Erfaring med fellesfeil etter driftsgjennomganger

Mary Ann Lundteigen (Mary.a.lundteigen@ntnu.no)

RAMS-gruppa v/ institutt for produksjons- og kvalitetsteknikk, NTNU

Kunnskap for en bedre verden

Formål med presentasjonen

Driftserfaring viser at fellesfeil er et større problem enn tidligere antatt:

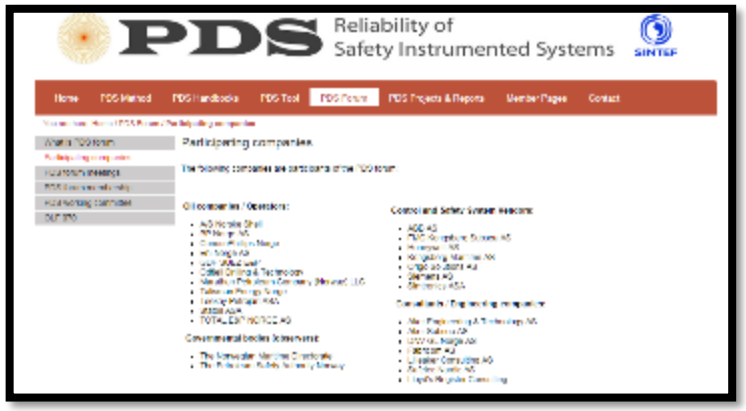
- ❑ Hvorfor?
- ❑ Betydning?
- ❑ Hva gjør vi?

1. Bakgrunn for presentasjonen
2. Fellesfeil – definisjoner, modeller og betraktninger
3. Erfaringer fra driftsgjennomgang
4. Refleksjoner
5. Konklusjon

Bakgrunn for presentasjonen

- **Treårig prosjekt om utvikling av metoder for helhetlig barrierestyring (2013-2015/16)**

Støttet av forskningsrådet og PDS-forums deltagere



SINTEF

NTNU – Trondheim
Norwegian University of
Science and Technology

www.sintef.no/pds

Sentrale aktiviteter i prosjektet:

- *Gjennomført **6** driftsgjennomganger med til sammen over **10 000** **notifikasjoner***
- Vurdere **betydningen fellesfeil** har for svekkelse av barrierer basert på erfaring fra driftsgjennomganger
- Utvikle **nye metoder** og **foreslå nye data** for bruk i pålitelighetsanalyser og driftsoppfølging

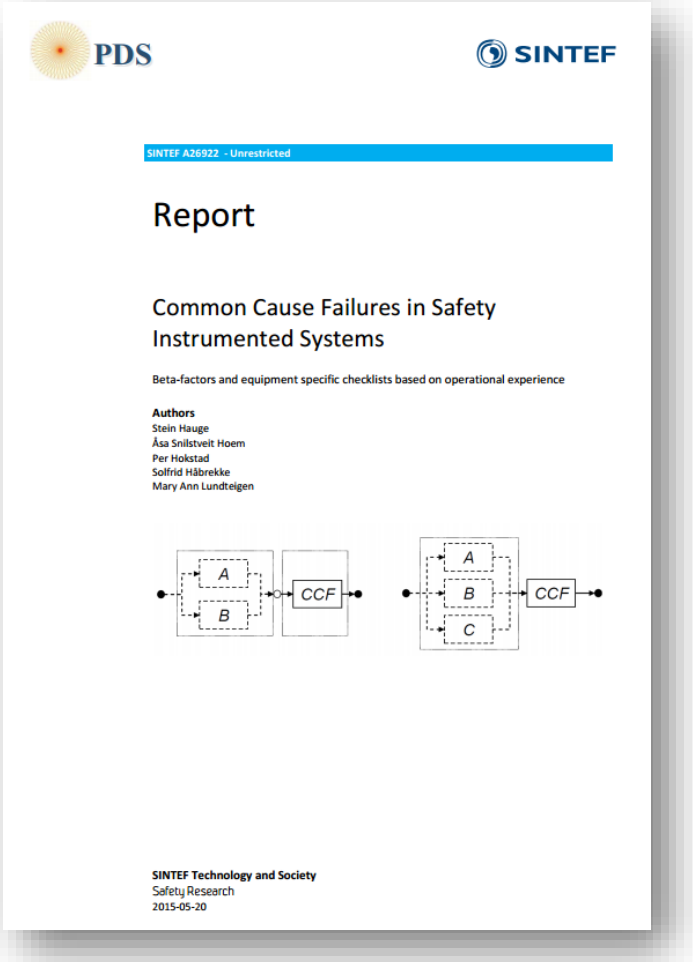
Involvert i prosjektet

Fra SINTEF:

- Stein Hauge
- Solfrid Håbrekke
- Åsa Hoem
- Per Hokstad

Fra NTNU:

- Mary Ann Lundteigen

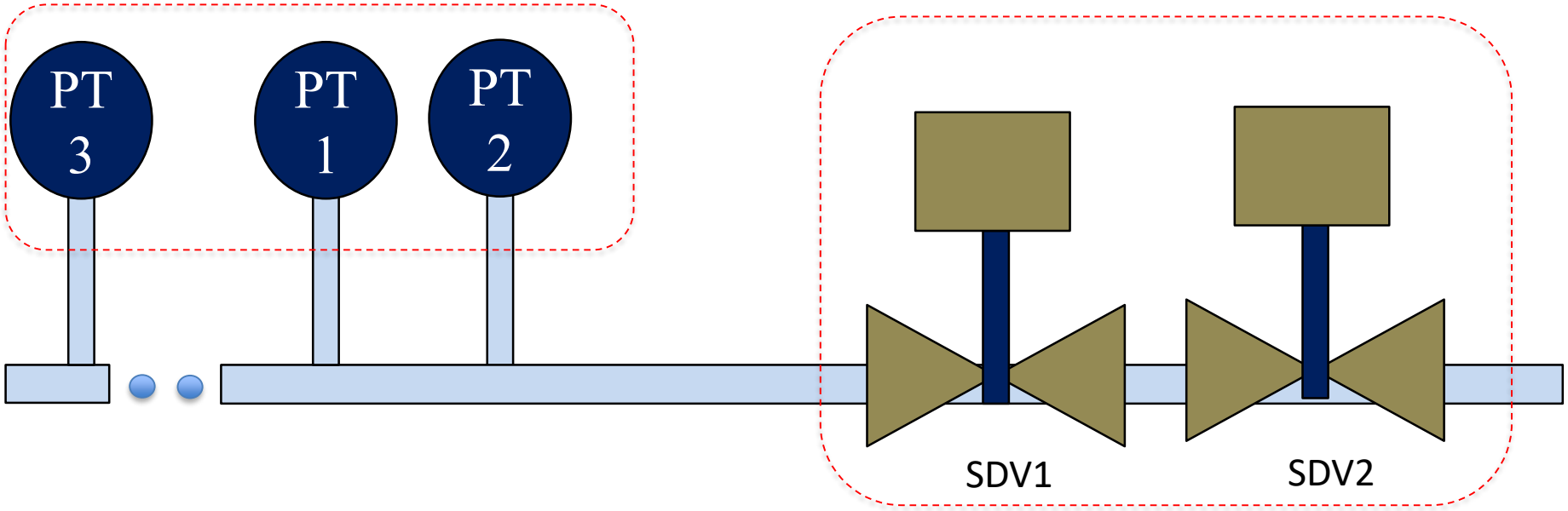


http://www.sintef.no/projectweb/pds-main-page/pds-research-projects/pds-reports/

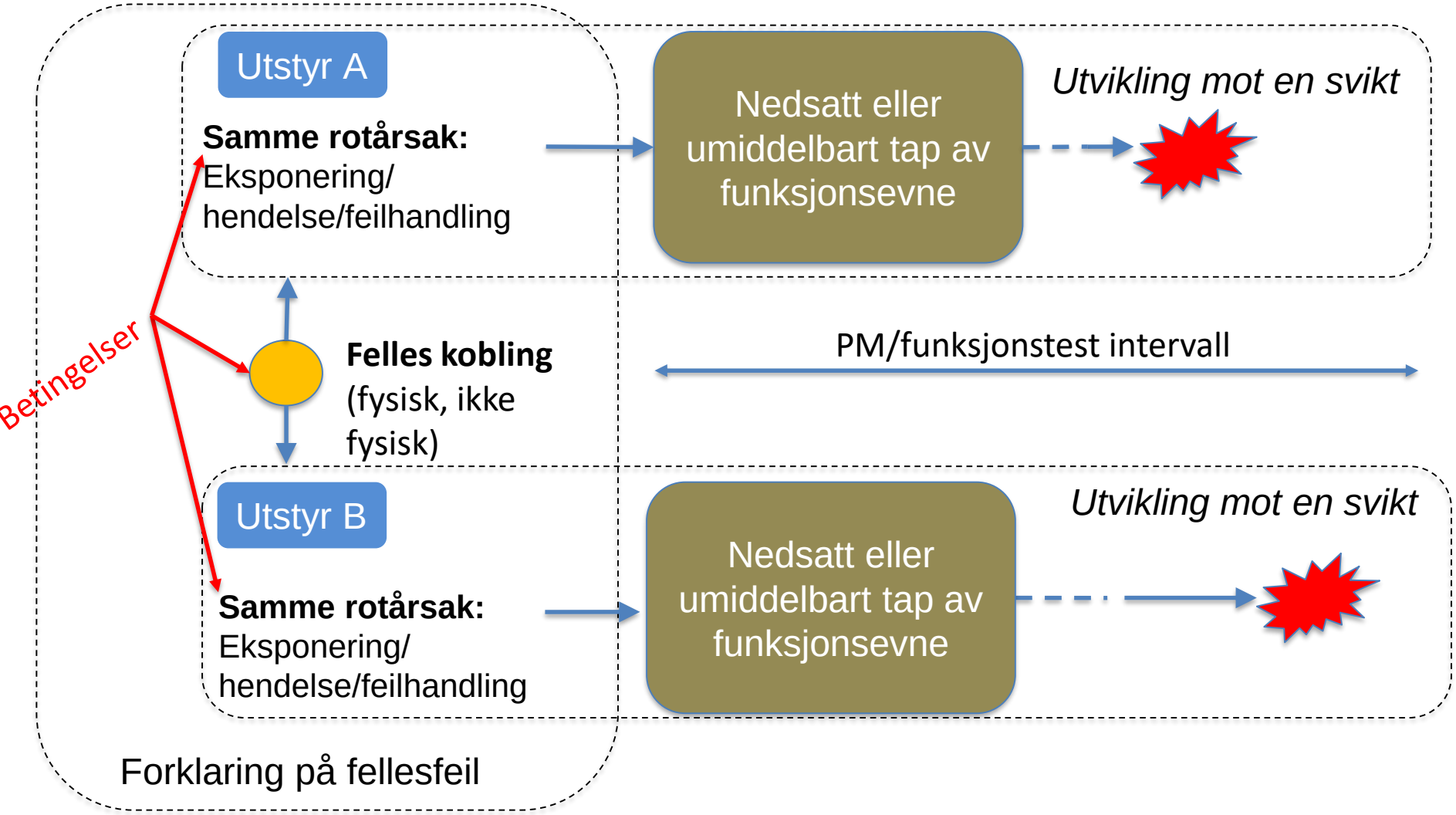
1. • Bakgrunn for presentasjonen
2. • Fellesfeil – definisjoner, modeller og betraktninger
3. • Erfaringer fra driftsgjennomgang
4. • Refleksjoner
5. • Konklusjon

