

Introduksjon til pålitelighetsanalyse

Jørn Vatn

NTNU

jorn.vatn@ntnu.no

Pålitelighet av hva?

- Komponent- og systempålitelighet
 - Fokus i denne presentasjonen
 - Terminologi
 - Metoder og modeller
- Strukturpålitelighet
 - Last-styrke modeller
- Menneskelig pålitelighet
- Programvarepålitelighet

Pålitelighet

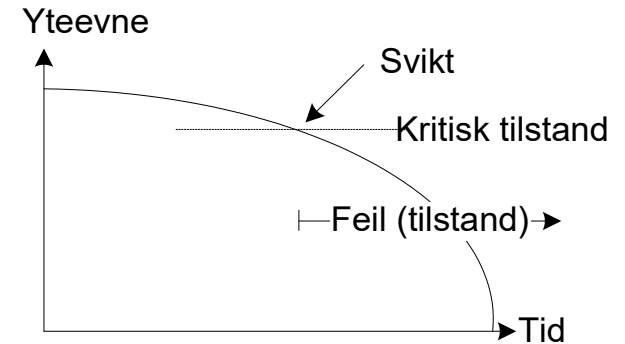
- En enhets evne til å utføre en påkrevd funksjon, under gitte miljø- og operasjonelle betingelser for en gitt tidsperiode
- Merk: man benytter også ordet
 - Driftssikkerhet = Evnen (egenskapen) til et system til å utføre sin tiltenkte funksjon over en gitt tidsperiode, under gitte forhold uten prestasjonsnedsetting pga feil/svikt og vedlikehold

Hvordan kvantifisere pålitelighet?

- Midlere tid til feil (MTTF)
- Antall feil per tidsenhet (feilrate)
- Sannsynligheten for at en enhet ikke svikter i et gitt tidsintervall $(0, t]$ (overlevelsessannsynlighet)
- Sannsynligheten for at enheten kan utføre tiltenkt funksjon ved tid t (tilgjengelighet)

Feil og feilklassifisering

- Merk forskjell på engelsk og norsk
 - Failure = Svikt (dvs tidspunkt/hendelse)
 - Fault = feil(tilstand)
- Svikt = Opphør av mulighet til å utføre krevd funksjon
- Feilmode (feilmodus) = effekten av en svikt slik den observeres på enheten som har sviktet (sett utenfra)



Kommentarer til feilmodebegrepet

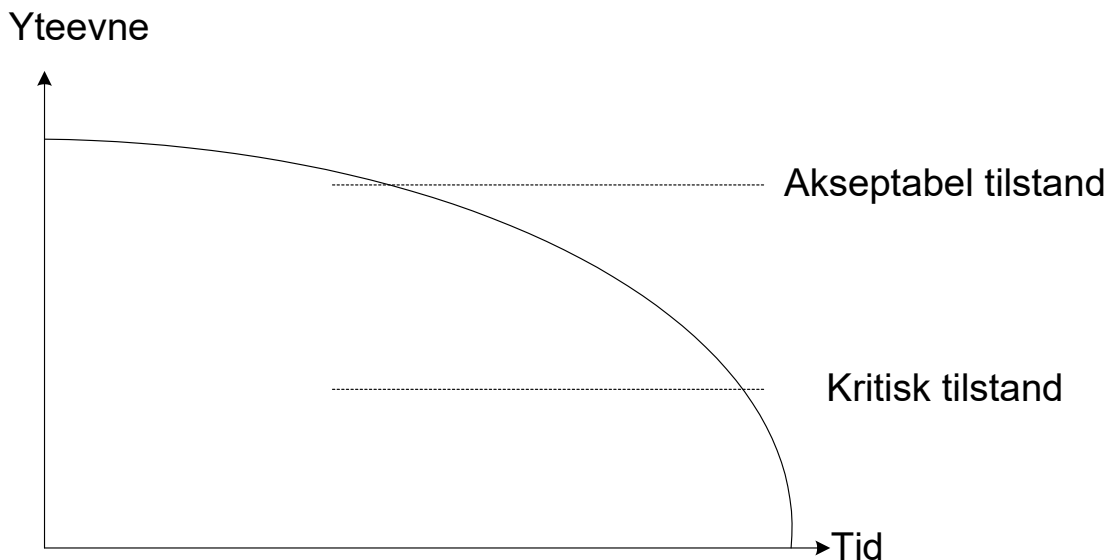
- Dersom man er eksplisitt på funksjons-angivelse kan man ha få feilmoder, i motsatt fall har man ofte flere feilmoder
- En del fremstillinger benytter begrepet (teknisk) feilmode om det vi her vil kalle feilårsak

