC forstand
- Gir ikke fellesfeil

**NB! Normalt trenger vi kun å forholde oss til $\lambda_{DU}$ (= $\lambda_{DU-RH}$+ $\lambda_{DU-S}$)**

# Vi får tre hovedbidragsytere til sikkerhetsutilgjengeligheten (CSU):

1. Tilfeldige hardware feil som vil avdekkes ved funksjonell testing (med rate $\lambda_{DU\text{-}RH}$)
2. Systematiske feil som vil avdekkes ved funksjonell testing (med rate $\lambda_{DU\text{-}S}$)
3. ”Test uavhengige” feil som bare opptrer ved en faktisk demand, med sannsynlighet $P_{TIF}$

Singel komponent: $CSU = \underbrace{(\lambda_{DU\text{-}RH} + \lambda_{DU\text{-}S})}_{\lambda_{DU}} \cdot \tau/2 + P_{TIF}$

# Downtime unavailability - DTU

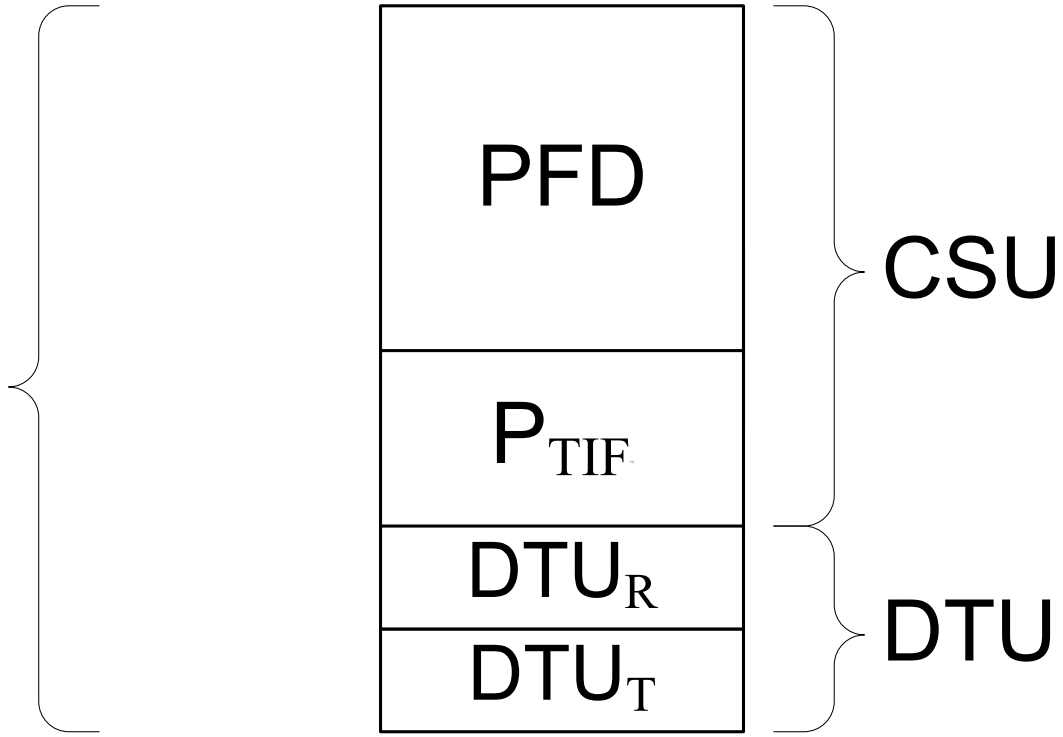
Vi har to bidrag til DTU:

1. Utilgjengelighet som skyldes reparasjon av farlige feil. Vi kaller denne for $DTU_R$ (erstatter tidligere $PFD_K$)
2. Utilgjengelighet som skyldes funksjonell testing / preventivt vedlikehold. Vi kaller denne for $DTU_T$ (erstatter tidligere NSU)