Fellesfeil (i vår kontekst)

*Kritisk (DU) feil hos mer enn ett utstyr av **samme type** med sammenfallende årsak og som er avdekket ved samme PM/test eller tilfeldig oppdaget innenfor samme testintervall.*



Betingelser for fellesfeil



Hva mener vi med kobling?

Alt utstyr har jo en ***viss*** kobling. Eksempel:

To trykktransmittere kan:

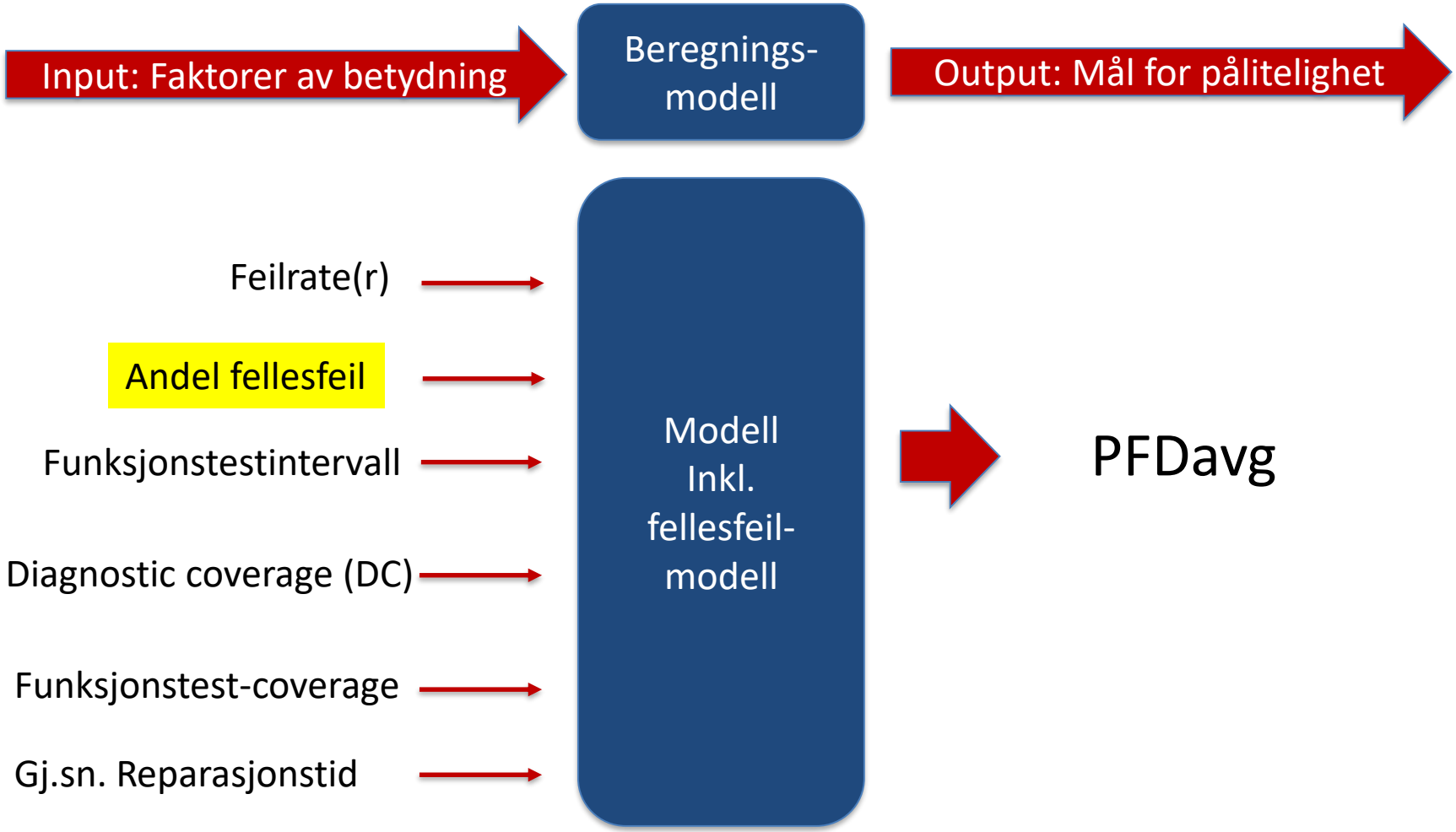
- Være av samme fabrikat/fra samme produksjonsserie
- Stå i samme omgivelser
- Være gjenstand for samme kalibreringsprosedyre