Klassifisering av svikt

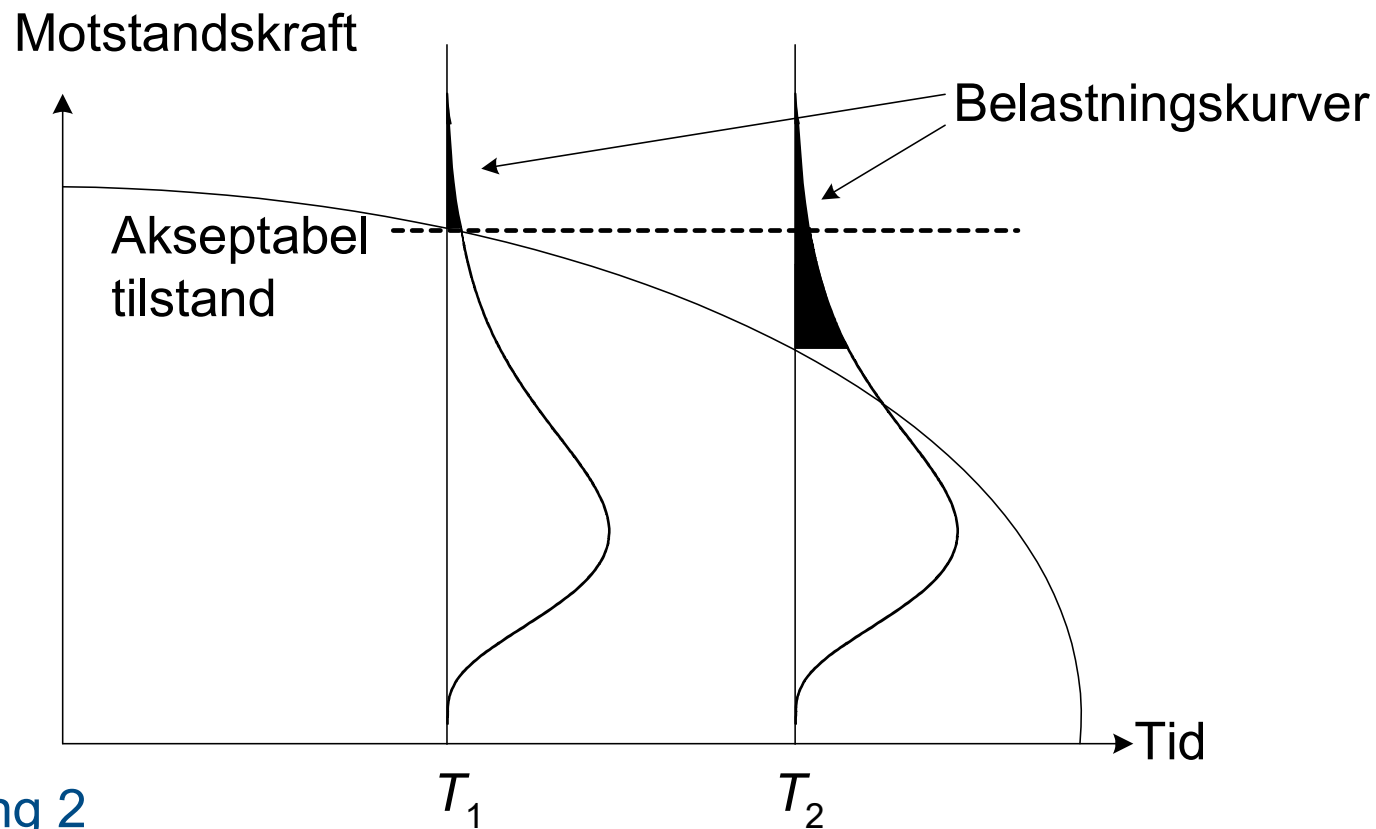
- Plutselig $\leftrightarrow$ gradvis svikt
 - "Plutselig" relateres oftest til virker/virker ikke
 - "Gradvis" relateres ofte til enheter som har en ytelse, eller enheter som har "målefunksjon"

- Øving 1

- Gi eksempler på "Plutselig"
- Gi eksempler på "Gradvis"



Gradvis svekket ytelse, tilfeldig belastning



Øving 2

Finn eksempler på gradvis svekket ytelse og tilfeldig belastning

Klassifisering, forts.

- Skjult $\leftrightarrow$ åpenbar feil
 - "Skjult" relateres ofte til enheter som ikke etterspørres kontinuerlig
 - Åpenbar relateres enheter som etterspørres kontinuerlig, og svikt blir avdekket umiddelbart
- Øving 3
 - Gi eksempler på "Skjult" funksjon
 - Gi eksempler på "Åpenbar" funksjon

Mer om skjult ↔ åpenbar feil

- Noen funksjoner er ikke åpenbar hele tiden, men kan verifiseres f eks ved oppstart (håndbrems på en bil) → åpenbar ved "uttak/oppstart"
- Noen funksjoner er skjult, men feil i funksjonen kan avdekkes ved f eks "selvtest", typisk for detektorsystemer
 - "Partial stroke test" er en test som avdekker noen feilårsaker, f eks ved å bevege på en ventil kan man avdekke om ventilen har "hengt seg opp", men man kan ikke finne ut om den vil holde tett i lukket posisjon
- Noen funksjonsfeil vil først bli åpenbar etter en stund
 - Svikt i en pumpe som skal holde trykket oppe i en oljetrykktank
 - Et filter som går tett vil gi systemeffekter etter en stund
- Noen funksjoner på komponentnivå er skjult, mens de på systemnivå er åpenbar
 - F eks dersom vi trenger 3-ut-av-4 bolter for å holde en struktur oppe
 - Det er åpenbart når strukturen faller ned, men det er ikke åpenbart om en bolt løsner.

