Analyseverktøy for pålitelighet av instrumenterte sikkerhetssystemer

Lars Bodsberg
Forskningssjef
SINTEF Teknologi og samfunn
lars.bodsberg@sintef.no

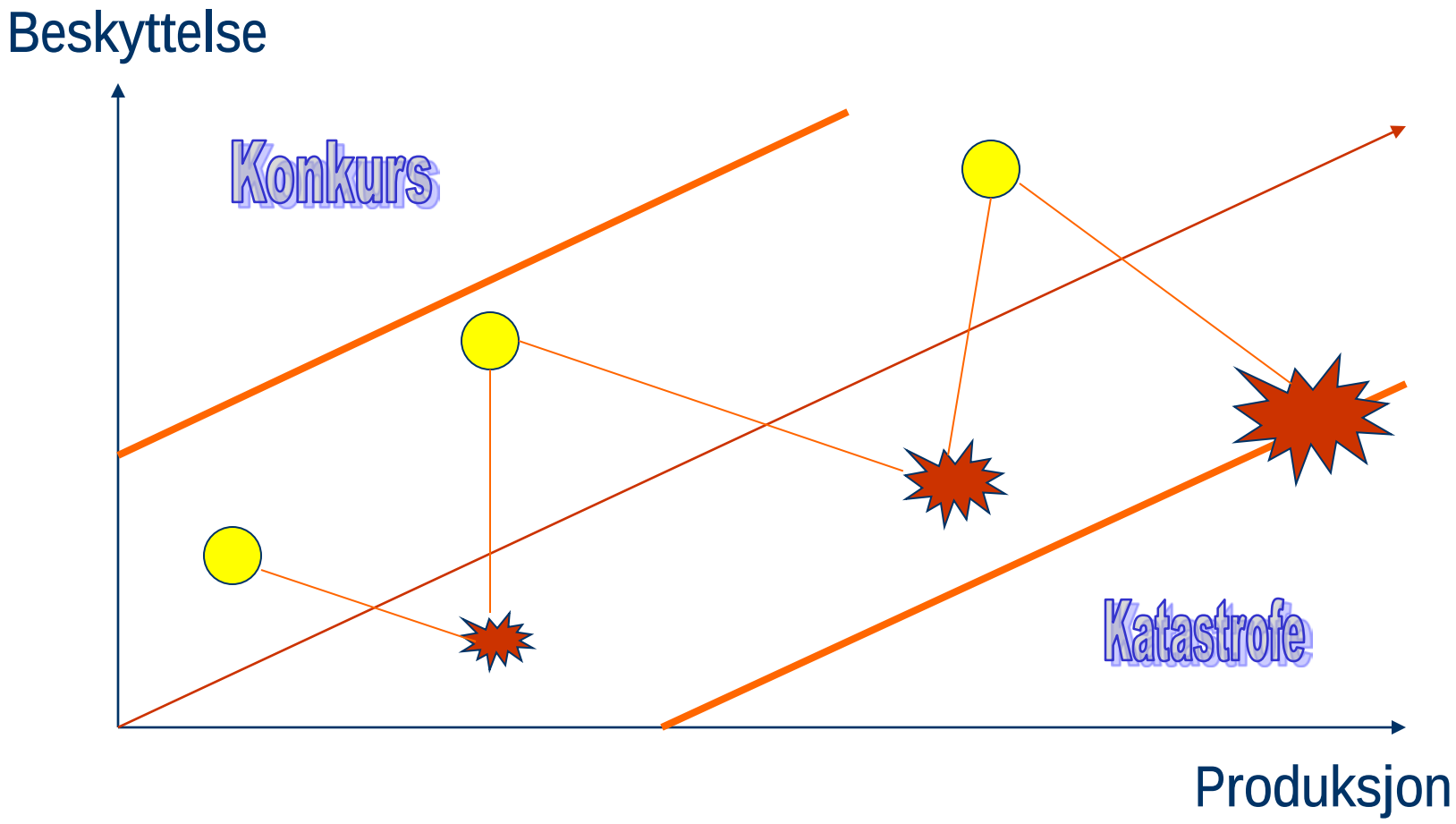
www.sintef.no/pds

Sikkerhetssystemkonferansen 2010
18-19 november 2010,
Park Inn Oslo Airport Hotel, Gardermoen

Innhold

1. Litt om sikkerhetssystemer og PDS forum
2. Hvilke faktorer påvirker påliteligheten av sikkerhetssystemer
3. På hvilken måte vil strengere miljøkrav påvirke tekniske løsninger
4. Nye perspektiver på sikkerhetsstyring

Balanse mellom produksjon og beskyttelse



Kilde: Reason (1998)

St.meld. nr. 12 (2005 – 2006)
Helse, miljø og sikkerhet i petroleumsvirksomheten

”Det er regjeringens målsetting at petroleumsvirksomheten skal være ***verdensledende på HMS***”

