Dependability

Paulo Maciel

Centro de Informática - UFPE

Objetive

- Learn methods and techniques for dependability assessment of systems.

Requirements

- Basic statistics and probability
- Discrete event systems

Program

- Dependability
  - History
  - Basic concepts and terminology
  - Background
  - Reliability data analysis
  - Detection and recovering mechanisms, and fault tolerance
  - Coherent systems
  - Operational and failure modes

Program

- Dependability
  - Combinational models: RBD, FT, RG
    - Structural and logic functions
    - Analysis methods
    - Modeling
  - CTMC modeling
  - SPN modeling
  - Hierachical and heterogenous modeling

Methodology

- Expositive classes
- Lab. classes

Evaluation

- Problem solving
- Homework

Basic bibliography

- **Dependability Modeling**. Paulo Maciel. Kishor S. Trivedi, Rivalino Matias and Dong Kim. In: Performance and Dependability in Service Computing: Concepts, Techniques and Research Directions ed.Hershey, Pennsylvania: IGI Global, 2011. Book Chapter.
- **Reliability, Maintainability and Risk: Practical methods for engineers**, David J Smith 8th edition, Elsevier. 2011.
- **Reliability: Probabilistic Models and Statistical Methods**, Lawrence M. Leemis, 2nd Edition, ISBN: 978-0-692-00027-4, 2009.
- **Uma Introdução às Redes de Petri e Aplicações**. MACIEL, P. R. M.; LINS, R. D.; CUNHA, Paulo Roberto Freire. Sociedade Brasileira de Computacão, 1996. v. 1. 213 p.
- **Modelling with Generalized Stochastic Petri Nets**, Marsan, A., Balbo, G., Conte, G., Donatelli, S., Franceschinis, G., *Wiley Series in Parallel* Computing, 1995.
- **Queueing Networks and Markov Chains:** Modeling and Performance Evaluation with Computer Science Applications, Second Edition, **Gunter Bolch, Stefan Greiner, Hermann de Meer**, Kishor S. Trivedi, WILEYINTERSCIENCE, 2007.
- **Probability and Statistics with Reliability, Queueing, and Computer Science Applications**, Trivedi. K., *2nd edition, Wiley*, 2002.
- Fundamental Concepts of Computer System Dependability, A. Avižienis, J. Laprie, B. Randell, IARP/IEEE-RAS Workshop on Robot Dependability: Technological Challenge of Dependable Robots in Human Environments – Seoul, Korea, May 21-22, 2001

Dependability

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

The service delivered by a system is its behavior as it is perceived by its user(s).

A user is another system (physical, human) that interacts with the former at the service interface.

The function of a system is what the system is intended for, and is described by the system specification.

[Laprie, J. C. (1985)].

Dependability

In early 1980s Laprie coined the term dependability for encompassing concepts such reliability, availability, safety, confidentiality, maintainability, security and integrity etc [Laprie, J. C. (1985)].

Dependable Computing and Fault Tolerance: Concepts and terminology. In Proc. 15th IEEE Int. Symp. on Fault-Tolerant Computing, (pp. 2-11).

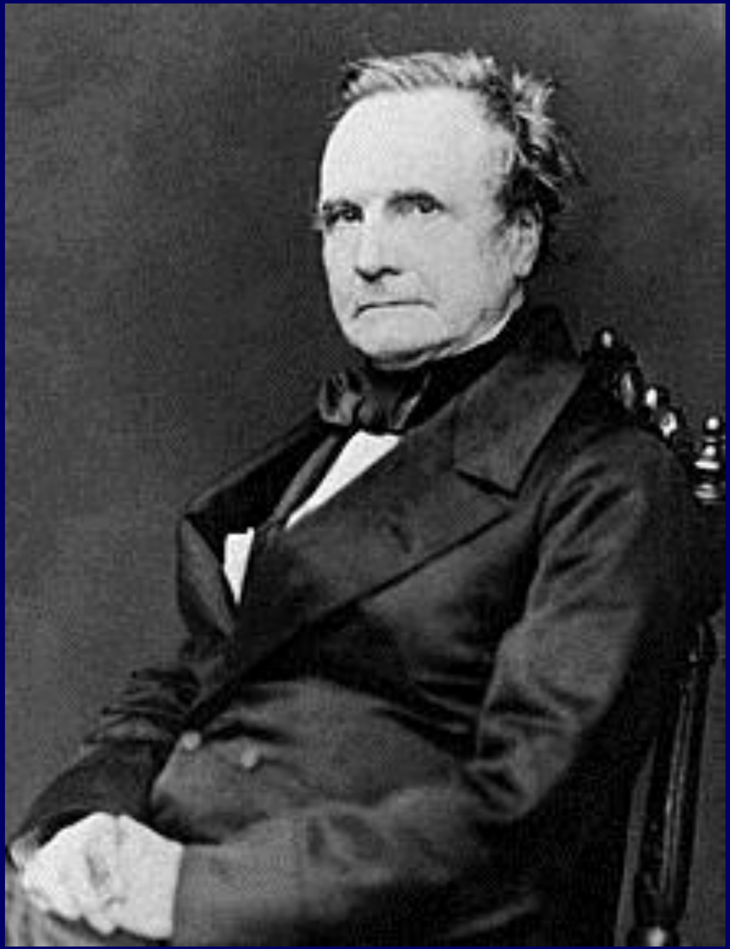
Jean Claude Laprie

A BRIEF HISTORY

A Brief History

Dependability is related to disciplines such as reliability and fault tolerance.

The concept of dependable computing first appeared in 1820s when Charles Babbage undertook the enterprise to conceive and construct a mechanical calculating engine to eliminate the risk of human errors. In his book, "On the Economy of Machinery and Manufacture", he mentions "'The first objective of every person who attempts to make any article of consumption is, or ought be, to produce it in perfect form'." (Blischke, W. R. & Murthy, D. N. P. (Ed.) 2003).



Charles Babbage in 1860

A Brief History

In the nineteenth century, reliability theory evolved from probability and statistics as a way to support computing maritime and life insurance rates.

In early twentieth century methods had been applied to estimate survivorship of railroad equipment [Stott, H. G. (1905)] [Stuart, H. R. (1905)].

A Brief History

The first IEEE (formerly AIEE and IRE) public document to mention reliability is "Answers to Questions Relative to High Tension Transmission" that summarizes the meeting of the Board of Directors of the American Institute of Electrical Engineers, held in September 26, 1902.

[Answers to Questions Relative to High Tension Transmission. (1904). Transactions of the American Institute of Electrical Engineers, XXIII, 571-604.]

In 1905, H. G. Stott and H. R. Stuart: discuss "Time-Limit Relays and Duplication of Electrical Apparatus to Secure Reliability of Services at New York and at Pittsburg.

In these works the concept of reliability was primarily qualitative.

A Brief History

In 1907, A. A. Markov began the study of an important new type of chance process.

In this process, the outcome of a given experiment can affect the outcome of the next experiment.

This type of process is now called a Markov chain [Ushakov, I. (2007)]

Andrei A. Markov

A Brief History

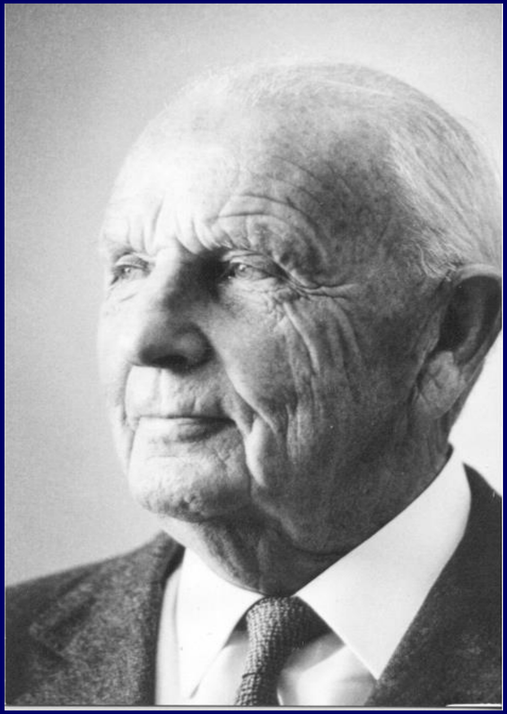
In 1910s, A. K. Erlang studied telephone traffic planning problems for reliable service provisioning [Erlang, A. K. (1909)].

Agner Karup Erlang

[Erlang, A. K. (1909)] Principal Works of A. K. Erlang - The Theory of Probabilities and Telephone Conversations . First published in Nyt Tidsskrift for Matematik B, 20, 131-137.

A Brief History

Later in the 1930s,
extreme value theory was applied to model fatigue life of materials by W. Weibull and Gumbel [Kotz, S., Nadarajah, S. (2000)].



Waloddi Weibull
1887-1979

Gumbel, Emil Julius
(18.7.1891 - 10.9.1966)

A Brief History

In 1931, Kolmogorov, in his famous paper "Über die analytischen Methoden in der Wahrscheinlichkeitsrechnung"

(Analytical methods in probability theory) laid the foundations for the modern theory of Markov processes [Kolmogoroff, A. (1931)].

Andrey Nikolaevich Kolmogorov
(25 April 1903 – 20 October 1987)

Kolmogoroff, A. (1931). Über die analytischen Methoden in der Wahrscheinlichkeitsrechnung (in German). Mathematische Annalen, 104, 415-458. Springer-Verlag.

A Brief History

In the 1940s quantitative analysis of reliability was applied to many operational and strategic problems in World War II [Blischke, W. R. & Murthy, D. N. P. (Ed.) (2003)] [Cox, D. R. (1989)].

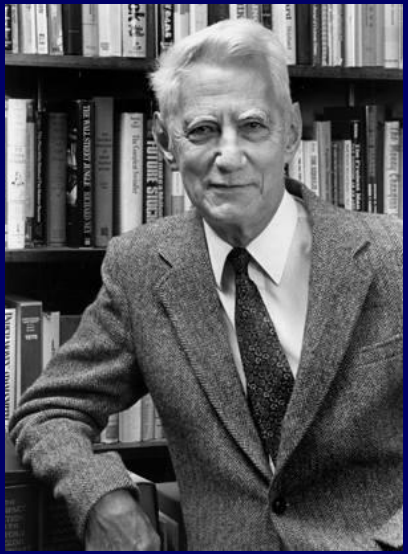
The first generation of electronic computers were quite undependable, thence many techniques were investigated for improving their reliability, such as error:

- control codes,
- replication of components,
- comparison monitoring and
- diagnostic routines.

A Brief History

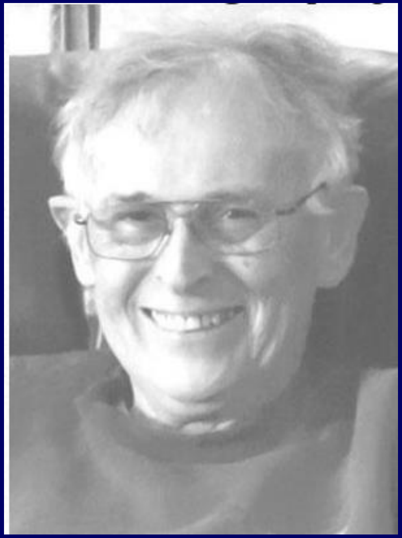
The most prominent researchers during that period were Shannon, Von Neumann and Moore, who proposed and developed theories for building reliable systems by using redundant and less reliable components.

These were the predecessors of the statistical and probabilistic techniques that form the foundation of modern dependability theory [Avizienis, A. (1997)].



C. E. Shanon

John von Neumann



Edward Forrest Moore

A Brief History

In the 1950s, reliability became a subject of great engineering interest as a result of the:

- cold war efforts,
- failures of American and Soviet rockets, and
- failures of the first commercial jet aircraft, the British de Havilland comet [Barlow, R. E. & Proschan, F. (1967)][Barlow, R. E. (2002)].

A Brief History

Epstein and Sobel's 1953 paper studying the exponential distribution was a landmark contribution.

Epstein, B. & Sobel, M. (1953). Life Testing. Journal of the American Statistical Association, 48(263), 486-502.

Milton Sobel

A Brief History

In 1954, the Symposium on Reliability and Quality Control (it is now the IEEE Transactions on Reliability) was held for the first time in the United States.

In 1958, the First All-Union Conference on Reliability took place In Moscow [Gnedenko, B. V., Ushakov, I. A. (1995)] [Ushakov, I. (2007)].

Gnedenko Boris V. (1912-1995)

Gnedenko, B. V., Ushakov, I. A. (1995). Probabilistic Reliability Engineering. J. A. Falk (Ed.), Wiley-Interscience.

Ushakov, I. (2007). Is Reliiabiility Theory Still Alive?. e-journal "Reliability: Theory& Applications", 1(2).

A Brief History

In 1957 S. J. Einhorn and F. B. Thiess adopted Markov chains for modeling system intermittence [Einhorn, S. J. & Thiess, F. B. (1957)].

In 1960, P. M. Anselone employed Markov chains for evaluating availability of radar systems [Anselone, P. M. (1960)].

In 1961 Birnbaum, Esary and Saunders published a milestone paper introducing coherent structures [Birnbaum, Z. W., J. D. Esary and S. C. Saunders. (1961)].

