Exam - Friday 24. may 2003

SIE 5025 Pålitelige systemer
Dependable systems

Løsningsforslag

Version 0.1; 9 May 2003; BEH

Oppgave 1

a) **Fordeler:**

- En varm reserve er hurtigere å få idriftsatt med enten funksjonsett A eller B enn en kald, Dvs kortere temporær nedetid etter feil.
- Feil i en varm reserve kan/vil bli oppdaget og avhjulpet før reserven trenges.

Ulempe:

- Raten av permanente maskinvarefeil er vanligvis levere hos avslått utstyr (lavere temperatur). I systemer uten vedlikehold kan dette gi et lengre liv, eller mer spesifikt bedre funksjonsannsynlighet for lange (misjons)tider ("Mission times").

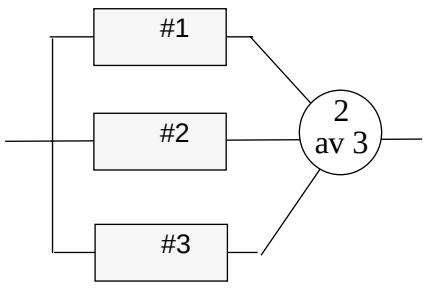
b) Et systems (eller enehets) feilsemantikk er det dominerende feilmodi for systemet, dvs den måten vi kan basere oss på at systemet ytrer seg på når det feiler. Feil-stopp semantikk innebærer at systemet ikke gir noen respons får det er gjennomført en feilhåndtering. Denne semantikken kan f.eks. oppnås for en prosessor ved å dublere denne, kjøre dublettene i mikrosynkronisme og stoppe ved "mismatch". Jfr. Delta-4s kommunikasjonsprosessor.

c) For utledning av uttrykk, se kompendiet.

$R_1(t) = (3e^{-(2\lambda)t} - 2e^{-(3\lambda)t})$

MTFF for en tjener er λ^{-1}. Følgelig er sannsynligheten for at systemet skal virke avbruddsfritt lengre en dette

$R_1(\lambda^{-1}) = (3e^{-2} - 2e^{-3}) = 0.30643171$



d) Det er to grunner til at blokkskjema ikke kan benyttes:

- reparasjon introduserer avhengighet mellom enhetene/tjenerne,

- blokkskjema kan ikke benyttes til å bestemme funksjonssannsynlighet for reparerte systemer fordi en på et gitt tidpunkt ikke kan avgjøre om systemet tidligere har vært nede og kommet oppigjen eller vært oppe hele tiden.

Bruker derfor tilstandsdiagram hvor feiltilstandene gjøre s absorberende. Sannsynligheten for å være i en oppetilstand ved et gitt tidspunkt korresponderer da til at systemet ikke har feilet ved dette tidpunktet. Finner disse sansynlighetene.

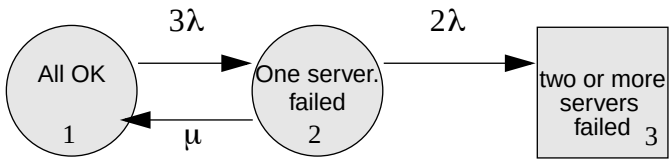


Figure 1.1 Simplified Markov model of the repaired server system

Fra dette diagrammet kan vi etablere differensiallikningene som bestemmer sannsynlighetene $\underline{P}(t) = \{P_1(t), P_2(t), P_3(t)\}^T$ for å være i de ulike tilstandene.

$$\frac{d}{dt}\underline{P}(t) = \Lambda\underline{P}(t) \qquad \text{hvor } \Lambda = \begin{bmatrix} -3\lambda & \mu & 0 \\ 3\lambda & -2\lambda-\mu & 0 \\ 0 & 2\lambda & 0 \end{bmatrix}$$
$$\underline{P}(0) = \{1, 0, 0\}^T$$

Og hvor som nevnt hvor funksjonssannsynligheten for systemet er $R_2(t) = P_1(t) + P_2(t)$.

e) Gitt at en tjener har feilet, så er sannsynligheten for at en ny feil inntreffer før den første er ferdigreparert $(2\lambda)/(2\lambda+\mu)$. Dette får systemet til å feile. Denne sannsynligheten vil avta med økende μ/λ og funksjonssannsynligheten vil bli bedre.

