Exercise 8

FMEA, problem 1.1, Exam problem

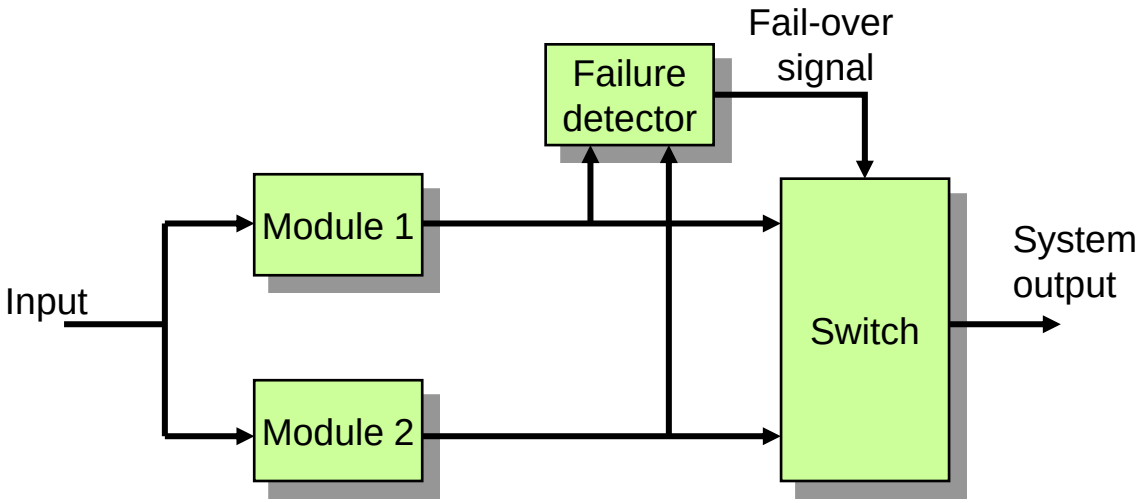
October 2011

FMEA and reliability analysis

- How do we calculate the reliability for a system where the failure detector (error detector) fails?
- Consider the hot standby system shown on the next slide.
- Failure mode assumptions for the failure detector:
  - Generates no fail-over signal when a module fails
  - Generates erroneous fail-over signal
- An FMEA is useful for specifying the failure mode assumptions

Standby redundancy

Hot standby system



Module 1 and 2 perform the same computations.

Module 1 delivers system output when the system is started.

The failure detector issues a *fail-over* when it detects a failure in the output of the module that is connected to the system output.

Simplified FMEA for Hot Standby System (Version 1)

Simplified FMEA for Hot Standby System				
Ref. No.	Unit	Failure mode	System effect	Failure rate
1	Module 1, primary module	Fail silent	System remains operational if no other unit are faulty. System fails if Module 2 is faulty	λ_m
2	Module 2, back-up module	Fail silent	System remains operational if no other unit are faulty. System fails if Module 1 is faulty	λ_m
3	Failure detector	No fail-over when active module fails	System failure when the active module fails	λ_{fd1}
4	Failure detector	False fail-over	System failure if one module is faulty	λ_{fd2}
5	Switch	No switch on fail-over signal	System failure when the active module fails	λ_{sw}

Simplified FMEA for Hot Standby System (Version 2)

Simplified FMEA for Hot Standby System				
Ref. No.	Unit	Failure mode	System effect	Failure rate
1	Module 1	Fail silent	System remains operational if no other units are faulty. System fails if Module 2 or Failure detector is faulty	λ_m
2	Module 2	Fail silent	System remains operational if no other units are faulty. System fails if Module 1 is faulty	λ_m
3	Failure detector (including switch)	No fail-over when active module fails	System failure when the active module fails	λ_d

Simplified FMEA for Hot Standby System (Version 2)

Table of States:

States for Modules M_1 and M_2

0 : OK

1 : Fail Silent Failure with the Rate of λ_m

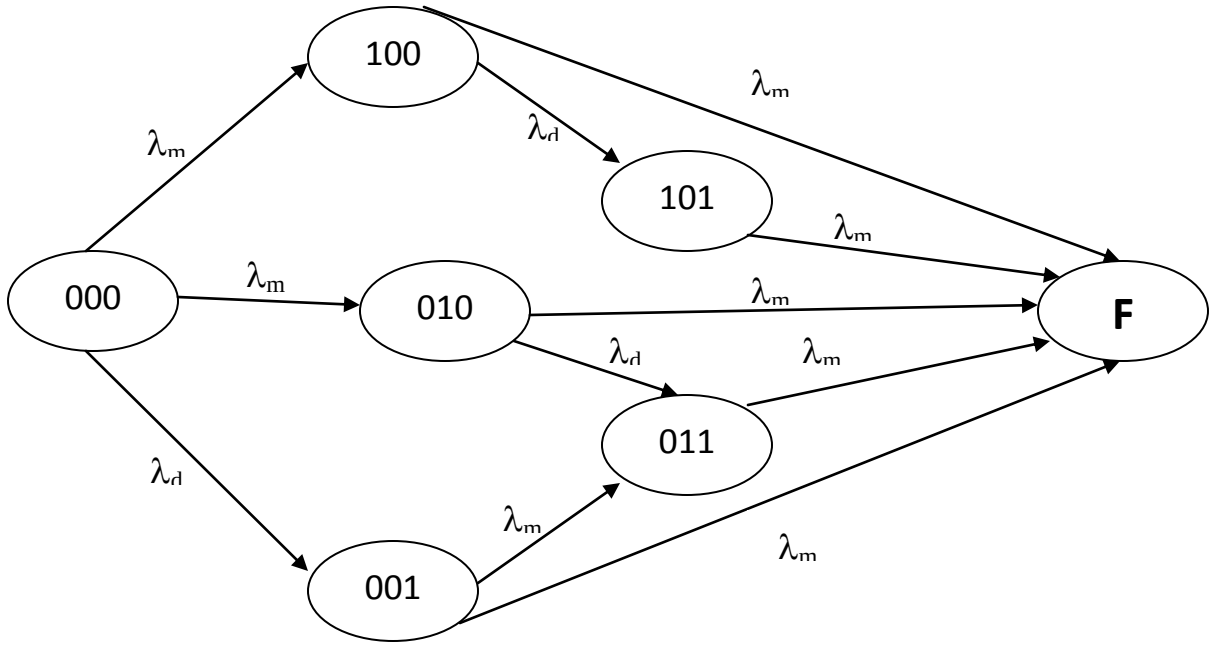
States for Failure Detector

0 : OK

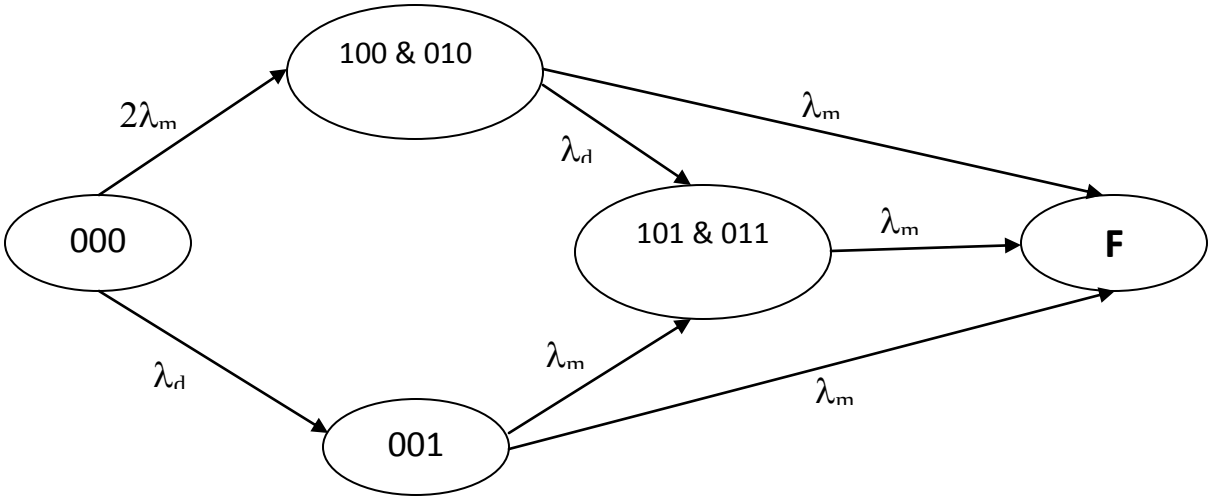
1 : No Fail-over with the Rate of λ_d

Number of Failures	M1 M2 FD	M1 M2 FD	failure rate	effect on the system
1	0 0 0	1 0 0	λ_m	OK
1	0 0 0	0 1 0	λ_m	OK
1	0 0 0	0 0 1	λ_d	OK
2	1 0 0	1 1 0	λ_m	Failure
2	1 0 0	1 0 1	λ_d	OK
2	0 1 0	1 1 0	λ_m	Failure
2	0 1 0	0 1 1	λ_d	OK
2	0 0 1	1 0 1	λ_m	Failure
2	0 0 1	0 1 1	λ_m	OK
3	1 0 1	1 1 1	λ_m	Failure
3	0 1 1	1 1 1	λ_m	Failure