PDS-forum

Et faglig og inkluderende nettverk som

- er drivkraft i utvikling og drift av pålitelige sikkerhetssystemer og gjennom dette bidrar til at petroleumsvirksomheten blir en foregangsnæring innen sikkerhet.
- gir økt konkurransekraft blant norske operatørselskaper, leverandørindustri, engineeringselskaper og konsulentselskaper innen sikkerhet og pålitelighet.
- bidrar til økt fokus på sikkerhet

http://pds.sintef.no/

PDS-forum

Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry

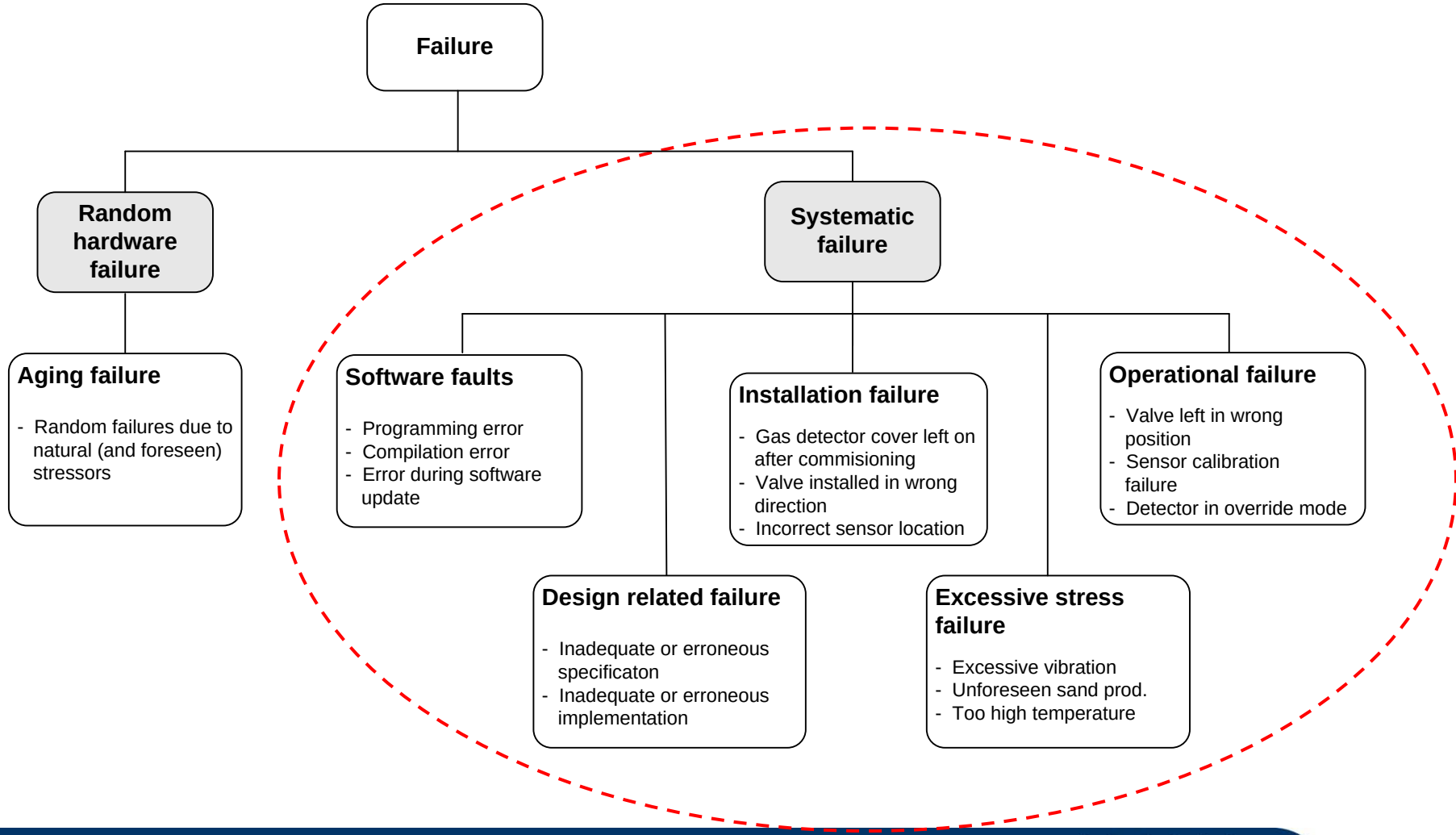
No.: 070 Date effective: October 2004 Revision no.: 02 Date revised: October 2004 1 of 159

