

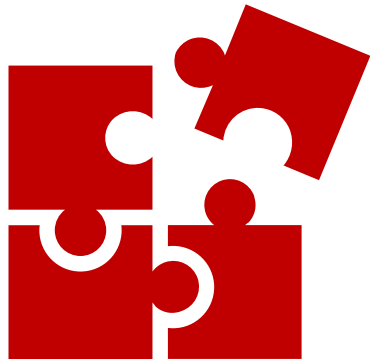
Sist
oppdatert
25.10.2023

TTK 2 – Design og analyse for funksjonell sikkerhet 2023

Seminar 5 – 25.10.2023

MARY ANN LUNDTEIGEN
TEKNISK KYBERNETIKK NTNU

TTK2



5. SIL analyse

Målsetning

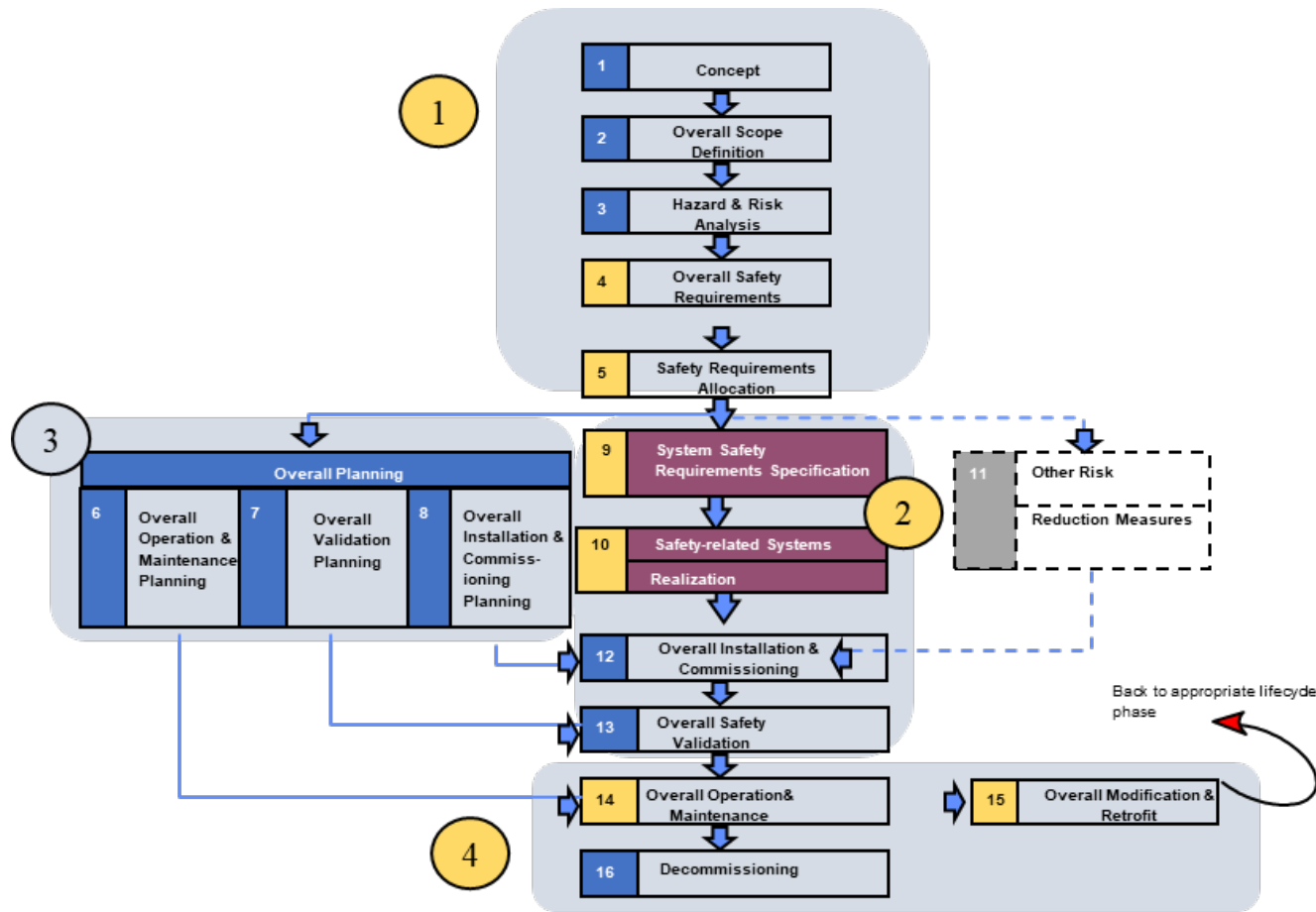
Pålitelighetsanalyse kan angi hvordan **sannsynlighet for overlevelse eller funksjonssvikt** påvirkes av **egenskaper** ved systemet og **måten det opererer** på. Vi skal her belyse pålitelighetsberegninger som skjer i en SIL analyse – både i design og i drift. Da er det fokus på systemsvikt.

Vi ønsker å belyse – gjennom **praktiske eksempler**: Hvilke **feildata** er viktig? Hvilke **test-strategier** kan velges? Hvilken **effekt** har de? Hvordan **oppdatere feilraten** med driftserfaring?

I arbeidet bruker vi **GRIF** sin SIL modul. Vi har fått låne denne lisensen frem til våren 2024.

- Bygger direkte på teori fra TTK 4175 instrumenteringssystemer
 - Kapittel 5 om SIS
 - Kapittel 6 om IEC 61508
 - Kapittel 7 om pålitelighetsanalyse
- Bruker GRIF verktøy «SIL modul»

IEC 61508 livsyklus og SIL analyse



SIL analyse dekker:

- Bestemme SIL krav til identifiserte SIFer (fase 4 & 5)
- Beregne SIL oppnådd for SIFene slik de er designet (fase 9 & 10)
 - Inkluderer pålitelighetsanalyse
- Beregne SIL oppnådd for SIFene i drift (14-15):
 - Inkluderer pålitelighetsanalyse

Hva er SIL?

SIL: discrete level (one out of four) allocated to the SIF for specifying the safety integrity requirements to be achieved by the SIS.

SIL	Allowed failure probability (PFD)	Allowed failure rate of dangerous failures per hour (PFH)
4	$1\text{E-}5 \leq \text{PFD} < 1\text{E-}4$	$1\text{E-}9 \leq \text{PFH} < 1\text{E-}8$
3	$1\text{E-}4 \leq \text{PFD} < 1\text{E-}3$	$1\text{E-}8 \leq \text{PFH} < 1\text{E-}7$
2	$1\text{E-}3 \leq \text{PFD} < 1\text{E-}2$	$1\text{E-}7 \leq \text{PFH} < 1\text{E-}6$
1	$1\text{E-}2 \leq \text{PFD} < 1\text{E-}1$	$1\text{E-}6 \leq \text{PFH} < 1\text{E-}5$

- **Probability of failure on demand (PFD):** The average probability that the SIF fails to perform its safety function on demand. The term "demand" means the event for which the SIF is expected to respond to.
- **Probability of having a dangerous failure *per* hour (PFH):** The average probability of having a dangerous failure per hour, or average frequency of SIF being in a failed state due to dangerous failure.

Hva som inngår i SIL analysen



I kravutviklingsfasen inngår å:

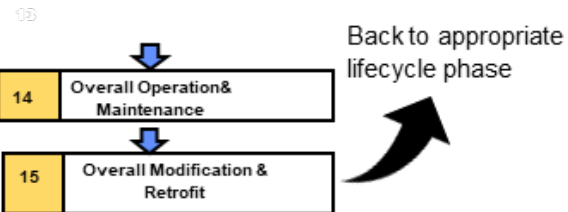
- **Utføre risikoanalyse** for å avdekke farekilder og risikoreduserende tiltak og funksjoner, inkludert SIFer.
- Allokere **SIL krav/PFD verdi** til hver enkelt SIF
- Utarbeide en safety requirements specification (SRS)

I design og sammenstillingsfasen inngår å:

- Velge votering utfra SIL krav (ikke dekket her)
- Følge arbeidsmetodikk som følger SIL kravet
- **Beregne PFD** for hver SIF funksjon slik de er realisert (utstyrdata, votering)
- **Sammenligne** PFD med **SIL kravet**
- Re-designe eller justere av testintervallet om SIL kravet ikke oppfylles

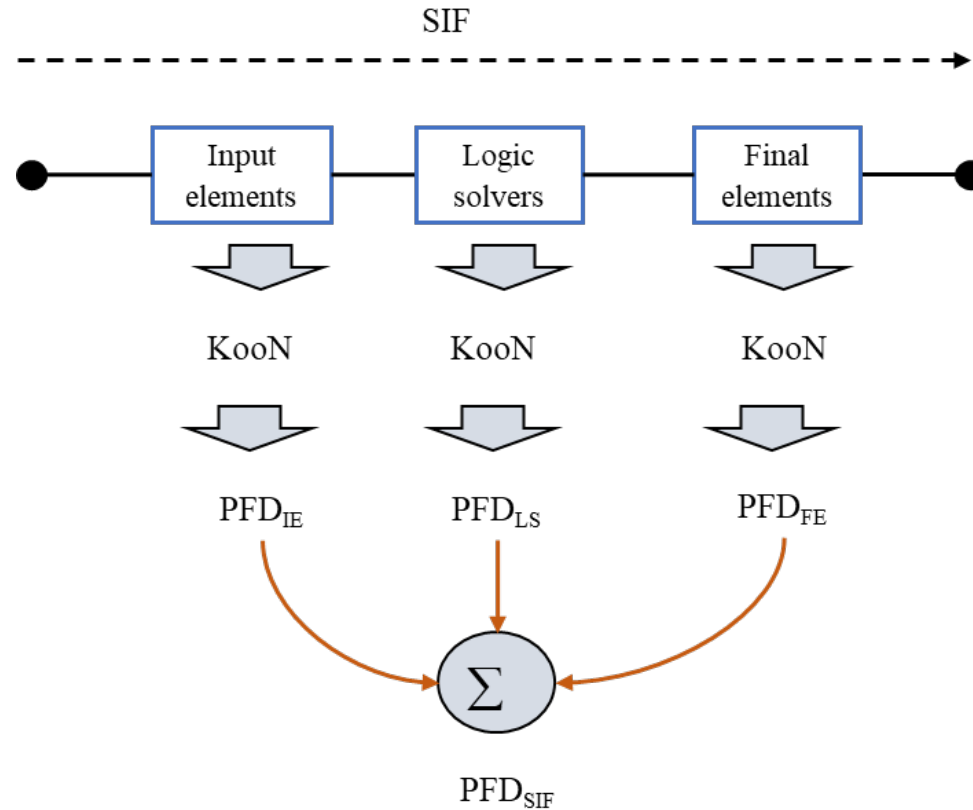
I driftsfasen inngår å:

- Rapportere og klassifisere feil
- Utføre funksjonstesting og vedlikehold
- Systematisk håndtering av alle endringsforslag
- **Beregne PFD** for hver SIF funksjon i drift basert på **oppdaterte feilrater (rapportere feil i drift)**
- **Sammenligne** med **SIL kravet**
- Justere testintervallet eller skifter ut utstyr om SIL kravet ikke møtes



TTK2

SIL analyse: Beregning av PFD

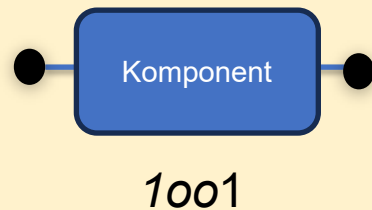


- PFD beregnet for hver SIF (low-demand)
- Sammenlignes med SIL kravet

SIL analyse: Hvordan bestemmes PFD?

PFD – gjennomsnittlig sannsynlighet for at funksjonen ikke virker

Eksempel (enkeltkomponent):

