



SIL i Boring

-Krav og oppfølging



Tor Onshus
Onshus teknisk sikkerhet



92 60 74 60



Tor.Onshus@ntnu.no



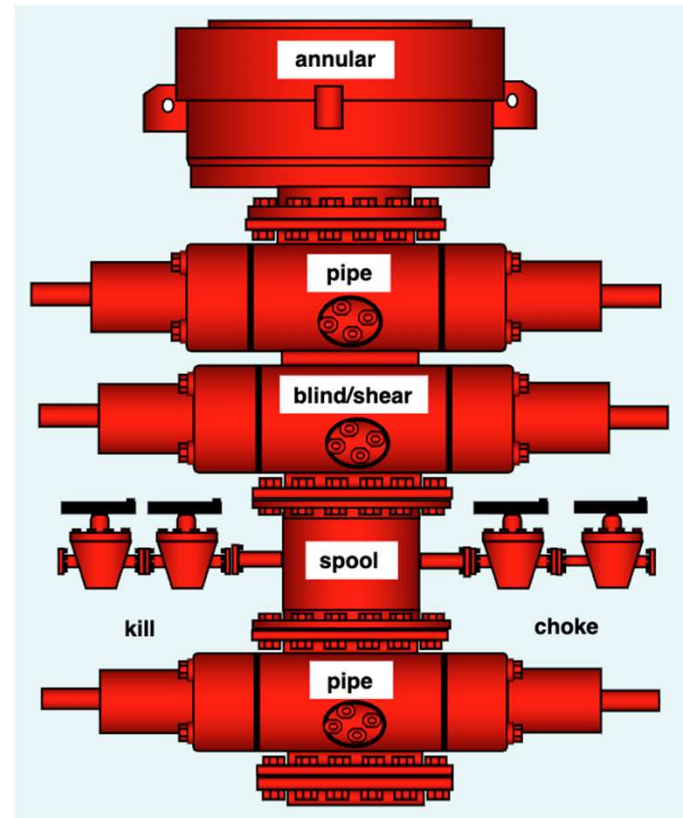
folk.ntnu.no/onshus





Introduksjon til SIL for BOP

- Krav
- Hva er SIL
- Dokumentasjon
- Oppfølging i drift
- PFD beregninger
- Oppfølging av ytelse





Bakgrunn

- Havtil krever i Styringsforskriften §5 at:
 - krav til ytelse av barrierene skal gis
 - det skal være kjent om barrierene er svekket
 - det skal kompensere for svekkede barrierer
 - barrierens funksjon skal alltid ivaretas
 - alt personell skal være kjent med barrierene
- Gjelder også for gamle installasjoner



Hvorfor SIL (veiledning til §5 i SF)

- Med ytelse som nevnt i fjerde ledd, menes verifiserbare krav til blant annet kapasitet, pålitelighet, tilgjengelighet, effektivitet, evne til å motstå laster, integritet og robusthet.
- For sikkerhetssystemer bør standarder som IEC 61508, IEC 61511, IEC 62061 og ISO 13849 legges til grunn. I tillegg bør Offshore Norges retningslinje nr. 070 legges til grunn for petroleumsvirksomheten til havs.



Krav til Shear RAM i 070

Funksjonskrav:

- Kutte det som er i borehullet og isolere brønn

IEC 61508
IEC 61511

Ytelseskrav:

- Funksjonen skal oppfylle
 - SIL 2 (Safety Integrity Level)
 - $PFD < 0.01$ (Probability of Failure of Demand)

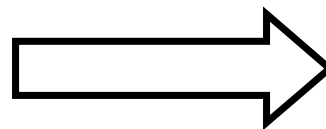
Også krav til

- Sekvensiell nedstengning og frakopling
- RAM låsing

Tabell 7.5.4
og
Appendiks 14
i 070

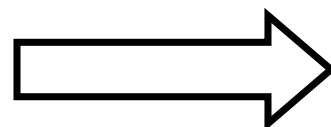


IEC 61508



For de som
utvikler
komponenter til
SIL funksjoner

IEC 61511



For de som bruker
komponenter
utviklet i henhold
til IEC 61508



IEC 61508/11

-konsekvenser av SIL

- Arbeidsmetodikk
 - kvalitetssikring
 - tiltak mot systematiske feil
- Sviktsannsynlighet (PFD)
 - Testing i drift
- Krav til systemstruktur



