Norges teknisk-naturvitenskapelige universitet
Institutt for telematikk

EKSAMEN I EMNE
TTM4120 PÅLITELIGE SYSTEMER

Faglig kontakt under eksamen: Poul Heegaard
Tlf.: 99286858

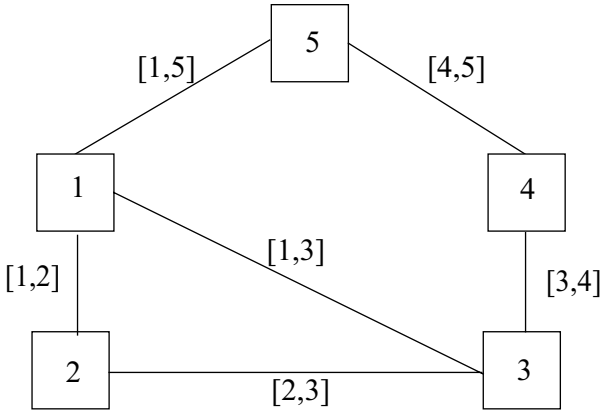
Eksamensdato:	18. mai 2004
Eksamenstid:	4 timer
Vekttall:	2,5 Vt
Tillatte hjelpemidler:	D
Språkform:	
Antall sider bokmål:	4
Antall sider nynorsk:	1
Antall sider engelsk:	4
Antall sider vedlegg:	0
Sensurdato[1]:	uke 24 - 2004

1. Merk! Studentene må primært gjøre seg kjent med sensur ved å oppsøke sensuroppslagene. Evt. telefoner om sensur må rettes til sensurtelefonene. Eksamenskontoret vil ikke kunne svare på slike telefoner.

BOKMÅL UTGAVE

For et nettsegment er et delvis maskenett definert. Dette består av to typer nettelementer, noder og linker. Noder er markert med indeks fra 1 til 5, mens linker er toveis (bidireksjonale) og identifisert ved endepunktene, dvs. link $[i, j]$ er toveis direkte link mellom nodene i og j.

Mengden av nettelementer angis som $\Omega = \Omega_N \cup \Omega_L$ hvor $\Omega_N = \{1, 2, 3, 4, 5\}$ er settet av alle noder, og $\Omega_L = \{[1, 2], [1, 3], [1, 5], [2, 3], [3, 4], [4, 5]\}$ er settet av alle linker, se figur 1.



Figur 1 Delvis maskenett

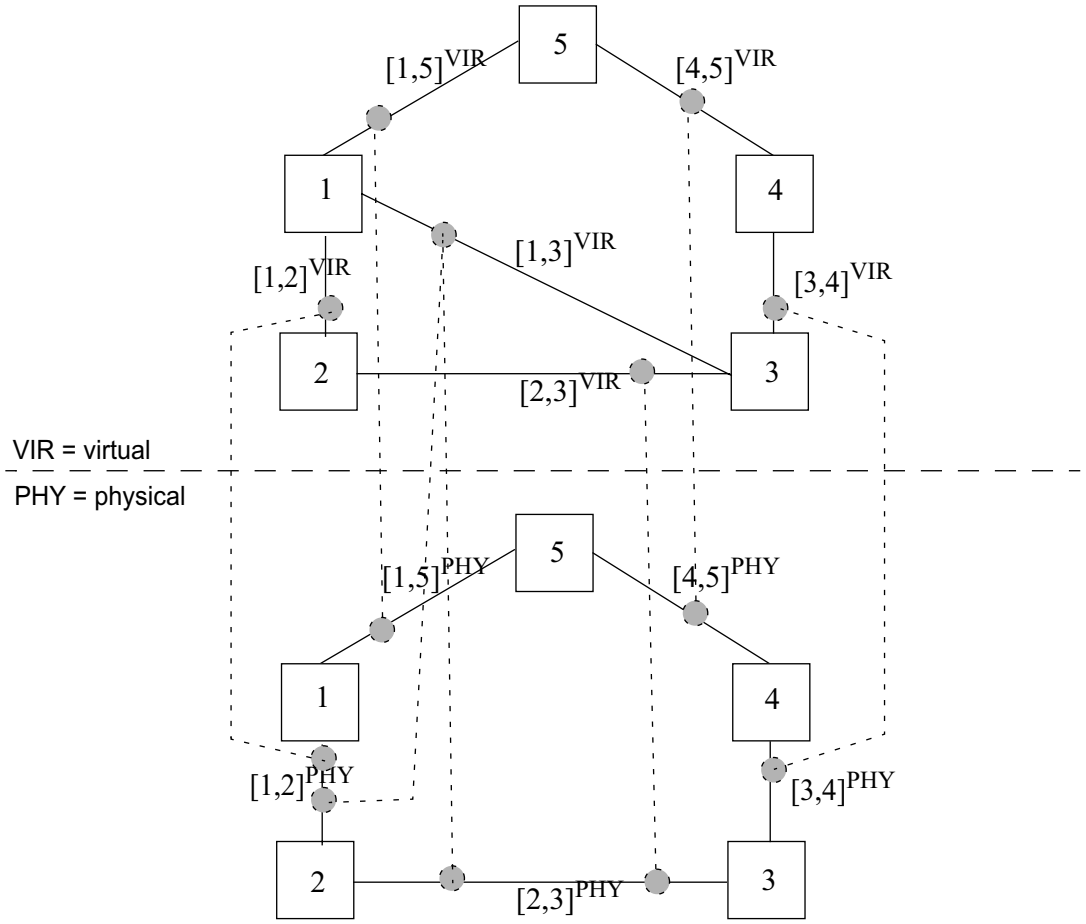
Kapasiteten på en link $[i, j]$ er $C_{[i, j]}$. Tilgjengeligheten og utilgjengeligheten for et nettelement angis som h.h.v. A_i og U_i hvor $i \in \Omega$.

