Norwegian University of Science and Technology
Department of Telematics

Contact during exam [Faglig kontakt under eksamen]:
Bjarne E. Helvik (92667)

EXAM IN COURSE [EKSAMEN I EMNE]
TTM4120 Dependable Systems [Pålitelige systemer]

Tuesday [Tirsdag] 2010-05-25
09:00 – 13:00

The English version starts on page 2.

Den norske bokmålsutgaven starter på side 5.

Hjelpemidler:
D - No printed or handwritten material is allowed. Predefined simple calculator [Ingen trykte eller håndskrevne hjelpemidler tillatt. Forhåndsbestemt enkel kalkulator]

Sensur 2010-06-16

English version[1]

This exam deals with some dependability issues related to a server park. It has a hardware architecture as illustrated in Figure 1. The servers are divided into two groups, each having its individual independent power supply. The internal communication system and the access to the Internet are duplicated in two separate sides, so a bus and/or a router on one side may fail without disturbing the operation of the system. The servers, the routers, the internal communication buses and the power supplies fail with constant failure rates λ_s, λ_r, λ_b and λ_p respectively. Failures occur independently of each other. The other elements indicated may be assumed to be fault free.

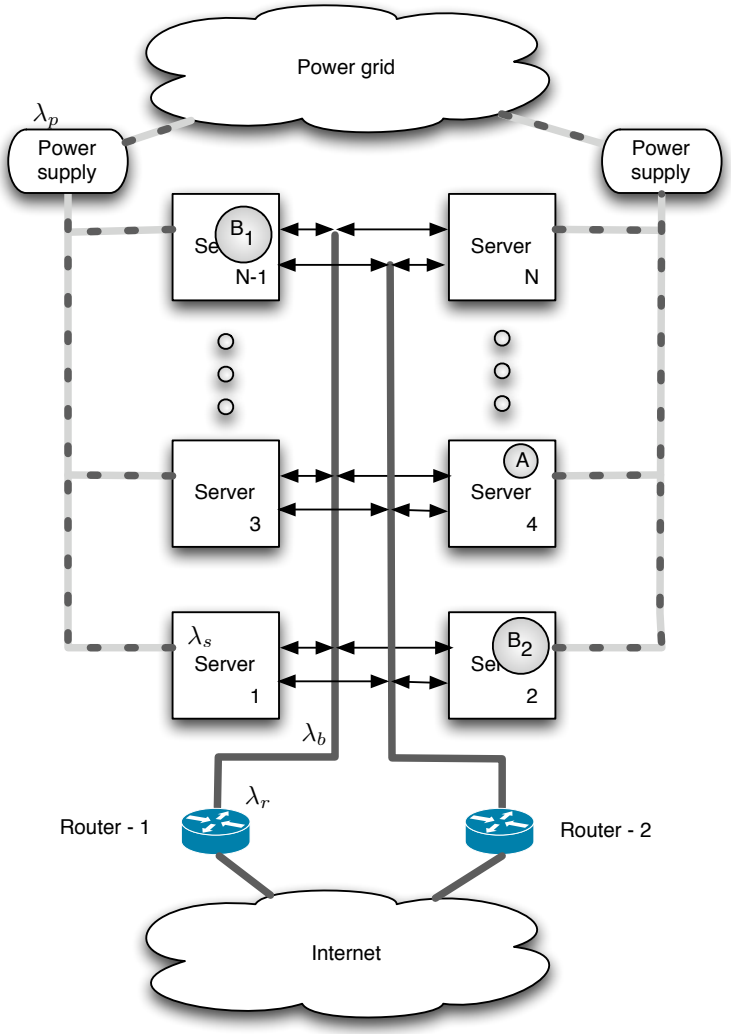

Figure 1: Hardware architecture of the server park.

