CHALMERS

Fault-tolerant Computer Systems

Exercises

JOHAN KARLSSON

Department of Computer Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY
Göteborg, Sweden, 2011

Contents

Problems

1. Basic relations in probability theory

1.1 Derive an expression for the failure rate function $h(t)$ in terms of the frequency function $f(t)$ and the reliability $R(t)$. Use this expression to calculate $h(t)$ for an exponentially distributed variable. The probability density function for the exponential distribution is $f(t) = \lambda e^{-\lambda t}$.

1.2 Derive a formula that expresses the reliability $R(t)$ in terms of the (instantaneous) failure rate function $h(t)$.

1.3 Derive a formula that expresses the expected lifetime of a component $E[X]$ in terms of the reliability $R(t)$ of the component.

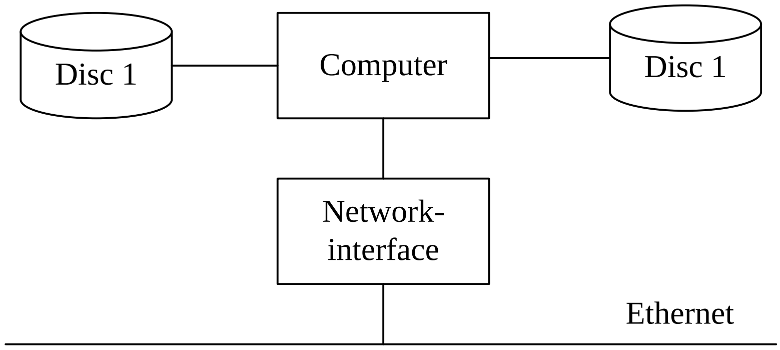
1.4 Derive an expression for the expectation value for the lifetime of a parallel system. Assume that the system consists of n identical components, whose lifetimes are exponentially distributed with the failure rate $\tilde{\lambda}$

2. M-of-N System

2.1 Derive expressions for the reliability and the MTTF for a TMR system consisting of three identical modules whose lifetimes are exponentially distributed with the failure rate λ.

2.2 Derive expressions for the reliability and the MTTF for a hot stand-by system consisting of two identical modules whose lifetimes are exponentially distributed with the failure rate λ.

2.3 A file server in a local area network uses mirrored discs, as shown in the figure below. This means that each file is stored on two separate disks, which allows the system to remain operational even if one disk fails.



a) Draw a reliability block diagram for the file server. The Ethernet cable is not a part of the server.

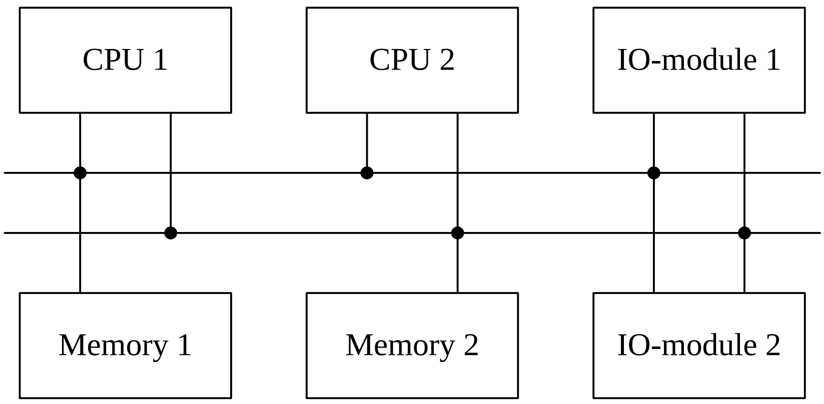
b) Draw a fault tree for the file server.

c) Calculate the reliability after one year of service. Assume that the components of the file server have exponentially distributed life times with the following failure rates:

$$\lambda_{comp} = 10^{-5} \text{ f/h}, \lambda_{disc} = 10^{-4} \text{ f/h}, \lambda_{interface} = 10^{-5} \text{ f/h}$$

d) Calculate the MTTF for the file server.

2.4 A fault tolerant computer system is illustrated in the figure below:



a) Draw circles around the error containment regions.

b) Draw a reliability block diagram for the system. Do not forget to include the buses.

c) Draw a fault tree for the system.

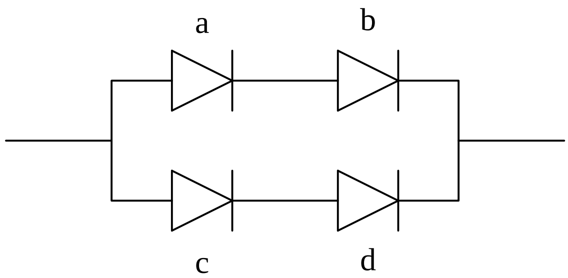
d) Calculate the reliability of the system after one year of service. Assume that the modules in the system operates in active redundancy and have exponentially distributed lifetimes with the following failure rates:

$$\lambda_{cpu} = 10^{-6} \text{ f/h}, \lambda_{memory} = 5 \cdot 10^{-6} \text{ f/h}$$
$$\lambda_{io} = 5 \cdot 10^{-7} \text{ f/h}, \lambda_{bus} = 10^{-7} \text{ f/h}$$

2.5 In the figure below a diode circuit is depicted. Such a circuit upholds the diode function even if one, or in some cases several of the diodes fails. Assume that:

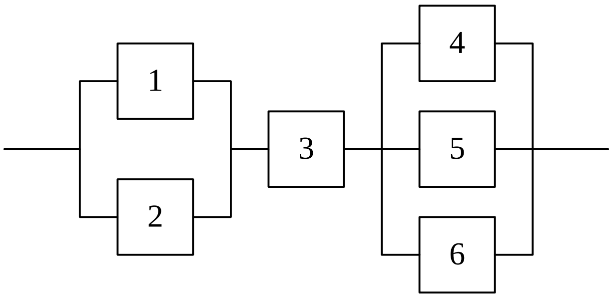
e) that failure mode of the diodes is an open circuit, and

f) the failure mode of the diodes is a short circuit.



For each case, draw the reliability block diagram and give an expression the reliability of the circuit. Let $R_d(t)$ denote the reliability for one diode.

2.6 A computer system has a reliability block diagram as below. Derive an expression for the reliability of the system $R_{sys}(t)$! Assume that the reliability of component *k* is $R(t)$.