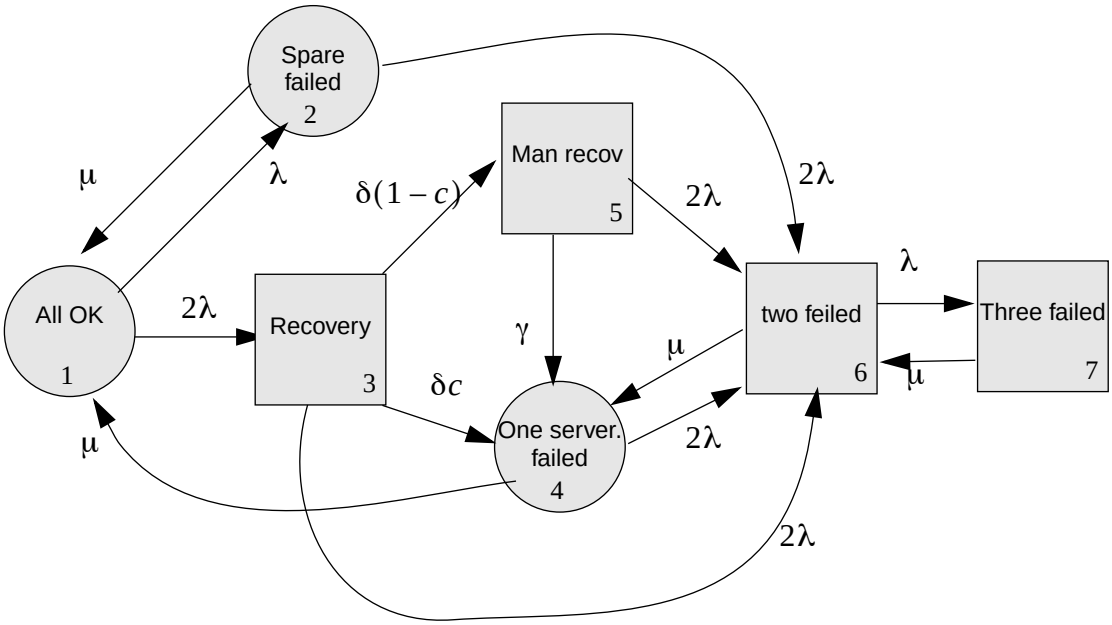
For $\mu/\lambda = 1$ er denne sannsynligheten 2/3, dvs i de fleste tilfellene får vi ikke ferdig før en ny feil intreffer og funksjonssansynligheten blir sammenlignbar med den vi fant i pkt. **c)**.

Når $\mu/\lambda \to \infty$ så vil funksjonsannsynligheten kunne tilnærmes med $R(t) = e^{-(6\lambda^2/\mu)t}$.

("Avansert" kommentar: Dette svarer til en ekvivalent feilrate på $6\lambda^2/\mu$. Ser vi bort fra transisjoner over i feltilstanden er annsynligheten for å være i en tilstand med en feil i systemet $3\lambda/(3\lambda+\mu) \approx 3(\lambda/\mu)$. Gitt vi er i denne tilstand er feilintensiteten 2λ. Intensiteten hendelser som gir systemfeil er da $3(\lambda/\mu)2\lambda$ dvs den ekvikalente systemfeilrate.)

f) Se etterfølgende diagram.

g) I nevner ser vi at leddet $\gamma\delta\mu^3$ er vesentlig større de øvrige, så $s_2 \approx \gamma\delta\mu^3$.



I telleren vil leddene med 1. orden i λ dominere. Vi ser også at ingen av disse opplagt større enn det andre og følgelig $s_1 \approx 2\gamma\lambda\mu^3 + 2\delta\lambda\mu^3(1-c)$. En tilnærming blir da:

$$U \approx \frac{2\lambda}{\delta} + \frac{2\lambda(1-c)}{\gamma} \tag{1.1}$$

Vi ser at første ledd tilnærmet er intensiteten inn i "recovery" tilstanden ganger oppholdstiden i denne. Dette leddet svarer til recoverys bidrag til utilgjengeligheten. Neste leddet er tilsvarende for den manuelle recovery etter en "coverage" feil.

Vi ser at med de forhold vi har mellom parametrene er reparasjonstiden av underordent betydning. Dersom vi ønsker å se effekten av denne kan vi andreordensleddene i λ. Vi får da:

$$U \approx \frac{2\lambda}{\delta} + \frac{2\lambda(1-c)}{\gamma} + \frac{6\lambda^2}{\mu^2} + \frac{4\lambda^2(1-c)}{\gamma\mu} + \frac{4\lambda^2}{\delta\gamma} \tag{1.2}$$

hvor vi ser at 4. og 5. ledd er vesentlig mindre enn 3. og kan neglisjeres. 3. svarer til sannsynligeheten for at systemet er nede pga. to feil. (Denne forklaringen kreves IKKE til eksamen: Sannsynligheten for å være i en tilstand med en feil i systemet er $3(\lambda/\mu)$. Intensiteten av andre ordensfeil i systemet er da $3(\lambda/\mu)2\lambda$ og disse en varighet på $1/\mu$.) Vi har følgelig nedenstående tilnærming hvor alle nedemodi og parametre er med

$$U \approx \frac{2\lambda}{\delta} + \frac{2\lambda(1-c)}{\gamma} + \frac{6\lambda^2}{\mu^2} \tag{1.3}$$

