

TTK2 – Pålitelighetsanalyse av sikkerhetsfunksjoner

SEMINAR 2: Pålitelighetsnettverk og beregning av PFD og PFH

Versjon
05.08.2026

2026

Faglærere: Mary Ann Lundteigen

<https://www.itk.ntnu.no/emner/fordypning/TTK2>

Om bruk av innhold fra slidene

© 2026 Mary Ann Lundteigen.

This presentation is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License. Under these terms, you are free to share and adapt the material for non-commercial purposes, provided you give appropriate credit to the original author.

Please note: Images, figures, and other materials cited or reproduced from external sources are not covered by this license and remain the intellectual property of their respective rights holders.

The content is updated regularly to improve precision and ensure relevance, which is reflected in the revision number. Please reach out to mary.a.lundteigen@ntnu.no if you have comments or suggestions for improvement.

La de gjerne inspirere, men husk å referere meg om du bruker noe fra presentasjonen direkte

Miniprojekt – oppgaver fra seminar 2

Ventilen som inngår i SIFen er en av/på ventil som også er designet feilsikkert (eng: fail-safe) med fjærretur i aktuatoren.

- a) Gi eksempler på DU og S feilmoder for stenge-ventilen som inngår i SIFen. Kommenter på hvorfor det ofte ikke antas DD feil for denne ventiltypen.
- b) Hva menes med at ventilen er feil-sikker?

En ganske god oversikt over hvilke typer pålitelighetsdata for prosessindustrien ses i kapittel 8.5 i GL 070 Application of IEC 61508 and IEC 61511⁵. Les igjennom denne.

- c) Feilrater publisert av leverandører dekker i hovedsak tilfeldige feil, mens man i drift også teller med systematiske feil. Hvorfor gir det mening å si at feilrater basert på driftsdata er «mer realistiske» enn leverandørdata?
- d) Hvorfor kan allikevel feilrater basert på mye driftsdata ha høy usikkerhet?

Kan være mindre justeringer i oppgaveformulering i siste versjon av miniprojekt

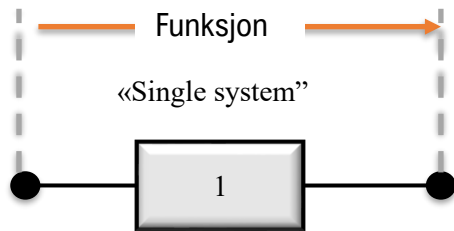
Det er flere metoder man kan bruke for å regne på pålitelighet. Først ser vi på formler basert på pålitelighetsblokkskjema (RBD – reliability block diagrams). Formler for utregningene oppgis i forelesningen.

- e) Lag et pålitelighetsnettverk («reliability block diagram») for hele SIF funksjonen, sett opp formler og regn ut:
 - i. PFD for hvert delsystem der kun uavhengige DU feil hensyntas
 - ii. PFD for hvert delsystem der også fellesfeil er hensyntatt med standard betafaktormodellen
 - iii. PFD for hvert delsystem der fellesfeil er hensyntatt med PDS metoden (C_MooN faktor inkludert for fellesfeil)
- f) Hva blir PFH for SIF funksjonen dersom vi antar at demand raten er oftere enn en gang per år? Regn ut med tilsvarende antagelser som i. og ii.
- g) Kommenter på hvilket SIL- nivå hele SIFen oppfyller (i begge operasjonsmodi – low demand og high demand).
- h) Lag en tabell, eksempelvis i excel, for kun delsystemet trykktransmittere der verdiene for PFD og PFH for dette delsystemet legges inn. Tabellen utvides med resultater fra seminar 3 (FTA) og seminar 4 (Markov) slik at man kan se i hvilken grad ulike metoder for utregning påvirker resultatene.

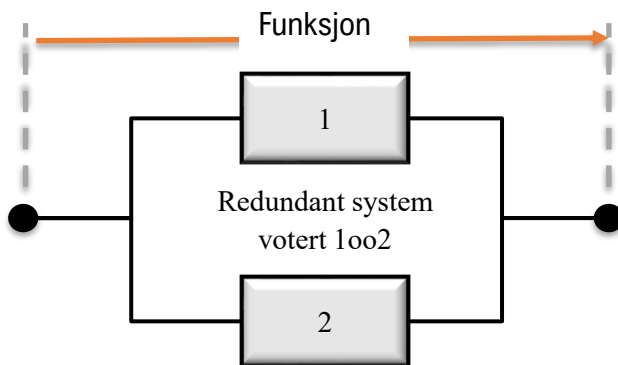
Hva mener vi med et pålitelighetsnettverk?

Pålitelighetsnettverk

- Nettverk som viser betingelser for at en funksjon skal **VIRKE**
- Funksjonen virker når man kan følge en sti igjennom diagrammet fra start til sluttpunkt
- Hver komponent kan ha en av **to tilstander**: Virker (1) eller virker ikke (feiler) (0)
- Vi kan bruke pålitelighetsnettverk til å **regne ut sannsynligheten** for funksjonen er i **en av de to tilstandene**



Funksjonen virker når komponent 1 virker

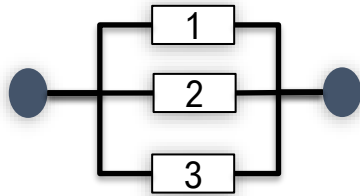


Funksjonen virker når komponent 1 ELLER komponent 2 virker

Pålitelighetsnettverk for andre voteringer (kooN)

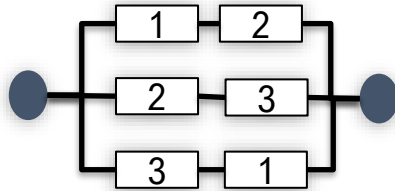
Suksessorientert

1003

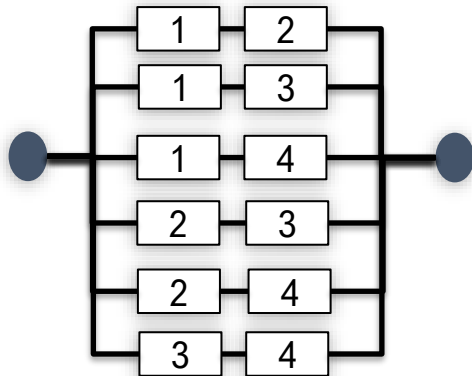


Alternativ

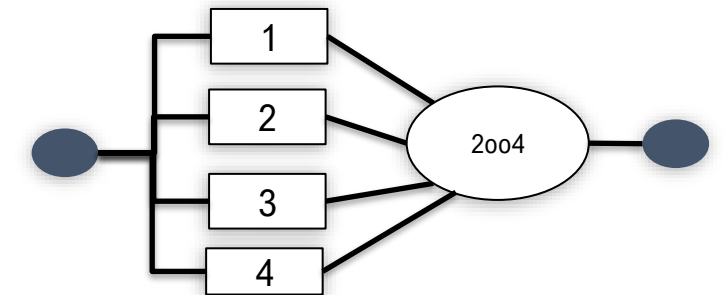
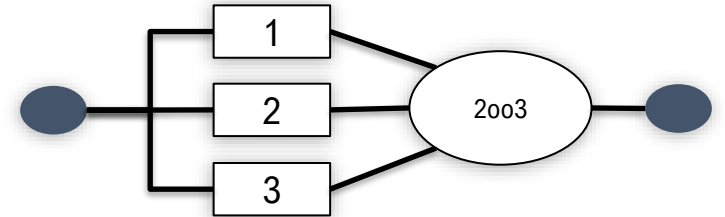
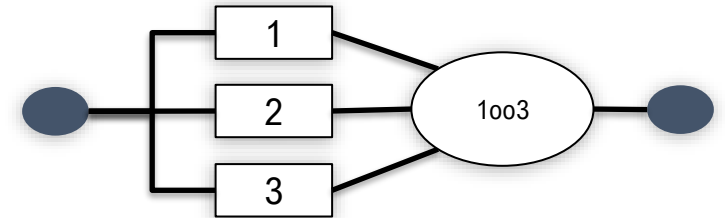
2003



2004



Forenklet tegnemåte

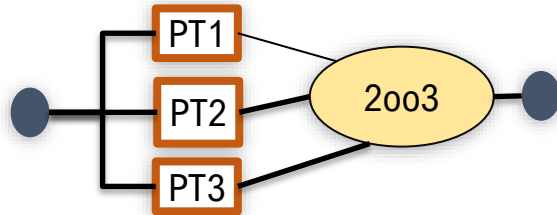


Merknad: Selve algoritmen for voteringen av komponentene *kan* ligge i logic solver. Men her betrakter vi altså effekten voteringen har på komponentene

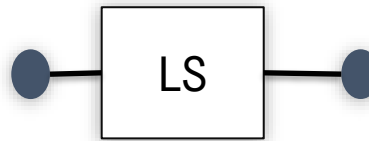
TTK2

Hvordan realiseres voteringen?

