IEC 61508

Hovedprinsipper og veiledning

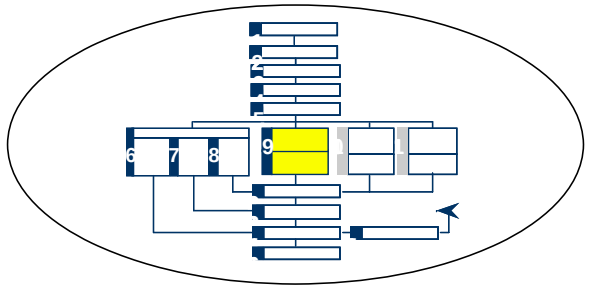
Stein Hauge

SINTEF Teknologiledelse

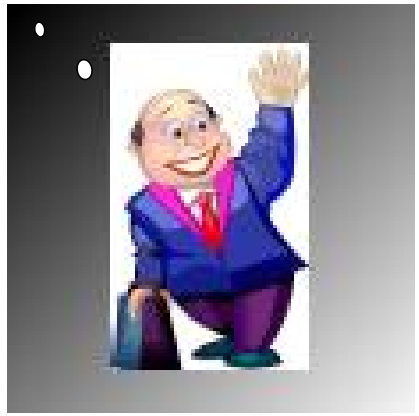
Tlf: 75 17 33 70 / 930 18 395

haustein@online.no / stein.hauge@sintef.no

Bare **måtte** bruke IEC 61508



ELLER?



Aktuell IEC standard

IEC 61508:

Functional safety of electrical/electronic/programmable electronic safety-related systems

Hvorfor bruke IEC 61508 ?

- E/E/PE systemer anvendes mer og mer
- IEC 61508 er en internasjonalt anerkjent standard – leverandører møter krav om bruk av strandarden
- Nasjonale myndigheter anser IEC 61508 som en “beste praksis” for implementering av instrumenterte sikkerhetssystemer (jfr. f.eks. krav i ODs nye forskrifter)
- Bruk av funksjonskrav og risikobasert design øker. Behov for et ”verktøy” som beskriver hvordan en slik risikobasert prosess skal gjennomføres

Noen eksempler på E/E/PE sikkerhetsrelaterte systemer

- Nødavstengningssystem på en oljeplattform
- Brann og gass deteksjonssystem
- DP system for skytteltanker
- Signalsystem for tog framføring
- Automatisk sikker last indikator for kran
- Turtalls kontroll system for en papir-kutte maskin

