Exam - Friday 11. may 2001

SIE 5025 Pålitelige systemer
Dependable systems

Solution to problems

Version 0.3; 7 June 2001; BEH

Problem 1

a) There are one requirement for the interval (un)availability and two requirements for the reliability[1], i.e:

Interval unavailability and unavailability:

$$1 - \bar{A}(0, 1\text{yr}) = \bar{U}(0, 1\text{yr}) = \frac{10}{365.25 \cdot 60 \cdot 24} = 1.90(10^{-5}) \tag{1.1}$$

Reliability function (Fuksjonssannsynlighet):

$$\begin{aligned} &R(1\text{hr}) \geq 1 - 10^{-5} \\ &R(7 \cdot 24\text{hr}) = R(168\text{hr}) \geq 1 - 10^{-3} \end{aligned} \tag{1.2}$$

b) When the failure process is an homogeneous Poisson process, we have a constant failure rate and intensity λ and independent failures, hence:

$$R(t_x) = e^{-\lambda t_x} \geq \text{Requirment}_x \tag{1.3}$$

which with the values of **(1.2)** yields

$$\begin{aligned} &\lambda_{1\text{hr}} \leq 1(10^{-5})\frac{1}{\text{hr}} \\ &\lambda_{1\text{week}} \leq 5.96(10^{-6})\frac{1}{\text{hr}} \end{aligned} \tag{1.4}$$

Hence the week requirement is the strictest.

[1] A definition of the attributes reliability and availability are of course welcome, but not required.

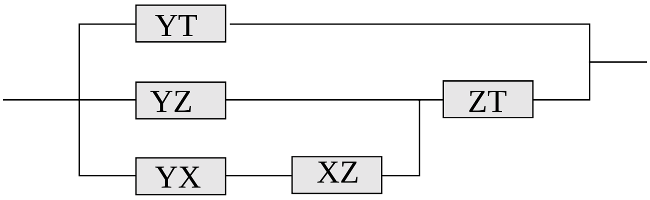
(The approximate approach $\lambda_{1\text{hr}}1\text{hr} \leq 10^{-5}$ and $\lambda_{1\text{week}}168\text{hr} \leq 10^{-3}$ are also acceptable since the valus are small in both cases. The approx. should be mentioned.)

From Korolyuks theorem $\text{MTBF} = 1/\lambda_{1\text{week}} \geq 167916\text{hr}$
(In the above calculation we does not include the down time portion of the MTBF, e.g. $\text{MTBF} = 1/\lambda_{1\text{week}} + \text{MDT}$, since it obviously does not have any numerical influence, i.e. both answers are considered correct.

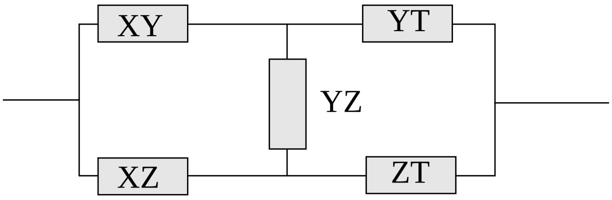
$$\frac{\text{MDT}}{\min(\text{MTBF})} \leq \bar{U}(0, 1\text{yr}) = \frac{10}{365.25 \cdot 60 \cdot 24} = 1.9010^{-5} \tag{1.5}$$

which yeilds $\text{MDT} \leq 3.19\text{hr}$.

c) Reliability block diagram, where each block represents a link.



BETWEEN USER Y AND SERVER T



BETWEEN USER X AND SERVER T

Between user Y and T we have a parallel series system. From the diagram, the availability between becomes directly from the diagram:

$$A_{YT} = 1 - (1 - A_l)(1 - A_{\text{Backup}})$$

where $A_{\text{Backup}} = A_l(1 - (1 - A_l)(1 - A_l A_l))$

which yields

$$A_{YT} = A_l(1 + A_l - 2A_l^3 + A_l^4).$$

Between user X and T we have a bridge system. This is solved by using the element YZ as a pivot element and condition on whether it is working or not. The two cases is then a series of two parallel links and a parallel of two links in series, i.e.

$$\begin{aligned} A_{XT} &= (1 - (1 - A_l)^2)^2 \cdot A_l \\ &+ (1 - (1 - A_l A_l)^2) \cdot (1 - A_l) \end{aligned} \tag{1.6}$$

which yields $A_{XT} = A_l^2(2 + 2A_l - 5A_l^2 + 2A_l^3)$.