APPLICATION OF IEC 61508 AND IEC 61511 IN THE NORWEGIAN PETROLEUM INDUSTRY

THE NORWEGIAN
OIL INDUSTRY ASSOCIATION

http://pds.sintef.no/

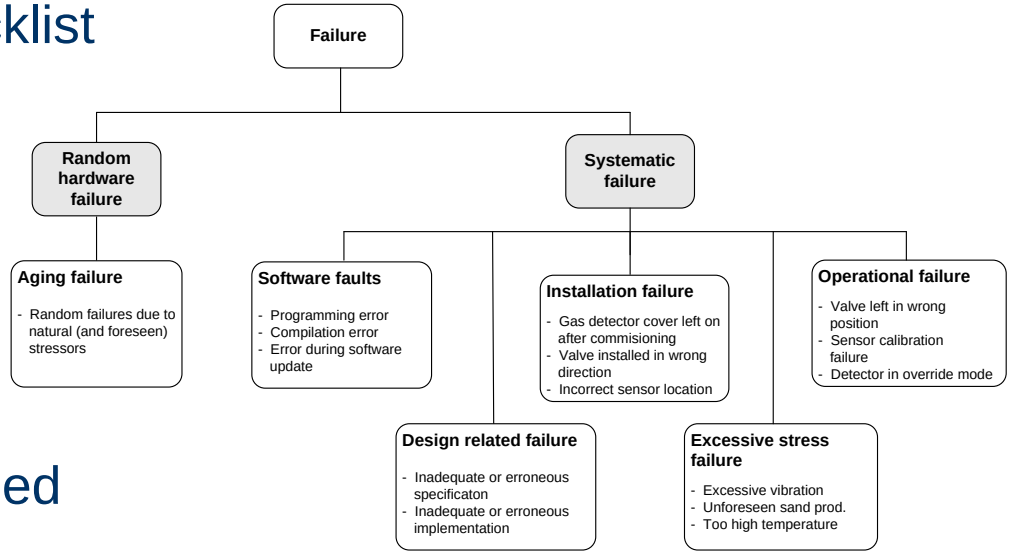
Failure classification by cause of failure



Systematic failures

IEC 61508

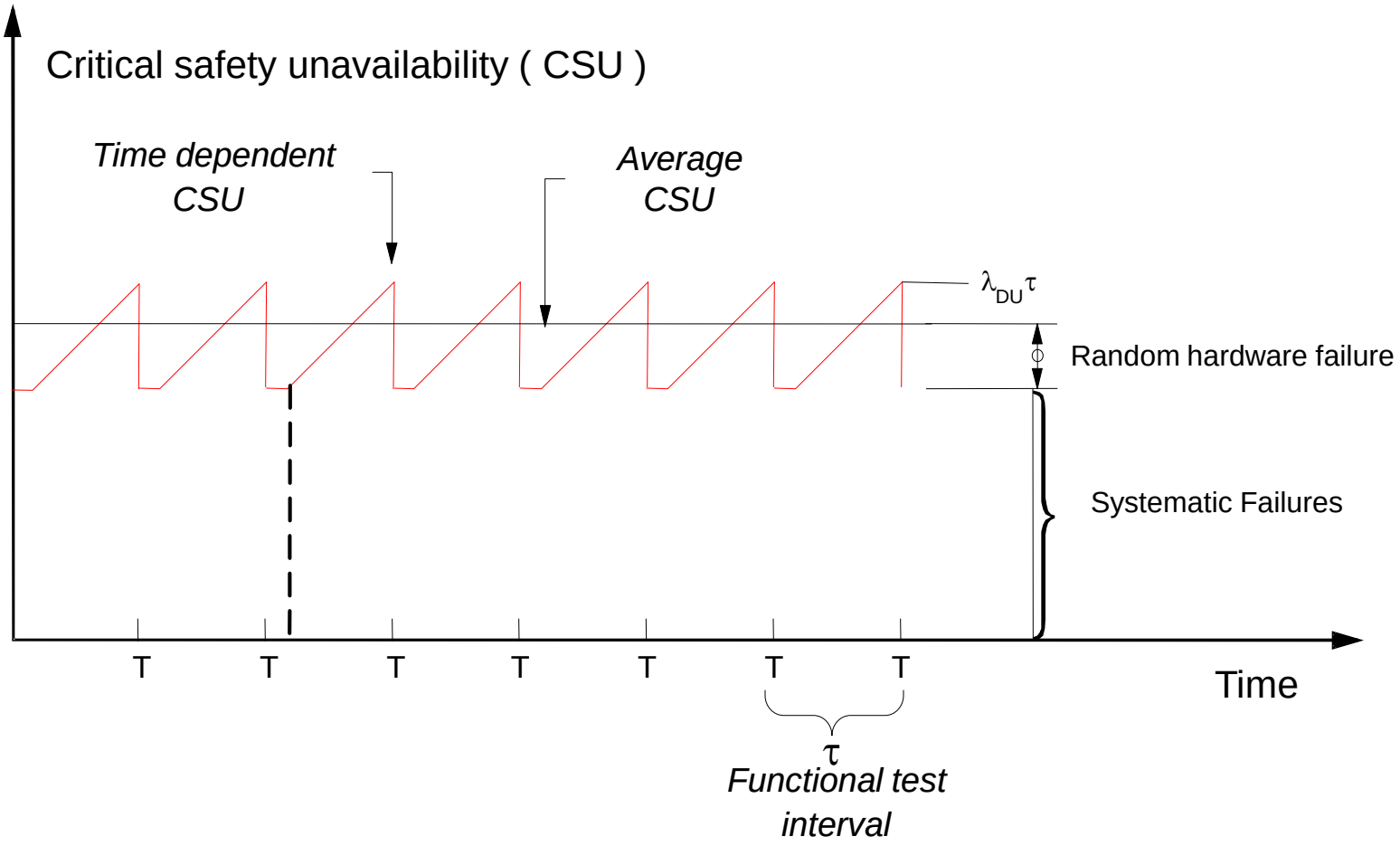
Systematic failures are treated qualitatively by means of checklist