Eksamen sie5025 pålitelige systemer 2003; Oppgave 2

```
<< "/Users/bjarne/Undervisning/MMA
   tools/Packages and demos/Dependability/BlockDiagrams.m"
```

Mathematica er brukt for å sikre at det ikke er regnefeil i løsningen og for å effektivisere arbeidet med tekstbehandlingen. Endel av utregningene er gjort med pakken BlockDiagrams basert på utrykkene i kompendiet.

Løsningsforslaget er primært laget for å understøtte rettingen og er ikke noen "mønsterløsning". Det inneholder en rekke detaljutregninger som selvsagt ikke kreves utført i en eksamensbesvarelse.

■ a

Kravene er gitt i ulike enheter, Konvertere alle til timer (uten at dette vises eksplisitt).

```
<< Miscellaneous`Units`
```

100 minuttter akkumulert nedetid i løpet av ett år svarer til en utilgjengelighet gitt av forholdet melom tidene:

```
Ub = SI[100 Minute / (1 Year)] // Simplify // N
```

```
0.000190259
```

Kravene til midlere tid mellom feil og midlere nedetid er gitt i oppgaven.

```
MTBFb = Convert[4 Month, Hour] / Hour
```

```
2920
```

```
MDTb = 3;
```

Dersom nedetiden er negativt eksponensialfordelt, svarer dette til at 95% av feilene er rettet innen T_p hvor

```
Solve[1 - .95 == Exp[-Tp / MDTb], Tp]
```

```
{{Tp → 8.9872}}
```

(eller løst "manuelt":)

```
Tp = - Log[1 - .95] * MDTb
```

```
8.9872
```

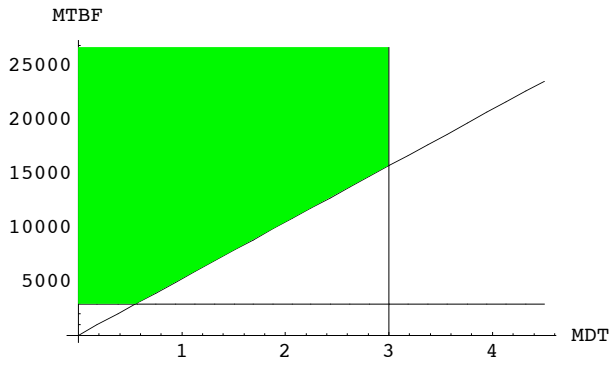
Linjene angir de tre pålitelighetskravene over, og det grønne området de Kombinasjonene av MTBF og MDT som fyller samtlige.

```
MDTbound = Graphics[Line[{{MDTb, 0}, {MDTb, 1.7 1 / Ub * MDTb}}]]
```

```
- Graphics -
```

```
WithinSec =
  Graphics[{RGBColor[0, 1, 0], Polygon[{{MDTb, 1.7 1 / Ub * MDTb}, {0, 1.7 1 / Ub * MDTb},
      {0, MTBFb}, {MTBFb Ub, MTBFb}, {MDTb, 1 / Ub MDTb}}]}];
```

```
Show[Plot[{1 / Ub * Td , MTBFb}, {Td, 0, 4.5}, AxesLabel → {"MDT", "MTBF"},
  DisplayFunction → Identity], WithinSec, MDTbound, DisplayFunction → $DisplayFunction]
```




```
- Graphics -
```

b

Fullstendig maskenett (Fully meshed network)

Maskenett er en topologi som typisk anvendes for WAN. (Fullstendig maskenett ofte benyttet på toppnivå i hierarkiske nett, f.eks. tradisjonelle telefonnett.)

c

Nettet kan ikke representeres ved en serie-paralell struktur siden det er en "bro" mellom B og D. Bruker derfor pivoteringsmetoden og betinger mhp. om bro-elementet BD er intakt eller ikke.