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 utilgjengeligheten $U(1, 3)$ 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 $U(1, 3)$ numerisk.

La nå kapasiteten på hver link $[i, j]$ være $C_{[i, j]} = 2$ kanaler for $[i, j] \in \Omega_L$. Transporttjenesten mellom node 1 og 3 krever 3 kanaler. *Basisfeilmodi* (feiltilstander) for dette nettsegmentet er alle enkeltfeil, dvs. 1 node eller 1 link feiler.

b) Definere 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 numeriske verdier 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.

Topologien i det foregående er et virtuelt nett som er implementert over en fysisk ringtopologi. Hver node er unikt mappet til en fysisk node med samme identitet. Mappingen av linker i det virtuelle nettet, $[i, j]^{\text{VIR}}$ til linker i det fysiske nettet $[i, j]^{PHY}$ er vist i figur 2.

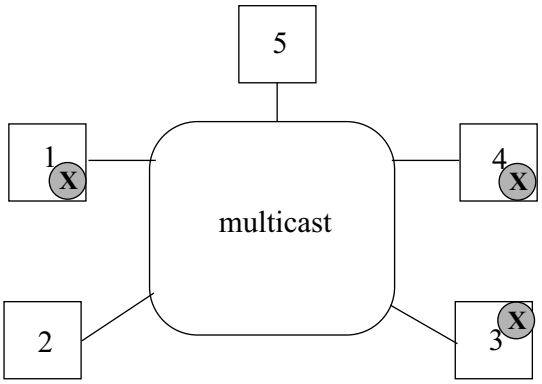


Figur 2 Mapping av virtuelt nett-topologi til underliggende fysisk topologi.

Anta at det ikke forekommer feil i nodene på fysisk lag.

c) Definér basisfeilmodi på fysisk lag, Φ_x^{PHY}, og identifiser korresponderende feilmodi, Φ_x^{VIR}, på overliggende virtuelt lag 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.

Nodene i nettet er vertsmaskiner i en distribuert prosesseringsomgivelse hvor 3 ulike prosesstyper, X, Y og Z kan instansieres på 1 eller flere av vertsmaskinene. Eksemplet i figur 3 viser distribusjon av 3 instanser av prosess X.



Figur 3 Eksempel på distribusjon av 3 instanser av prosesstype X.