Zygmunt William Birnbaum

A Brief History

Fault Tree Analysis (FTA) was originally developed in 1962 at Bell Laboratories by H. A. Watson to evaluate the Minuteman I Intercontinental Ballistic Missile Launch Control System.

Afterwards, in 1962, Boeing and AVCO expanded use of FTA to the entire Minuteman II.

Minuteman I

Minuteman II

A Brief History

In 1967, A. Avizienis integrated masking methods with practical techniques for error detection, fault diagnosis, and recovery into the concept of fault-tolerant systems [Avizienis, A., Laprie, J.-C., Randell, B. (2001].

Fundamental Concepts of Dependability. LAAS-CNRS, Technical Report N01145.

A. Avizienis

A Brief History

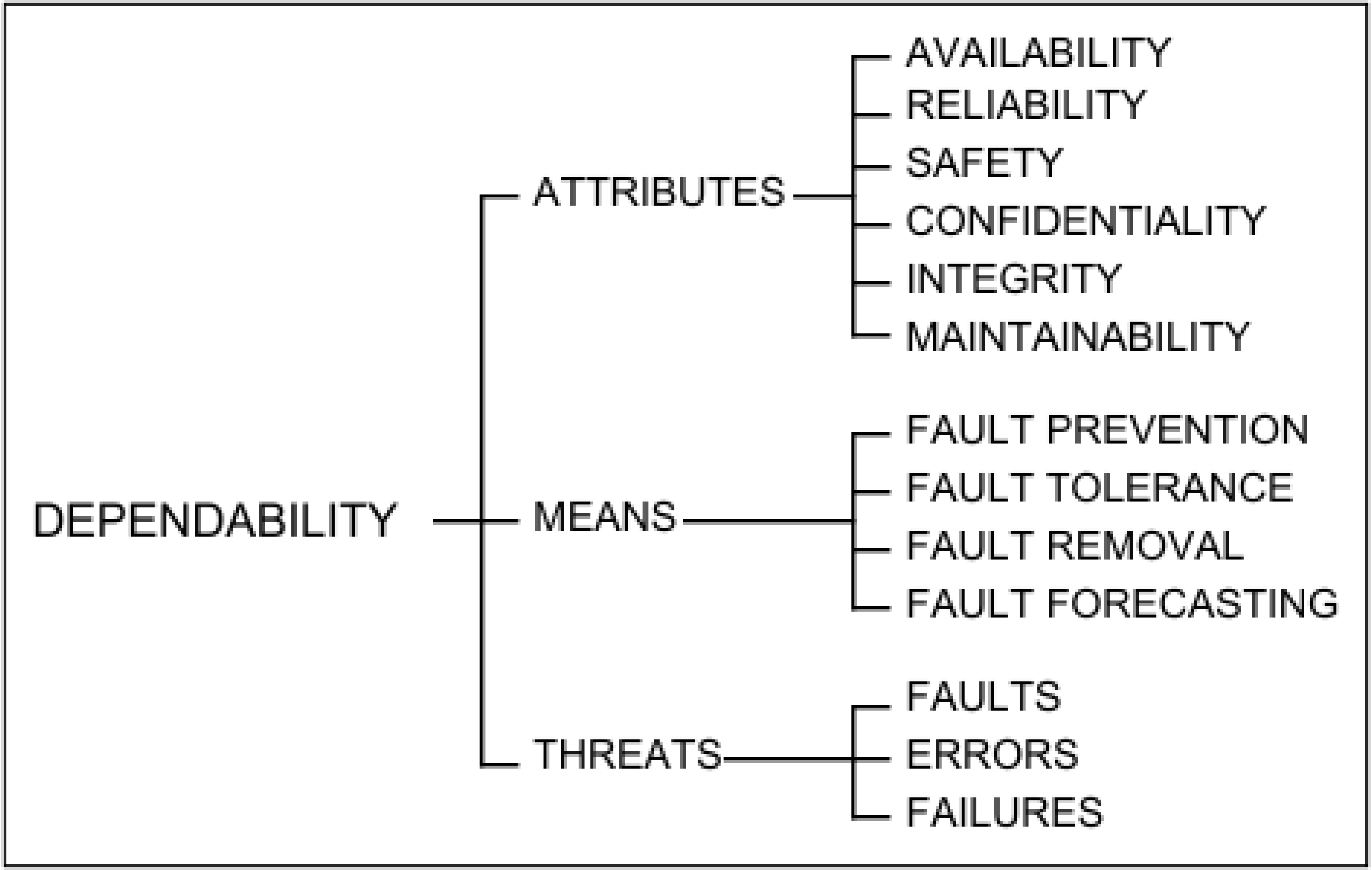
In late 1970s some works were proposed for mapping Petri nets to Markov chains [Molloy, M. K. (1981)][Natkin, S. 1980][Symons, F. J. W. 1978].

These models have been widely adopted as high-level Markov chain automatic generation models as well as for discrete event simulation.

Natkin was the first to apply what is now generally called Stochastic Petri nets to dependability evaluation of systems.

BASIC CONCEPTS

Basic Concepts



The dependability tree

Avizienis, A., Laprie, J.-C., Randell, B. (2001). Fundamental Concepts of Dependability. LAAS-CNRS, Technical Report N01145.

Basic Concepts

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

A correct service is delivered when the service implements what is specified.

- A system failure is an event that occurs when the delivered service deviates from correct service.

A failure is thus a transition from correct service to incorrect service.

A transition from incorrect service to correct service is service restoration.

Basic Concepts

- An error is that part of the system state that may cause a subsequent failure.

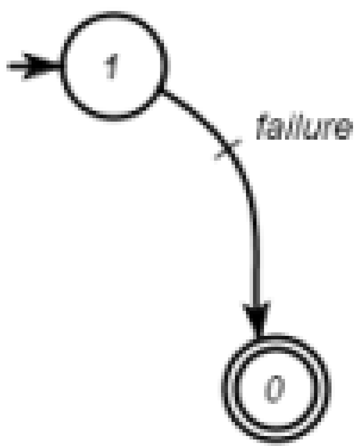
A failure occurs when an error reaches the system interface and alters the service.

Basic Concepts

- Fault is the adjudged or hypothesized cause of an error.

A fault is active when it produces an error; otherwise it is dormant.

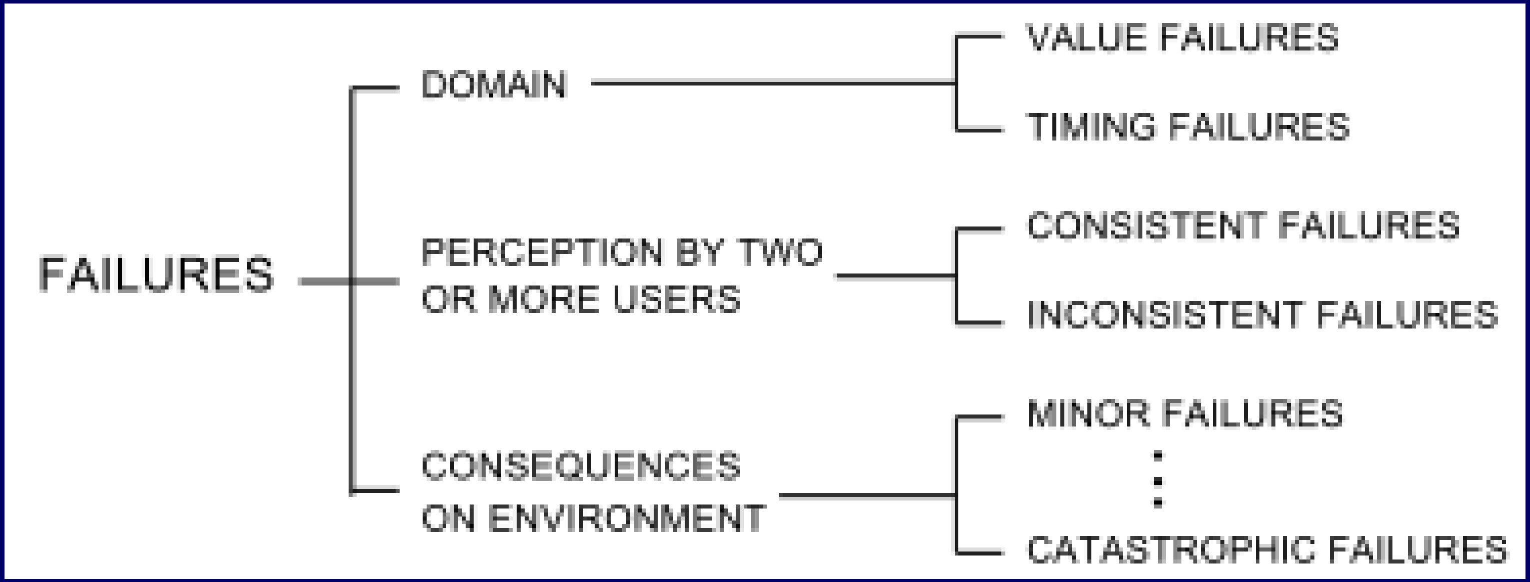
$$X_S(t) = \begin{cases} 0, & if \;\; S \;\; has\, failed \\ 1, & if\, S\, is\, operational \end{cases}$$



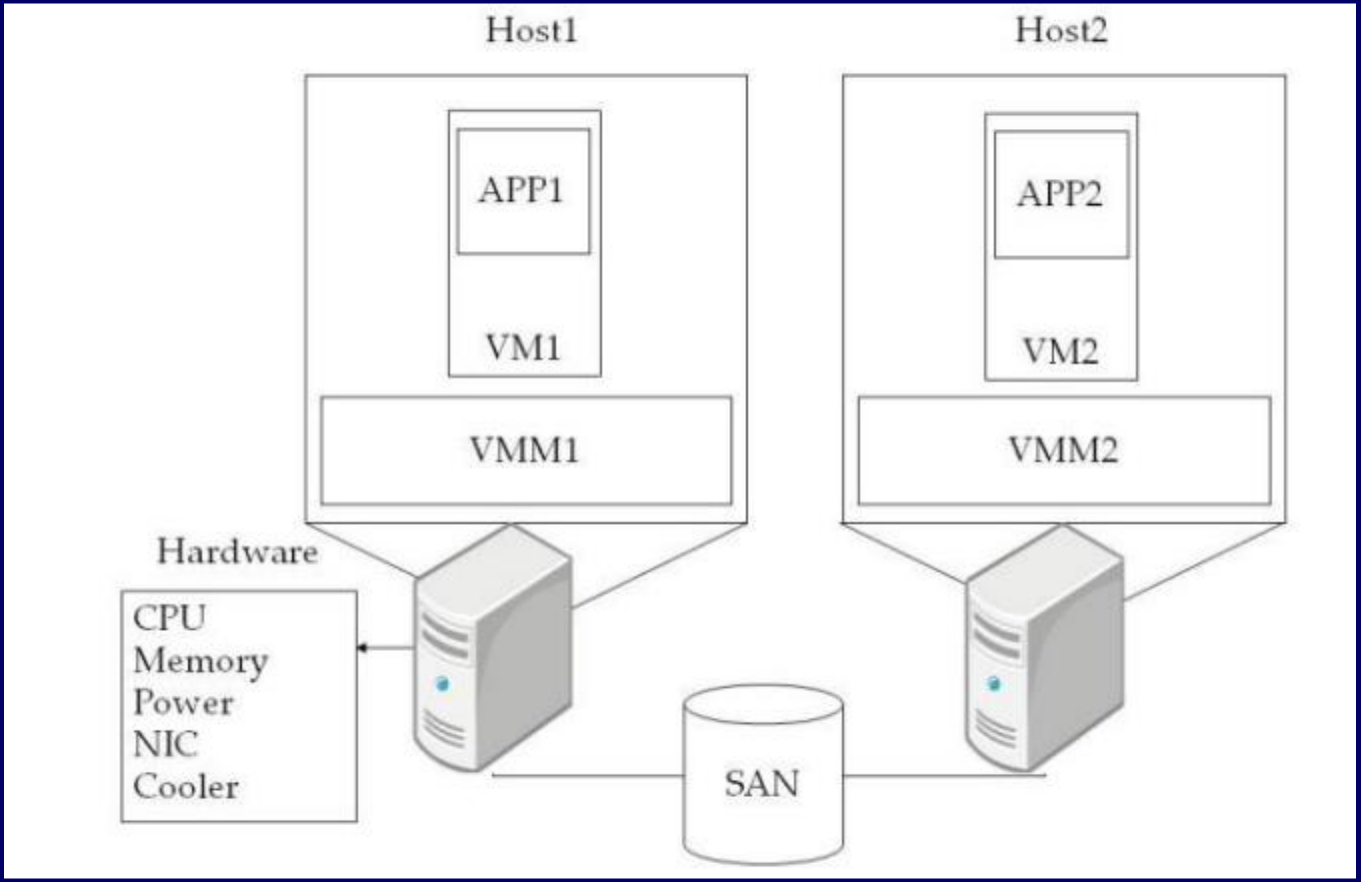
Consider an indicator random variable X(t) that represents the system state at time t.