2.7 A fault-tolerant computer system consists of four identical computers. The system is a hot stand-by system. The system delivers service as long as two computers are operating correctly. The system is shut down when only one correctly working computer remains.

a) Calculate the reliability of the system after one year of service if the lifetime of one computer is exponentially distributed with a failure rate of 10^{-6} f/h.

b) Calculate the MTTF for the system.

3. Markov modelling

If nothing else is specified, the lifetimes of components and modules are exponentially distributed.

Reliability modeling

3.1 Derive expressions for the reliability and the MTTF (Mean Time To Failure) for a TMR/Simplex system consisting of three identical modules whose lifetimes are exponentially distributed with the failure rate λ. (A TMR/Simplex system works as follows: When a module fails, the failing module and one of the non-faulty modules are taken off-line. Since the system cannot tolerate more than one failure, taking one of the working modules off-line will actually increase the reliability as the total failure rate of the system decreases.)

3.2 A computer system consists of three identical modules. At system start-up, two modules are active while one module is acting as a cold stand-by spare. The failure rate is λ for an active module and μ for a cold (inactive) module. At least two modules must be operational for the whole system to work. Derive an expression for the reliability of the system. Assume that the coverage is ideal (i.e., 100%).

3.3 Derive an expression for the reliability of a TMR system. The failure rate of a module is λ and the probability for the first failure to cause a system crash is 1 - c. Derive also an expression for the MTTF of the system.

3.4 A parallel redundant system consists of two modules M_1 and M_2 which have failure rates λ_1 andλ_2, respectively. If M_1 fails, there is a certain risk that M_2 also fails. The probability for this is 1 - c. Derive an expression for the reliability of the system.

3.5 Derive an expression for the reliability of a cold stand-by system with one spare module. Assume that the coverage is c. Derive also an expression for the MTTF of the system. The failure rate of the active module is λ, while the failure rate of cold module is assumed to be zero.

3.6 Derive expressions for the reliability and MTTF of a cold stand-by system with one active module and one spare module. The failure rate of the active module λ and the dormancy factor is k.

Safety modelling

3.7 Derive an expression for the safety of a TMR system which is shut down after the first module failure. Assume that the shut-down time for the system is exponentially distributed with the expected value $1/\mu = 1$ hour. Also assume that the modules in the TMR system have a failure rate of $\lambda = 10^{-5}$ f/h. Calculate the safety of the system.

3.8 Derive an expression for the safety of a TMR system which is shut down after the second module failure. Assume that the shut-down is successful with a probability c. Also, assume that the modules in the system have a failure rate of λ. Calculate the steady-state safety.

3.9 Derive an expression for the safety of a hot-standby system which is shut down after the first module failure. Assume that the shut-down time is exponentially distributed with the expected value $1/\mu$ 30 minutes. The fa ilure rate of the modules is $\lambda = 10^{-7}$ f/h.

3.10 Consider a hot stand-by system that from system start has one active and two spare modules. The system is shut down when one module remains operational. Assume that the shut-down time is exponentially distributed with the expected value $1/\mu$. A catastrophic failure occurs if the last remaining module fails before the shut-down is completed. The fault coverage is c ($c < 1$) for an active module and ideal for a spare module. The occurrence of a non-covered fault in the active module leads to a catastrophic failure.

Draw a state diagram for a Markov model of the system and derive an expression for the steady-state safety of the system. Hint: the steady-state safety can be directly derived from the transition intensities in the Markov model.

Availability modelling

3.11 Derive an expression of the steady-state availability of a TMR system where failed modules are repaired. Assume that the time to repair a module is exponentially distributed with an expectation value of $1/\mu$. Assume also that the modules in the system have a failure rate of λ. Only one module at a time can be repaired.

3.12 Derive an expression of the steady-state availability for a cold stand-by system with one primary module and one spare. Assume that the coverage is c. If the system crashes, it is restarted immediately when one module has been repaired. Assume that the time to repair a module is exponentially distributed with an expectation value of $1/\mu$. Also, assume that the modules in the system have a failure rate of λ. Only one module at a time can be repaired. The failure rate of the cold spare can be neglected. If the system fails due to insufficient coverage, both active modules are considered faulty.

3.13 Derive an expression for the steady-state availability of a cold stand-by system consisting of one primary module and to stand-by modules. The lifetime of a module is assumed to be exponentially distributed with a failure rate of λ. Assume that the coverage is 100% and that the failure rate of the spares is zero. The time to repair a module is exponentially distributed with a repair rate of μ. Assume that only one repair-person is available.

4. Generalized Stochastic Petri Nets

4.1 A system uses three identical modules in a TMR configuration. Each of the modules has a lifetime that is exponentially distributed with a failure rate λ.

Define a GSPN model suitable for calculating the reliability of the system.

Define a GSPN model of the system for calculating the availability. Failed modules are repaired with a rate of μ and one model at a time can be repaired.

4.2 *Variant of Problem 2.7.*
A fault-tolerant computer system consists of four identical computers. The system is a hot stand-by system. The system delivers service as long as two computers are operating correctly. The system is shut down when only one correctly working computer remains. Define a GSPN model of the system.

4.3 *Variant of Problem 4.9.*
A fault tolerant computer system is built from two subsystems, one subsystem consists of three processor modules and the other subsystem consists of two I/O modules. One processor module and one I/O module must be working in order for the system to deliver its service. The two subsystems are connected by a number of buses providing full-connectivity between all modules. Both subsystems use cold stand-by spares. The failure rate is λ_p for an active processor and λ_{io} for an active I/O-module. All modules are assumed to obey the exponential failure law. The failure rate for buses and cold stand-by spares are assumed to be negligible and the coverage is assumed to be ideal. Define a GSPN model of the system.

4.4 Define a GSPN model of a hot standby system that consists of two identical components. The lifetime of the components is exponentially distributed with λ and failed modules are repaired one at a time with the rate μ. The coverage for reconfigurations is c. For non-covered failures, the system repair time is assumed to be exponentially distributed with the rate ρ.