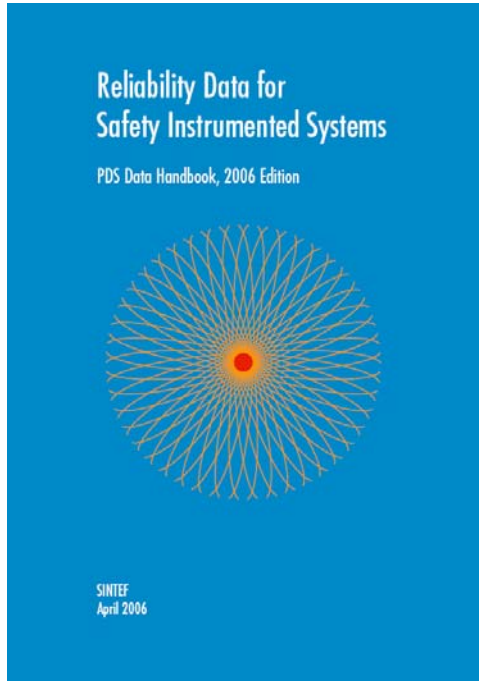
**Bidraget fra DTU vil avhenge av operasjonsfilosofien knyttet til henholdsvis reparasjon og testing/vedlikehold**

# Total sikkerhetsutilgjengelighet - $CSU_{TOT}$

$CSU_{TOT}$
(incl. downtime unavailability)



# Del 2
# Ny revisjon av datahåndboka



# Sentrale datakilder / input

- OREDA® databasen fase III, IV og V og OREDA® håndbøker
- Data fra RNNS for sikkerhetskritisk utstyr
- Diskusjoner og samtaler med eksperter, samt egne (SINTEF) vurderinger
- Andre datahåndbøker

# Ny revisjon av datahåndboka (1)

- Inputdata og parametere er gjennomgått og oppdatert i henhold til ny taksonomi og modeller
- Tabellene i datadossieret er gjennomgått og oppdatert
- Estimater for $r = \lambda_{DU\text{-}RH} / \lambda_{DU}$ (dvs. andelen av $\lambda_{DU}$ som kan tilskrives tilfeldige hardware feil) er gitt for ulike utstyr
- Verdier for $P_{TIF}$ er gjennomgått og oppdatert
  - For B&G detektorer antar vi nå **eksponert detektor**. Dette er i tråd med OLF-GL, og baserer seg på at sannsynlighet for eksponering dekkes i andre analyser (risikoanalysen)
  - For ESV/XV ventiler er det skilt mellom hvordan ventilene testes
- $\beta$ og $\beta_{SF}$ er slått sammen (vektet) til en ny felles $\beta$

# Ny revisjon av datahåndboka (2)

- En del feilrater og coverage verdier er oppdatert
- Data for PSV er gitt som to ulike feilrater;
  - for feil ved +20% av sett punktet for ventilen.
  - for feil ved testtrykk.
- Data for brytere og reléer er inkludert
- Data for ”field bus coupler” og ”field bus CPU/ communication unit” er tatt ut av boka

# Del 3
# Applikasjonsspesifikke modeller

Pålitelighetsberegninger for et bestemt / spesifikt anlegg

# Innledning

Hensikten med å utvikle applikasjonsspesifikke modeller er at pålitelighetsberegningene skal bli mer representative for et bestemt anlegg, og at de skal bidra til å gi kreditt for spesifikke tiltak som reduserer muligheten for feil. Målet er dermed todelt:

1. Å redusere muligheten for feil (systematiske feil og fellesfeil) på et bestemt anlegg ved å iverksette hensiktsmessige tiltak
   - Her har utstyrsleverandører og –brukere et hovedansvar, fordi de vet best hvilke tiltak som er aktuelle, hvilke som er vanlig praksis, og hvilken effekt tiltakene gir. ”Bevisbyrden” for å identifisere egnede spesifikke tiltak samt å bedømme effekten av disse er derfor lagt til utstyrsleverandører og –brukere (*troverdighet*)
2. Å gi kreditt for tiltakene i pålitelighetsberegningene
   - Nå lagt til rette for i PDS gjennom enkle applikasjonsspesifikke modeller (*enkelhet*)

