High/low demand - Når kan PFD brukes?

Mary Ann Lundteigen (NTNU) og Eva Kvam (Safetec)

Hvem er vi?

Mary Ann Lundteigen

Professor ved institutt for teknisk kybernetikk innenfor instrumenteringssystemer og sikkerhet. Industri- og forskningserfaring fordelt over 30 år med fokus på instrumenterte sikkerhetssystemer.

Kontaktinfo:
https://www.ntnu.no/ansatte/mary.a.lundteigen
(velg Engelsk versjon for mer info)

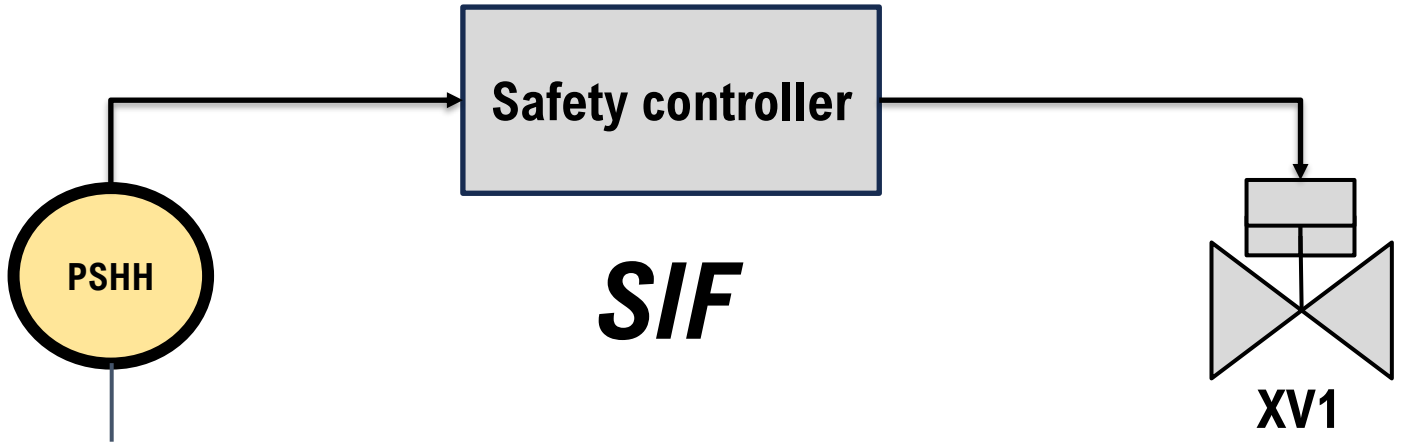
Eva Kvam, Safetec

Principal sikkerhetsrådgiver med 15 års erfaring innen pålitelighetsanalyse, med spesialisering i funksjonell sikkerhet av instrumenterte sikkerhetssystemer (SIS).

Eva.Kvam@safetec.no

Motivasjon

- Av og til eksempler der «tradisjonelle SIFer» i prosessindustrien blir **high demand.**
- Standarden tillater **ulike tilnærminger for pålitelighetsanalyse** – ***uten*** gode føringer
- Ønsket vårt: **Belyse** disse og komme med noen **forslag** til håndtering



Mer enn en demand per år

Tradisjonelle high-demand systemer

- Innebygget i styring (kontinuerlige) eller operert relativt ofte

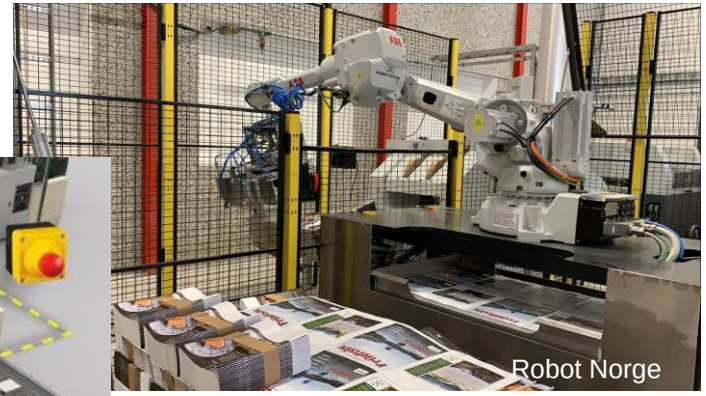
Advanced Emergency Braking System (AEBS)

Signalanlegg jernbane og trikk

Dekket av Maskindirektivet (med IEC 62061 og ISO 13849)

Nødstoppkrets

Utkobling m/dørsensor



Agenda

1. **Part 1**:
   - IEC 61511 om high-demand og refleksjoner (Mary Ann Lundteigen)