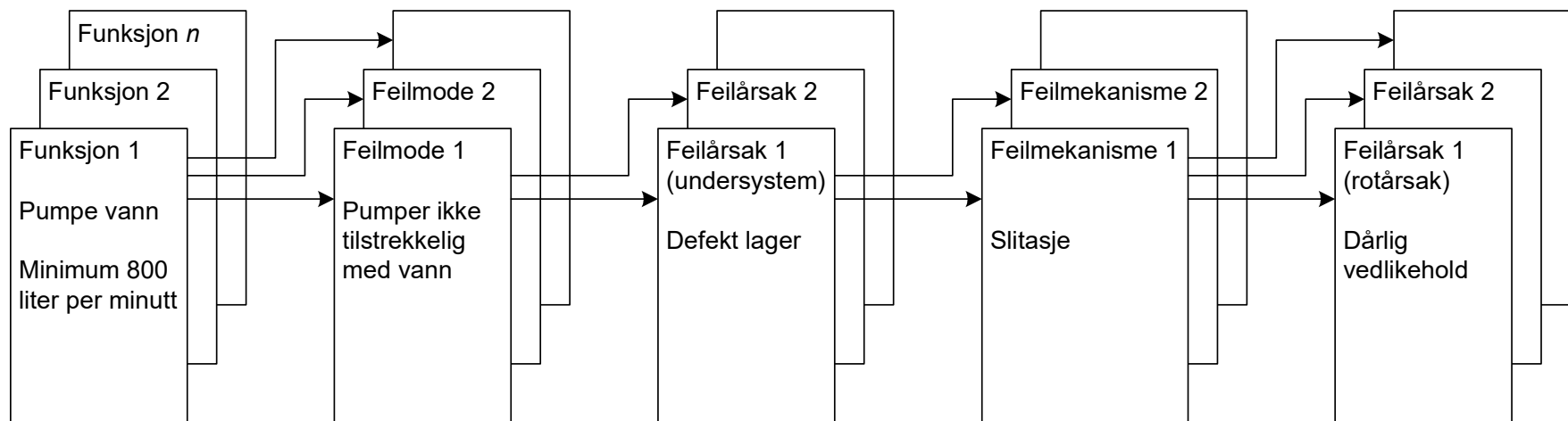
Klassifisering, forts.

- Fysiske $\leftrightarrow$ funksjonelle svikt (feil)
 - Fysiske feil kan elimineres ved reparasjon, evt skifte av fysisk enhet
 - Naturlig aldring (innenfor design område)
 - Eksternt påtrykk
 - Funksjonelle feil relateres til feil design, feil plassering, feil bruk, osv. Skifte av enhet vil ikke løse problemet

Feilmekanismer og årsaker

- Feilmekanismer relaterer seg til fysiske, kjemiske eller andre prosesser som forringer enheten, og leder til svikt
- Feilårsak benyttes på to måter
 - Svikt på et lavere nivå, f eks defekt lager i ei pumpe
 - Rotårsak, f eks dårlig vedlikehold, uhensiktsmessig design osv

Sammenheng mellom funksjon, feilmode, feilårsak og feilmekanisme



Øving 4

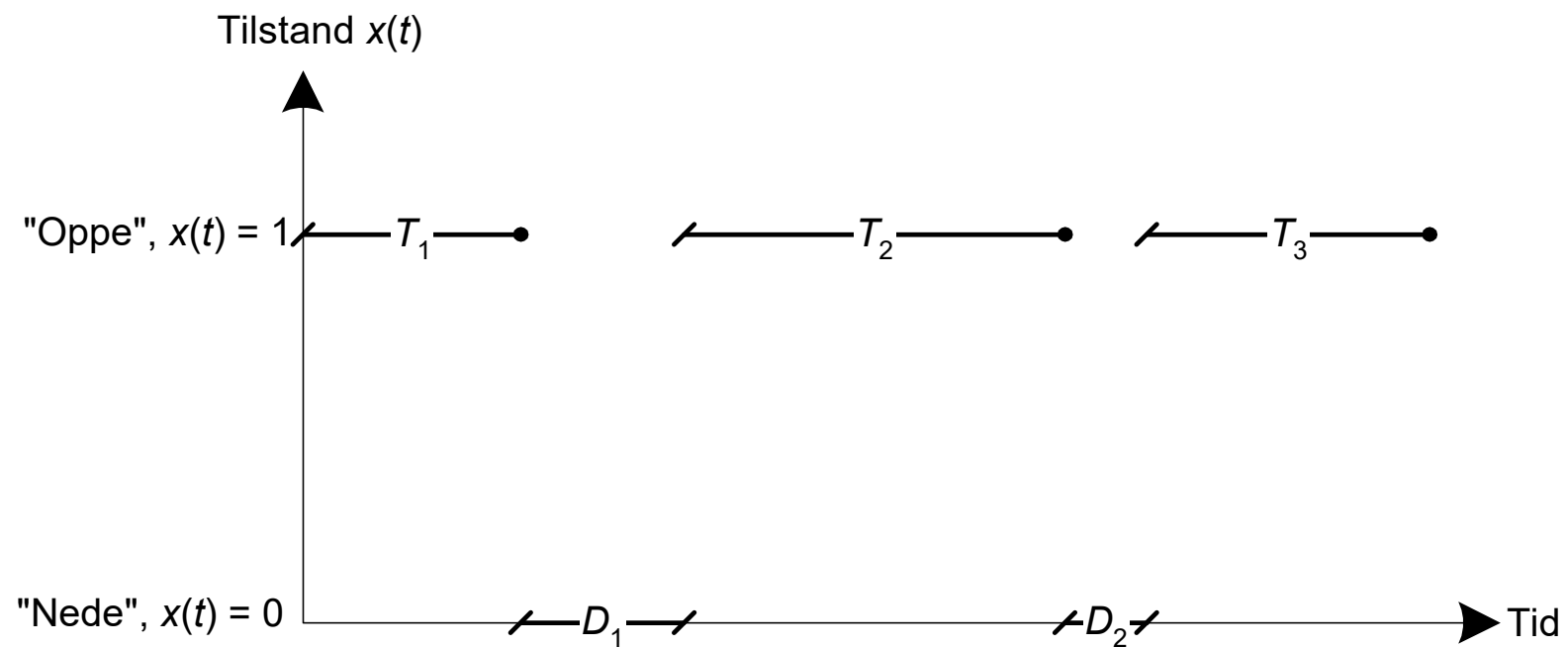
Gi eksempler på en slik fremstilling for et system du kjenner godt