# Innledning, forts.

- Standard pålitelighetsberegninger baserer seg i utgangspunktet på parameterverdier (f.eks. $\beta$, $\lambda_{DU}$, og $P_{TIF}$) hentet fra datahåndbøker og databaser hvor verdiene er gjennomsnittsverdier for én type utstyr for mange anlegg
- Verdiene er ikke representative for et bestemt anlegg, og de bidrar *ikke* til å gi kreditt for spesifikke tiltak på et bestemt anlegg
- I PDS er det nå utviklet enkle modeller for å tilpasse gjennomsnittlige parameterverdier til applikasjonsspesifikke verdier
- Konkret skjer dette gjennom applikasjonsspesifikk håndtering av ***systematiske feil*** og ***fellesfeil*** ved at tiltak for å forhindre eller kontrollere slike feil påvirker verdiene for $\beta$, $\lambda_{DU\text{-}S}$ og $P_{TIF}$

# Innledning, forts.

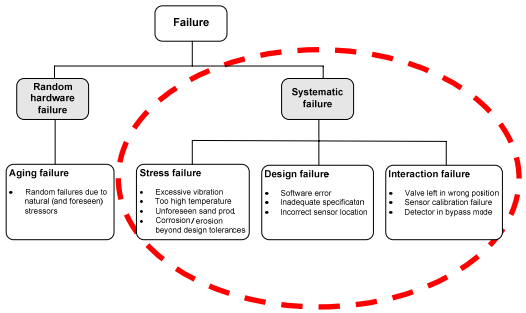
- Forenklet formel for votert (MooN) system:

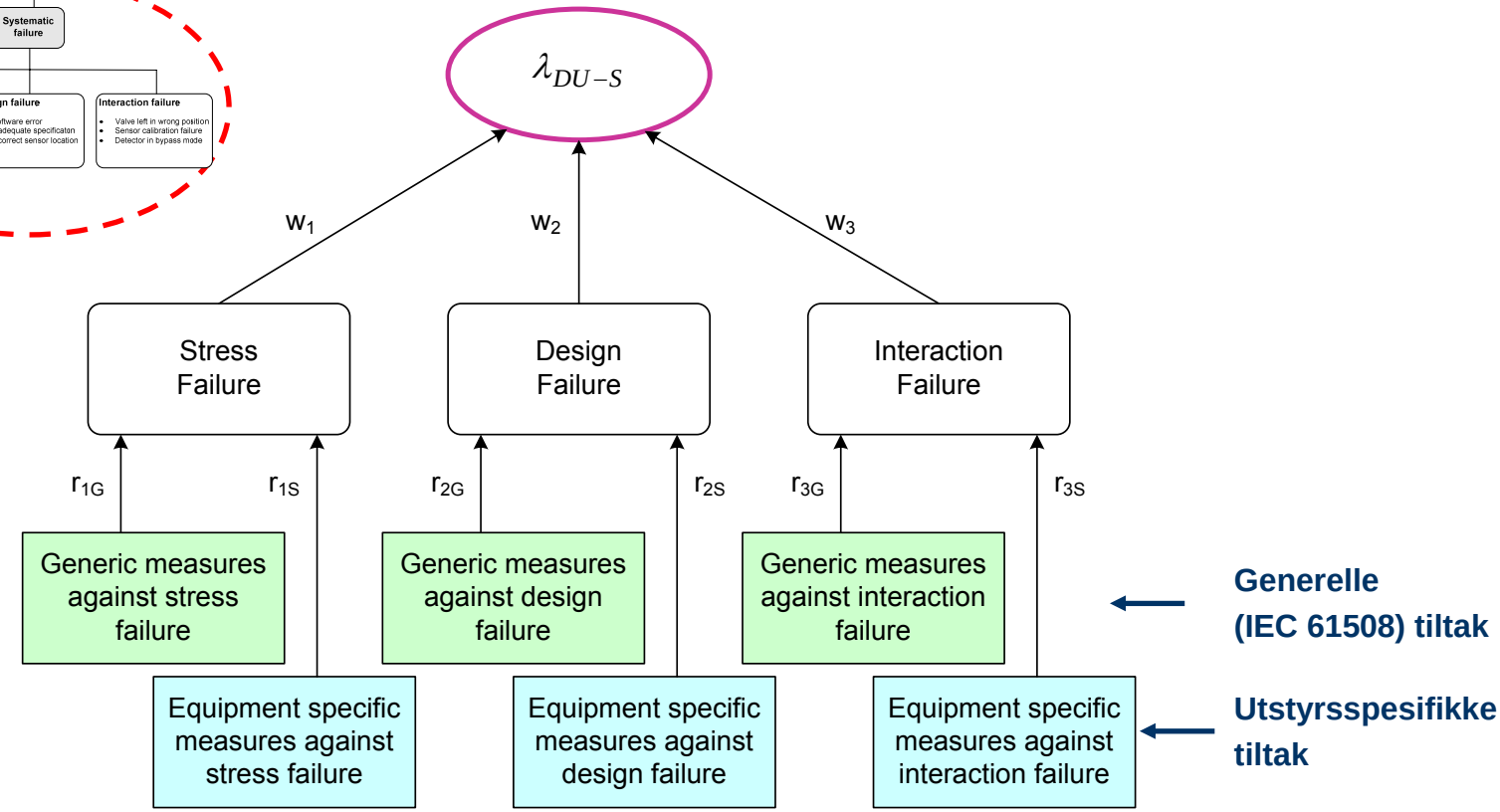
$$CSU(MooN) = c_{MooN} \cdot \beta \, (\lambda_{DU} \cdot \tau/2 + P_{TIF})$$

