TELECOM ParisTech

Institut Mines-Télécom

Reliability

Embedded Systems

Lirida Alves de Barros-Naviner
Master Program

Outline

Outline

Table of Contents

Dependability

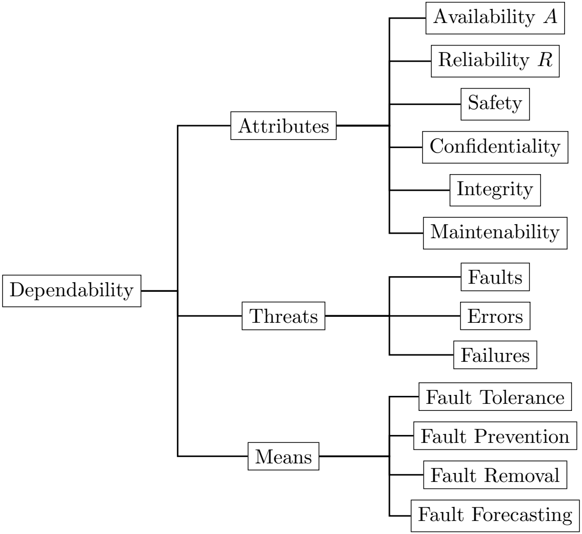
Definition

Dependability is the ability of a system to deliver service that can *justifiably* be trusted.

Definition

Dependability is the ability of a system to avoid *service failures* that are *more frequent or more severe* than is *acceptable*.

Taxonomy


Dependability
Attributes
Availability A
Reliability R
Safety
Confidentiality
Integrity
Maintenability
Threats
Faults
Errors
Failures
Means
Fault Tolerance
Fault Prevention
Fault Removal
Fault Forecasting

Dependability Attributes

- **Availability:** readiness for correct service.
- **Reliability**: continuity of correct service.
- **Safety**: absence of catastrophic consequences on the user(s) and the environment.
- **Integrity**: absence of improper system alterations.
- **Maintainability**: ability to undergo modifications and repairs.

Dependability Threats

- **Fault**: an *unexpected (incorrect) condition* that can lead the system to achieve *abnormal states*. A fault can lead to an error.
- **Error**: an *undesired (incorrect) state* of the system. An error can lead to an incorrect response of the system.
- **Failure**: an *incorrect response* of the system. It means the service provided by the system differs from the expected one.

Means to Ensure Dependability

- **Fault prevention**: avoid things go wrong!
- **Fault tolerance**: deal with, when things go wrong!
- **Fault removal**: make it right, if things went wrong!
- **Fault forecasting**: be aware of how wrong things can go

Commun Measures

- Failure Rate
- Mean Time to Failure
- Mean Time to Repair
- Availability
- Mean Time Between Failures
- Fault Coverage

Failure Rate

Definition

The **failure rate** λ is the expected number of failures per unit time.

- For a system with n components λ can be estimated as:

$$\lambda = \sum_{i=1}^{n} \lambda_i$$

n independent components

$$\boxed{\lambda = \sum_{i=1}^{n} \lambda_i}$$

Mean Time to Failure

Definition

The **Mean Time to Failure (MTTF)** of a system is the expected time of the occurrence of the first system failure.

n components

$$\text{MTTF} = \frac{1}{n}\sum_{i=1}^{n} t_i$$

Failures In Time

$$\text{FIT} = \frac{10^9}{MTTF}$$

Mean Time to Repair

Definition

The **Mean Time to Repair (MTTR)** of a system is the average time required to repair the system.

- MTTR is often given in terms of the repair rate μ, which is the expected number of repairs per unit of time

$$\boxed{\text{MTTR} = \frac{1}{\mu}}$$

Availability

Definition

Instantaneous availability $A(t)$ is the probability the system operates at time t.