d) To obtain the failure intensity, we first obtain the mean time between failures. Since all links are independent we may successively use the relations:

General

$$(1 - A) = \frac{\text{MDT}}{\text{MTBF}} \qquad \text{MUT} = A\text{MTBF} \tag{1.7}$$

Series of two elements:

$$A_s = A_1 A_2 \qquad \text{MUT}_s = 1/\left(\frac{1}{\text{MUT}_1} + \frac{1}{\text{MUT}_2}\right) \tag{1.8}$$

Parallel of two elements

$$(1 - A_p) = (1 - A_1)(1 - A_2) \qquad \text{MDT}_p = 1/\left(\frac{1}{\text{MDT}_1} + \frac{1}{\text{MDT}_2}\right) \tag{1.9}$$

For the system at hand, the intermediate results are shown in the table below.

Subnetwrk	Availability	MDT	MTBF
XT	A	m	$\frac{m}{1-A}$
YZ	A	m	$\frac{m}{1-A}$
(YX, XZ)	A^2	$\frac{(1+A)\,m}{2\,A}$	$\frac{m}{2\,A-2\,A^2}$
(YX, XZ)||YZ	$A + A^2 - A^3$	$\frac{(1+A)\,m}{1+3\,A}$	$\frac{m}{(-1+A)^2\,(1+3\,A)}$
((YX,XZ) || YZ), ZT	$A^2 + A^3 - A^4$	$\frac{(-1-A+A^3)\,m}{A\,(-2-3\,A+4\,A^2)}$	$\frac{m}{2\,A+A^2-7\,A^3+4\,A^4}$
(((YX, XZ)||YZ), ZT)||XT	$A\,(1 + A - 2\,A^3 + A^4)$	$\frac{(1+A-A^3)\,m}{1+3\,A+3\,A^2-5\,A^3}$	$-\frac{m}{(-1+A)^2\,(-1-3\,A-3\,A^2+5\,A^3)}$

(At the exam, it is <u>not</u> required that all intermediate and final result are computed. It is sufficient to show how they may be computed.)

The failure intensity seen from user Y is then

$$\lambda_{YT} = \frac{1}{\text{MTBF}_{YT}} \tag{1.10}$$

e) The unavailability of the network may be obtained by the equation

$$U = \sum_{\forall\phi_x}(1 - I(\phi_x))P(\phi_x) \tag{1.11}$$

where $I(\phi_x) = 1$ if the traffic can be carried in failure mode $\phi_x \in \Phi$, zero otherwise, and $P(\phi_x)$ is the probability of the mode. If we subdivide the failure modes into two disjoint sets, Φ_D and $\Phi_E = \Phi - \Phi_D$, we may obtain the lower and upper bound by taking the traffic carrying capability into account the modes in Φ_D, and make an optimistic $(I(\phi_x) = 1), \forall\phi_x \in \Phi_E$ and an pessimistic assumption $(I(\phi_x) = 0), \forall\phi_x \in \Phi_E$ for the traffic carrying capability in the remaining, i.e.

$$\begin{aligned}\sum_{\forall\phi_x \in \Phi_D}(1 - I(\phi_x))P(\phi_x) \le U \le \sum_{\forall\phi_x \in \Phi_D}(1 - I(\phi_x))P(\phi_x) + \sum_{\forall\phi_x \in \Phi_E}P(\phi_x) \\ = \sum_{\forall\phi_x \in \Phi_D}(1 - I(\phi_x))P(\phi_x) + \left(1 - \sum_{\forall\phi_x \in \Phi_D}P(\phi_x)\right)\end{aligned} \tag{1.12}$$

f) Makes a table of the routes in the failure modes in Φ_D

Tabell 1.1

F_mode	$\pi_{YT}(\ldots)$	$\pi_{XT}(\ldots)$
…	YT	XZT
XY	YT	XZT
XZ	YT	XYZT
YZ	YT	XZT
YT		XZT
ZT	YT	XZYT

When a route is found we have $I(\phi_x) = 1$ otherwise zero. The probabilities of the failure modes are:

$$\begin{aligned}&P(\ldots) = A_l^5 \\ &P(\beta) = A_l^4(1 - A_l), \beta = XY, XZ, YZ, YT, ZT\end{aligned} \tag{1.13}$$