$$CSU(MooN) = c_{MooN} \cdot \beta \, [(\lambda_{DU\text{-}RH} + \lambda_{DU\text{-}S}) \cdot \tau/2 + P_{TIF}]$$


- Samme tiltak kan påvirke flere parametere, men for å forenkle modelleringen antar vi at de fleste tiltak påvirker $\lambda_{DU\text{-}S}$, noen få tiltak (f.eks. diversitet) påvirker $\beta$ og at det i hovedsak er fullstendighet / kvalitet av funksjonstest som påvirker $P_{TIF}$

# 1. Modell for applikasjonsspesifikk $\lambda_{DU-S}$



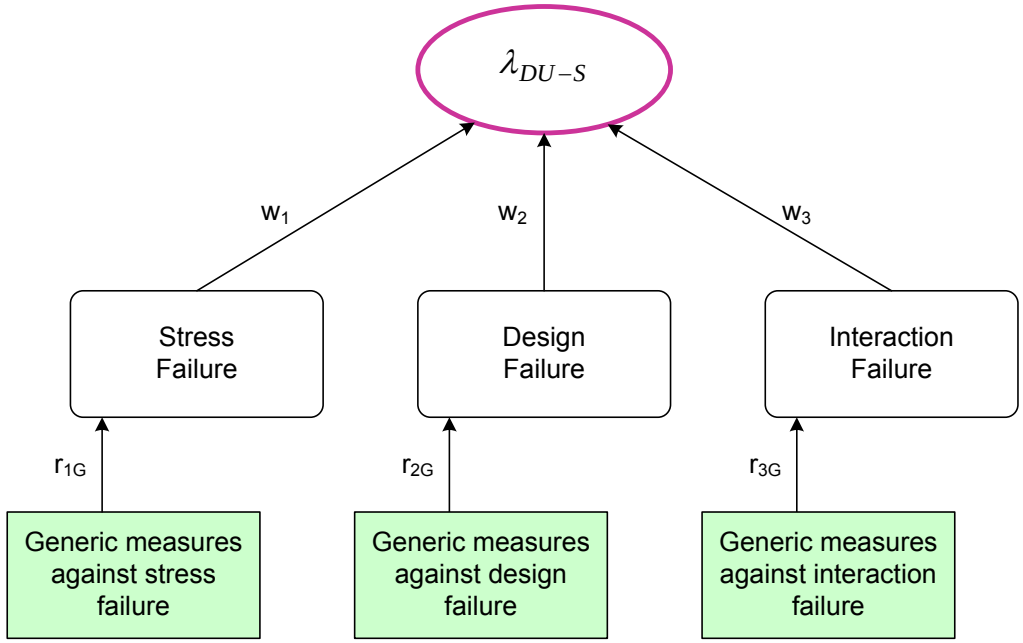




$$\lambda_{DU\text{-}S}^{*} = \lambda_{DU\text{-}S}\left(w_1 \cdot r_{1G} \cdot r_{1S} + w_2 \cdot r_{2G} \cdot r_{2S} + w_3 \cdot r_{3G} \cdot r_{3S}\right)$$

# Modellparametere ($w_i$, $r_{iG}$, $r_{iS}$)

- $w_i$ er en ”vekt” som angir andelen av feilraten som skyldes feilårsaks-kategori *i*; stressfeil (*i*=1), designfeil (*i*=2), interaksjonsfeil (*i*=3)
- $r_{iG}$ angir endring i feilraten ($\lambda_{DU-S}$) pga *generelle tiltak* for å forhindre eller kontrollere systematiske feil av feilårsakskategori *i*
  - $r_{iG}$ angir i hvilken grad de anbefalte tiltak i IEC 61508 er fulgt
  - $r_{iG}$=1 indikerer at obligatoriske tiltak er gjennomført (= vanlig praksis til nå)
- $r_{iS}$ angir endring i feilraten ($\lambda_{DU-S}$) pga *utstyrsspesifikke tiltak* for å forhindre eller kontrollere systematiske feil av feilårsakskategori *i*
  - $r_{iS}$ angir i hvilken grad utstyrsspesifikke tiltak og egenskaper går utover det som er vanlig for denne type utstyr
  - $r_{iS}$=1 indikerer at de utstyrsspesifikke tiltak og egenskaper til utstyret benyttet på dette bestemte anlegget er i samsvar med vanlig praksis

# Generelle tiltak og valg av $r_{iG}$-verdier




- Functional testing under environmental conditions
- Interference surge immunity testing
- Measures against voltage breakdown, overvoltage, ..
- Separation of electrical energy lines
- Increase of interference immunity
- Measures against the physical environment
- Fault insertion testing

- Observance of guidelines and standards
- Functional testing (integration)

- Operation and maintenance instructions
- User friendliness
- Maintenance friendliness
- Modification protection