Basic Concepts

- Failure Modes



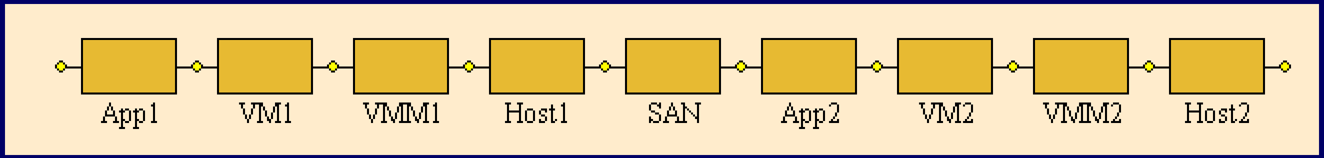
A motivational example



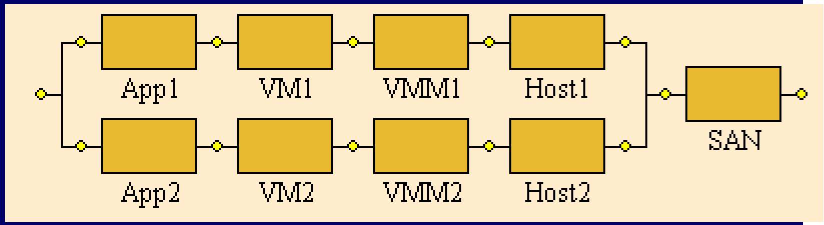
A motivational example

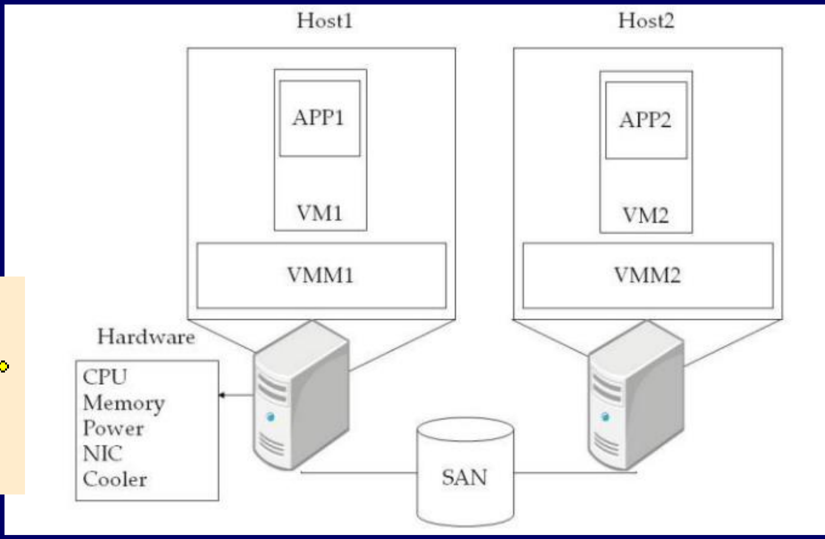
- What is the respective RBD?

This?



Or this?





A motivational example

- It is not clear.

Something is still missing!

- What is it?

  The operational mode(s)

  (success oriented networks: RBD and Relgraph)

  or

  The failure mode(s)

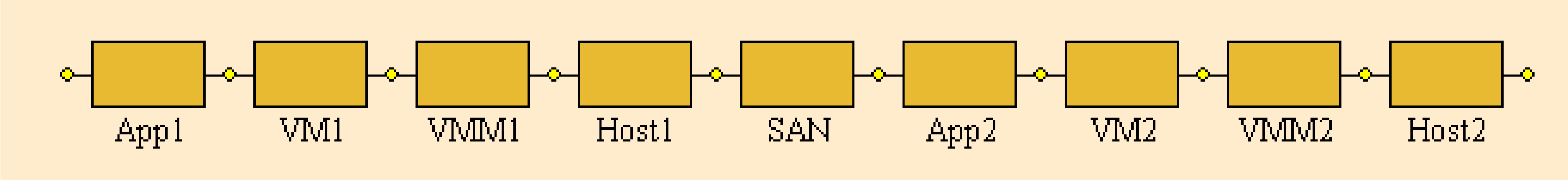
  (failure oriented networks: FT)

Operational Mode

is a condition that defines the system as operational.

- Operational Mode 1

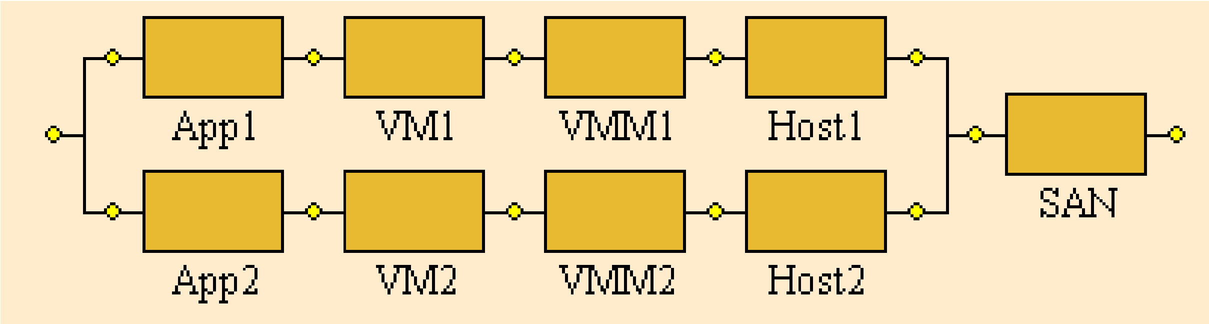
$$OM_1 = App_1 \wedge VMM_1 \wedge VM_1 \wedge H_1 \wedge SAN \wedge App_2 \wedge VMM_2 \wedge VM_2 \wedge H_2$$



Operational Mode

- Operational Mode 2

$$OM_2 = ((App_1 \wedge VMM_1 \wedge VM_1 \wedge H_1) \vee (App_2 \wedge VMM_2 \wedge VM_2 \wedge H_2)) \wedge SAN$$



$$R(t) = 0.975215145, \qquad t = 0.002 \ \ tu$$

Basic Concepts

- Fault prevention: how to prevent the occurrence or introduction of faults;
- Fault tolerance: how to deliver correct service in the presence of faults;
- Fault removal: how to reduce the number or severity of faults;
- Fault forecasting: how to estimate the present number, the future incidence, and the likely consequences of faults.

Basic Concepts

Fault prevention is attained by quality control techniques employed during the design and manufacturing of hardware and software, including structured programming, information hiding, modularization, and rigorous design.

Operational physical faults are prevented by shielding, radiation hardening, etc.

Interaction faults are prevented by training, rigorous procedures for maintenance, "foolproof" packages.

Malicious faults are prevented by firewalls and similar defenses.

Basic Concepts

Fault Tolerance is intended to preserve the delivery of correct service in the presence of active faults.

- Active strategies

  Phase:

  1) Error detection
  2) Recovery

- Passive strategies

  Fault masking

Basic Concepts

Fault Removal is performed both during the development phase, and during the operational life of a system.

Fault removal during the development phase of a system life-cycle consists of three steps: verification, diagnosis, correction.

Checking the specification is usually referred to as validation.

Basic Concepts

Fault Forecasting is conducted by performing an evaluation of the system behavior with respect to fault occurrence or activation.

Classes:

qualitative evaluation identifies event combinations that would lead to system failures;

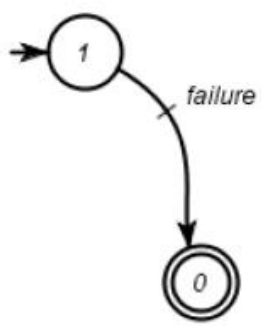
probabilistic evaluation evaluates the probabilities of attributes of dependability are satisfied.

The methods for qualitative and quantitative evaluation are either specific (e.g., failure mode and effect analysis for qualitative evaluation, or Markov chains and stochastic Petri nets for quantitative evaluation), or they can be used to perform both forms of evaluation (e.g., reliability block diagrams, fault-trees).

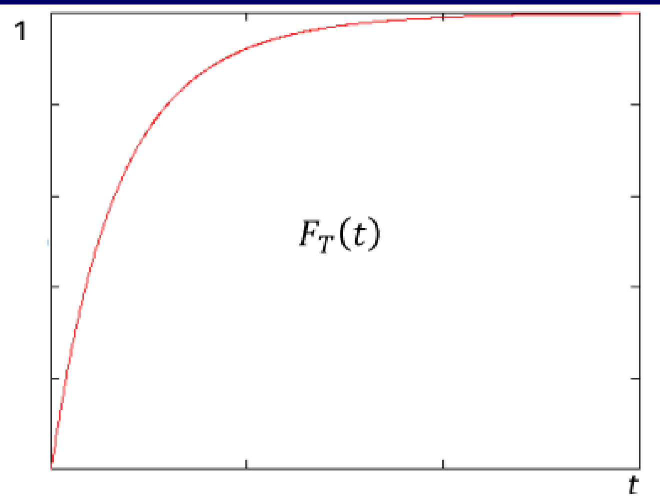
Basic Concepts

- Time to Failure

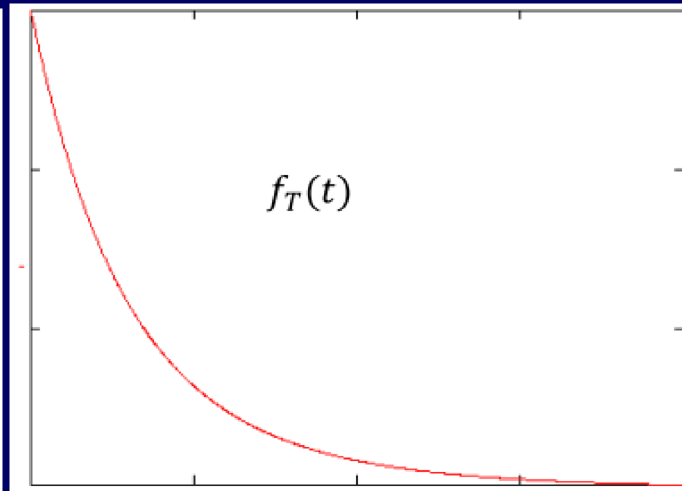
$$X_S(t) = \begin{cases} \mathbf{0}, & \textbf{\textit{if S has failed}} \\ \mathbf{1}, & \textbf{\textit{if S is operational}} \end{cases}$$



States of $X_S(t)$



$F_T(t)$ – Cumulative Distribution Function



$f_{T)}(t)$ - Density Function t

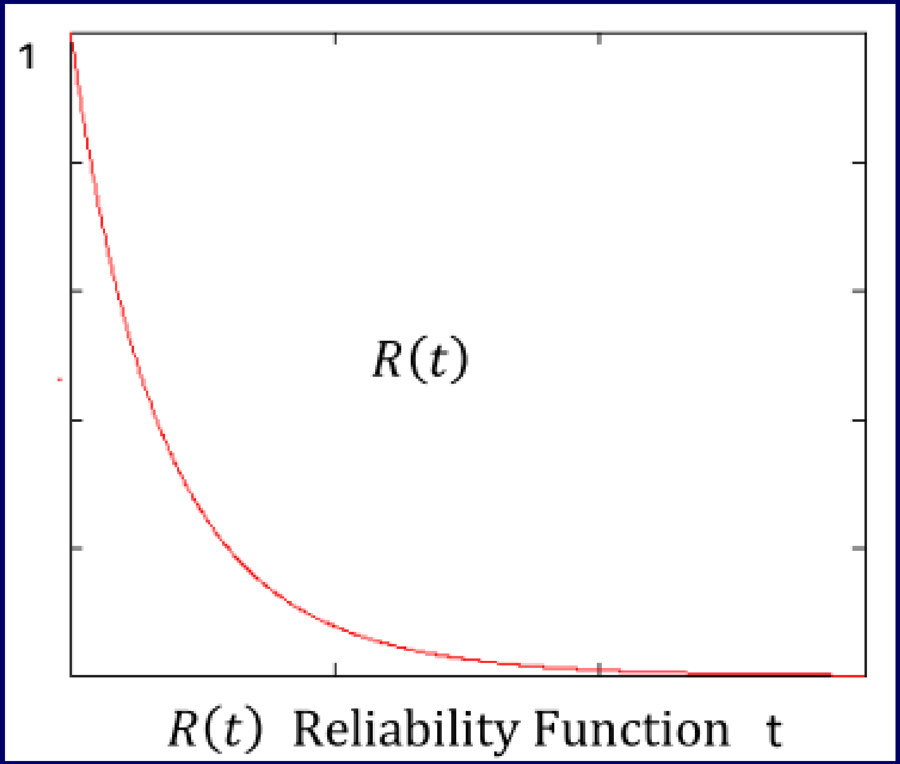
Now, consider a random variable T as the time to reach the state X(t) = 0, given that the system started in state X(t) = 1 at time t = 0. Therefore, the random variable T represents the **time to failure** of the system S, $\boldsymbol{F_T(t)}$ its **cumulative distribution function**, and $\boldsymbol{f_T(t)}$ the respective **density function**, where:

$$F_T(0) = 0 \quad and \quad \lim_{t \to \infty} F_T(t) = 1,$$

$$\boldsymbol{f_T(t) = \frac{dF_T}{dt}}, \qquad \int_0^\infty f_T(t) \times dt = 1$$