Inserting into **(1.12)** it is obtained

$$\begin{aligned}A_l^4(1 - A_l) \le U_{YT} \le 1 - A_l^5 - 4A_l^4(1 - A_l) \\ 0 \le U_{XT} \le 1 - A_l^5 - 5A_l^4(1 - A_l)\end{aligned} \tag{1.14}$$

g) Rewrites the expression in **(1.14)** in terms of U_l where only the terms of the lowest order is taken into account, i.e. the most significant terms. Uses $\overline{U}_{\dots}$ and $\underline{U}_{\dots}$ to denote the upper and lower bounds respectively.

$$
\begin{aligned}
&\underline{U}_{YT} \ge A_l^4(1-A_l) \approx U_l \\
&\overline{U}_{YT} \le 1 - A_l^5 - 4A_l^4(1-A_l) \approx 1-(1-5U_l)-4(1-4U_l)U_l \approx U_l \\
&\underline{U}_{XT} \ge 0 \qquad (1.15)\\
&\overline{U}_{XT} \le 1 - A_l^5 - 5A_l^4(1-A_l) \approx 1-\left(1-5U_l+\binom{5}{2}U^2{}_l\right)-5(1-4U_l)U_l = 10U^2{}_l
\end{aligned}
$$

In the “connectivity case” the unavailability was in the order of U_l^2 for both connections. This indicates that an arbitrary single link failure may be tolerated. In the traffic constrained case, $U_{YT} \approx U_l$ and cannot tolerate all single link failures, while $0 \le U_{ZT} \le 10U^2{}_l$ indicates that (at least) an arbitrary single link failure may be tolerated.

h) Extends the **Tabell 1.1** of the routes in the failure modes in Φ_D with single ditch failure (in bold italic)

Tabell 1.2

F_mode	$\pi_{YT}(\dots)$	$\pi_{XT}(\dots)$
…	YT	XZT
XY	YT	XZT
XZ	YT	XYZT
YZ	YT	XZT
YT		XZT
ZT	YT	XZYT
XZ	YT	
YZ		XZT
ZT		

When a route is found we have $I(\phi_x) = 1$ otherwise zero. The probabilities of the failure modes becomes:

$$
\begin{aligned}
&(\dots) = A_l^5(1-U_d)^3 \\
&(\beta) = A_l^4(1-A_l)(1-U_d)^3,\ \beta = XY, XZ, YZ, YT, ZT \qquad (1.16)\\
&(\beta) = A_l^5U_d(1-U_d)^3,\ \beta = \boldsymbol{XZ, YZ, ZT}
\end{aligned}
$$

In the above equations we consider the failure associated link independent of the “state” of the ditch it resides in.

Inserting into **(1.12)** it is obtained

$$\begin{aligned}
&\underline{U}_{YT} \geq A_l^4(1-A_l)(1-U_d)^3 + 2A_l^5(1-U_d)^2U_d \\
&\overline{U}_{YT} \leq 1-(A_l^5 + 4A_l^4(1-A_l))(1-U_d)^3 - A_l^5(1-U_d)^2U_d \\
&\underline{U}_{XT} \geq 2A_l^5(1-U_d)^2U_d \\
&\overline{U}_{XT} \leq 1-(A_l^5 + 5A_l^4(1-A_l))(1-U_d)^3 - A_l^5(1-U_d)^2U_d
\end{aligned} \tag{1.17}$$

Problem 2

a) *Cut from jgroup manual:*

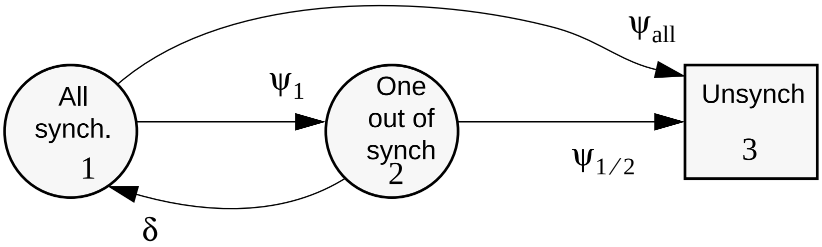
The object group paradigm has been proposed [7]. In this paradigm, functions of a distributed service are replicated among a collection of logically related server objects gathered together in an object group. A group constitutes a logical addressing facility: clients transparently interact with object groups by remotely invoking methods on them, as if they were single, non-replicated remote objects. A method invocation on a group results in the method executed by one or more of the servers forming the group, depending on the invocation semantics.

b) The basic requirements are:

All replicas must receive there messages in exactly the same sequence, i.e. the message passing must be according to atomic multicast
- total order,
- termination
- Atomicity (all correct receivers receives the same message or none.)