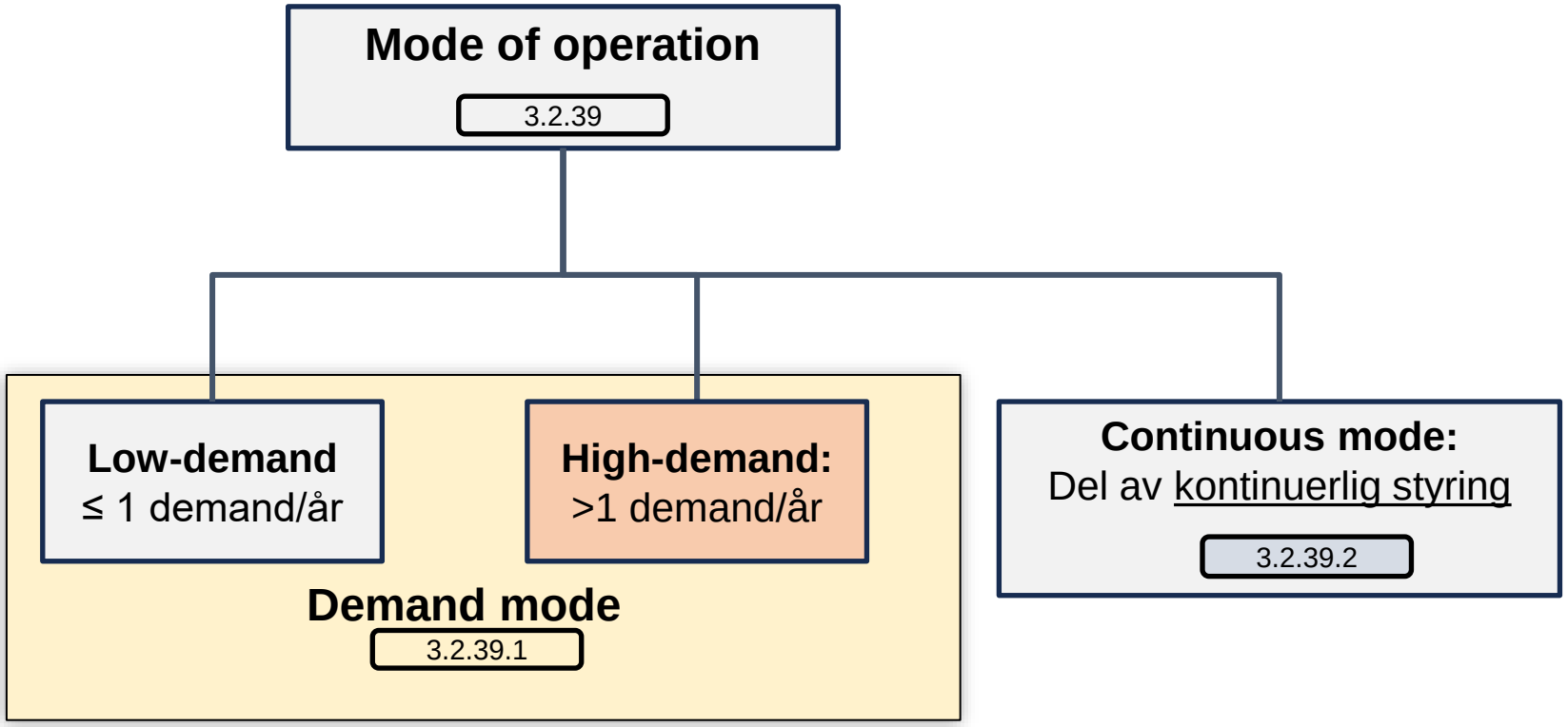
2. **Part 2:**
   - Implikasjoner med et praktisk eksempel (Eva Kvam)

3. **Part 3:**
   - Forslag til kriterier med diskusjon (begge)

1. HVA SIER IEC 61511 OM HIGH DEMAND

High-demand er tydelig definert

Altså: SIF med **mer enn 1 demand** per år OG **ikke** del av **kontinuerlig styring**.



Noen forskjeller for arkitekturkrav (redundans)

Kan få strengere krav til feiltoleranse.

Tre valgmuligheter:

1. IEC 61511 sin egen tabell + bruk av feilrate med 70% konfidens
2. IEC 61508 rute 1H m/ noen restriksjoner om klassifisering av DD feil (og implikasjon for SFF)
3. IEC 61508 rute 2H

Gjelder uavhengig av om PFH eller PFD velges!

IEC 61511 tabell

SIL	Mode	Minimum HFT
1	All	0
2	Low demand	0
2	**High demand or continuous**	**1**
3	All	1
4	All	2

Hardware fault tolerance (HFT): Antall feil et SIF delsystem tåler uten å svikte. **Safe failure fraction (SFF):** Andel sikre (S) og farlig detekterte (DD) feil av total feilrate

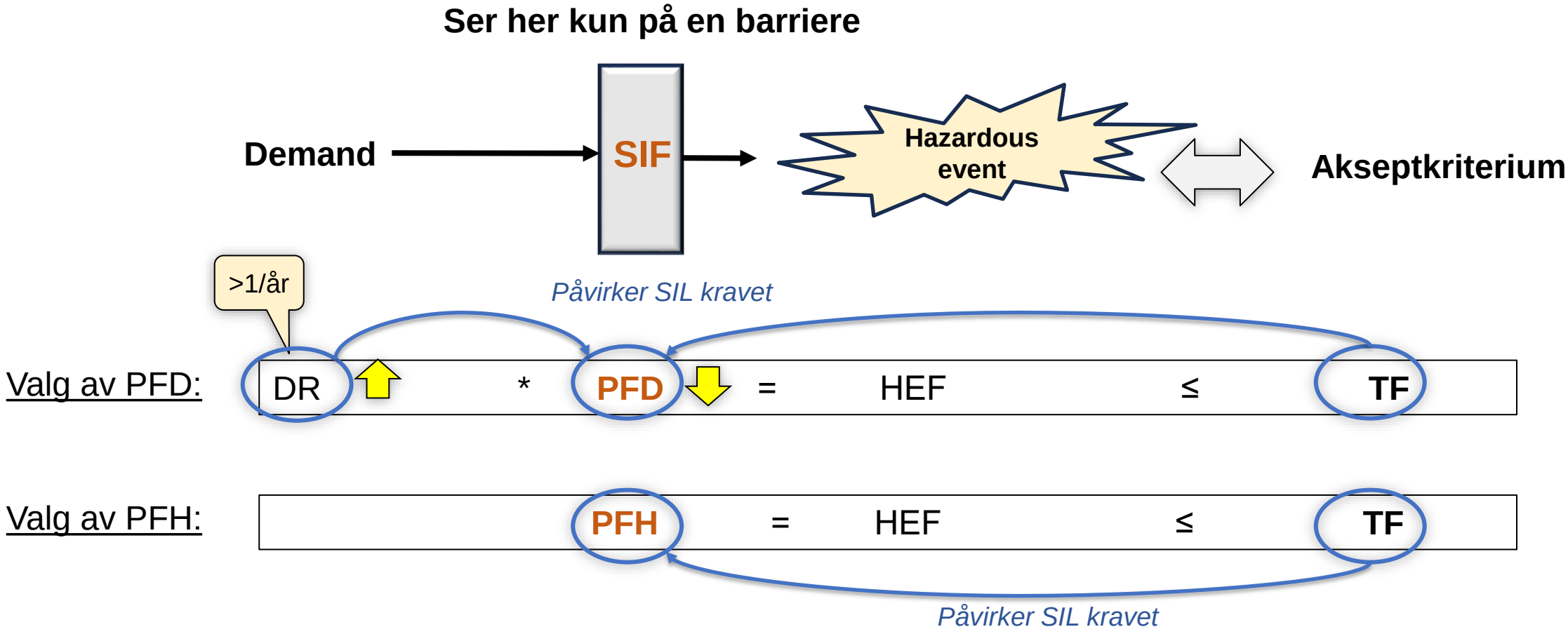
Kan velge mellom PFD og PFH

- Kan velge å bruke enten PFD eller PFH, men «PFH er *vanligvis* best egnet»
- **Mangler føringer/veiledning til *når* PFD er egnet….**