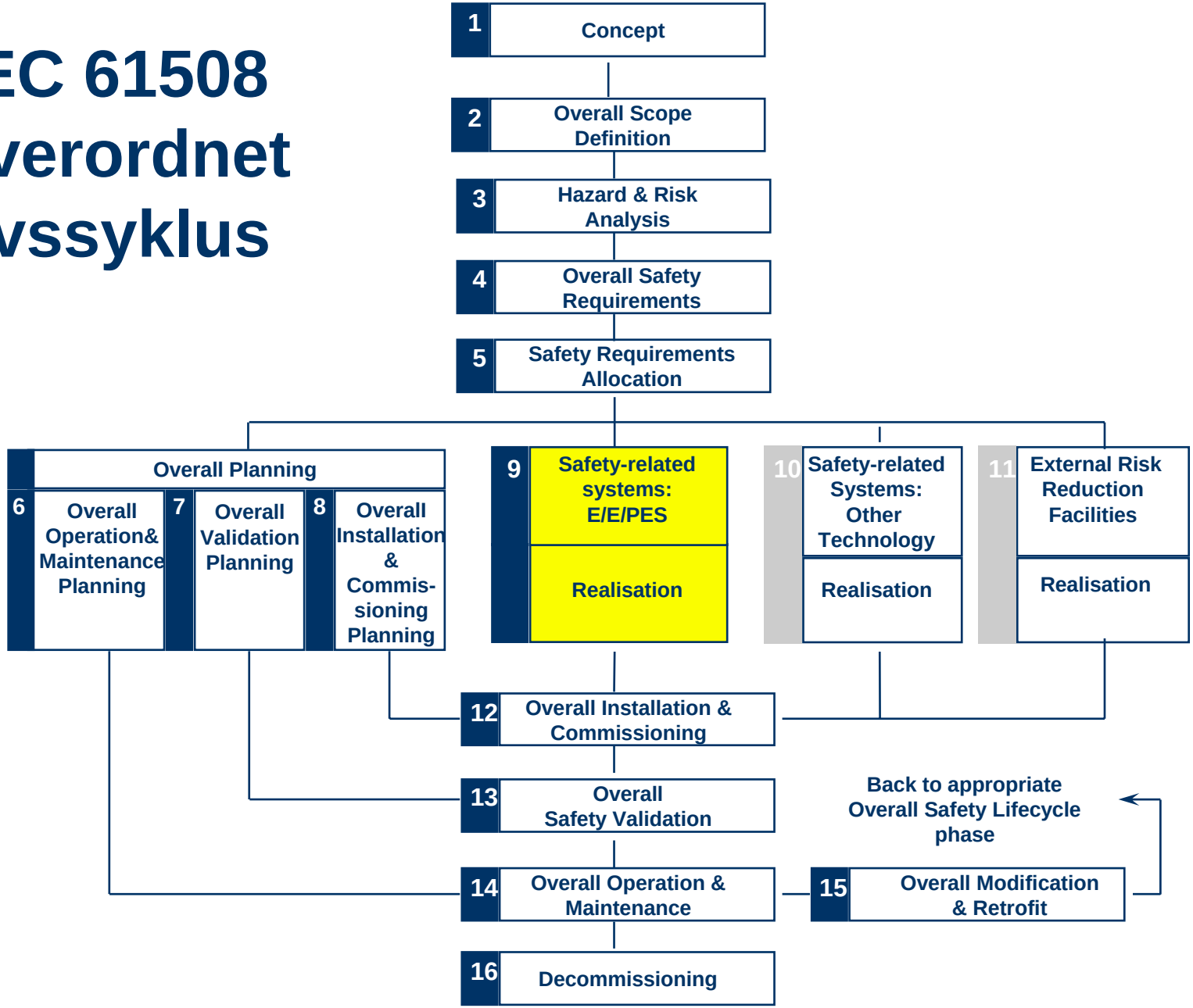
Hovedformål med standarden

Beskrive en (risikobasert) metodikk for å spesifisere og realisere instrumenterte sikkerhetssystemer slik at et akseptabelt nivå av funksjonell sikkerhet oppnås