- **Interval availability** stands for the average of $A(t)$ over a mission period:

$$\boxed{\text{A(T)} = \frac{1}{T}\int_0^T A(t)dt}$$

- **Steady-state availability** applies when availability is time independent:

$$\boxed{\text{A}(\infty) = \lim_{T\to\infty} A(T) = \frac{n \times MTTF}{n \times MTTF + n \times MTTR} = \frac{\mu}{\mu+\lambda}}$$

  - Supposes n failures during lifetime

Mean Time Between Failures

Definition

The **Mean Time Between Failures (MTBF)** is the average time between failures of the system.

$$\text{MTBF} = \text{MTTF} + \text{MTTR}$$

Assuming repair makes the item perfect

$$\text{MTBF} = \frac{MTTF}{A(\infty)}$$

Fault Coverage

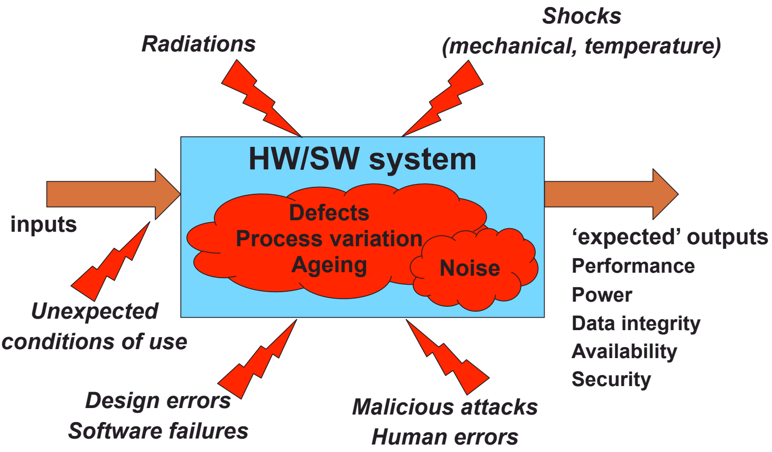
Definition

The **Fault Coverage** FC is the conditional probability related to expected actions when faults occurs.

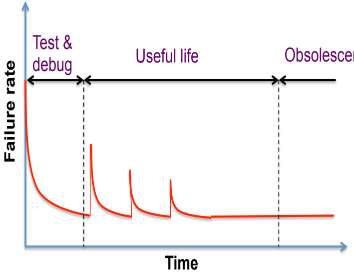
- FC= P(detected faults | existent faults)
- FC= P(located faults | existent faults)
- FC= P(recovered faults | existent faults)
- FC= P(contained faults | existent faults

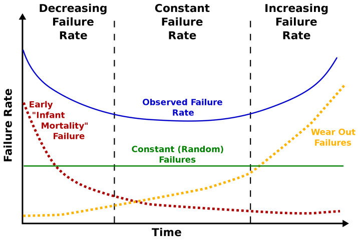
Table of Contents

What About Embedded Systems?

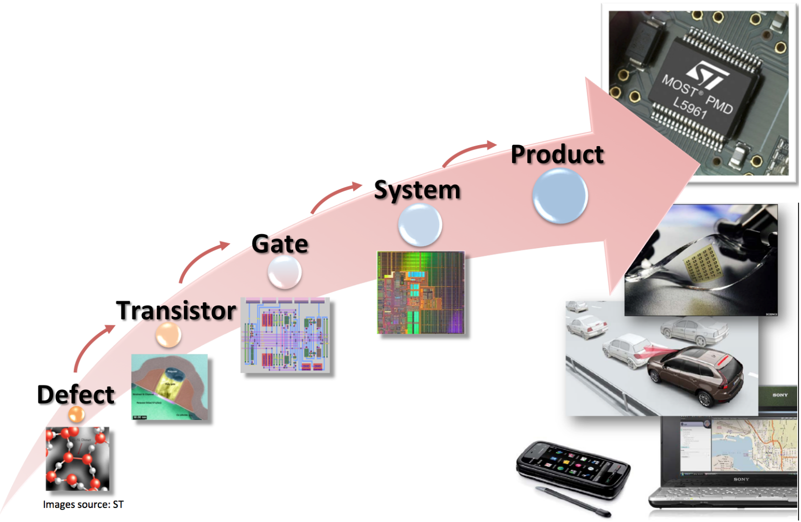


SW and HW Faults

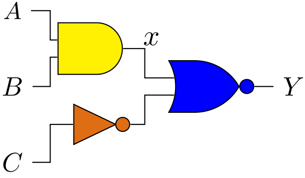




Default/Fault Propagation

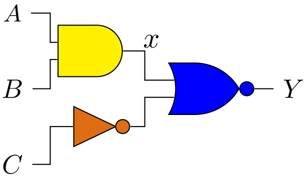


Fault Models: Bit-flip and Stuck-at



A	B	C	x	Y
0	0	0	0	0
0	0	1	0	1
0	1	0	0	0
0	1	1	0	1
1	0	0	0	0
1	0	1	0	1
1	1	0	1	0
1	1	1	1	0

