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]

Thursday [Torsdag] 2007-05-31
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 kalulator]

Sensur week 25, 2007

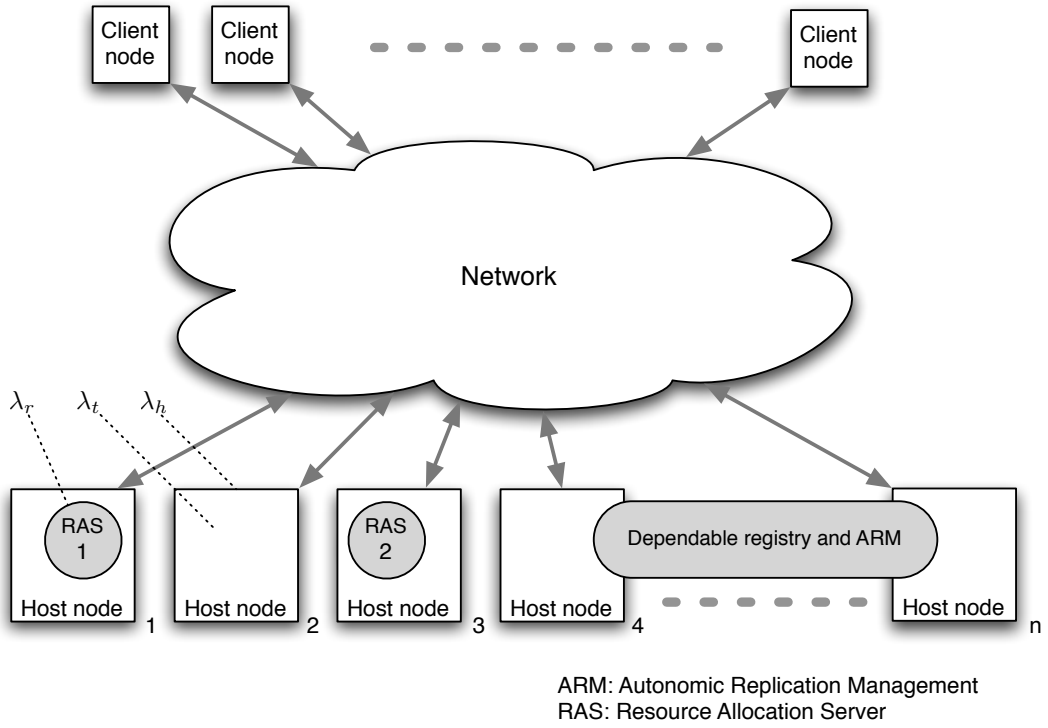

Figure 1: Illustration of system studied.

English version[1]

This exam will use as its basis a system providing a resource allocation service, similar to the one developed and studied by the students during the course. The main difference is that it is extended with an autonomic replication management (ARM) module as presented in the course curriculum. The core functionality of ARM, the replication manager (RM) enables us to extend the failure detection, and to reconfigure the system in case of host node and replica failures, as described in the syllabus. In normal operation, the resource allocation service is provided by two load shared resource allocation servers (RAS). In case of a failure, the remaining server will take the entire load, and, if feasible, the RM will create a new RAS, which will synchronize with the remaining replica and take a part of the load. The RAS and interaction between clients and servers are handled by the Jgroup middleware. For the sake of simplicity, it is assumed that the clients, the network as well as the dependable registry (DR) and the RM do not fail. A sketch of the system is shown in Figure 1. The rate of permanent and temporary host node failures are λ_h and λ_t respectively. A RAS replica fails with a rate λ_r. All failures are independent and are crash failures.

a) Define what is meant by a crash failure. Why do we often design system units to have this

[1]In case of divergence between the English and the Norwegian version; the English version is in force.

behaviour when they fail? What is the term for the most likely (dominating) failure behaviour of a system unit?

b) Define verbally the reliability of a system, and give the mathematical definition of the reliability function for a system which is as new when service/system is started. If a system is modelled by a reliability block diagram and this diagram shall be used to predict the reliability function of the system, what are the requirements (assumptions that must be made) for each of the system elements if they are modelled as blocks in the diagram?

c) We are interested in finding the service life time if the system presented in the introduction is put into operation and left without manual maintenance, i.e., when a host node fails it is not repaired. The RM will seek to maintain a working configuration of the service. Short down time periods during reconfiguration are, when dealing with this question, acceptable. The system has n host nodes, each having a failure rate λ_h. Nodes fail independently of each other. Argue very briefly why the requirements mentioned in b) are met. Find expressions for the expected life time of the service, t_L, and the time that the system will survive with a probability of 0.9, $t_{0.9}$.