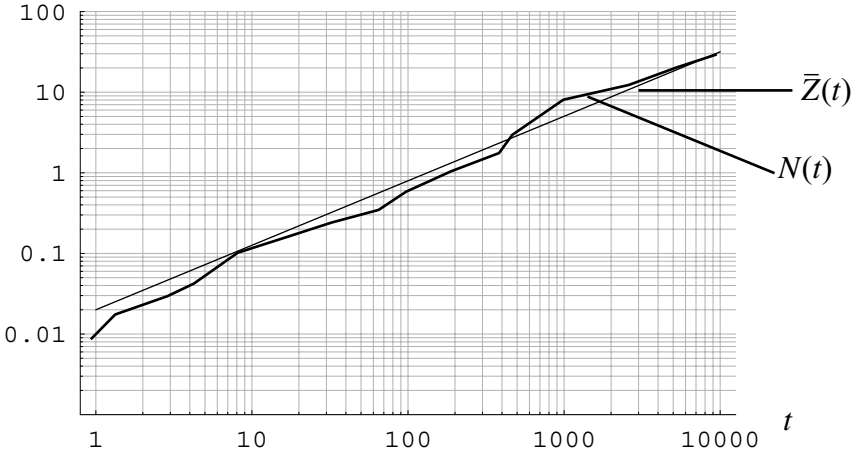
Vertsmaskinene inneholder avansert programvare for å håndtere alle aspekter ved prosessinstansiering, feilhåndering, og kommunikasjon mellom prosesser og mellom noder. Denne progamvaren er svært kritisk for at den distribuerte prosesseringsomgivelsen skal kunne levere den spesifisert tjenesten med god pålitelighet. Det er derfor viktig å evaluere påliteligheten til denne programvaren.

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

Programvaren gjennomgår testing og feil fjernes. Påliteligheten blir gradvis bedre og ønsket er å estimere når påliteligheten til programvaren er akseptabel for lansering.

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 modell?

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 estimert akkumulert feilintensitet, $\bar{Z}(t)$, over tid t på en log-log skala. Estimér parametrene α og β.



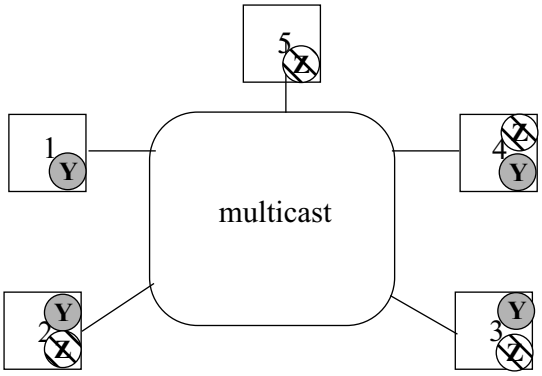
Figur 4 Plott av kumulativt antall progamvarefeil som funksjon av tiden.

Hver av nodene har tilgjengelighet $A_N = 0.9$. Kommunikasjonen mellom nodene kan antas feilfritt. En tjeneste, S_1, som skal leveres er avhengig av at minst en instans av prosess X er tilgjengelig. Tilgjengelighetskravet til tjenesten er $A_{S_1} > 0.995$.

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.

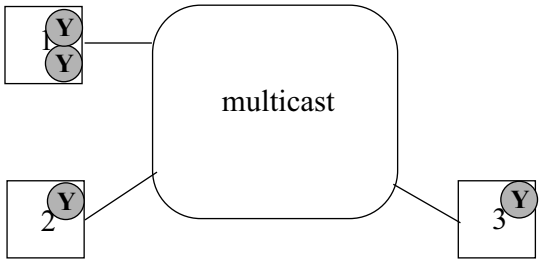
En annen tjeneste, S_2, er avhengig av at minst 3 instanser av prosess Y og 4 instanser av type Z er tilgjengelig for at tjenesten skal være tilgjengelig. Det antas at instansene ikke feiler så lenge noden er operativ. Ved feil i en node så stoppes instansene av Y og/eller Z på denne noden. Reparasjon skjer først når tjenesten S_2 er utilgjengelig. Reparasjon skjer med intensitet μ og medfører samtidig restart av samtlige noder og prosesser. Distribusjon av prosessene er som angitt i figur 5. Nodene har feilintensitet $\lambda_i = \lambda$, $i = 1, \ldots, 5$.

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 $R_{S_2}(t)$.



Figur 5 Distribusjon av prosess type Y og type Z.

For å spare vedlikhold så vurderes det å redusere antall noder til 3. Før dette besluttes må det vurderes om en av storkundene som er avhengig av tjenesten S_3 fortsatt får tilfredstillende kvalitet. Tjenesten S_3 er tilgjengelig når minst 3 prosess-instanser av type Y er tilgjengelig. Endringene er angitt i figur 6.



Figur 6 Re-distribusjon av prosess type Y

i) Etabler en tilstandmodell og sett opp likningsettet med sikte på å bestemme 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.

NYNORSK UTGÅVE

For ikkje å få ulike semantikk i bokmål og nynorsk oppgåvetekst så er inga eige nynorsk oppgåvetekst laga. Sjå i staden bokmåloppgåve på side 2-5.

Ved problem ta kontakt med faglærar.