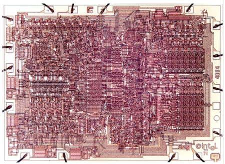
Fault Models: Bit-flip and Stuck-at



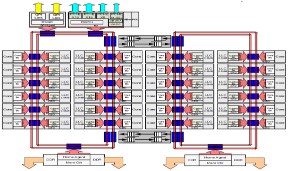
A	B	C	x	Y
0	0	0	1	0
0	0	1	1	0
0	1	0	1	0
0	1	1	1	0
1	0	0	1	0
1	0	1	1	0
1	1	0	1	0
1	1	1	1	0

Advances in CMOS

- Moore's law (popular form): $2\times\ N_{tr}/mm^2$ every 18 months



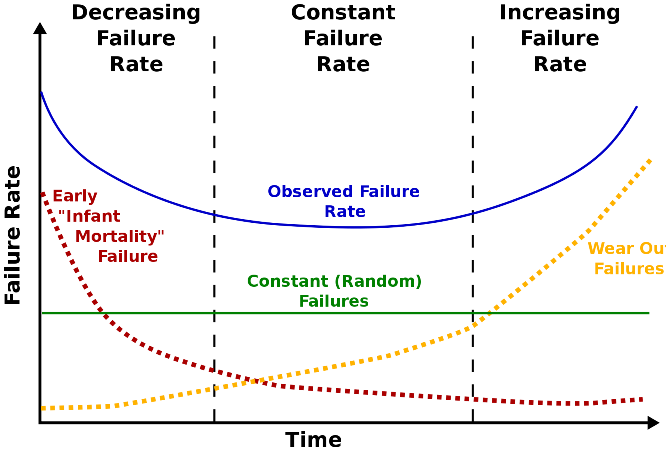
Intel 4004 (1971): 10μm and 2.3×10^3 tr



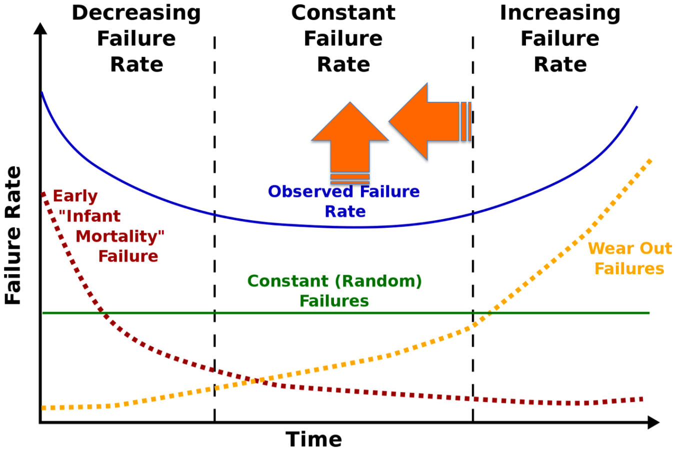
Intel 22-core Xeon Broadwell-E5-2699Rv4 (2016): 14nm and 7.2×10^9 tr

- Scaling issues
  - Design complexity, test challenge, low power voltage
  - Variability – Modelling
  - Sensitivity to unscaled environmental disturbances
- Scaling effects
  - Yield decrease
  - Reliability decrease

Scaling and Reliability



Scaling and Reliability



Outline

Table of Contents

Traditional Approaches

Diagnostics experience

Insufficient to analyze complex designs

Heuristic approaches

Prior to Beginning

- We focus on system modeling
- We consider the system consists of several components: $c_1, c_2, \cdots, c_n$
- We look for a function that enables reliability analysis

Deterministic Model

Definition

The **state of a component** c_i is defined as

$$x_i = \begin{cases} 0 & \text{if the component } c_i \text{ is not fonctionning} \\ 1 & \text{if the component } c_i \text{ is functionning} \end{cases}$$

Definition

The **state set** is defined as the vector composed by the components states

$$\mathbf{x} = (x_1 x_2 \cdots x_n)$$

Deterministic Model (cont.)