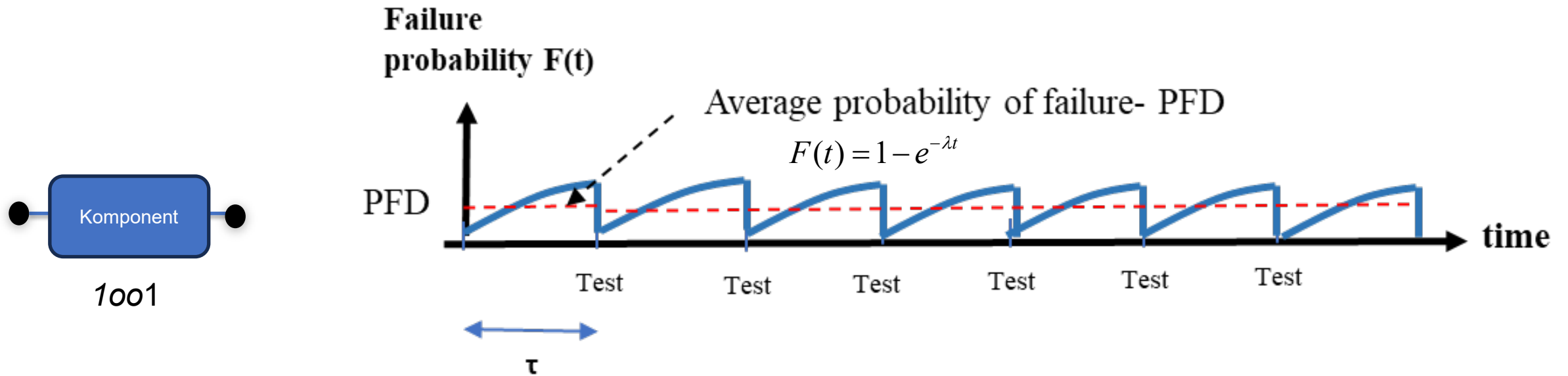


Feilrate (DU feil) for komponent

$$PFD \approx \frac{\lambda_{DU} \tau}{2}$$

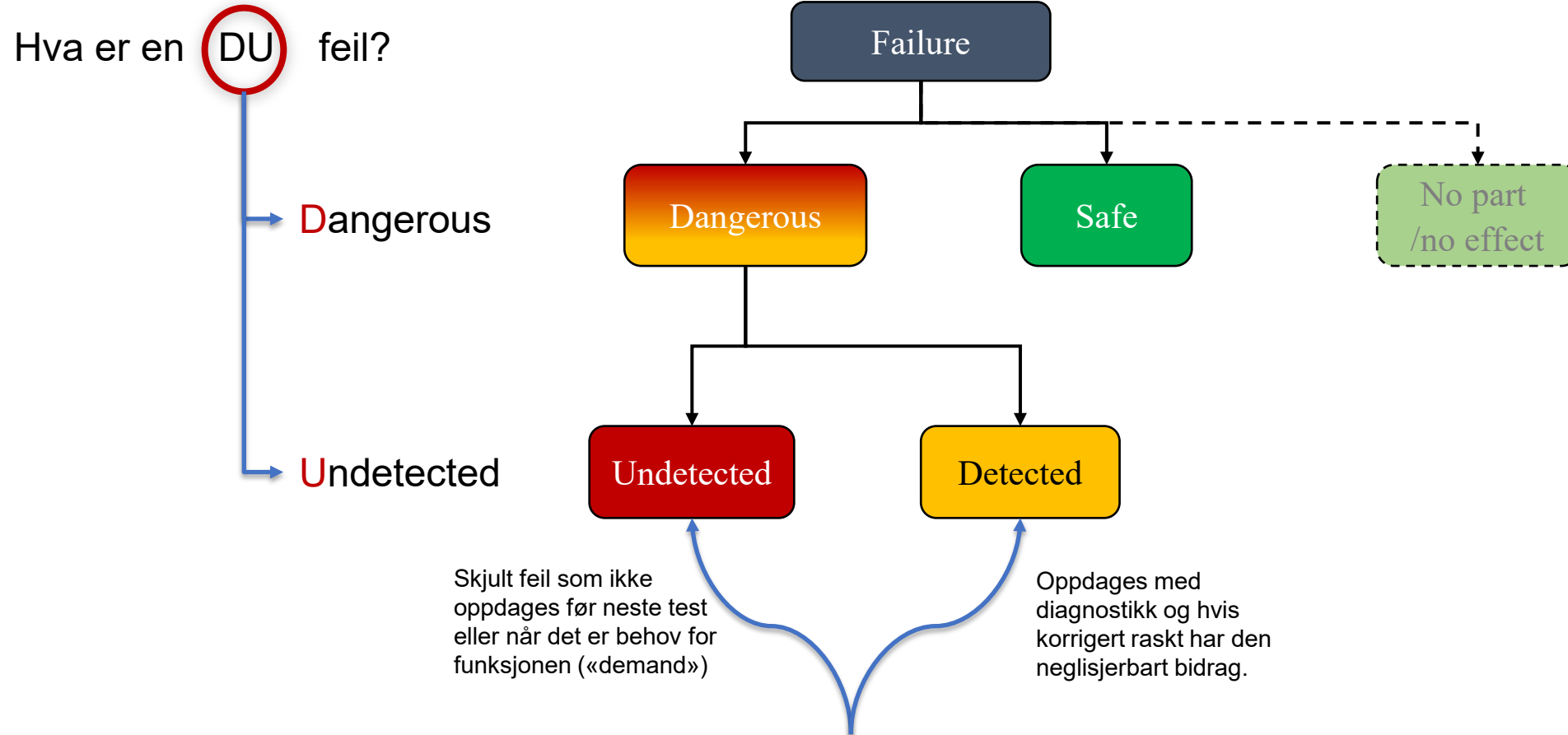
Funksjonstest-
intervall

SIF pålitelighet – Hvordan fremkom PFD?



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

Hvilke feil hensyntas? – feilklassifisering (I)

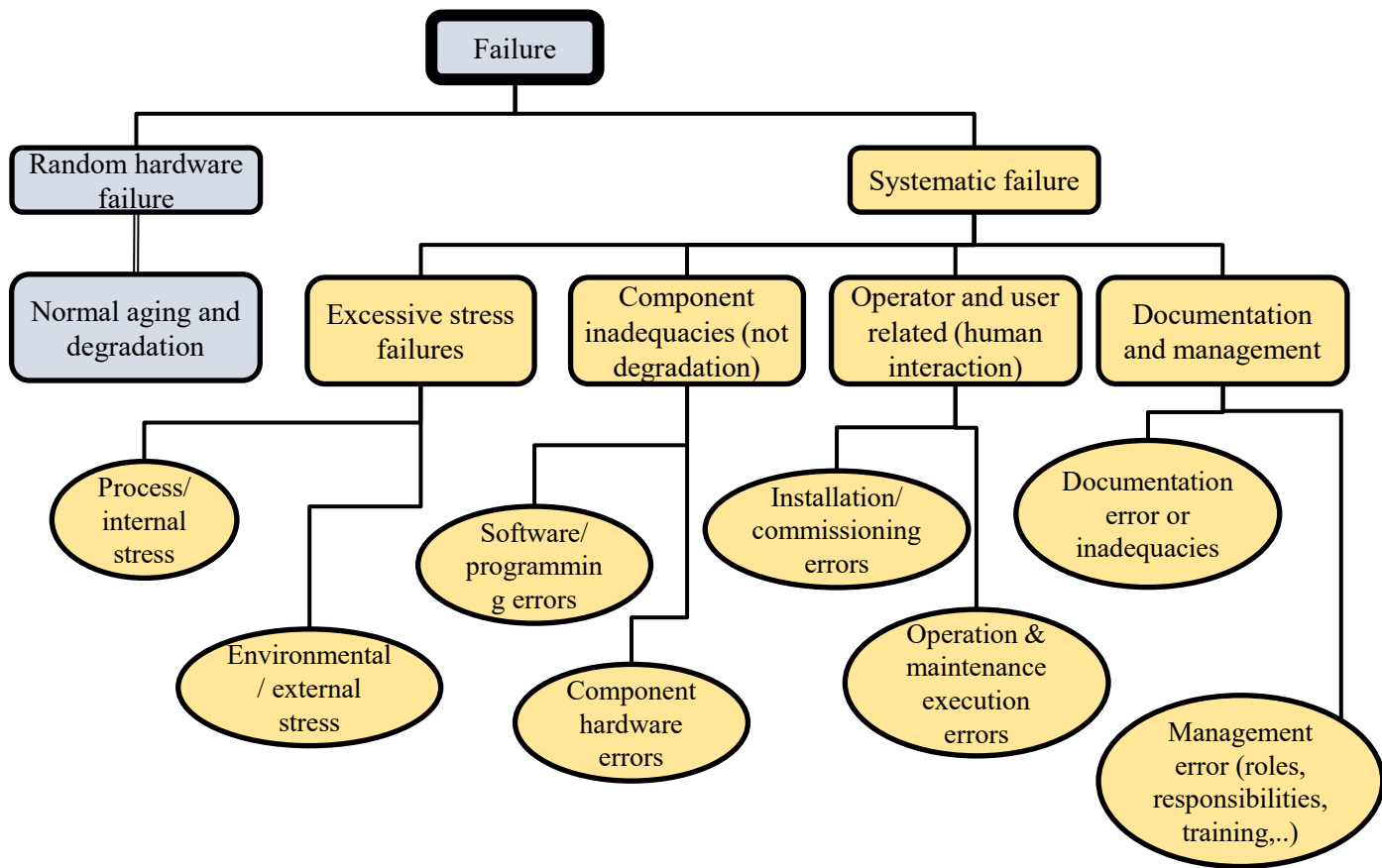


Hvorfor er DU feil viktigst i beregning av PFD?

Hvilke feil hensyntas? Feilklassifisering (II)

En DU (og DD, S etc) kan være **tilfeldig** (random hardware) eller **systematisk**, avhengig av feilårsaken.

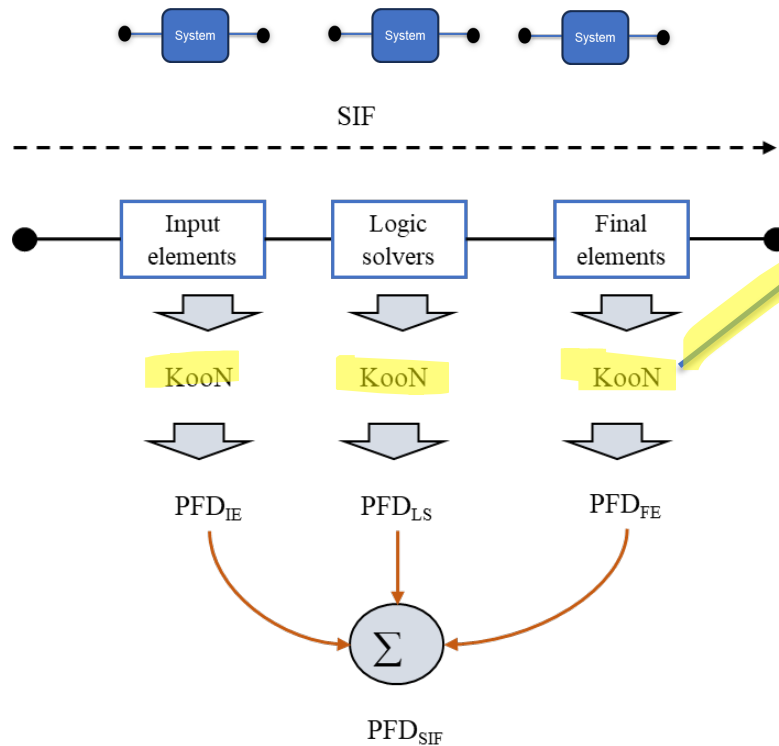
I **feilraten** inngår **alle random feil**, og **en del av de systematiske** som gjentar seg



Formler for PFD (subsystem av like komponenter)

PFD:

- Average Probability of failure on demand
- Beregnes først for hvert delsystem og deretter samlet



Formler for delsystem av **LIKE** komponenter

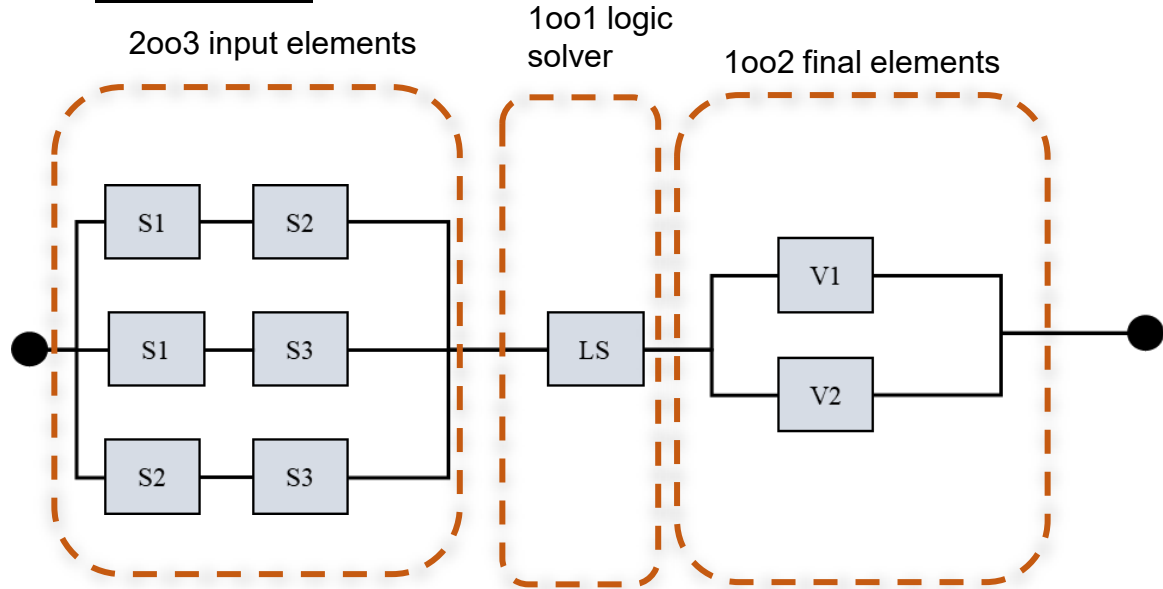
k/n	1	2	3	4
1	$\frac{\lambda_{DU}\tau}{2}$	$\frac{(\lambda_{DU}\tau)^2}{3}$	$\frac{(\lambda_{DU}\tau)^3}{4}$	$\frac{(\lambda_{DU}\tau)^4}{5}$
2	--	$\lambda_{DU}\tau$	$(\lambda_{DU}\tau)^2$	$(\lambda_{DU}\tau)^3$
3	--	--	$\frac{3(\lambda_{DU}\tau)^2}{2}$	$2(\lambda_{DU}\tau)^2$
4	--	--	--	$2\lambda_{DU}\tau$

Funksjonstestintervall

(Konstant) Feilrate for dangerous undetected (DU) feil

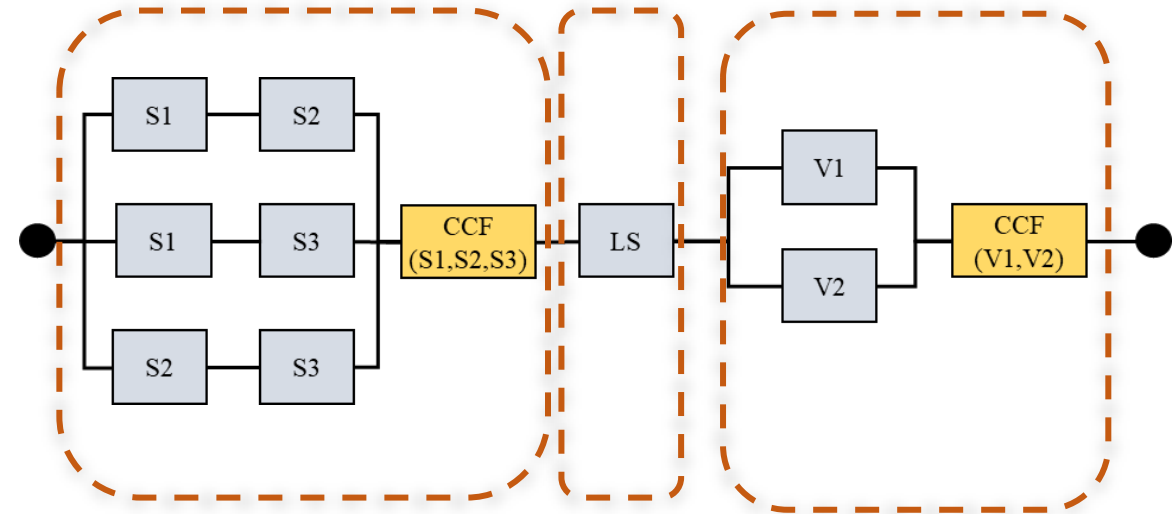
SIS pålitelighetsanalyse

Uten fellesfeil, antar like komponenter ved redundans



$$PFD = (\lambda_{DU,S}\tau)^2 + \frac{\lambda_{DU,L}\tau}{2} + \frac{(\lambda_{DU,V}\tau)^2}{3}$$

Med fellesfeil, antar like komponenter ved redundans



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

Hvor finner vi data?