SIL	Low demand	High demand	Continuous
	PFD	PFH (per time)	
4	1E-5 ≤ PFD < 1E-4	1E-9≤ PFH < 1E-8	
3	1E-4 ≤ PFD < 1E-3	1E-8 ≤ PFH < 1E-7	
2	1E-3 ≤ PFD < 1E-2	1E-7 ≤ PFH < 1E-6	
1	1E-2 ≤ PFD < 1E-1	1E-6 ≤ PFH < 1E-5	

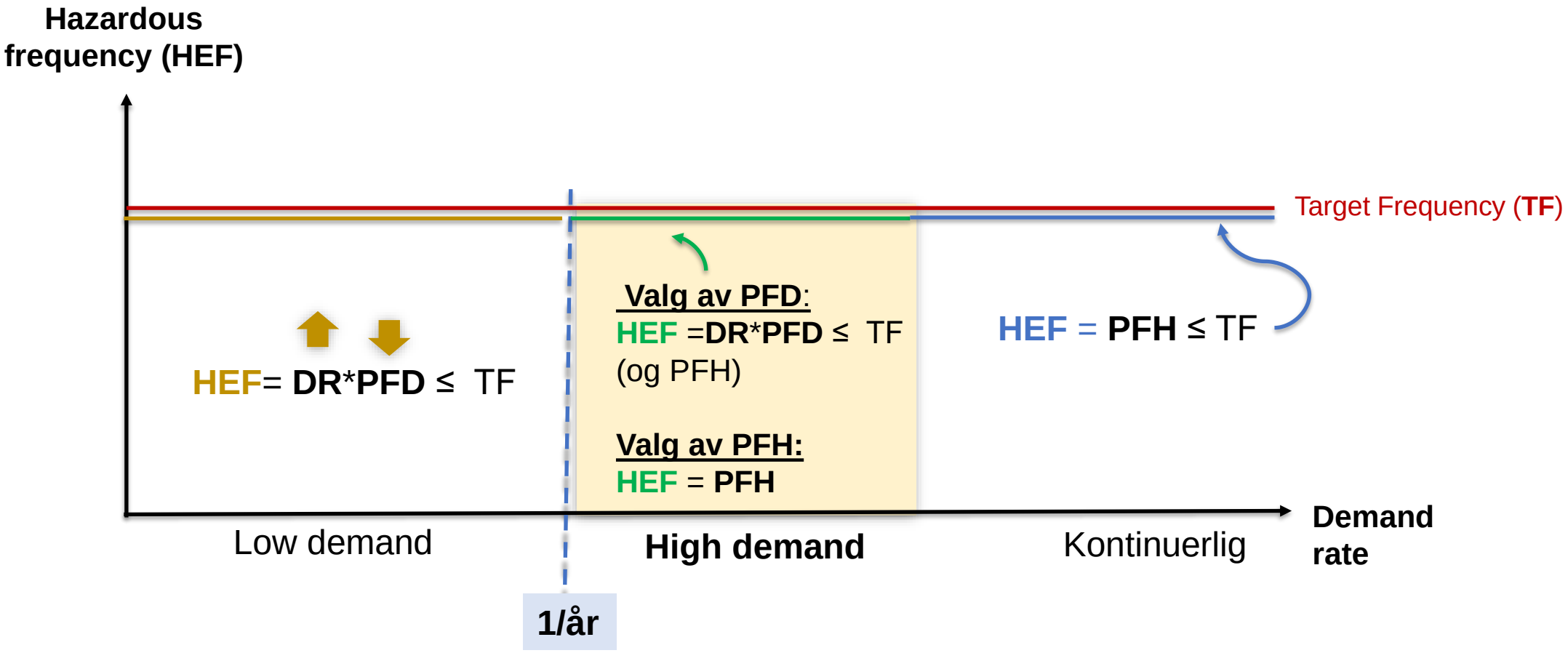
PFD: Average probability of failure on demand. **PFH:** Average dangerous failure frequency (per hour)

Implikasjon av å velge PFD eller PFH

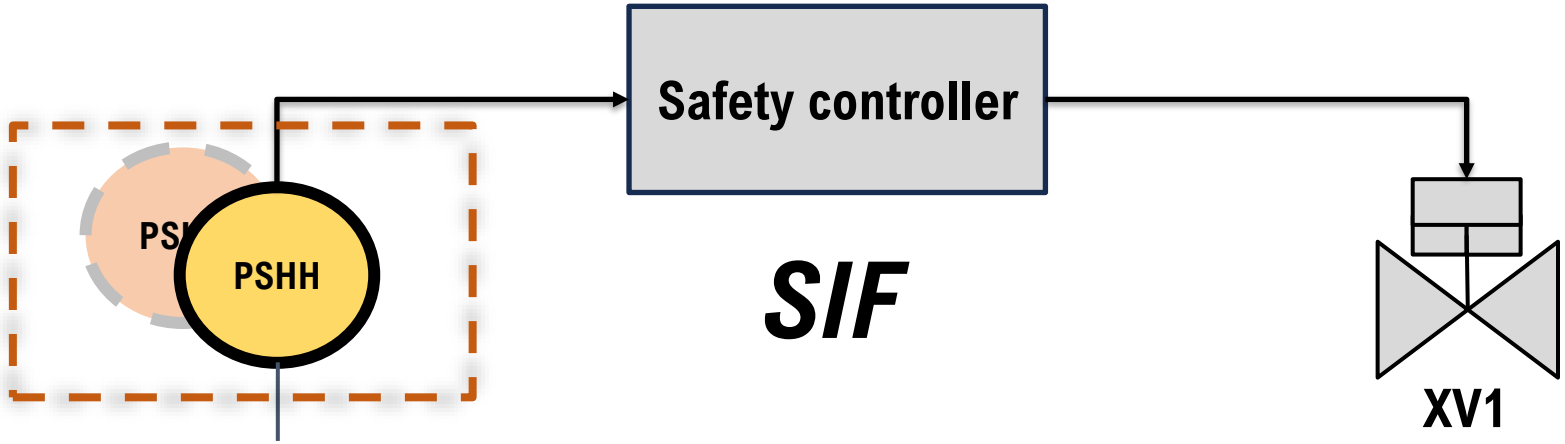


DR: Demand rate (frequency). **HEF:** Hazard event frequency. **TF:** Target (tolerated) frequency