Basic Concepts

- Reliability



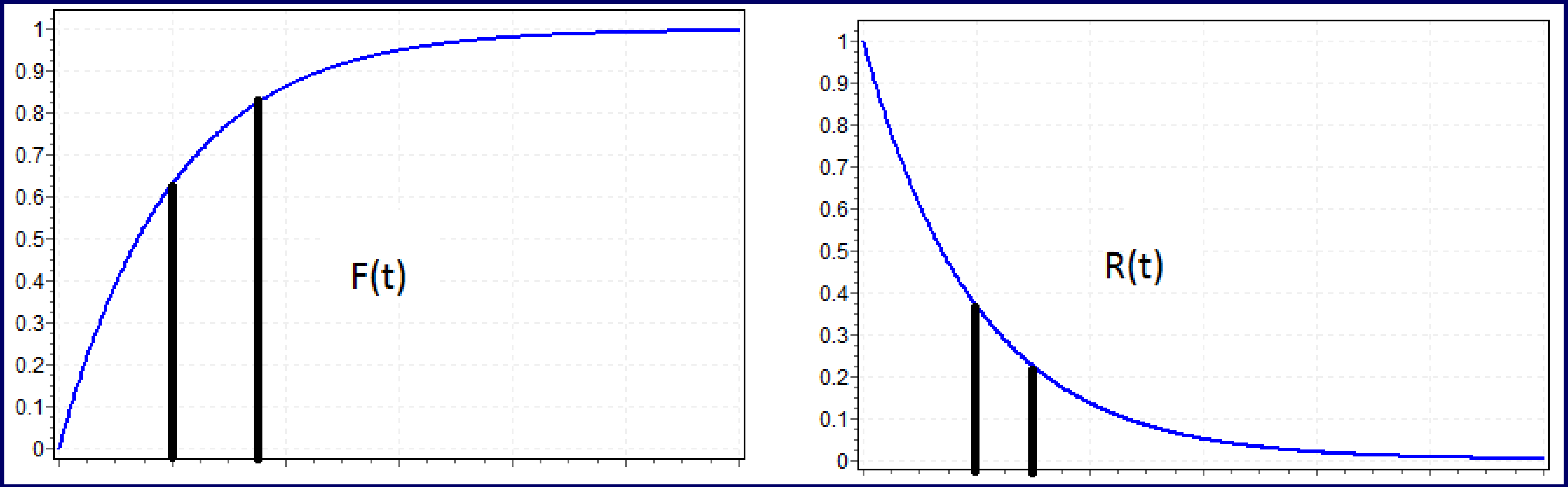
The **probability that the system S does not fail up to time *t* (reliability)** is

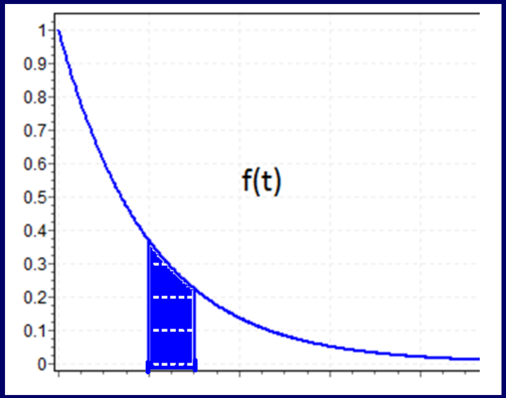
$$P\{T \geq t\} = \boldsymbol{R(t)} = 1 - F_T(t),$$

$$R(0) = 1 \quad and \quad \lim_{t \to \infty} R(t) = 0.$$

Basic Concepts

- Hazard function





Basic Concepts

- Reliability

Reliability (Survivor function) - Complementary of the distribution function: $R(t) = 1 - F(t)$. Therefore, $F(t)$ is the unreliability function.

- DPM

It is common to measure service unreliability as defects per million operations. DPM values are related to a time period. The time period may be in minutes, hours, days, weeks, months etc.

DPM2R(t)
R(t)2DPM

Basic Concepts

- Unreliability as DPM

$$R(t) = 1 - F_T(t)$$

Now consider that n devices have been placed under test.

If after a testing period ΔT, n_i devices survived, then the reliability may be estimated as

$$\widehat{R(\Delta T)} = \frac{n_i}{n}$$

Therefore, the unreliability $UR(\Delta T) = F_T(\Delta T)$ may also be estimated by:

$$U\widehat{R(\Delta T)} = F_T\widehat{(\Delta T)} = 1 - \widehat{R(\Delta T)} =$$

$$1 - \widehat{R(\Delta T)} = 1 - \frac{n_i}{n} = \frac{n - n_i}{n}$$

$n - n_i$ is the number of failures (defects -D) in the test period, so

$$D = n - n_i = U\widehat{R(\Delta T)} \times n$$

If $n = 10^6$ (one million), then

$$DPM = U\widehat{R(\Delta T)} \times 10^6$$

$$(DPM - Defect\ per\ million)$$

Therefore:

$$DPM = UR(t) \times 10^6$$

$$DPM = (1 - R(t)) \times 10^6$$

$$R(t) = 1 - (DPM \times 10^{-6})$$

$$Time\ period = t - 0$$

Basic Concepts

- Hazard function

The probability of the system S failing during the interval $[t, t + \Delta t]$ if it has survived to the time t (conditional probability of failure) is

$$P\{t \leq T \leq t + \Delta t | T > t\} =$$

$$\frac{R(t) - R(t + \Delta t)}{R(t)}.$$

$P\{t \leq T \leq t + \Delta t | T > t\}/\Delta t$ is conditional probability of failure per time unit. When $\Delta t \longrightarrow 0$, then

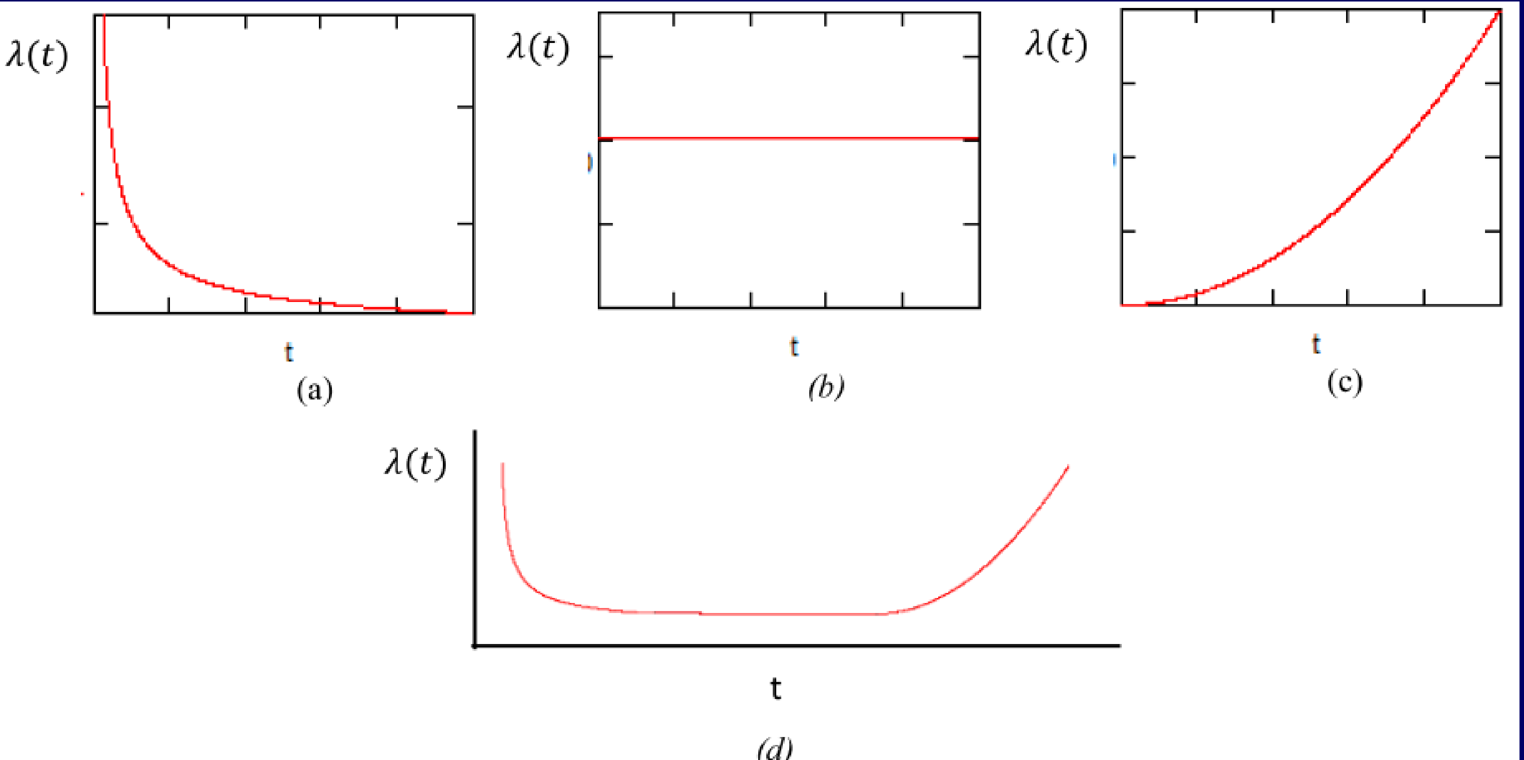
$$\lim_{\Delta t \longrightarrow 0} \frac{R(t) - R(t + \Delta t)}{R(t) \times \Delta t} = \lim_{\Delta t \longrightarrow 0} \frac{-[R(t + \Delta t) - R(t)]}{\Delta t} \times \frac{1}{R(t)} = -\frac{dR(t)}{dt} \times \frac{1}{R(t)} =$$

$$\frac{dF_T(t)}{dt} \times \frac{1}{R(t)} = \frac{f_T}{R(t)} = \lambda(t)$$

Basic Concepts

- Hazard function

Hazard rates may be characterized as decreasing failure rate (DFR), constant failure rate (CFR) or increasing failure rate (IFR) according to $\lambda(t)$.



Hazard rate: (a) Decreasing, (b) Constant, (c) Increasing, (d) Bathtub curve

Basic Concepts

- Cumulative Hazard function

Since

$$\lambda(t) = -\frac{dR(t)}{dt} \times \frac{1}{R(t)},$$

$$\lambda(t)dt = -\frac{dR(t)}{R(t)},$$

thus,

$$\int_0^t \lambda(t)dt = -\int_0^t \frac{dR(t)}{R(t)} =$$

$$-\int_0^t \lambda(t)dt = \ln R(t) =$$

$$R(t) = e^{-\int_0^t \lambda(t)dt} = e^{-H(t)}$$

Basic Concepts

- Mean Time To Failure

$$MTTF = E[T] = \int_0^{\infty} t \times f_T(t)dt.$$

Since

$$f_T(t) = \frac{dF_T}{dt} = -\frac{dR(t)}{dt},$$

thus,

$$MTTF = E[T] = -\int_0^{\infty} \frac{dR(t)}{dt} \times t\, dt.$$

Let $u = t$, $dv = \frac{dR(t)}{dt} \times dt$, and applying integration by parts $\left(\int u\, dv = uv - \int v\, du\right)$, then $du = dt$, $v = R(t)$, hence:

Basic Concepts

- Mean Time To Failure

$$MTTF = -\int_0^{\infty} \frac{dR(t)}{dt} \times t\, dt = -\left[t \times R(t)|_0^{\infty} - \int_0^{\infty} R(t) \times dt \right] =$$

$$-\left[0 - \int_0^{\infty} R(t) \times dt \right] = \int_0^{\infty} R(t) \times dt,$$

hence

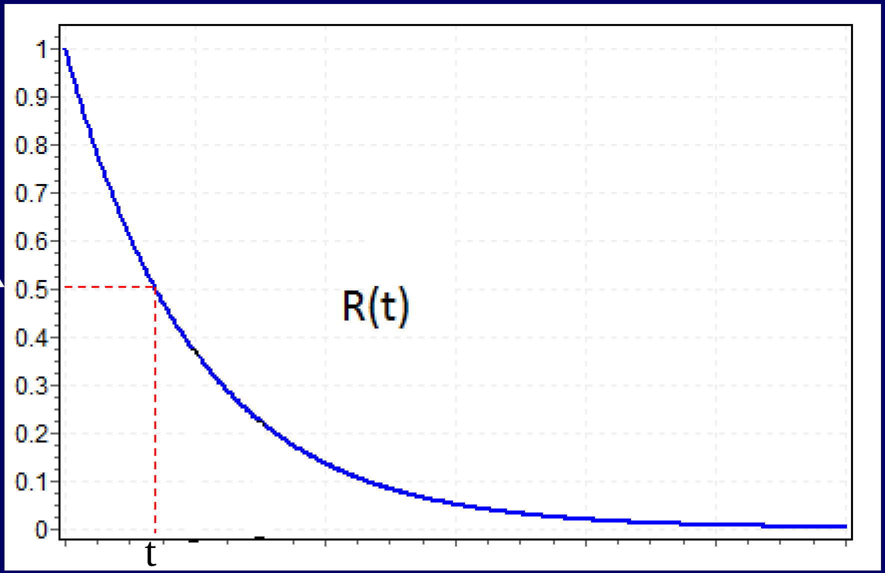
$$MTTF = \int_0^{\infty} R(t) \times dt$$

Basic Concepts

- Median Time To Failure

$$MedTTF = t,\ F_T = R(t) = 0.5$$

R(t)

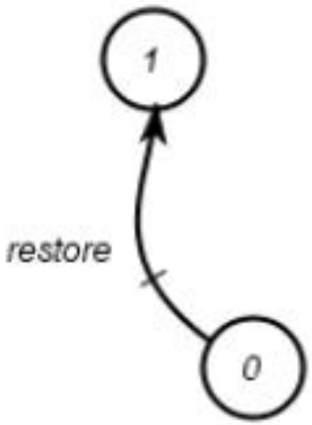


The median time to failure divides the time to fail distribution into two halves, where 50% of failures occur before $MedTTF$ and the other 50% after.