SRS dokumentet

Table 4-1 Summary of requirement allocation

IEC 61511 req. #	Requirement description	General / system / PS	SIF	Tag
a	SIF description	a	M	
b	A list of the plant input and output devices related to each SIF		M	
c	Requirements to identify and take account of common cause failures.	M	a	a
d	A definition of the safe state of the process for each identified SIF	a	M	a
e	A definition of any individually safe process states	a	M	
f	The assumed sources of demand and demand rate on each SIF	a	M	a
g	Requirements relating to proof test intervals	a	a	M
h	Requirements relating to proof test implementation	a		M
i	Response time requirements for each SIF	i	M	i
j	The required SIL, mode of operation and PFD (or PFH) if relevant		M	a
k	A description of SIS process measurements, range, accuracy and their trip points	M		a
l	A description of SIF process output actions	a	M	a
m	The functional relationship between process inputs and outputs	a	M	
n	Requirements for manual shutdown for each SIF	M	i	(a)
o	Requirements relating to energize or de-energize to trip for each SIF	a	M	i
p	Requirements for resetting each SIF after a shutdown	M	a	a
q	Maximum allowable spurious trip rate for each SIF.	M	a	(a)
r	Failure modes for each SIF and desired response of the SIS	a	a	M
s	Procedures for starting up and restarting the SIS	M		
t	All interfaces between the SIS and any other system	M		(a)
u	Modes of operation of the plant and requirements to SIF operation for each mode	M	a	(a)
v	The application program safety requirements	M		
w	Requirements for bypasses including written procedures to be applied	a	M	
x	Specification of any [manual] action necessary to achieve or maintain a safe state	M	(a)	(a)
y	The mean repair time which is feasible for the SIS	a	a	M
z	Identification of the dangerous combinations of output states of the SIS	M		
aa	Identification of the extremes of all environment conditions	M		i
bb	Identification of normal and abnormal process operating modes	M	(a)	
cc	Requirements for any SIF necessary to survive a major accident event	M		(a)
Additional requirements				
A-1	Description or reference on method of SIL allocation	a	M	
A-2	Description of other protection layers	M	(a)	
A-3	A statement on which barrier/sub-barrier/barrier element the SIF is part of	i	M	
A-4	Modification and change control	M	(a)	(a)
A-5	Diagnostics: provisions of additional diagnostics	a	(a)	M

- SIF subsystems & voting
- Function (or proof) test intervall
- Demand rate

PDS DATA HANDBOOK - 2021 EDITION

Reliability Data for Safety Equipment



Reliability Data for Safety Equipment
PDS Data Handbook, 2021 Edition

4.4 Topside Final Elements

4.4.1 Topside ESV and XV

Module: Final Elements		PDS Reliability Data Dossier	
Equipment Group: Topside Shutdown and Isolation Valves			
Component: Topside ESV and XV			
Component Boundaries / Failure Definition			
Includes the main valve (ESV or XV) and the actuator (both gate, ball and some butterfly valves). Not including solenoid/pilot valve (differs from ISO 14224 where pilot and solenoid are included in the equipment class = Valves). Valve/actuator assumed to be spring return to closed position. Full stroke with tight shut off.			
Dangerous failure typically defined as "the valve does not close upon signal or within specified time (if response time requirement given), or has a higher internal leakage rate in closed position than the specified acceptance criterion (if given)".			
SINTEF's Best Estimates			
Failure rates (per 10 ⁶ h)	Coverage/Other	Failure mode distribution	
$\lambda_{DU} = 2.3$	DC = 0.05	FTC:	45 %
$\lambda_D = 2.5$	$\beta = 0.08$	DOP:	40 %
$\lambda_S = 2.0$		LCP:	15 %
$\lambda_{DU} = 4.5$			
λ_{DU} (per 10 ⁶ h) Uncertainty and Population Details			
All operational review data			
$\lambda_{DU} = 2.3$	$DU_{obs} = 248$	Observation period:	2006 – 2019
$\lambda_{DU}^{70\%} = 2.4$	$DU_{calc} = 215$	Population size:	1846
$\lambda_{DU}^{5-95\%} = [2.1, 2.6]$	$T = 9.2 \cdot 10^6$ h	No. of facilities:	10 (5 operators)
Application: ESD and combined ESD/PSD service			
$\lambda_{DU} = 2.3$	$DU_{obs} = 112$	Observation period:	2006 – 2019
$\lambda_{DU}^{70\%} = 2.6$	$DU_{calc} = 93$	Population size:	837
$\lambda_{DU}^{5-95\%} = [1.9, 2.8]$	$T = 4.0 \cdot 10^6$ h	No. of facilities:	10 (5 operators)
Application: PSD service			
$\lambda_{DU} = 2.3$	$DU_{obs} = 136$	Observation period:	2006 – 2019
$\lambda_{DU}^{70\%} = 2.5$	$DU_{calc} = 122$	Population size:	1009
$\lambda_{DU}^{5-95\%} = [2, 2.7]$	$T = 5.2 \cdot 10^6$ h	No. of facilities:	8 (3 operators)
Size: Small (0-1 inch)			
$\lambda_{DU} = 1.3$	$DU_{obs} = 6$	Observation period:	2006 – 2019
$\lambda_{DU}^{70\%} = 1.7$	$DU_{calc} = 6$	Population size:	97
$\lambda_{DU}^{5-95\%} = [0.6, 2.6]$	$T = 4.6 \cdot 10^6$ h	No. of facilities:	5 (2 operators)
Size: Medium (1-3 inches)			
$\lambda_{DU} = 1.7$	$DU_{obs} = 47$	Observation period:	2006 – 2019
$\lambda_{DU}^{70\%} = 1.9$	$DU_{calc} = 39$	Population size:	407
$\lambda_{DU}^{5-95\%} = [1.3, 2.2]$	$T = 2.3 \cdot 10^6$ h	No. of facilities:	5 (2 operators)

- Failure rate for each of the components based on aggregated experience from use in sector

99 of 216

Certificate / Certificat / Zertifikat / 合格証

ROS 1107062 C003

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 2@HFT=0, SIL 3@HFT=1, Route 1_n (models SFF ≥ 90%)
SIL 2@HFT=0, SIL 3@HFT=1, Route 2_n (low demand, SFF < 90%)
SIL 2@HFT=1, SIL 3@HFT=1, Route 2_n (high demand, 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_n.

IEC 61508 Failure Rates in FIT²

Route 1 _n Table					
Device	λ_{DU}	λ_{DU}	λ_{DU}	λ_{DU}	SFF
Rosemount® 3051 Coplanar Differential & Coplanar Gage	0	84	258	31	91%
Rosemount® 3051 Coplanar Absolute, In-line Gage & Absolute	0	94	279	42	90%
Route 2 _n Table ³					
Device	λ_{DU}	λ_{DU}	λ_{DU}	λ_{DU}	
Rosemount® 3051 Coplanar Differential & Coplanar Gage	0	84	258	32	
Rosemount® 3051 Coplanar Absolute, In-line Gage & Absolute	0	94	279	41	
Rosemount® 3051 Flowmeter Series based on 1195, 405, or 485 Primaries					
Flowmeter Series ⁴	0	92	258	41	
Rosemount® 3051 Level Transmitter (two 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 ⁵					

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 1301-010 R009 V4R3 or later

Safety Manual: 00809-0100-4007

¹BRS 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_n data. For information detailing the Route 2_n approach as defined by IEC 61508-2, see Technical Document entitled "Route 2_n 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.



80 N Main St
Sellersville, PA 18960

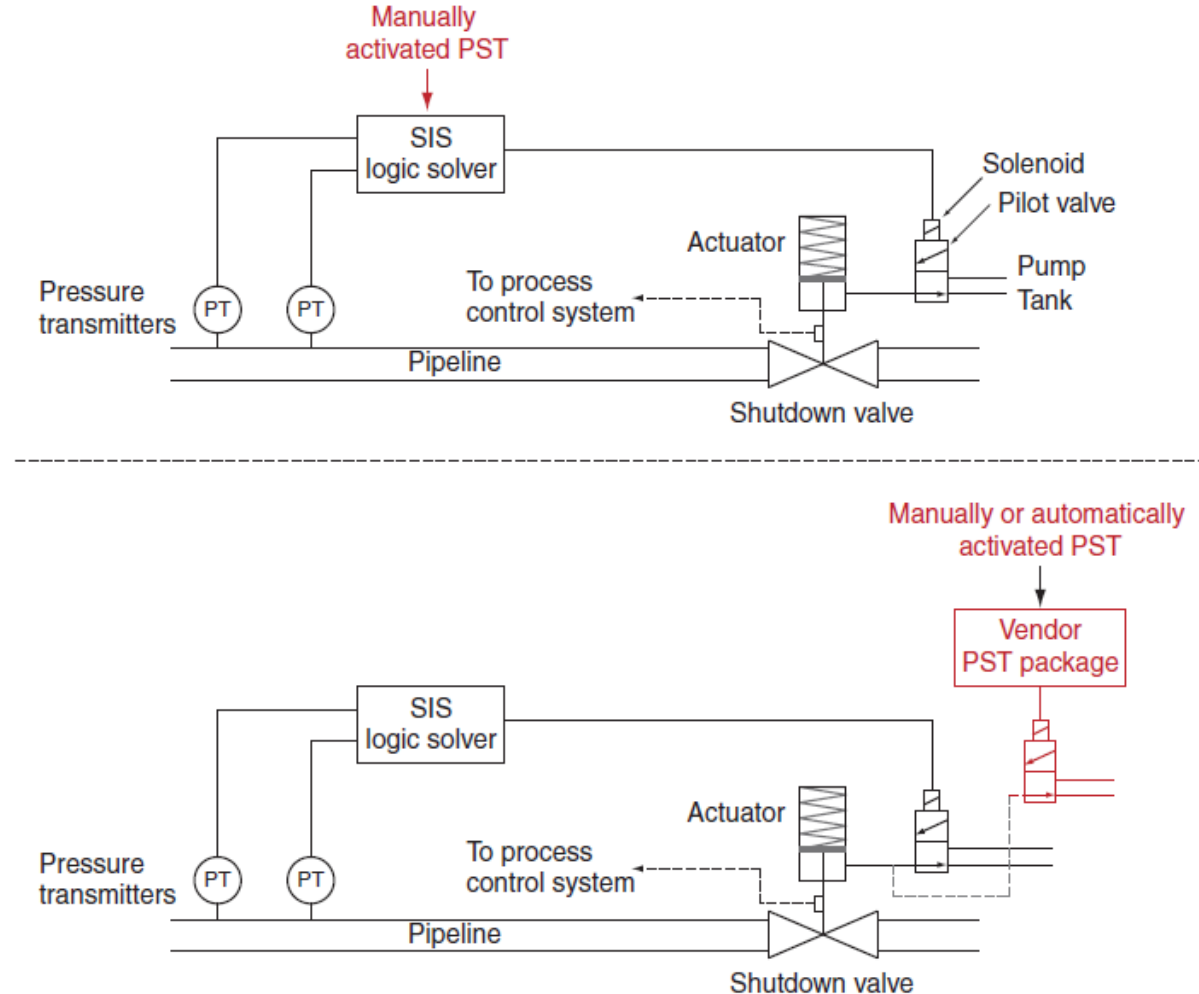
T-002, V6R1

Page 2 of 2

- Failure rate for each of the components manufacturers' SIL certificate

Test strategier: Delvis (partial) testing

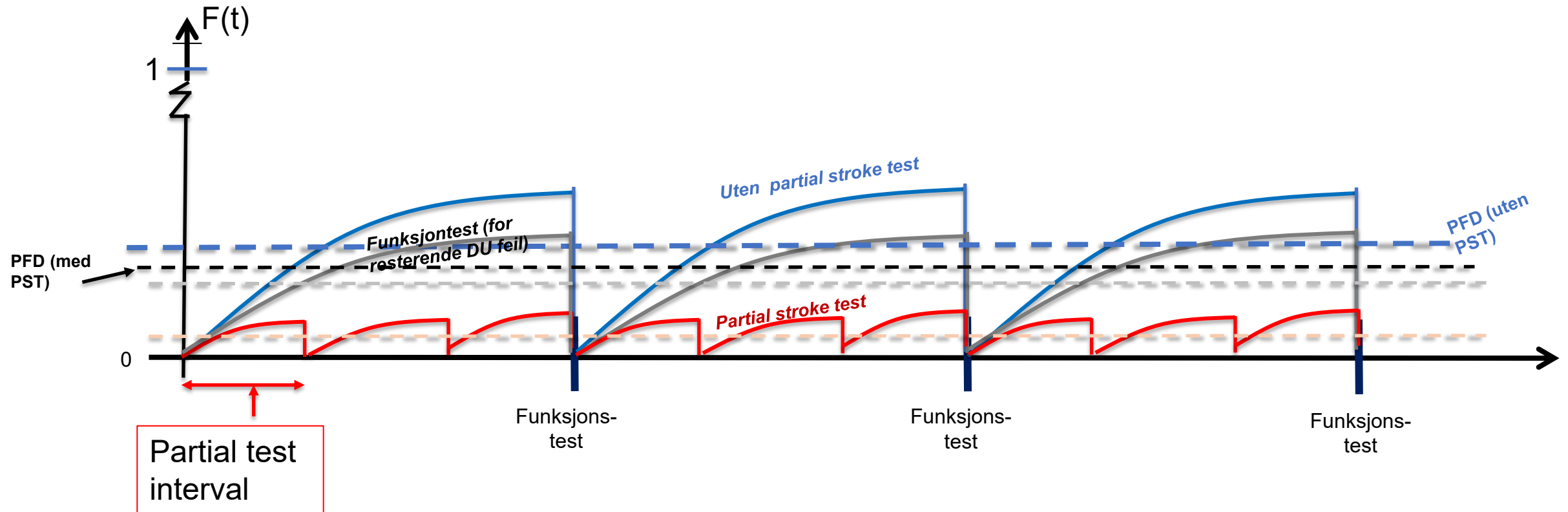
Eksempel: Partial stroke testing av ventiler



TTK2

Partial test coverage (PST*)

- **Partial stroke test (PST) coverage:** Andel av feil (DU) som oppdages i ved partial stroke test.
- Kan utføres **hyppigere** enn en funksjonstest da den ikke forstyrrer produksjonen