[1] In case of divergence between the English and the Norwegian version, the English version prevails.

a) Assume that the system starts and all system entities are working at $t = 0$. What is the failure intensity, $z_A(0)$ at this point in time of a process A running on server 4? Motivate the answer. Give the formal definitions of failure intensity, $z(t)$, and failure rate, $\lambda(t)$. What are the relation between the failure intensity $z_A(0)$ and the failure rate $\lambda_A(0)$ at the beginning of system operation?

b) If there are no repairs in the system, determine the reliability function $R_A(t)$ of process A. Use this result to show how we may find its failure rate $\lambda_A(t)$. What is the limit of the failure rate when the process has been operational for a long period, i.e., the limit $\lambda_A(\infty)$? It is sufficient that the result is obtained by a direct (physical) argument.

c) Assume that all system entities are repaired independently of each other and have a constant repair time of d_x, where $x, = s, r, b, p$ according to the type of entity. What is the asymptotic availability, A_x, of an entity of type x? We would like to obtain the asymptotic availability of the the server park, A_{park}, when we require that at least K, where $N \geq K > N/2$, out of the the N servers must provide service towards the Internet for the system to be operational. What modelling method may be used? Motivate the answer. Make a dependability model of the server park and obtain an expression for A_{park}. Establish the equations necessary to obtain the mean time between failures of the server park, $\text{MTBF}_{\text{park}}$. Note that it is *not* necessary to solve or reduce the equations.

On the servers shown in Figure 1 runs a middleware, JaSoS used in the laboratory of the course, supporting the processes. The middleware is not perfect, so a server failure will with probability $1-c$ crash the middleware platform, i.e., processing on all servers stops. The middleware is restarted again (on the non-failed servers) in a negative exponentially distributed time with expectation d_c. Assume that the other repair times in the system are negative exponentially distributed as well, with expectations d_x, where $x, = s, r, b, p$ according to the type of entity. The active repair times are independent. However, at most one failure is repaired at a time.

Two processes, B_1 and B_2, provides the same service. There is a huge number of clients using this service. Each client interaction involves considerable computations. If these are interrupted because of failures, the intermediate state of client requests may be lost without causing a failure in the service provisioning. However, the final state caused by a request should be maintained and be available for further processing also after a server failure. The processes operate load shared and one may take the load of the other if it fails. They run on server $N-1$ and 2, and will not be reallocated to or restarted on another server if these fails, but they will be restarted on the same server after it is repaired.

d) Taking into account the middleware, what is the failure intensity of process A, regarded in Question a), when all system entities are working?

In the following, the process pair B and the service they provide are regarded. To simplify, assume that:

- all servers but $N-1$ and 2 have zero repair time, i.e., $d_s^{(z)} \to 0$ for $z = 1, 3, \ldots, N-2, N$ and $d_s^{(z)} > 0$ for $z = 2, N-1$;

- The routers and internal communication do not fail, i.e., $\lambda_r = \lambda_b \to 0$.
- It is not necessary to expand the state diagram further (include more failure events) when the service of B has failed.
- Unpowered servers will not fail.

Under the above assumptions and the further assumption that the power supplies do not fail, i.e., $\lambda_p \to 0$, establish a state diagram (Markov model) that may be used to determine the availability of the service provided by the process pair B, $A_B(t)$.

Next, *remove* the assumption that the power supplies does not fail, i.e., $\lambda_p > 0$, and extend the model to include this cause of failure.

In the modelling, identify the operational mode of each state clearly. Indicate whether the service is available or not in each state. Show which part of the model (i.e. which states and transitions) that describes the case without power supply failures.

e) JaSoS (as well as some other group communication systems) distinguish between internal and external group invocations. Explain what is meant by internal and external group invocations, and the rationale for this division. What is the difference between anycast and multicast invocations? Outline briefly how you would apply these operations to make the processes B_1 and B_2 to provide a service tolerant to single server failures.

The middleware platform, JaSoS, is continuously debugged and improved to increase c, i.e. to improve its reliability. It is hypothesized that this reliability growth may be modelled by the relation $z_p(t) = \alpha + \beta \exp(\delta t)$, where in the above context $z_p(t) = N\lambda_s(1 - c(t))$.

f) Give a short physical interpretation of the three parameters α, β and δ, and indicate their range when we require that the model should be physical and that we in fact have a growth. According to this model, what is the expected number of platform crashes (failures) in the interval $[0, \tau]$, and what is the probability that there is no crashes (failures) in the interval, as a function of the model parameters? We have observed crashes/failures at the times $t_1, t_2, \ldots, t_n$. Establish a set of equations that may be used to estimate the three parameters. What method do you use?