PDS

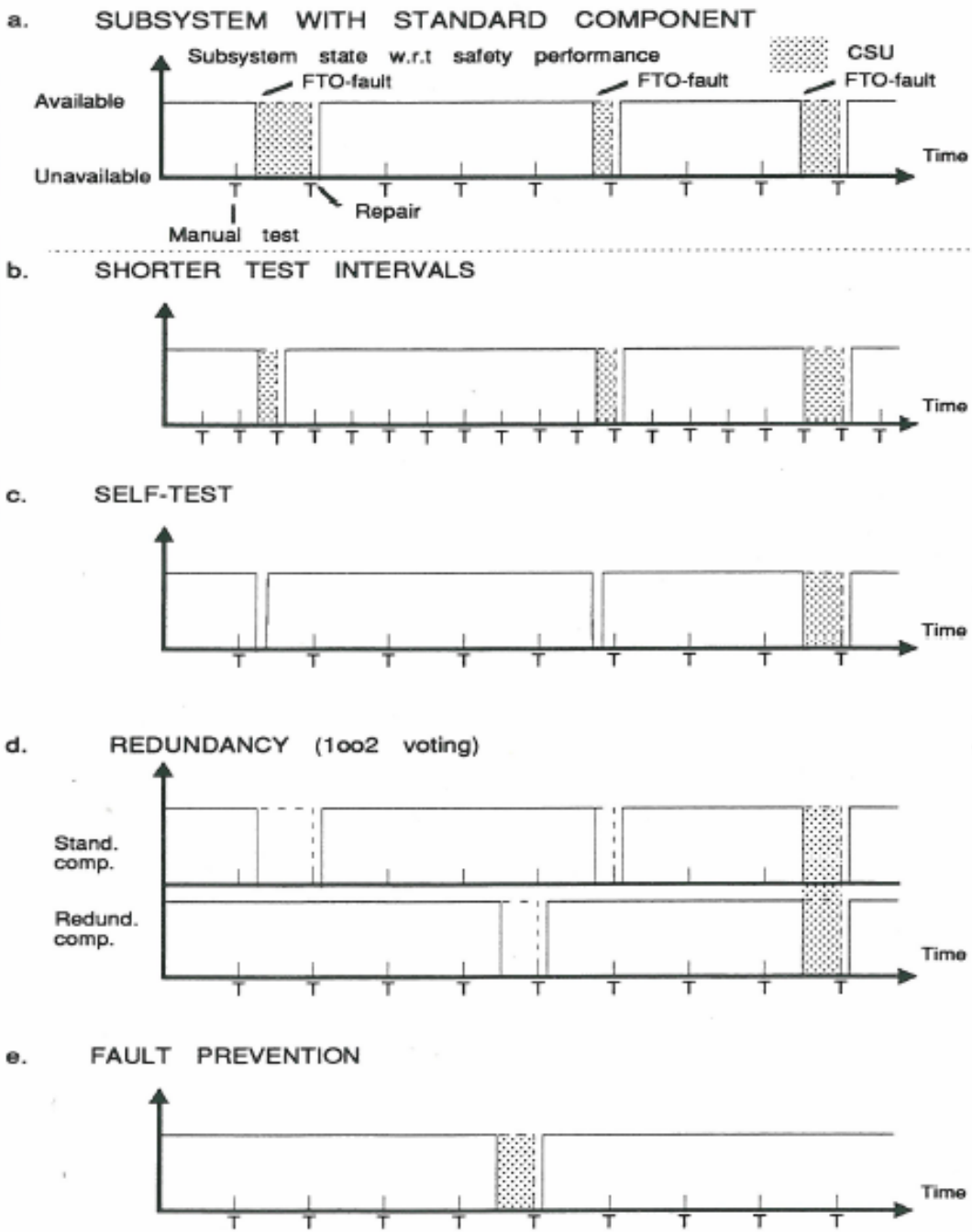
Systematic failures are modelled and quantified as part of the critical safety unavailability

Contributions to CSU



Hvilke tiltak gir økt tilgjengelighet?

Voting	PFD calculation formulas		
	Common cause contribution		Contribution from independent failures
1oo1	-		$\lambda_{DU} \cdot \tau /2$
1oo2	$\beta \cdot \lambda_{DU} \cdot \tau /2$	+	$[\lambda_{DU} \cdot \tau]^2/3$



PDS metoden

Tallfester pålitelighet av instrumenterte sikkerhetssystemer iht IEC 61508

Presenterer forholdsvis enkle beregningsformler med tilhørende/ tilpassede erfaringsdata

