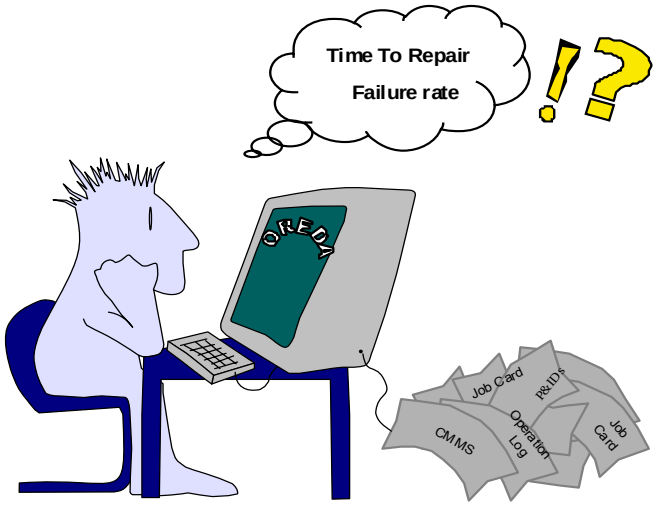
”Erfaringsbaserte datakilder”

IEC 61508 seminar, Sandefjord 04. mars 2008

Stein Hauge, SINTEF

Jeg skal snakke om:

1. Innledning – litt generelt om feildata
2. Eksempler på datakilder
3. Hvordan etableres anbefalte feildata?
   - Et eksempel
4. Hvor usikre er tallene?
5. Kort om oppfølging i drift
   - Et eksempel



Del 1

Innledning – generelt om feildata

“Experience data is what makes you able to recognize a mistake when you do it again”

Hvorfor trenger vi feildata ?

- Til bruk i ulike pålitelighets- og risikoanalyser
- I designfasen som input til valg av ”riktig” utstyr med god nok pålitelighet
- For å overvåke trender og kunne gjøre sammenligninger (“Benchmarking”)
- Kunne gi tilbakemelding til utstyrleverandører ang. ytelse på utstyret
- For å systematisere operativ erfaring og følge opp ytelseskrav i drift
- For å overholde krav fra myndighetene

Noen relevante forskriftskrav

- Styringsforskriften §18:

  Den ansvarlige skal sikre at data blir samlet inn, bearbeidet og brukt til å:

  a) overvåke og kontrollere tekniske, operasjonelle og organisatoriske forhold,
  b) utarbeide måleparametere, indikatorer og statistikk,
  c) utføre og følge opp analyser i ulike faser av virksomheten,
  d) bygge opp generiske databaser,
  e) sette i verk korrigerende og forebyggende tiltak, deriblant forbedring av systemer og utstyr.

- Innretningsforskriften §7:
  - Det skal fastsettes krav til ytelsen for sikkerhetsfunksjoner.

Eksempler på behov for data iht. IEC 61508

- Hva (hvilken komponent) har feilet ?
- Type feil - Dangerous (D) eller Safe (S) feil ?
- Hvordan er feilen oppdaget ? (DD, DU, SU, SD)
- Årsaken til feilen (”Failure cause”)
- Hyppighet av fellesfeil
- Antall aktiveringer (”demand rate”)