Basic Concepts

Consider a continuous time random variable $X_S(t)$ that represents the system state. $X_S(t)$=0 when S is failed, $X_S(t)$ =1 when S is operational

$$X_S(t) = \begin{cases} 0, & if \;\; S \;\; has\, failed \\ 1, & if\; S\; is\; operational \end{cases}$$



States of $X_S(t)$

Now, consider the random variable D that represents the time to reach the state $X_S(t) = 1$, given that the system started in state $X_S(t) = 0$ at time $t = 0$.

Therefore, the random variable **D** represents the system **time to repair**, $\boldsymbol{F_{\mathrm{D}}(t)}$ its **cumulative distribution function**, and $\boldsymbol{f_{\mathrm{D}}}\,(\boldsymbol{t})$ the respective **density function**

$$F_{\mathrm{D}}\,(0) = 0 \quad and \quad \lim_{t \longrightarrow \infty} F_{\mathrm{D}}\,(t) = 1,$$

$$\boldsymbol{f_D(t) = \frac{dF_{D(1)}}{dt}},$$

$$f_D(t) \geq 0, \text{ and}$$

$$\int_0^{\infty} f_D(t) \times dt = 1$$

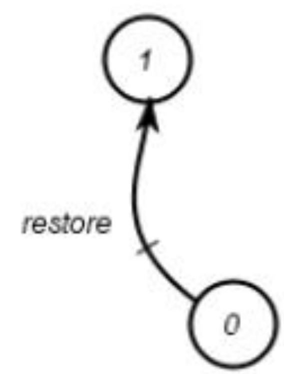
Basic Concepts

Maintainability

Maintainability is the probability the system S will be repaired by t, hence

$$M(t) = P\{D \leq t\} = F_D(t) = \int_0^t f_D(t)dt$$

$$X_S(t) = \begin{cases} 0, & if \;\; S \;\; has\, failed \\ 1, & if\, S\, is\, operational \end{cases}$$



States of $X_S(t)$

Basic Concepts

- Mean Time To Repair

The **mean time to repair (MTTR)** is defined by:

$$MTTR = E[D] = \int_0^\infty t \times f_D(t)dt$$

Basic Concepts

- Repairable Systems

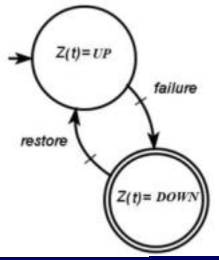
Consider a repairable system S that is either operational (Up) or faulty (Down). Whenever the system fails, a set of activities are conducted in order to allow the restoring process.

These activities might encompass administrative time, transportation time, logistic times etc.
When the maintenance team arrives to the system site, the actual repairing process may start.

Further, this time may also be divided into diagnosis time and actual repair time, checking time etc.

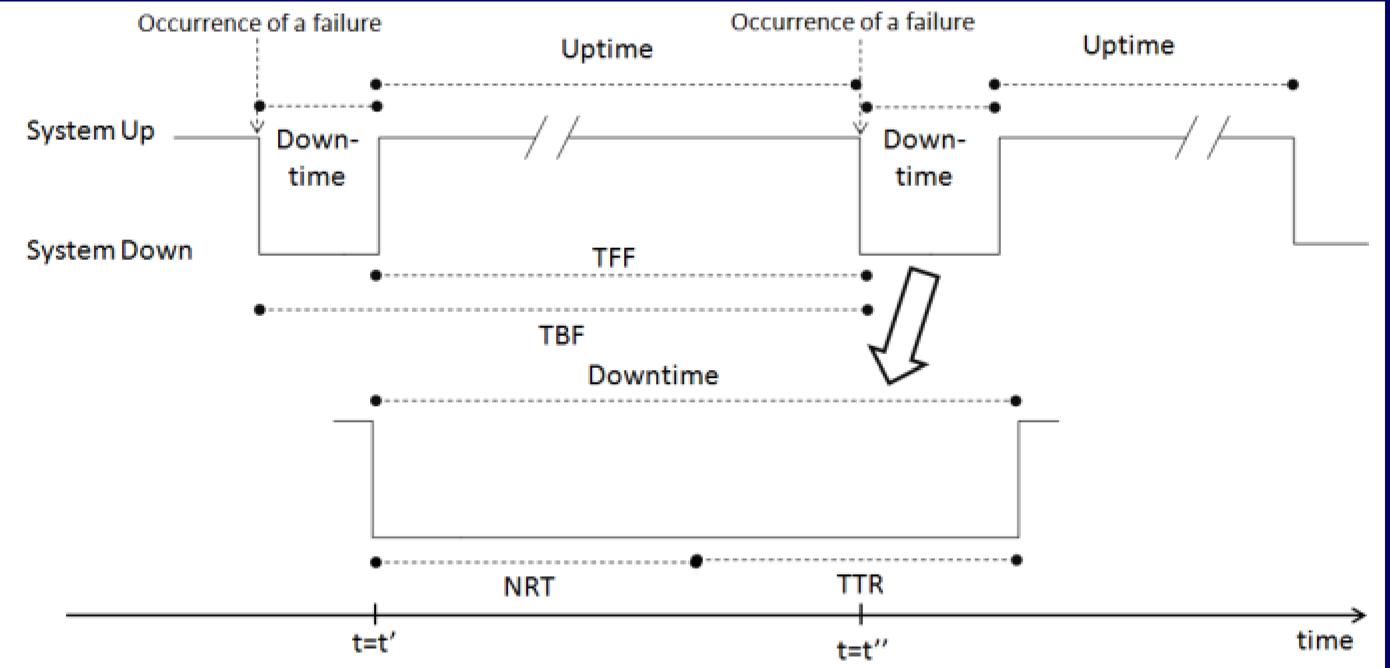
$$Downtime = TR = NRT + TTR.$$

However, for sake of simplicity, we group these times such that the **downtime** equals the **time to restore** –***TR***, which is composed by **non-repair time** – ***NRT*** – (that groups transportation time, order times, deliver times, etc.) and **time to repair** – ***TTR***



Basic Concepts

- Downtime and Uptime



Downtime and Uptime

Basic Concepts

- Availability

The simplest definition of **Availability** is expressed as the ratio of the expected system uptime to the expected system up and downtimes:

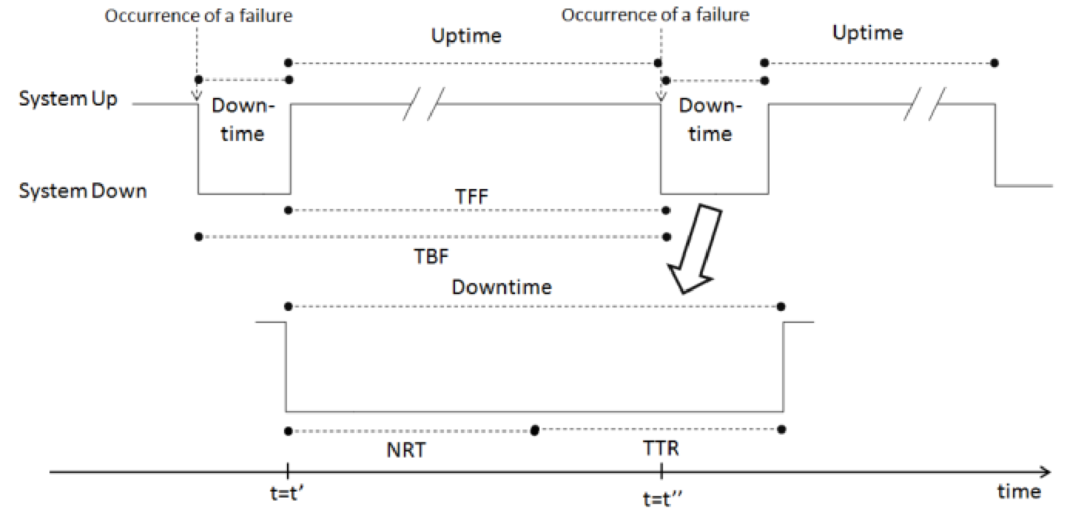
$$A = \frac{E[Uptime]}{E[Uptime]+E[Downtime]}$$

Basic Concepts

- Availability

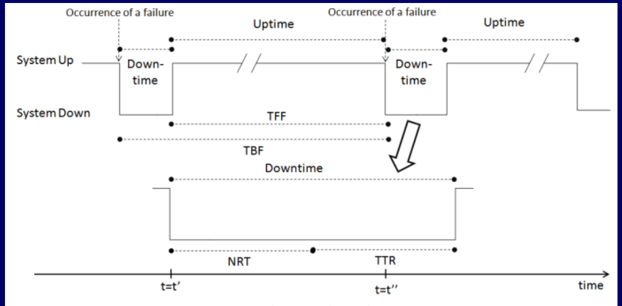
Consider that the system started operating at time $t = t'$ and fails at $t = t''$, thus $\Delta t = t'' - t' = Uptime$.
Therefore, the system availability may also be expressed by:

$$A = \frac{MTTF}{MTTF+MTR}$$



Downtime and Uptime

Basic Concepts



Downtime and Uptime

- Availability

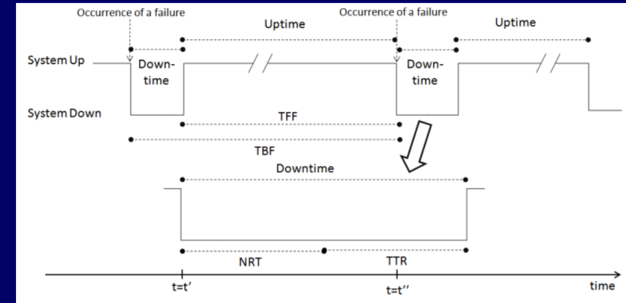
where ***MTR*** is the **mean time to restore**, defined by $MTR = MNRT + MTTR$ ($MNRT$ – **mean non-repair time**, $MTTR$ –**mean time to repair**), so:

$$A = \frac{MTTF}{MTTF + MNRT + MTTR}.$$

If $MNRT \cong 0$,

$$A = \frac{MTTF}{MTTF + MTTR}$$

Basic Concepts



Downtime and Uptime

- Availability

As $MTBF = MTTF + MTR = MTTF + MNRT + MTTR$,
and if $MNRT \cong 0$, then $MTBF = MTTF + MTTR$.

Since $MTTF \gg MTTR$, thus $MTBF \cong MTTF$, therefore:

$$A = \frac{MTBF}{MTBF + MTTR}$$

Basic Concepts

- Instantaneous Availability

The instantaneous availability is the probability that the system is operational at t, that is,

$$A(t) = P\{Z(t) = 1\} = E\{Z(t)\}, \qquad t \geq 0.$$

If repairing is not possible, the instantaneous availability, $A(t)$, is equivalent to reliability, $R(t)$.

Basic Concepts

- Steady State Availability

If the system approaches stationary states as the time increases, it is possible to quantify the steady state availability

$$A = \lim_{t \to \infty} A(t)\,,\ t \geq 0$$

Basic Concepts

Batery test

MTBF *vs* Useful Life Time

Sometimes MTBF is confused with useful life. Consider, a battery has a useful life of four hours and MTBF of 100,000 hours. This means that in a set of 100,000 batteries, there will be about one battery failure every one hour during their useful lives.

The reason of sometimes these numbers are so much high is that these numbers are calculated based on the failure rate of usefulness period of component, and it is assumed that the component will remain in this stage for a long period of time. In the above example, wear out period affects the life of component, and the usefulness period becomes much smaller than its MTBF.

Basic Concepts

ULT vs MTBF

MTBF *vs* Useful Life Time

Consider another example in which 100,000 20-year-old people in the sample. We monitored this sample for one year. During that period, the death rate calculated was 100/ 100,000 = 0.1%/year. Considering TTF exponentially distributed, the MTBF is the inverse of the failure rate, that is 1/0.001 = 1000.