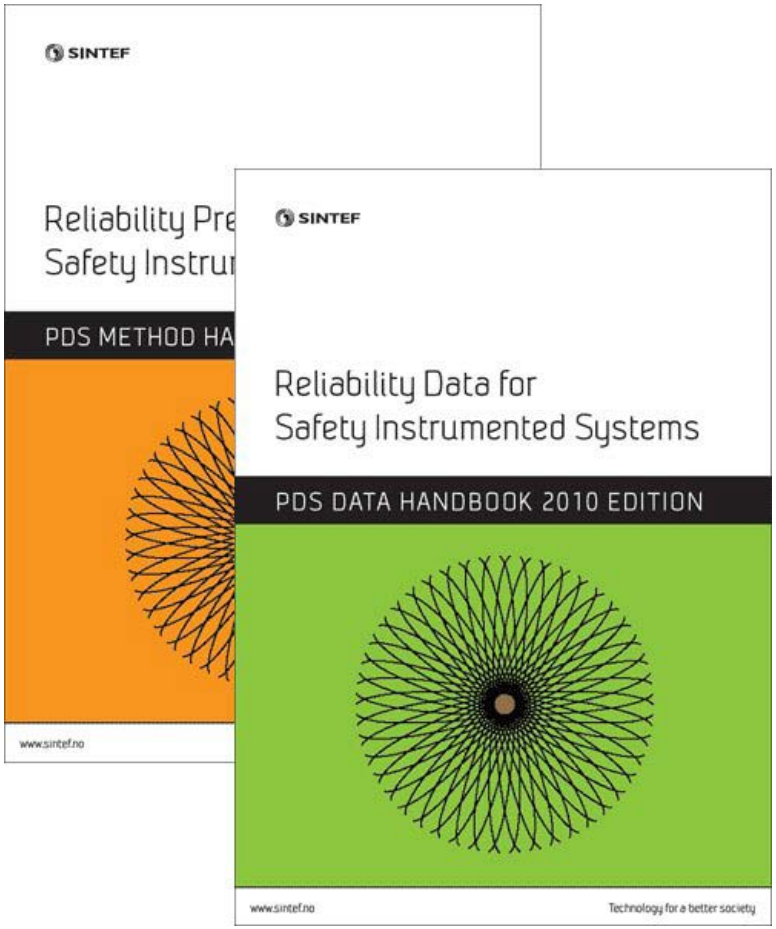
Inkluderer ”alle” realistiske feilårsaker og feilmoder

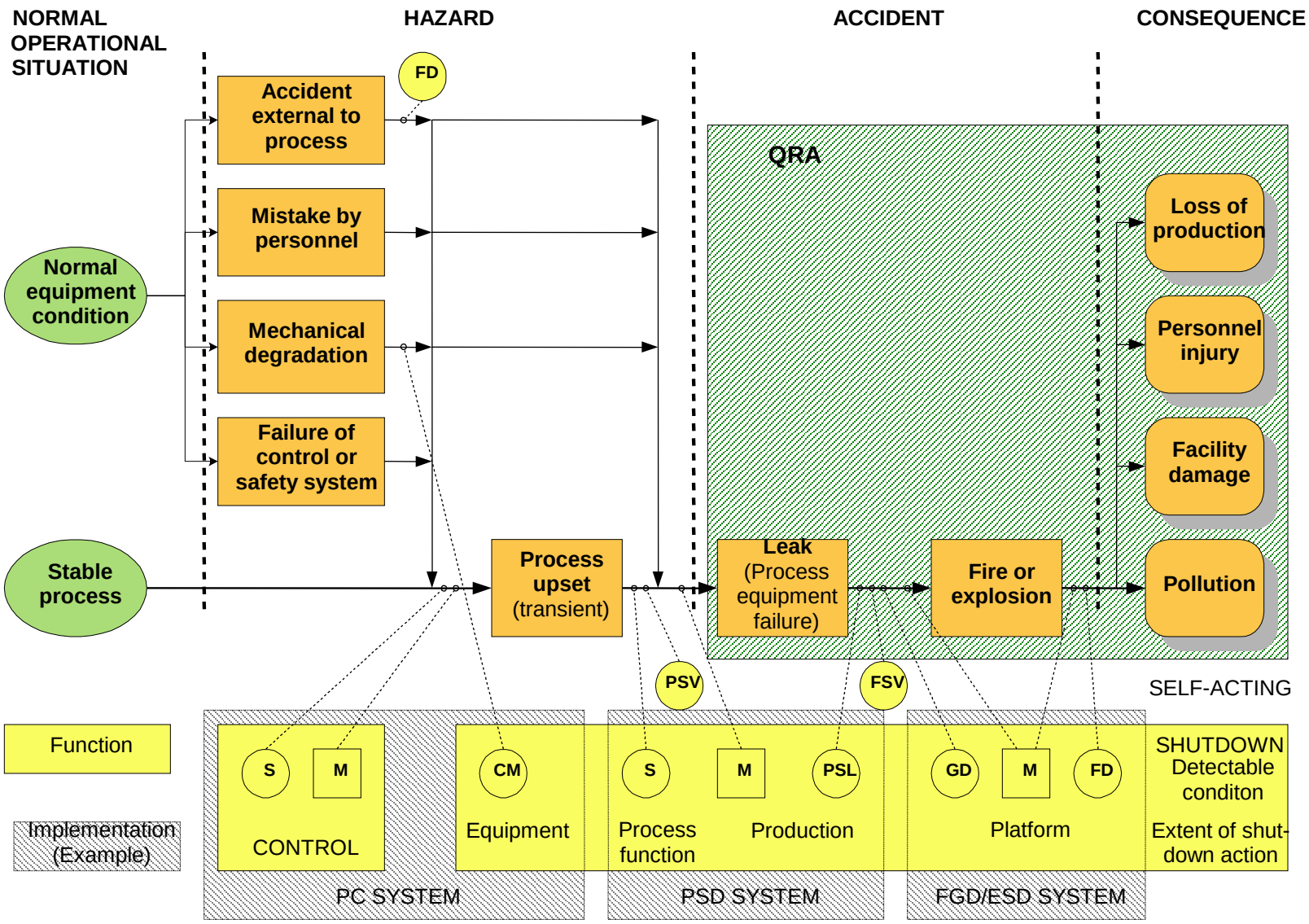
Tallfester også systematiske feil

Tar høyde for ulike typer testing og deteksjonsmåter

Inkluderer hele "sløyfa" (sensor, logisk enhet, ventil)

