

Exam - Friday 24. may 2003

SIE 5025 Pålidelige systemer *Dependable systems*

Løsningsforslag

Version 0.1; 9 May 2003; BEH

Oppgave 1

a) Fordeler:

- 1/2 En varm reserve er hurtigere til driftsatt med enten funksjonsett A eller B enn en kald, Dvs kortere temporerettedid etter feil.
- 1/2 Feil i en varm reserve kan/vil bli oppdaget og avhjulpet før reserven trenges.

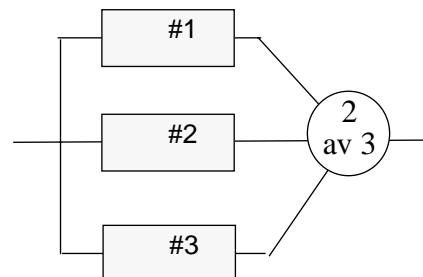
Ulempe:

- 1/2 Raten av permanente maskinvarefeil er vanligvis lavere hos avsluttet utstyr (lavere temperatur). I systemer uten vedlikehold kan dette gi et lengre liv, eller mer spesifikt bedre funksjons sannsynlighet for lange (misjons)tider (Mission times).
- b) Et systems (eller enhets) feilsemantikk er det dominerende feilmodi for systemet, dvs den må vi kan basere oss på at systemet ytrer seg på at det feiler. Feil-stopp semantikk innebærer at systemet ikke gir noen respons før det er gjennomført en feilhåndtering. Denne semantikken kan f.eks. oppnås for en prosessor ved å dublere denne, kjøpe dublettene i mikrosynkronisme og stoppe ved mismatch for Delta-4s kommunikasjonsprosessor.
- c) For utledning av uttrykk, se kompendiet.

$$R_1(t) = (3e^{-(\lambda_1 + \lambda_2)t} + 2e^{-(\lambda_1 + \lambda_3)t})$$

MTFF for en tjener er $\frac{1}{\lambda}$. Følgelig er sannsynligheten for at systemet skal virke avbruddsfritt lengre enn dette

$$R_1(\rightarrow \infty) = (3e^{-\lambda_1 t} + 2e^{-\lambda_2 t}) = 0.30643171$$



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

- 1/2 reparasjon introduserer avhengighet mellom enhetene/tjenerne,

1/2 blokkskjema kan ikke benyttes til å bestemme funksjonssannsynlighet for reparerte systemer fordi en på et gitt tidspunkt ikke kan avgjøre om systemet tidligere har vært nede og kommet opp igjen eller vært oppe hele tiden.

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

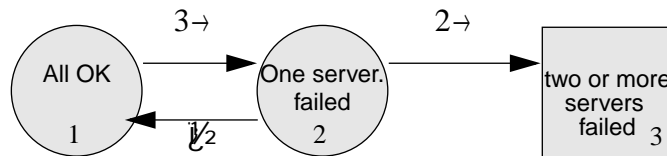


Figure 1.1 Simplified Markov model of the repaired server system

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.

$$\frac{d}{dt}\underline{P}(t) = \mathbf{v}\underline{P}(t) \quad \text{hvor } \mathbf{v} = \begin{bmatrix} -3 & 1/2 & 0 \\ 3 & -2 & 1/2 \\ 0 & 2 & 0 \end{bmatrix}$$

$$\underline{P}(0) = \{1, 0, 0\}^T$$

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, skal sannsynligheten for at en ny feil inntreffer før den første er ferdigreparert ($2 \rightarrow 0$) ($2 \rightarrow + 1/2$) Dette før systemet til å feile. Denne sannsynligheten vil avta med tiden $1/2$ og funksjonssannsynligheten vil bli bedre.