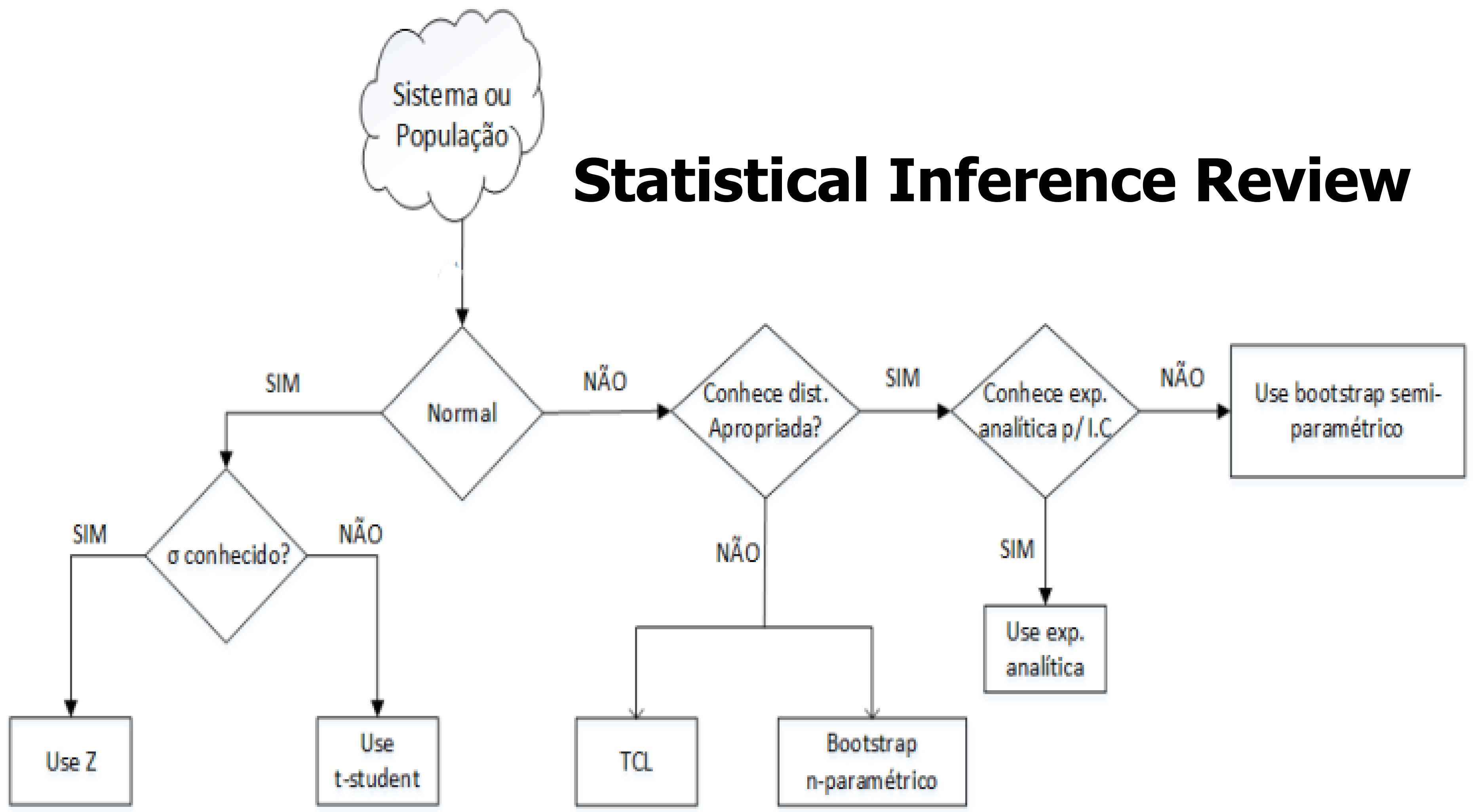
This example shows that high MTBF is different from the life expectancy. As people become older, more deaths occur, so the best way to compute MTBF would be monitor the sample to reach their end of life. After that, the average of these life spans is computed. Then, we reach values of order of 75-80, which would be much more realistic.

A REVIEW ON STATISTICAL INFERENCE

Basic Concepts

Check Performance Evaluation Slides (Exploratory Data Analysis and Statistical Inference)

Statistical Inference Review



Some Important Probability Distributions

Exponential Distribution

- Arises commonly in reliability & queuing theory.
- A non-negative continuous random variable.
- It exhibits memoryless property (continuous counterpart of geometric distribution).
- Related to (discrete) Poisson distribution

Exponential Distribution

- Often used to *model*
  - Interarrival times between two IP packets (or voice calls)
  - Service times at a file (web, compute, database) server
  - Time to failure, time to repair, time to reboot etc.
- The use of exponential distribution is an assumption that needs to be validated with experimental data; if the data does not support the assumption, then other distributions may be used

Exponential Distribution

- For instance, Weibull distribution is often used to model times to failure;
- Lognormal distribution is often used to model repair time distributions
- Markov modulated Poisson process is often used to model arrival of IP packets (which has non-exponentially distributed inter-arrival times)

Mathematica

Exponential Distribution: EXP(λ)

- Mathematically (CDF and pdf are given as):

$$\text{CDF: } F(x) = \begin{cases} 1 - e^{-\lambda x}, & \text{if } 0 \leq x < \infty \\ 0, & \text{otherwise} \end{cases}$$

where λ is a paramter and the base of natural logarithm, $e = 2.7182818284$

$$\text{pdf: } f(x) = \begin{cases} \lambda e^{-\lambda x}, & \text{if } x > 0 \\ 0, & \text{otherwise} \end{cases}$$

- Also

$$P(X > t) = \int_t^{\infty} f(x)dx = e^{-\lambda t}$$

$$P(a < X \leq b) = \int_a^b f(x)dx = F(b) - F(a) = e^{-\lambda a} - e^{-\lambda b}$$

Exponential Distribution: EXP(λ)

$$R(t) = e^{-\lambda t}, \qquad t \geq 0,$$

$$F(t) = 1 - e^{-\lambda t}, \qquad t \geq 0,$$

$$h(t) = \lambda,$$

$$E[T] = MTTF = \frac{1}{\lambda},$$

$$Var[T] = \sigma^2 = \frac{1}{\lambda^2}.$$

Exponential Distribution: EXP(λ)

The memoryless property can be demonstrated with conditional reliability:

$$R(x \mid t) = \Pr(T > x + t \mid T > t) = \frac{\Pr(T > x + t)}{\Pr(T > t)}$$

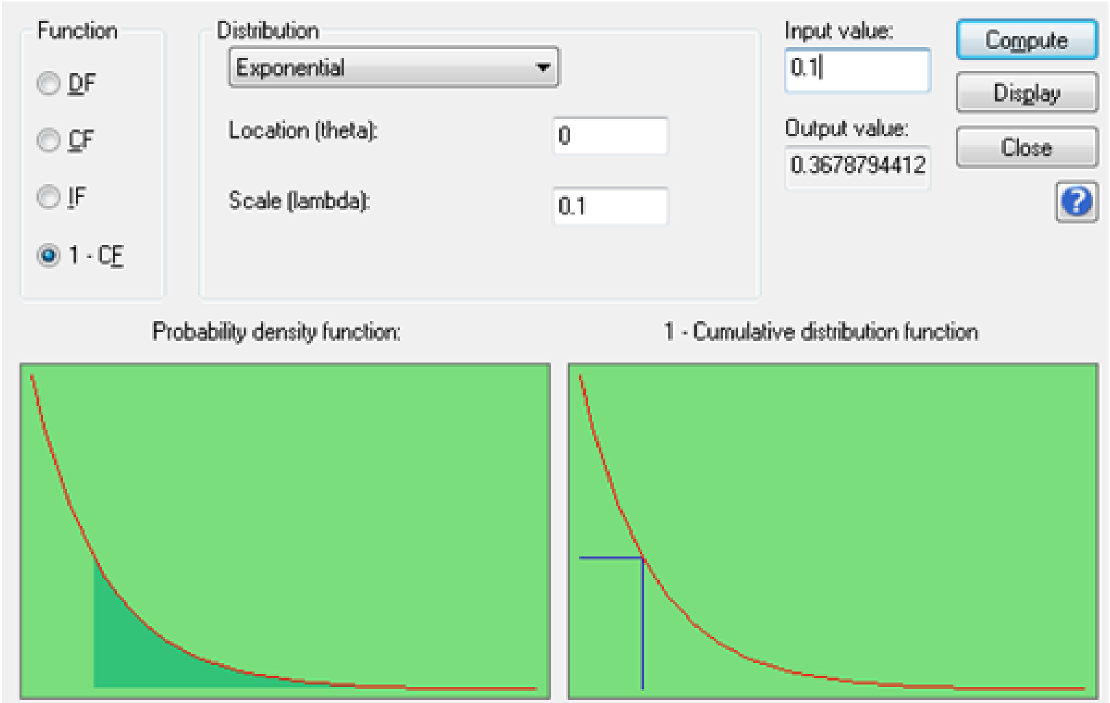
$$= \frac{e^{-\lambda(t+x)}}{e^{-\lambda t}} = e^{-\lambda x} = R(x), \qquad x \geq 0.$$

Exponential Distribution: EXP(λ)

$\text{Exp}(\lambda = 10) \Rightarrow E[X] = 0.1$

R(0.1)=0.367879   R(0.2|0.1)=0.36788

R(0.2)=0.135335

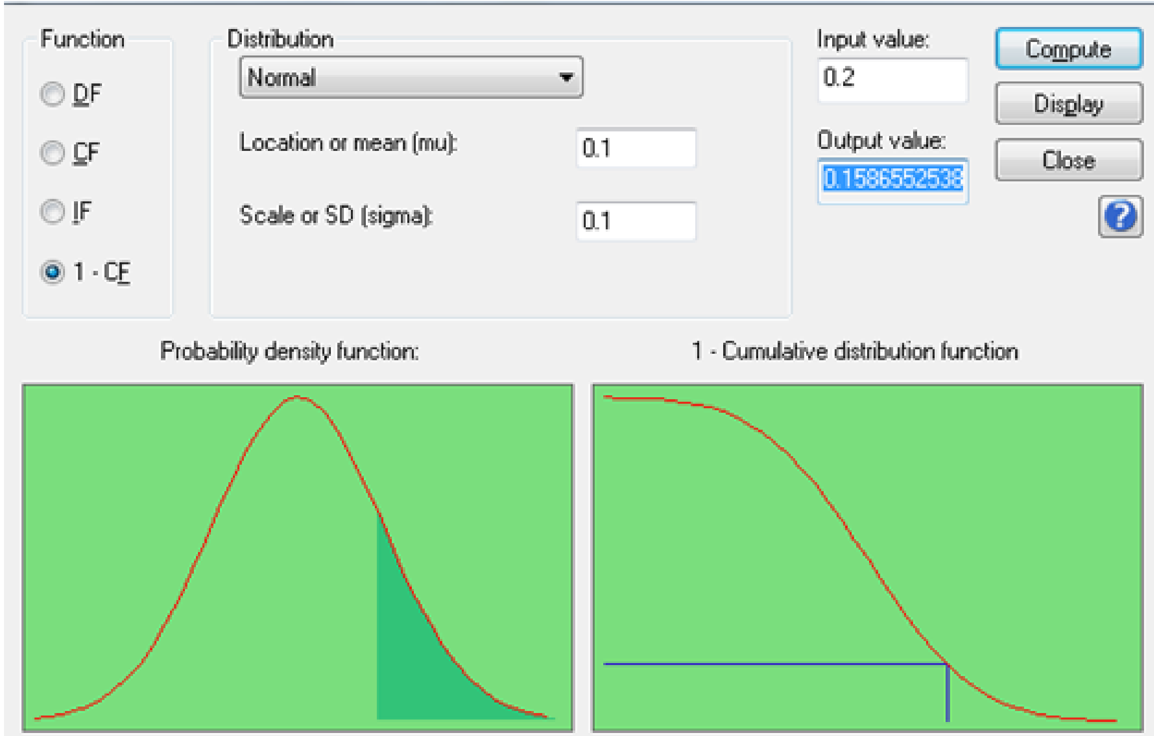


Exponential Distribution: EXP(λ)

$N(\mu = 0.1, \sigma = 0.1)$

R(0.1)=0.5   R(0.2|0.1)=0.317311

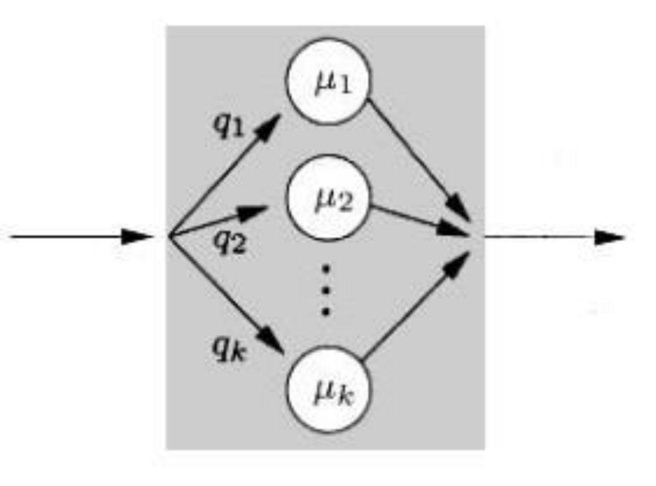
R(0.2)=0.158655



Mathematica

Hyperexponential Distribution

$$F_X(x) = \sum_{j=1}^{k} q_j (1 - \mathrm{e}^{-\mu_j x}), \qquad x \geq 0.$$



pdf: $$f_X(x) = \sum_{j=1} q_j \mu_j \, \mathrm{e}^{-\mu_j x}, \quad x > 0,$$

mean: $$\overline{X} = \sum_{j=1}^{k} \frac{q_j}{\mu_j} = \frac{1}{\mu}, \quad x > 0,$$

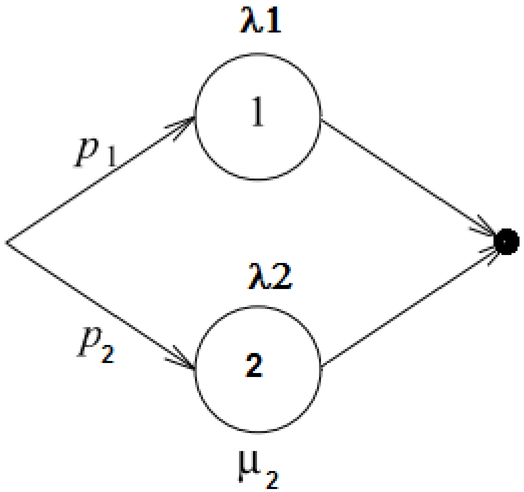
variance: $$\mathrm{var}(X) = 2 \sum_{j=1}^{k} \frac{q_j}{\mu_j^2} - \frac{1}{\mu^2},$$

$$c_X = \sqrt{2\mu^2 \sum_{j=1}^{k} \frac{q_j}{\mu_j^2} - 1} \quad \geq 1$$

Hyperexponential Distribution

In case $c_X \geq 1$, one fits a $H_2(p_1, p_2; \mu_1, \mu_2)$ distribution.

$$F_X(x) = \sum_{i=1}^{2} q_j(1 - e^{-\lambda_j x}), \qquad x \geq 0.$$



$H_2(p_1, p_2; \mu_1, \mu_2)$ is not uniquely determined by its first two moments.