In the following, the system will also undergo manual maintenance (repair). The expected manual repair time of a host is μ_h^{-1}. The expected restart time of a host after it has crashed due to a non-permanent fault is μ_t^{-1}. The expected time it takes for the RM and Jgroup to create a new replica on a running host (including the time possibly needed to synchronize with the other replica) is μ_n^{-1}. We have that $\mu_n \gg \mu_t \gg \mu_h$.

d) Use a reliability block diagram to obtain an approximation of the asymptotic availability of the resource allocation service when the system has the minimal number of host nodes ($n = 2$): A_2. If additional assumptions are necessary, state these..

e) Obtain an approximation of the asymptotic availability of the resource allocation service when the system has a large number of host nodes (n approaches infinity): A_∞. (Hint: A reliability block diagram may be used.) If additional assumptions are necessary, state these..

f) In order to create new replicas after failures, ARM must become aware of the failure. Describe two means used in the Jgroup/ARM system for failure discovery.

The models of the service availability developed under d) and e) are not sufficiently accurate for the purpose, and a more detailed model is needed. To keep the model simple, assume that $\lambda_t = 0$. Assume that at most one permanent failure in the system may be rectified at a time. Studies of the ARM fault management have shown that, as long as there are other non-failed replicas in a group, a single replica may be started and synchronized in a negative exponentially distributed time with expectation μ_n^{-1} after a replica failure in the group. If all, or the last, replicas in the group fail, the entire group is restarted in a negative exponentially distributed time with expectation μ_{nn}^{-1} after the last replica failure.

g) Give two reasons why a reliability block diagram *can not* be used for analysis in this case. Draw a complete state diagram of the system providing the service, i.e., include all states and transitions, for the case where $n = 3$. Denote a state with $[a, b]$ where a is the number of working hosts in the system and b is the number of working RAS. (Hint: to ease the devising, as well as the interpretation, of the diagram, take care to give it a structure reflecting the operational modes of and the symmetries in the system.) Indicate which states that represent a working and failed service.

In the following question, we are interested in the reliability of the resource allocation service as seen from a client. Assume that a resource is allocated to a client for identically independently negatively exponentially distributed times with expectation θ^{-1}, i.e., the client refreshes its resource allocation according to a Poisson process with intensity θ. A client experiences a service failure when it, at the expiration of the allocation time, finds the service down. When the regarded service delivery starts, we assume the system is in steady state[2]. The time until the service delivery to the client fails is denoted T_F. The reliability function of the system as seen from the client $R_c(t) = \Pr(T_F > t)$ should be obtained.

h) Extend and/or modify the the state diagram found in question g) so it may be used to find $R_c(t)$. (NB! make it clear which part of the diagram that belongs to question g) and which part that belongs to this question.)[3]

[2]The system is stationary.

[3]If question g) is not solved, use a generic (arbitrary) diagram with up- and down-states and extend this diagram instead.

Norsk bokmål utgave[4]

Denne eksamenen tar som utgangspunkt et system som leverer en ressursallokeringstjenste tilsvarende den som ble utviklet og studert av studentene i løpet av kurset. Den vesentligste forskjellen er at systemet også har en autonom replikahåndtering (autonomic replication management - ARM) modul. En sentral funksjonalitet i denne er replikahåndtereren (replication manager - RM), som gir flere feildetekteringsmuligheter og gjør det mulig å rekonfigurere systemet dersom en vertsnode eller et replika feiler. Dette som beskrevet i pensumlitteraturen. I normal drift er ressursallokeringstjenesten levert av to lastdelte ressursallokeringstjenere (resource allocation servers - RAS). I tilfelle en feiler, så vil den gjenværende ta hele lasten, og hvis mulig vil RM opprette en ny RAS, som vil synkronisere seg med den gjenværende og ta sin del av lasten.

RASene, og interaksjonene mellom klienter og tjenere er håndtert av Jgroup mellomvaren. For enkelhets skyld antas det at klientene, nettet såvel som det pålitelige registeret (dependable registry - DR) samt RMen ikke feiler. En skisse er vist i Figur 1 på side 2.

Raten av permanente og temporære vertsnodefeil er henholdsvis λ_h og λ_t. Et RAS replika feiler med raten λ_r. Alle feil er uavhengige og er krasj feil (crash failures).

a) Definer hva som menes med en krasj feil (crash failure). Hvorfor tilstreber en ofte å gi systemenheter denne oppførselen ved feil? Hva er betegnelsen på den mest sannsynlige (dominerende) feiloppførselen til en systemenhet?

b) Definer verbalt hva som menes med funksjonssikkerheten (the reliabiliy) til et system, og gi en matematisk definisjon av funksjonssannsynligheten (the reliability function) til et system som er som nytt idet det, og tjenesten det leverer, startes. Dersom et system skal modelleres som et pålitelighetsblokkskjema, og vi ønsker å bruke dette for å bestemme funksjonssannsynligheten til systemet, hvilke forutsetninger stiller dette til (antagelser må gjøres om) de systemelementene som modelleres som blokker i diagrammet?

c) Vi er interessert i å finne levetiden til tjenesten dersom den blir satt i drift i et system som ikke har noe manuelt vedlikehold. Dvs. dersom en vertsnode feiler, vil den ikke bli reparert. RM vil forsøke å opprettholde en arbeidende konfigurasjon for tjenesten. Korte nedetider mens rekonfigurering foregår er akseptable. (Gjelder kun besvarelsen av dette spørsmålet.) Systemet har n vertsnoder, hvor hver av disse har en feilrate λ_h. Nodene feiler uavhengig av hverandre. Forklar meget kort hvorfor kravene nevnt i punkt b) er oppfylt. Finn uttrykk for den forventede levetid til tjenesten, t_L, og tiden systemet vil overleve med sannsynlighet 0.9, $t_{0.9}$.