Markov Chain:



Simplified Markov Chain:



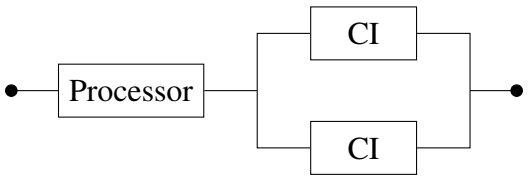
1.

a)

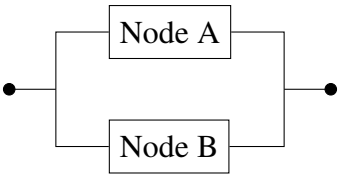
There are six error containment regions. Each processor and each communication interface must constitute an error containment region to achieve maximum reliability of the FTU.

b)

We can model a single node in the FTU using the following reliability block diagram:



The FTU, which consists of two nodes, is modelled by the following reliability block diagram:



Let R_p denote the reliability of a processor, R_c the reliability of a communication interface, and R_{cc} the reliability of two communication interfaces. We then obtain:

$$\begin{aligned}
R_p(t) &= e^{-\lambda_p t} \\
R_c(t) &= e^{-\lambda_c t} \\
R_{cc}(t) &= 1 - (1 - R_c)^2 = 2R_c - R_c^2 = 2e^{-\lambda_c t} - e^{-2\lambda_c t} \\
R_{node}(t) &= R_p \cdot R_{cc} = e^{-\lambda_p t}\left(2e^{-\lambda_c t} - e^{-2\lambda_c t}\right) \\
R_{FTU}(t) &= 1 - (1 - R_{node})^2 = 2R_{node} - R_{node}^2.
\end{aligned}$$

c)

For a single communication interface, the rate for a fail-silence violation is $(1 - \mathit{fsc})\lambda_c$. Let F denote the expected time from the start of four communication interfaces to the first fail-silence violation.

$$F = \int_0^\infty e^{-4(1-\mathit{fsc})\lambda_c t} dt = \frac{1}{4(1-\mathit{fsc})\lambda_c}$$

Exercise 8

We will solve problem 1.1 and some problems from old exams in this exercise.

Problem 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 $f(t) = \lambda e^{-\lambda t}$.

Solution

Let X denote the lifetime for a unit. We define $h(t)$ so that $h(t) \cdot \delta$ is the probability that the unit fails in the interval $(t, t+\delta]$, given that the unit works at time t. We also define the two events A and B:

A The unit fails in the interval $(t, t+\delta]$.
B The unit works at time t.

The probability of the two events are

$$\begin{aligned} P(A) &= P(t < X \leq t+\delta) \\ P(B) &= P(X > t) \end{aligned}$$

The formula for calculating conditional probability

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

gives

$$\begin{aligned} h(t) \cdot \delta &= P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{P(A)}{P(B)} \\ &= \frac{P(t < X \leq t+\delta)}{P(X > t)} = \frac{F(t+\delta) - F(t)}{R(t)} \end{aligned}$$

Let $\delta \to \infty$

$$h(t) = \lim_{\delta \to \infty} \frac{1}{\delta} \frac{F(t+\delta) - F(t)}{R(t)} = \frac{F'(t)}{R(t)} = \frac{f(t)}{R(t)}$$

For the exponential distribution:

$$\begin{aligned} f(t) &= \lambda e^{-\lambda t} \\ \Rightarrow h(t) &= \frac{f(t)}{R(t)} = \frac{f(t)}{1 - F(t)} = \frac{\lambda e^{-\lambda t}}{1 - (1 - e^{-\lambda t})} = \frac{\lambda e^{-\lambda t}}{e^{-\lambda t}} \\ &= \lambda \end{aligned}$$