MEN det betyr ikke at alle feil funnet for en type utstyr er fellesfeil!

For at koblingen skal være reell (i vår kontekst) så må det være en **én sammenfallende og relevant forklaring** på hvorfor **samme sviktårsak** er funnet på samme utstyrstype.

Sviktet utstyr	Sviktårsak	Forklaring (på kobling)
Trykktransmittere	Feilkalibrering	Samme prosedyre brukt
Detektorer	Jordfeil pga fukt	Uheldig innføring av kabel til boks
Nivåmålere	Feilmåling ved skumming i tank	Samme (uegnede) måleprinsipp

Betydning av fellesfeil i analyse



Modeller for fellesfeil

- **Standard betafaktor-modellen:**

$$\lambda_C = \beta \cdot \lambda$$

"The parameter β can be interpreted as the mean fraction of all failures of a channel that also affect all the other channels of the system." [Hokstad & Rausand, 2008]

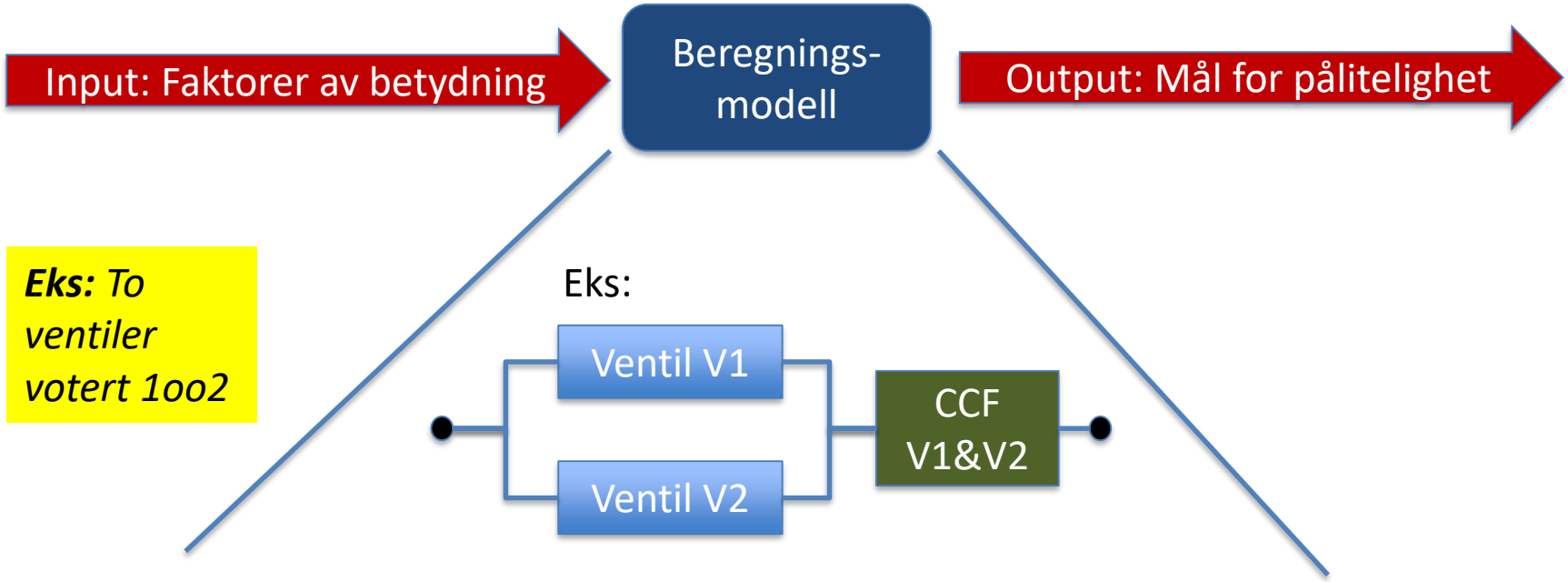
Andel fellesfeil

- **PDS metoden:**

$$\lambda_C = C_{MooN} \cdot \beta \cdot \lambda$$

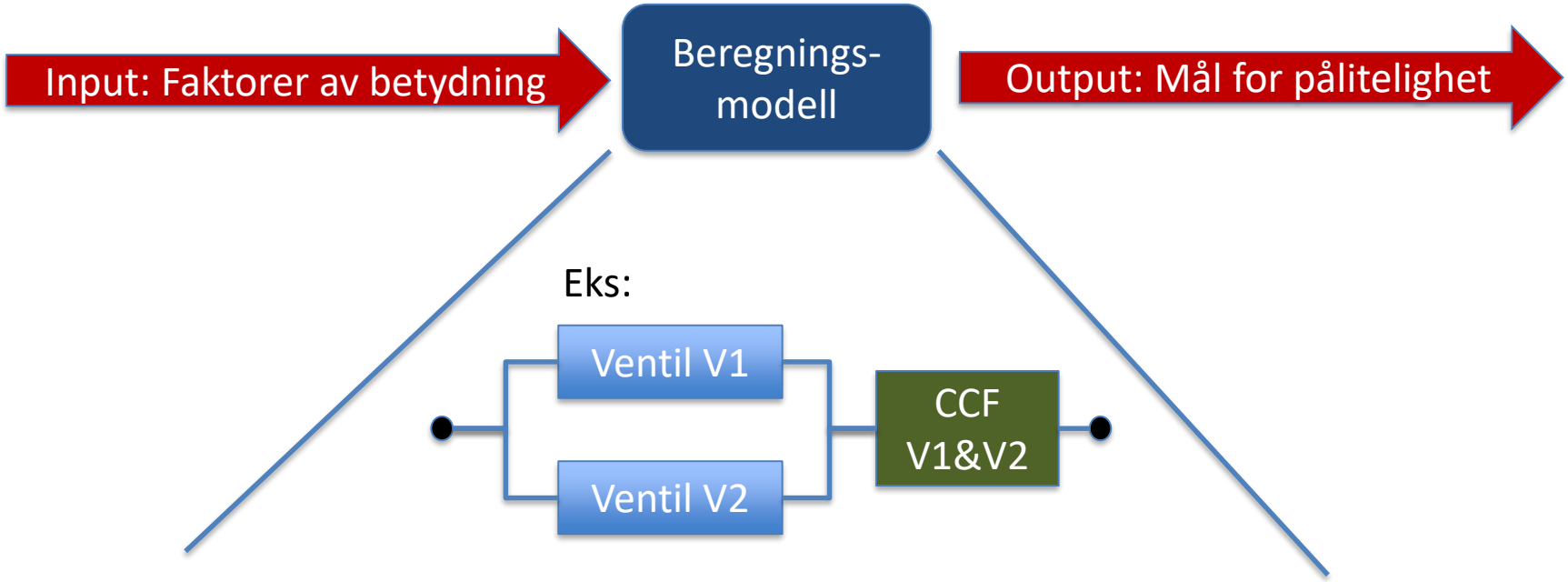
β er andel av feil som berører TO kanaler. PS: $C_{1oo2}=1$.

Betydning av fellesfeil i analyse



PFDavg:
Gjennomsnittelig sannsynligheten for at **ENTEN** V1 og V2 svikter samtidig men uavhengig, **ELLER** at V1 og V2 svikter «samtidig» pga felles årsak.