Hvis komponentene er sensorer

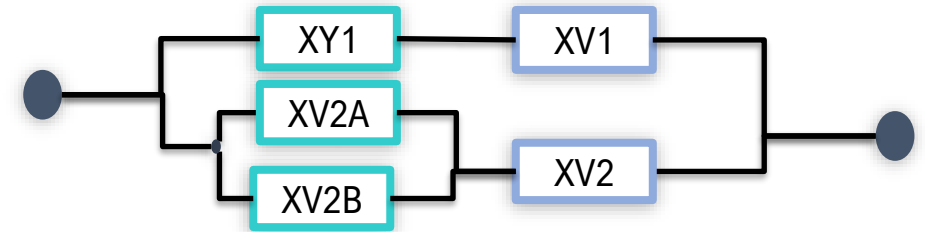


Logic solver

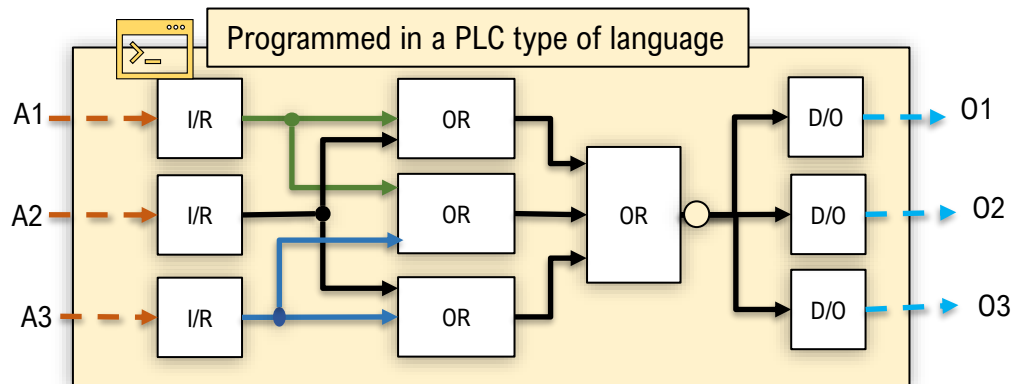


...så er ofte voteringen en algoritme i software lagt inn i logic solver

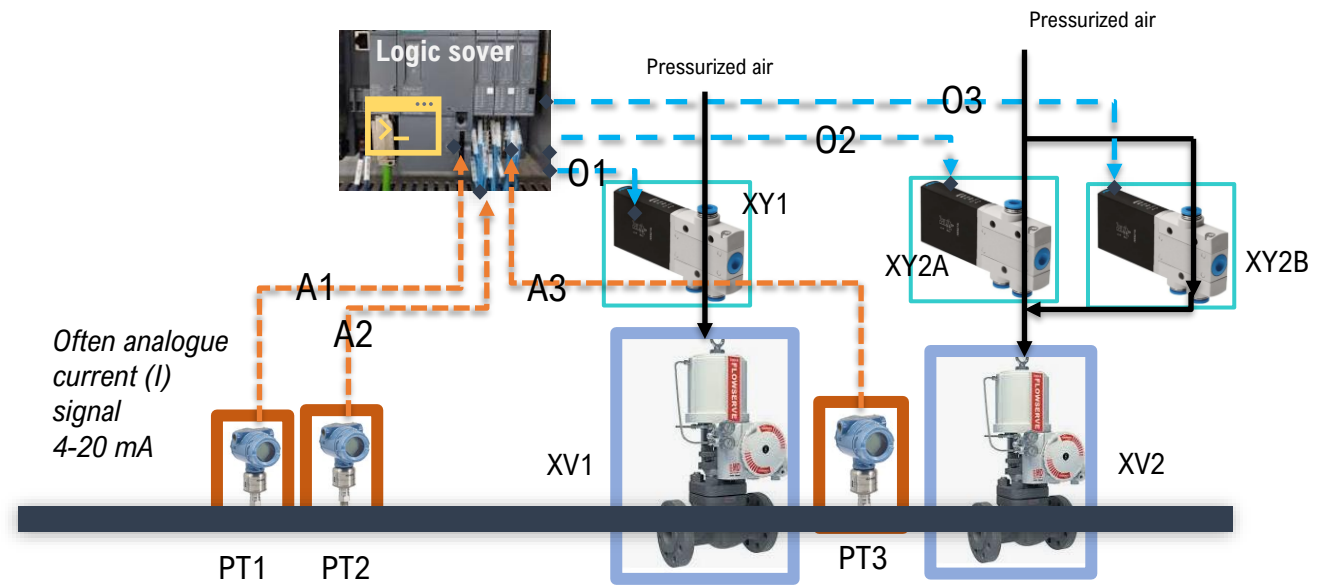
Hvis komponentene aktivert utstyr



...så er ofte voteringen ofte et resultat av fysisk installasjon.

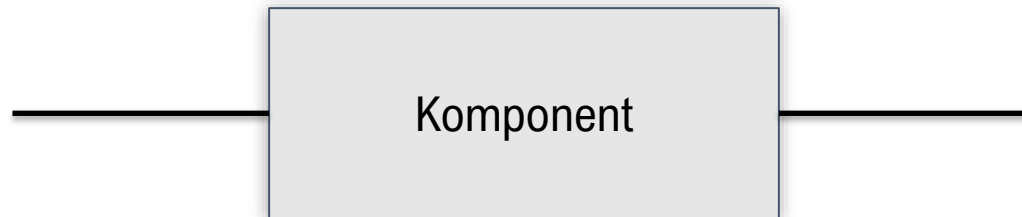


I/R: Conversion of current signal to a region ($\geq$ setpoint) $\rightarrow$ 1 Yes, 0: No
D/O: Digital to output signal (on/off)



TTK2

Hvorfor svikter utstyr?



Hvorfor skjer komponentfeilene?

Komponentfeil kan inntreffe på grunn av:

- **Normal slitasje («random/random feil»):**
Skyldes forventet slitasje når utstyret brukes slik det er designet for
- **Systematiske feil:** Feil som skyldes designfeil, programmeringsfeil monteringsfeil, bruksfeil og eksponering utover det utstyret er beregnet for
- Ikke alltid så enkelt å skille i praksis. Alle «random» og en stor andel av de systematiske tas med i utstyrets **feilrate**.

Tilfeldig feil:

- Svikt i elektronikk-komponenter pga degradering over tid

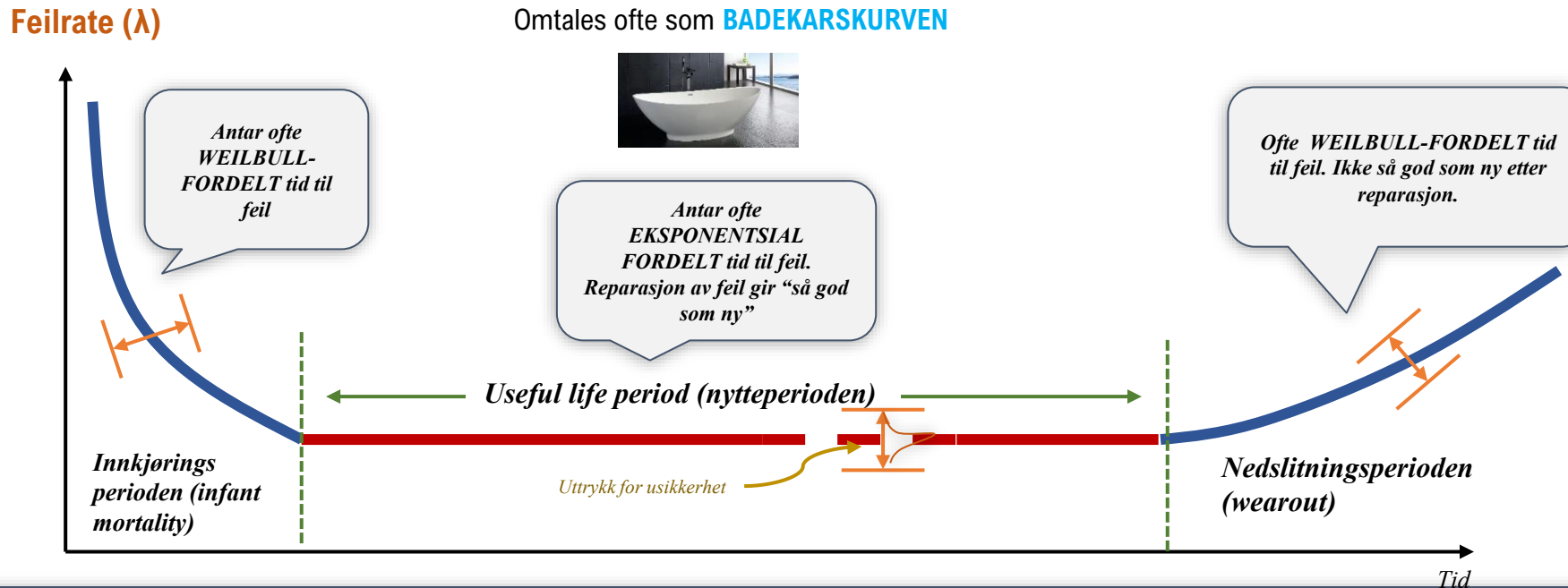


Systematisk feil:

- Transmitter med feil måleområde
- Feilkalibrering
- Vanninntrenging pga montasjefeil

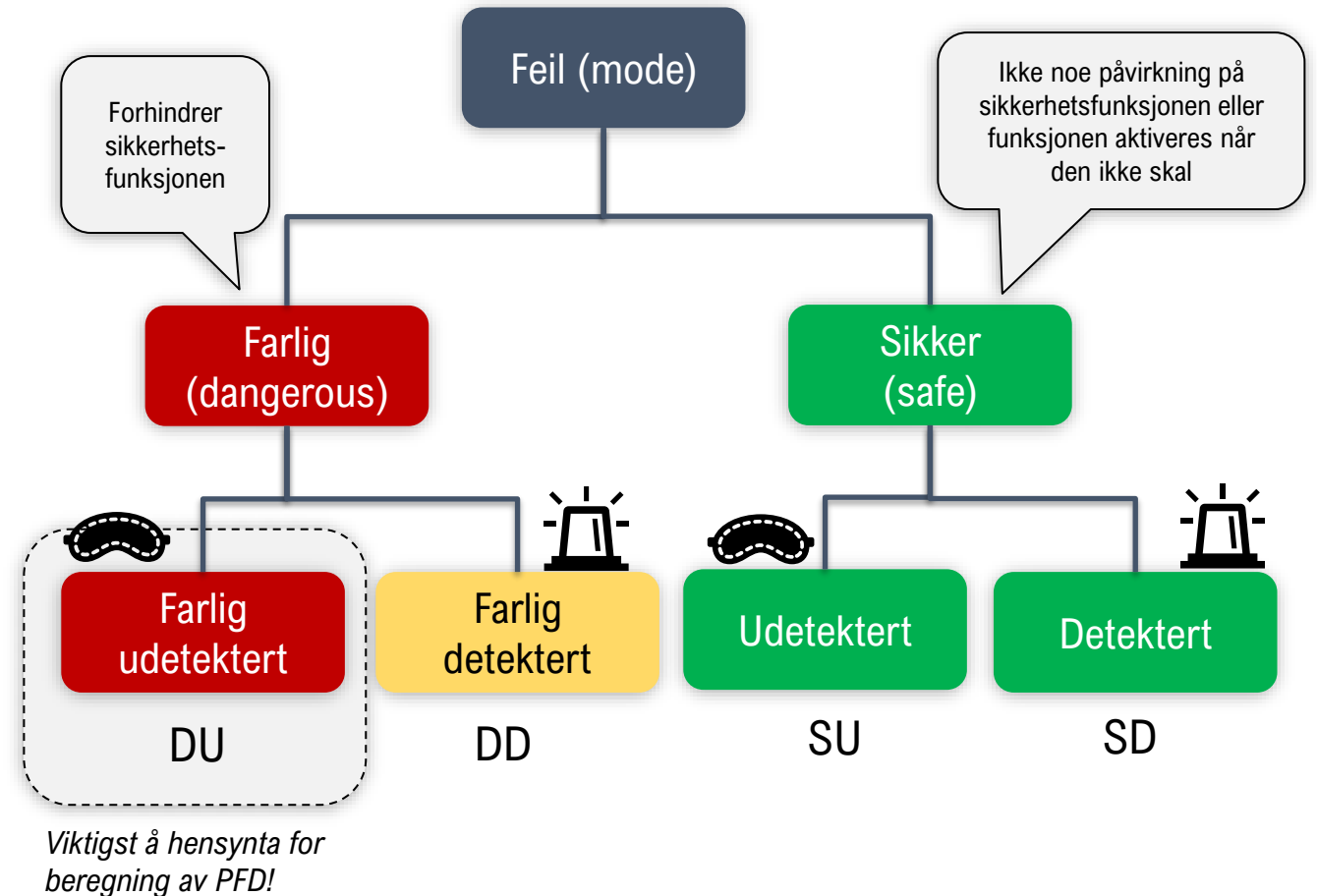
Hvordan opptrer feilene?