Definition

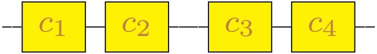
The **system state** is defined as

$$\xi(\mathbf{x}) = \begin{cases} 0 & \text{if the system is not fonctionning with state set } \mathbf{x} \\ 1 & \text{if the system is functionning with state set } \mathbf{x} \end{cases}$$

Reliability Block Diagram

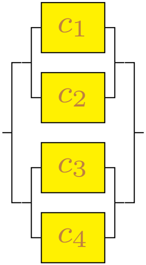
- Static representation (no reference to time)
- Each component represented by a block
- Based on logic (Boolean algebra)
- Independence of components failures
- Behavior facing faults represented by the connections between blocks

Series System



$$
\begin{aligned}
\xi(\mathbf{x}) &= \begin{cases} 0 & \text{if there exists an } i \text{ such that } x_i = 0 \\ 1 & \text{if } x_i = 1 \text{ for all } i \in [1;n] \end{cases} \\
&= \prod_{i=1}^{n} x_i
\end{aligned}
$$

Parallel System

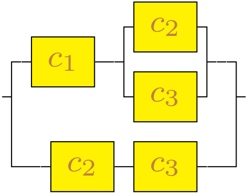


$$\xi(\mathbf{x}) = \begin{cases} 0 & \text{if } x_i = 0 \text{ for all } i \in [1; n] \\ 1 & \text{if there exists an } i \text{ such that } x_i = 1 \end{cases}$$

$$= 1 - \prod_{i=1}^{n} (1 - x_i)$$

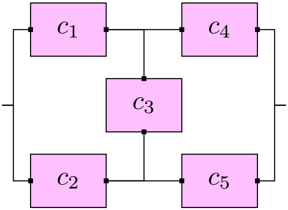
Combined Series-Parallel System

Example: 2 out of 3 structure



$$\xi(\mathbf{x}) = \begin{cases} 0 & \text{if } \sum_{i=1}^{n} x_i < k \\ 1 & \text{if } \sum_{i=1}^{n} x_i \geq k \end{cases}$$

Non Series-Parallel System



Coherent System

Definition

A system of n components is **coherent** if its function $\xi(\mathbf{x})$ is nondecreasing in $\mathbf{x}$ and there are no irrelevant components.

Definition

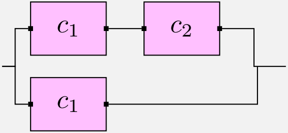
A function $\xi(\mathbf{x})$ is **nondecreasing** in $\mathbf{x}$ if $\xi(x_1 \cdots x_{i-1}\mathbf{0}x_{i+1} \cdots x_n) \leq \xi(x_1 \cdots x_{i-1}\mathbf{1}x_{i+1} \cdots x_n)$.

Definition

A component c_i is **irrelevant** if its state x_i has no impact on the function $\xi(\mathbf{x})$.

Coherent System (cont.)

A non coherent structure:



Structural Importance

Definition

The **structural importance** of a component c_i in a coherent system of n components is

$$I_\xi(i) = \frac{1}{2^{n-1}} \sum [\xi(1_i, \mathbf{x}) - \xi(0_i, \mathbf{x})]$$

Path Vector

Definition

A **path vector** for a coherent system is a vector $\mathbf{x}$ such as $\xi(\mathbf{x}) = 1$.

Definition

A **minimal path** for a coherent system is a path vector $\mathbf{x}$ such as $\xi(\mathbf{y}) = 0$ for all $\mathbf{y} < \mathbf{x}$.

Definition

Given two vectors $\mathbf{x}$ and $\mathbf{y}$, $\mathbf{x} < \mathbf{y}$ if and only if $x_i \leq y_i$ for $i = 1, 2, \cdots, n$ and $x_i < y_i$ for some i.

Definition

A **minimal path set** P_j for a coherent system is a set with all components associated to a given minimal path vector.

Cut Vector

Definition

A **cut vector** for a coherent system is a vector $\mathbf{x}$ such as $\xi(\mathbf{x}) = 0$.

Definition

A **minimal cut vector** for a coherent system is a cut vector $\mathbf{x}$ such as $\xi(\mathbf{y}) = 1$ for all $\mathbf{y} > \mathbf{x}$.

Definition

A **minimal cut set** C_j for a coherent system is a set with all components associated to a given minimal cut vector.