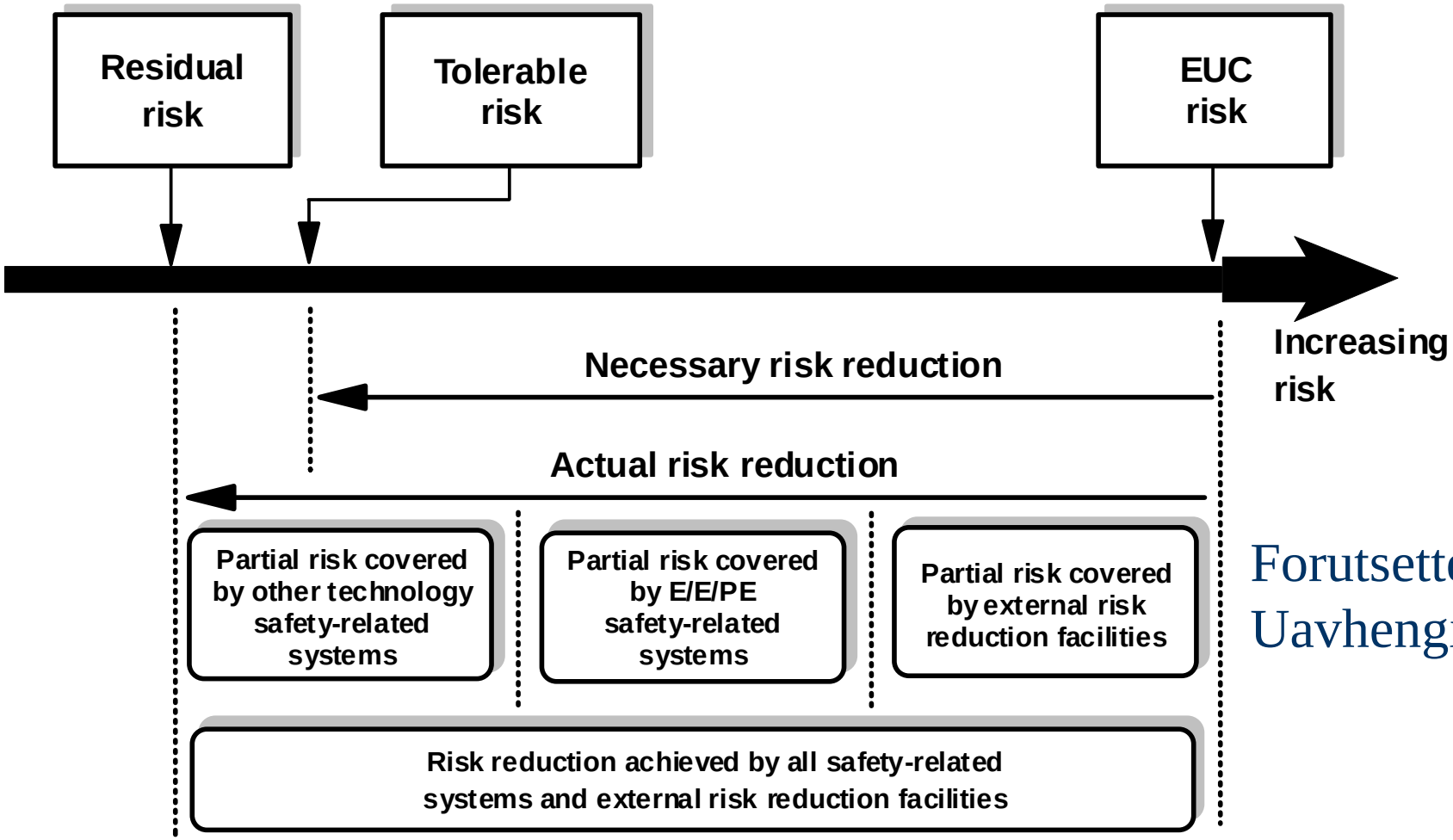
Omfang for IEC 61508

- Generisk standard – dekker ”alle” bransjer
- Dekker E/E/PE/ sikkerhetsrelaterte systemer, men forutsetter at krav også stilles til andre typer sikkerhetssystemer
- Dekker alle livssyklusfasene til sikkerhetssystemene
- Kan anvendes både for systemer som fungerer ved behov (”on-demand”) og kontinuerlige systemer
- Dekker tilfeldige (hardware) feil og systematiske (f. eks. software) feil
- Brukeren setter selv grenser for det systemet / den prosessen (EUC) som skal beskyttes