I det etterfølgende vil systemet også ha manuelt vedlikehold (reparasjon). Den forventede manuelle reparasjonstiden av en vert er μ_h^{-1}. Den forventede restarttiden av en vert etter den har krasjet pga. en ikke-permanent feil er μ_t^{-1}. Den forventede tiden det tar RM og Jgroup å lage et nytt replika på en arbeidende vert (inkludert tiden det eventuelt tar å synkronisere med det andre replikaet) er μ_n^{-1}. Vi har at $\mu_n \gg \mu_t \gg \mu_h$.

[4] I tilfelle uoverensstemmelse mellom den engelske og norske utgaven, er det den engelske som er gjeldende.

d) Bruk pålitelighetsblokkskjema for å finne den tilnærmede asymptotiske tilgjengeligheten til ressursallokeringstjenesten når systemet har det minimale antall vertsnoder ($n = 2$): A_2. Hvis tilleggsantakelser er nødvendige, gjør og skriv ned disse.

e) Finn den tilnærmede asymptotiske tilgjengeligheten til ressursallokeringstjenesten når systemet har et stort antall vertsnoder (n går mot uendelig): A_∞. (Hint, teknikken med pålitelighetsblokkskjema kan brukes.) Hvis tilleggsantakelser er nødvendige, gjør og skriv ned disse.

f) For å opprette nye replika etter en feil, trenger ARM å bli kjent med feilen. Beskriv to metoder som brukes i Jgroup/ARM-systemet for å detektere feil.

Modellen for tjenestetilgjengelighet utviklet i d) og e) er for unøyaktig for formålet, og en mer detaljert modell er nødvendig. For å holde denne modellen enkel, anta at $\lambda_t = 0$. Anta også at maksimalt en permanent feil kan avhjelpes av gangen. Studier av ARM feilhåndtering har vist at så lenge det er andre ikke-feilte replika i en gruppe, så kan et enkelt replika startes og synkroniseres i løpet av en negativt eksponentialfordelt tid med forventning μ_n^{-1} etter at et replika i gruppen feilet. Dersom alle, eller det siste, replikaet i gruppen feiler, så vil hele gruppen bli restartet i løpet av en negativt eksponentialfordelt tid med forventning μ_{nn}^{-1} etter at det siste replikaet feilte.

g) Angi to grunner til at pålitelighetsblokkskjema *ikke* kan brukes for analyse i dette tilfelle. Tegn et fullstendig tilstandsdiagram for systemet som leverer tjenesten, dvs. inkluder alle transisjoner, for tilfelle hvor $n = 3$. Kall en tilstand $[a, b]$ hvor a er antall arbeidende vertsnoder i systemet og b er antallet arbeidende RAS. (Hint: for å lette utviklingen og tolkningen av diagrammet, vær påpasselig med å gi det en struktur som avbilder de operasjonelle modiene og symmetriene i systemet.) Indiker hvilke tilstander som representerer en arbeidende og feilet tjeneste, og hva som er systemkonfigurasjonen i de ulike tilstandene.

I det følgende spørsmålet er vi interessert i funksjonssannsynligheten (reliability function) til ressursallokeringstjensten sett fra en klient. Anta at en ressurs er allokert til en klient for uavhengige identisk negativt eksponentialfordelte tider med forventning θ^{-1}. Dette innebærer at en klient fornyer sin ressursallokering ifølge en Poisson prosess med intensitet θ. En klient opplever/får en tjenestefeil når den, ved utløpet av sin allokeringstid, opplever at systemet er nede. Når den tjenesteleveransen vi betrakter starter, kan vi anta at systemet er i stasjonærtilstand. Tiden fra tjenesteleveransen starter til klienten opplever en feil kalles T_F. Funksjonssannsynligheten til systemet sett fra en klient $R_c(t) = \Pr(T_F > t)$ skal finnes.

h) Utvid og/eller modifiser tilstandsdiagrammet funnet i spørsmål g) så det kan brukes til å finne $R_c(t)$. (NB! pass på å få klart frem hvilken del av diagrammet som er en besvarelse av spørsmål g) og hvilke som tilhører dette spørsmålet.)[5]

[5]Dersom du ikke har besvart spørsmål g), tegn og benytt et generisk (vilkårlig) diagram med oppe- og nedetilstander og utvid dette.