Minimal Sets and System State

Minimal Path Set

$$\xi(\mathbf{x}) = \max_j \prod_{i \in P_j} x_i = 1 - \prod_{j=1}^{l} \left[1 - \prod_{i \in P_j} x_i \right]$$

Minimal Cut Set

$$\xi(\mathbf{x}) = \min_j \left[1 - \prod_{i \in C_j} (1 - x_i) \right] = \prod_{j=1}^{k} \left[1 - \prod_{i \in C_j} (1 - x_i) \right]$$

Table of Contents

Probabilistic Model

Definition

The **random state of a component** c_i is defined as

$$X_i = \begin{cases} 0 & \text{if the component } i \text{ has failed} \\ 1 & \text{if the component } i \text{ is functionning} \end{cases}$$

Definition

The **random state of the set of components** in a system is defined as

$$\mathbf{X} = (X_1 X_2 \cdots X_n)$$

Component and System Reliability

Definition

The **reliability of a component** c_i is defined as the *probability* that component c_i is functionning [at prescribed time]

$$R_i = P\{X_i = 1\} = q_i$$

Definition

The **reliability of a coherent system** is defined by

$$R = P\{\xi(\mathbf{X}) = 1\}$$

Alternative Reliability Calculation

Alternative expressions

$$
\begin{aligned}
R &= P\{\mathbf{X} \text{ is a path vector}\} \\
R &= 1 - P\{\mathbf{X} \text{ is a cut vector}\} \\
R &= R(1_i, \mathbf{q}).q_i + R(0_i, \mathbf{q})(1 - q_i)
\end{aligned}
$$

Reliability Importance

Definition

The **reliability importance of a component** c_i in a coherent system of n components is given by

$$I_{R_i} = \frac{\partial R(\mathbf{q})}{\partial q_i} = R(1_i, \mathbf{q}) - R(0_i, \mathbf{q})$$

for $i = 1, 2, \cdots, n$

Reliability Bounds

Theorem

The reliability of a coherent system of n independent components respects

$$\prod_{i=1}^{n} q_i \leq R(\mathbf{q}) \leq 1 - \prod_{i=1}^{n}(1 - q_i)$$

Bounds: Path and Cut Vectors

Theorem

The reliability of a coherent system of independent components, minimal path sets $P_1, P_2, \cdots, P_l$ and minimal cut sets $C_1, C_2, \cdots, C_k$ respects

$$\prod_{j=1}^{k}\left[1-\prod_{i\in C_j}(1-q_i)\right] \leq R(\mathbf{q}) \leq 1-\prod_{j=1}^{l}\left[1-\prod_{i\in P_j} q_i\right]$$

Table of Contents

Lifetime Models

Definition

Reliability is the ability of an item to perform its *required functions* under *stated conditions* and for a *specified period of time* (IEEE definition).

- A *item* or a *component* may mean a simple (i.e logic gate) or a complex system.
- The definition suggests *behaviour item evolution*.

Lifetime Representations

- We denote T a continuos nonnegative random variable that represents the **lifetime** of a item.
  - Note that *time* may stand to hours but also to number of flips, number of km, etc.
- We consider functions that define the distribution of T, representing the **failure time** of a item.

Probability Density Function

Definition

The **probability density function** (PDF) is defined as

$$f(t) = \lim_{\Delta t \to 0} \frac{P\{t \leq T \leq t + \Delta t\}}{\Delta t}$$

$$f(t) = 0 \text{ for } t < 0 \quad f(t) \geq 0 \text{ for } t \geq 0 \quad \int_0^1 f(t)dt = 1$$

- The PDF indicates the likelihood of failure for any t

Cumulative Distribution Function

- The cumulative distribution function gives the probability that a failure occurs at a time smaller or equal to t is

$$F(t) = \int_{-\infty}^{t} f(t)dt$$

where $f(t)$ is the probability density function (PDF) of the random variable time to failure.

$$P\{t_1 \leq T \leq t_2\} = \int_{t_1}^{t_2} f(t)dt = F(t_2) - F(t_1)$$

Reliability (or Survivor) Function

Definition

The **reliability function** $R(t)$ is defined as

$$R(t) = R(\mathbf{q}, t) = \quad = \quad P\{T \geq t\} \quad \forall t \geq 0$$

$R(t)$ must be nonincreasing and respect $R(0) = 1$, $\lim_{t \to \infty} R(t) = 0$