ENGLISH EDITION[1]

In this task a network segment defined as a partial mesh network will be studied. It consists of two types of network elements; nodes and links. The nodes are indexed from 1 to 5, while links are bi-directional and indexed by their end nodes, i.e. link $[i, j]$ is the bi-directional direct link between node i and j.

The set of network elements are $\Omega = \Omega_N \cup \Omega_L$ where $\Omega_N = \{1, 2, 3, 4, 5\}$ is the set of all nodes, and $\Omega_L = \{[1, 2], [1, 3], [1, 5], [2, 3], [3, 4], [4, 5]\}$ is the set of all links, see Figure 1.

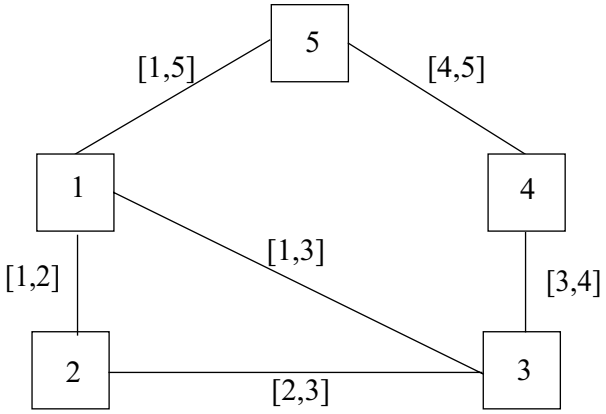


Figure 1 Partial mesh network.

The capacity of a link $[i, j]$ is $C_{[i, j]}$. The availability and unavailability of a network element is denoted A_i and U_i where $i \in \Omega$, respectively.

a) A transport connection between node 1 and 3 is to be established. Assume that $C_{[i, j]} = \infty$ for all $[i, j] \in \Omega_L$. This connection can be established directly between node 1 and 3 or via transit nodes in between. Assume that the unavailability of nodes 1 and 3 is $U_1 = U_3 = 0$, while for all other network elements the unavailability is $U_i > 0$. Make the necessary assumptions, create a model, and establish an expression of the unavailability $U(1, 3)$ for the transport connection between node 1 and node 3. Let $U_2 = U_4 = U_5 = 10^{-3}$, and $U_{[i, j]} = 0.5 \cdot 10^{-1}$ for all $[i, j] \in \Omega_L$, except $U_{[1, 3]} = 10^{-1}$ and calculate $U(1, 3)$ numerically.

Now, let the capacity of each link $[i, j]$ be $C_{[i, j]} = 2$ channels for $[i, j] \in \Omega_L$. The transport service between node 1 and 3 requires 3 channels. *The basic failure modes* (failure state) for this network segment is all single failure, i.e. one node or one link failed.

b) Define a measure of the dependability of the transport service between node 1 and 3 that takes the capacity into account. What is the probability that node 5 has failed? Give both the symbolic expression and calculate the numerical value based on the parameters given above. Define an identity function that reflects the availability of transport service between node 1 and 3, given a specific failure mode. Determine the value of this indicator function for all basic failure modes of this network segment.

1. If there are any differences between the Norwegian and English versions in semantics, the Norwegian version is superior.

The topology in the previous is considered as a virtual network implemented on top of a physical ring topology. There is a one-to-one mapping between each node in the virtual network and the nodes in the physical network. The mapping of links in the virtual network, $[i, j]^{\text{VIR}}$, to links in the physical network, $[i, j]^{PHY}$, is given in Figure 2.