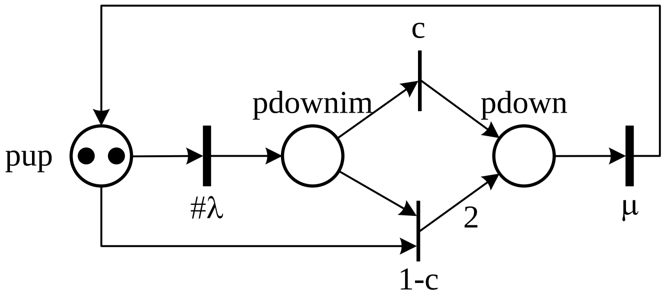
4.5 A fault-tolerant computer system from start consists of N_A active modules and N_S spare modules. The failure rate for an active module is λ and the failure rate of the spare modules is negligible. The coverage for all reconfigurations is assumed to be ideal. Define a GSPN model of the system.

4.6 A system consists from start of two active modules and two cold standby modules. The failure rate of an active module is λ and the dormancy factor is k. Failed modules are repaired one at a time with a rate of μ. The coverage for all reconfigurations is assumed to be ideal. Define a GSPN model of the system.

4.7 The figure below shows a GSPN model of a duplex system with non-perfect coverage.

a) Derive the extended reachability graph of the GSPN model.

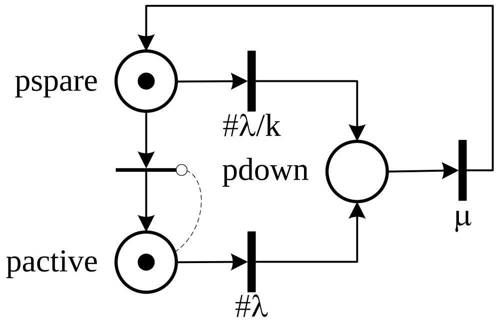
b) Derive the reachability graph of the GSPN model.



4.8 The figure below shows a GSPN model of a cold standby system with a dormancy factor k, a "hot" failure rate λ and a repair rate μ.

a) Derive the extended reachability graph of the GSPN model.

b) Derive the reachability graph of the GSPN model.



5. System modelling - Exam Problems

5.1 A fault tolerant computer system consists of four identical computers. The system uses hot stand-by sparing. One computer is the primary computer that interacts with the users. The others are spare units. The spares are updated in parallel with the primary computer, and are thus prepared to take over immediately if the primary fails. The system delivers the expected service as long as at least two computers are operational, and is shut down when one working computer remains. The fault coverage for the system is assumed to be 100%.

a) Determine the reliability of the system assuming that the life time of each computer exponentially distributed with a failure rate $\lambda$of 10^{-6} failures per hour.

b) The system is repaired only after a system failure. It is not restarted until all faulty computers have been repaired. The average down-time in such a case, is 2 days. Determine the steady-state availability.

c) In some applications a system shut-down is necessary before all of the redundant computers have failed. What is such a shutdown called?

5.2 A fault tolerant computer system consists of four identical computers. From system start, one is the primary computer, one is a hot stand-by spare, and the other two are cold stand-by spares. The cold stand-by spares are powered up one after the other as the active computers fail, acting first as the hot stand-by spare and then as the primary computer. The system is shut-down when only one computer remains operational.

a) Derive an expression for the system reliability assuming that the life time of one computer is exponentially distributed with a failure rate λ when it operates either as the hot stand-by spare or the primary computer. The failure rate for a cold stand-by spare is assumed to be negligible, i.e., zero. The coverage for the system is assumed to be 100%.

b) The repair of a failed computer is started immediately after the failure occurs. The repair time for one computer is assumed to be exponentially distributed. Only one repair-person is available. Derive an expression for the steady-state availability assuming that the repair rate is μ.

5.3 A fault-tolerant computer system consists of two active modules and two cold standby spare modules. The spares can replace any of the active modules in case any of them fails. A working system requires at least two fault-free modules. The probability for correct activation of a spare in case of failure of an active module is c. If the activation fails it is assumed that the system crashes immediately. The life times of the active modules are exponentially distributed with a failure rate λ. The failure rates of the cold stand-by spares can be neglected.

a) Draw a Markov model state-diagram of the system.

b) Calculate the system reliability after one year of operation. Assume that the failure rate $\lambda = 10^{-5}$ failures per hour and that the fault coverage $c = 0.99$.

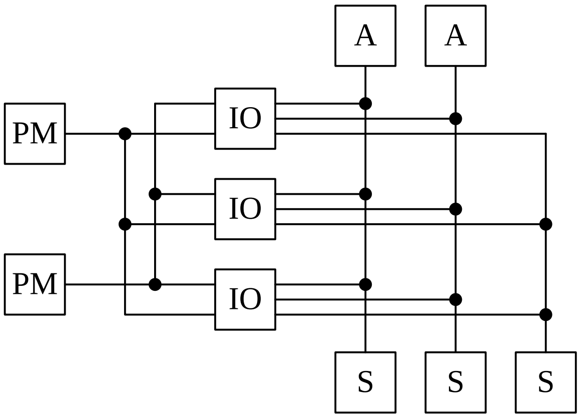
c) Assume that a safe shutdown is initiated when two working modules remain. The shut-down time for the system is exponentially distributed with an average shut-down time of 2 hours. An unsafe shutdown occurs immediately if any of the two modules fails during the shut-down time. Calculate the steady-state safety of the system. Hint: the steady-state safety can be derived directly from the transition rates in the Markov model.

5.4 Derive the steady-state availability for a system consisting of two active modules and one cold stand-by spare. For the system to work, at least two modules must be working. The life time as well as the repair time for each module is exponentially distributed with a failure rate $\lambda$and repair rate μ. The dormancy factor for the spares is *k*. The repair of an active module starts immediately after it has failed. Only one repair-person is available so the modules can only be repaired one at a time. A failure in the spare modules will not be detected until the system tries to activate the spare after a failure of one of the active modules. The coverage for the reconfiguration is assumed to be 100%. Disregard failures that may occur after the system is down.

5.5 Derive an expression for the system reliability and calculate the MTTF for a 3 of 5 system. The modules obey the exponential failure law and the failure rate is λ. The coverage for all reconfigurations is assumed to be ideal (c=1).

5.6 Derive an expression for the steady-state availability of a system that from start consists of two active modules and one cold stand-by spare. The system is operational as long as at least one module works. The modules obey the exponential failure law with a failure rate of λ. Assume a dormancy factor *k* for the cold stand-by spare and that only one module can be repaired at a time. Assume that the repair time is exponentially distributed with a repair rate of μ. The coverage for all reconfigurations are assumed to be ideal (c=1).