Tallfester både "Fail-to-operate" og "Spurious operation”



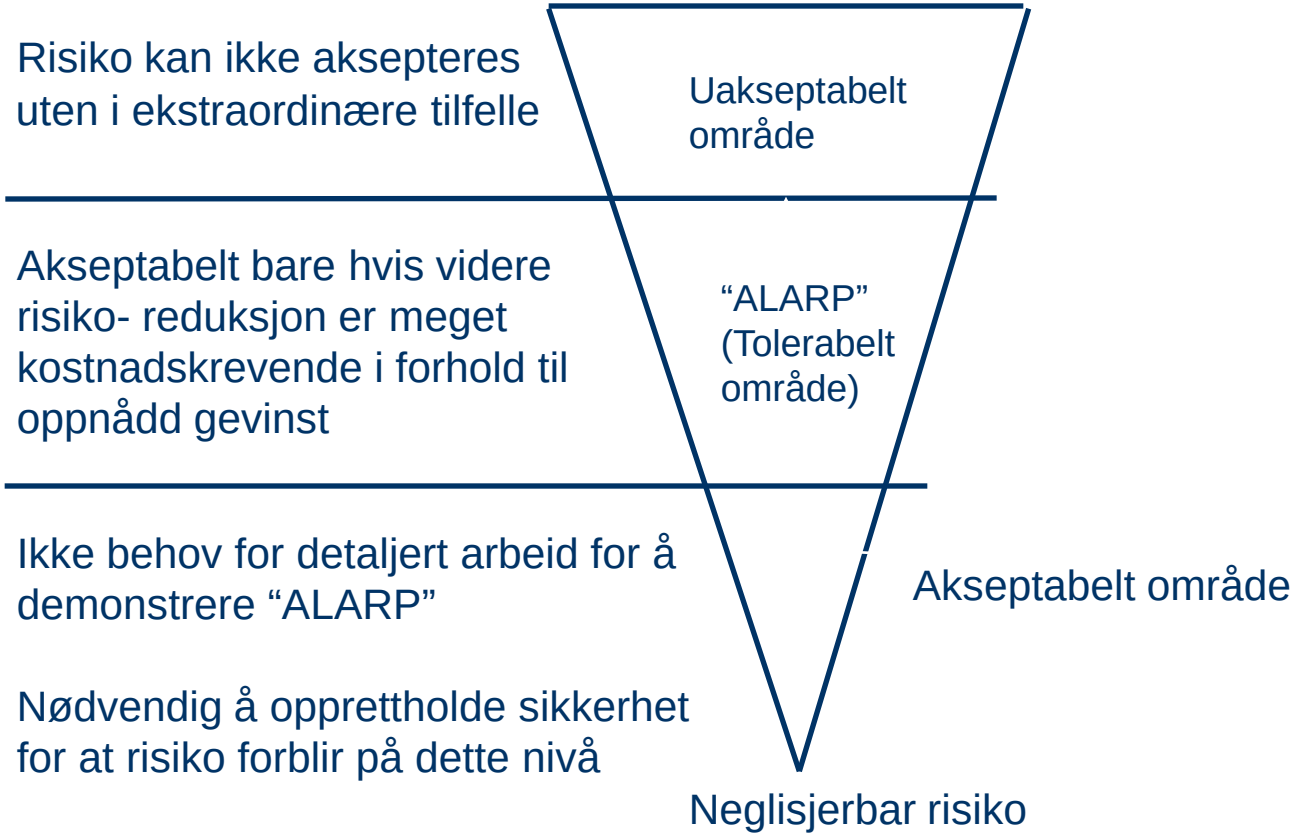


CM:Condition Monitoring, S:Process sensor, PSV:Pressure relief, PSL:Pressure switch low, FSV:Check valve, GD:Gas detector, FD:Fire Detector, M:Manual

API RP14: “Analysis, design, installation and testing of basic surface safety systems for offshore production platforms”