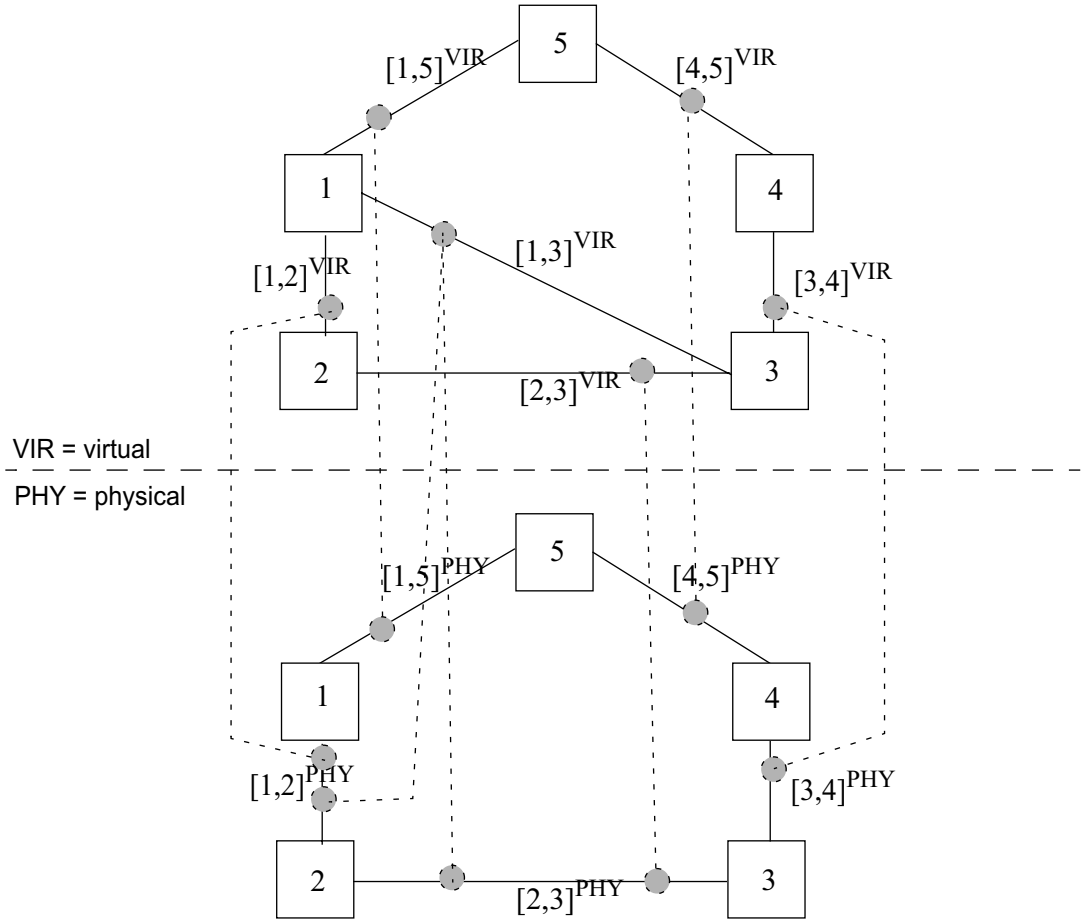


Figure 2 Mapping between the virtual and physical network topologies.

Assume no failure in the nodes in the physical network.

c) Define basic failure mode in the physical network, Φ_x^{PHY}, and identify the corresponding failure modes in the overlaid virtual network, Φ_x^{VIR}, for each of the Φ_x^{PHY}. Determine the value of the identity function for the transport service between node 1 and 3 in the virtual network for each basic failure mode in the physical network. Express the unavailability of this transport service by the probabilities of failure in physical network, i.e. the $P(\Phi_x^{PHY})$. Assume only single failures in the physical network.

The nodes in the network are host machines in a distributed processing environment where 3 different process types might be instantiated. The example in Figure 3 shows a distribution of 3 instances of process type X.

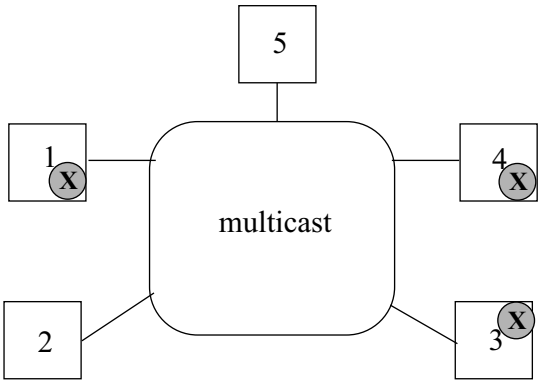


Figure 3 Example of 3 instances of process type X.

The host machines executes advanced software for management of all aspects related to process instantiations, fault managements, communication between processes and between nodes. This software is critical for the correct operation of the distributed processing environment. Hence, it is important to evaluate the dependability of this software.

d) Describe briefly 3 different software metrics with respect to purpose, approach, and their potentially strengths and weaknesses.

The software is tested and debugged. The dependability is gradually increased. The objective is to estimate the time when the software reliability is acceptable for release.

e) We look at Duane's model for software reliability growth. Describe briefly the background and assumptions of this model. How is the fault activation and removal process modelled?

f) In Duane's model the cumulative failure intensity at time t is modelled as $Z(t) = E(N(t)) = \alpha \cdot t^{\beta}$. What is the time t representing? What is the expected number of failures at time $t = 0$ assumed in this model? Figure 4 shows the cumulative number of software failures and estimated cumulative failure intensity, $\bar{Z}(t)$, as function of the time t on a log-log scale. Estimate the parameters α and β.