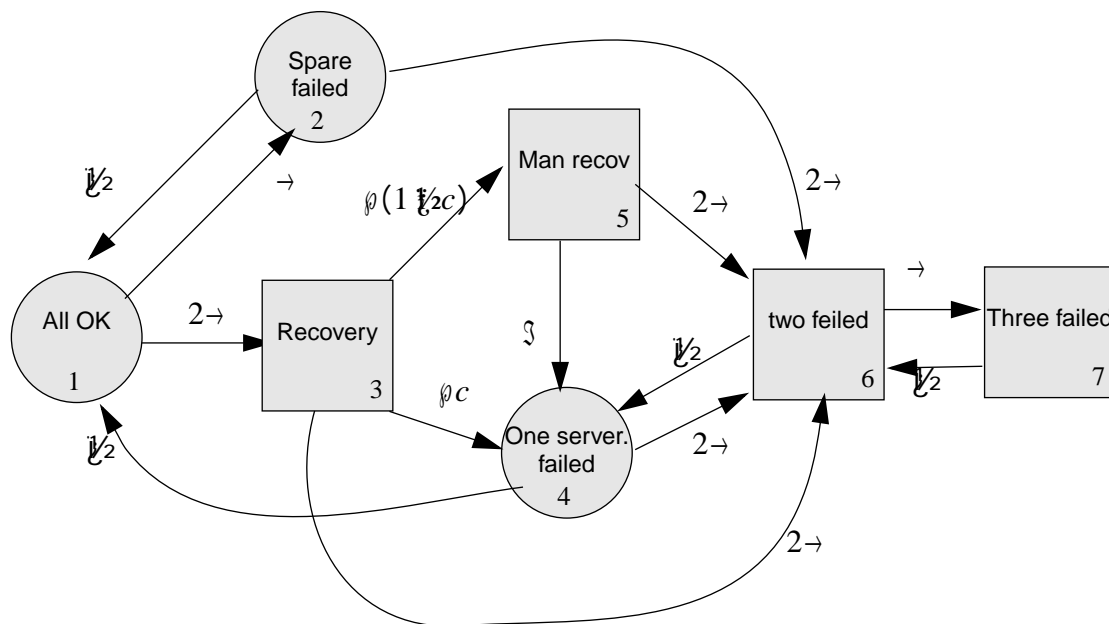
For $1/2 = 1$ er denne sannsynligheten $2/3$, dvs i de fleste tilfellene før vi ikke ferdig før en ny feil inntreffer og funksjonssannsynligheten blir sammenlignbar med den vi fant i pkt. c).

Nett $1/2 \rightarrow \gamma$ skal funksjonsannsynligheten kunne tilnærmes med $R(t) = e^{-(6 \rightarrow 2) \gamma t}$.

(Kvansertkommentar: Dette svarer til en ekvivalent feilrate på $6 \rightarrow 2$. Over vi bort fra transisjoner over i feiltilstanden er sannsynligheten for å være i en tilstand med en feil i systemet $3 \rightarrow 0$ ($3 \rightarrow + 1/2$) $\Xi 3 \rightarrow 0$. Gitt vi er i denne tilstand er feilintensiteten $2 \rightarrow$. Intensiteten hendelser som gir systemfeil er da $3 \rightarrow 0$ ($2 \rightarrow$ dvs den ekvivalente systemfeilrate.)

- f) Se etterfølgende diagram.

- g) I nevner ser vi at leddet $3 \rightarrow 1/2$ er vesentlig større enn de øvrige, så $s_2 \Xi 3 \rightarrow 1/2$



I telleren vil leddene med 1. orden i \rightarrow dominere. Vi ser også at ingen av disse opplagt står enn det andre og tilslutt $s_1 \approx 2 \rightarrow \frac{1}{2} + 2 \rho \rightarrow \frac{1}{2} (1 \frac{1}{2} c)$ En tilslutt ming blir da:

$$U \approx \frac{2 \rightarrow}{\rho} + \frac{2 \rightarrow (1 \frac{1}{2} c)}{\frac{1}{2}} \quad (1.1)$$

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

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

$$U \approx \frac{2 \rightarrow}{\rho} + \frac{2 \rightarrow (1 \frac{1}{2} c)}{\frac{1}{2}} + \frac{6 \rightarrow^2}{\frac{1}{2}} + \frac{4 \rightarrow^2 (1 \frac{1}{2} c)}{\frac{1}{2} \frac{1}{2}} + \frac{4 \rightarrow^2}{\rho \frac{1}{2}} \quad (1.2)$$

hvor vi ser at 4. og 5. ledd er vesentlig mindre enn 3. og kan neglisjeres. 3. svarer til sannsynligheten 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 $3 \rightarrow \frac{1}{2}$). Intensiteten av andre ordensfeil i systemet er da $3 \rightarrow \frac{1}{2} 2 \rightarrow$ og disse en varighet på $\frac{1}{2}$. Vi har tilslutt nederste ledd tilslutt hvor alle nedemodi og parametre er med

$$U \approx \frac{2 \rightarrow}{\rho} + \frac{2 \rightarrow (1 \frac{1}{2} c)}{\frac{1}{2}} + \frac{6 \rightarrow^2}{\frac{1}{2}} \quad (1.3)$$