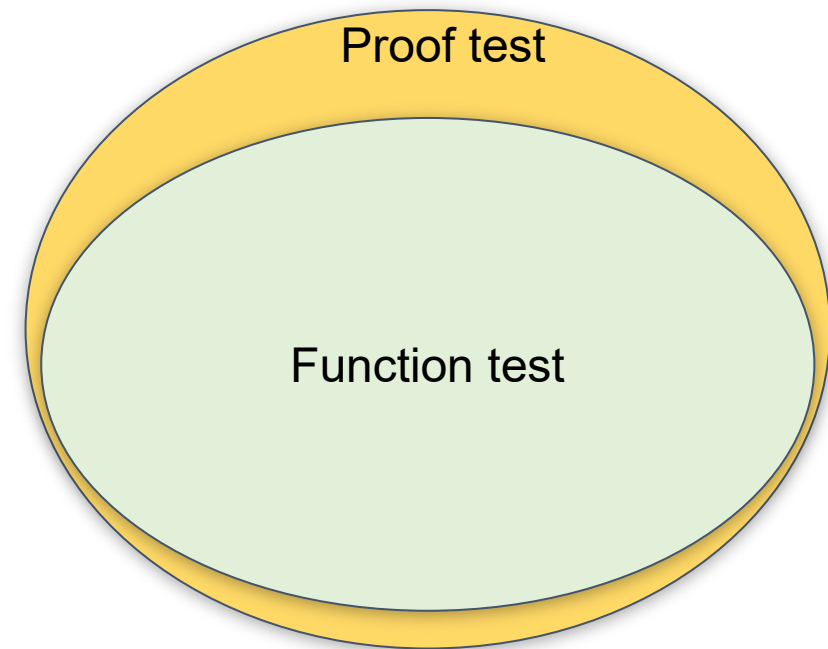


Partial test

- Man kan også ha partial test for sensorer og logikk
- Her har vi bare fokus på ventiler

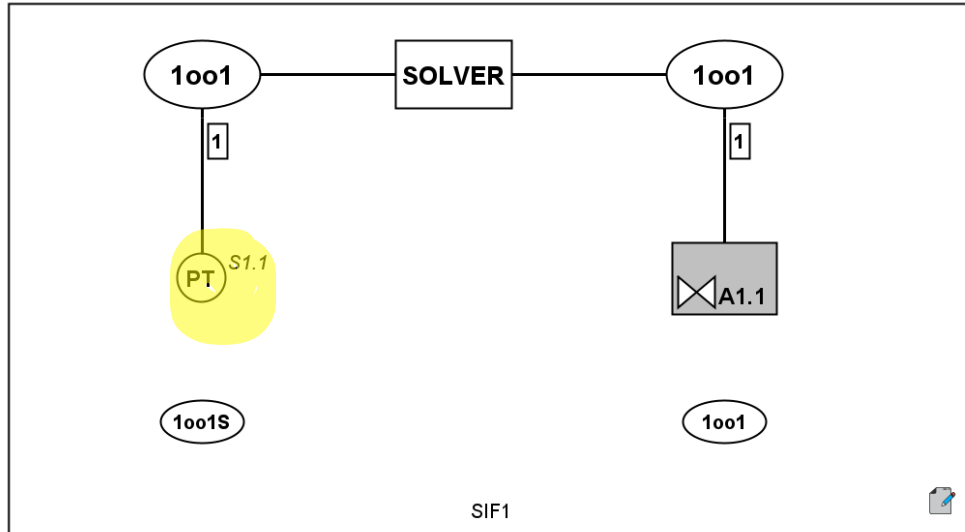
Proof test coverage

- Proof test – utvidet test som dekker all mulig funksjonalitet – også utenom sikkerhetsfunksjonen
 - Utføres etter modifisering/ oppgradering
 - Eventuelt «aldri» om utstyret «ikke røres»
- Funksjonstest – fokus på test av sikkerhetsfunksjon
 - Utføres jevnlig



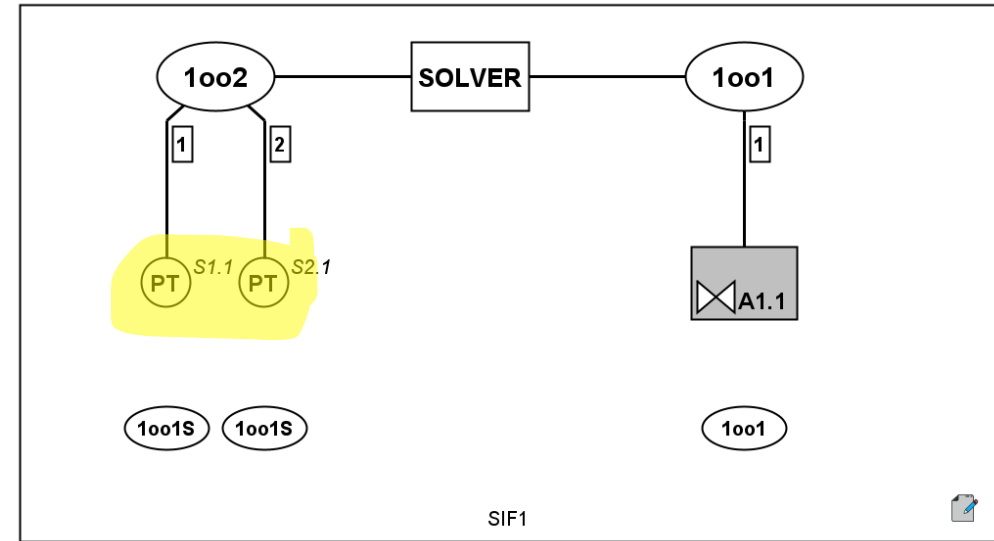
Proof test coverage (PTC): Andel DU feil som ikke oppdages ved jevnlig funksjonstesting

Praktiske eksempler - Test scenarier



- PFD(t) per komponent
- PFD (t) for SIF
- PFD avg for SIF

Med og uten partial stroketesting
Med proof test coverage < 100%



- PFD(t) per komponent
- PFD (t) for SIF
- PFD avg for SIF

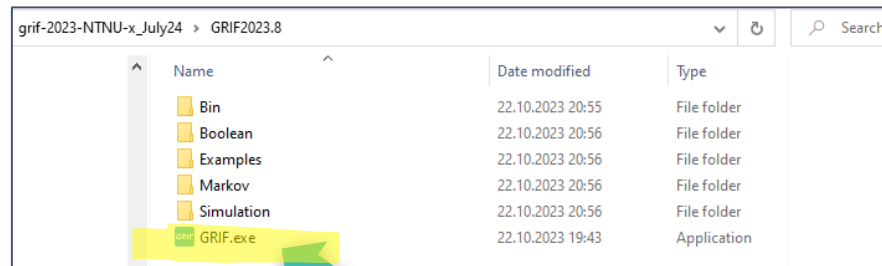
Med og uten fellesfeil
Med og uten partial stroke testing
Med proof test coverage < 100%

Default data i GRIF verktøyet er benyttet som utgangspunkt med noen små justeringer. Se opplastede filer.

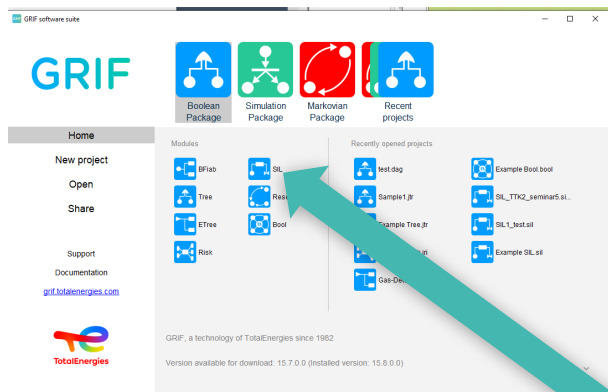
TTK2

GRIF verktøyet (<https://grif.totalenergies.com/en>)

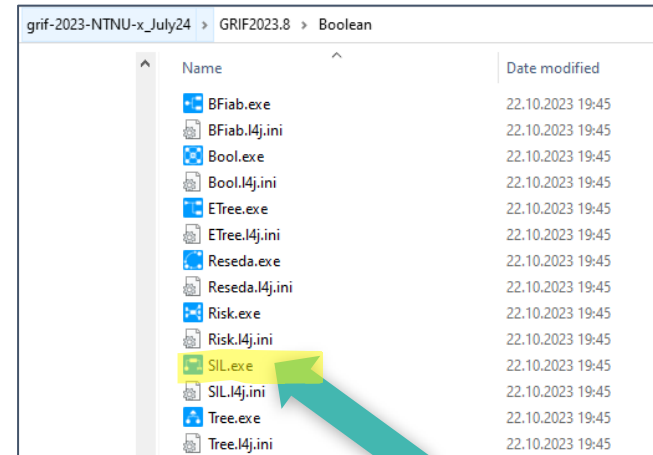
Bruk av GRIF verktøyet SIL modul går igjennom i seminarat. Husk å laste ned (se innlegg på teamssiden for TTK2!)
Last ned fra NTNU nett så går det raskere!



Dobbeltklikk på denne (og vent litt. Treg oppstart)



Velg så denne



Eller direkte SIL.exe under katalogen Boolean



Startes da direkte

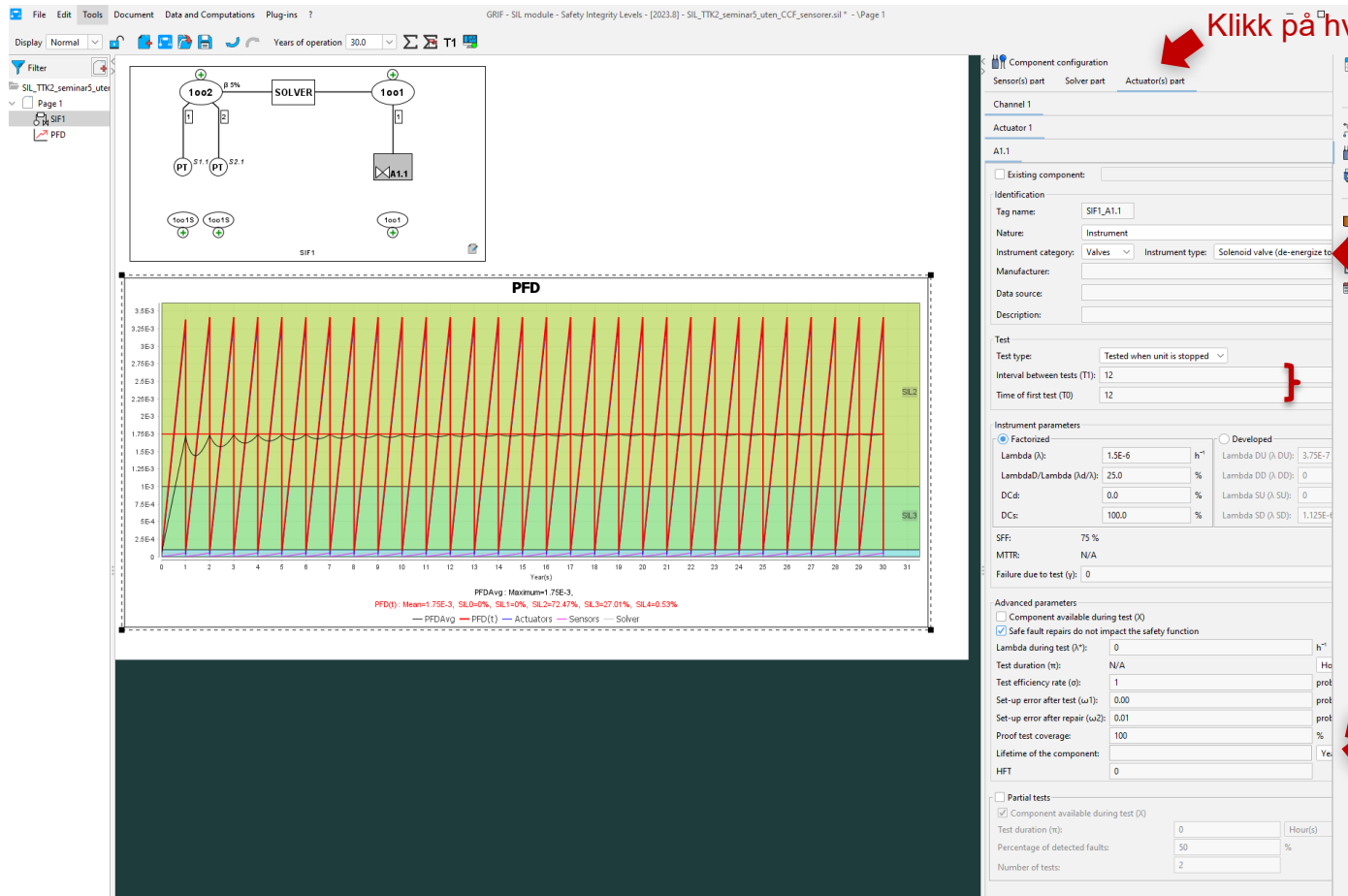


Og du får opp følgende vindu

TTK2

«Krasjkurs»: Meny for komponent data

PS: Solver part har litt annet oppsett. Oppgir en feilsannsynlighet, ikke feilrate.



Klikk på hvilken type komponent du vil endre data for

Votering for subsystemer, fellesfeil

Komponentdata

Type ventil (vi har her bare brukt solenoideventil som eksempel)

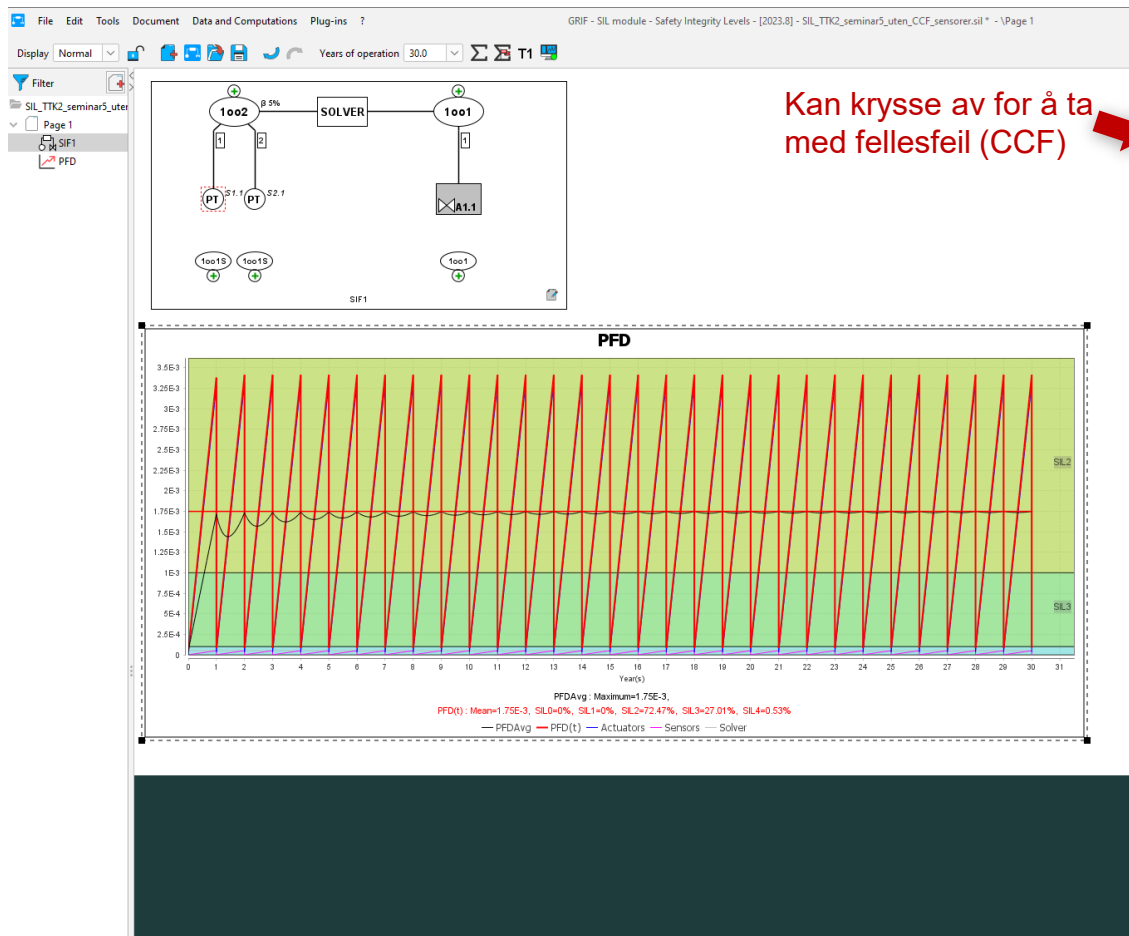
Funksjonstestintervall

Bestemme om proof test coverage skal være mindre enn 100%
Må velge hvor ofte proof test utføres