- For **reparerbart** utstyr så opptrer feil som en **stokastisk prosess** der tid til (neste) feil følger en angitt statistisk fordeling
- Hyppigheten av feil oppgis som en **feilrate (λ)**, det vil si antall feil over en angitt periode.
- Feilraten kan utvikle seg forskjellig over tid
- For utstyr som inngår i sikkerhetsfunksjoner antar vi som oftest at vi er i **nytteperioden (Useful life period)**. Det betyr at vi antar at **feilraten** er **konstant**
- Vi kan forsøke å estimere λ som en **gjennomsnittsverdi** (mean), men det vil være noe usikkerhet



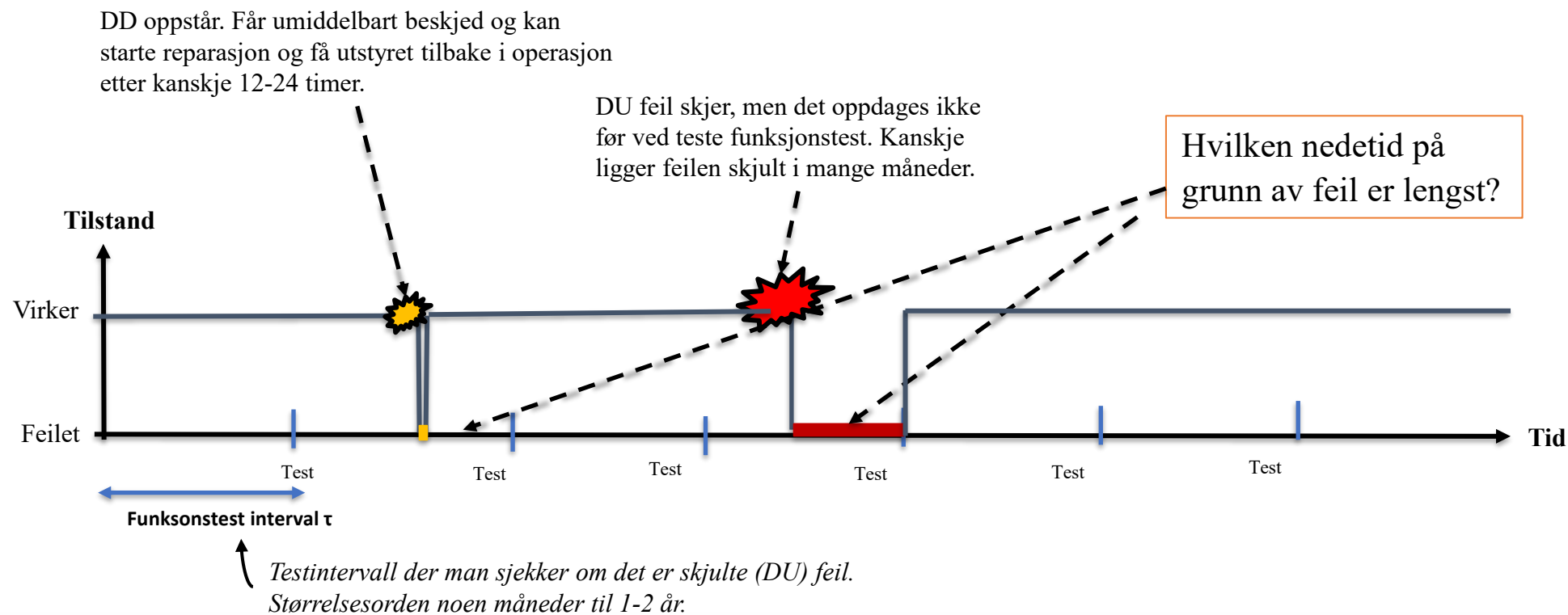
Ikke alle typer feil er like kritiske

- For sikkerhetsfunksjoner skiller vi mellom feilmoder som er:
 - **Sikre** (safe)
 - **Farlige** (dangerous)
- Av disse kan begge være **detekterte** (gis alarm via diagnostikk når feilen inntreffer) eller **udetekterte** (forblir skjulte frem til det er behov for sikkerhetsfunksjonen)
- Farlig udetektert (DU)** er feilene som bidrar mest til sannsynligheten for at SIFen (safety-instrumented function) ikke virker når den skal.
- For å oppdage DU feil før neste demand, må **utstyret testes jevnlig**



Hvorfor er DU feil viktigst?

- Vi ser på **nedetiden**, det vil si perioden komponenten ikke kan utføre sin sikkerhetsfunksjon
- Her kan vi observere at nedetiden for **DU feil er mye lengre** enn for DD feil



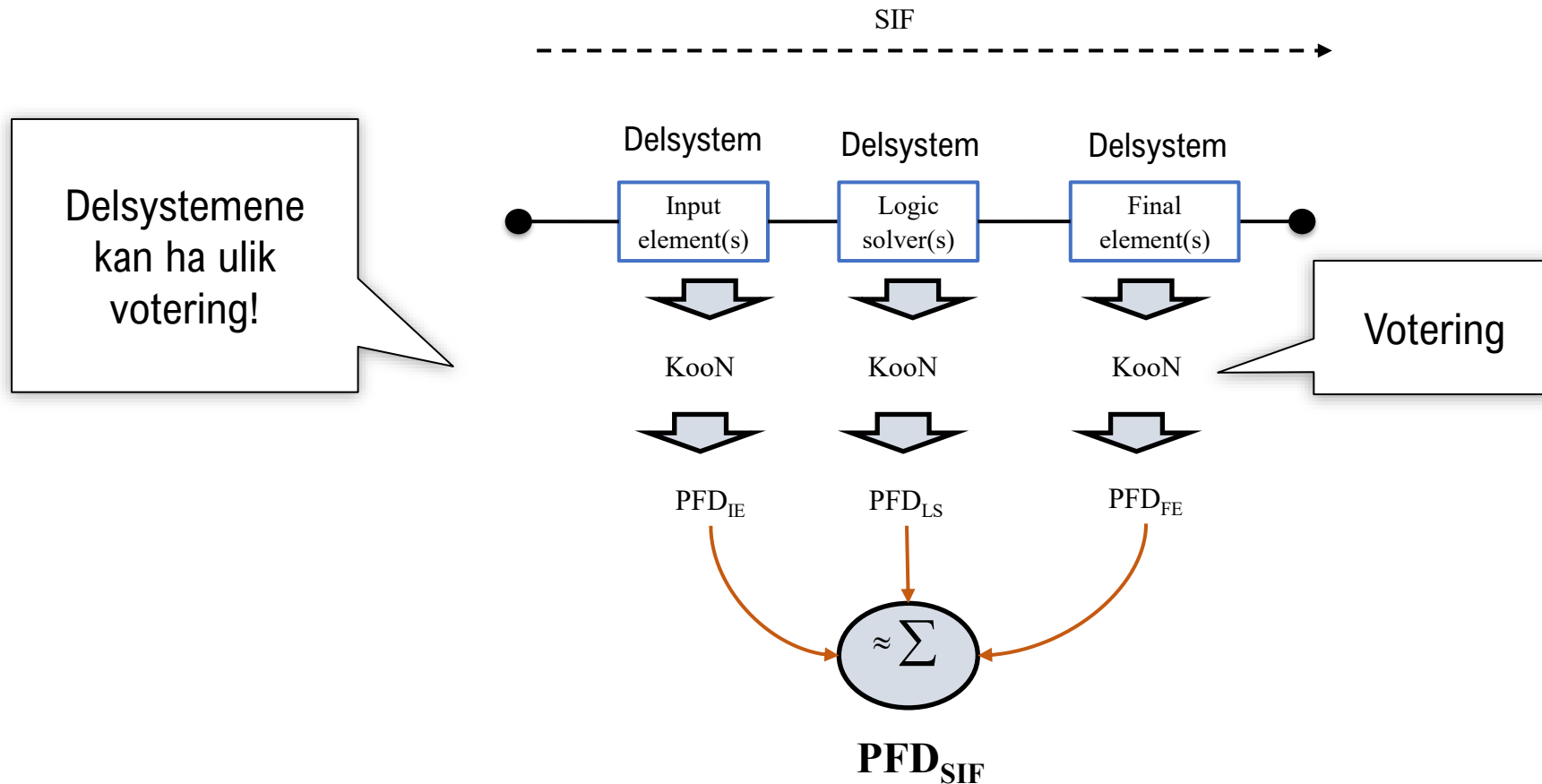
Hvordan bestemme sannsynligheten for at SIFen svikter



... da må vi først må vi spørre...

- Hvor ofte oppstår det situasjoner («demand») som SIFen må ta aksjon på?
- Hvis 1 gang per år eller sjeldnere:
 - Low-demand mode
 - Da ønsker vi å bestemme gjennomsnittlig **sannsynlighet** for at hele eller deler av SIFen ikke virker
→ **Average probability of failure on demand (PFD)**
- Hvis mer enn 1 demand per år:
 - High-demand/continuous mode
 - Da ønsker vi å bestemme gjennomsnittlig **frekvens** for hvor ofte SIFen svikter
→ **Probability of having a dangerous failure per hour (PFH)**

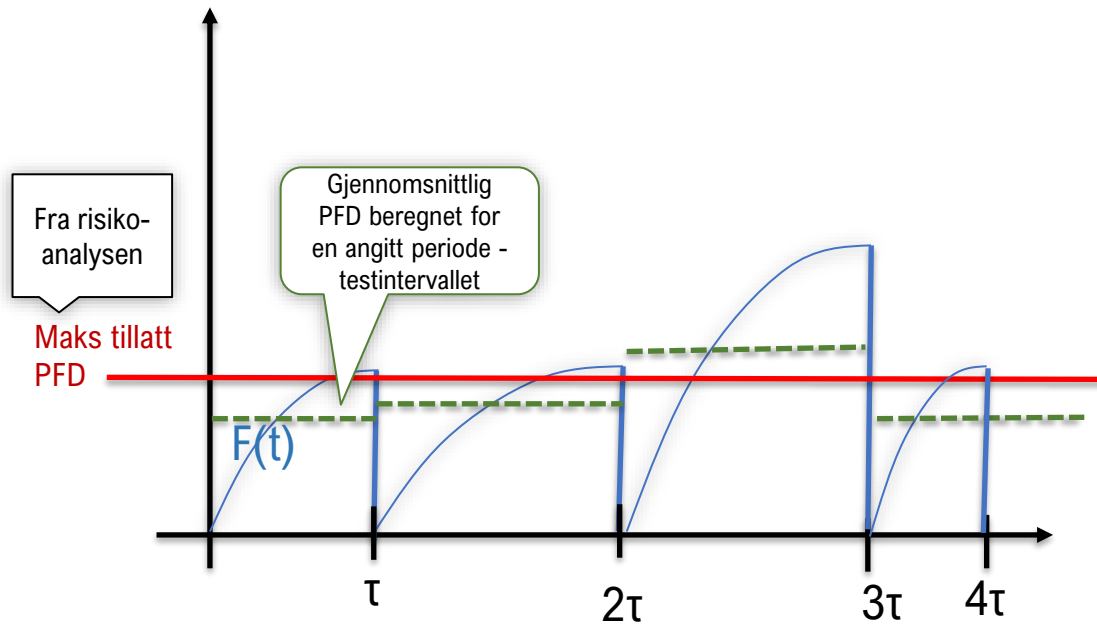
Beregne PFD for en hel SIF



Vi har **lov til å summere PFD** for hvert delsystem fordi PFD-verdiene er **veldig små**.