Sviktmodeller

- Binær-representasjon
 - enheten er enten i stand til å utføre tiltenkt funksjon (virker), eller feiler i å utføre tiltenkt funksjon (feiltilstand). Tilstanden til en enhet kan da beskrives som en tilstandsvariabel $x(t)$

$$x(t) = \begin{cases} 1 & \text{om enheten er funksjonsdyktig ved tidspunkt } t \\ 0 & \text{om enheten er i feiltilstand ved tidspunkt } t \end{cases}$$

Tidsperspektiv



Notasjon

- "Oppetidene" angitt ved T_1 , T_2 og T_3
- "Nedetidene" er angitt ved D_1 og D_2
- Oppe- og nedetidene er stokastiske (tilfeldige)
- Tilstandsvariabelen, $x(t)$ er også stokastisk, vi skriver $X(t)$
- Ofte antar vi
 - Oppetidene er uavhengige og identisk fordelt
 - Nedetidene er uavhengige og identisk fordelt
 - Oppetider og nedetider er uavhengig av hverandre

Forhold som påvirker oppetidene:

- Innebygd komponentpålitelighet
- Forebyggende vedlikehold (smøring, rengjøring, utskifting av deler, inspeksjon)
- Driftsbetingelser
- Eksternt påtrykk
- Menneskelig interaksjon (feil eller skader introdusert under vedlikehold, feil bruk osv)
- mm

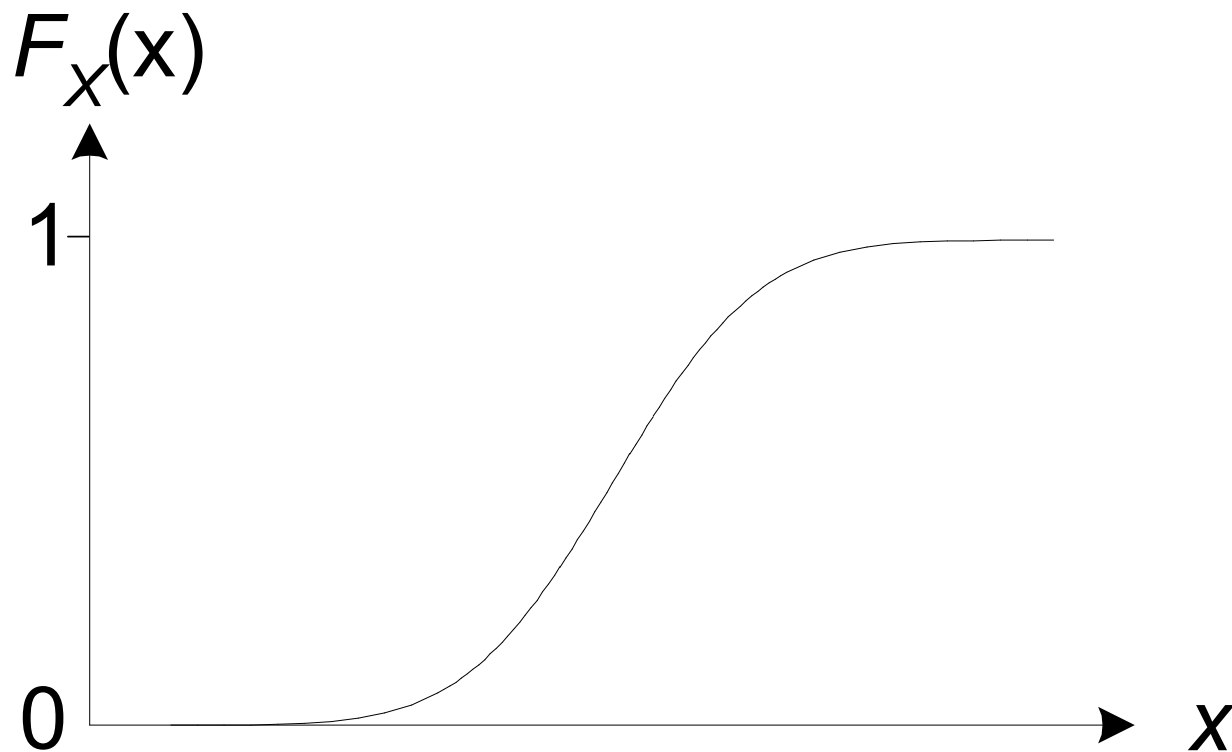
Forhold som påvirker nedetidene:

- Reservedelshold og logistikk
- Tilgjengelige vedlikeholdsresurser, beredskap
- Vedlikeholdskompetanse
- Intervall for funksjonstesting
- mm