5.7 Conduct a reliability analysis of the following fault tolerant computer system for the control of an unmanned aeroplane. The dynamics of the aeroplane are controlled by a program executed on two processor modules. The processors are configured as hot stand-by system according to the figure below. The system controls the actuators of the control surfaces according to commands from control centre on ground and by reading sensor values such as velocity, altitude, etc. Sensors and actuators are connected to three serial buses. These buses are connected to the processors via three I/O modules. The processor modules are connected to the I/O modules via one parallel bus each. For the system to be operational at least one module of each kind must be working. The life times of all modules are exponentially distributed. Ideal coverage for all reconfigurations is assumed. The failure rates of the serial and parallel buses can be neglected.



Module	Reliability	Failure rate
PM (processor + memory)	$R_{pm}(t)$	λ_{pm}
IO (I/O-Modules)	$R_{io}(t)$	λ_{io}
A (Actuator modules)	$R_a(t)$	λ_a
S (sensor modules)	$R_s(t)$	λ_s

a) Divide the system into error containment regions. Motivate your answer.

b) Draw a reliability block diagram for the computer system and derive the system reliability R_{sys} from that.

c) Draw a state diagram for a Markov model of the subsystem that consists of the serial buses, the sensors and the actuators.

5.8 Consider a TMR-system with a cold stand-by spare. The system works as a standard TMR-system with the exception that the spare replaces the active module that first fails. The life times of all modules are exponentially distributed. The active modules have a failure rate λ. The dormancy factor for the cold stand-by spare is k. The coverage for all reconfigurations is c.

a) Assume that a safe shutdown is made when only one module remains operational. The time for the safe shutdown can be neglected, i.e., the safe shutdown can be considered instantaneous. A catastrophic failure occurs if a reconfiguration fails due to a non-covered fault in an active module. An activation of the cold stand-by module always results in a catastrophic failure, if that module has failed before it is activated. Disregard repairs.

   Draw a state diagram for a Markov model of the system and derive an expression for the steady-state safety of the system. Hint: the steady-state safety can be derived directly from the transition intensities in the Markov model.

b) Assume that repairs are possible. Disregard the possibility of catastrophic failures, and assume that the coverage is perfect. Derive an expression for the steady-state availability of the system. Only one module at a time can be repaired. The repair time is assumed to be exponentially distributed with an expected time to repair of $1/\rho$.

5.9 A fault tolerant computer system is built from two subsystems, one subsystem consists of three processor modules and the other subsystem consist of two I/O modules. One processor module and one I/O module must be working in order for the system to deliver its service. The two subsystems are connected by a number of buses providing full-connectivity between all modules. Both subsystems use cold stand-by spares. The failure rate is λ_p for an active processor and λ_{io} for an active I/O-module. All modules are assumed to obey the exponential failure law. The failure rate for buses and cold stand-by spares are assumed to be negligible and the coverage is assumed to be ideal. Derive an expression for the system reliability.

5.10 Derive an expression for the steady-state availability of a system consisting of two modules operating in active redundancy. The modules are assumed to be fail-silent and should under normal circumstances produce identical results. If a fail-silent violation occurs, which implies that the modules produces non-identical results, then the system is immediately shut-down by an external unit. The life time of both modules is exponentially distributed with the failure rate λ. The assumption coverage for the fail-silent property is c. The repair time for each of the modules is exponentially distributed with a repair rate μ. If the system crashes due to a fail-silent violation, then the system repair time can be approximated as being exponentially distributed with a repair rate ρ. Only one repair-person is available.

Answers and Solutions

1. Basic relations in probability theory

1.1

$$h(t) = \frac{f(t)}{R(t)}$$
$$\exp(\lambda) \Rightarrow h(t) = \frac{\lambda e^{-\lambda t}}{e^{-\lambda t}} = \lambda$$

1.2

$$R(t) = e^{-\int_0^t h(x)dx}$$

1.3

$$E[X] = \int_0^\infty R(t)dt$$
$$\exp(\lambda) \Rightarrow E[X] = 1/\lambda$$

1.4

$$E[X] = \int_0^\infty \{1 - \left(1 - e^{-\lambda t}\right)^n\} dt = \frac{1}{\lambda}\sum_{i=1}^n \frac{1}{i}$$

2. M-of-N Systems

2.1

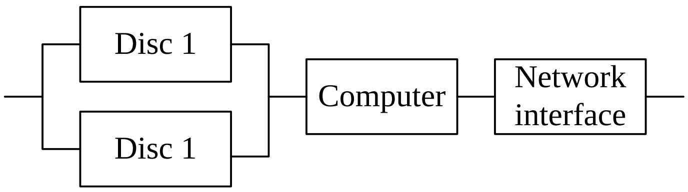
$$(t) = 3e^{-2\lambda t} - 2e^{-3\lambda t}$$
$$MTTF = \frac{5}{6} \cdot \frac{1}{\lambda}$$

2.2

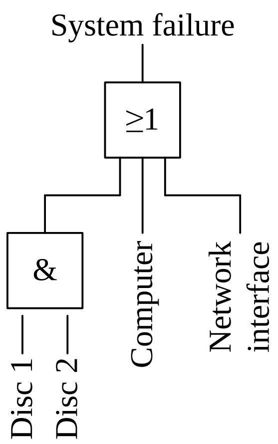
$$R(t) = 2e^{-\lambda t} - e^{-2\lambda t}$$
$$MTTF = \frac{3}{2} \cdot \frac{1}{\lambda}$$

2.3

a)



b)



c)