Therefore, the normalization

$$\frac{p_1}{\mu_1} = \frac{p_2}{\mu_2}$$

may be adopted, so that:

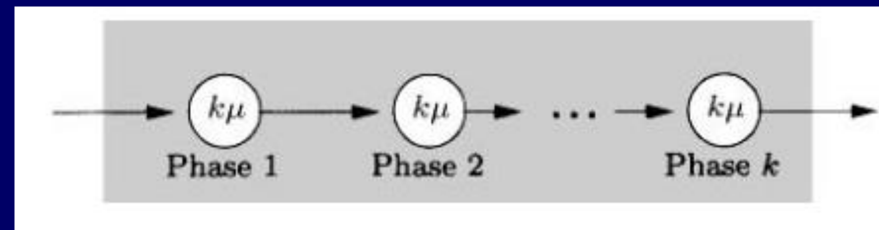
$$p_1 = \frac{1}{2}\left(1 + \sqrt{\frac{c_X^2 - 1}{c_X^2 + 1}}\right), \qquad p_2 = 1 - p_1,$$

$$\mu_1 = \frac{2p_1}{E(X)}, \qquad \mu_2 = \frac{2p_2}{E(X)}.$$

Mathematica

Erlang Distribution

$$F_X(x) = 1 - e^{-k\mu x} \cdot \sum_{j=0}^{k-1} \frac{(k\mu x)^j}{j!}, \quad x \geq 0, \; k = 1, 2 \ldots .$$

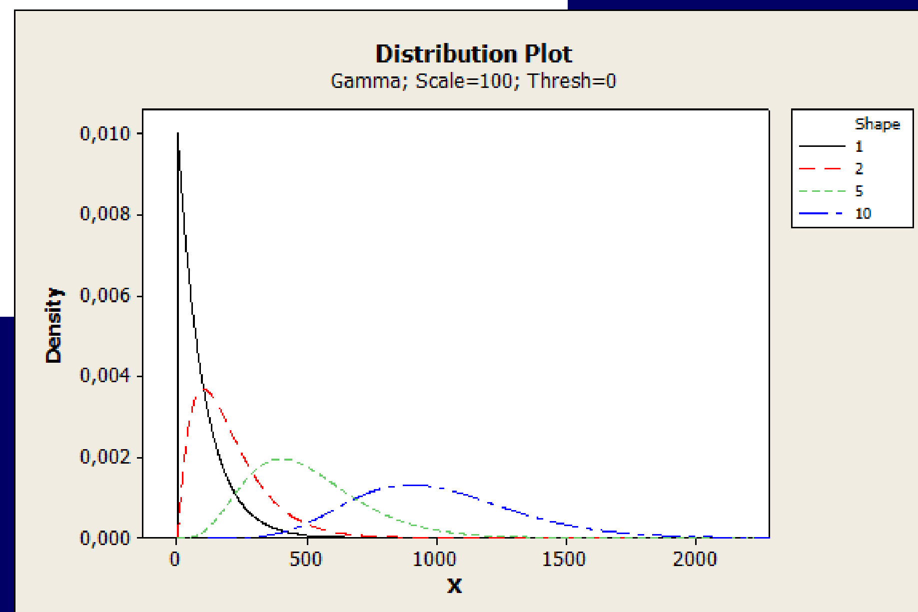


pdf: $f_X(x) = \dfrac{k\mu(k\mu x)^{k-1}}{(k-1)!} e^{-k\mu x}, \; x > 0, \; k = 1, 2, \ldots ,$

mean: $\overline{X} = \dfrac{1}{\mu},$

variance: $\operatorname{var}(X) = \dfrac{1}{k\mu^2},$

coefficient of variation: $c_X = \dfrac{1}{\sqrt{k}} \leq 1 .$



$$k = \left\lceil \frac{1}{c_X^2} \right\rceil$$

$$\mu = \frac{1}{c_X^2 k \overline{X}} .$$

Hypoexponential Distribution

$$\text{pdf:} \quad f_X(x) = \sum_{i=1} a_i \mu_i \, \mathrm{e}^{-\mu_i x}, \quad x > 0,$$

$$\text{with } a_i = \prod_{j=1, j \neq i}^{k} \frac{\mu_j}{\mu_j - \mu_i}, \quad 1 \leq i \leq k,$$

$$\text{mean:} \quad \overline{X} = \sum_{i=1}^{k} \frac{1}{\mu_i},$$

$$\text{coefficient of variation:} \quad c_X = \left(1 + 2 \frac{\sum_{i=1}^{k} \left(\mu_i \sum_{j=i+1}^{k} \mu_j \right)}{\sum_{i=1}^{k} \mu_i^2} \right)^{-\frac{1}{2}}.$$

Weibull Distribution

$$F_X(x) = 1 - \exp(-(\lambda x)^\alpha), \quad x \geq 0$$

$$f_X(x) = \alpha\lambda(\lambda x)^{\alpha-1} \exp(-(\lambda x)^\alpha), \ \lambda > 0,$$

shape parameter α

scale parameter $\lambda > 0$.

$\alpha < 0$ means infant mortality and $\alpha > 0$ means wear out

$$\overline{X} = \frac{1}{\lambda}\Gamma\left(1 + \frac{1}{\alpha}\right),$$

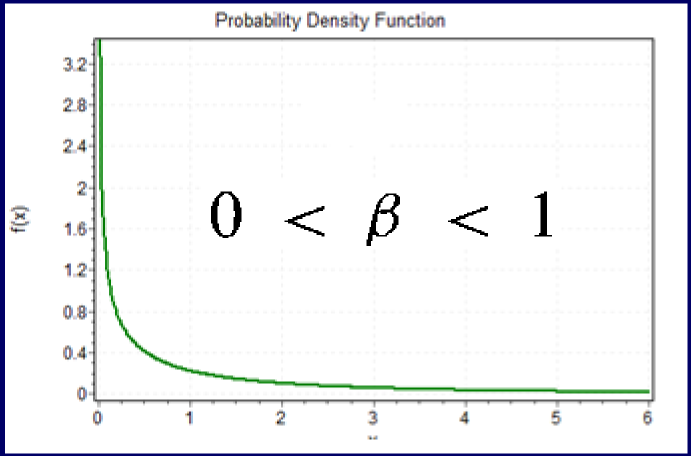
$$c_X^2 = \frac{\Gamma(1 + 2/\alpha)}{\{\Gamma(1 + 1/\alpha)\}^2} - 1$$

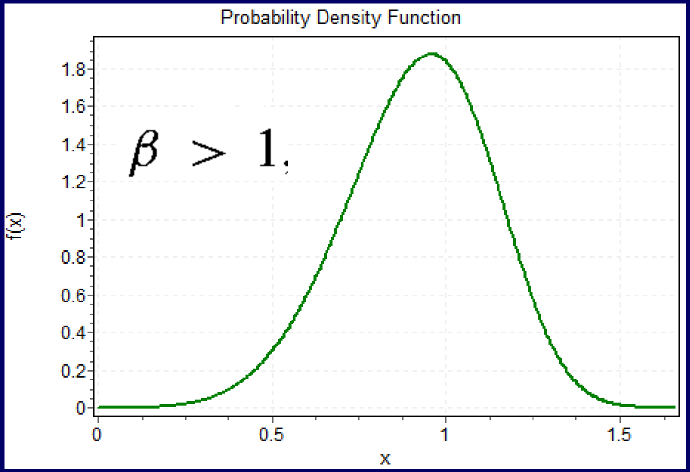
Weibull distribution is often used to model times to failure

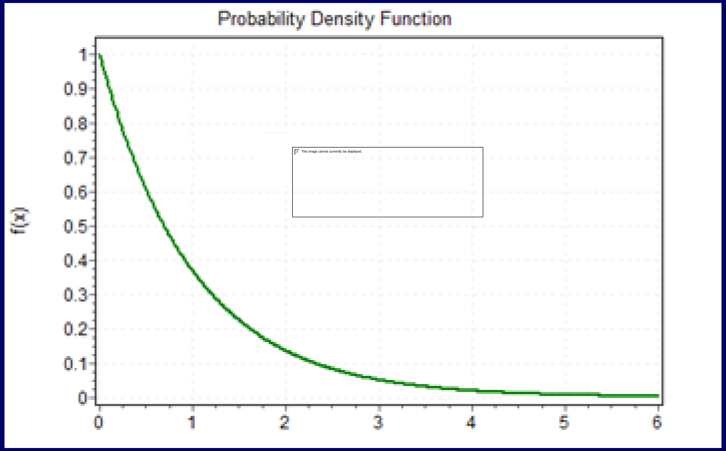
Use o EasyFit e o Probability Plot do Minitab

Mathematica

Weibull Distribution







Use o EasyFit

Lognormal Distribution

$$F_X(x) = \Phi\left(\frac{\ln(x) - \lambda}{\alpha}\right), \quad x > 0$$

$$f_X(x) = \frac{1}{\alpha x \sqrt{2\pi}} \exp(-\{\ln(x) - \lambda\}^2 / 2\alpha^2), \quad x > 0$$

$$\overline{X} = \exp(\lambda + \alpha^2/2)$$

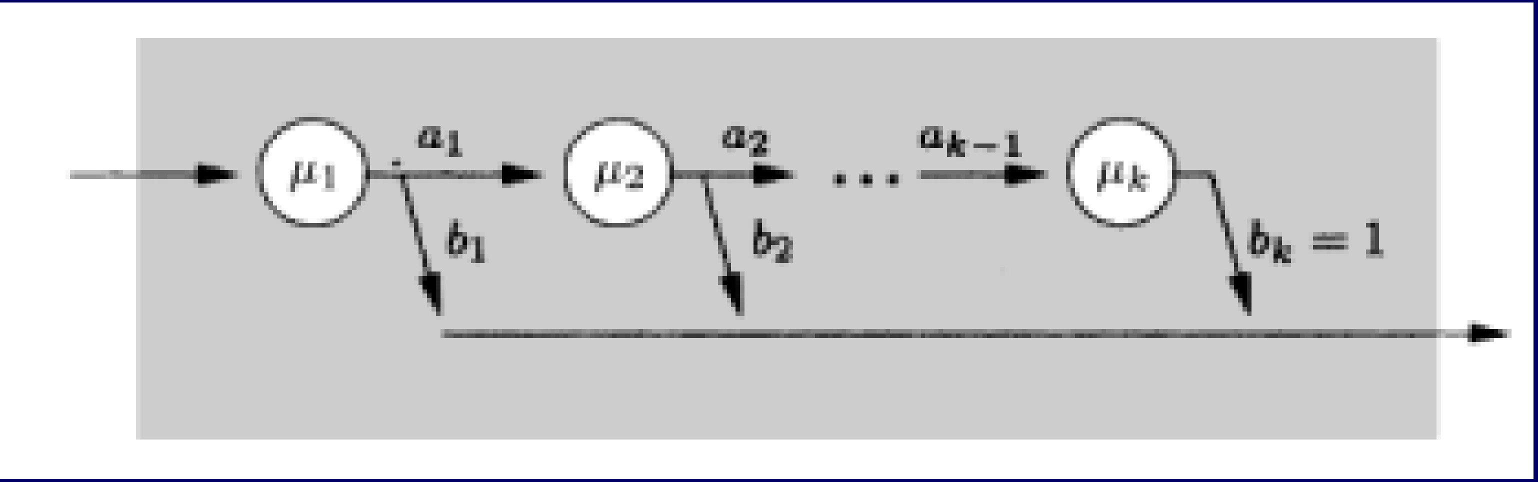
$$c_X^2 = \exp(\alpha^2) - 1$$

$$\alpha = \sqrt{\ln(c_X^2 + 1)}, \qquad \lambda = \ln \overline{X} - \frac{\alpha^2}{2}$$

Lognormal distribution is often used to model repair time distributions

The importance of this distribution arises from the fact that the product of n mutually independent random variables has a lognormal distribution in the limit $n \to \infty$.