Given: The likelihood function of an inhomogeneous Poisson process with intensity $z(t)$ where events takes place at $x_1, x_2, \cdots, x_m$ is $L(x_1, x_2, \cdots, x_m) = \exp(-\int_0^{x_m} z(t)dt) \cdot \prod_{i=1}^{m} z(x_i)$.

Norsk bokmål utgave[2]

Denne eksamenen omhandler noen pålitelighetsspørsmål knyttet til en tjenerpark. Den har en maskinvarearkitektur som illustrert i figur 1. Tjenerne er delt i to grupper, hver med sin egen uavhengige strømtilførsel. Den interne kommunikasjonen og tilgang til Internett er duplisert i to separate sider, slik at en buss og/eller en ruter på den ene siden kan feile uten å forstyrre driften av systemet. Tjenerne, ruterne, de interne kommunikasjonsbussene og strømforsyningene feiler med konstante feilrater på henholdsvis λ_s, λ_r, λ_b og λ_p. Feil inntreffer uavhengig av hverandre. De andre elementene som er angitt kan antas å være feilfrie.

a) Anta at systemet starter og alle systemenhetene er arbeidende på tidspunkt $t = 0$. Hva er feilintensiteten, på dette tidspunktet, til en prosess A som kjører på tjener 4, $z_A(0)$? Begrunn svaret. Gi de formelle definisjonene av feilintensitet, $z(t)$, og feilrate, $\lambda(t)$. Hva er sammenhengen mellom feilintensiteten $z_A(0)$ og feilraten $\lambda_A(0)$ ved start?

b) Anta at feilte enheter i systemet ikke repareres. Bestem pålitelighetsfunksjonen $R_A(t)$ for prosess A. Bruk dette resultatet til å vise hvordan vi kan finne feilraten $\lambda_A(t)$. Hva er grensen for feilraten når prosessen har vært operativt i en lang periode, med andre ord, grensen $\lambda_A(\infty)$. Det er tilstrekkelig at svaret finnes ved en direkte (fysikalsk) argumentasjon.

c) Anta at alle enheter i systemet blir reparert uavhengig av hverandre og at vi har konstante reparasjonstider på d_x, hvor $x = s, r, b, p$ i henhold til type enhet. Hva er den asymptotiske tilgjengeligheten, A_x, av en enhet av type x? Vi ønsker å finne den asymptotiske tilgjengeligheten til tjenerenparken, A_{park}, når vi krever at minst K, der $N \geq K > N/2$, av de N tjenerne må yte service mot Internett for at systemet skal være operativt. Hvilken modelleringsmetode kan brukes? Begrunn svaret. Lag en pålitelighetsmodell av tjenerparken og finn et uttrykk for A_{park}. Sett opp et sett av likninger som kan benyttes for å finne midlere tid mellom feil av tjenerparken, $\text{MTBF}_{\text{park}}$. Merk at det *ikke* er nødvendig å løse eller redusere ligningene.

På tjenerne vist i figur 1 kjører en mellomvare, JaSoS som ble brukt i laboratoriedelen av kurset, for å understøtte prosessene. Denne mellomvaren er ikke perfekt, slik at når en tjener feiler vil med sannsynlighet $1 - c$ mellomvareplattformen krasje, dvs. prosessering på alle tjenerne stopper. Mellomvaren starter igjen (på ikke-feilte tjenere) i løpet av en negativt eksponensielt fordelt tid med forventning d_c. Anta at de andre reparasjonstidene i systemet også er negativt eksponensielt fordelte med forventninger d_x, hvor $x = s, r, b, p$ i henhold til type enhet. De aktive reparasjonstidene er uavhengige av hverandre, men kun en feil blir reparert av gangen.