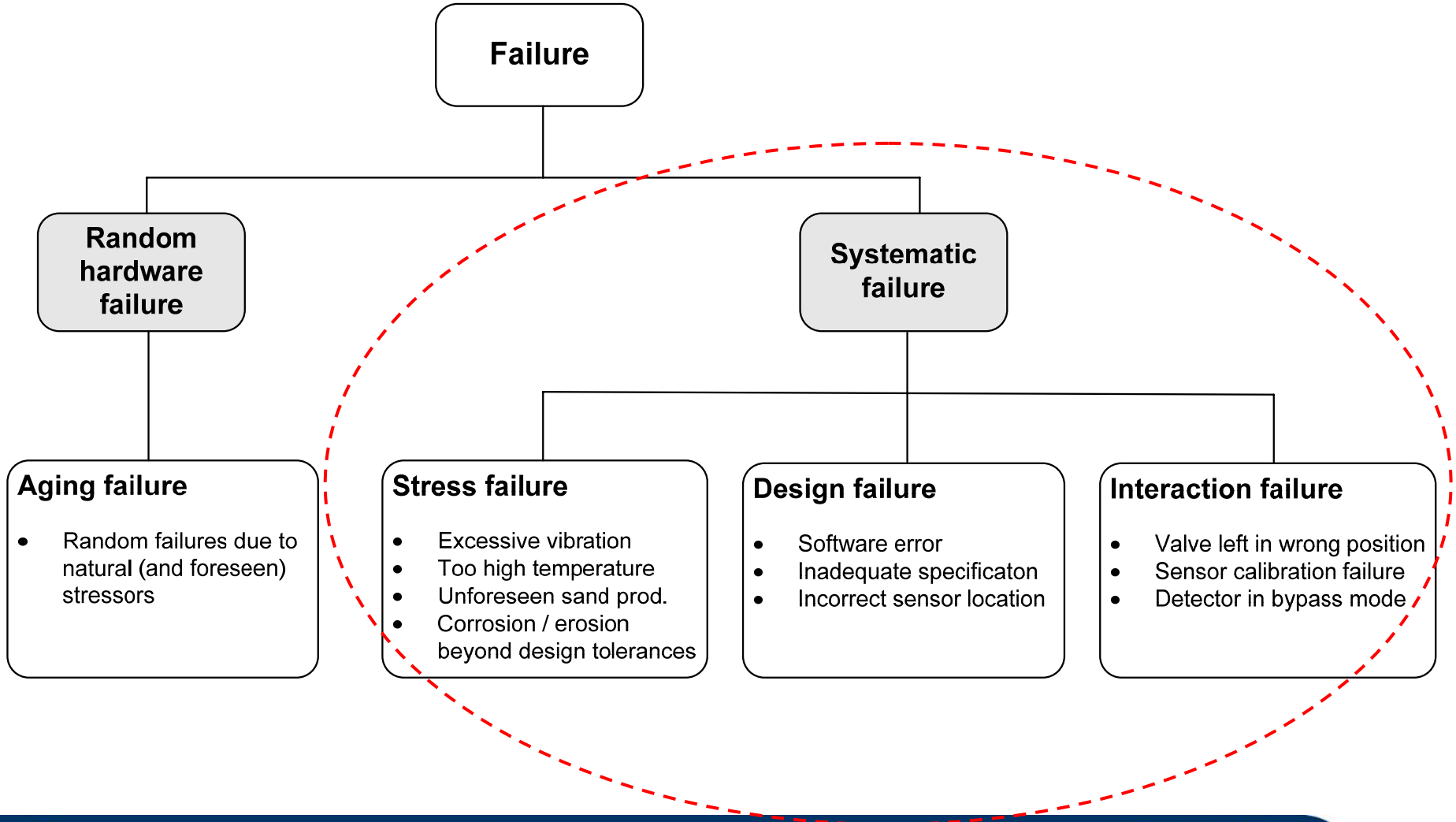
Utfordringer / forhold å ta hensyn til

- Datainnsamling er tids- og ressurskrevende
- Viktig med entydig definisjon av system/utstyrsgrenser - hva er egentlig inkludert i tallene?
- At det er tilstrekkelig antall data (populasjon) til at man kan trekke fornuftige konklusjoner (konfidensintervaller)
- Sporbarhet - det skal være mulig å spore dataene tilbake til kilden

Noen ”paradokser”

- Vi ønsker *ingen feil* men *mye feildata*
- Erfaringsdatabaser er per definisjon ‘gamle’ data – hva med nytt utstyr?
- Jo mer vi spesifiserer/avgrenser utstyret, jo mindre (relevante) data finnes
- Leverandør-/sertifikatdata for feilrater er ofte en tierpotens (eller mer) bedre enn generiske data – hvorfor?

Hvilke feil er inkludert?



Hvorfor inkludere også de systematiske feilene?

- Systematiske feil er ofte en hovedbidragsyter inn mot feilsannsynligheten til utstyret
- Når vi gjør pålitelighetsberegninger ønsker vi gjerne å predikere hvordan utstyret faktisk kommer til å oppføre seg “i felt”
- Tilsvarende i QRA er det viktig å bruke realistiske feilsannsynligheter for å reflektere den faktiske risikoen
- Systematiske feil er normalt inkludert i erfaringsdata!
- På dette området er IEC 61508 uklar!