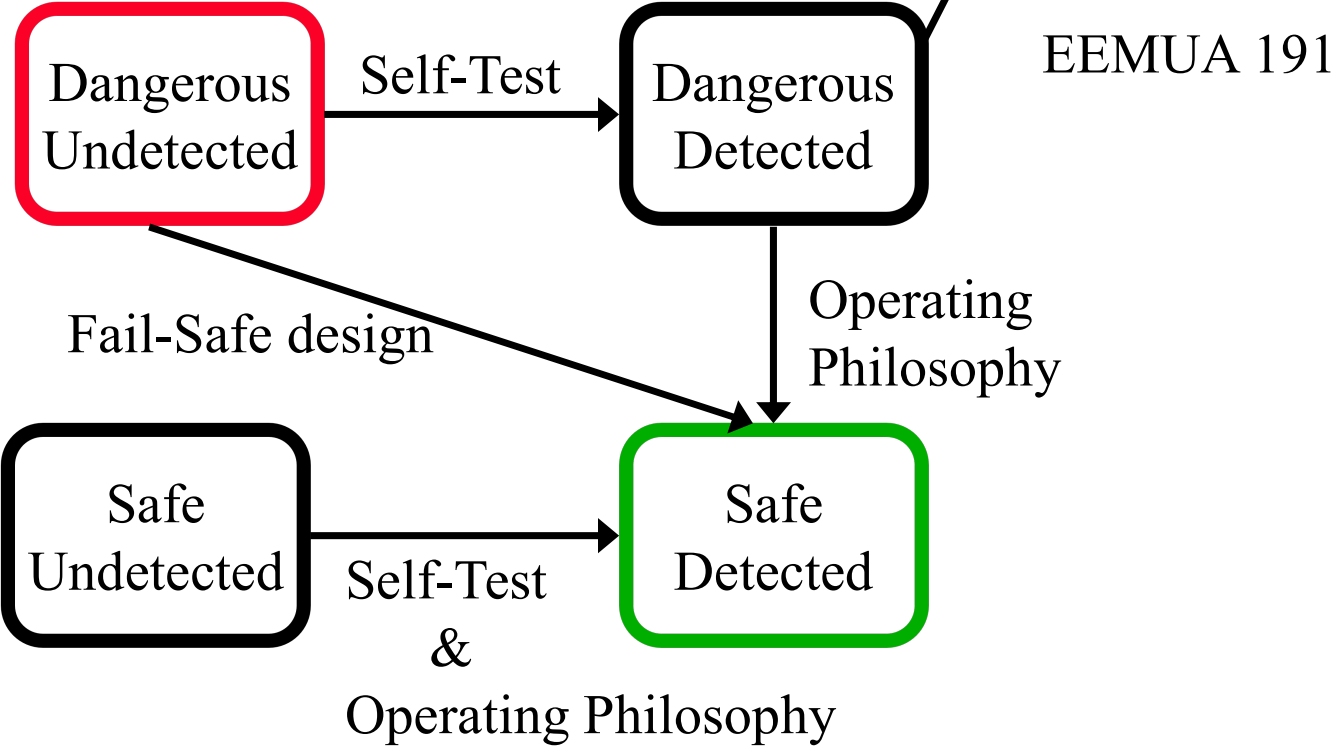
FEILMODI

-hva er effekten av feilen

- Farlig svikt/Feilfunksjon
 - Systemet er ikke i stand til å utføre den operasjonen det får beskjed om
- Trip/Utilsiktet operasjon
 - Systemet utfører en operasjon det ikke har fått beskjed om å utføre
 - Mange utilsiktede nedstengninger virker negativt på sikkerheten



Feilmodi i IEC 61508



Bare feil som påvirker funksjonen skal være med



SIL-Safety Integrity Level
For en funksjon

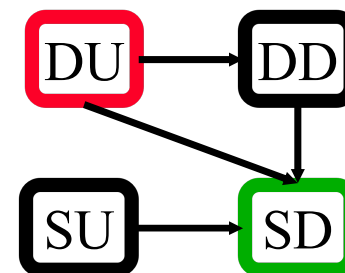
SIL	PFD	Svikt sjeldnere enn
1	$0.01 \leq \text{PFD} < 0.1$	1/10
2	$0.001 \leq \text{PFD} < 0.01$	1/100
3	$0.0001 \leq \text{PFD} < 0.001$	1/1000
4	$0.00001 \leq \text{PFD} < 0.0001$	1/10 000