PFD vs PFH

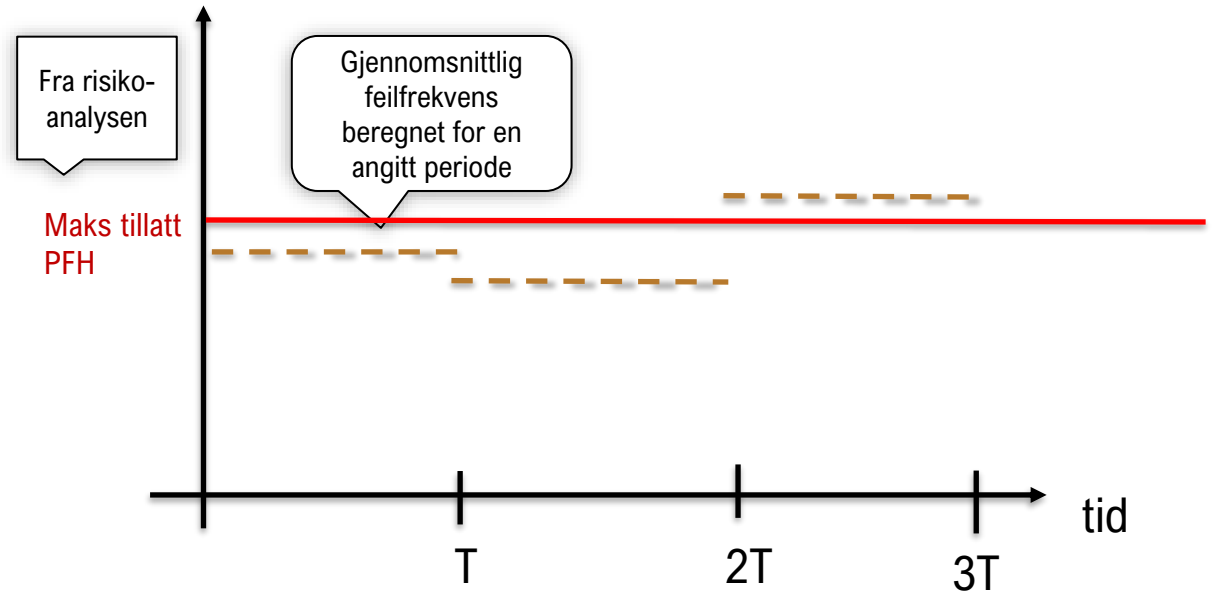
Feilsannsynlighet $F(t)$
og PFD



(Utregnet) PFD: — — — — —

- Gjennomsnittsverdi av $F(t)$ innenfor hver periode τ , der τ er intervallet mellom hver gang funksjonen testes for å avdekke DU feil og alle repareres «perfekt»
- Noen metoder inkluderer også DD feil, men de får vanligvis ikke mye å si
- τ bestemt slik at PFD for SIF er $\leq$ maks tillatt PFD

Gjennomsnittlig feilfrekvens PFH
(per time)



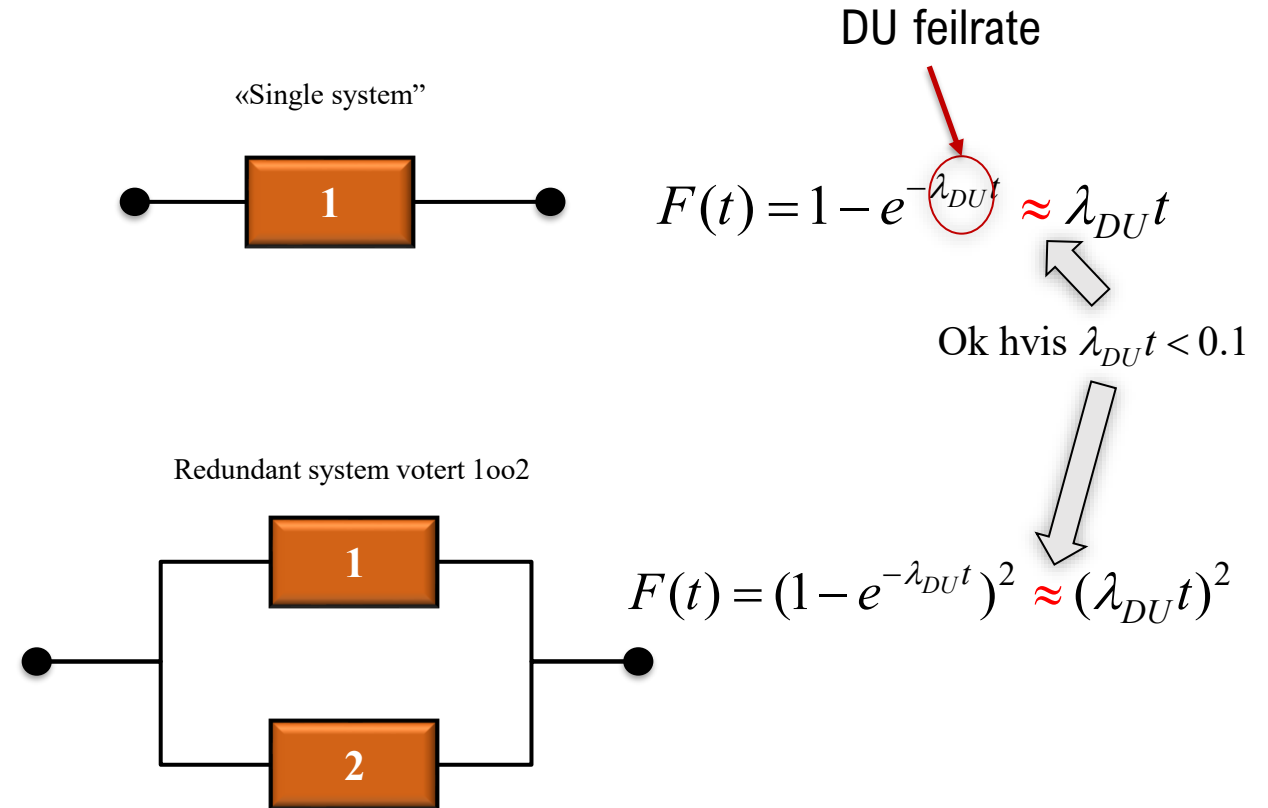
(Utregnet) PFH: — — — — —

- Gjennomsnittsverdi for frekvensen av DU feil (og noen ganger også med DD feil inkludert)
- Tilnærmes $F(T)/\text{perioden i timer}$ hvis perioden ikke er for lang. I
- T bestemt utfra litt andre kriterier

Beregning av PFD basert på pålitelighetsnettverk

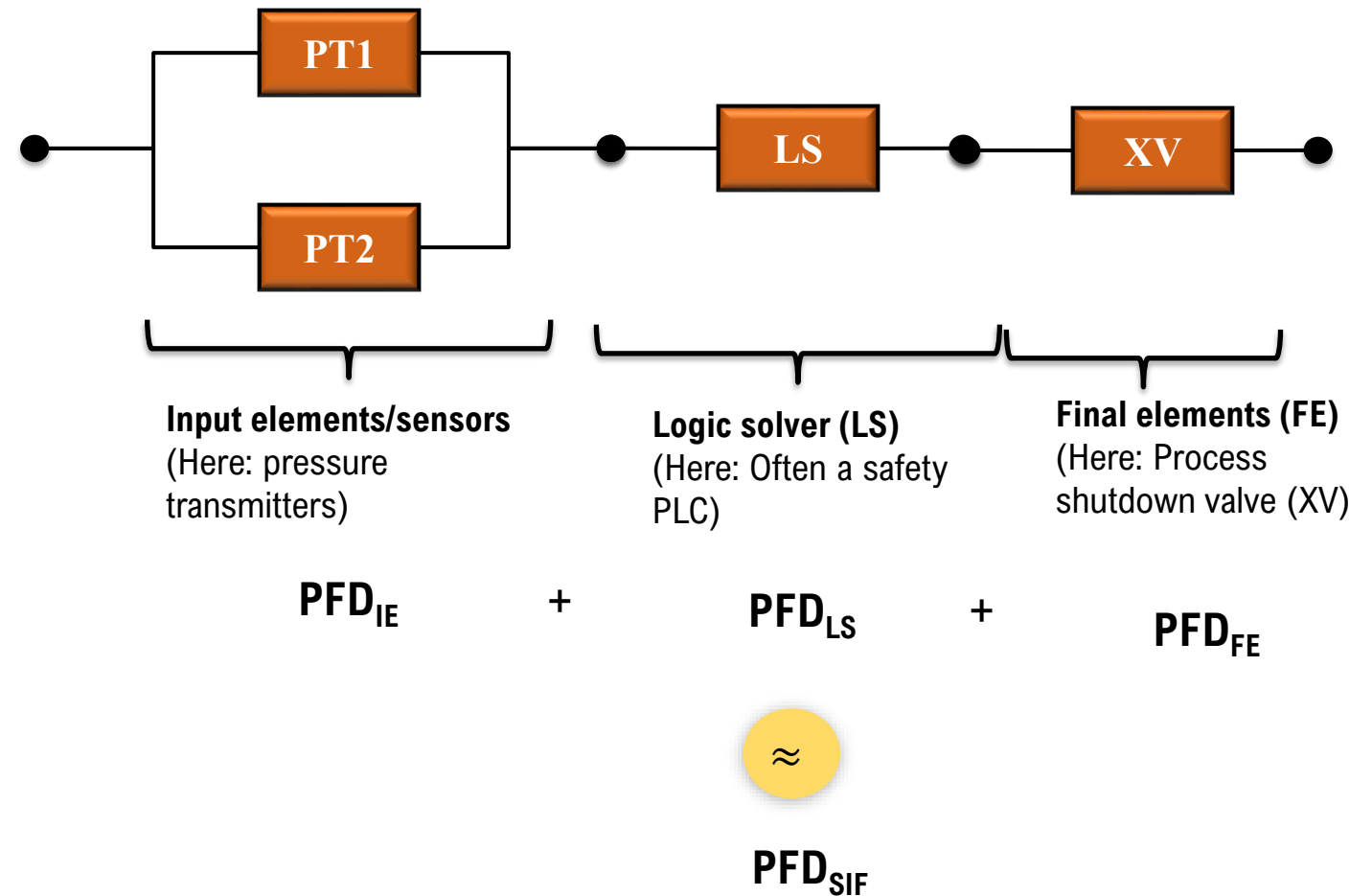
En SIF er ofte uttrykt med tre pålitelighetsnettverk i serie – ett for hvert delsystem. For hvert delsystem antar vi at:

- Hvert delsystemet har **identiske** komponenter som feiler helt **uavhengig** av hverandre (vi skal senere legge til også avhengige feil).
- Tid til (DU eller DD) feil for hver komponent er **eksponential fordelt** (feil blir perfekt reparert ifbm hver funksjonstest)
- **Feilsannsynligheten $F(t)$** kan settes opp hvor hvert delsystem



Beregning av PFD basert på pålitelighetsnettverk

- Hvert delsystem får sitt tilpassede pålitelighetsnettverk
- Disse «henger sammen» for å dekke hele SIFen
- For vert delsystemet antas ofte å ha **identiske** komponenter som feiler helt **uavhengig** av hverandre (vi skal senere legge til også avhengige feil).
- **PFD** regnes ut for hver av delsystemene og **summeres** så (som er lov når $PFD \leq 0.1$)