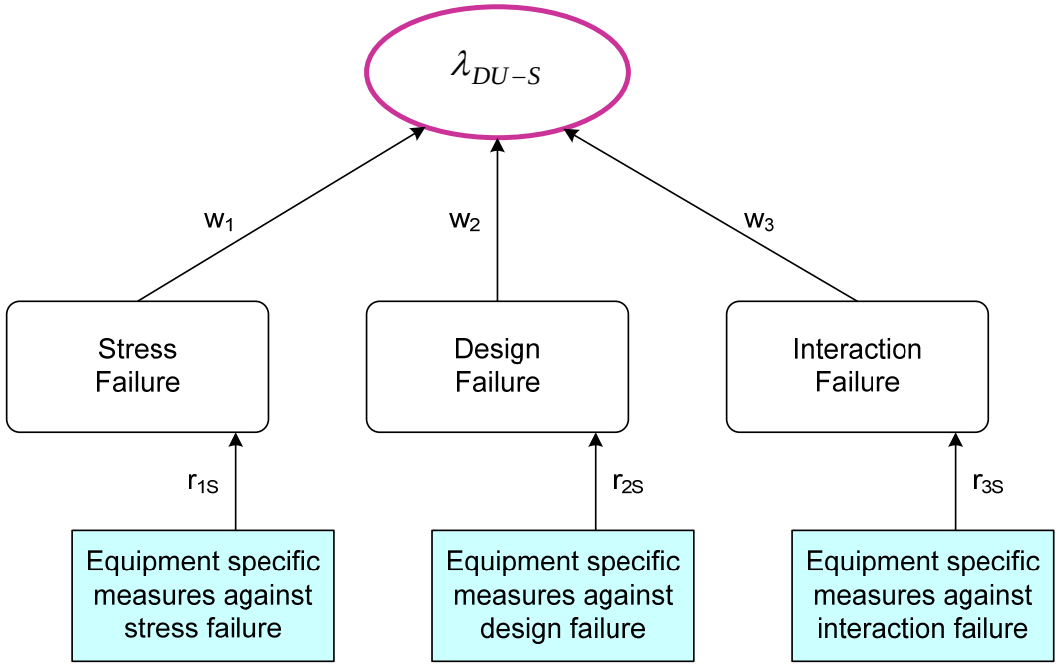
| $r_{iG}$ | **Compliance with IEC 61508 (Tables B.1 – B.5 and A.16 – A.18 in Part 2)** |
|---|---|
| 0.1 | All measures are complied with |
| 0.3 | Mandatory and several highly recommended measures are complied with |
| 1 | Mandatory measures are complied with |
| 10 | (All) mandatory measures are not complied with |

# Krav til dokumentasjon for valgt $r_{iG}$

| $r_{iG}$ | **Compliance with IEC 61508 (Tables B.1 – B.5 and A.16 – A.18 in Part 2)** |
|---|---|
| 0.1 | All measures are complied with |
| 0.3 | Mandatory and several highly recommended measures are complied with |
| 1 | Mandatory measures are complied with |
| 10 | (All) mandatory measures are not complied with |

- Angitte verdier er veiledende og det kan argumenteres for andre verdier
- Default settes $r_{iG}$ til 10, og det må begrunnes og dokumenteres dersom $r_{iG} \leq 1$ benyttes. Dette gjelder også for $r_{iG} = 1$.
- For å benytte eksempelvis $r_{1G} = 0.5$ betyr det at man har implementert alle obligatoriske tiltak samt noen sterkt anbefalte tiltak, OG man antar at disse tiltakene vil bidra til å redusere feilraten av systematiske feil ($\lambda_{DU\text{-}S}$) som skyldes stressfeil med 50%. Denne vurderingen må begrunnes (sannsynliggjøres) og dokumenteres.
- Tilsvarende krav til begrunnelse og dokumentasjon gjelder for $r_{iS}$

# Utstyrsspesifikke tiltak og valg av $r_{iS}$-verdier




- Protection by valve housing
- Use of heat tracing
- Fluid not vulnerable to hydrates formation
- Production ensured within design envelope
- Purity requirements for fluid and air fulfilled