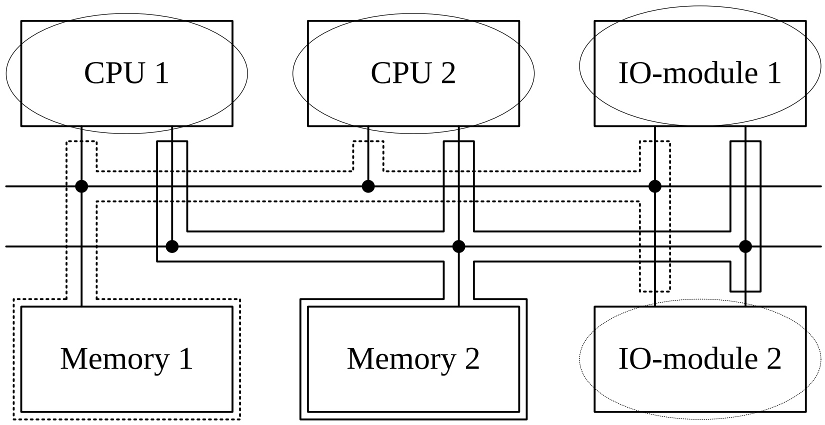
$$R_{sys} = R_{disks} \cdot R_{comp} \cdot R_{net}$$
$$R_{disks} = 1 - (1 - R_{disk1}) \cdot (1 - R_{disk2}) = 1 - (1 - R_d)^2$$
$$= 2R_{disk} - R_{disk}^2$$
$$R_{sys} = (2R_{disk} - R_{disk}^2) \cdot R_{comp} \cdot R_{net}$$
$$= \left(2e^{-\lambda_{disk} \cdot t} - e^{-2\lambda_{disk} \cdot t}\right) \cdot e^{-(\lambda_{comp} + \lambda_{interface}) \cdot t}$$
$$= 2e^{-(\lambda_{disk} + \lambda_{comp} + \lambda_{interface}) \cdot t} - e^{-(2\lambda_{disk} + \lambda_{comp} + \lambda_{interface}) \cdot t}$$
$$R_{sys}(t = 1 \text{ year} = 8760\ h) = 0{,}533$$

d)

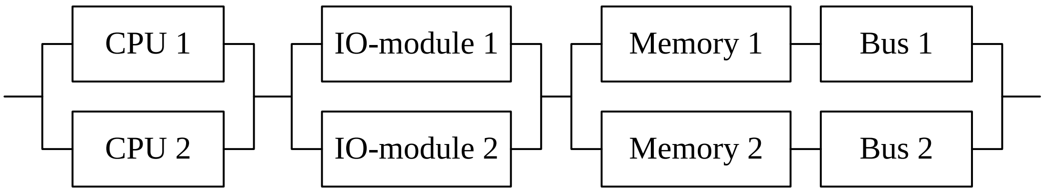
$$
\begin{aligned}
MTTF &= \int_0^\infty R_{sys}(t)dt = \int_0^\infty \left(2e^{-\lambda_{disk}\cdot t} - e^{-2\lambda_{disk}\cdot t}\right)\cdot e^{-(\lambda_{comp}+\lambda_{interface})\cdot t}\,dt \\
&= \int_0^\infty e^{-(\lambda_{disk}+\lambda_{comp}+\lambda_{interface})\cdot t}dt - \int_0^\infty e^{-(\lambda_{disk}+\lambda_{comp}+\lambda_{interface})\cdot t}dt \\
&= \frac{2}{(\lambda_{\mathrm{disk}}+\lambda_{\mathrm{comp}}+\lambda_{\mathrm{interface}})} - \frac{1}{(2\lambda_{\mathrm{disk}}+\lambda_{\mathrm{comp}}+\lambda_{\mathrm{interface}})} \\
&= \frac{2}{(10^{-4}+10^{-5}+10^{-5})} - \frac{1}{(2\cdot 10^{-4}+10^{-5}+10^{-5})} \\
&= 1{,}21\cdot 10^{-4}\mathrm{h} \approx 1{,}4 \text{ years}
\end{aligned}
$$

2.4

a)

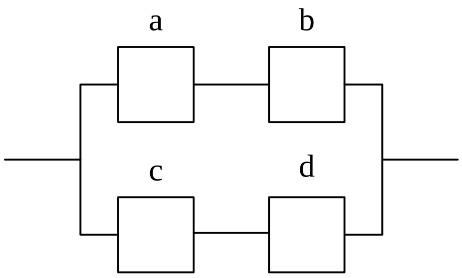


b)



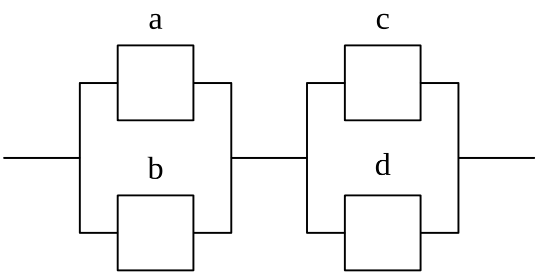
2.5

a)



$$R(t) = 2R_d^2(t) - R_d^4(t)$$

b)



$$R(t) = 4R_d^2(t) - 4R_d^3(t) + R_d^4(t)$$

2.6

$$R_{sys}(t) = \Big(1 - \big(1 - R_1(t)\big) \cdot \big(1 - R_2(t)\big)\Big) \cdot R_3(t) \cdot \Big(1 - \big(1 - R_4(t)\big) \cdot \big(1 - R_5(t)\big) \cdot \big(1 - R_6(t)\big)\Big)$$

2.7

The system is a 2-of-4 system.

a)

$$\begin{aligned} R_{sys}(t) &= \textstyle\sum_{i=2}^{4} \binom{4}{i} \cdot R^i \cdot (1-R)^{4-i} \\ &= 3R^4 - 8R^3 - 6R^2 \\ R_{sys}(t) &= 3e^{-4\lambda t} - 8e^{-3\lambda t} + 6e^{-2\lambda t} \\ \lambda\ &= 10^{-6}\mathrm{f/h}, t = 8760h \\ R_{sys}(t) &= 0{,}999997 \end{aligned}$$

b)

$$\begin{aligned} MTTF\ &= \int_0^{\infty} \left(3e^{-4\lambda t} - 8e^{-3\lambda t} + 6e^{-2\lambda t}\right) dt \\ &= \frac{13}{12} \cdot \frac{1}{\lambda} = 1{,}08 \cdot 10^6 h \end{aligned}$$

3. Markov modelling

3.1

$$R(t) = \frac{3}{2} \cdot e^{-\lambda t} - \frac{1}{2} \cdot e^{-3\lambda t}$$
$$\mathrm{MTTF} = \frac{4}{3} \cdot \frac{1}{\lambda}$$

3.2

$$R(t) = \left(1 - \frac{2\lambda + \mu}{\mu}\right) \cdot e^{-(2\lambda+\mu)t} + \left(\frac{2\lambda + \mu}{\mu}\right) \cdot e^{-2\lambda t}$$

3.3

$$R(t) = (1 - 3c) \cdot e^{-3\lambda t} + 3c \cdot e^{-2\lambda t}$$
$$MTTF = \frac{1 - 3c}{3\lambda} + \frac{3c}{2\lambda}$$