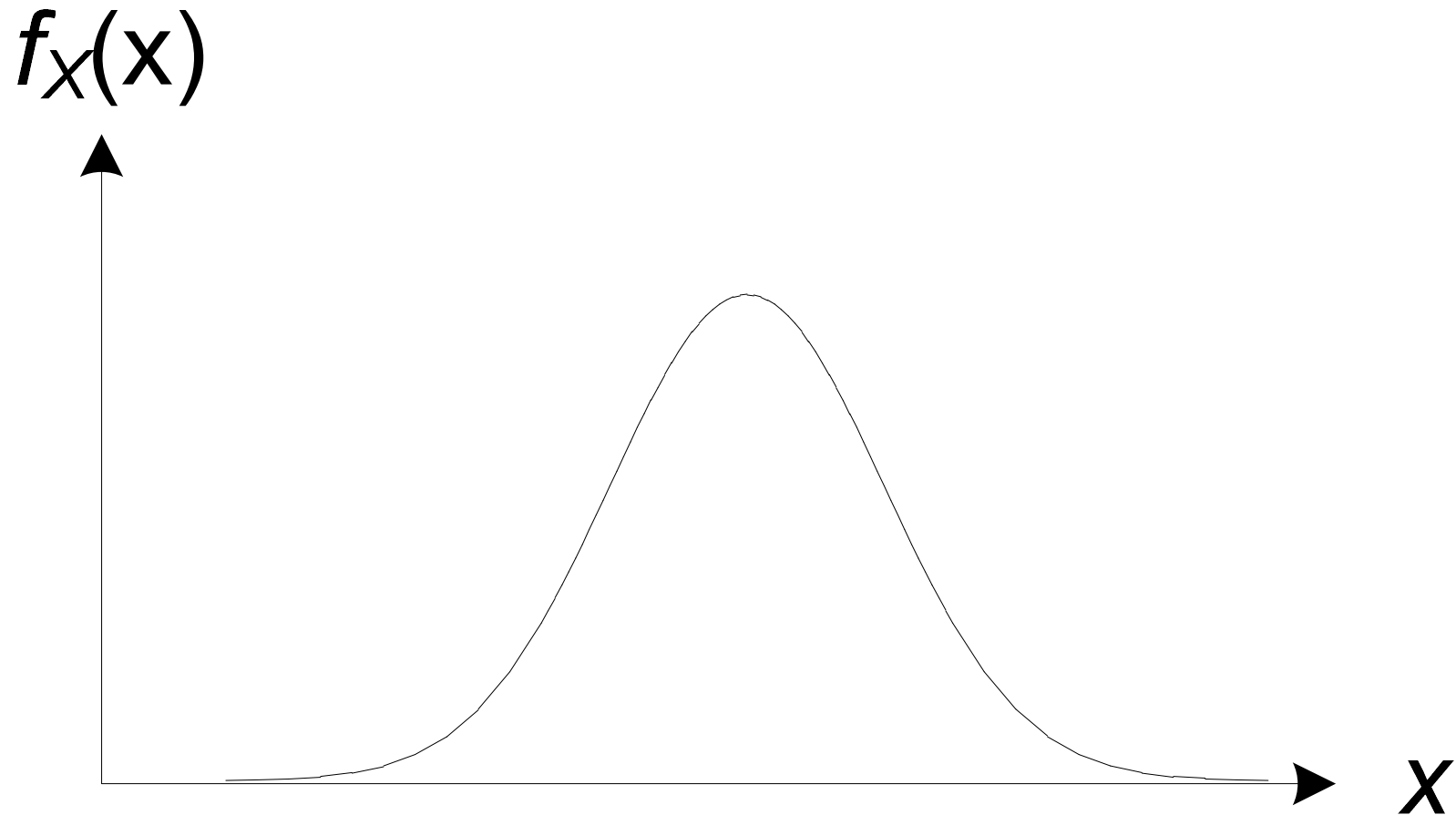
Sannsynlighetsregning - grunnlag

- Hendelse = Noe som kan hende, evt ikke hende
- Sannsynlighet er et mål som avbilder hendelser ned på tall-linja fra 0 til 1
- Vi skriver $\Pr(A)$ for å uttrykke sannsynligheten for at hendelsen A inntreffer
 - Eks: $\Pr(\text{"6-er"}) = 1/6$ (fair terning, ett kast)
- Stokastiske variable, eller tilfeldige størrelser kan ta ulike *verdier*
- Fordelingsfunksjon, og sannsynlighetstetthet beskriver stokastiske variable

Fordelingsfunksjon: $F_X(x) = \Pr(X \leq x)$



Sannsynlighetstetthet: $f_X(x) = \frac{d}{dx} F_X(x)$

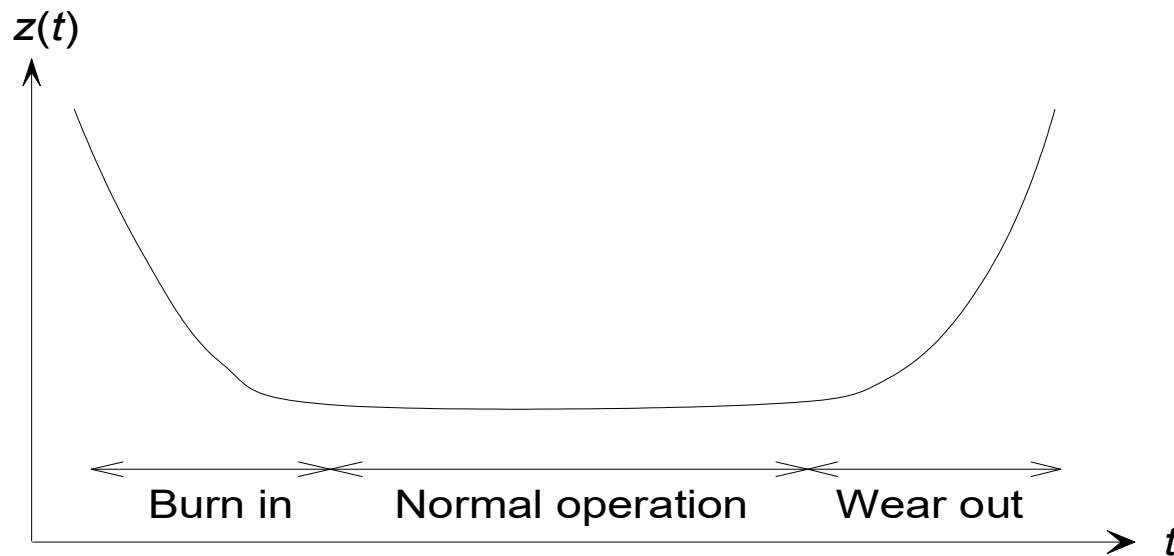


Tid til svikt

- Hva kan vi si om T_1 (og de andre t-ene)?
- Benytter generell T om tid til svikt
 - Fordelingsfunksjon, $F(t) = \Pr(T \leq t)$
 - Overlevelsessannsynligheten $R(t) = \Pr(T > t) = 1 - F(t)$
 - Sviktintensitet $z(t)$
 - Midlere tid til feil (svikt), $MTTF = E(T)$, «E = Expectation»