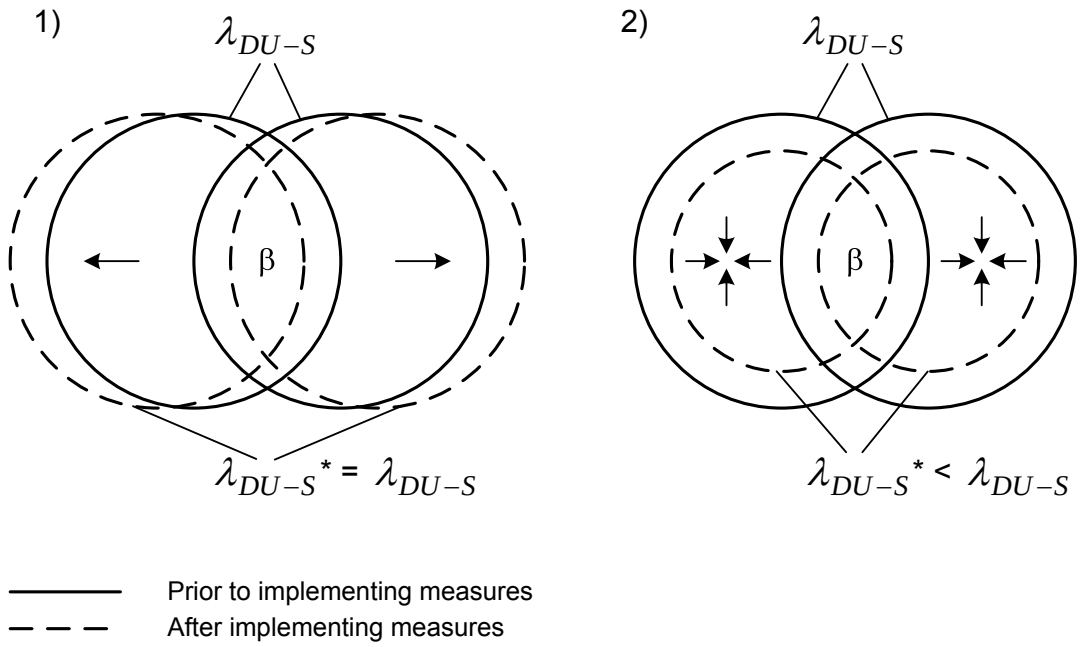
- Favourable function principle (e.g. single versus double acting actuator)
- Capable manufacturer (reliable equipment)

- Favourable maintenance strategy (replacement versus repair)
- Adequate procedures
- Adequate training
- Control of work

| $r_{iS}$ | **Extent of equipment specific measures and favourable attributes** |
|---|---|
| 0.1 | All known specific measures and favourable attributes are implemented |
| 0.3 | A number of additional measure or favourable attributes are implemented |
| 1 | In accordance with normal practice |
| 10 | Equipment specific measures and attributes are less than adequate |

# 2. Modell for applikasjonsspesifikk β

- Modell: $\beta^* = k_\beta \cdot k_S \cdot \beta$
- To effekter av tiltak for å redusere β:
  1. Direkte effekt på β av tiltak rettet mot β - uttrykt ved $k_\beta$
  2. Indirekte effekt på β av å redusere $\lambda_{DU\text{-}S}$ - uttrykt ved $k_S$



# Modellparametere ($k_\beta$, $k_S$)

- $k_\beta$ angir endring i andelen fellesfeil ($\beta$) pga direkte tiltak for å beskytte seg mot fellesfeil, f.eks. – fra IEC 61508:
  1. *Separation/segragation*
  2. *Diversity/redundancy*
- $k_S$ angir endring i andelen fellesfeil ($\beta$) pga tiltak som endrer raten av systematiske feil ($\lambda_{DU-S}$), f.eks.:
  3. *Complexity/design/application/maturity/experience*
  4. *Assessment/analysis and feedback of data*
  5. *Procedures/human interfaces*
  6. *Competence/training/safety culture*
  7. *Environmental control*
  8. *Environmental testing*

# Parameterverdier

- $k_\beta$ - basert på grad av direkte beskyttelse mot fellesfeil:

| $k_\beta$ | Protection | Comments |
|---|---|---|
| 0.1 | Very high protection | Separation/segregation and diversity/redundancy fully implemented |
| 0.5 | Extended protection | Some additional protection implemented and documented |
| 1 | Normal protection | Average level of protection – current practice |
| 5 | Reduced protection | Less protection than typically implemented |

  - Valg av verdi samt krav til begrunnelse og dokumentasjon av valgt verdi er tilsvarende som for $r_{iG}$, og $r_{iS}$