Bestemme om partial test er med

TTK2

«Krasjkurs»: Meny for votering av subsystem



Kan krysse av for å ta med fellesfeil (CCF)

Votering sensorsystem

Votering for subsystemer, fellesfeil

Komponentdata

Endrer ikke på disse. Gjelder intern redundans

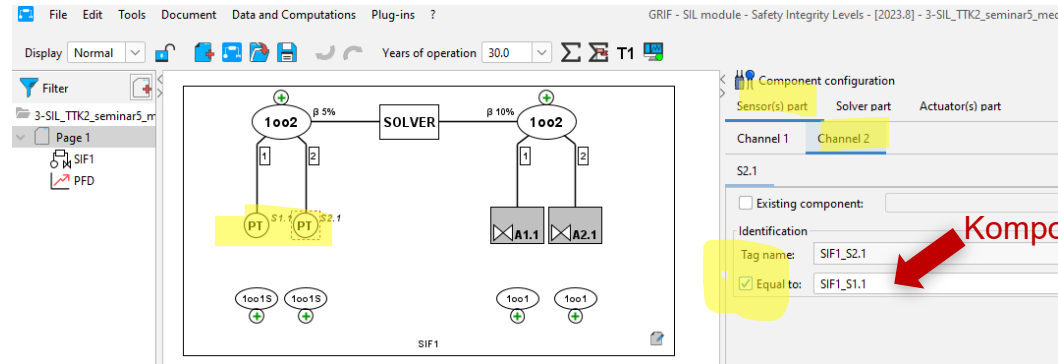
Votering aktuatorer

Endrer ikke på disse. Gjelder intern redundans

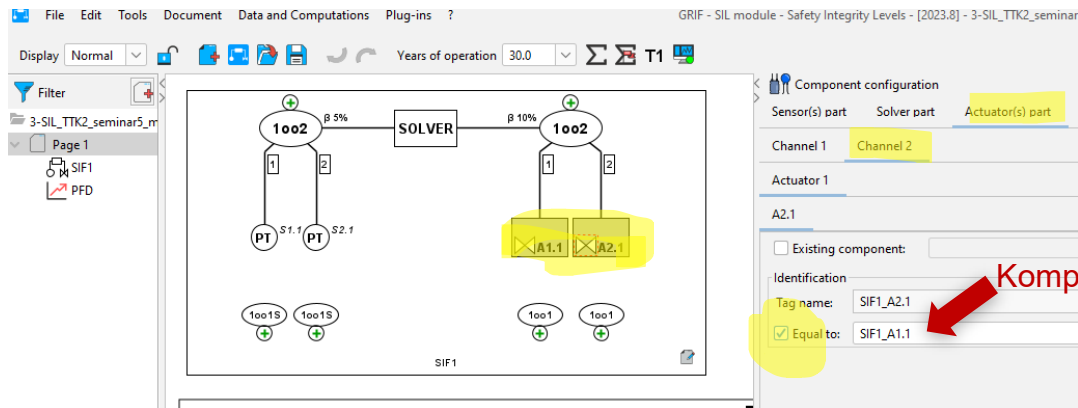
I verktøyet får vi ikke endret på votering logikk

«Krasjkurs»: Valg av data for den redundante komponenten

Når du legger til en redundant kanal, husk å la den nye kanalen(e) kopiere data fra den første.



Komponent i kanal 2 får kopiert inn data fra komponent i kanal 1

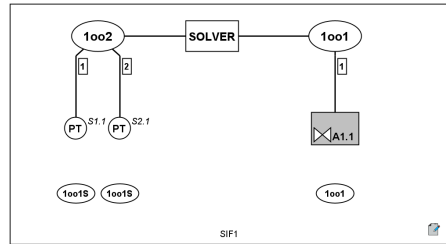


Komponent i kanal 2 får kopiert inn data fra komponent i kanal 1

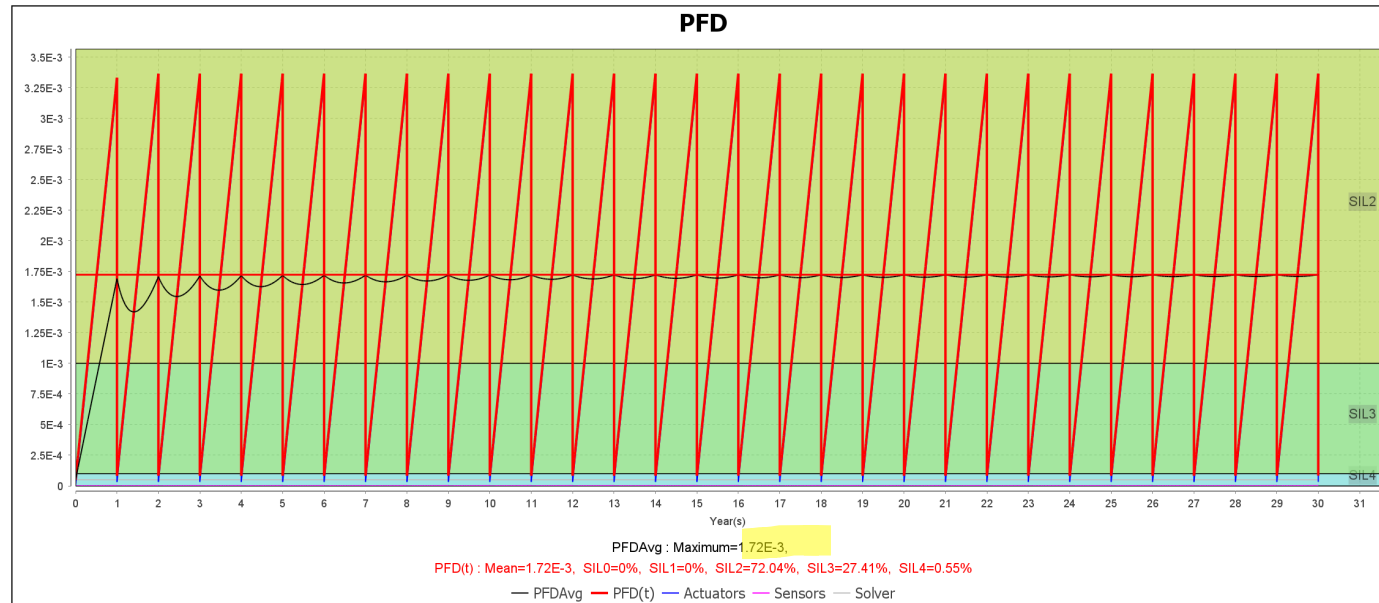
TTK2

SIF m/1oo2 voterte sensorer

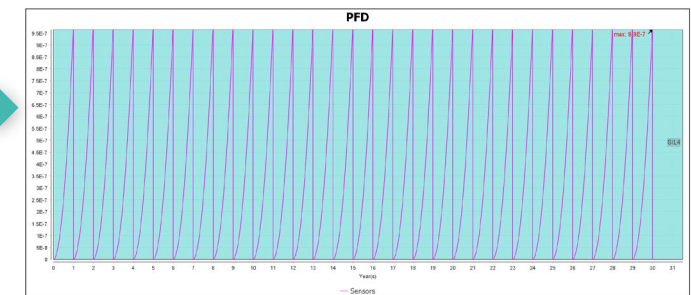
Fil: 1-SIL_TTK2_seminar5_uten_CCF_sensorer.sil



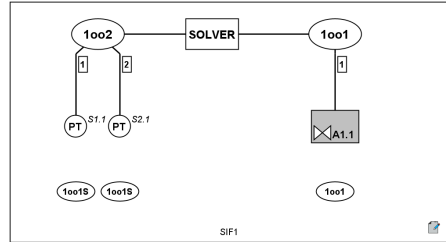
Uten fellesfeil (CCF) for sensorene



Sensorene har neglisjerbar betydning



SIF m/1oo2 voterte sensorer



Med fellesfeil (CCF) for sensorene. Beta satt til 5%

Fil: 2-SIL_TTK2_seminar5_med_CCF_sensorer.sil

Sensor architecture

Number of channels configured in

☒ Take into account Common Cause Failures

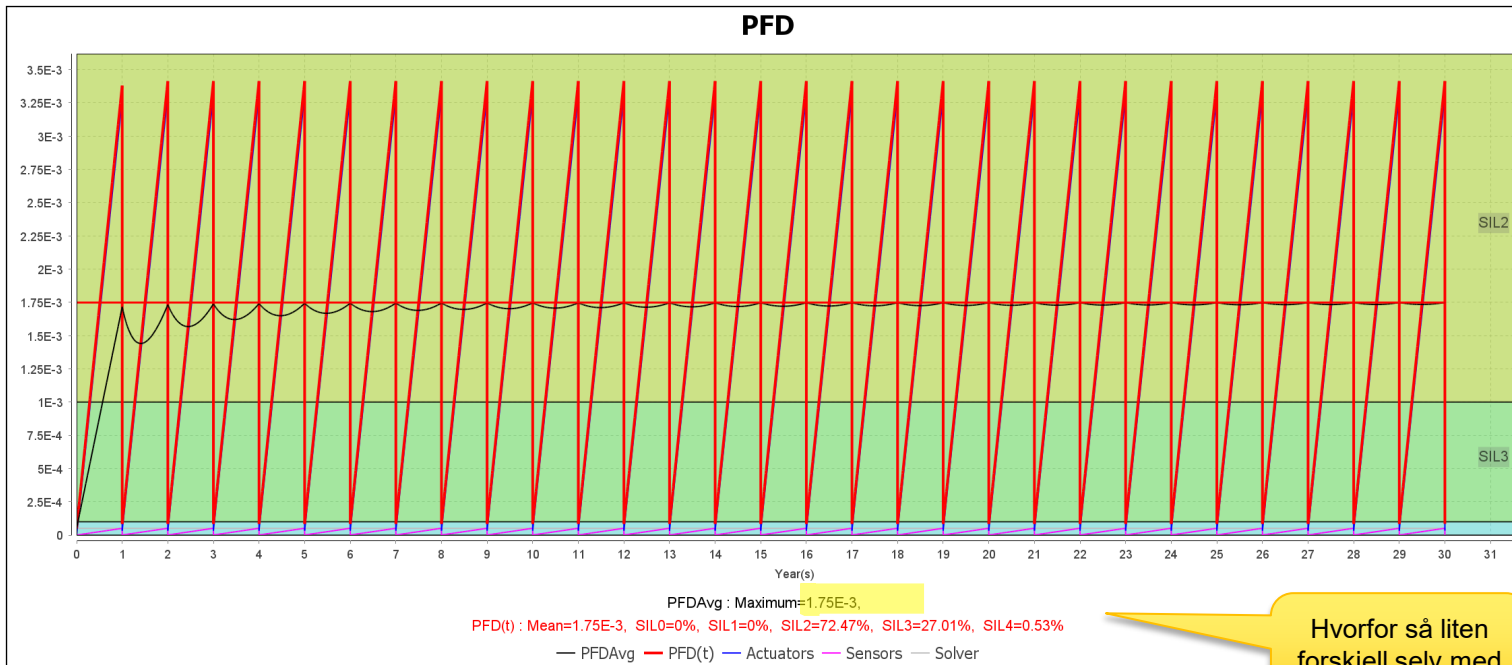
Beta inter-channels (du) % ☐ Beta IEC61508-6 D ...

Channel 1 Channel 2

Number of sensors configured in 1 detected fault le

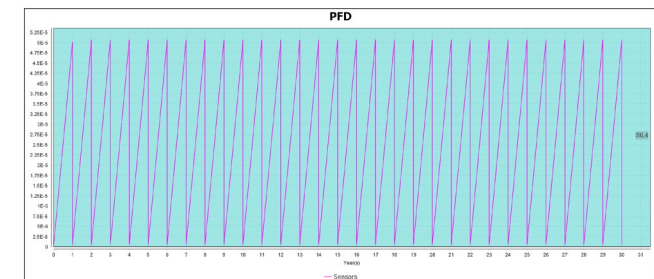
☐ Take into account Common Cause Failures

Beta sensors (du) % ☐ Beta IEC61508-6 D ...



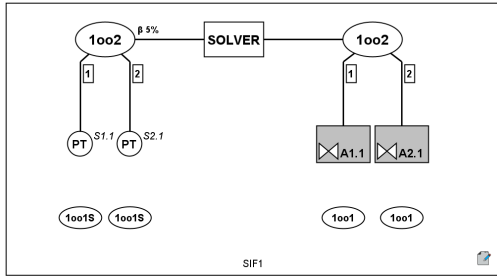
Hvorfor så liten forskjell selv med CCF?