Benytter en notasjon hvor ⨅ angir serie mellom to element og ⨆ angir paralell. Øvrig strukturinfo i serie paralell struktuter er gitt av parenteser.

```
?SeriesSystem
```

```
SeriesSystem[Ei, Ej, Ek,..] = SquareIntersection[Ei, Ej, Ek,..]returns  the
  availability and mean up time {A,MUT} of a series  system with two or more
  elements or subsystems Ex characterised by their  availability and mean up time,
  i.e. Ex={AEx, MUTEx}.  May also be written with the infix operator  Ei ⨅ Ej ⨅ Ej
```

```
mutl = m (1 - Ul);
```

Definerer et generelt nettelement *e*:

```
e = {1 - Ul, mutl};
```

■ Stuktur når broelementet BD ikke fungerer

```
(S1 = (e ⨅ e) ⨆ (e ⨅ e) ⨆ e) // First
```

```
1 - (1 - (1 - Ul)^2)^2 Ul
```

■ **Stuktur når broelementet BD fungerer**

```
(S2 = ((e ⨆ e) ⨅ (e ⨆ e)) ⨆ e) // First
```

$$1 - Ul \left(1 - (1 - Ul^2)^2\right)$$

■ **Fjerner betingelsen gitt av om broelementet BD fungerer eller ikke.**

```
? BridgeStruct
```

```
BridgeStruct[S1, S2, E] returns  the availability and mean up time {A,MUT} of a
  non series paralell  system which can be transformed into two series paralell
  systems S1 and S2 by pivoting on the 'bridge element' E.  S1 is the system when E
  is always working,  S2 is the system when E is working working. All elements or
  systems X characterised by their  availability and mean up time, i.e. X={AX, MUTX}.
```

```
1 - ((SX = BridgeStruct[S2, S1, e] // Simplify) // First)
```

$$2\,Ul^3 + 2\,Ul^4 - 5\,Ul^5 + 2\,Ul^6$$

d

Bruker de generelle utrykkene for berengning av serie paralellsystem gitt i kompendies avsnitt 1.7.

```
({A₁ , m₁ A₁} ⨅ {A₂ , m₂ A₂})
```

$$\left\{A_1\,A_2,\ \frac{1}{\frac{1}{A_1\,m_1} + \frac{1}{A_2\,m_2}}\right\}$$

og for en paralellstruktur:

```
({A₁ , m₁ A₁} ⨆ {A₂ , m₂ A₂})
```

$$\left\{1 - (1 - A_1)\,(1 - A_2),\ \frac{(A_1\,(-1 + A_2) - A_2)\,m_1\,m_2}{(-1 + A_1)\,m_1 + (-1 + A_2)\,m_2}\right\}$$

på stukturen for å finne.

```
Spb = (e ⨅ e) ⨆ e
```

$$\left\{1 - (1 - (1 - Ul)^2)\,Ul,\ \frac{m\,(1 - 2\,Ul^2 + Ul^3)}{(4 - 3\,Ul)\,Ul}\right\}$$

hvor

```
U_pb = 1 - Spb[[1]] // Expand
```

$$2\,Ul^2 - Ul^3$$

```
MTBF_pb = Spb[[2]] / Spb[[1]] // Simplify
```

$$\frac{m}{(4 - 3\,Ul)\,Ul}$$

```
MDT_pb = MTBF_pb U_pb // Simplify
```

$$\frac{m\,(-2 + Ul)\,Ul}{-4 + 3\,Ul}$$

e

Ser at ved å rute trafikken
• langs direktelenken som primærvei, og
• benytte en rute via A eller/og B som "back-up paths" for 8 Gbit/s trafikken og
• en rute via en diagonallenke for 2 Gbit/s trafikken,
Så kan en håndtere all trafikk ved alle enkeltlenkefeil.

```
AB_routes = {{AB}, {AC, CB}};
AC_routes = {{AC}, {AB, BC}};
AD_routes = {{AD}, {AC, CD}};
BC_routes = {{BC}, {BA, AC}};
BD_routes = {{BD}, {BA, AD}};
CD_routes = {{CD}, {CB, BA, AD}};
```

Symmeriske rutes for returveien

Hovedfordelen er at en for en bedre utnyttelse av overføringskapasiteten i nettet ved at flere primæruter kan dele samme lenkekapasitet i sin reservevei. En anne fordel ar at hånderingen av trafikken blir enkel ved at en i ingressnodene svitsjer over til reserveien når feil detekteres (og at dette kan skje fort når reserveiene er prereservert). Implementasjonen kan benytte ATM eller MPLS labler for "enkel" realisering.