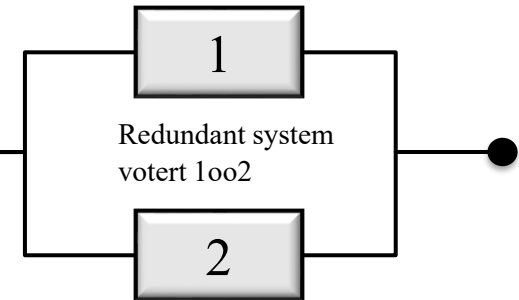
PFD utregnet for et testintervall

«Single system»



$$PFD = \frac{1}{\tau} \int_0^{\tau} F(t) dt = \frac{1}{\tau} \int_0^{\tau} 1 - e^{-\lambda_{DU} t} dt \approx \frac{1}{\tau} \int_0^{\tau} \lambda_{DU} t dt = \frac{\lambda_{DU} \tau}{2}$$

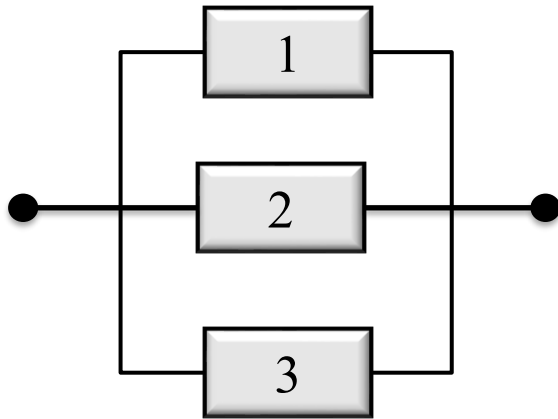
Redundant system
votert 1oo2



$$PFD = \frac{1}{\tau} \int_0^{\tau} F(t) dt \approx \frac{1}{\tau} \int_0^{\tau} (\lambda_{DU} t)^2 dt = \frac{(\lambda_{DU} \tau)^2}{3}$$

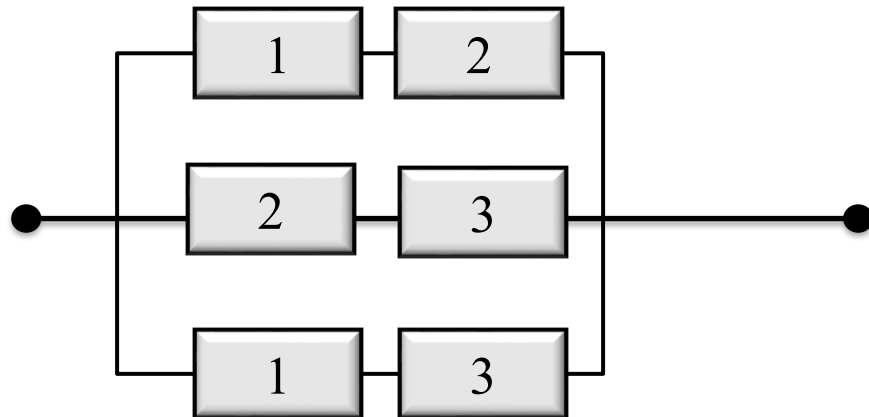
PFD utregnet for et testintervall

1oo3



$$PFD = \frac{1}{\tau} \int_0^{\tau} F(t) dt = \frac{1}{\tau} \int_0^{\tau} (1 - e^{-\lambda_{DU}t})^3 dt \approx \frac{1}{\tau} \int_0^{\tau} (\lambda_{DU}t)^3 dt = \frac{(\lambda_{DU}\tau)^3}{4}$$

2oo3



$$\begin{aligned} PFD &= \frac{1}{\tau} \int_0^{\tau} F(t) dt \approx \frac{1}{\tau} \int_0^{\tau} 3(1 - e^{-\lambda_{DU}t})^2 dt \\ &= \frac{1}{\tau} \int_0^{\tau} 3 \cdot (\lambda_{DU}t)^2 dt = 3 \cdot \frac{(\lambda_{DU}\tau)^2}{3} = (\lambda_{DU}\tau)^2 \end{aligned}$$

Generell formel når komponentene er like

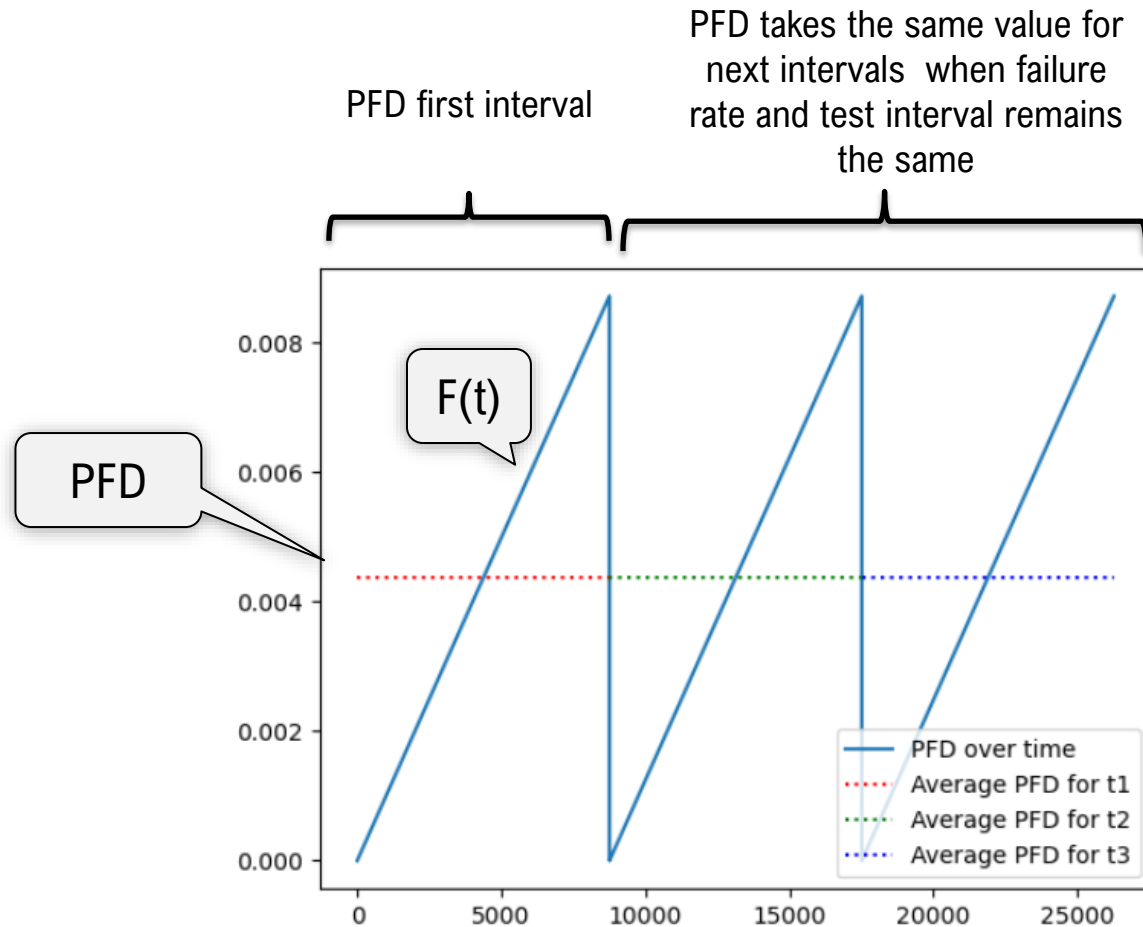
Generelt for et kooN system:

$$PFD = \binom{n}{n-k+1} \frac{(\lambda_{DU}\tau)^{n-k+1}}{n-k+2}$$

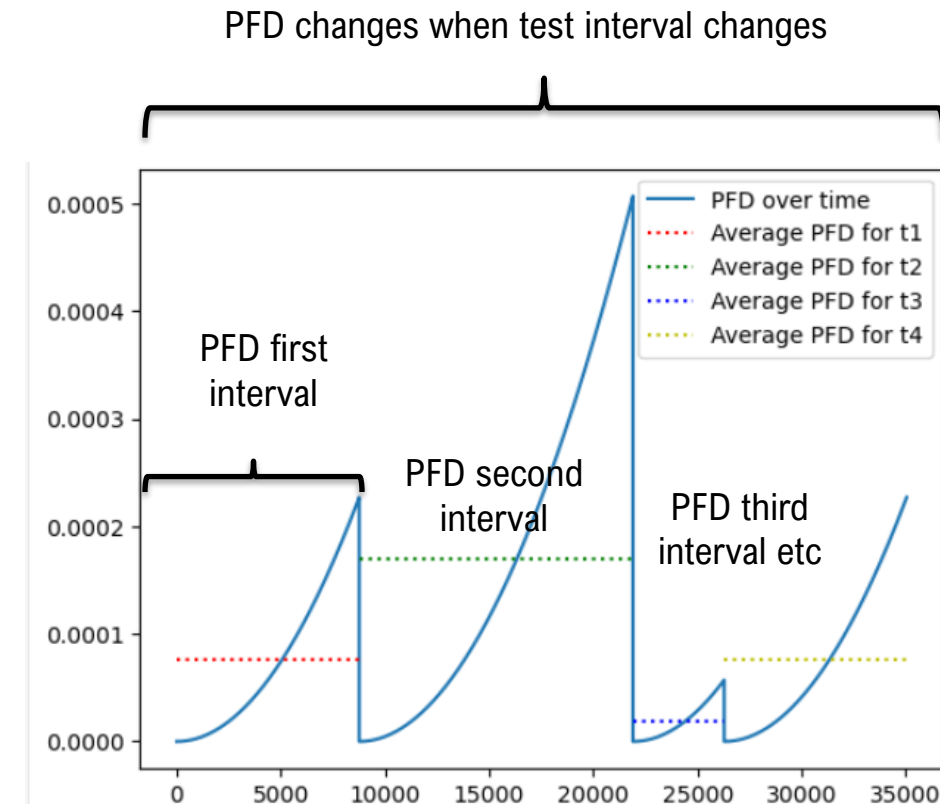
k/n	1	2	3	4
1	$\frac{\lambda_{DU}\tau}{2}$	$\frac{(\lambda_{DU}\tau)^2}{3}$	$\frac{(\lambda_{DU}\tau)^3}{4}$	$\frac{(\lambda_{DU}\tau)^4}{5}$
2	--	$\lambda_{DU}\tau$	$(\lambda_{DU}\tau)^2$	$(\lambda_{DU}\tau)^3$
3	--	--	$\frac{3(\lambda_{DU}\tau)^2}{2}$	$2(\lambda_{DU}\tau)^2$
4	--	--	--	$2\lambda_{DU}\tau$

Examples

1001 system



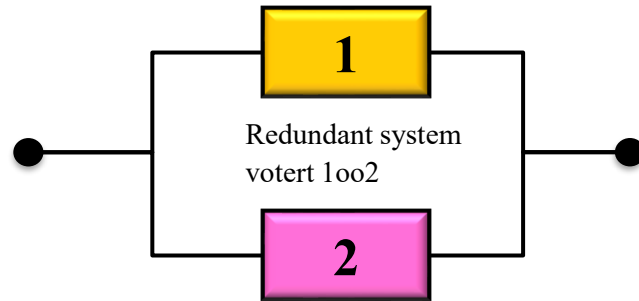
2003 system



Examples taken from: <https://git.ntnu.no/lundteig/TTK2-ReliabilityAnalysis>

Vi kan også beregne PFD om komponentene *ikke* er identiske!