Sensorene



SIF m/1oo2 voterte ventiler (oppdatere)

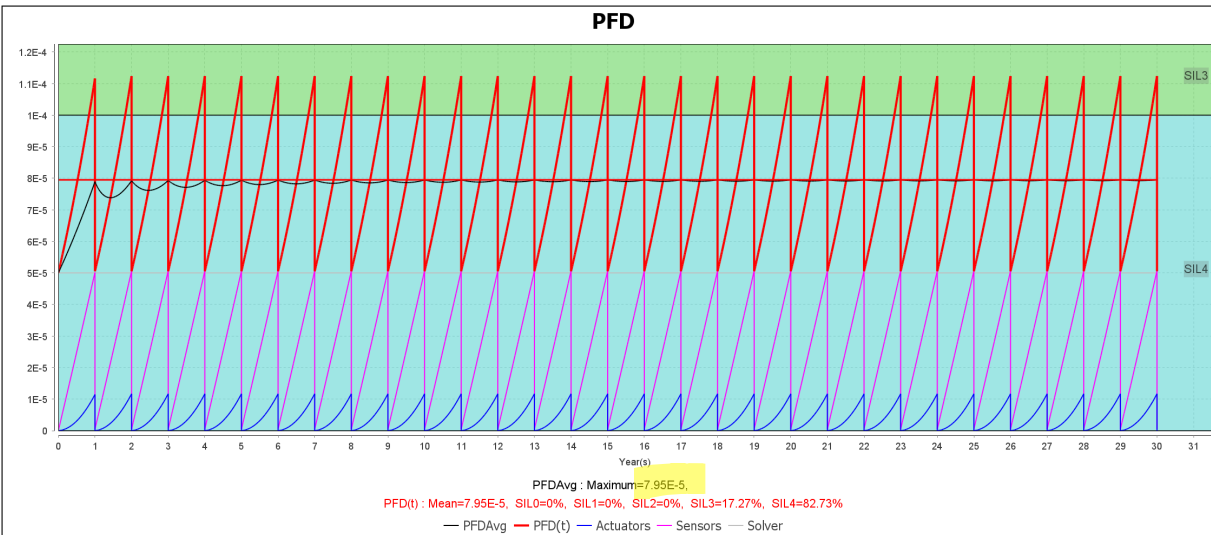
Fil: 3-SIL_TTK2_seminar5_med_CCF_sensor_og_ventiler.sil



Legger til også fellesfeil (CCF) for ventilene. Beta satt til 10%.

Uten fellesfeil ventiler (CCF)

Med fellesfeil ventiler (CCF)

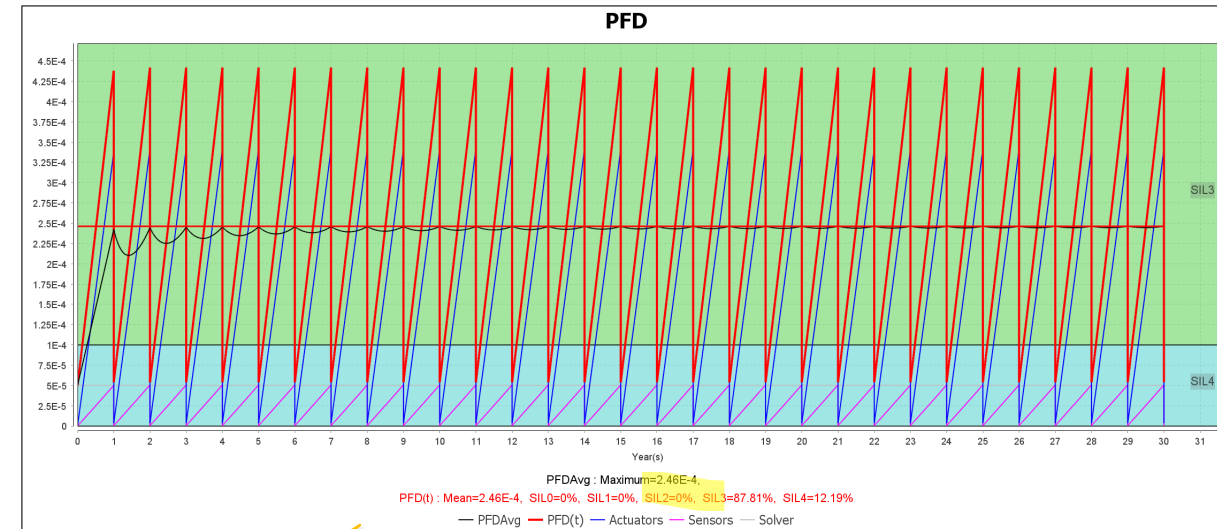


Actuator architecture

Number of channels configured in

☐ Take into account Common Cause Failures

Beta inter-channels (du) % ☐ Beta IEC61508-6 D ...



Her får CCF noe mer å si. Hvorfor?

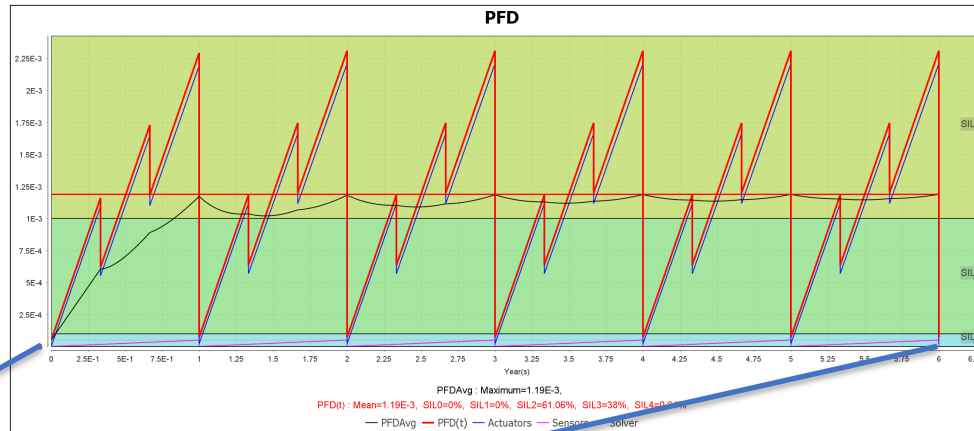
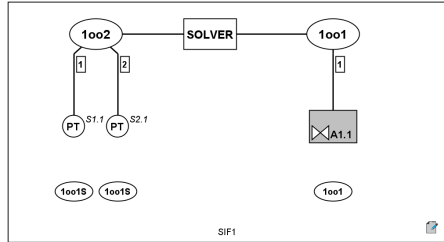
Actuator architecture

Number of channels configured in

☒ Take into account Common Cause Failures

Beta inter-channels (du) % ☐ Beta IEC61508-6 D ...

SIF med partial stroke testing ventiler



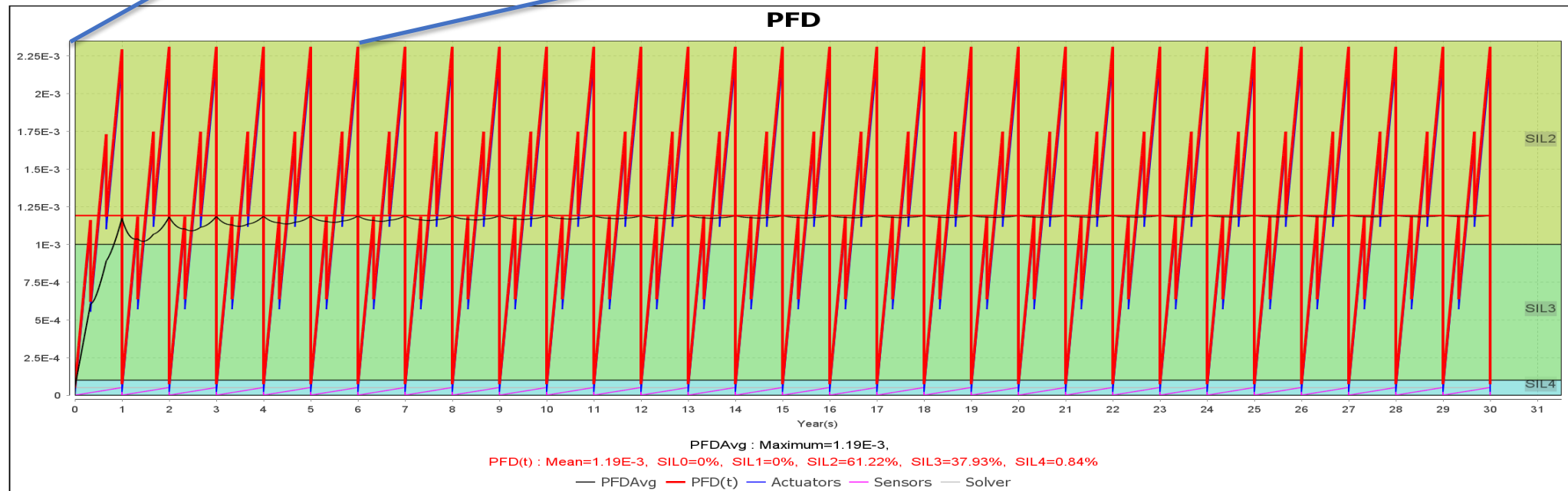
Fil: 4-SIL_TTK2_seminar5_PartialTest.sil

☒ Partial tests
☒ Component available during test (X)

Test duration (π): Hour(s)

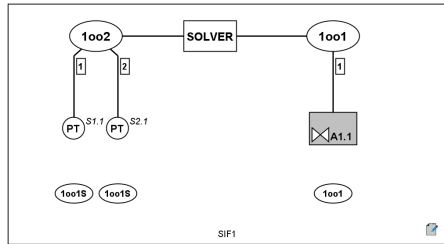
Percentage of detected faults: %

Number of tests:



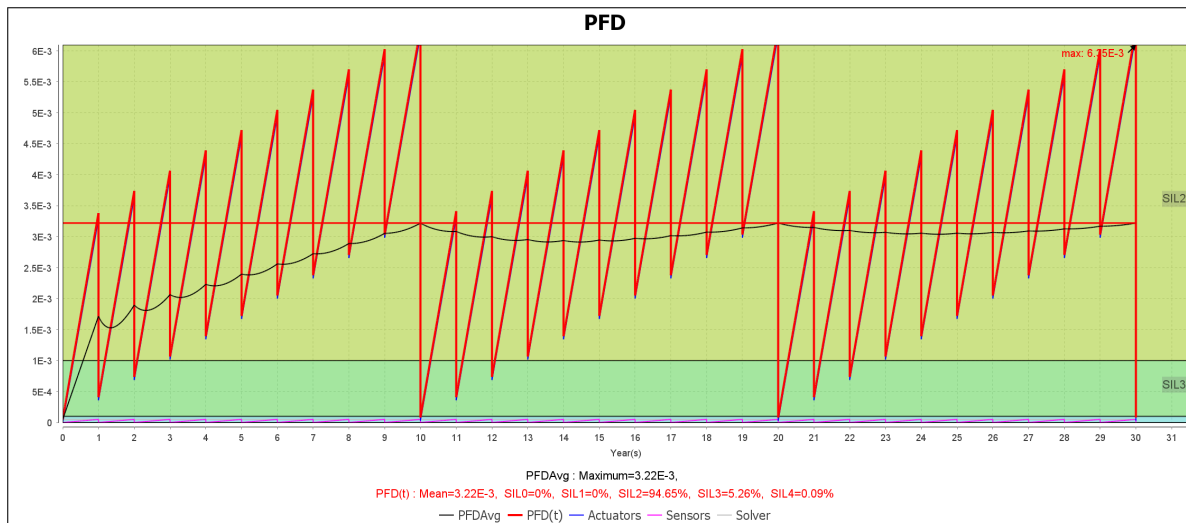
SIF med justert proof test coverage for ventil

Fil: 5-SIL_TTK2_seminar5_PTC.sil



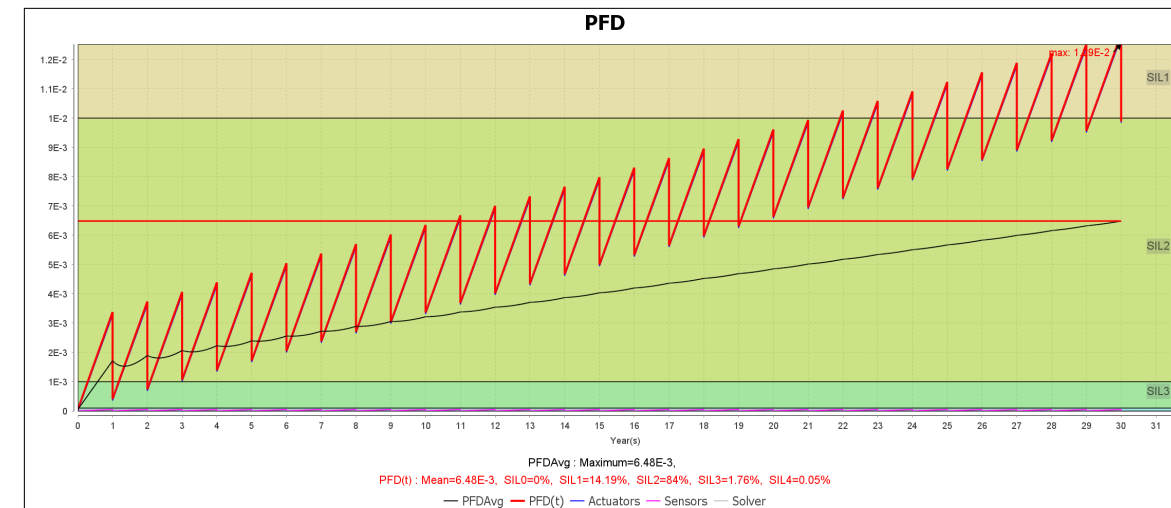
Advanced parameters	
☐ Component available during test (X)	
☒ Safe fault repairs do not impact the safety function	
Lambda during test (λ^*):	0
Test duration (π):	N/A
Test efficiency rate (σ):	1
Set-up error after test (ω_1):	0.00
Set-up error after repair (ω_2):	0.01
Proof test coverage:	90.0
Lifetime of the component:	10

Proof test hvert 10 år



Advanced parameters	
☐ Component available during test (X)	
☒ Safe fault repairs do not impact the safety function	
Lambda during test (λ^*):	0
Test duration (π):	N/A
Test efficiency rate (σ):	1
Set-up error after test (ω_1):	0.00
Set-up error after repair (ω_2):	0.01
Proof test coverage:	90.0
Lifetime of the component:	30

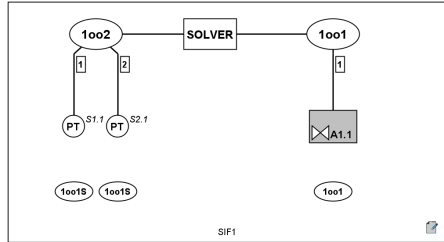
Ingen proof test i løpet av livsløpet (30 år)