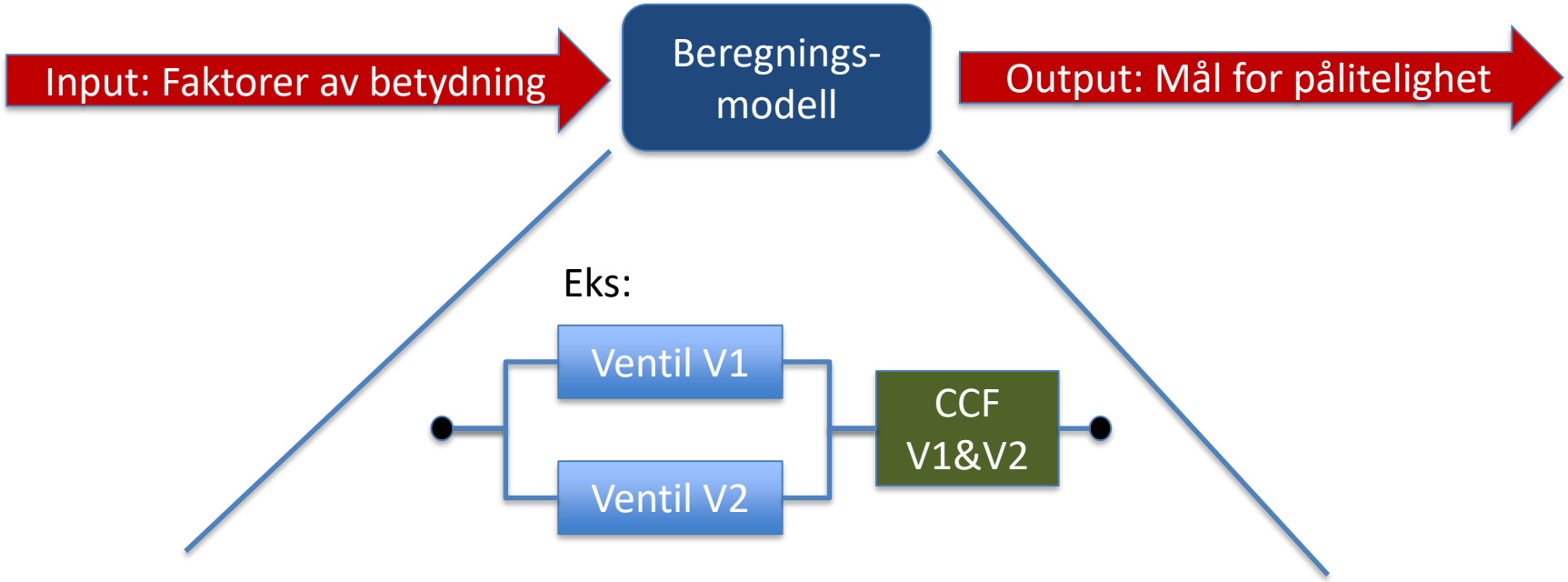
Betydning av fellesfeil i analyse



"Standard metoden":

$$PFD_{avg} \approx \frac{((1-\beta)\lambda_{DU}\tau)^2}{3} + \frac{\beta\lambda_{DU}\tau}{2} \approx \frac{\beta\lambda_{DU}\tau}{2}$$

Betydning av fellesfeil i analyse



"PDS metoden":

$$PFD_{avg} \approx \frac{(\lambda_{DU}\tau)^2}{3} + C_{1oo2}\frac{\beta\lambda_{DU}\tau}{2} \approx C_{1oo2}\frac{\beta\lambda_{DU}\tau}{2}$$

Hvordan bestemme beta (β)?

- **Sjekklister:**
  - For eksempel IEC 61508-6 (appendiks D) eller IEC 62061 (appendiks F)
  - Krever stor detaljkunnskap om spesifikk design
  - Relevant å bruke for utstyrsprodusenter
- **Driftserfaring:**
  - Krever analyse av rapporterte feil
  - Viser ofte at det kan være andre årsaker enn de som fremkommer i sjekklister
  - Dekker ikke alle typer fellesfeil som kan inntreffe, bare de som er erfart
- **Andre:**
  - Ekspertvurdering, Generiske gjennomsnittstall
  - Kan bygge på flere ulike kilder og erfaring
  - Eksempel: PDS data
  - Litt vanskelig å etterprøve. Viktig å vurdere relevans og beskrive antagelser

Eksempel: Generiske data (PDS)

Table 9: β value for various components

Component group	Component	β	Comment/source
Input devices	Pressure switch	0.06	Updated SINTEF estimates based on former values and additional knowledge from operational reviews.
	Proximity switch	0.06	
	Process transmitters	0.06	
	Fire/gas detectors	0.07	
	ESD push button	0.04	
Control logic units	Standard industrial PLC	0.07	SINTEF estimates based on additional judgements.
	Programmable safety system	0.05	
	Hardwired safety system	0.03	
	ESV/XV incl. X-mas tree valves (main valve + actuator)	0.05	
	HIPPS valve	0.05	
	Blowdown valves (main valve +	0.05	

Source: PDS data handbook, 2013

Generiske verdier for beta i PDS (per 2013)

Equipment group	βs from PDS 2013 data handbook
ESD/PSD valves (incl. riser ESD valves)	5 %
Blowdown valves	5 %
Fire dampers	5 %
PSVs	5 %
Gas detectors (point and line)	7 %
Fire detectors (flame, smoke and heat)	7 %
Process transmitters (level, pressure, temperature and flow)	6 %

From table 1 and table 2 in Hauge et al (2015)

Beregnet på bakgrunn av driftsdata

[NUREG, 1988]:

$$\hat{\beta}_1 = \frac{N_{DU,CCF}}{N_{DU}} \qquad \hat{\beta}_2 = \frac{2 \cdot N_{CCF}}{N_{DU,I} + 2 \cdot N_{CCF}}$$