... Her er et eksempel:



$$PFD = \frac{1}{\tau} \int_0^{\tau} F(t) dt \approx \frac{1}{\tau} \int_0^{\tau} (\lambda_{DU,1} t)(\lambda_{DU,2} t) dt = \frac{\lambda_{DU,1} \lambda_{DU,2} \tau^2}{3}$$

...men vi forenkler i vår analyse til å se på identiske/veldig like type komponenter når de er redundante!

Beregning av PFD: Eksempel

Vi regner ut PFD med $\lambda_{DU}=2E-6/\text{time}$ og $\tau = 8760$ timer (1 år)

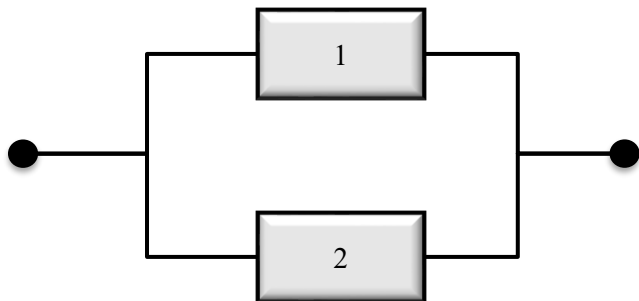
«Single system»



$$PFD = \frac{\lambda_{DU}\tau}{2} = \frac{2E-6 \cdot 8760}{2} = 8.7E-3$$

Innenfor SIL 2

Redundant system votert 1oo2

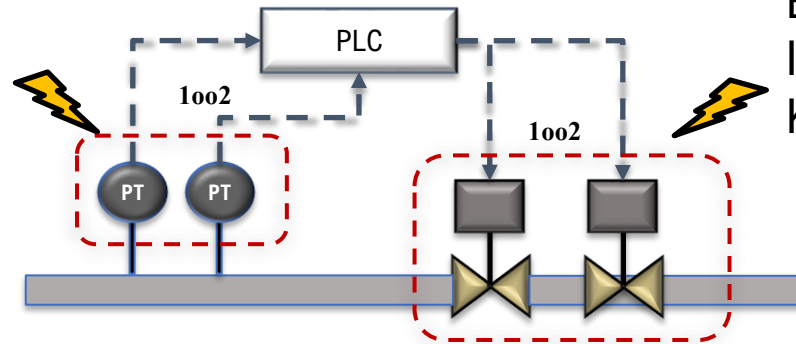


$$PFD = \frac{(\lambda_{DU}\tau)^2}{3} = \frac{(2E-6 \cdot 8760)^2}{3} \approx 1.02E-4$$

Innenfor SIL 3

Fellesfeil (CCF) i delsystemer med redundans

Eksempel:
Regn og snø,
kalibreringsfeil



Eksempel:
Ising pga uttette pakninger,
Korrosjon pga valgt materiale

Felles(årsaks)feil (Common cause failures - CCF) er når to eller flere utstyr feiler av en samme årsak og der vi ikke kan si at feilene skjer uavhengig av hverandre.

Resterende andel ($1-\beta$) av feilraten der komponenten feiler uavhengig av de andre komponentene

$$(1-\beta)\lambda_{DU}$$

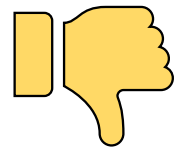
$$\lambda_{DU}$$

$$\beta\lambda_{DU}$$

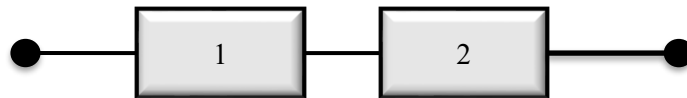
En andel (β) er andel av feilraten der komponenten feiler samtidig med de andre komponentene den er votert med og forklaringen er en felles årsak.

«Standard **beta** faktor modellen»

Hvordan tar vi med fellesfeil (CCF) i beregningen av PFD?



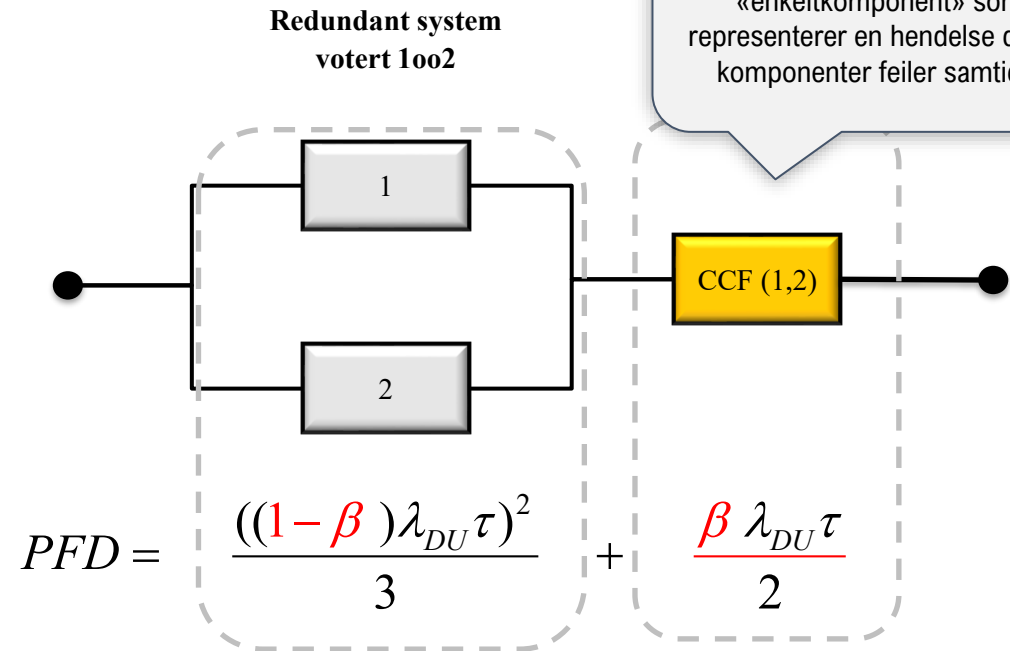
Fellesfeil er **IKKE relevant** for enkeltutstyr og utstyr i serie i pålitelighetsnettverket.



«Single system/komponenter i serie»



Fellesfeil relevant. Vises som en «enkeltkomponent» som representerer en hendelse der to komponenter feiler samtidig



Leses slik:

Et 1oo2 votert system feiler når

- komponent 1 og 2 **feiler uavhengig** av hverandre

ELLER

- de to komponentene **feiler samtidig** på grunn av en fellesfeil (CCF).

Flere fellesfeilmodeller. Vi fokuserer på to av dem!

Med **standard betafaktor-modellen** antas det at **ALLE** redundante komponenter **feiler samtidig eller innenfor et kort tidsintervall** i en felles(årsaks)feil. Det kan jo være litt vel konservativt.

I Norge – via **PDS forum** – utviklet man en egen parameter **CkooN** som modifierer bidraget fra fellesfeil utfra votering.

Vi omtaler den som **PDS metoden**.

Eksempel: Hvis man har et delsystem bestående av 3 komponenter votert 1oo3, så vil ikke doble feil medføre at det voterte systemet feiler, kun hvis alle tre feiler. Dersom komponentene er votert 2oo3 så vil både doble feil og triple feil medføre at funksjonen svikter. De to voteringene har derfor ulik sårbarhet ovenfor fellesfeil.

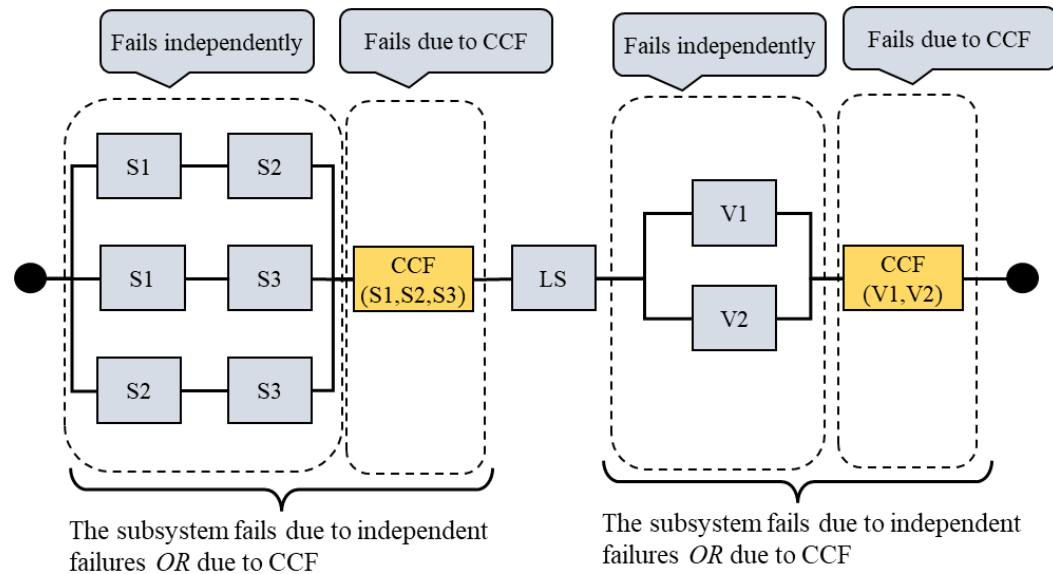


$$\text{PFD}_{CCF} = \frac{\beta \lambda_{DU} \tau}{2}$$



$$\text{PFD}_{CCF} = \frac{C_{kooN} \beta \lambda_{DU} \tau}{2}$$

Hva blir forskjellen for PFD med de to fellesfeilmodellene



Tab. 7. C_{MooN} values

k=M, N=N

M/N	2	3	4	5	6
1	$C_{1002}=1.0$	$C_{1003}=0.5$	$C_{1004}=0.3$	$C_{1005}=0.2$	$C_{1006}=0.15$
2		$C_{2003}=2.0$	$C_{2004}=1.1$	$C_{2005}=0.8$	$C_{2006}=0.6$
3			$C_{3004}=2.8$	$C_{3005}=1.6$	$C_{3006}=1.2$
4				$C_{4005}=3.6$	$C_{4006}=1.9$
5					$C_{5006}=4.5$

Standard beta faktormodellen

$$PFD_{SIF} = ((1-\beta_S)\lambda_{DU,S}\tau)^2 + \frac{\beta_S\lambda_{DU,S}\tau}{2} + \frac{\lambda_{DU,L}\tau}{2} + \frac{((1-\beta_V)\lambda_{DU,V}\tau)^2}{3} + \frac{\beta_V\lambda_{DU,V}\tau}{2}$$

PDS metoden

$$PFD_{SIF} = (\lambda_{DU,S}\tau)^2 + \frac{C_{2003}\beta_S\lambda_{DU,S}\tau}{2} + \frac{\lambda_{DU,L}\tau}{2} + \frac{(\lambda_{DU,V}\tau)^2}{3} + \frac{C_{1002}\beta_V\lambda_{DU,V}\tau}{2}$$