TTK2

SIL med Proof test coverage (ventil) på 90%

Fil:6-SIL_TTK2_seminar5_PartialTest_and_PTC.sil



Med også partial stroke testing av ventil

☒ Partial tests

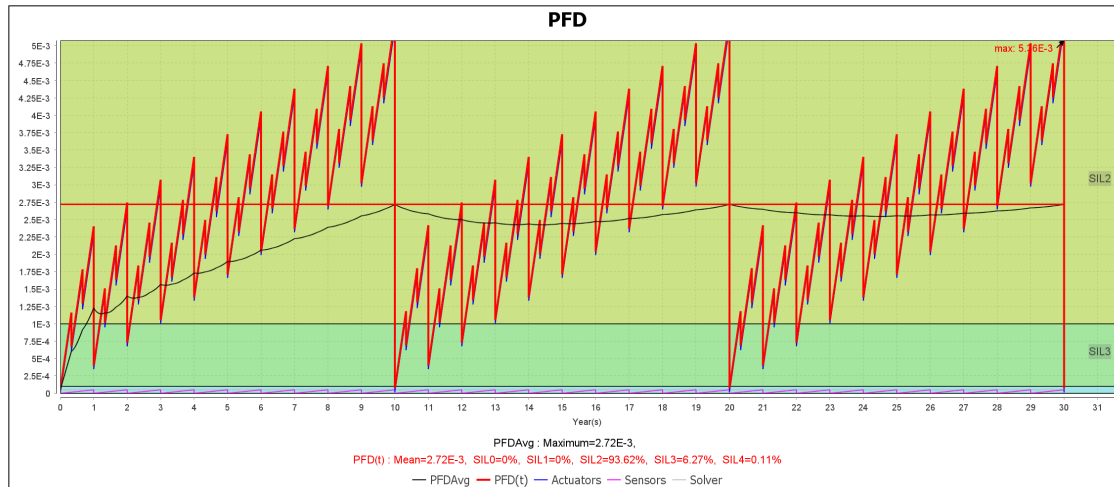
☒ Component available during test (X)

Test duration (π): Hour(s)

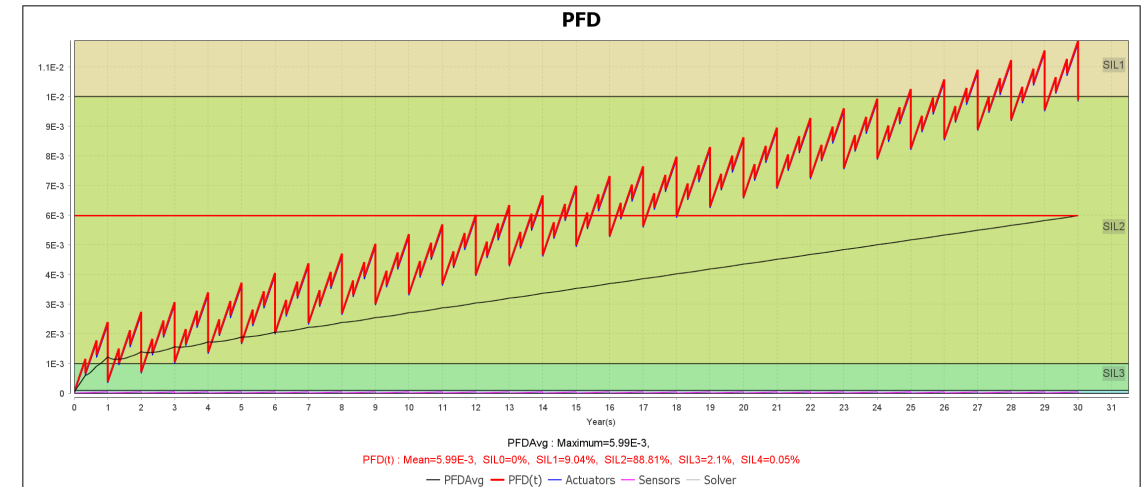
Percentage of detected faults: %

Number of tests:

Proof test hvert 10 år



Ingen proof test i løpet av livsløpet (30 år)



TTK2

SIF pålitelighet i drift: SIL oppfølging

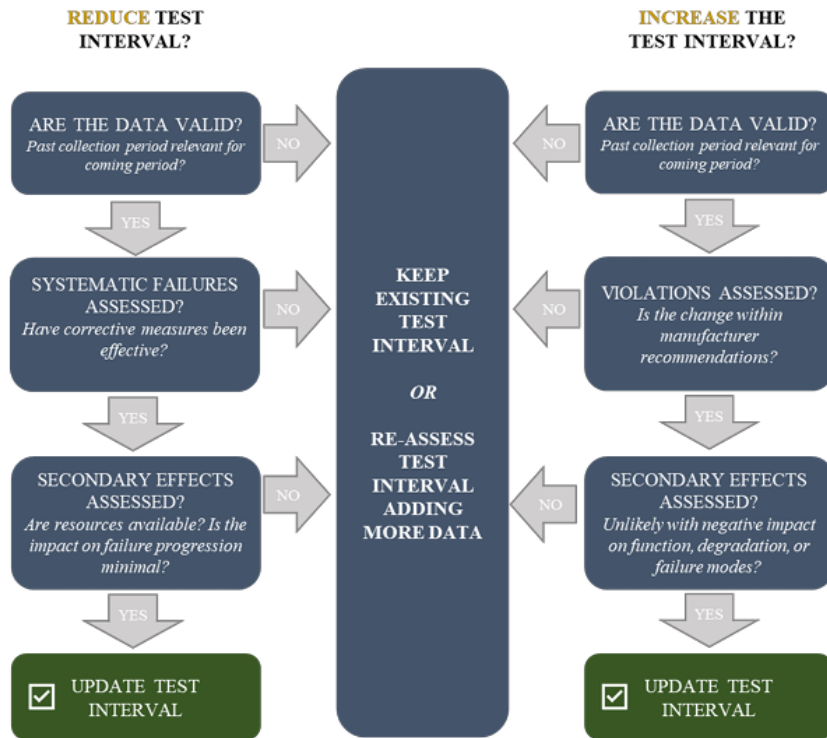
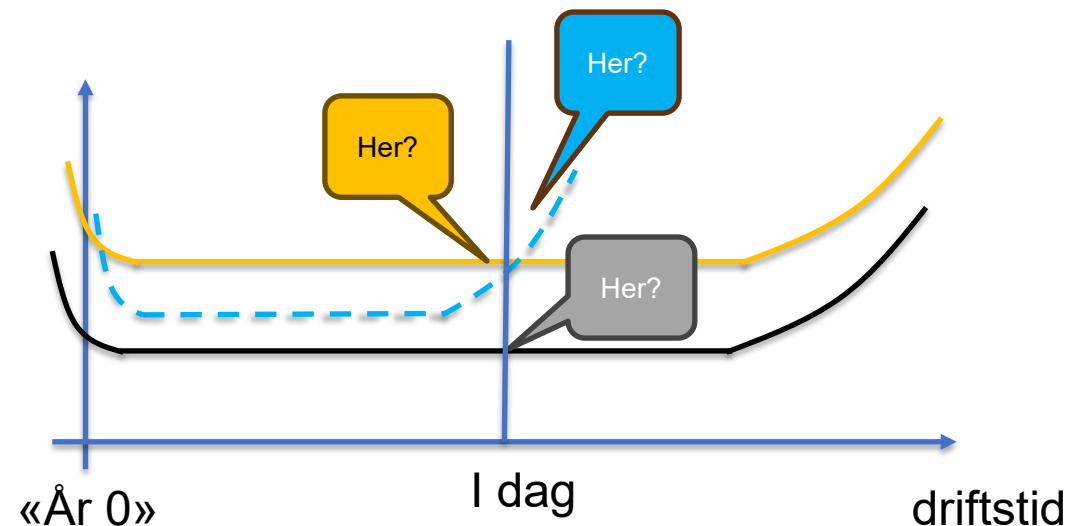


Figure 6: Flow chart for qualitative assessment prior to test interval update.

<https://pds-forum.com/wp-content/uploads/2023/03/APOS-Guideline-for-follow-up-of-SIS-in-operation-phase-signed.pdf>

- Hva er den erfarte DU feilraten for en komponent i drift?



TTK2

SIF pålitelighet i drift: SIL oppfølging



- Hva er den **erfarte** DU feilraten for en komponent i drift?

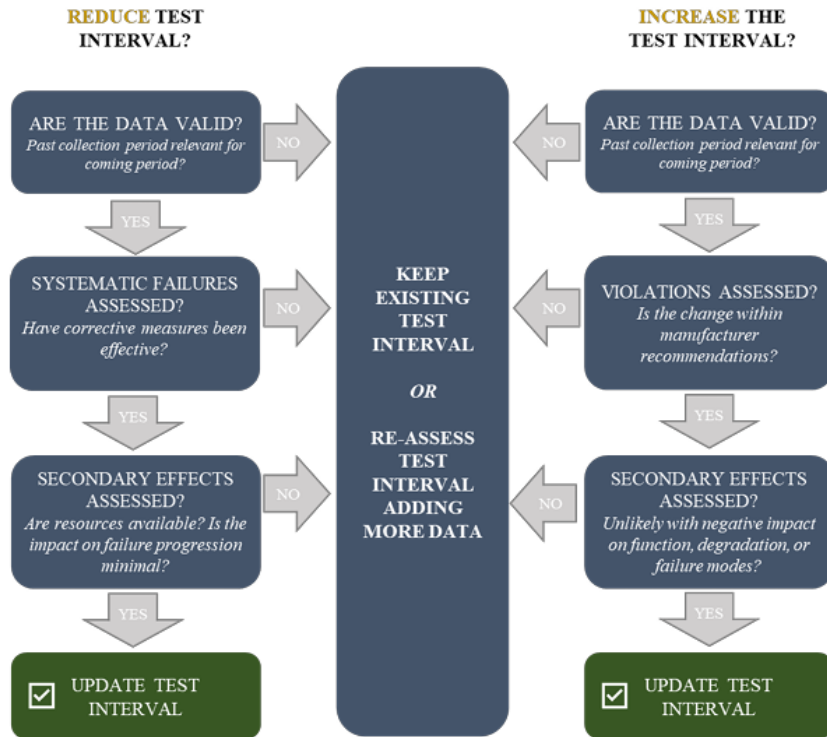
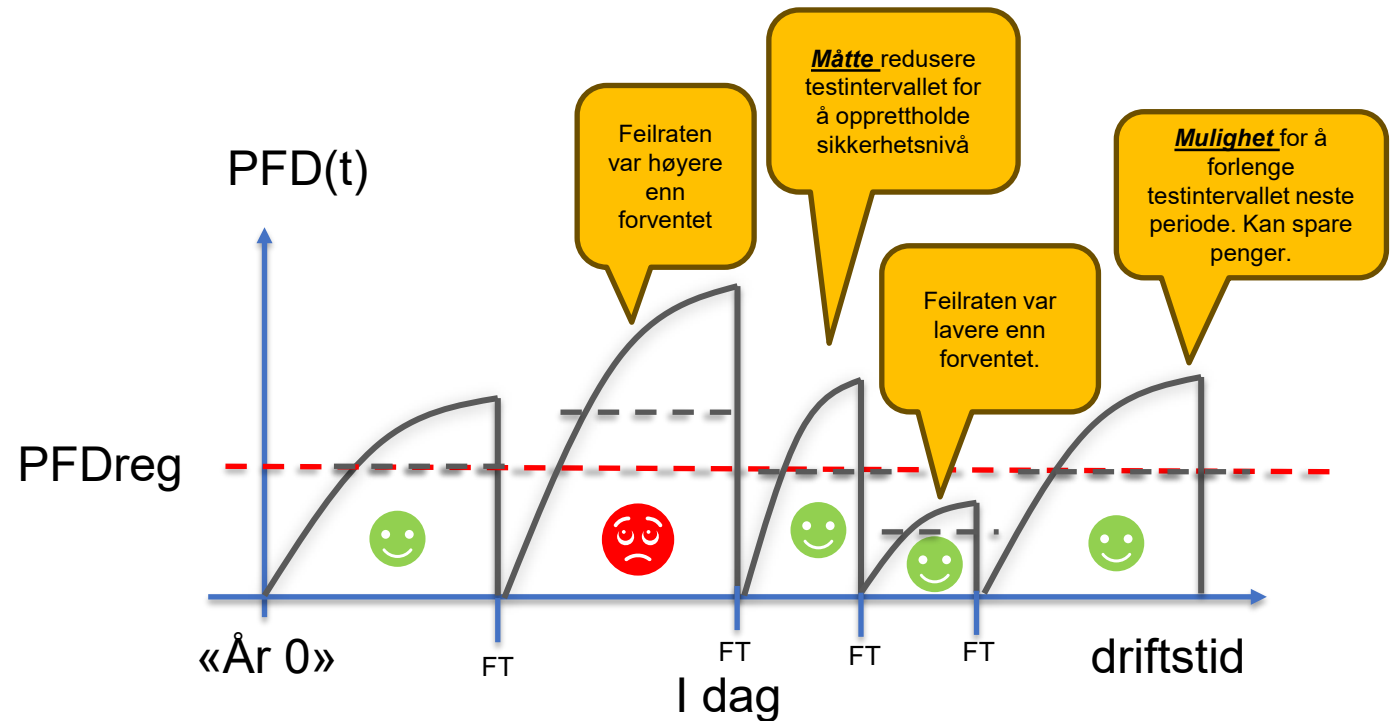


Figure 6: Flow chart for qualitative assessment prior to test interval update.

<https://pds-forum.com/wp-content/uploads/2023/03/APOS-Guideline-for-follow-up-of-SIS-in-operation-phase-signed.pdf>

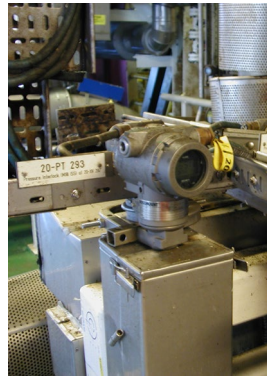
Illustrasjon med noe mer «jo-jo» bilde enn virkeligheten



TTK2

Prosess for å samle inn data

Oppdage feil



Utstyret kommer inn med alarm på display i kontrollrom



Feil avdekkes under funksjonstest

Feil avdekkes tilfeldig ifbm annet arbeid

Registrere feil

Notification: 42673477 M2 Gassdetektor defekt..