The computation within fault free) each replica must be deterministic, i.e. If non-faulty replicas process identical input message streams, the approach must guarantee that they produce identical output message streams. (This may be achieved with the state machine approach.)

c) Three states may be identified according to how many replicas that are synchronous.



Denote the probability of being in state i by $P_i(t)$ and $\underline{P}(t) = \{P_1(t), P_2(t), P_3(t)\}^T$. It is given that $\underline{P}(0) = \{1, 0, 0\}^T$. $\underline{P}(t)$ may be obtained by solving the following set of linear differential equations:

$$\frac{d}{dt}\underline{P}(t) = \Lambda \cdot \underline{P}(t) \text{ where } \Lambda = \begin{pmatrix} -\psi_1 - \psi_{all} & \delta & 0 \\ \psi_1 & -\delta - \psi_{1/2} & 0 \\ \psi_{all} & \psi_{1/2} & 0 \end{pmatrix} \tag{2.1}$$

The time until synchronization failure is equal to the time until state 3 is reached. Hence, $P_3(t)$ is the distribution function (PDF) of this time and the pdf becomes

$$f(t) = \frac{d}{dt}P_3(t). \tag{2.2}$$

d) Since ψ is much less than δ we may Taylor expand α around δ^2, i.e.

$$\begin{aligned} \alpha = \sqrt{\delta(\delta+4\psi)} &= \sqrt{\delta^2} + \frac{4\delta\psi}{2\sqrt{\delta^2}} - \frac{16(\delta\psi)^2}{8\delta^2\sqrt{\delta^2}} + o(4(\delta\psi)^2) \\ &\approx \delta + 2\psi - 2\frac{\psi^2}{\delta} \end{aligned} \tag{2.3}$$

Inserted into the expression for $f(t)$ and simplified this yields:

$$f(t) = \frac{\psi^2}{\delta + 2\psi - 2\frac{\psi^2}{\delta}}\left(e^{-\frac{\psi^2}{\delta}\cdot t} - e^{-\delta + 2\psi - \frac{\psi^2}{\delta}\cdot t}\right) \tag{2.4}$$

The pdf has two time constants reflecting the time constants in the system. $\left(\delta + 2\psi - \frac{\psi^2}{\delta}\right)^{-1}$ is very much shorter than $\left(\frac{\psi^2}{\delta}\right)^{-1}$ an will have negligible influence on the pdf. It represents the "transient information" that the system is initiated in state 1. The time constant $\left(\frac{\psi^2}{\delta}\right)^{-1}$ governs the overall behaviour.

Hence, we may use the approximation $e^{-\delta + 2\psi - \frac{\psi^2}{\delta}\cdot t} \approx 0$. We also see that $\delta + 2\psi - 2\frac{\psi^2}{\delta} \approx \delta$. As a result we have the approximate pdf

$$f(t) = \frac{\psi^2}{\delta}e^{-\frac{\psi^2}{\delta}\cdot t} \tag{2.5}$$

It is seen that the above is the pdf of a negative exponential distribution with expectation δ / ψ^2. Hence, the time until synchronization failure is inverse proportional with the expected synchronization time δ^{-1} and proportional with the square of the expected time between out-of-order arrival of messages ψ^{-2}.

e) The time is found straight forwardly from the pdf in the problem formulation or an approximation from **(2.5)**.

$$\mathrm{MTFF}_{\mathrm{order}} = \int_0^{\infty} (t \cdot f(t) dt) \approx \delta / \psi^2 \tag{2.6}$$

If $\psi_{\mathrm{all}} \neq 0$ the $\mathrm{MTFF}_{\mathrm{order}}$ will decrease since we have another “source” of order failures - corresponding to a direct path in the state diagram. From the diagram it is seen that we will have more order failures due to all replicas receiving messages out of order when $\psi_{\mathrm{all}} > \psi^2 / \delta$, since state 1-3 will more often lead to failure than the path(s) (1-2)*-3. * indicates that the transition may be iterated.