Eksamen TTM4120 Pålitelige systemer 18. mai 2004
LØSNINGSSKISSE

a) Det skal etableres en transportforbindelse fra node 1 til node 3 . Anta at $C_{[i,j]} = \infty$ for alle $[i,j] \in \Omega_L$. Denne forbindelsen kan etableres direkte fra node 1 til 3 eller via mellomliggende noder. Videre, anta at utilgjengeligheten til nodene 1 og 3 er $U_1 = U_3 = 0$, mens for alle andre nettelementer er $U_i > 0$. Gjør nødvendige antakelser, lag en modell, og sett opp et uttrykk for utilgjengligheten $U(1,3)$ for transportforbindelse mellom node 1 og node 3 . Sett inn $U_2 = U_4 = U_5 = 10^{-3}$, og $U_{[i,j]} = 0.5 \cdot 10^{-1}$ for alle $[i,j] \in \Omega_L$, unntatt $U_{[1,3]} = 10^{-1}$ og beregn $U(1,3)$.

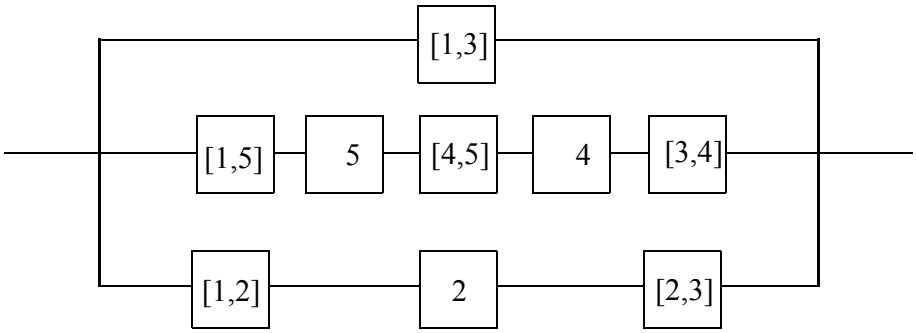
Antar

- uavhengighet mellom feil i nettelementene
- reparasjon i et nettelement er uavhengig av tilstanden til andre nettelementer

Lager pålitlighetskjema => ok siden $C_{[i,j]} = \infty$ for alle $[i,j] \in \Omega_L$

- kan neglisjere node 1 og 3 ettersom tilgjengeligheten er 1, de er feilfrie.

gir følgende pålitelighetsblokkskjema:



Figur 1 Pålitelighetsblokkskjema for transportforbindelsen 1->3.

og utilgjengelighet:

$$U(1,3) = U_{gren1} U_{gren2} U_{gren3} \tag{1}$$

hvor

$U_{gren1} = U_{[1,3]} = 0.1$

$U_{gren2} = 1 - (1 - U_{[1,5]}) \cdot (1 - U_5) \cdot (1 - U_{[4,5]}) \cdot (1 - U_4) \cdot (1 - U_{[3,4]}) = 0.1443$

$U_{gren3} = 1 - (1 - U_{[1,2]}) \cdot (1 - U_2) \cdot (1 - U_{[2,3]}) = 0.0984$

Innsatt tallverdier: $U(1,3) = 0.00142$

b) Definer et kapasitetsavhengig mål på påliteligheten til transporttjenesten mellom node 1 og 3. Hva er sannsynligheten for at node 5 har feilet? Angi uttrykket både symbolske og med nummeriske veridier som oppgitt ovenfor. Definér en identitetsfunksjon som angir om transporttjenesten mellom node 1 og 3 er tilgjengelig for et gitt basisfeilmodus. Angi verdien på denne funksjonen for alle basisfeilmodi for dette nettsegmentet.

Transporttjenesten mellom 1 og 3: $X(1, 3)$ krever kapasietet $C(1, 3) \geq 3$ kanaler.

Påliteligheten til $X(1, 3)$ defineres som tilgjengeligheten til $X(1, 3)$, som igjen kan deinferes som sannsynligheten for at $C(1, 3) \geq 3$,, dvs.

$$A(1, 3) = P(I(C(1, 3) \geq 3)) \tag{2}$$

hvor $I(x)$ er indikatorfunksjon som returnerer 1 når x er sann og 0 ellers.

Sannsynligheten for at (kun) node 5 har feilet er sannsynligheten for at

- node 5 har feilet
- ingen andre noder har feilet
- ingen linker har feilet.