[Hokstad, 2006]

$$\hat{\beta}_3 = \frac{\sum_{j=1}^{K} Y_j(Y_j - 1) / [n_j(n_j - 1)]}{\sum_{j=1}^{K} Y_j / n_j}$$

Table 2 **β-estimates for the equipment groups**

Equipment group	$\hat{\beta}_1$	$\hat{\beta}_2$	$\hat{\beta}_3$ [1)]	New suggested (generic) β	β from PDS 2013 data handbook (for comparison)
ESD/PSD valves (incl. riser ESD valves)					5 %
Blowdown valves					5 %
Fire dampers					5 %
PSVs					5 %
Gas detectors (point and line)					7 %
Fire detectors (flame, smoke and heat)					7 %
Level transmitters					6 %
Pressure transmitters					6 %
Temperature and flow transmitters					6 %

Expert judgment based on $\beta_1, \beta_2, \beta_3$

1. Bakgrunn for presentasjonen
2. Fellesfeil – definisjoner, modeler og betraktninger
3. Erfaringer fra driftsgjennomgang
4. Refleksjoner
5. Konklusjon

Fremgangsmåte

- Fellesfeil vurdert som en **del** av driftsgjennomganger
- **Avmerket** i hvert tilfelle om flere DU feil inntraff for samme type utstyr i observasjonsperioden
  - Vurdert årsak og kobling
- Notert ned **antall DU feil** som inngikk i hver «fellesfeil-hendelse»

Beta-verdier basert på driftserfaring

Equipment group	Total population	N_{DU}	$N_{DU,CCF}$	New suggested generic βs	βs from PDS 2013 data handbook
ESD/PSD valves (incl. riser ESD valves)	1120	229	68	**12 %**	5 %
Blowdown valves	228	73	17	**12 %**	5 %
Fire dampers	458	44	23	**20 %**	5 %
PSVs	2356	148	32	**11 %**	5 %
Gas detectors (point and line)	2239	74	20	**15 %**	7 %
Fire detectors (flame, smoke and heat)	5921	65	19	**15 %**	7 %
Process transmitters (level, pressure, temperature and flow)	1746	112	32	**15 %**	6 %

From table 1 and table 2 in Hauge et al (2015)

Erfaringer om fellesfeil - generelt

- Introdusert både **før** idriftsettelse og **i** driftsfasen
- Noen ganger **mangelfull** beskrivelse av svikt og sviktårsak (ved tvil, ikke registrert som fellesfeil)
- Flest skyldes **systematiske** feil
  (e.g. feilhandlinger, designfeil, produksjonsfeil, feil utført under testing og kalibrering)
- Men også en del **tilfeldige** hendelser og påvirkninger (e.g.: Snøfall, fuktighet, fester som løsner, etc)

Ventiler – Eksempler på årsaker

Designrelatert:

- "Dårlig" design av hydraulisk kobling (for lang lukketid)
- Feil type ventil installert (stengte ikke)
- For svak aktuator
- Feil materialvalg for aktuatorstamme

Driftsrelatert:

- Endret viskositet i hydraulikk (temperaturendringer)
- Avleiringer
- En rekke gangtidsfeil som skyldes feiljustering i avblødningsmekanisme samt mangelfull kapasitet
- Feilmontering ved utskiftning av solenoid-ventiler

Refleksjoner:

- Går **en del tid** før feil fra designfasen utbedres
- Definere **hva** som faktisk er **krav** til gangtid (lukke/åpningstid)

Brann og gassdeteksjon - årsaker

Designrelatert:

- Avdekket svakheter med konkrete detektortyper
- «Fryst» signal
- Fukt/vanninntrengning (designrelatert)

Driftsrelatert:

- Feilkalibrering
- Løs/løsnet innfesting
- En del uten kjent årsak

Refleksjoner:

- Generelt **vanskelig å avdekke** feilårsaker (byttes bare ut)
- Behov for kalibrering versus risiko for **feil-kalibrering**?
- Kan man **unngå feil valg** av detektortype og montering?
- Ikke god nok **diagnostikk**? En del feil kunne en forventet blitt meldt som alarm

Transmittere

- **Designrelatert:**
  - Feil valg av transmitter (feil måleområde, endrede betingelser fra design)
  - Ikke egnet (krevende varierende prosessforhold)
  - Feil i dataark (og derfor innlagte data)

- **Driftsrelatert:**
  - Feilkalibrering
  - Tett rør prosesstilkobling
  - Ising

Refleksjoner:

- Hvorfor **feilkalibrering**? Eller er det stor drift i signal?
- Hva kan man gjøre med **"umulige"** måleforhold (eks. Nivå)?

1. • Bakgrunn for presentasjonen
2. • Fellesfeil – definisjoner, modeller og betraktninger
3. • Erfaringer fra driftsgjennomgang
4. • Refleksjoner
5. • Konklusjon

Høye beta-verdier & hva gjør vi?