Utfordringen (ulempen) med metoden er å finne og dynamisk tilpasse primær og reserveveiene. (Metoden er ikke optimal mhp. ressursutnyttelse da reserveveien ikke velges ut fra den feilen som inntreffer.)

f

Siden lenkefeilene inntreffer uavhengig av hverandre og har uavhengig reparasjon vil antallet lenkefeil i systemet til enhver tid være binomisk fordelt, dvs.:

```
P[0] = (1 - Ul)^6;
```

```
P[1] = Binomial[6, 1] Ul (1 - Ul)^5
```

```
6 (1 - Ul)^5 Ul
```

```
P[flere] = 1 - P[0] - P[1]
```

```
1 - (1 - Ul)^6 - 6 (1 - Ul)^5 Ul
```

Siden vi vet fra foregående punkt at trafikken mellom A og C blir ført ved ingen feil og alle enkelt feil, får vi

```
Ind[Tapt] = 1;
Ind[Ført] = 0;
```

```
U_nedre = P[0] Ind[Ført] + P[1] Ind[Ført]
```

```
0
```

```
U_øvre = P[0] Ind[Ført] + P[1] Ind[Ført] + P[flere]
```

```
1 - (1 - Ul)^6 - 6 (1 - Ul)^5 Ul
```

Forenkler øvere grense for å se på de viktigste leddene.

```
Series[%, {Ul, 0, 3}]
```

$$15\,Ul^2 - 40\,Ul^3 + O[Ul]^4$$

Ser at resultatet er i samme størrelseorden som i punkt d). Dvs. Ul^2 er orden på det dominerende leddet som tilsier at to feil tolereres. Resultatet over er konservativt ved at detvogså inkluderer de triple feilne som ikke påvirker trafikken mellom A og C. [At trafikken rutes forskjellig påvirker ikke dette.] Resultatet i punkt c) er optimistisk siden det ikke tar hensyn til restriksjoner som forårsakes av konkurranse med annen trafikk eller begrensinger i ruting.

---

g

■ Sannsynlgheten for ingen feil i nettet:

```
P[0] = (1 - Ul)^6 (1 - Ud)^4;
```

■ Ser på sannsynlighetene for enkeltfeil i nettet

Sannsynligheten for at en spesifikk lenke er feilet og ingen traseefeil.

```
Pl = Ul ( 1 - Ul)^5 (1 - Ud)^4;
```

Sannsynligheten for at en spesifikk traseefeil og ingen lenke er feilet.

```
Pd = Ud ( 1 - Ul)^6 (1 - Ud)^3;
```

■ Sannsynligheten for mer enn en feil

```
P[flere] = 1 - P[0] - 6 Pl - 4 Pd // Simplify
```

$$1 - (-1 + Ud)^4\,(-1 + Ul)^6 + 4\,(-1 + Ud)^3\,Ud\,(-1 + Ul)^6 + 6\,(-1 + Ud)^4\,(-1 + Ul)^5\,Ul$$

■ Øvre og nedre grenser.

Som i foregående punkt vil ingen enkeltlenkefeil gi feil i forbindelsen mellom A og C. Derimot ser vi av figur 2.2 at feil assosiert med to av de fire traseene (AB og BC) vil gi feil

```
U_nedre = P[0] Ind[Ført] + 6 Pl Ind[Ført] + 2 Pd Ind[Tapt] + 2 Pd Ind[Ført]
```

$$2\,(1 - Ud)^3\,Ud\,(1 - Ul)^6$$

```
U_øvre = P[0] Ind[Ført] + 6 Pl Ind[Ført] + 2 Pd Ind[Tapt] + 2 Pd Ind[Ført] + P[flere]
```

$$1 + 2\,(1 - Ud)^3\,Ud\,(1 - Ul)^6 - (-1 + Ud)^4\,(-1 + Ul)^6 + 4\,(-1 + Ud)^3\,Ud\,(-1 + Ul)^6 + 6\,(-1 + Ud)^4\,(-1 + Ul)^5\,Ul$$

Forenkler overstående for å se på de viktigste leddene:

```
Series[U_nedre, {Ul, 0, 3}, {Ud, 0, 2}]
```

$$(2\,Ud - 6\,Ud^2 + O[Ud]^3) + (-12\,Ud + 36\,Ud^2 + O[Ud]^3)\,Ul + (30\,Ud - 90\,Ud^2 + O[Ud]^3)\,Ul^2 + (-40\,Ud + 120\,Ud^2 + O[Ud]^3)\,Ul^3 + O[Ul]^4$$

```
Series[Uøvre, {Ul, 0, 3}, {Ud, 0, 2}]
```

$$(2\,Ud + O[Ud]^3) + (12\,Ud - 36\,Ud^2 + O[Ud]^3)\,Ul + (15 - 90\,Ud + 180\,Ud^2 + O[Ud]^3)\,Ul^2 + (-40 + 200\,Ud - 360\,Ud^2 + O[Ud]^3)\,Ul^3 + O[Ul]^4$$