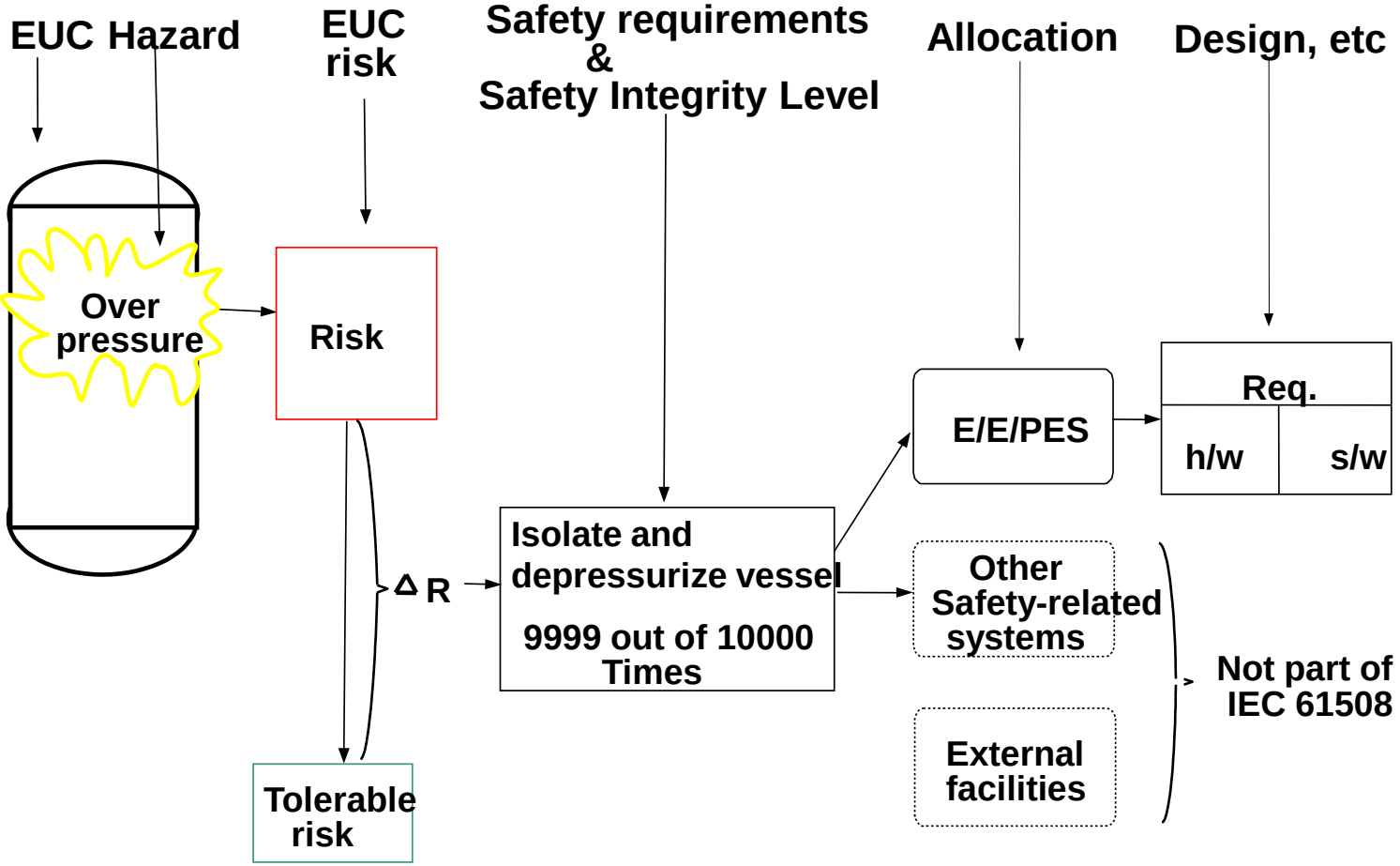
Fra tallfesting til beslutningstøtte for design