Sviktintensitet, $z(t)$

- $z(t) \cdot \Delta t \approx \Pr(t < T \leq t + \Delta t \mid T > t) =$ Sannsynligheten for svikt i $(t, t + \Delta t]$ gitt enheten har overlevd tid t
- Et annet begrep for sviktintensitet er badekarskurven



Utilgjengelighet

- Når enheten betraktes som en serie av oppe- og nedetider kan man beregne utilgjengeligheten = $\Pr(\text{enheten er nede})$
- $$U = \frac{\text{MDT}}{\text{MTTF} + \text{MDT}}$$
- MDT = Mean Down Time (Midlere nedetid)
- Hvor $\text{MTTF} = 1/\lambda$
- Øving 5
 - Finn U for en enhet som svikter en gang i året, og det tar 10 timer å reparere den
 - Hva om den svikter hvert andre år i snitt?

PFD = Probability of Failure on Demand

- Betrakt en (passiv) komponent som funksjonstestes med intervall av lengde τ
- Anta at enheten har konstant feilrate $\lambda = 1/\text{MTTF}$
- Dersom reparasjonstiden er kort i forhold til τ får vi:
- $$U = \frac{\text{MDT}}{\text{MTTF} + \text{MDT}} = \frac{\tau/2}{\text{MTTF} + \tau/2} \approx \frac{\lambda\tau}{2} = \text{PFD}$$
- Hvor PFD = Probability of Failure on Demand
- Øving 6
 - En enhet med skjult funksjon har konstant feilrate $\lambda = 0.3$ per år. Hvor ofte må vi teste denne enheten for at $\text{PFD} < 1\%$?
 - Dvs, finn τ

Klasser av levetidsfordelinger

- Ulike parametriske modeller benyttes til å beskrive levetidsfordelinger (tid til svikt)
- Valg av klasse er i regelen et avveining mellom en enkel modell, og en realistisk modell
- De mest brukte i denne sammenheng er:
 - Eksponensialfordelingen
 - Weibullfordelingen

Eksponeensialfordelingen

- Eksponeensialfordelingen er karakterisert ved:
 - $R(t) = e^{-\lambda t}$
 - $MTTF = 1/\lambda$
 - $z(t) = \lambda = \text{konstant}$, dvs uavhengig av alder
- Dvs en brukt enhet er stokastisk sett like god som en ny enhet, ingen grunn til å skifte en enhet som virker (hvis modellen er riktig)

Weibull-fordeling

- Weibull-fordelingen er karakterisert ved
 - $R(t) = e^{-(\lambda t)^\alpha}$
 - $MTTF = \Gamma\left(\frac{1}{\alpha} + 1\right) / \lambda$
 - $z(t) = \alpha\lambda(\lambda t)^{\alpha-1} \propto t^{\alpha-1}$
- Sviktintensiteten er
 - økende for $\alpha > 1$ (IFR=increasing failure rate)
 - avtagende for $\alpha < 1$ (DFR=decreasing failure rate)
 - Konstant for $\alpha = 1$
- For enheter med økende sviktintensitet vil effektiv feilrate reduseres ved periodisk skifte av enheten

Strukturfunksjon og pålitelighetsblokkdiagram

- For komponenter har vi

$$x(t) = \begin{cases} 1 & \text{om komponenten er funksjonsdyktig ved tidspunkt } t \\ 0 & \text{om komponenten er i feiltilstand ved tidspunkt } t \end{cases}$$

- For systemer kan vi tilsvarende sette

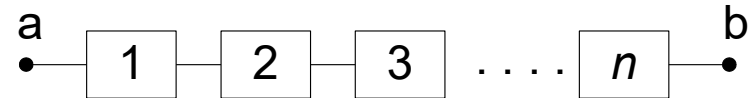
$$\phi(\mathbf{x}, t) = \begin{cases} 1 & \text{om systemet er funksjonsdyktig ved tidspunkt } t \\ 0 & \text{om systemet er i feiltilstand ved tidspunkt } t \end{cases}$$