Notific. Status: NOCO ORAS

Order: 22202603

Notification Long text Documents Location data Dates Activities

Reference object

Functional loc. 1175-700PR351A-80 Gas detector point IR chemical Ind plant

Equipment 10405753 DETECTOR,GAS,128-810867.2,GD10P,5IMRAD

Assembly

Responsibilities

Planner group POM / 1175 Plattform D&V

Main WorkCtr POMAUT / 1175 D&V Automasjon

Person Responsi

Reported by

Effect on the system

Failure Impact B Dead (CF)

Start/End Dates

Required End 10.10.2011 Priority High <= 5 days

Item

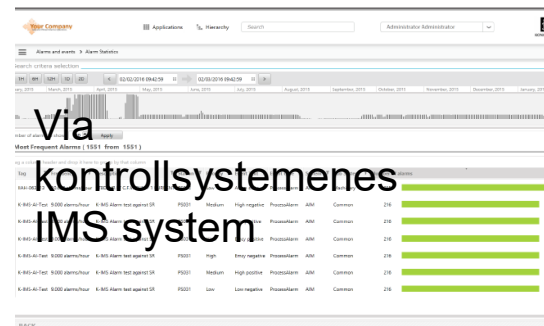
Detect Mthd P00M-005 2

Failure Mode P00M-155 BRD

Fail Mech

ISO Scheduled activities - ISO Functional testing

ISO Fire and gas detectors - CST Breakdown



Klassifisere feil

- Feilårsak
- Deteksjonsmetode
- Delvis via registrering og/eller etterarbeid

Lage statistikk

- Hvor mange DU feil for ulike utstyrsgupper
- Driftsperiode, eventuelt antall tester gjennomført i periode

Eksempel på «dump» fra vedlikeholdssystem

SAP generert										Manuelt arbeid		
Søk IW69	Priority	System	FunctLocation	Description	Created on	Notification	Failure impact	Obs method	Klassifisering	Kommentar (hentet fra SAP)	Kvalitet registrering	
70MC*	U	70	11xx-70MCP300A-7H07	Skifte plastnippel	23.05.2007	406475xx	U (Unwell)	080 (periodisk aktivitet)	S	Feil oppdaget på FV:	Ok.	
70GP*	H	70	11xx-70GPR160B-8308	Gasspunkt-detektor gikk i feil	20.03.2007	406272xx	D (Dead)	085 (kontinuerlig overvåkning)	DD	Detektoren viste -8% LEL. Skiftet.	Ok.	
	H	70	11xx-70GPQ330A-6664	Gasspunkt-detektor går i feil	24.06.2007	406563xx	D (Dead)	085 (kontinuerlig overvåkning)	DD	Gasspunkt-detektor går i feil, drifter viser -20%LEL og ligger inne med IO feil.	Ok	
	M	70	11xx-70GPQ112C-9314	Punkt-detektor failer - luftinntak sør.	24.04.2007	406xx729	S (Seriously ill)	085 (kontinuerlig overvåkning)	DD	(Ser ut til å dekke flere hendelser)	1) I prinsippet bør det skrives en M2 per DD hendelse, 2) Skal det å gå i feil kodes som S (seriously ill) eller D (dead)?	
	M	70	11xx-70GPP300A-8D01	Kalibrer/reparker gassdetektor	20.05.2007	406xx577	S (Seriously ill)	080 (Periodisk aktivitet)	DU	Kommer ikke med HH-alarm ved 50% LEL test gass	Muligens burde koden her vært D (Dead)?	
	M	70	11xx-70GPP300A-8E12	Kalibrer/reparker gassdetektor	20.05.2007	40644xx8	S (Seriously ill)	080 (Periodisk aktivitet)	DU	Kommer ikke med HH-alarm ved 50% LEL test gass	Muligens burde koden her vært Dead?	
	H	70	11xx-70GPP300A-8D09	Kalibrer/reparker gassdetektor	20.05.2007	40xx4659	D (Dead)	080 (periodisk aktivitet)	DU	Detektoren reagerer ikke i det hele tatt når den blir tilført testgass.	Ok	
70GS*			Ingen registrert									
70GH*	M	70	11xx-70GHQ222C-6639	Skifte H2 sensor	20.02.2007	40xx9145	S (Seriously ill)	085 (kontinuerlig overvåkning)	DD	Ustabil over lengre tid	Ingen info om årsak. Muligens burde koden her vært Dead?	
	M	70	11xx-70GHP133D-7Q39	Ustabil H2 detektor	18.03.2007	40xx6415	S (Seriously ill)	085 (kontinuerlig overvåkning)	DD	Detektoren er ustabil og kommer opp med alarm. Pendler fra 3 til -3 Lel.	Muligens burde koden her vært Dead?	
	M	70	11xx-70GHP133D-7Q39	Detektor viser feil	14.04.2007	40633xx79	S (Seriously ill)	085 (kontinuerlig overvåkning)	DD	Detektoren ligger inne med 14% LEL selv om det ikke er H2 i rommet.	Muligens burde koden her vært Dead?	
70GO*			Ingen registrert									
70GL*	H	70	11xx-70GLP100A-7Q44	Linjedetektor feiler.	09.02.2007	406xx082	Mangler	000 hva egen instrumentering	DD	Prøvde først det tradisjonelle med rengjøring og finjustering. Ok signal på ca. 0.8. Likevel fortsatte den å komme inn med sporadiske feil, så da byttet vi både GRP&GLP.	Gamle/mangelfulle feilkoder. Men dette var like etter overgangen til de nye kodene.	
	U	70	11xx-70GRP300A-8F01	Linjedetektor i Lav alarm pga snø	22.02.2007	xx619589						
	U	70	11xx-70GRP300A-8F06	Sjekk detektor, kommer med feil.	03.06.2007	4xx48268	U (Unwell)	085 (kontinuerlig overvåkning)	DD	Detektor feiler hele med utstyr feil	Skulle kode vært Dead?	

Notification42673477M2Gassdetektor defekt..
Notfic. StatusNOCO ORAS
Order22202603
NotificationLong textDocumentsLocation data
Reference object
Functional loc.1175-70GPR351A-80...Gas detector p
Equipment10405753DETECTOR,GA
Assembly
Responsibilities
Planner groupPOM / 1175Plattform D&V
Main WorkCtrPOMAUT / 1175D&V Automasjon
Person Responsi
Reported byI. KYVANDENotif.date
Effect on the system
Failure ImpactD Dead (CrF)
Start/End Dates
Required End10.10.2011
PriorityHigh <= 5 days
Breakdown
Item
Detect MthdPMDM-0052ISO Scheduled activities - ISO Functional testing
Failure ModePMDM-155BRDISO Fire and gas detectors - CST Breakdown
Fail Mech

Eksport fra SAP (vedlikeholdssystem) til excel – pluss ekstra kolonner for klassifisering (manuelt arbeid)

Eksport fra SAP (vedlikeholdssystem) til excel – pluss ekstra kolonner for klassifisering (manuelt arbeid)

Presentasjon av Bjørnar Berg, Statoil lastet ned fra:
<https://esra.no/kursdokumentasjon/sil-fra-design-til-drift/>

Utklipp fra årlig gjennomgang

A.1 A10 26 Blow down valve (33 stk.)

Class	No of funct loc.	No of tests	No of failures	Target
26 Blow down valve	33	31	1	3

To nye LPP ventiler er ikke driftsatt eller testet enda.

Target verdi er feil, GL0114 sier 0,5% tillatt feil, A10 benytter 10%

Notification	Description	Functional Loc.	Fail mode	Det meth	Failure Imp	Created on	Klass
42777939	23ESV1023 hakker veldig og aktuator er i	1175-23ESV1021	OTH	1	S	29.01.2012	SU
42801432	Ventil går rykkvis.	1175-23ESV1021	OTH	2	S	24.02.2012	NA
42801594	Ventil går rykkvis.	1175-23ESV1021	OTH	2	S	24.02.2012	NA
43101945	Defekt hydraulikkslange	1175-45ESV1009	BRD	1	S	03.11.2012	SD
43114313	Korrosjon på hovedbolter og drenstusser	1175-13ESV2506	OTH	3	U	08.11.2012	SU
42893696	Alarm ved test av blowdown ventil	1175-20ESV1412	DOP	2	U	02.06.2012	DU
42972029	Utvendig korrosjon på aktuator 43ESV4102	1175-43ESV4102	STD	7	U	26.08.2012	NA

Registrerte feil (7 notifikasjoner)

- 1 SD feil på slitte hydraulikkslanger
- 2 SU rykkete gange (men innenfor krav) samt rust.
- 1 DU, ventil bruker for lang tid på å åpne, OK etter justering av flow controller
- 4 NA feil, forbedringsforslag eller uklare notifikasjoner med uidentifiserbare ukritiske feil

Vurdering:

- Kun en M2 på slitte hydraulikk-slanger, dette er en vesentlig nedgang fra foregående år.
- Relativt få feil i forhold til tidligere år.
- Ingen feil på grensebrytere eller solenoid ventiler

Det gjøres en kvalitetssikring av resultatene sammen med relevante fag-/systemansvarlige. Videre aksjoner avtales med disse.

18



Presentasjon av Bjørnar Berg, Statoil lastet ned fra:
<https://esra.no/kursdokumentasjon/sil-fra-design-til-drift/>

Samlet statistikk fra 2006 til i dag

- Vi har også tilsvarende oversikt med ytterligere klassifisering i sikre/farlige og detekterte/udetekterte feil for alle SIL funksjoner

KRISTIN												
System	Sikkerhetsfunksjon	SIL	Ant tag	Ant test	DU feil	SIL krav ant.	DD feil	SD feil	SU	Spurious	Ikke	N
	Isolering av et rom i skroget (butterfly ventiler)	2	291	291	0	2,91	0	4	2	0	1	
79	26 - Åpne trykkavlastningsventil	2	180	175	0	1,75	0	15	1	0	7	
	Åpne ESV nedstrøms høytrykksfaldel væskeutskiller (HP KO drum)	2	6	6	0	0,06	0	0	0	0	0	
	LAHH (NAS signal) i væskeutskiller (KO drum)	2	6	6	0	0,06	0	2	0	0	0	
	24 - ESD riser valve test	2	107	75	2	1,33	2	16	14	0	32	
	49 - NAS seksjonalisering ved å benytte en nødavstengningsventil	2	307	458	1	4,59	0	46	7	1	20	
	9 - Manuell initiering av nødavstengningssystemet (79ES)	2	334	319	0	3,27	0	0	0	0	3	
	Elektrisk isolering (singel gass i prosess område)	2	70	70	0	0,7	0	0	0	0	0	
	ESD logikk	2	18	27	2	0,12	3	1	0	0	2	
Sum 2006 2007 2008 2009 2010 2011 2012 Sheet2 Sheet1												

24



TTK2

Oppdatering av feilraten i drift

Failure rate update

Annual

Input failure rate [per hour] Mandatory (E.g. 1e-6)

Conservative estimate (CE) [per hour] Optional: If the input failure rate is based on operational experience, the conservative estimate for the experienced period can be used.

First year of observation Enter the first year of observation and the table below is updated. (E.g. 2020)

	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
DU failures within observation period, x										
Components within equipment group, n										
Aggregated time in operation - per year, T [hours]	0	0	0	0	0	0	0	0	0	0
Aggregated number of DU failures, X	0	0	0	0	0	0	0	0	0	0
Aggregated time in operation, ΣT [hours]	0.0E+00	0.0E+00	0.0E+00	0.0E+00	0.0E+00	0.0E+00	0.0E+00	0.0E+00	0.0E+00	0.0E+00
Updated Bayesian failure rate λ_{DU} [per hour]										
Sufficient operational experience achieved to update test interval?										

NB: Vi antar 2x

Legend: Failure rate (blue line), Lower bound (green line), Upper bound (red line), Operational failure rate (red line).

NB: Vi antar 2x konservativ feilrate

$$\beta = \frac{\lambda_{DU,init}}{(\lambda_{DU,cons} - \lambda_{DU,init})^2}$$

$$\alpha = \beta \cdot \lambda_{DU,init}$$

Failure rate update

Annual

Input failure rate [per hour] Mandatory: (Eg. 1e-6)

Conservative estimate (CE) [per hour] Optional: If the input failure rate is based on one or more years of data, the experienced period can be extended.

First year of observation Enter the first year of observation and the table below is updated. (Eg. 2014)

Velg start år fra det året data legges inn.

	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
DU failures within observation period	4	0	2							
Components within equipment group, n	100	100	100							
Aggregated time in operation - per year, T [hours]	876000	876000	876000	0	0	0	0	0	0	0
Aggregated number of DU failures, Σx	4	4	6	6	6	6	6	6	6	6
Aggregated time in operation, ΣT [hours]	8.8E+05	1.8E+06	2.6E+06	2.6E+06	2.6E+06	2.6E+06	2.6E+06	2.6E+06	2.6E+06	2.6E+06
Updated Bayesian failure rate λ_{DU} [per hour]	2.7E-06	1.8E-06	1.9E-06	1.9E-06	1.9E-06	1.9E-06	1.9E-06	1.9E-06	1.9E-06	1.9E-06
Sufficient operational experience achieved to update test interval?	NO	YES								

Hvis man legger inn feildata for flere år, bruker

Velg start år fra det året data legges inn.

Hvis man legger inn feildata for flere år, bruker man den feilraten som ble regnet ut for det året der perioden slutter

<https://mobilitet.sintef.no/pds/>

Gruppeoppgave

1. Last ned SIL module i Grif-verktøy fra link på TTK2 sin teamsside (se eget innlegg/post)
2. Forklar betydningen av følgende parametere:
 - a) DU feil og DU feilrate. Hvorfor den er viktigst for PFD
 - b) Fellesfeil (CCF) og hva beta representerer
 - c) Funksjonstest vs proof test (og proof test coverage)
 - d) Partial test og partial test coverage
 - e) Average vs tidsavhengig PFD(t)
3. Gå igjennom alle de samme scenariene som i forelesningen, men endre votering til 2003 for sensorene. Noter ned resultater tilsvarende som gjort i forelesningen.
4. Bruk fila SIL_TTK2_seminar5_med_CCF_sensorer.sil. Anta at du har 50 (solenoid) ventiler og at det i perioden 2021-2023 har vært hhv erfart 2,0,1 feil. Bruk DU feilrate (init) som vist, og
 - a) Bruk PDS tool <https://mobilitet.sintef.no/pds/> til å regne ut ny erfart feilrate i 2023
 - b) Oppdater med ny DU feilrate (Kryss av for «developed» og legg inn ny DU feilrate)
 - c) Regn ut ny PFD for SIFen og sammenlign med resultatet som ble regnet ut uten driftsefaringPS: Trenger ikke å ta med partial stroke testing og proof test coverage i oppdateringen, kun den med fellesfeil på sensorene (fil nummer 2).
5. Reflekter over kilder til usikkerhet i pålitelighetsanalysene: Hvilke type data kan være usikre og hvorfor?

Med $DC=0$, er
 $\lambda_{DU,init}=25\% * \lambda=3.75E-7/time$ (som init).
 $\lambda_{DU,cons}=2 * \lambda_{DU}$

Instrument parameters	
☒ Factorized	☐ Developed
Lambda (λ):	1.5E-6 h ⁻¹
LambdaD/Lambda (λd/λ):	25.0 %
DCd:	0.0 %
DCs:	100.0 %
SFF: 75 %	
MTTR: N/A	
Failure due to test (y): 0	

Instrument parameters	
Lambda DU (λ DU):	3.75E-7
Lambda DD (λ DD):	0
Lambda SU (λ SU):	0
Lambda SD (λ SD):	1.125E-6