Merk: $(1-\beta)$ er IKKE med

Eksempel fortsettelse

Standard beta faktormodellen

$$PFD_{SIF} = ((1 - \beta_S) \lambda_{DU,S} \tau)^2 + \frac{\beta_S \lambda_{DU,S} \tau}{2} + \frac{\lambda_{DU,L} \tau}{2} + \frac{((1 - \beta_V) \lambda_{DU,V} \tau)^2}{3} + \frac{\beta_V \lambda_{DU,V} \tau}{2}$$

PDS metoden

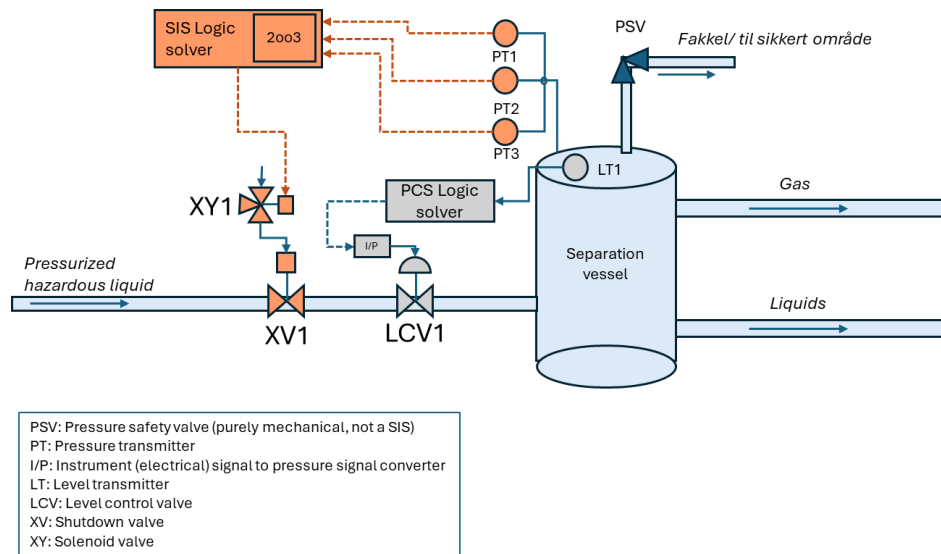
$$PFD_{SIF} = (\lambda_{DU,S} \tau)^2 + \frac{C_{2003} \beta_S \lambda_{DU,S} \tau}{2} + \frac{\lambda_{DU,L} \tau}{2} + \frac{(\lambda_{DU,V} \tau)^2}{3} + \frac{C_{1002} \beta_V \lambda_{DU,V} \tau}{2}$$

Assume that $\tau = 8760$ and that $\lambda_{DU,S} = 1E-6$ per hour, $\beta_S = 5\%$, $\lambda_{DU,L} = 1E-7$ per hour, and $\lambda_{DU,V} = 3E-6$ per hour, and $\beta_V = 10\%$. Then:

$$PFD_{SIF} = [6.93E-5 + 2.19E-4] + 4.38E-4 + [1.86E-4 + 1.31E-3] \\ = 2.22E-3$$

$$PFD_{SIF} = [7.67E-5 + 4.27E-4] + 4.38E-4 + [2.30E-4 + 1.31E-3] \\ = 2.49E-3$$

Miniprojekt oppgave 2a)



Start med å skrive ned hva sikkerhetsfunksjonen er til de to komponenttypene:

- Trykktransmitter:
 - Måle og sende det (reelle) trykket i tanken
- Logisk enhet:
 - Gi kommando til ventil om å stenge dersom 2 av de 3 trykktransmitterne har sendt en måleverdi som er høyere enn settpunktet
- Shutdown ventil:
 - Stenge på kommando innen 15 sekunder og holde tett i lukket posisjon.

- a) I pålitelighetsanalyser for en SIF er det som regel tilstrekkelig å hensynta DU feil, der DU betyr dangerous undetected (farlig udetektert) feilmoder.
- i. Hva er eksempler på en DU feilmode for trykktransmitteren, for den logiske enheten og for ventilen?
 - ii. Hva er eksempel på en sikker (S) feil mode for ventilen?
 - iii. Hva er det som avgjør om en farlig (D) feil kan klassifiseres som detektert (DD) feil? Gi et eksempel på en DD feilmode for trykktransmitteren.
 - iv. Hva er diagnostic coverage (DC) og safe failure fraction?

Dernest: Bruk informasjon om funksjoner til å defnere feil og plasser de på rett kategori feilmode

Utstyr	DU feilmoder	DD feilmoder	S feilmoder
Trykktransmitter	Måleverdi er lavere enn reell verdi	Måleverdi sendes ikke	Måleverdi er høyere enn reell verdi
Logisk enhet	Votering er 3oo3 i stedet for 2oo3 Feil satt alarmgrense	Utgang blir ikke satt selv om kommando er gitt	Kommando gis selv om betingelse ikke er oppfylt
Ventil	Stenger ikke på kommando Stenger for sent/bruker for lang tid Holder ikke tett i lukket posisjon	---	Ventilen stenger tilfeldig uten at kommando er gitt

Miniprojekt oppgave 2a)

Leverandør-data

Emerson's
Rosemount® 3051
Pressure Transmitters
with 4-20mA HART



80 N Main St
Sellersville, PA 18960

T-002_V6R1

Certificate / Certificat / Zertifikat / 合格証

ROS 1107062 C001

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 2@HFT=0, SIL 3@HFT=1, Route 1_H (models SFF ≥ 90%)

SIL 2@HFT=0, SIL 3@HFT=1, Route 2_H (SFF < 90%)

PFD_{avg} / PFH and Architecture Constraints must be verified for each application

Systematic Capability:

These products have met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.

A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated.

Random Capability:

The SIL limit imposed by the Architectural Constraints for each element. This element meets exida criteria for Route 2_H.

IEC 61508 Failure Rates in FIT²

Device	λ _{SD}	λ _{SD}	λ _{SD}	λ _{SD}	SFF
Rosemount® 3051 Coplanar Differential & Coplanar Gage	0	52	470	34	94%
Rosemount® 3051 Coplanar Absolute, In-line Gage & Absolute	0	63	490	43	93%

Device	λ _{SD}	λ _{SD}	λ _{SD}	λ _{SD}
Rosemount® 3051 Coplanar Differential & Coplanar Gage	0	52	470	34
Rosemount® 3051 Coplanar Absolute, In-line Gage & Absolute	0	63	490	43
Rosemount® 3051 Flowmeter Series based on 1195, 405, or 485 Primaries				
Flowmeter Series ³	0	94	258	43
Rosemount® 3051 Level Transmitter (w/o additional Seal)				
Coplanar Differential & Coplanar Gage	0	84	258	67
Coplanar Absolute, In-line Gage & Absolute	0	94	279	75
Rosemount® 3051 with Remote Seals ⁴				

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFD_{avg} / PFH considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are a mandatory part of this certification:

Assessment Report: ROS 13/01-010 R002 V4R4 or later

Safety Manual: 00809-0100-4007

¹BR5 or BR6 must be ordered with option code QT for this certificate to be valid below -40C

²FIT = 1 failure / 10⁹ hours

³SFF not required for devices certified using Route 2_H, data. For information detailing the Route 2_H approach as defined by IEC 61508-2, see Technical Document entitled "Route 2_H SIL Verification for Rosemount Type B Transmitters with Type A Components".

⁴Refer to ROS 13/04-008 R001 V1R0 "Primary Element FMEDA for Flowmeters" report for models that are excluded.

⁵Refer to the Remote Seal (ROS 1105075 R001 V3R1 or later) FMEDA report for the additional failure rates to use when using with attached Remote Seal(s), or use exSILentia.

Page 2 of 2

DC=93.3%
SFF=93.9%%

Eksempelberegning

Diagnostic coverage: To tolkninger

- Andelen av den farlige feilraten (D) som er detektert vha av diagnostikk (DD)
- Sannsynligheten for at det er en DD feil gitt at man har fått en farlig D feil.

$$DC = \frac{\lambda_{DD}}{\lambda_D} = 1 - \frac{\lambda_{DU}}{\lambda_D}$$

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_{DD} + \lambda_{DU}}$$

- I pålitelighetsanalyser for en SIF er det som regel tilstrekkelig å hensynta DU feil, der DU betyr dangerous undetected (farlig udetektert) feilmoder.
 - Hva er eksempler på en DU feilmode for trykktransmitteren, for den logiske enheten og for ventilen?
 - Hva er eksempel på en sikker (S) feil mode for ventilen?
 - Hva er det som avgjør om en farlig (D) feil kan klassifiseres som detektert (DD) feil? Gi et eksempel på en DD feilmode for trykktransmitteren.
 - Hva er diagnostic coverage (DC) og safe failure fraction (SFF)?

Safe failure fraction: To tolkninger

- Andelen av feil av den totale feilraten som enten er sikre (S) eller farlig detekterte (DD)
- Sannsynligheten for at det er en S eller DD feil gitt man har fått en feil.

Eksempel

Miniprojekt oppgave 2 a)

PDS data. Basert på mye driftserfaring

Til sammenligning (og som et eksempel): Emerson oppgir for en type Rosemount trykktransmitter at $\lambda_{DU} = 34FIT = 34E-9/time = 0.032E-6/time$

Tabell 1 Modellparametere som skal benyttes (feilrate er per time)

Pålitelighetsdata	Parameter	Verdi
DU feilrate trykktransmittere	$\lambda_{DU,PT}$	0,5E-6 per time
DU feilrate logic solver	$\lambda_{DU,LS}$	0,8E-6 per time
DU feilrate solenoid valve XY	$\lambda_{DU,XY}$	0,6E-6 per time
DU feilrate shutdown valve (XV)	$\lambda_{DU,XV}$	1,9E-6 per time
Fellesfeilandel trykktransmittere	β	5%
Testintervall	τ	8760 hours (1 år)

Oppgave b) :

- v. Feilrater publisert av leverandører dekker i hovedsak tilfeldige feil, mens man i drift også teller med systematiske feil. Hvorfor gir det mening å si at feilrater basert på driftsdata er «mer realistiske» enn leverandørdata?
- vi. Hvorfor kan allikevel feilrater basert på mye driftsdata ha usikkerhet i seg?

Stikkord (v):

- Leverandørdata inneholder ikke særlig mye systematiske feil
- Leverandører får bare tilbakemelding på feil i garantitida
- I drift får man feil som kan skyldes driftsmiljø, måten man vedlikeholder, bruker feil mm (altså systematiske feil). De telles med.