3.4

$$R(t) = e^{-\lambda_1 t} + c\left(e^{-\lambda_2 t} - e^{-(\lambda_1+\lambda_2)t}\right)$$

3.5

$$R(t) = (1 + c\lambda t) \cdot e^{-\lambda t}$$

$$MTTF = \frac{1 + c}{\lambda}$$

3.6

$$R(t) = \frac{\lambda + \mu}{\mu} \cdot e(-\lambda t) - \frac{\lambda}{\mu} \cdot e^{-(\lambda+\mu)}$$

3.7

$$S(t) = \frac{\mu}{2\lambda + \mu} - \frac{6 \cdot \lambda^2}{(2\lambda + \mu) \cdot (\mu - \lambda)} \cdot e^{-(2\lambda+\mu)t} + \frac{2\lambda}{(\mu - \lambda)} \cdot e^{-3\lambda t}$$

3.8

$$S(t) = c + 3 \cdot (1 - c) \cdot e^{-2\lambda t} + 2(c - 1) \cdot e^{-3\lambda t}$$
$$S(\infty) = c$$

3.9

$$S(t) = \frac{\mu}{\lambda + \mu} - \frac{\lambda}{\lambda - \mu} \cdot e^{-2\lambda t} + \frac{2 \cdot \lambda^2}{(\lambda + \mu) \cdot (\lambda - \mu)} \cdot e^{-(\lambda+\mu)t}$$

3.10

$$S(\infty) = \frac{\lambda(2 + c)}{3\lambda} \cdot \frac{\lambda(1 + c)}{2\lambda} \cdot \frac{\mu}{\lambda + \mu}$$

3.11

$$A(\infty) = \frac{3\lambda\mu^2 + \mu^3}{3\lambda\mu \cdot (2\lambda + \mu) + \mu^3 + 6\lambda^3}$$

3.12

$$A(\infty) = \frac{\mu^2 + \lambda\mu}{\lambda^2 + (2 - c)\lambda\mu + \mu^2}$$

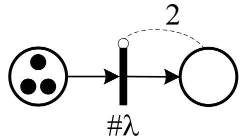
3.13

$$A(\infty) = \frac{\mu^3 + \lambda\mu^2 + \lambda^2\mu}{\mu^3 + \lambda\mu^2 + \lambda^2\mu + \lambda^3}$$

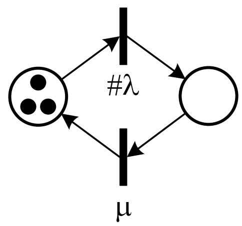
Answers and Solutions

4.1

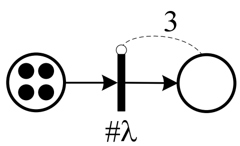
a)



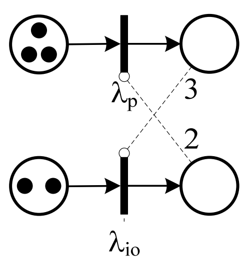
b)



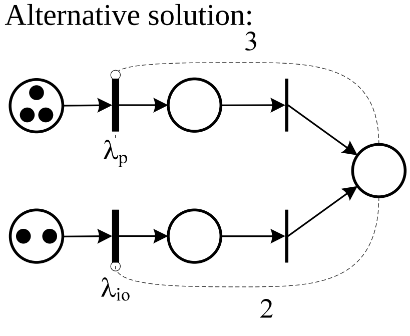
4.2



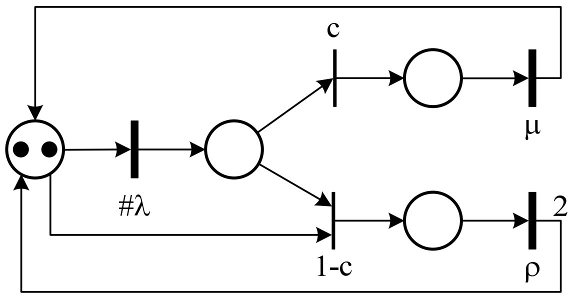
4.3



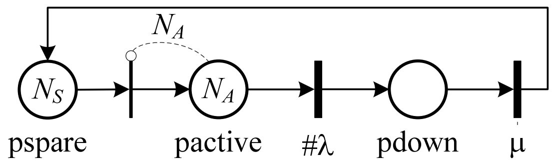
Alternative solution:



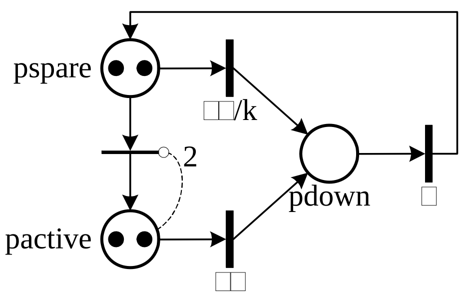
4.4



4.5

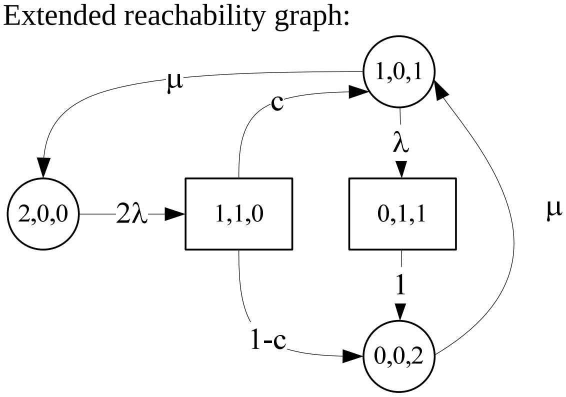


4.6

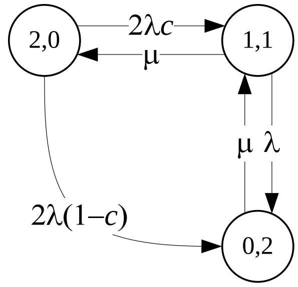


4.7

17 Extended reachability graph:

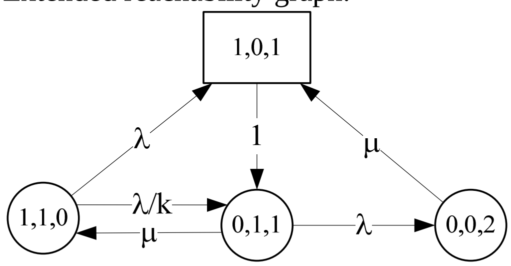


b) Reachability graph:

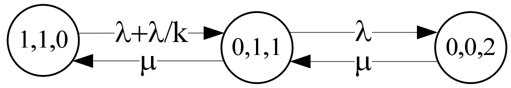


4.8

a) Extended reachability graph:



b) Reachability graph:



5. System modelling - Exam Problems

5.1

a)

$$R(t) = 3 \cdot e^{-4\lambda t} - 8 \cdot e^{-3\lambda t} + 6 \cdot e^{-2\lambda t}$$

b)

$$MTTF = \int_0^\infty (3 \cdot e^{-4\lambda t} - 8 \cdot e^{-3\lambda t} + 6 \cdot e^{-2\lambda t})dt = \frac{13}{12} \cdot \frac{1}{\lambda}$$

$$MTTR = 48h, MTTF = \frac{13}{12} \cdot 10^6$$

$$\lim_{t \to \infty} A(t) = \frac{MTTF}{MTTF + MTTR} = \frac{\frac{13}{2} \cdot 10^{-6}}{48 + \frac{13}{12} \cdot 10^{-6}} = 0{,}999956$$

c) Safe shutdown

5.2

a)

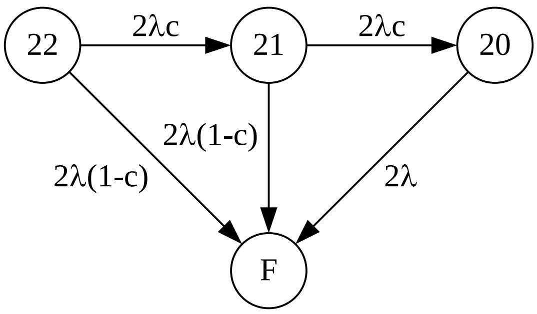
$$R(t) = (1 + 2\lambda t + 2\lambda^2 t^2)e^{-2\lambda t}$$

b)

$$\lim_{t \to \infty} A(t) = \frac{\mu^3 + 2\lambda\mu^2 + 4\lambda^2\mu}{\mu^3 + 2\lambda\mu^2 + 4\lambda^2\mu + 8\lambda^3}$$

5.3

a)



State Labelling

XY:

X= # of working active modules

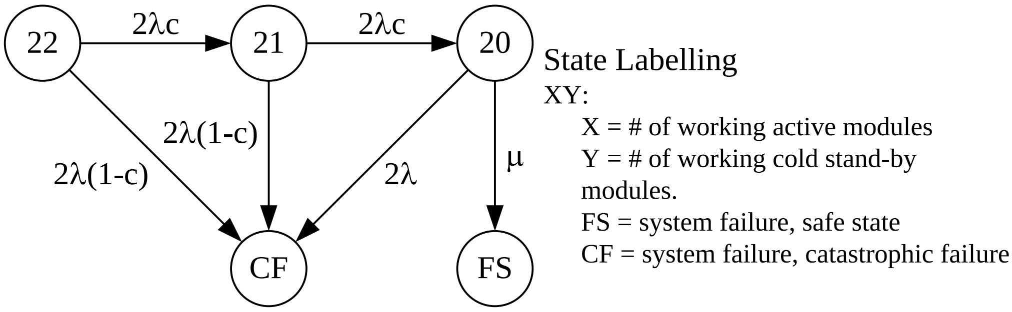
Y= # of working cold stand-by modules.

F = system failure

b)

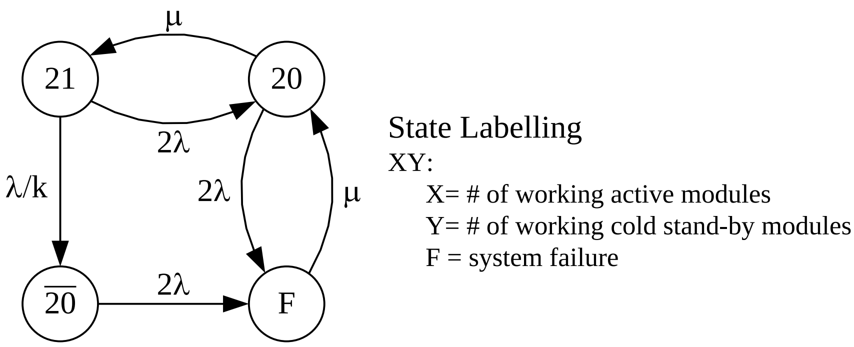
$$R(t) = P_{22}(t) + P_{21}(t) + P_{20}(t)$$
$$= (1 + 2\lambda ct + 2(\lambda ct)^2) \cdot e^{-2\lambda t}$$
$$\lambda = 10^{-5}, c = 0{,}99 \text{ gives}$$
$$R(t) = 0{,}9973$$

c)



$$\lim_{t\to\infty} P_{FS}(t) = \frac{\mu \cdot c^2}{2\lambda + \mu} \approx 0{,}98$$

5.4

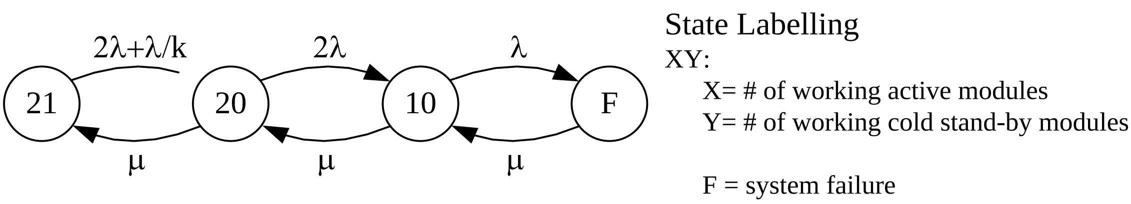


$$\lim_{t\to\infty} A(t) = \frac{\mu^2\left(1+\frac{1}{2k}\right)+\mu\left(2\lambda+\frac{\lambda}{k}\right)}{\mu^2\left(1+\frac{1}{2k}\right)+\mu\left(2\lambda+\frac{\lambda}{k}\right)+2\lambda\left(2\lambda+\frac{\lambda}{k}\right)+\frac{\lambda\mu}{k}}$$