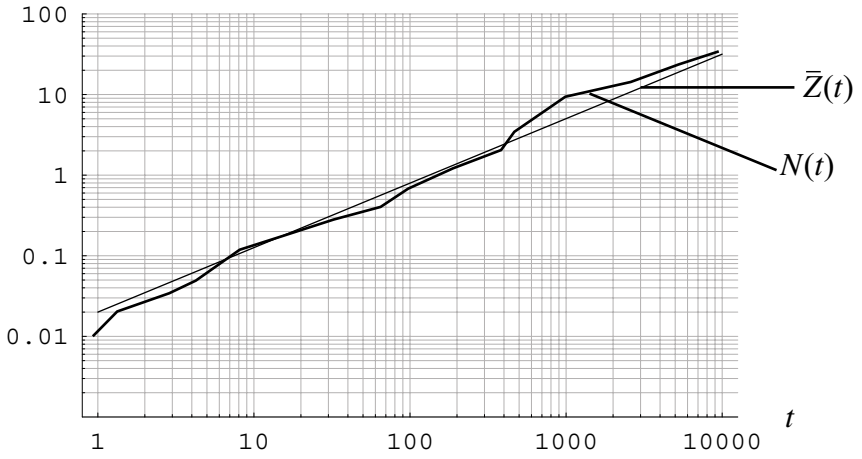


Figure 4 Plot of the cumulative number of software failures as function of the time.

Each node has an availability of $A_N = 0.9$. The communication between the nodes is always available. A service, S_1, depends on that at least one instance of process X is available. The availability requirement of the service is set to $A_{S_1} > 0.995$.

g) Make necessary assumptions and determine the number of instances of process type X necessary to meet the availability requirement of service S_1. Propose a distribution of these instances.

An other service, S_2, depends on the availability of 4 instances of process type Z and at least 3 instances of process type Y. It is assumed no instance failures as long as the node is operational. On a node failure, the corresponding instances will stop. A repair is postponed until the service S_2 is unavailable. The repair intensity is μ and implies that all nodes are restarted and their processes are re-instantiated. The distribution of the processes are according to Figure 5. The node failure intensities are $\lambda_i = \lambda, \forall i$.

h) The reliability function, $R_{S_2}(t)$, for the service S_2 is to be determined. Discuss whether the reliability block diagram or state diagram approach can and should be used. Based on your conclusion, establish either a reliability block diagram and determine an expression for $R_{S_2}(t)$, or establish a state diagram and the corresponding set of equations to determine $R_{S_2}(t)$.

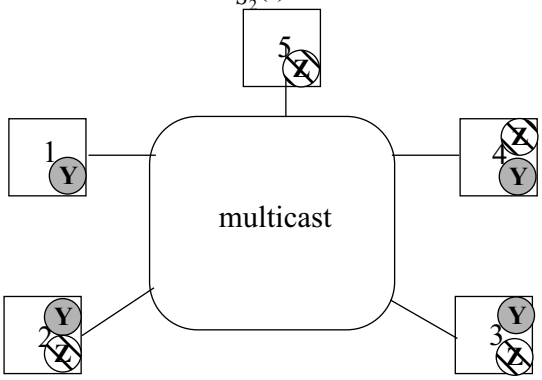


Figure 5 Distribution of process type Y and type Z.

To save money on management the number of nodes is considered to be reduced to 3, The decision depends on whether it is possible to maintain a satisfactory quality of service S_3 essential for an important customer. The service is available when at least 3 instances of process type Y are available. The changes are illustrated in Figure 6.

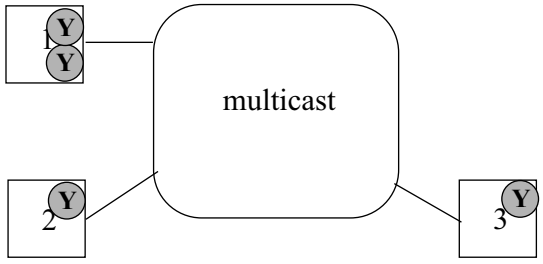


Figure 6 Re-distribution of process type Y

i) Establish a state model and a set of equations in order to determine the steady state availability for service S_3. Indicate clearly in the state diagram where the service is not available. The node failure and repair assumptions are similar to the assumptions in previous task.