De to prosessene, B_1 og B_2, leverer den samme tjenesten. Det er et stort antall klienter som bruker denne tjenesten. Hver klientforespørsel innebærer betydelige beregninger. Hvis disse blir avbrutt pga. feil, kan den foreløpige tilstanden knyttet til håndteringen av klientforespørselen gå tapt uten at det forårsaker feil i tjenesteleveransen. Imidlertid må sluttilstanden som er resultatet av en forespørsel,

[2] I tilfelle uoverensstemmelse mellom den engelske og norske utgaven, er det den engelske som er gjeldende. Engelske betegnelser anvendes hvor ingen norsk oversettelse ble funnet.

beholdes og være tilgjengelig for videre bearbeiding også etter at en tjener har feilet. Prosessene opererer lastdelt og den ene kan ta lasten til den andre dersom den feiler. De kjører på tjenerne $N-1$ og 2, og vil ikke bli overflyttet til eller startet på nytt på en annen tjener om de feiler. De vil bli startet på nytt på den samme tjeneren etter at den er reparert.

d) Ta hensyn til mellomvaren, hva er nå feilintensiteten til prosess A, betraktet i spørsmål a), når alle systemenheter er arbeidende?

I det følgende betraktes prosessparet B og den tjenesten de leverer. For å forenkle, anta at:

- alle tjenere, untatt $N-1$ og 2 har ingen reparasjonstid (øyeblikkelig reparasjon), dvs. $d_s^{(z)} \to 0$ for $z = 1, 3, \ldots, N-2, N$ og $d_s^{(z)} > 0$ for $z = 2, N-1$;
- rutere og intern kommunikasjon feiler ikke, dvs. $\lambda_r = \lambda_b \to 0$.
- det er ikke nødvendig å utvikle tilstandsdiagrammet videre (inkludere flere feilhendelser) når tjenesten til B har feilet.
- tjenere uten strømtilførsel vil ikke feile.

Under de ovennevnte antakelsene og den ytterligere antakelsen at strømtilførselen ikke feiler, dvs. $\lambda_p \to 0$, etabler et tilstandsdiagram (Markov-modell) som kan brukes til å bestemme tilgjengeligheten av tjenesten som tilbys av prosessparet B, $A_B(t)$.

Deretter, *fjern* antakelsen om at strømforsyningene ikke feiler, dvs. anta at $\lambda_p > 0$, og utvid modellen til å inkludere også denne feilårsaken.

I modelleringen, identifiser tydelig det operasjonelle modus for hver tilstand. Vis om tjenesten er tilgjengelig eller ikke i hver av tilstandene. Vis hvilken del av modellen (dvs. hvilke tilstander og overganger) som beskriver tilfellet uten strømforsyningsfeil.

e) JaSoS (samt noen andre gruppekommunikasjonssystem) skiller mellom interne og eksterne gruppe-"invocations". Forklar hva som menes med interne og eksterne gruppe-"invocations", og grunnen til denne delingen. Hva er forskjellen mellom "anycast" og "multicast" "invocations"? Beskriv kort hvordan du ville anvende disse operasjonene for å få prosessene B_1 og B_2 til å yte en tjeneste som tolererer at en enkelt tjener feiler.

Mellomvare plattformen, JaSoS, blir kontinuerlig feilsøkt og forbedret for å øke c, dvs. for å forbedre påliteligheten. Det er en hypotese at denne pålitelighetsveksten kan modellers av sammenhengen $z_p(t) = \alpha + \beta \exp(\delta t)$, hvor i ovennevnte sammenheng $z_p(t) = N\lambda_s(1 - c(t))$.

f) Gi en kort fysisk tolkning av de tre parametrene α, β og δ, og angi deres aktuelle tallområde når vi krever at modellen skal være fysikalsk og at vi faktisk har en vekst. Ifølge denne modellen, hva er forventet antall plattformkrasj (feil) i intervallet $[0, \tau]$, og hva er sannsynligheten for at det ikke er noen krasj (feil) i intervallet, som funksjon av modellens parametere?

Vi har observert krasj/feil ved tidspunktene $t_1, t_2, \ldots, t_n$. Etablere et sett av likninger som kan brukes til å estimere de tre parameterene. Hvilken metode bruker du?

Gitt: "Likelihood"-funksjonen til en inhomogen Poissonprosess med intensitet $z(t)$ der hendelser finner sted ved tidene $x_1, x_{2,} \cdots, x_m$ er $L(x_1, x_{2,} \cdots, x_m) = \exp(-\int_0^{x_m} z(t)dt) \cdot \prod_{i=1}^{m} z(x_i)$.