IEC 61508 Overordnet livssyklus



Risikoreduksjon i IEC 61508



Forutsetter Uavhengighet

Sikkerhetsfunksjoner i IEC 61508

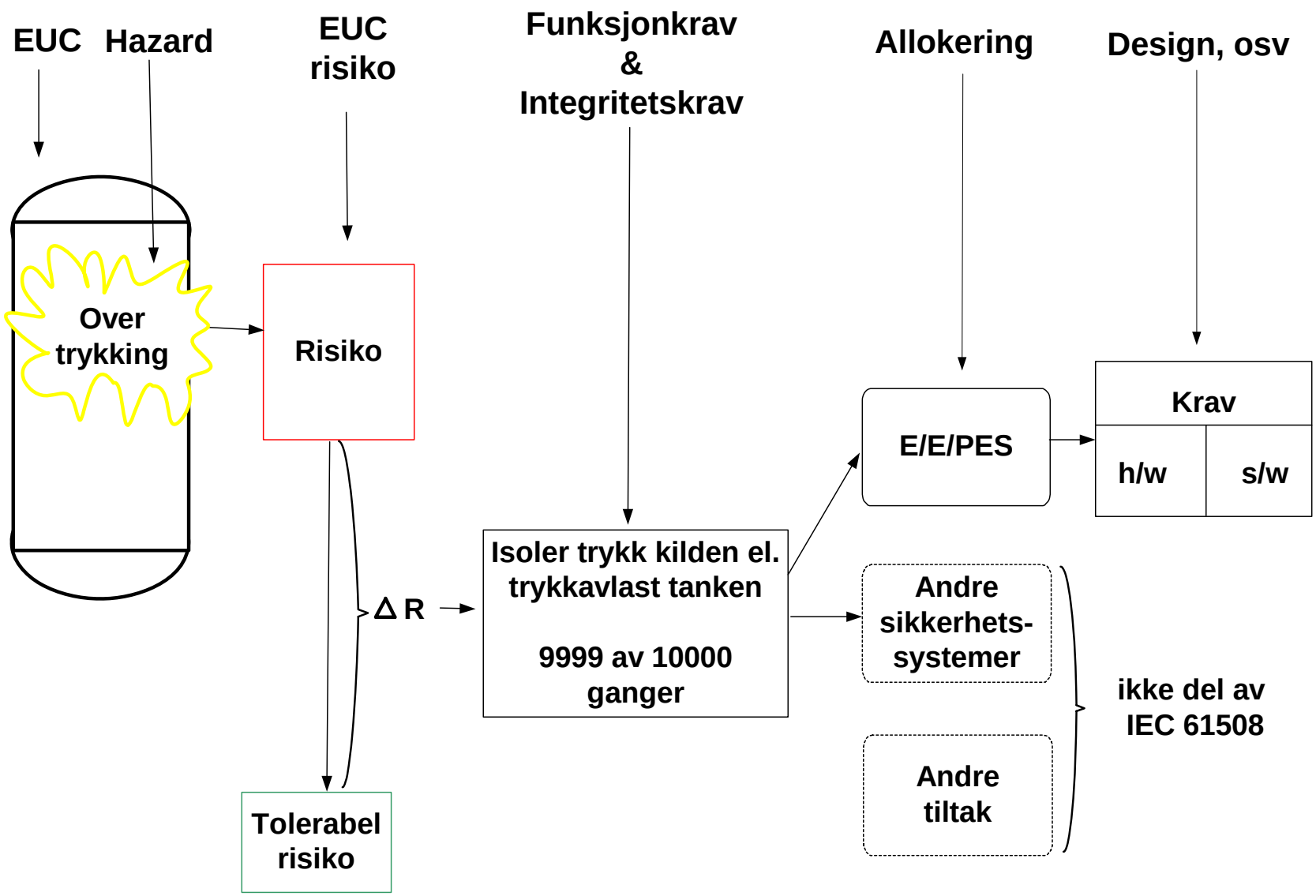
En overordna sikkerhetsfunksjon er en påkrevd ”aksjon” for å sikre at risikoen knyttet til en spesifikk fare er akseptabel

En nøyaktig spesifikasjon av hver sikkerhetsfunksjon i forhold til funksjonalitet og integritet er en grunnpilar i IEC 61508

Implementering av sikkerhetsfunksjoner i IEC 61508

- Instrumenterte systemer (E/E/PES)
  - Sensor/detektor
  - Logikk
  - Aktuator (ventiler, elektriske brytere, osv.)
- ”Other technology systems” kan for eksempel være en trykkavlastningsventil (PSV)
- ”External risk reducing facilities”, kan for eksempel være prosedyrer, en brannvegg, drenering, osv.