Med symboler:

$$P(\Phi_5) = U_5 \cdot \prod_{\forall(i \in \Omega_N) \wedge i \neq 5} 1 - U_i \cdot \prod_{\forall(i \in \Omega_I)} 1 - U_i \tag{3}$$

Innsatt tallverdier:

$$P(\Phi_5) = 10^{-3} \cdot (1 - 10^{-3})^2 \cdot (1 - 0{,}5 \times 10^{-1})^5 \cdot (1 - 10^{-1}) = 6{,}95 \times 10^{-4} \tag{4}$$

Indikatorfunksjonen

$$I(C(1, 3) \geq 3, \Phi) = \begin{cases} 1 & \text{hvis kapasiteten } C(1, 3) \geq 3 \text{ når } \Phi \text{ her feilet} \\ 0 & \text{ellers} \end{cases} \tag{5}$$

Basisfeilmodi

- for nodene, $\Phi_i = \{i\}$ for alle $i \in \Omega_N$
- for linkene, $\Phi_6 = \{[1, 2]\}$, $\Phi_7 = \{[1, 3]\}$, $\Phi_8 = \{[1, 5]\}$, $\Phi_9 = \{[2, 3]\}$, $\Phi_{10} = \{[3, 4]\}$, $\Phi_{11} = \{[4, 5]\}$

Indikatorfunksjonen blir 1 for alle basisfeilmodi.

c) Definér basisfeilmodi på fysisk lag, Φ_x^{PHY}, og identifier korresponderende feilmodi på overliggende virtuelt lag, Φ_x^{PHY}, for hver av Φ_x^{PHY}. Angi verdi på identitetsfunksjonen for transporttjenesten mellom node 1 og 3 i det virtuelle nettet for alle

basisfeilmodi på fysisk lag. Uttrykk utilgjengeligheten av transporttjenesten mellom node 1 og 3 ved sannsynlighetene for feil på fysisk lag, dvs. $P(\Phi_x^{PHY})$. Anta at maksimalt en feil kan skje av gangen og kun på fysisk lag.

Basisfeilmodi på fysisk lag (noder er feilfrie)

- for linkene, $\Phi_1^{\text{PHY}} = \{[1, 2]\}$, $\Phi_2^{\text{PHY}} = \{[1, 5]\}$, $\Phi_3^{\text{PHY}} = \{[2, 3]\}$, $\Phi_4^{\text{PHY}} = \{[3, 4]\}$, $\Phi_5^{\text{PHY}} = \{[4, 5]\}$

Mappet til virtuelt lag og indikatorfunksjon

- $\Phi_1^{\text{PHY}} = \{[1, 2]\} \Rightarrow \Phi_1^{\text{VIR}} = \{[1, 2], [1, 3]\} \Rightarrow I(C(1, 3) \geq 3, \Phi_1^{\text{VIR}}) = 0$ (nede)
- $\Phi_2^{\text{PHY}} = \{[1, 5]\} \Rightarrow \Phi_2^{\text{VIR}} = \{[1, 5]\} \Rightarrow I(C(1, 3) \geq 3, \Phi_2^{\text{VIR}}) = 1$ (oppe)
- $\Phi_3^{\text{PHY}} = \{[2, 3]\} \Rightarrow \Phi_3^{\text{VIR}} = \{[2, 3], [1, 3]\} \Rightarrow I(C(1, 3) \geq 3, \Phi_3^{\text{VIR}}) = 0$ (nede)
- $\Phi_4^{\text{PHY}} = \{[3, 4]\} \Rightarrow \Phi_4^{\text{VIR}} = \{[3, 4]\} \Rightarrow I(C(1, 3) \geq 3, \Phi_4^{\text{VIR}}) = 1$ (oppe)
- $\Phi_5^{\text{PHY}} = \{[4, 5]\} \Rightarrow \Phi_5^{\text{VIR}} = \{[4, 5]\} \Rightarrow I(C(1, 3) \geq 3, \Phi_5^{\text{VIR}}) = 1$ (oppe)

Utilgjengeligheten antatt kun single fysiske feil:

$$U(1, 3) = P(\Phi_1^{\text{PHY}}) + P(\Phi_3^{\text{PHY}}) \tag{6}$$

d) Beskriv kort 3 ulike programvarepålitelighetsmål (software metrics) med vekt på hensikt, framgansmåte, og evt. styrker og svakheter ved disse.

Programvarepålitelighetsmål (generelt: enkelt, men ser bare p åsluttproduktet og ikke utviklingsprosessen)

- Direkte: teller kodelinjer - kan skille ulike kodelinjer (kommentarer, instruksjoner, deklarasjoner, osv.); dess fler dess større sjanse for feil
- Halstead: baserer seg på entropi - relaterer usikkerhet (upålitelighet) til antall operatorer og operander (forskjellige og instansieringer av disse); dess fler dess større sjanse for feil
- McCabe syklomatisk nummer: måler kontrollflytstukturer ved å lage avhengighetsgraf og telle antall mulige kontrollflytveier, dess fler dess større sjanse for feil.

e) Vi velger Duanes modell for å modellere pålitelighetsvekst. Nevn kort bakgrunn for modellen og antakelser som denne baserer seg på. Hvordan beskrives feilaktivering- og feilfjerningsprosessen med Duanes model?