Hazard Function

Definition

The **hazard function** $h(t)$ is defined as the amount of risk associated to an item at time t.

$$\text{h(t)} = \frac{f(t)}{R(t)}$$

$$\begin{aligned} h(t) &= \lim_{\Delta t \to 0} P\{t \leq T \leq t + \Delta t | T \geq t\} \\ &= \lim_{\Delta t \to 0} \frac{P\{t \leq T \leq t + \Delta t\}}{P\{T \geq t\}} \\ &= \lim_{\Delta t \to 0} \frac{R(t) - R(t + \Delta t)}{R(t)\Delta t} \\ &= \frac{f(t)}{R(t)} \end{aligned}$$

- $h(t)$ represents the instantaneous **failure rate**.
- $h(t)$ must respect $\int_0^\infty h(t)dt = \infty$, $h(t) \geq 0 \quad \forall t \geq 0$

System Lifetime Representation

- Component i
  - Individual representations: $f_i(t)$, $R_i(t)$, $h_i(t)$
  - Individual measures: μ_i, σ_i^2, $t_{k,i}$
- Combine measures according to the structure function

Example

Reliability of a series structure

$$\begin{aligned} R(t) &= R\left(R_1(t), R_2(t), \cdots, R_n(t)\right) \\ & R_1(t).R_2(t). \cdots .R_n(t) \end{aligned}$$

Lifetime & Depend. Measures

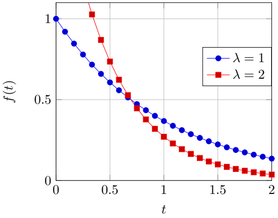
$$\mathbb{E}\{T\} = \int_0^\infty t f(t) dt = \int_0^\infty R(t) dt$$

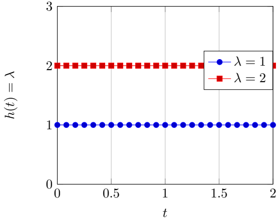
- For nonrepairable systems, the mean corresponds to the mean time to failure $MTTF$. It represents the expected value of time before failure.
- For completely repairable items, the mean represents the mean time between failures $MTBF$.

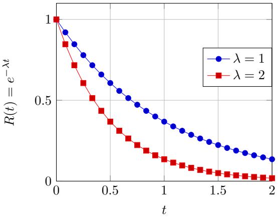
Lifetime Distributions

	Exponential	Weibull	Gamma
$R(t)$	$e^{-\lambda t}$	$e^{-(\lambda t)^\kappa}$	$1 - I(\kappa, \lambda t)$
$f(t)$	$\lambda e^{-\lambda t}$	$\kappa \lambda^\kappa t^{\kappa-1} e^{-(\lambda t)^\kappa}$	$\frac{\lambda}{\Gamma(\kappa)} (\lambda t)^{\kappa-1} e^{-\lambda t}$
$h(t)$	λ	$\kappa \lambda^\kappa t^{\kappa-1}$	$\frac{f(t)}{R(t)}$

Exponential Distribution







Applies for useful life zone in bathtub curve

Table of Contents

Markov Chain

State	Time
Discrete	Discrete
Discrete	Continuous
Continuous	Discrete
Continuous	Continuous

Continuous Time Markov Chains (CTMC)

- Memoryless system
- Discrete space
- Exponential distribution (events at constant rates)

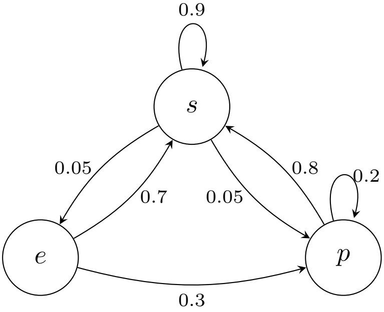
Markov Chain

A lazy, gourmand, and lovely hamster

- When Doudou sleeps, there are 9 chances out of 10 that it will be lying in bed the next minute. When it wakes up, it climbs to its happiness, so there is 1 chance out of 2 that it will be playing and 1 chance out 2 it will be eating.
- Its meals last for one minute and then it starts to play (3 chances out of 10) or it goes to sleep (7 chances out of 10).
- Doudou gets tired quickly. Frequently it goes back to sleep (8 chances out of 10) but, as it loves its spinning wheel, sometimes it continues to play.