Del 2

Eksempler på datakilder

Eksempler på datakilder

- OREDA® håndbøker / database (N)
- PDS datahåndbok (N)
- RNNS (N)
- EXIDA Safety Equipment Reliability Handbook (US)
- OGP forum (UK)
- T-book (S) / EiReData (F)
- FARADIP.THREE (UK)

Ulike typer datakilder

Type data	Eksempel på datakilder
Anleggsspesifikke data	Eksempel: Manuelle logger, driftsoppfølgingsrapporter, OREDA databasen, SAP, Synergi, osv
Leverandør-/utstyrsspesifikke data	OREDA databasen, EXIDA håndbok, leverandørdata
Generiske data - Industrispesifikke vs. mer generelle	OREDA håndbøker/database, PDS datahåndbok, EXIDA håndbok, FARADIP.THREE
Selskapsspesifikke	Selskapenes egne anbefalte datasett

Del 3

Etablering av feilrater – et eksempel

PDS datahåndboka - kilder / input

- OREDA® databasen fase III, IV og V og OREDA® håndbøker
- Data fra RNNS for sikkerhetskritisk utstyr
- Diskusjoner og samtaler med fagfolk, samt egne (SINTEF) vurderinger
- Andre datahåndbøker

Eksempel: Etablering av feilrate for ESV/XV

- Data fra OREDA fase IV & V (samlet inn i perioden 1994-1999)
- 140 ventiler fra 7 ulike installasjoner
- Total operasjonsperiode: 4.631.440 timer (i snitt ca 3.8 år per ventil)
- Antall observerte kritiske feil (feil på pilotventil ikke inkludert): 16
- Dette gir en λ_{crit} = 16 / 4631440 timer= $3.45 \cdot 10^{-6}$ / time
- Må se på fordeling av feilmoder

Etablering av feilrate for ESV/XV (2)

Failure mode	Detection method	#
Delayed operation	Continuous condition monitoring	1
Delayed operation	Periodic preventive maintenance	1
External leakage - Utility medium	Continuous condition monitoring	1
Fail to close on demand	Casual observation	2
Fail to close on demand	Continuous condition monitoring	1
Fail to close on demand	On demand	1
Fail to close on demand	Other method	2
Fail to close on demand	Production interference	1
Fail to open on demand	Other method	3
Spurious operation	Continuous condition monitoring	1
Spurious operation	Production interference	1
Structural deficiency	Production interference	1

Etablering av feilrate for ESV/XV (3)

- Antall vurderte farlige feil (D): 9 stk
- Dette gir: $\lambda_D = 9 / 4631440$ timer$= 1.9 \cdot 10^{-6}$ / time
- Antall feil som er detektert på anna måte enn ved testing eller on-demand (DD) er anslått til: 2 stk
- $c_D = 2/9 = 0.22$
- Og dermed: $\lambda_{DU} = 7 / 4631440$ timer$= 1.5 \cdot 10^{-6}$ / time

Etablering av feilrate for ESV/XV (4)

- Dataene over inkluderer ikke feil på pilot / ventilstyring
- Erfaringer fra RNNS for stigerørs ESVer gir en feilrate på omtrent $2.4 \cdot 10^{-6}$ per time når en antar 1 års testintervall
- For de anbefalte ESV/XV feilratene i PDS håndboka er det i tillegg brukt data fra andre faser av OREDA
- Anbefalt λ_{DU} feilrate i PDS håndboka for komplett ESV/XV ventil er $2.9 \cdot 10^{-6}$ per time (som med årlig testing gir en PFD på omtrent 0.01)

“The probability is extremely small – actually it is less than zero”

Del 4

Hvor usikre er tallene vi bruker?

Hvorfor er tallene usikre?

- Usikkerhet knyttet til datainnsamling - feilrapportering, klassifisering og tolkning av data
- Feilrater er sterkt avhengig av driftsmiljø og av vedlikeholdsaktiviteter - variasjon mellom installasjoner/anlegg hvor dataene er samlet inn
- Relevans av data – hva er inkludert i tallene og hvilke forutsetninger ligger til grunn?
- Mengde data: tilstrekkelig populasjon til at man kan trekke fornuftige konklusjoner (konfidensintervall)

Generelt om usikkerhet

Studier av data fra ulike industrier (forsvar, telekommunikasjon og prosess) indikerer følgende:

En kan være 90% sikker på…	**…at den endelige feilraten vil være BEDRE enn:**
Anleggsspesifikke data	2 ½ ganger den estimerte
Industrispesifikke data	4 ganger den estimerte
Generiske (flere bransjer) data	6 ganger den estimerte

(Kilde: Smith & Simpson, 2001)

70% krav til konfidens av anvendte feilrater

IEC 61508-2, section 7.4.7.4, point a)

- NOTE 1: *Any failure rate data used should have a confidence level of at least 70 %....*