PFD-Probability of Failure on Demand

For en komponent

$$\text{PFD} = \lambda_{\text{DU}} \cdot \frac{\tau}{2}$$



- τ - tid mellom funksjonsprøving [timer]
 - 1 år = 8760 timer
- λ_{DU} -farlig udetekterte feil [feil/time]

FIT = 10^{-9} feil/time



Dokumentasjon

Safety Requirement Specification (SRS)

- Operatørens krav

SIL Compliance

- Fra leverandøren
- Viser at kravene i SRS er oppfylt
- Operatøren oppdaterer (årlig) basert på driftserfaring



Hva er SRS?

- Spesifikasjon som inneholder alle krav til funksjonen som skal utføres av det sikkerhetsrelaterte systemet.
 - funksjonskrav
 - ytelseskra
- GL 070 Appendiks E (IEC 61511, kapittel 10.3)



Safety Requirement Specification

- Beskrivelse av alle sikkerhetsfunksjonene og kravene til disse (SIL og PFD)
- Definisjon av sikker prosessstilstand for hver funksjon
- Krav til testintervall
- Krav til responstid



SIL Compliance

- Dokumentere at komponentene er kvalifisert for bruk i SIL funksjoner
 - Sertifikat, Safety Manual, Safety Analysis Report
 - Feildata basert på lignende bruk
- Vise at funksjonene oppfyller kravene i SRS
 - Pålitelighetsblokkdiagram (RBD-Reliability Block Diagram)
 - Beregning av PFD



Oppfølging i drift

Sørge for at vi opprettholder den ytelsen vi trenger



Testing

-for å opprettholde PFD

- Teste funksjonen med gitt frekvens
 - Omfang og kvalitet som antatt i beregninger
 - Finner vi alle DU feil?
- Følge opp hendelser i drift
 - behov for funksjonen
 - svikt av funksjon eller deler av funksjon
- Kontroll med utkoblinger



Rapportering fra drift/test

- Alltid rapportere status slik den ble funnet
 - Hva ville skjedd hvis vi trengte den nå?
- Riktig klassifisering av feil
 - Alle kritiske feil er ikke DU feil
- Rapporter på rett tag
- Bruke fritekst for å beskrive feilen



PFD beregninger

Sannsynlighet for at funksjonen svikter
når vi har bruk for den



Beregning av en funksjon

- Definer funksjonen
- Definer sikker tilstand
- Identifiser funksjonens fysiske elementer og evt. hjelpesystemer
- Bruke feildata basert på erfaring fra lignende bruk (IEC 61511, 11.9.3)



Driller
Tool pusher

Funksjonen



Komponent	Feilrate	Testintervall [uker]	PFD
Trykknapp	1,10E-07	4	3,70E-05
Trykknapp	1,10E-07	4	3,70E-05
PLS	5,60E-07	2	9,41E-05
Solenoide	3,00E-07	2	5,04E-05
Shear RAM	3,40E-06	2	5,71E-04
			7,90E-04
	PFD oppnådd		0,001
	Krav		0,010

Feildata fra
PDS Data Handbook
2021 utgave

$$PFD = \lambda_{DU} \cdot \frac{\tau}{2}$$



Blind Shear RAM

- Hva må virke
 - Blø av åpne trykk (Solenoider, Pilot, DCV osv.)
 - Tilføre lukketrykk
 - Selve ventilen må virke og kunne kutte det som er i hullet
- Overvåker kontinuerlig at vi har tilstrekkelig hydraulikktrykk
 - HPU ikke del av lukkefunksjonen
- Kuttefunksjonen blir aldri testet
 - Resertifisering, overhaling og vedlikehold sørger for at kvaliteten opprettholdes



Er funksjonene fortsatt bra nok?