Utvikling av sikkerhetskrav i IEC 61508



SIL bestemt av tre typer hovedkrav

- Et kvantitativt SIL krav (gitt som PFD eller feilrate)
- For et gitt SIL krav er det tilknyttet ulike ”hardware arkitektur” krav
- Krav til kontroll med systematiske feil

Kvantitative SIL krav

SAFETY INTEGRITY LEVEL - SIL	DEMAND MODE OF OPERATION (Probability of Failure on Demand - PFD)	CONTINUOUS/HIGH DEMAND MODE OF OPERATION (Probability of a dangerous failure per hour)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

Hardware relaterte SIL krav (på komponent / sub-system nivå)

- Bestemme andelen av sikre feil (Safe Failure Fraction - SFF)
- Bestemme hardware feil toleranse (Hardware Fault Tolerance - HFT)
- Vurdere muligheten for å beskrive alle mulige feilmoder (beskrevet som ”A-type” eller ”B-type” system)

Kombinasjonen av disse tre parametrene avgjør, i tillegg til pålitelighetskravet, hvilket SIL nivå som kan oppnås.

Hardware arkitektur krav i IEC 61508

Safe Failure Fraction	Hardware fault tolerance:					
	0		1		2	
	A	B	A	B	A	B
< 60 %	SIL1	NA	SIL2	SIL1	SIL3	SIL2
60 % - < 90 %	SIL2	SIL1	SIL3	SIL2	SIL4	SIL3
90 % - < 99 %	SIL3	SIL2	SIL4	SIL3	SIL4	SIL4
≥ 99 %	SIL3	SIL3	SIL4	SIL4	SIL4	SIL4

Kontroll med systematiske feil

- IEC 61508 kvantifiserer ikke systematiske feil
- Isteden anbefales bruk av teknikker og tiltak under design for å unngå systematiske feil
- IEC 61508-2 og IEC 61508-3 inneholder tabeller hvor slike teknikker/tiltak er listet for hhv hardware og software utvikling

Andre sentrale krav i IEC 61508

- Ta hensyn til fellesfeil
- Ta hensyn til ”human factors”
- Diverse dokumentasjonskrav (SRS, prosedyrer, planer, osv.)
- Krav til Safety Management aktiviteter (verifikasjon, validering, FSA, osv.)
- Krav til operasjon og vedlikehold
  - Testing av funksjonen med gitt frekvens
  - Oppfølging av SIL krav i drift
  - Kompenserende tiltak i.f.m. svikt eller utkobling

Noen positive sider ved IEC 61508

- Setter fokus på hele livsløpet
- Krever at det skal gjøres systematiske risikovurderinger
- Krever dokumentasjon av hvorfor ting er blitt som de er blitt (jfr. SRS)
- Risikobasert - men inneholder også kvalitative minimumskrav
- Setter fokus på andre forhold som ofte ”neglisjeres”, slik som fellesfeil og menneskelige faktorer, men…..
- Har gitt sikkerhetsdisiplinen et ”redskap” for å kreve pålitelighets-dokumentasjon fra leverandører
- Krever aktiv oppfølging i drift

og noen minus

- Ordrik og omstendelig, behov for veiledninger (jfr. for eksempel OLF guideline 070)
- Mange fortolkningsmuligheter, eks:
  - Hvordan ta høyde for ”human factors”
  - Hvordan beregnes SFF
- Fordyrende?
- Riktig tilnærming for alle industrier og for alle typer ulykker?

IEC 61508 – keiserens nye klær eller svaret på alt vi lurte på ?