IEC 61511-1, section 11.9.2, point c)

- NOTE: The estimated rates of failure of a subsystem can be determined by ….. or from experience of the previous use of the subsystem in the same environment as for the intended application, *and in which the experience is sufficient to demonstrate the claimed mean time to failure on a statistical basis to a single-sided lower confidence limit of at least 70 %.*

Eksempel med ESV/XV - usikkerhet

- 90% konfidensintervall for anbefalt $\lambda_{DU} = 2.9 \cdot 10^{-6}$ / time *dersom alle dataene kom fra en installasjon*:

  $[1.7 \cdot 10^{-6}$ / time , $4.6 \cdot 10^{-6}$ / time$]$

- 90% konfidensintervall for anbefalt $\lambda_{DU} = 2.9 \cdot 10^{-6}$ / time dersom dataene som i vårt tilfelle kom fra 7 ulike installasjoner, kan for eksempel være:

  $[0.3 \cdot 10^{-6}$ / time , $7.5 \cdot 10^{-6}$ / time$]$

- En kan i dette tilfelle være 70% sikker på at feilraten (λ_{DU}) vil være mindre enn:

  $3.6 \cdot 10^{-6}$ / time

Del 5

Kort om oppfølging i drift

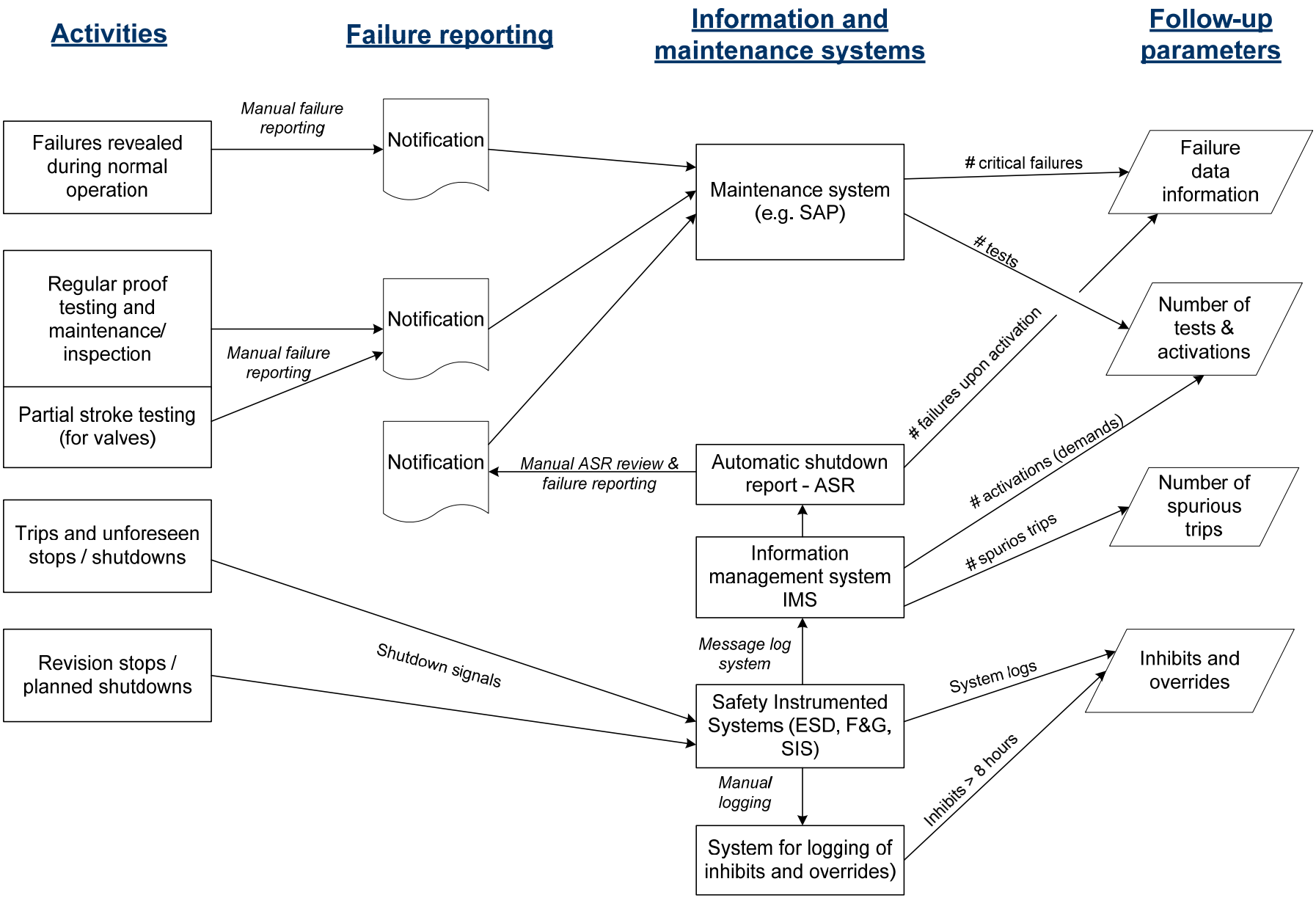
Oppfølging av SIL krav i drift

- Få verifisert at antagelser og føringer fra design som ligger til grunn for operasjon, testing og vedlikehold oppfylles i driftsfasen
- Med andre ord: de tallene som er brukt for å verifisere designen bør være utgangspunktet for oppfølging i drift
- God / detaljert feilrapportering og påfølgende klassifisering av feil blir helt sentralt
- Alle sikkerhetsfunksjoner med SIL krav skal følges opp

Oppfølging i drift (forts.)

- Et anlegg består ofte av flere hundre ulike looper / sikkerhetsfunksjoner
- Svært utfordrende å følge opp SIL krav på enkeltfunksjonsnivå
- *Men*: dersom en ”har kontroll” med hver enkelt utstyrsgruppe kan en anta at en også har kontroll med totalen
- Utfordrende å holde oversikt over all tilgjengelig informasjon om utstyrsfeil – ulike kilder

Informasjonskilder - drift



Hva skal en måle mot ? - valg av ytelsesindikator

- Failure fraction (*FF*) er en mye brukt ytelsesindikator. Denne er definert som: *FF* = # feil / # aktiveringer
- I praksis brukes ofte antall tester i nevneren (som i RNNS)
- *Men*:
  - Ofte brukes faste verdier/mål for *FF* som ikke nødvendigvis er knyttet opp mot antatte feilrater i design
  - *FF* er avhengig av lengden på testintervallet – hva dersom komponenter har ulike testintervall?
  - Må holde telling med antall aktiveringer (inkludert tester, faktiske aktiveringer, nedstengninger, # partial stroke tester, osv.)
  - Og hva med feil avdekket på andre måter (som i normal drift)?
- *Bedre*: ta utgangspunkt i feilraten λ_{DU} (fra design), beregn forventet antall feil for en gitt populasjon og bruk dette som en oppfølgingsparameter (uavhengig av antall aktiveringer)

Oppfølging i drift – et enkelt eksempel

- Ser på et eksempel med 600 røykdetektorer på et spesifikt anlegg.
- Antatt feilrate fra design er: $\lambda_{DU} = 0.8 \cdot 10^{-6}$ / time
- Forventet antall feil X for n komponenter i løpet av en observasjonsperiode t er da gitt som: $E(X) = \lambda_{DU} \cdot t \cdot n$
- For de 600 detektorene kan en da for eksempel i løpet av *ett år* forvente følgende antall feil: $E(X) = 0.8 \cdot 10^{-6} \cdot 8760 \cdot 600 \approx 4$ feil
- Si at en erfarer 3 feil på 2 år. Da vil et estimat for *erfart feilrate* være:

$$\hat{\lambda}_{DU} = 3 / (600 \cdot 8760 \cdot 2) \approx 0.3 \cdot 10^{-6} \text{ / time}$$

- Ved å sammenligne erfarte antall feil mot forventet antall feil, eller alternativt erfart feilrate mot antatt feilrate kan en konkludere ift. hvorvidt observert ytelse er akseptabel eller ikke.
- Denne informasjon kan brukes videre ifm. en vurdering av lengde på testintervallet

Kort oppsummert

- Det er krav til innsamling og bearbeiding av data - både som en følge av regelverk og fra IEC standarder
- Utvalget av datakilder er delvis begrenset og mengden (relevante) data reduseres kraftig etter hvert som en ønsker å spesifisere/avgrense utstyret
- Viktig å være klar over hva som er inkludert i feilratene som benyttes
- Feildata er generelt sett beheftet med større usikkerhet enn det som ligger i en ytterligere raffinering av selve pålitelighetsmodellen
- Det bør etableres en logisk kobling mellom oppfølgingsparametrene i drift og de antatte feilratene fra design – da det er disse som ligger til grunn for de verifiserte SIL kravene!

Takk for meg!