- Knowing that Doudou is sleeping now, what will it likely be doing in three minutes?

Markov Chain & Simulation Matrix



$$S = \begin{bmatrix} 0.9 & 0.05 & 0.05 \\ 0.7 & 0 & 0.3 \\ 0.8 & 0 & 0.2 \end{bmatrix}$$

- There are three states: sleep (s), eat (e) and play (p)
- Each element $s_{i,j} \in S$ gives the probability of next state being j given that actual state is i

Simulation Matrix & Behavior

- $P(t) = \begin{bmatrix} P_s(t) & P_e(t) & P_p(t) \end{bmatrix}$ gives the probability of each state for a given time t
- Hypothesis: initial state is s, then
  - $P(0) = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}$
- Probability of next states are:
  - $P(1) = P(0).S = \begin{bmatrix} 0.9 & 0.05 & 0.05 \end{bmatrix}$
  - $P(2) = P(1).S = \begin{bmatrix} 0.885 & 0.045 & 0.07 \end{bmatrix}$
  - $P(3) = P(2).S = \begin{bmatrix} 0.884 & 0.04425 & 0.07175 \end{bmatrix}$
- Probability at time n: $\boxed{\mathrm{P(n)=P(n\text{-}1).S=P(0)S}^n}$

Markov Chain & Transition Matrix

$$P_i(t+dt) = P_i(t)\left[1 - \sum_{j\neq i} s_{i,j}(t)dt\right] + \sum_{j\neq i} P_j(t)s_{j,i}dt$$

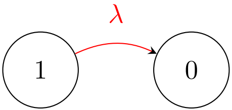
$$\frac{P_i(t+dt) - P_i(t)}{dt} = -P_i(t)\sum_{j\neq i} s_{i,j}(t)dt + \sum_{j\neq i} P_j(t)s_{j,i}dt$$

$$\frac{dP(t)}{dt} = M(t)P(t)$$

- M is the transition matrix. Each $m_{i,j} \in M$ gives the rate with sytem passes from state i to state j
  - $m_{i,j,i\neq j} = s_{j,i}$ and $m_{i,i} = \sum_{j\neq i} s_{j,i}$

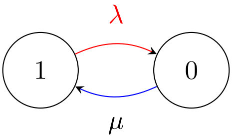
Markov Chain & Transition Matrix (cont.

- One component without repair



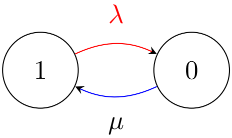
$$M = \begin{bmatrix} m_{11} & m_{10} \\ m_{01} & m_{00} \end{bmatrix} = \begin{bmatrix} -\lambda & \lambda \\ 0 & 0 \end{bmatrix}$$

- One component with repair



$$M = \begin{bmatrix} m_{11} & m_{10} \\ m_{01} & m_{00} \end{bmatrix} = \begin{bmatrix} -\lambda & \lambda \\ \mu & -\mu \end{bmatrix}$$

State Transition Equations (STE)



$$M = \begin{bmatrix} m_{11} & m_{10} \\ m_{01} & m_{00} \end{bmatrix} = \begin{bmatrix} -\lambda & \lambda \\ \mu & -\mu \end{bmatrix}$$

$$\begin{aligned} -\lambda P_1 + \mu P_0 &= 0 \\ \lambda P_1 - \mu P_0 &= 0 \\ P_1 + P_0 &= 1 \end{aligned}$$

$$\boxed{P_1 = \frac{\mu}{\lambda + \mu} \text{ and } P_0 = \frac{\lambda}{\lambda + \mu}}$$

Reliability and STE

$$R(t)=\sum_{i\in\mathcal{T}} P_i(t)$$

$$R(t)=1-\sum_{i\in\mathcal{F}} P_i(t)$$

Assuming repair makes the item perfect, $\mathcal{T}$ is the set of fonctionning states, $\mathcal{F}$ is the set of failing states

Outline

Conclusions

- This course focuses on reliability, which is a dependability's attribute
  - Dependability is an essential quality metric for many systems
- This lesson dealt with different methods for dependability analysis
- The reliability of digital electronics components has specific characteristics
  - Fault models, quality metrics, etc.
- We will explore techniques for reliability improvement and reliability assessment