PFD vs PFH og forholdet til demand raten



Beregne PFD vs PFH for en spesifikk SIF



$$PFD \approx \frac{\beta \lambda_{DU} T}{2}$$

Påvirkes av **test intervall** og **DU feilrate** (fellesfeil)

$$PFH \approx \beta \lambda_{DU}$$

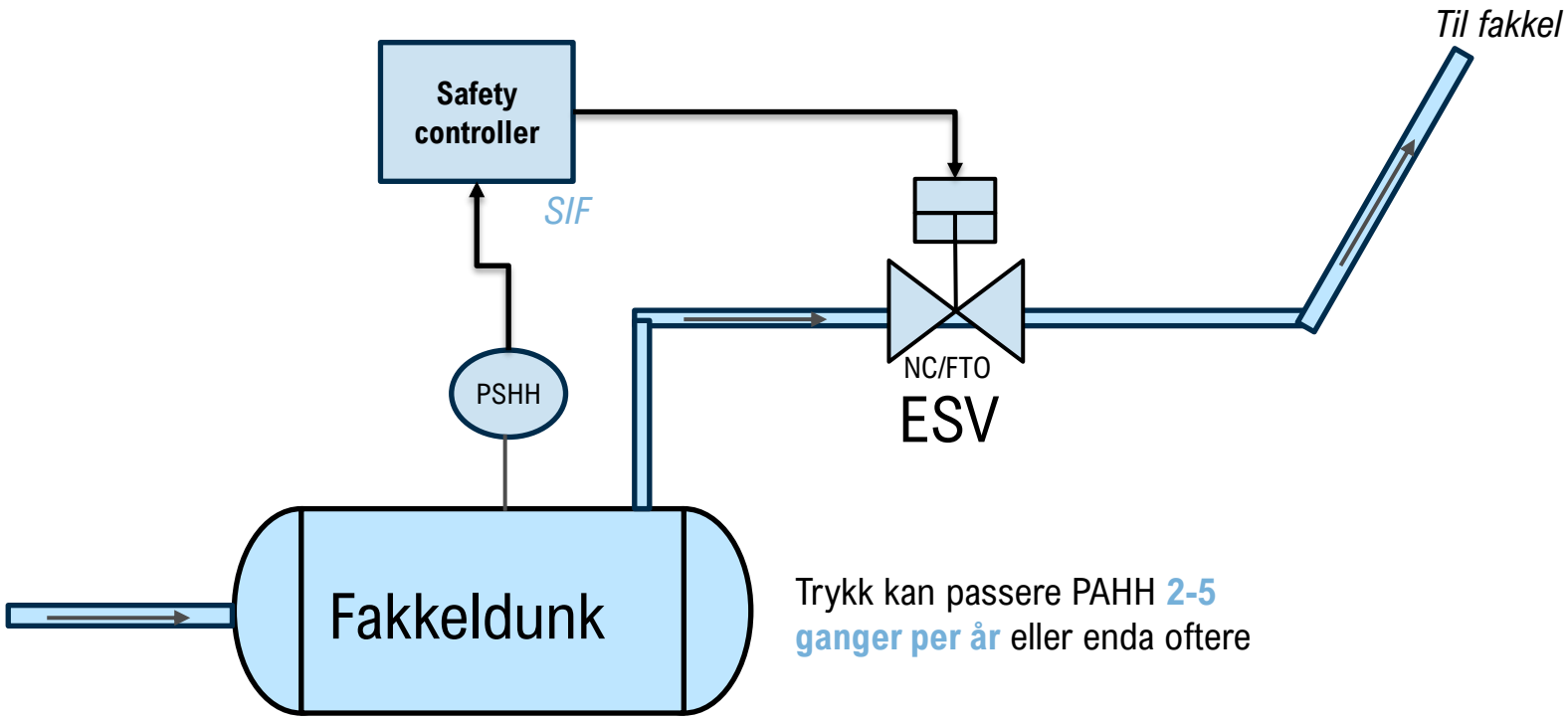
Påvirkes av (kun) **DU feilrate** (fellesfeil)