- ϕ betegnes strukturfunksjonen, og avhenger av $\mathbf{x}$ 'ene

Strukturfunksjon for noen enkle strukturer

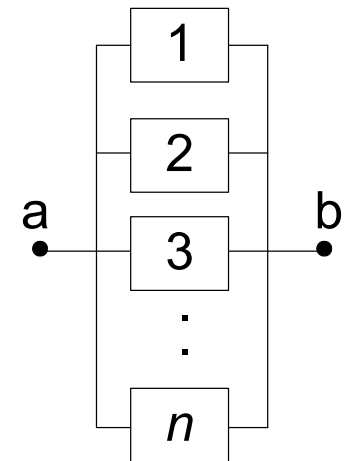
- For en seriestruktur gjelder

- $\phi(\mathbf{x}) = x_1 \cdot x_2 \cdot \dots \cdot x_n$



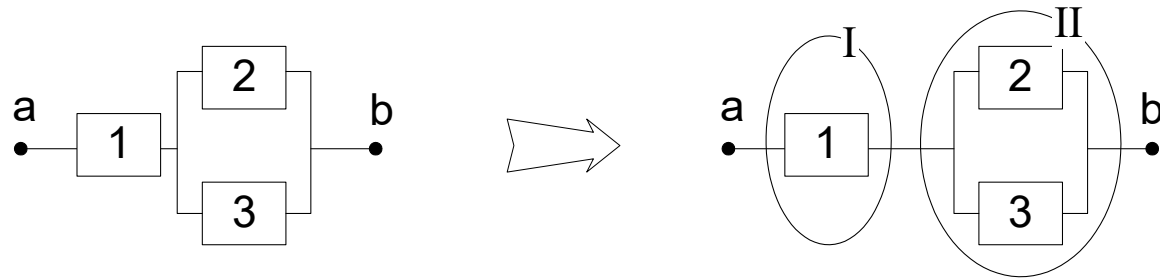
- For en parallellstruktur (redundans) gjelder

- $\phi(\mathbf{x}) = 1 - (1 - x_1)(1 - x_2) \dots (1 - x_n)$



- For strukturer som er sammensatt av serie og parallellstrukturer kan formlene ovenfor settes sammen

Eksempel



$\phi(x) = \phi_I \times \phi_{II}$ fordi I og II er i serie

$$\phi_I = x_1$$

$\phi_{II} = 1 - (1 - x_2)(1 - x_3)$ fordi 2 og 3 er i parallell

$$\text{Dvs } \phi(x) = x_1(1 - (1 - x_2)(1 - x_3)) = x_1x_2 + x_1x_3 - x_1x_2x_3$$

Nytte av strukturefunksjonen

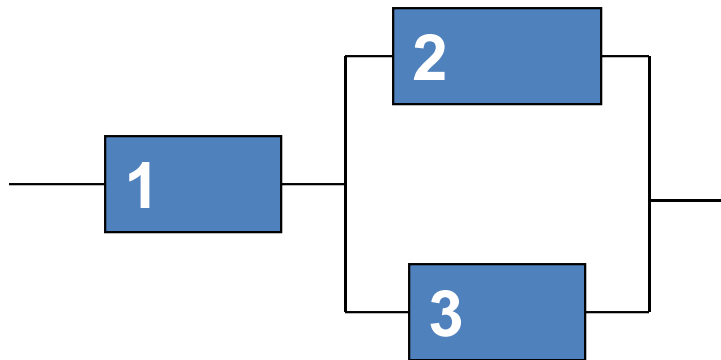
- Dersom vi kjenner strukturefunksjonen (matematisk), og vi kjenner verdien på x -ene (komponenttilstandene), kan vi avgjøre om systemet fungerer ved å "sette inn" x -verdier.
- Dersom vi kjenner strukturefunksjonen, og vi kjenner komponentpålitelighetene ($p = 1-U$) kan vi sette inn p 'er på plassen til x 'ene for å få systempåliteligheten (notasjon: $h(\mathbf{p})$)
 - Komponentene må være uavhengige
 - Helst bør vi "gange" ut strukturefunksjonen først
 - Metoden er "trygg" dersom vi ikke har "repeterende" hendelser i strukturen
 - Dersom vi har repeterende hendelser i strukturen bør vi gange ut strukturefunksjonen, og stryke alle potenser i uttrykket, f eks $x^2 \rightarrow x$

Mål for kritisk betydning

- Hvor kritiske er de ulike komponentene i et system?
- Ulike mål finnes
- Birnbaums mål benyttes ofte:
 - $I^B(i) = \partial h(\mathbf{p}) / \partial p_i$
 - Komponenter med høy $I^B(i)$ er i utgangspunktet viktigst å vedlikeholde

Øving 9

- Betrakt følgende system



- Finn strukturfunksjonen til systemet

Øving 10

- Finn systempåliteligheten til systemet
- Finn Birnbaums mål for hver komponent
- Dersom du bare har råd til å vedlikeholde en enhet, hvilken velger du?