Duanes modell:

- inspirert av hw modellering av pål. vekst
- basert på observasjon av at akkumulerte antall feil plottet mot tiden er en rett linje når begge aksene er logaritmiske
- ren empirisk modell, dvs. parametrene i modellen estimeres fra målinger
- betyr også: feilaktivering og feilfjerningsprosessene modelleres IKKE.

f) I Duanes modell blir den akkumulerte feilintensiteten ved tid t modellert som $Z(t) = E(N(t)) = \alpha \cdot t^{\beta}$. Hva representerer denne tiden t? Hvor mange feil antar modellen at programmet inneholdt ved tiden $t = 0$? Figur 4 viser det akkumulerte antall feil observert og akkumulert feilintensitet, $\bar{Z}(t)$, over tid t på en log-log skala. Estimér parametrene α og β.

Duanes modell er robust med hensyn på hva tiden t representerer. Kan være kalendertid, CPU forbruk, utviklingtid, osv.

Når tiden går mot uendelig går det kummulative antall feil også mot uendelig. Dette betyr at når programmet var nytt var det uendelig antall feil i det.

Estimerer parametre fra figuren $\bar{Z}(t) = \hat{\alpha} \cdot t^{\hat{\beta}}$

- α: leser av $\bar{Z}(t)$ for $t = 1 \Rightarrow \bar{Z}(1) = \alpha = 0.02$
- leser av av $\bar{Z}(1) = 0.02$ og av $\bar{Z}(10000) \approx 31$ og beregner stigningstallet ved

$$\hat{\beta} = \frac{\log \bar{Z}(10000) - \log \bar{Z}(1)}{\log 10000 - \log 1} = 0.8 \qquad (7)$$

g) Gjør nødvendige antakelser og beregn antall prosessinstansieringer av X for at tilgjengelighetskravet for tjenesten S_1 skal være oppfylt. Foreslå en distribusjon av disse.

- Nodene feiler og reparerers uavhengig av hverandre.
- Kommunikasjonen mellom nodene er feilfri.
- Prosessene har ingen interaksjon som medfører utbredelse av feiltilstander (dvs prosessene feiler uanhengig av tilstanden til andre prosesser)

Ser på et økende antall instansieringer

1: $A_{S_1}^1 = A_N = 0.9 < 0{,}995$, dvs. kravet er ikke oppfylt

2: $A_{S_1}^2 = 1 - (1 - A_N)^2 = 0.99 < 0{,}995$, dvs. kravet er ikke oppfylt

3: $A_{S_1}^3 = 1 - (1 - A_N)^3 = 0.999 < 0{,}995$, dvs. kravet er oppfylt

Disse tre prosessene kan distribueres på et vilkårlig utvalg av de 5 så lenge det ikke er mer enn 1 på en av nodene (hvorfor ikke?)

En mer "elegant" løsning er å løse følgende ligning:

$A_{S_1}^n = 1 - (1 - A_N)^n > 0.995$

som gir

$n > \frac{\log(0{,}005)}{\log(0{,}1)} = 2{,}3$ som gir heltallig $n = 3$.

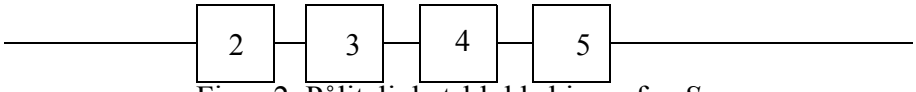
h) Funksjonssannsynligheten, $R_{S_2}(t)$, for tjenesten S_2 skal bestemmes. Vurder om pålitelighetsblokkskjema eller tilstandsdiagram kan og bør benyttes. Basert på din konklusjon, lag pålitelighetsblokkskjema og finn uttrykket for $R_{S_2}(t)$, eller lag tilstandsdiagram og sett opp likningssettet med sikte på å beregne $R_{S_2}(t)$.

Ettersom prosess-instansene er feilfrie sålenge nodene er feilfrie er det kun tilstanden til nodene som skal betraktes.