- $k_S$ – beregnes ut i fra reduksjon i $\lambda_{DU\text{-}S}$:

$$k_S = (1-r^*) / (1-r)$$

# 3. Modell for applikasjonsspesifikk $P_{TIF}$

- Modell: $P_{TIF}^* = k_T \cdot P_{TIF}$
- Modellparameter $k_T$ angir fullstendighet av funksjonstest, dvs. funksjonstestens evne til å avdekke feil
- Parameterverdi (generelt):

| $k_T$ | Test Performance | Comments |
|---|---|---|
| 0.1 | Complete test | Testing for all known failure modes |
| 0.3 | Extended test | Additional test features included in the test |
| 1 | Normal test | Average test – current practice |
| 10 | Simplified test | No documented test procedure |

- Parameterverdi (eksempel ESV):

| $k_T$ | Test Performance | Comments |
|---|---|---|
| 0.1 | Complete test | Complete stroke and pressure testing |
| 0.3 | Extended test | Additional opportunity testing |
| 1 | Normal test | Complete stroke |
| 10 | Simplified test | Partial stroke |

- Valg av verdi samt krav til begrunnelse og dokumentasjon av valgt verdi er tilsvarende som for $r_{iG}$, $r_{iS}$, og $k_\beta$

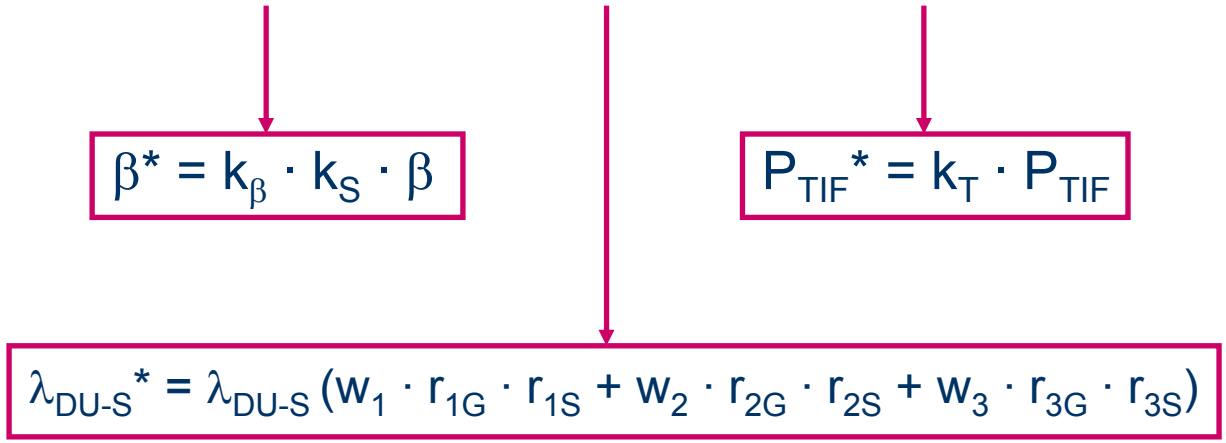
# Oppsummering / oversikt

- Generisk beregning:

  $CSU(MooN) = c_{MooN} \cdot \beta \, (\lambda_{DU} \cdot \tau/2 + P_{TIF})$

- Applikasjonsspesifikk beregning:

  $CSU(MooN)^* = c_{MooN} \cdot \beta^* \, [(\lambda_{DU\text{-}RH} + \lambda_{DU\text{-}S}^*) \cdot \tau/2 + P_{TIF}^*]$



# Oppsummering / oversikt

- Generisk beregning:

  $CSU(MooN) = c_{MooN} \cdot \beta \, (\lambda_{DU} \cdot \tau/2 + P_{TIF})$

- Applikasjonsspesifikk beregning:

  $CSU(MooN)^* = c_{MooN} \cdot \beta^* \, [(\lambda_{DU\text{-}RH} + \lambda_{DU\text{-}S}^*) \cdot \tau/2 + P_{TIF}^*]$