Komp	MTTF	MDT
1	1000	2
2	100	3
3	100	4

Svar – Øving 9 og 10

Strukturfunksjon $\phi(\mathbf{x}) = x_1x_2 + x_1x_3 - x_1x_2x_3$

Systempålitelighet $h(\mathbf{p}) = p_1p_2 + p_1p_3 - p_1p_2p_3 = 0.996886$

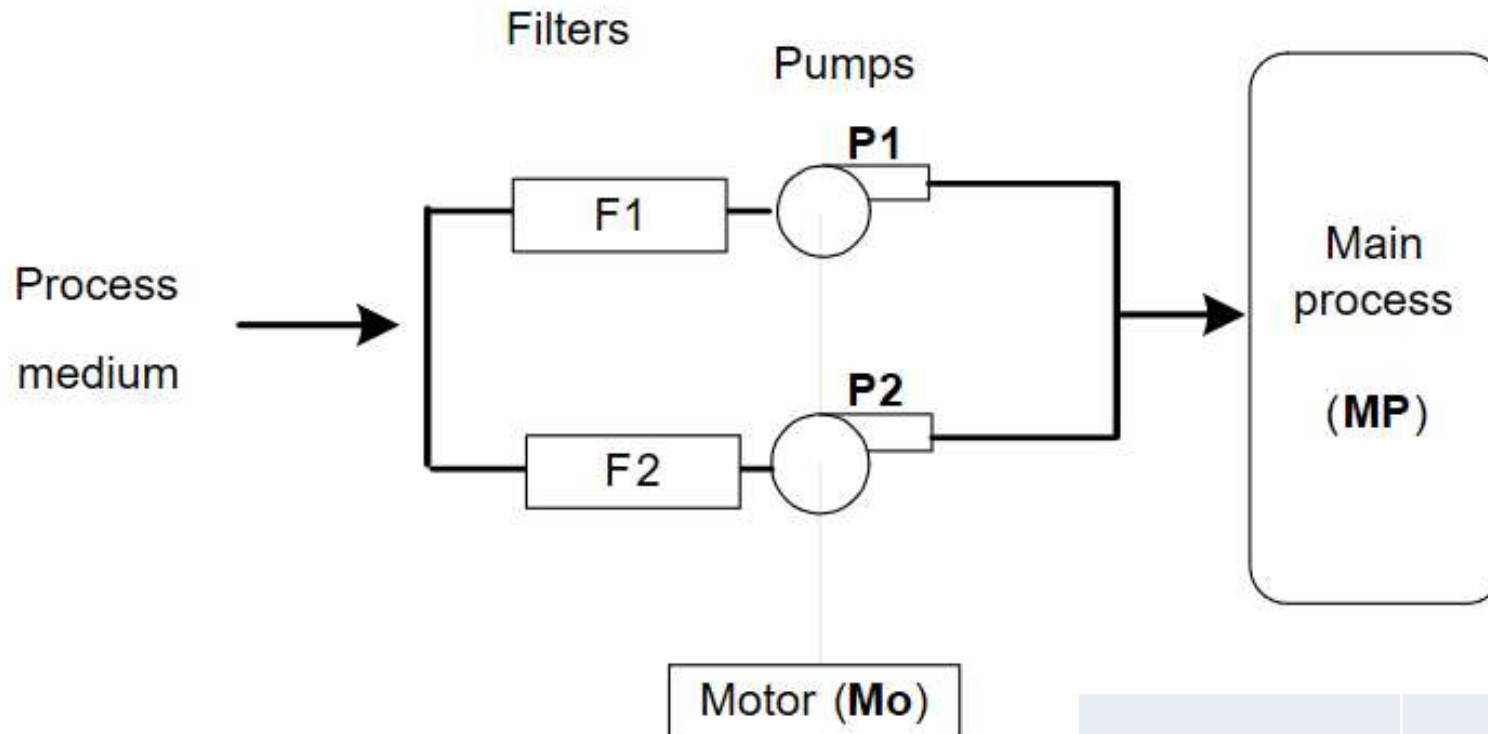
Birnbaum's mål:

$$I^B(1) = \partial h(\mathbf{p}) / \partial p_1 = p_2 + p_3 - p_2p_3 = 0.9988797$$

$$I^B(2) = \partial h(\mathbf{p}) / \partial p_2 = p_1 - p_1p_3 = 0.0383848$$

$$I^B(3) = \partial h(\mathbf{p}) / \partial p_3 = p_1 - p_1p_2 = 0.02906811$$

Avansert øvingsoppgave



Finn systempåliteligheten til systemet

Komponent	MTTF	MDT
P1 /P2	1460	16
F1 /F2	1460	4
Mo	17520	24
MP	26280	48

Repetisjon, systempålitelighet

- MTTF = Mean Time To Failure
 - $MTTF_E$ = Effektiv MTTF med vedlikehold
 - $MTTF_N$ = Naked MTTF, dvs MTTF uten vedlikehold
- MDT = Mean Down Time (fra svikt, til vi er "oppe" igjen)
- $U = MDT / (MTTF_E + MDT)$ = Unavailability =
utilgjengelighet
 - For enheter med skjult funksjon er $U = \lambda \tau / 2$
- $A = 1 - U = MTTF_E / (MTTF_E + MDT)$ = Availability =
Tilgjengelighet

Repetisjon, forts

- $X_i(t)$ = Tilstandsvariabel, 1 hvis OK, 0 ellers
- $p_i(t) = \Pr(X_i(t) = 1)$ = tidsavhengig pålitelighet
 - For reparerbare enheter vil tidsavhengigheten dempes bort
 - $p_i(t) = p_i = \text{MTTF}_E / (\text{MTTF}_E + \text{MDT})$
- $q_i(t) = \Pr(X_i(t) = 0) = 1 - p_i(t)$
 - For reparerbare enheter vil tidsavhengigheten dempes bort
 - $q_i(t) = q_i = \text{MDT} / (\text{MTTF}_E + \text{MDT})$

Repetisjon, forts

- For systemer:
- $\phi(\mathbf{x})$ = strukturfunksjonen, og avhenger av x 'ene
- For seriestruktur: $\phi(\mathbf{x}) = x_1 \cdot x_2 \cdot \dots \cdot x_n$
- For parallellstruktur: $\phi(\mathbf{x}) = 1 - (1 - x_1)(1 - x_2) \dots (1 - x_n)$
- Vi kan sette sammen serie og parallell ved å lage moduler
- Vi kan sette inn p -er på plassene til x -ene for å finne systempåliteligheten:
- $p_S = h(\mathbf{p}) = \Pr(\phi(\mathbf{x}) = 1)$

Trinn - pålitelighetsblokkdiagram

1. "Oversett" fysisk system til pålitelighetsblokkdiagram
2. Finn strukturfunksjonen, $\phi(\mathbf{x})$, som funksjon av x-ene ved å sette sammen resultat for serie- og parallellstrukturer
3. Multipliser ut strukturfunksjonen (løse opp parenteser)
4. Stryk potenser i x-ene
5. Finn p_i -ene ved formler for tilgjengelighet
6. Bytt ut x-ene med p-er i strukturfunksjonen for å finne systemtilgjengeligheten $p_S = h(\mathbf{p})$
7. Viktigheten av komponent nr i finnes ved å derivere systempåliteligheten mhp p_i