Hva gjør vi for å redusere beta:

- Mange gjengangere – mer fokus på **utbedringer** som gir **varig** forbedring
- Større fokus på analyse av **rotårsaker**, for mange gjentakende feil
- Bedre **erfaringsoverføring** fra drift til de som produserer utstyr og løsninger

Hva gjør vi med de nye (høye) tallene:

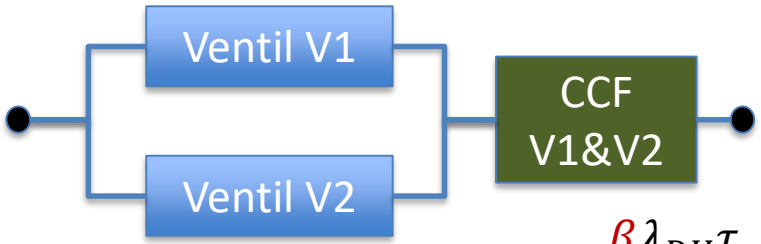
- Vurdere å bruke **mer konservative** verdier i analyser
- Gjøre **anleggsspesifikke** vurderinger (egne sjekklister foreslått i CCF-rapport)

Liten effekt av redundans?

- Høy beta gir noe redusert effekt…
- **Men:** Redundans gir positiv effekt på pålitelighet:

  Feilraten blir tross alt redusert med (1-β) (%) i eksempelet vist

- Redundans gir også mer fleksibilitet/robusthet
- Må veies opp mot kompleksitet og kostnad



$$PFD_{avg} \approx \frac{\beta \lambda_{DU} \tau}{2}$$

ELLER

$$PFD_{avg} \approx \frac{\lambda_{DU} \tau}{2}$$

Liten effekt av redundans?

- Flere funksjoner blir single (SIL 1 og SIL 2). Er da fellesfeil relevant lenger?

- Ja:
  - Viktig for SIL 3 funksjoner.
  - Dessuten samme komponent type inngår i flere ulike barrierer og på tvers av definerte SIFer (for eksempel ESD og BDV ventiler i prosessen).
  - Fellesfeil/kobling mellom barrierer er kanskje et **undervurdert** tema i risikoanalyser.

Table 6 – Minimum HFT requirements according to SIL

SIL	Minimum required HFT
1 (Any mode)	0
2 (demand mode)	0
2 (continuous mode)	1
3 (Any mode)	1
4 (Any mode)	2

IEC 61511-1 (FDSI of rev 2)

Anbefaling å se mer helhetlig på fellesfeil

Erkjennelser:

- Eksisterer alltid en ***viss kobling*** mellom barrierer, ikke bare internt i en barriere
- Effekt av kobling mellom barrierer **ofte utelatt** fra analyser
- Fysisk uavhengighet på samme nivå som topside er kanskje **ikke veien å gå** i alle sammenhenger (eksempelvis subsea)

Derfor:

- Se på **ulike strategier** for å redusere effekten eller kompensere av kobling (feiltolerante løsninger)
- Viktig å hensyn-ta effekten av kobling i risikoanalyser for å unngå optimistiske/feilaktig risikobilde
- Å hensyn-ta er **ikke først og fremst** å gjøre regneøvelse, men å vurdere gode måter å løse det på designmessig.

1. • Bakgrunn for presentasjonen
2. • Fellesfeil – definisjoner, modeller og betraktninger
3. • Erfaringer fra driftsgjennomgang
4. • Refleksjoner
5. • Konklusjon

Konklusjon

- Driftserfaring gir **entydig** indikasjon om høyere beta-verdier
- Mye **gjentagende feil** har bidratt delvis til dette
- Industrien bør se på **tiltak** – operatører og leverandører bør jobbe **sammen** om dette!
- Grad av kobling er **økende** – selv om idealet er å unngå kobling mellom systemer. Må finne **strategier** for å håndtere og hensyn-ta effekten av dette!
- **Heller** enn mer regning ønskes mer fokus på å finne gode (og vurdert som pålitelige) tekniske løsninger

Referanser (utover IEC-standardene)

- Hauge, S., Hoem, Å.S., Håbrekke,S., Lundteigen, M.A. **Common cause failures in safety instrumented systems: Beta-factors and equipment specific checklists based on operational experience (Report no SINTEF A26922).** SINTEF, Trondheim, Norway (2015)
- **Hokstad P., Rausand M.** Common cause failure modeling: status and trends. In*Handbook of performability engineering* (Ed. Misra K. B.), 2008, Chapter 39, pp.621–640 (Springer, London)
- **NUREG/CR-4780.** Procedures for treating common cause failures in safety and reliability studies, vol. 2U.S. Nuclear Regulatory Commmission, Washington DC (1989)
- N**UREG/CR-5485** Guidelines on modeling common-cause failures in probabilistic risk assessment**.** U.S. Nuclear Regulatory Commmission, Washington DC (1998)

Takk for oppmerksomheten!

- Mary Ann Lundteigen (mary.a.Lundteigen@ntnu.no)