Hva må vi gjøre

1. Teste og vedlikeholde
2. Registrere DU feil
3. Oppdatere feilrater basert på erfaring
4. Sjekke at PFD kravet til funksjonen fortsatt er oppfylt



Oppdatere feilrater

Parameter		Beskrivelse
λ_i	per time	Oppdatert feilrate
λ_0	per time	Initiell feilrate
T_i	timer	Totalt antall timer i operasjon
X_i		Totalt antall DU feil

Starter med antatt feilrate fra design

IEC 61511,ch 11.9.3
“..shall be based on field feedback from similar devices used in similar operating environment”

Etter et år i drift

Initiell feilrate	1,00E-06
Tid i operasjon	8760
Antall feil	1
Estimert feilrate	1,98E-06
Økning	98 %

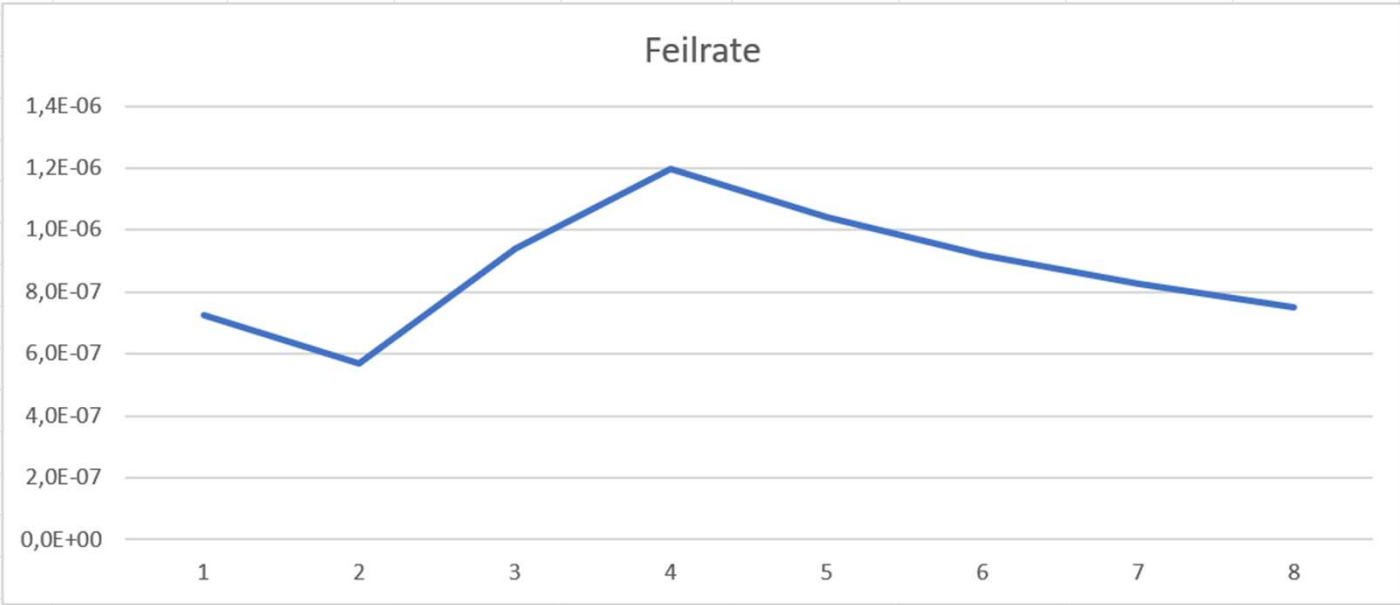
$$\lambda_i = \frac{1 + X_i}{1/\lambda_0 + T_i}$$

Gir fornuftig estimat også når vi ikke har registrert noen feil



Oppdatere feilrater (2)

	Initial est	1,00E-06						
Periode	2016	2017	2018	2019	2020	2021	2022	2023
DU fail	0	0	1	1	0	0	0	0
Op tid	376680	376680	376680	376680	376680	376680	367920	367920
Feilrate	7,3E-07	5,7E-07	9,4E-07	1,2E-06	1,0E-06	9,2E-07	8,3E-07	7,5E-07



42 like
Komponenter
i et år

42×8760
 $=$
376 680 timer



Andre krav

Det er strenge krav også til:

- Utstyret vi bruker
- Til utvikling av applikasjonen
- Til kompetanse for personell



IEC 61508/11

-konsekvenser av SIL

- Arbeidsmetodikk
 - Kvalitetssikring
 - Tiltak mot systematiske feil
- Sviktsannsynlighet (PFD)
 - Testing i drift
- Krav til systemstruktur