5.5 R denotes the reliability of the system, and R_m denotes the reliability of a module.

$$R = 10R_m^3 - 15R_m^4 + 6R_m^5, R(t) = e^{-\lambda t}$$
$$R = 10e^{-3\lambda t} - 15e^{-4\lambda t} + 6e^{-5\lambda t}$$
$$MTTF = \int_0^\infty R(t)dt = \frac{10}{3\lambda} - \frac{15}{4\lambda} + \frac{6}{5\lambda} = \frac{47}{60} \cdot 1/\lambda$$

5.6

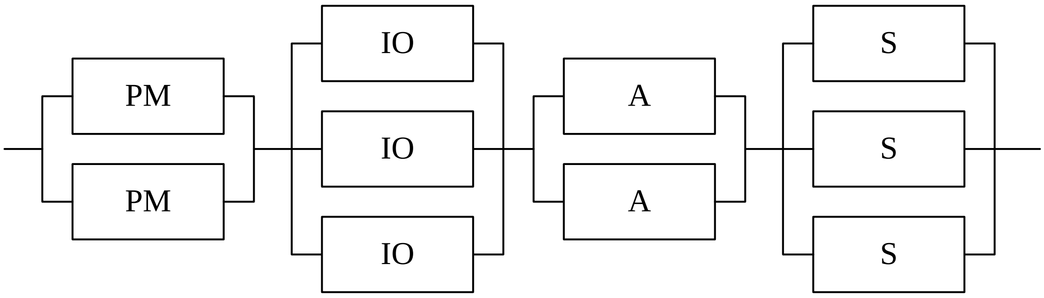


$$\lim_{t\to\infty} A(t) = \frac{\mu^3+\lambda\mu^2\left(2+\frac{1}{k}\right)+2\lambda^2\mu\left(2+\frac{1}{k}\right)}{\mu^3+\lambda\mu^2\left(2+\frac{1}{k}\right)+2\lambda^2\mu\left(2+\frac{1}{k}\right)+2\lambda^3\left(2+\frac{1}{k}\right)}$$

5.7

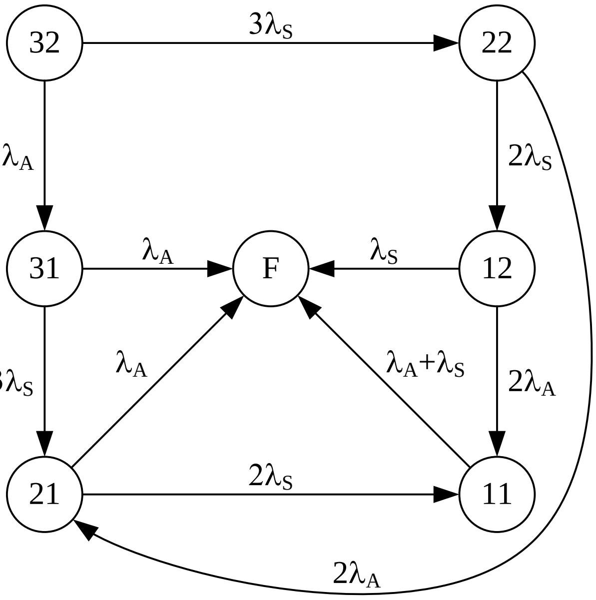
b)

Reliability block diagram



$$R_{sys}(t) = \left\{1-\left(1-R_{pm}(t)\right)^2\right\}\left\{1-\left(1-R_{io}(t)\right)^3\right\}\left\{1-\left(1-R_a(t)\right)^2\right\} \cdot \left\{1-\left(1-R_{s(t)}\right)^3\right\}$$

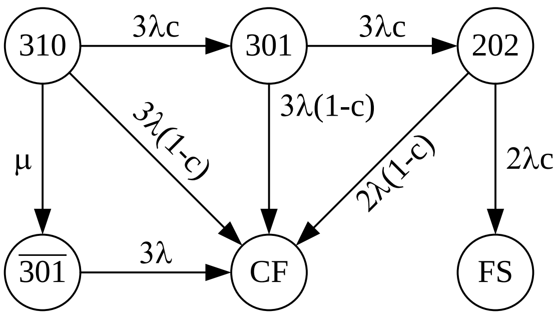
c)



State Labeling
XY:
X= # of working sensors
Y= # of working actuators
F = system failure

5.8

a)

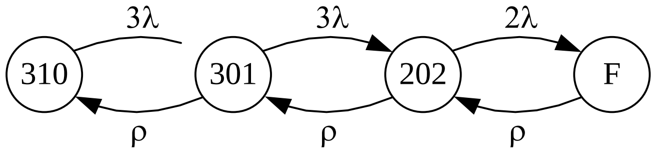


State Labelling
XYZ:
X= # of working active modules
Y= # of working cold stand-by modules
Z= # of working modules

$\overline{301}$ = failed spare, but not activated
FS = fail-safe
CF = catastrophic failure

$$\lim_{t\to\infty} S(t) = \frac{3\lambda c}{3\lambda+\mu}\cdot\frac{3\lambda c}{3\lambda}\cdot\frac{2\lambda c}{2\lambda} = c^3\frac{3\lambda}{3\lambda+\mu}$$

b)



State Labelling

XY:

X= # of working active modules

Y= ## of working cold stand-by spares

Z= # of working modules

F = system failure

$$\lim_{t\to\infty} A(t) = \frac{\rho^3 + 3\lambda\rho^2 + 9\lambda^2\rho}{\rho^3 + 3\lambda\rho^2 + 9\lambda^2\rho + 18\lambda^3}$$

5.9 The system can be divided in to two subsystems, one for the processor part and one for the I/O part. Let R_p denote the reliability of the processor part and R_{io} the reliability of the I/O-part. Finally, let R_{sys} denote the reliability of the total system.

$$R_p = \left(1 + \lambda_p t + \frac{1}{2}\left(\lambda_p t\right)^2\right) \cdot e^{-\lambda_p t}$$
$$R_{io} = (1 + \lambda_{io} t) \cdot e^{-\lambda_{io} t}$$
$$R_{sys} = R_p \cdot R_{io}$$

5.10

$$\lim_{t\to\infty} A(t) = \frac{\rho\mu^2 + \rho\mu\lambda(1+c)}{(1-c)\lambda\mu^2 + \rho\mu^2 + \rho\lambda\mu(1+c) + \rho\lambda^2(1+c)}$$