Stikkord (vi):

- Gamle historiske data
- Oppgraderinger
- Omlegging vedlikehold og testing

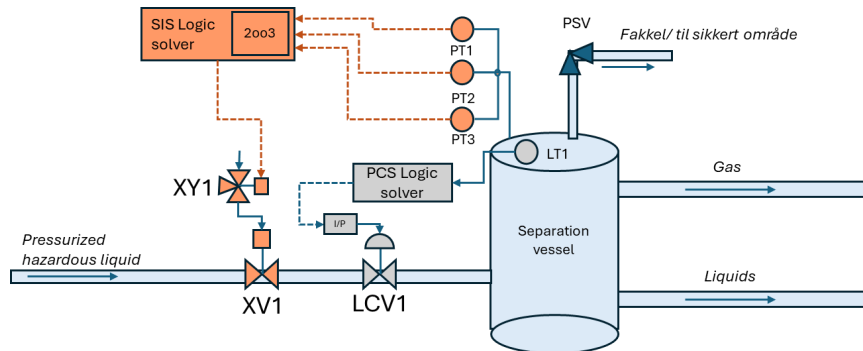
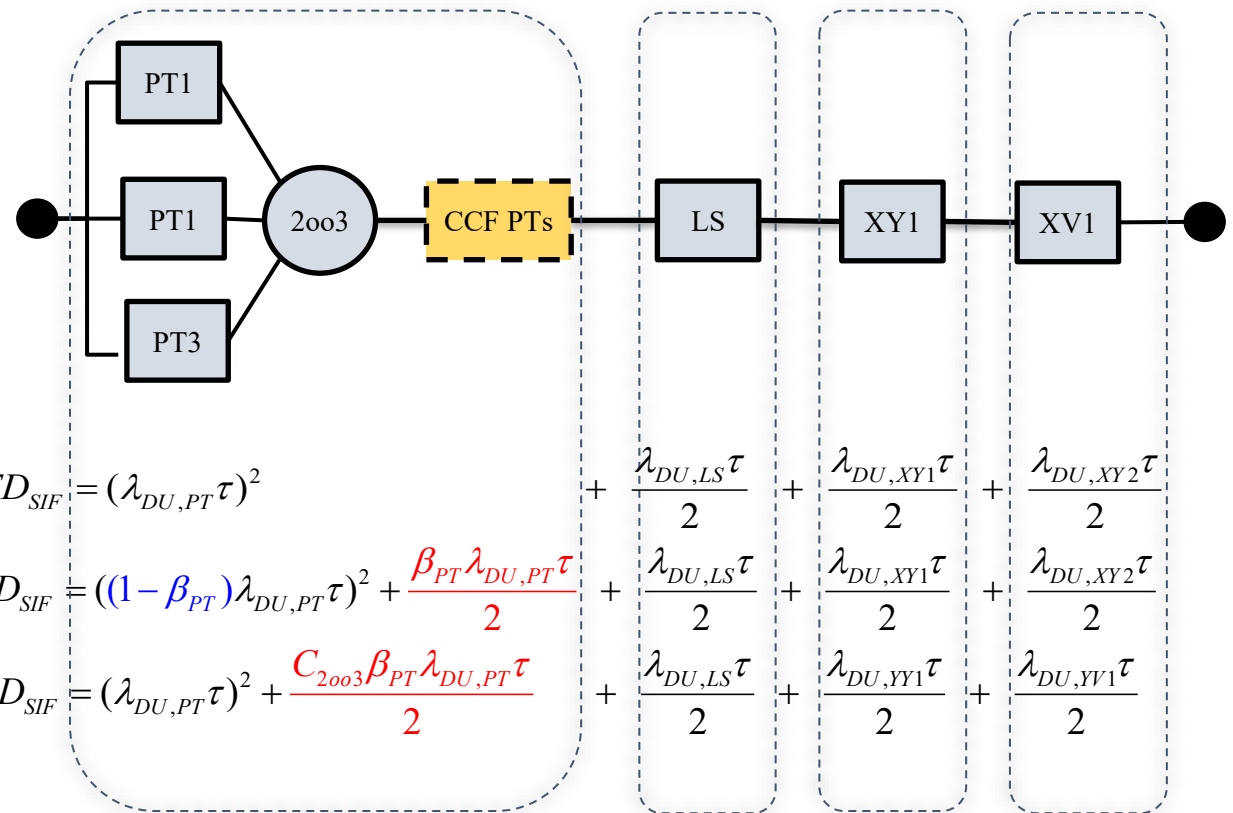
Eksempel på leverandørdata for en trykktransmitter er: https://www.exida.com/2024/ROS_11-07-062_C003_R4.8_3051_Certificate.pdf

Miniprojekt oppgave 2b)

c) Vi antar at SIF er low-demand. Lag et pålitelighetsnettverk («reliability block diagram») for hele SIF funksjonen for caset, sett opp formler og regn ut:

- PFD for hvert delsystem der kun uavhengige DU feil hensyntas
- PFD for hvert delsystem der også fellesfeil er hensyntatt med standard betafaktormodellen
- PFD for hvert delsystem der fellesfeil er hensyntatt med PDS metoden (C_{MooN} faktor inkludert for fellesfeil)

Pålitelighetsnettverk:

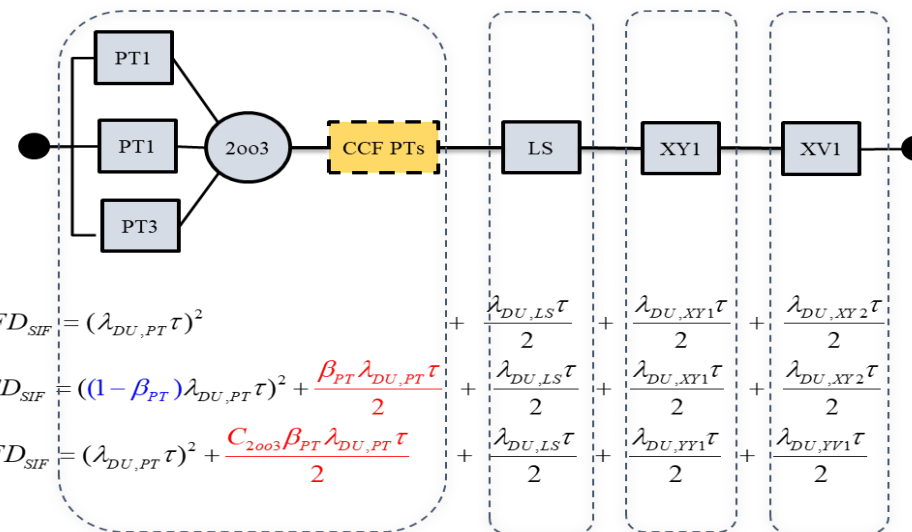


PSV: Pressure safety valve (purely mechanical, not a SIS)
 PT: Pressure transmitter
 I/P: Instrument (electrical) signal to pressure signal converter
 LT: Level transmitter
 LCV: Level control valve
 XV: Shutdown valve
 XY: Solenoid valve

Miniprojekt oppgave 2b)

Tabell 1 Modellparametere som skal benyttes (feilrate er per time)

Pålitelighetsdata	Parameter	Verdi
DU feilrate trykktransmittere	$\lambda_{DU,PT}$	0,5E-6 per time
DU feilrate logic solver	$\lambda_{DU,LS}$	0,8E-6 per time
DU feilrate solenoid valve XY	$\lambda_{DU,XY}$	0,6E-6 per time
DU feilrate shutdown valve (XV)	$\lambda_{DU,XV}$	1,9E-6 per time
Fellesfeilandel trykktransmittere	β	5%
Testintervall	τ	8760 hours (1 år)



In this case study: The subsystem input elements have a small influence on the PFD compared to the other systems

Result	Input elements subsystem	Logic solver subsystem	Final elements subsystem (XY and XV)	Total for SIF	SIL level
PFD					
PFD no CCFs	1.92E-5	3.5E-3	1.1E-2	1.45E-2	SIL 1
PFD w CFFs standard beta	1.27E-4	3.5E-3	1.1E-2	1.46E-2	SIL1
PFD w CCF using PDS method	2.38E-4	3.5E-3	1.1E-2	1.47E-2	SIL 1

Hva om vi skal regne på PFH heller enn PFD?

KooN systemer. Identiske komponenter som feiler uavhengig av hverandre.

$$PFH^{koon} = \binom{n}{n-k+1} \lambda_{DU}^{n-k+1} T^{n-k}$$

KooN systemer. Identiske komponenter som enten feiler uavhengig av hverandre eller feiler som resultat av fellesfeil.

Standard beta faktormodellen

$$PFH^{koon} = \binom{n}{n-k+1} \left((1-\beta) \lambda_{DU} \right)^{n-k+1} T^{n-k} + \beta \lambda_{DU}$$

PDS metoden

$$PFH^{koon} = \binom{n}{n-k+1} \lambda_{DU}^{n-k+1} T^{n-k} + C_{kooN} \beta \lambda_{DU}$$

Miniprojekt oppgave 2 c)

- d) I noen tilfeller kan man avdekke at demand-raten er mye høyere enn først antatt. Hva blir PFH for SIF funksjonen dersom vi antar at demand raten er oftere enn en gang per år? Regn ut med tilsvarende antagelser som i. og ii.
- d) Kommenter på hvilket SIL- nivå SIFen oppfyller (i begge operasjonsmodi – low demand og high demand).
- e) Lag en tabell som samler alle resultatene fra oppgave 1 (utregnet PFD og PFH) slik at de kan sammenlignes med andre metoder som brukes i etterfølgende oppgaver. Eksempelvis i et regneark.

Uten fellesfeil (i.)

$$PFH = 3(\lambda_{DU,PT})^2 T + \lambda_{DU,LS} + \lambda_{DU,XY1} + \lambda_{DU,XV1}$$

Standard beta faktormodellen (ii.)

$$PFH = 3((1 - \beta_{PT})\lambda_{DU,PT})^2 T + \beta_{PT}\lambda_{DU,PT} + \lambda_{DU,LS} + \lambda_{DU,XY1} + \lambda_{DU,XV1}$$

PDS metoden (til info)

$$PFH = 3\lambda_{DU,PT}^2 T + C_{2003}\beta_{PT}\lambda_{DU,PT} + \lambda_{DU,LS} + \lambda_{DU,XY1} + \lambda_{DU,XV1}$$

Miniprojekt oppgave 2 d) og e)

KUN for Subsystem input elements (PTs)

Result	Forenklete formler (oppgave 2)	Feiltreanalyse (oppgave 3)	Markov analyse (oppgave 4)
PFD			
PFD no CCFs	1.92E-5		
PFD w CCFs	1.27E-4		
PFD w CCF using PDS method	2.38E-4		
PFH (per time)			
PFH no CCFs	6.57E-9 (per hour)		
PFH w CFFs (standard beta)	3.09E-8 (per hour)		
PFH w CCF (PDS method)	5.66E-8 (per hour)		

Oppsummering

- Pålitelighetsnettverk er brukt til å visualisere SIFen og betingelsene for at SIFen virker eller feiler
- Valg av pålitelighetsmål avhenger av operasjonsmodi – low-demand eller high demand/continuous mode
- Low-demand: PFD er utledet fra pålitelighetsfunksjonen eller feilfunksjonen for en SIF delsystem
 - Gjennomsnitt over et testintervall
 - Sentrale parametere er votering, DU feilrate, testintervall τ og fellesfeilandel
 - Man kan skru på testintervallet for å sikre at kravet til PFD (fra risikoanalyse) oppfylles om feilraten er høyere eller lavere enn antatt
 - Vi kan ofte utelate DD feil
- High-demand/Continuous:
 - Gjennomsnittlig sviktrate for SIF delsystem over et intervall T
 - Sentrale parametere er DU feilrate og andel fellesfeil (T får liten betydning i formelen, men betyr ikke at den ikke er viktig)
- Vi kan bruke forenklede formler når delsystemene består av like komponenter og bare DU feil tas med