Eksempel: Enkeltkomponent

2. PRAKTISK EKSEMPEL

Praktisk eksempel 1

SIF:
Åpne ESV hvis trykk = HH settpunkt

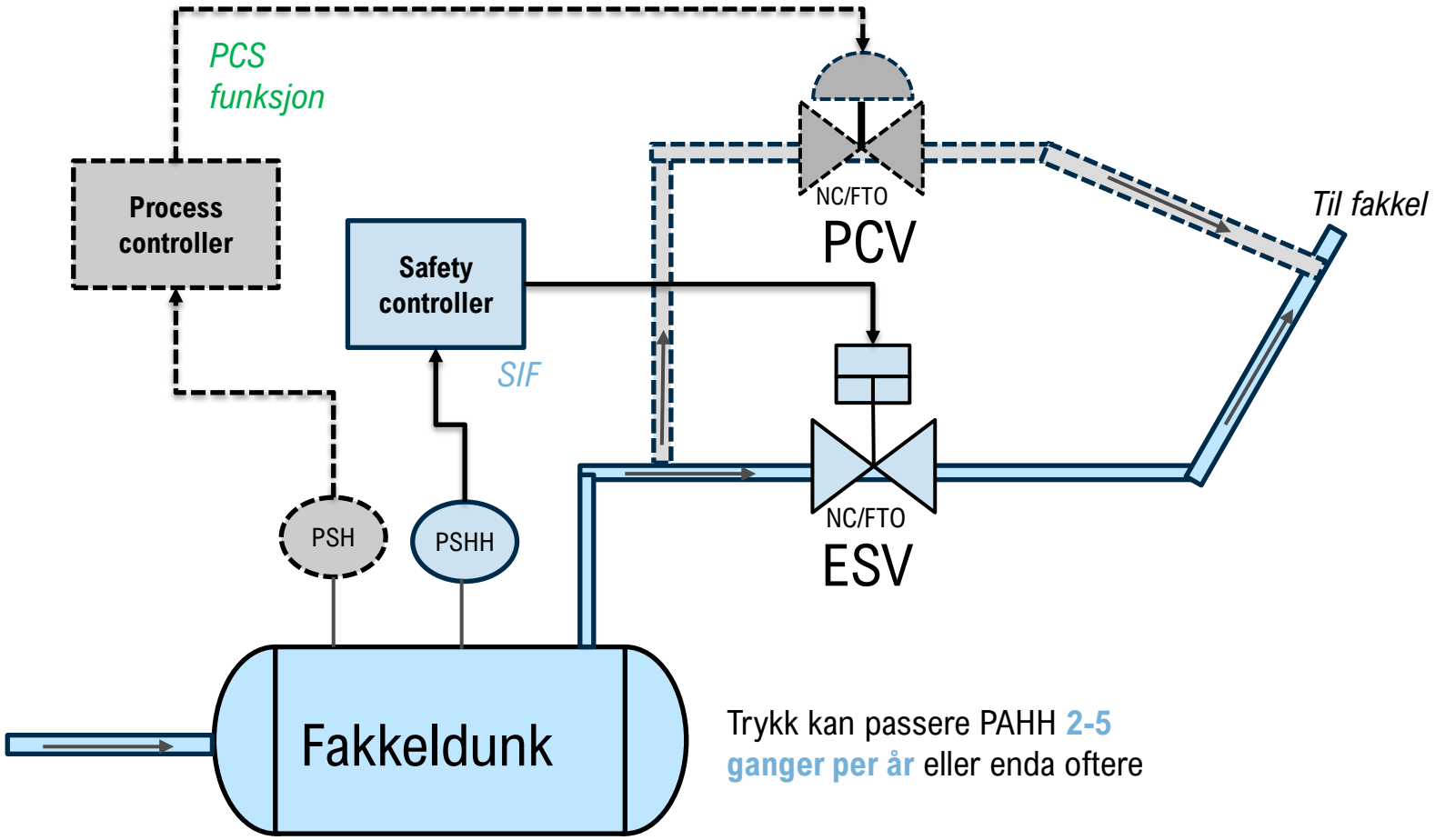


Trykk kan passere PAHH **2-5 ganger per år** eller enda oftere

SIF blir **high-demand**

TÜVRheinland®
safetec

Praktisk eksempel 1



Trykk kan passere PAHH **2-5 ganger per år** eller enda oftere

SIF:
Åpne ESV hvis trykk = HH settpunkt

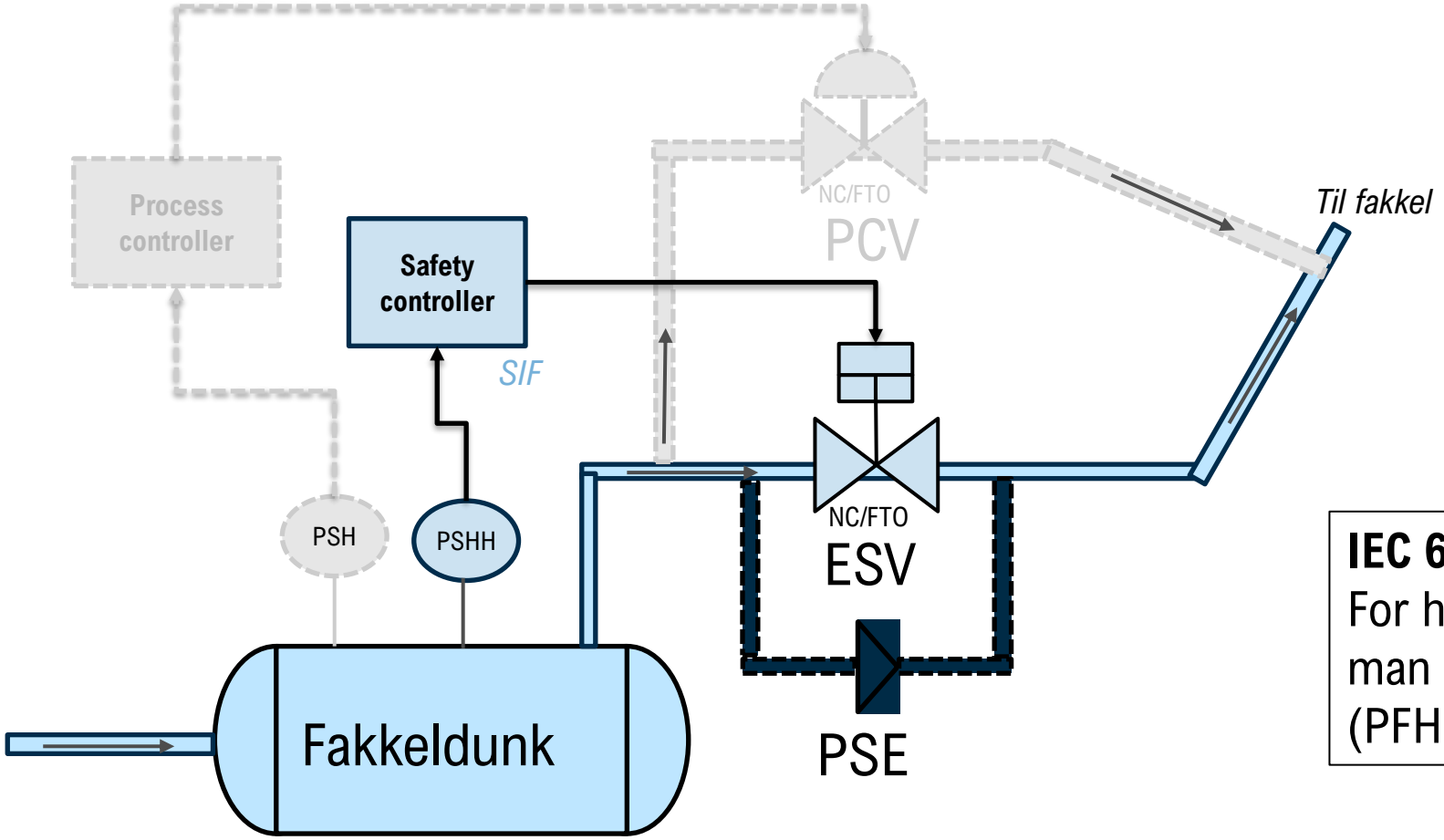
Mulig tilleggsfunksjon (PCS):
Åpne PCV hvis trykk= H settpunkt