ALARP-prinsippet



IEC 61508

Development of Safety System Requirements

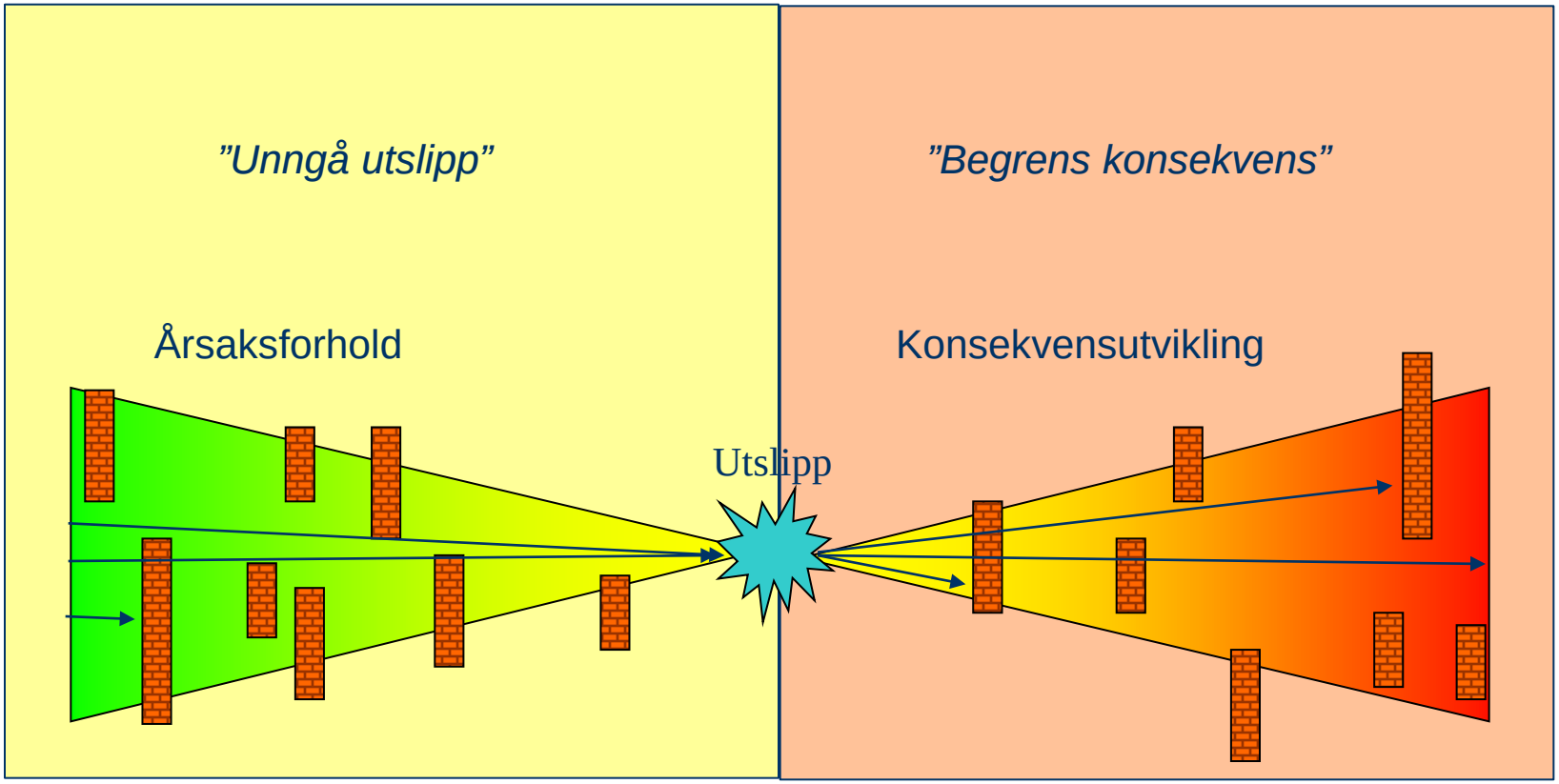


Regjeringens politisk plattform for 2009 – 2013 (Soria Moria 2)

- *”Regjeringen vil styrke overvåknings- og varslingssystemet for havområdene og beredskapen mot forurensning til sjøs”*

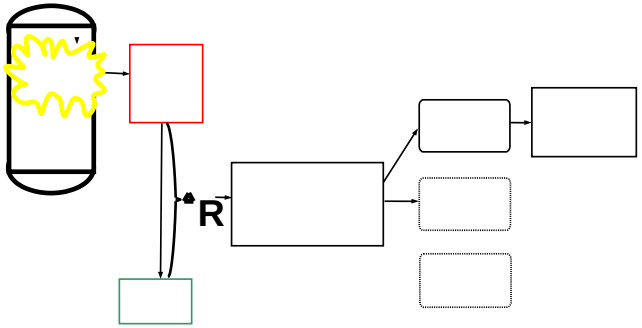
- *”Petroleumsvirksomhet på norsk sokkel skal være verdens fremste i forhold til oljevernberedskap og miljøovervåking”.*

Miljørisikoanalyse



PDS forum
Brukerstyrt innovasjonsprosjekt (2010-2012)

Utvikling av barrierer og indikatorer for å hindre og begrense miljøutslipp til sjø



Energy transfer theory
Gibson & Haddon (1963)

Hazard
(energy source)

Barrier

Victim
(vulernable target)

”Injury results only when there is energy transfer beyond the ability of the body or structure to resist it.”

Barrierefunksjoner

Unngå bruk av farlig energi

Unngå oppbygging av farlig energi

Unngå utslipp av farlig energi

Begrens utslipp av farlig energi

Atskill farlig energi fra sårbart objekt i tid og rom

Isoler farlig energi fra sårbart objekt

Øk objektets motstandskraft

Tilpasset fra Haddon

Petroleumstilsynets Styringsforskrift § 2 omhandler barrierer

Det skal være kjent hvilke barrierer som er etablert og hvilken funksjon de skal ivareta,

samt hvilke krav til ytelse som er satt til de tekniske, operasjonelle, eller organisatoriske elementene som er nødvendige for at den enkelte barrieren skal være effektiv.

Resilience Engineering (RE) – en alternativ tilnærming

Tradisjonell tilnærming	RE- tilnærming
Feil og svikt ses på som unormalt	Feil ses på som en normal variasjon i ulike måter å gjennomføre en arbeidsoppgave på
Ulykker kan forklares gjennom enkle årsakskjeder	Ulykker kan forklares gjennom uforutsette samspilleffekter
Barrierer mot kjente, planlagte hendelsesforløp	Forberede organisasjonen til å takle uforutsette situasjoner
Fokus på hva som kan gå galt – risikoanalyser	Fokus på hva som skaper sikkerhet

Integrated operations

External experts

Service Company's onshore operation centre

External experts

Trondheim

Bergen

Stavanger

Aberdeen

Control room offshore

Real time data

Real time data

Operator's onshore operation centre

* Data integration
* Knowledge
* Information
* Decisions
* Visualisation
* Actions

Remote collaboration room

y Association

www.olf.no

Kilde: OLF

Hvorfor skjer det ikke flere ulykker?

- Vi etablerer og vedlikeholder barrierer,
  - Barrierer er planlagte tiltak for å hindre bestemte hendelsesforløp i å utvikle seg til ulykker
- Vi har evne til å improvisere når det oppstår en situasjon ingen har forutsett
  - Improvisasjon må være basert på **kompetanse**