Ut fra kravene som er stilt til prosesstype Z ser vi at node 2,3,4 og 5 må virke for at tjeneste S_2 skal kunne leveres. Kravet til prosesstype Y er mindre strengt og vil alltid være oppfylt når kravet til Z er oppfylt. Når node 2-5 er operative så vil alltid kravet om 3 av 4 Y prosesser være oppfylt

Pålitelighetsblokskjema kan benyttes ettersom reparasjon ikke inntreffer før tjenesten er utilgjengelig. Pålitelighetsblokkskjema kan benyttes.

Dermed står vi igjen med en seriestruktur av 4 elementer i en pålitelighetsblokkskjema, se figuren under.

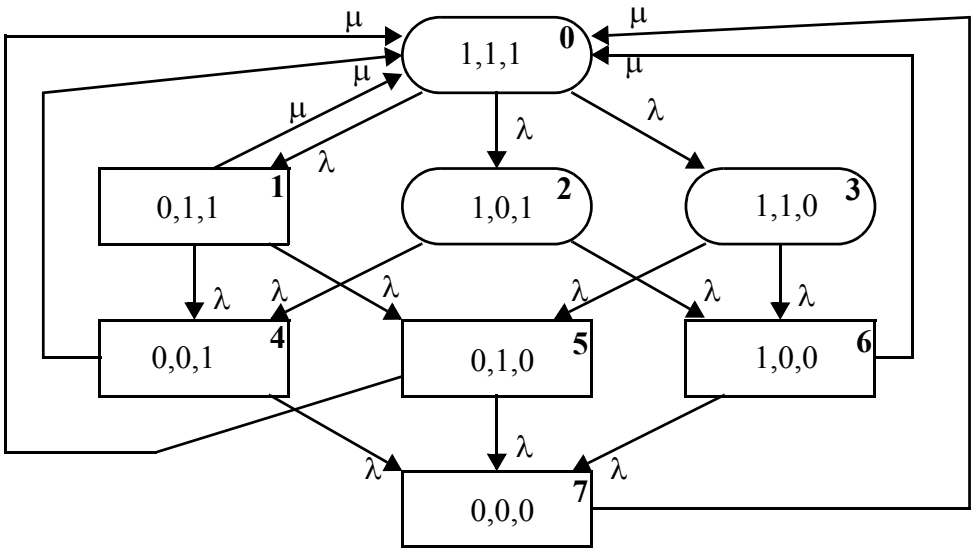


Figur 2 Pålitelighetsblokkskjema for S_2.

Funksjonssannsynligheten blir

$$R_{S_2}(t) = e^{-4\lambda t} \tag{8}$$

i) Etabler en tilstandmodell og sett opp likningsettet med sikte på å bestemme de stasjonær-tilgjengeligheten til tjenesten S_3 i dette reduserte systemet. Marker tydelig hvilke tilstander hvor tjenesten S_3 ikke kan leveres. Reparasjon og feil-antagelser er som i foregående oppgave.



Figur 3 Tilstandsdiagram for tjeneste S_3.

Ligningssett:

$$3\lambda p_0 = \mu(p_1 + p_3 + p_4 + p_6 + p_7)$$

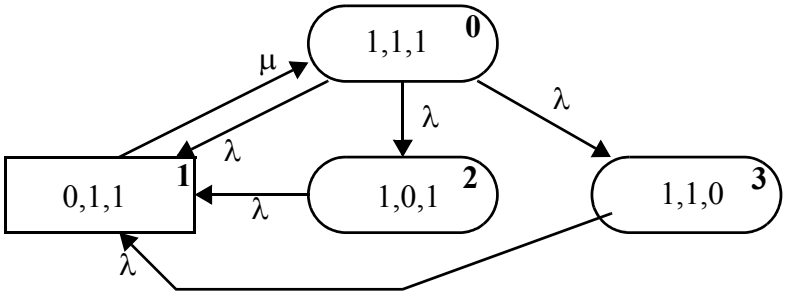
$$(2\lambda + \mu)p_1 = \lambda p_0$$

$$2\lambda p_2 = \lambda p_0$$
$$2\lambda p_3 = \lambda p_0$$
$$(\lambda + \mu) p_4 = \lambda (p_1 + p_2)$$
$$(\lambda + \mu) p_5 = \lambda (p_1 + p_3)$$
$$(\lambda + \mu) p_6 = \lambda (p_2 + p_3)$$
$$\mu p_7 = \lambda (p_4 + p_5 + p_6)$$

Normering:

$$p_0 + p_1 + p_2 + p_3 + p_4 + p_6 + p_7 = 1$$

Modellen kan reduseres ved ikke å eksamendere feiltilstandene videre (anta at rep. er mye kortere enn tid mellom feil).



Figur 4 Redusert tilstandsdiagram for tjeneste S_3.