SIF + PCS funksjon:
- SIF er **low-demand**

SIF uten PCS-funksjon:
- SIF blir **high-demand**

TÜVRheinland®
safetec

Praktisk eksempel 2



Trykk kan passere PAHH **2-5 ganger per år** eller enda oftere

SIF uten PCS-funksjon:
- SIF blir **high-demand**

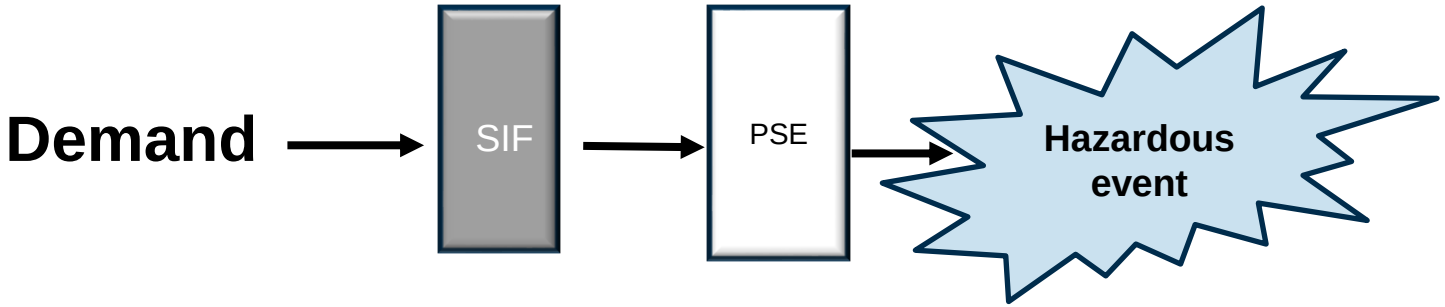
PSE reduserer ikke demand på SIF

IEC 61511, Clause 9.2.3:
For high demand SIF, er det valgfritt om man bruker tabell 4 (PFD) eller tabell 5 (PFH).

TÜVRheinland®
safetec

Regneeksempel

LOPA betingelse:
HEF ≤ Target frequency



Valg av PFD:

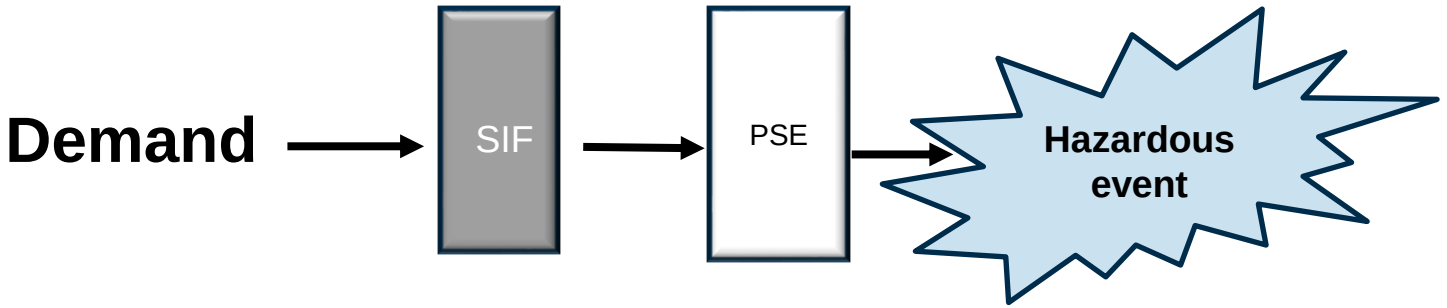
$$DR * PFD_{SIF} * PFD_{PSE} = HEF \leq \mathbf{TF}$$

Valg av PFH:

$$PFH_{SIF} * PFD_{PSE} = HEF \leq \mathbf{TF}$$

TÜVRheinland®
safetec

Regneeksempel



LOPA betingelse:
HEF ≤ Target frequency

- TF = 1E-04 pr år
- PFD_{PSE}=1E-02
- DR = 2 ganger pr år

Valg av PFD:

$$DR * PFD_{SIF} * PFD_{PSE} = HEF \leq \mathbf{TF}$$

PFD_{SIF} = 5E-03, **SIL 2**

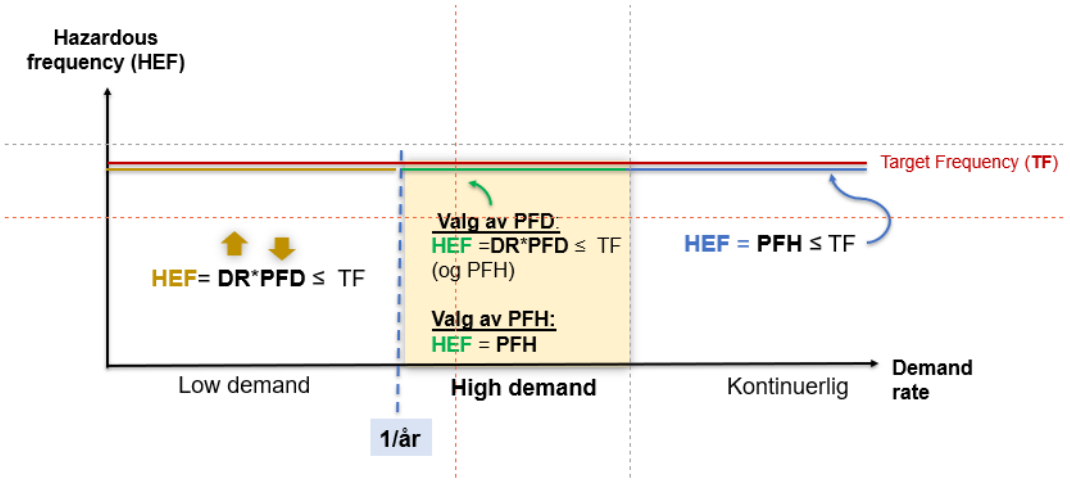
Valg av PFH:

$$PFH_{SIF} * PFD_{PSE} = HEF \leq \mathbf{TF}$$

PFH_{SIF} = 1E-02 per year (1.14E-06 per hour), **SIL 1**

TÜVRheinland®
safetec

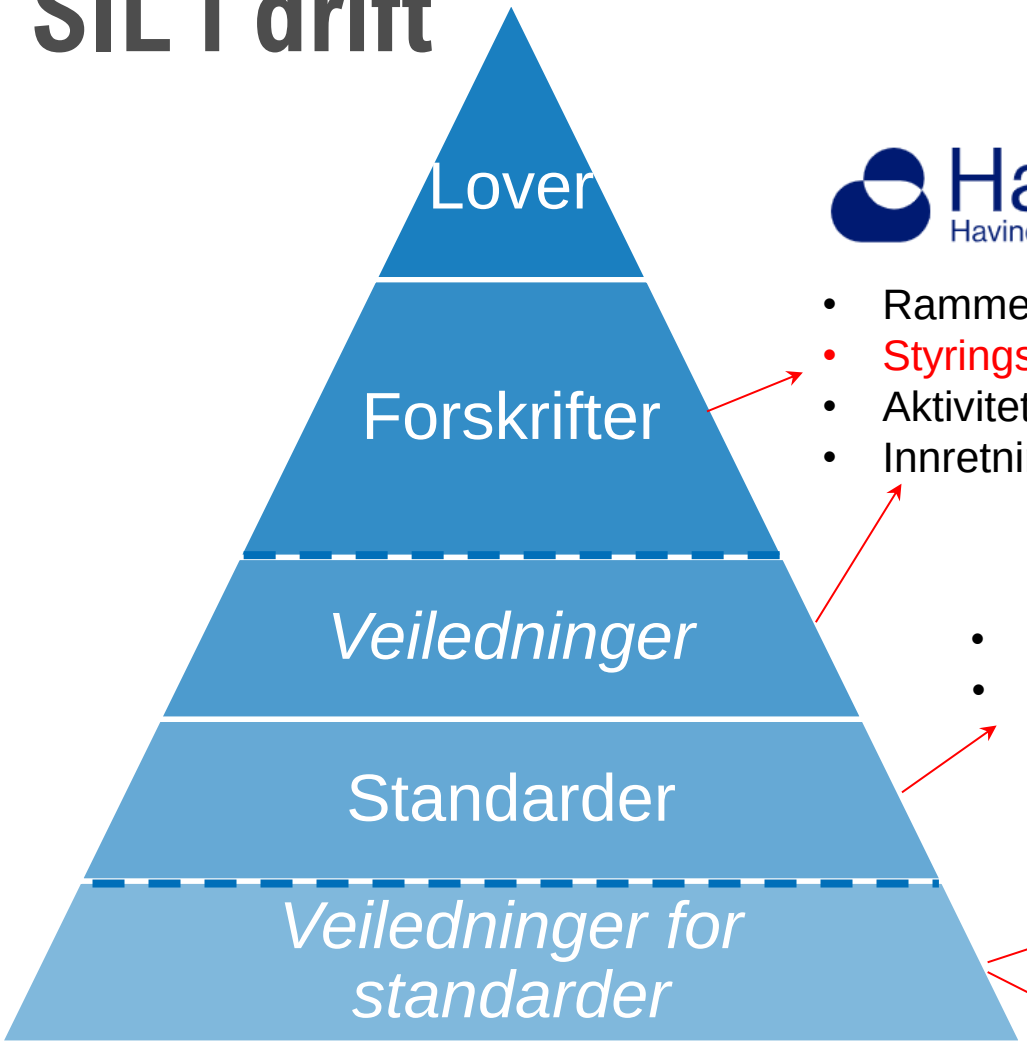
PFD/PFH med økende demandrate



Demand rate	PFD	PFH
2	5E-03 (SIL 2)	1.14E-06 per hour (SIL 1)
5	2E-03 (SIL 2)	1.14E-06 per hour (SIL 1)
10	1E-03 (SIL 2/3)	1.14E-06 per hour (SIL 1)
20	5E-04 (SIL 3)	1.14E-06 per hour (SIL 1)

TÜVRheinland®
safetec

Lover, regler og standarder knyttet til oppfølging av SIL i drift

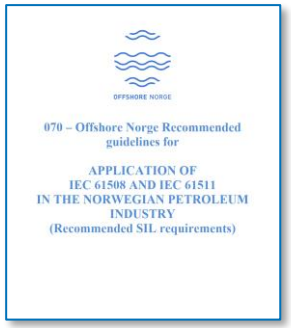


Havtil
Havindustritilsynet

- Rammeforskriften (§11 Prinsipper for risikoreduksjon)
- Styringsforskriften (§5 Barrierer, §19 Innsamling, bearbeiding og bruk av data)
- Aktivitetsforskriften (§26 Sikkerhetssystemer, §47 Vedlikeholdsprogram)
- Innretningsforskriften (§8 Sikkerhetsfunksjoner)

- **IEC 61508**
- **IEC 61511**

- **070** Offshore Norge – Recommended guideline for IEC 61508/IEC 61511



- **APOS** (rapporter og anbefalinger)

TÜVRheinland®
safetec

APOS metodikk for oppdatering av feilrate og optimalisering av testintervall

Ref. «Guideline for follow-up of Safety Instrumented Systems (SIS) in the operating phase»
(Report No: 2023:00107, Version 3, 22.03.2023)

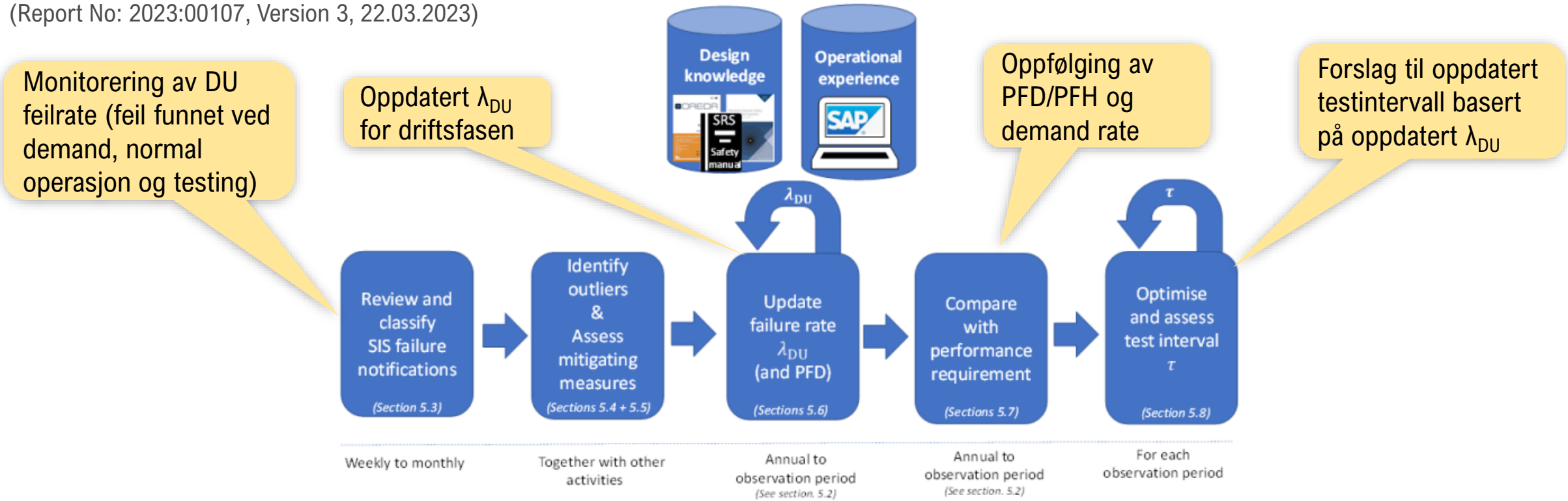


Figure 2: Overall method for updating failure rates and optimising test intervals.

APOS = Automatisert prosess for oppfølging av instrumenterte sikkerhetssystemer

TÜVRheinland®
safetec

3. FORSLAG TIL KRITERIER (FOR VALG AV PFD ELLER PFH)

I designfasen

Generelt:

- High-demand kan kreve **mer feiltoleranse** sammenlignet med low-demand:
  - Som resultat av endrede krav til diagnostikk og potensielt lavere SFF (IEC 61508-2, route 1H), eller
  - Høyere feiltoleransekrav for SIL 2 (IEC 61511)

I tillegg:

- Må velge PFD eller PFH **før man utleder** SIL krav for SIF i «demand mode» og demand rate >1/år.
  - PFD *kan* lede til **høyere SIL krav** (enn ved valg av PFH) (må sjekkes)

Safe failure fraction (SFF): Andel sikre og farlig detekterte (DD) feil av total feilrate

Oppfølging i drift

Skilles ikke på low og high (gjelder felles for demand mode).

Krav til å overvåke:

- Demand raten
- Farlige feil funnet ved demand, normal operasjon og testing

Krav til å korrigere om nødvendig:

- Test intervall bestemmes PFD og PFH

Eksempel: Enkeltkomponent

Med PFD:

$$DR \cdot PFD = \text{HEF} \leq \text{TF}$$

$$DR \cdot \frac{\lambda_{DU} T}{2} = \text{HEF} \leq \text{TF}$$

$$T \leq \frac{2 \cdot TF}{DR \cdot \lambda_{DU}}$$

- SIL krav påvirket av demand rate
- Funksjonstester hovedkilde for overvåkning DU feilrate
- Funksjonstestintervall bestemt av både demand rate og DU feilrate.

Med PFH:

$$PFH = \text{HEF} \leq \text{TF}$$

$$(i)\ \lambda_{DU} = HEF \leq TF$$

$$(ii)\ DR \cdot \frac{\lambda_{DU} T}{2} = PFH = \lambda_{DU} \rightarrow T = \frac{2}{DR}$$

- SIL krav ligger fast
- Demand hovedkilde for å overvåke DU feil (i)
- MEN: Funksjonstest må være supplement – intervall relativt til demand rate

Forslag til kriterier

PFD		PFH
Velg tidlig. Mulig implikasjon for utforming av SIF	Pålitelighets-parameter	Velg tidlig. Mulig implikasjon for utforming av SIF
HEF = DR*$\mathbf{PFD} \leq$ TF		HEF = $\mathbf{PFH} \leq$ TF
Funksjonstesting inngår i PFD-kravet	Behov for funksjonstesting?	Funksjonstesting er supplement til oppfølging av demand rate
Testintervall bestemmes av PFD-kravet og demandraten	Testintervall	Testintervall relativt til demand rate, T=2/DR

VS

Uavhengig av om man velger PFD eller PFH som pålitelighetsmål er det krav til å overvåke:

- Demand rate
- $\lambda_{DU,}$ dvs farlige feil funnet ved demand, normal operasjon og testing

- Noen synspunkter?
- Innspill til oppdatering av IEC 61511?
- Spørsmål?

TÜVRheinland®
safetec

Takk for oss!

Mary Ann Lundteigen
Professor ved institutt for teknisk kybernetikk
mary.a.lundteigen@ntnu.no

Eva Kvam
Principal Safety Advisor
Eva.Kvam@safetec.no