Cox Distribution

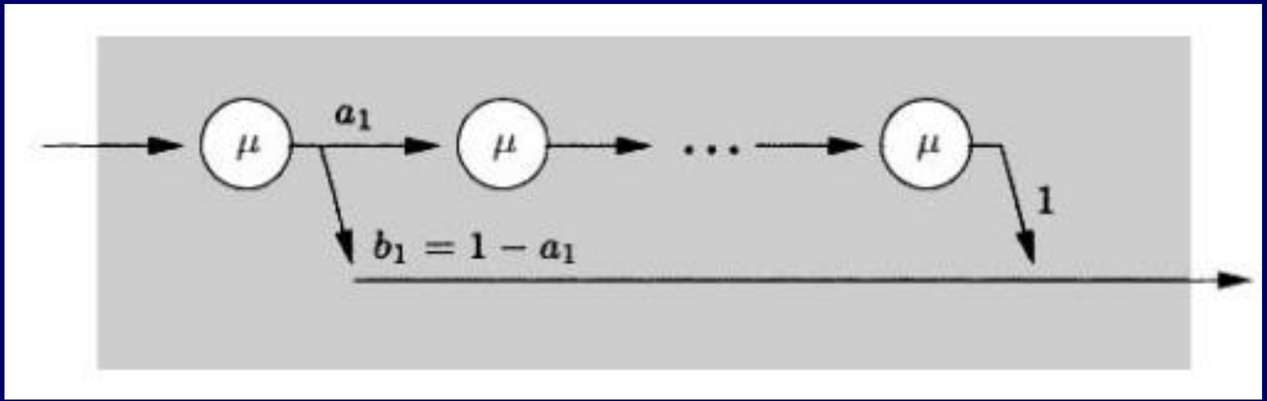


The model consists of k phases in series with exponentially distributed times and rates $\mu_1, \mu_2, \ldots, \mu_k$. After phase j, another phase $j+1$ follows with probability a_j and with probability $b_j = 1 - a_j$ the total time span is completed.

Cox Distribution

Case 1: $c_X \leq 1$

$$\mu_j = \mu \quad j = 1, \ldots, k,$$
$$a_j = 1 \quad j = 2, \ldots, k-1$$



$$\overline{X} = \frac{b_1 + k(1 - b_1)}{\mu},$$

$$\operatorname{var}(X) = \frac{k + b_1(k-1)\left(b_1(1-k) + k - 2\right)}{\mu^2},$$

$$c_X^2 = \frac{k + b_1(k-1)\left(b_1(1-k) + k - 2\right)}{[b_1 + k(1-b_1)]^2}.$$

$$k = \left\lceil \frac{1}{c_X^2} \right\rceil$$

$$b_1 = \frac{2kc_X^2 + (k-2) - \sqrt{k^2 + 4 - 4kc_X^2}}{2(c_X^2 + 1)(k-1)},$$

$$\mu = \frac{k - b_1 \cdot (k-1)}{\overline{X}}.$$

Cox-1

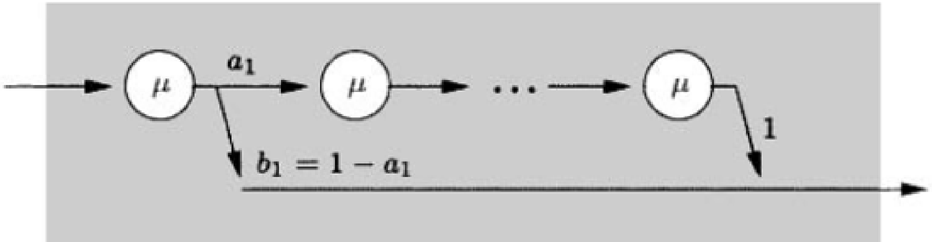
Cox Distribution

Case 1: $c_X \leq 1$

Example

Let us construct a phase-type distribution having expectation $E[X] = 4$ and variance $SD[X] = 2.236068$.

With these parameters, we have $Cov[X]$ =0.559017, which is less than 1. We may choose parameters for a Coxian distribution as represented in



$$k = \left\lceil \frac{1}{Cov[X]^2} \right\rceil = \left\lceil \frac{1}{0.559017^2} \right\rceil = \lceil 3.2 \rceil = 4$$

$$a_1 = \frac{2 \times 4 \times 0.559017^2 + (4-2) - \sqrt{4^2 + 4 - 4 \times 4 \times 0.55}}{2 \times (0.559017^2 + 1) \times (4-1)}$$

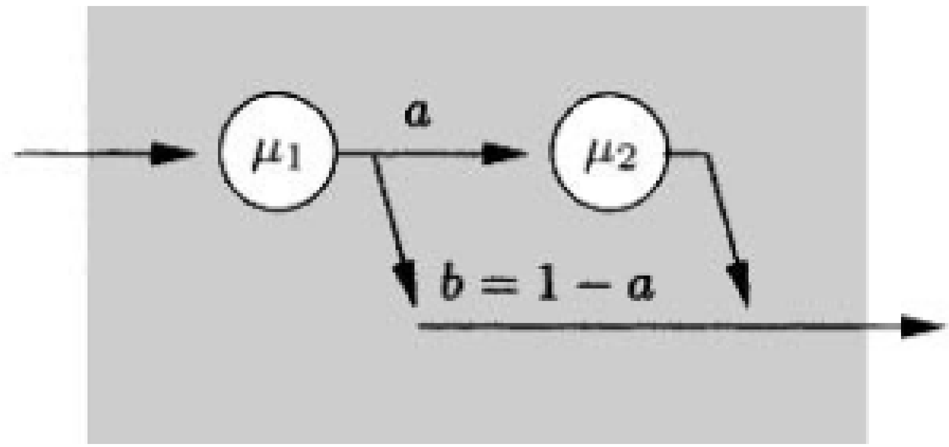
$$a_1 = 0.9203788377837205$$

$$\lambda = \frac{4 - 0.9203788377837205 \times (4-1)}{4}$$

$$\lambda = 0.9402841283377904$$

Cox Distribution

Case 2: $c_X > 1$



$$\overline{X} = \frac{1}{\mu_1} + \frac{a}{\mu_2},$$

$$\operatorname{var}(X) = \frac{\mu_2^2 + a\mu_1^2(2-a)}{\mu_1^2 \cdot \mu_2^2},$$

$$c_X^2 = \frac{\mu_2^2 + a\mu_1^2(2-a)}{(\mu_2 + a\mu_1)^2}.$$

$$\mu_1 = \frac{2}{\overline{X}}$$

$$a = \frac{1}{2c_X^2}$$

$$\mu_2 = \frac{1}{\overline{X}c_X^2}$$

Cox Distribution

Example

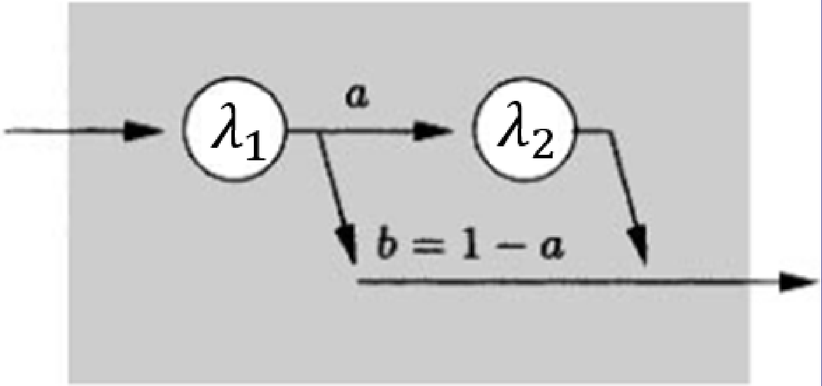
Case 2: $c_X > 1$

A random variable X having expectation $E[X] = 3$ and standard deviation equal to $\sigma_X = 4$ may be modeled as a two-phase Coxian. Given that $E[X] = 3$ and $Cov[X] = 4/3$, we may take the parameters of the Coxian distribution to be:

$$\lambda_1 = \frac{2}{E[X]} = \frac{2}{3}$$

$$\lambda_2 = \frac{2}{E[X] \times Cov[X]^2} = \frac{3}{16}$$

$$a = \frac{1}{2 \times Cov[X]^2} = \frac{9}{32}$$



Reliability Data Analysis

Reliability Data Analysis

The aim is the selection and the specification of suitable reliability (and maintainability) models based on failure (and repair) data.

- Non-parametric approaches
- Parametric approaches

Reliability Data Analysis

The observation of failures (or repairs) times can be represented by:

Failure	1^{st}	2^{nd}	...	n
Time	t_1	t_2		t_n

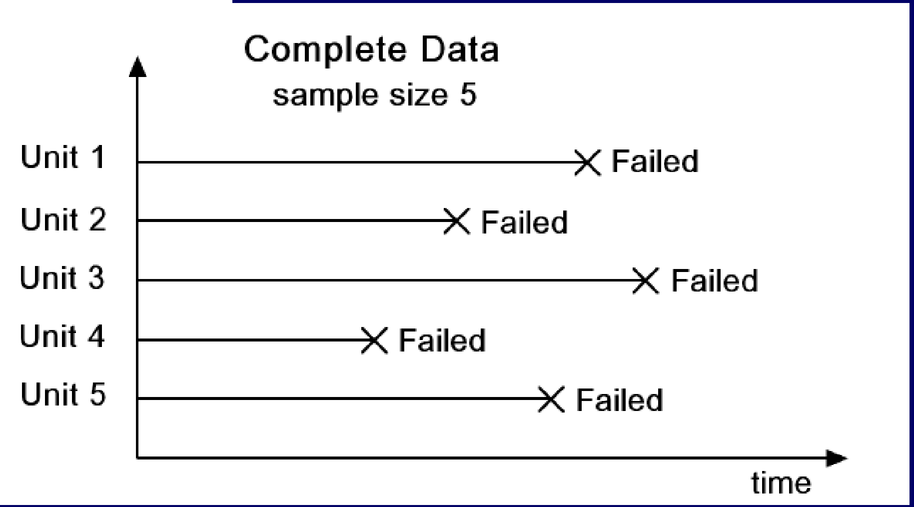
The functions $f_T(t)$, $F_T(t), R(t)$ $(M(t))$ and $h(t)$ and $H(t)$ represent the failure time (repair time) of the population.

Reliability Data Analysis

A taxonomy of data

Failure data may be classified as:

- Operational × Test-generated failures
- Grouped × Ungrouped data
- Large samples × Small samples
- Complete × Censored data



Reliability Data Analysis

A taxonomy of data

Failure data may be classified as:

- Operational × Test-generated failures
- Grouped × Ungrouped data
- Large samples × Small samples
- Complete × Censored data

Failure times are usually either field data or failures observed from reliability testing.

Often failure field data are grouped into time intervals in which the exact failure times are not preserved.

For large sample sizes, grouping data into time intervals may be preferred.

Testing may result in small sample sizes.

Failure data obtained from testing are likely to be more precise and appropriate.

However, field data usually provide larger data samples and reflect the operating environment conditions.

Reliability Data Analysis

A taxonomy of data

Failure data may be classified as:

- Operational × Test-generated failures
- Grouped × Ungrouped data
- Large samples × Small samples
- Complete × Censored data

Censoring occurs when data are incomplete when units are removed from the analysis. The censoring occurs because:

- units may have been removed before their failures or
- because the test finishes before the respective failures occur.

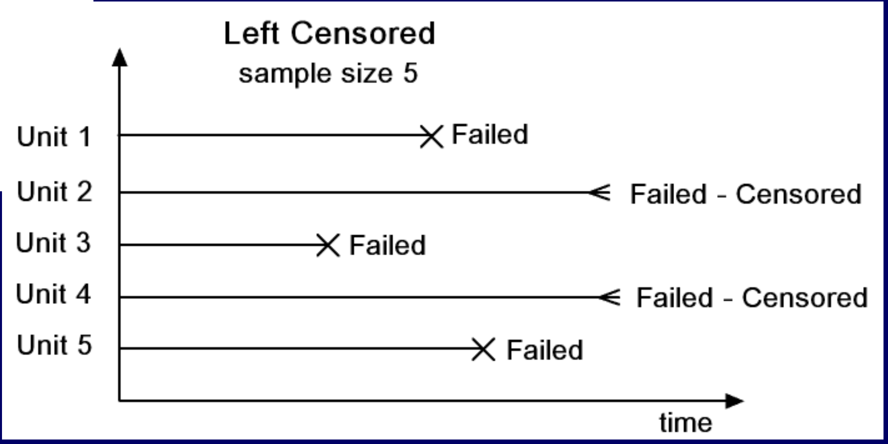
Reliability Data Analysis

- Singly censored data: all units have the same test time.
- Multiply censored data: test time or operating time differ from censored units.
- Left censored: failure time occurs before a specified time.
- Right censored: failure time occurs after a specified time.
  - Type I - right censored: the testing stops at T time units.
  - Type II - right censored: the testing stops when r *out* n failures occur.

A taxonomy of data

Failure data may be classified as:

- Operational × Test-generated failures
- Grouped × Ungrouped data
- Large samples × Small samples
- Complete × Censored data



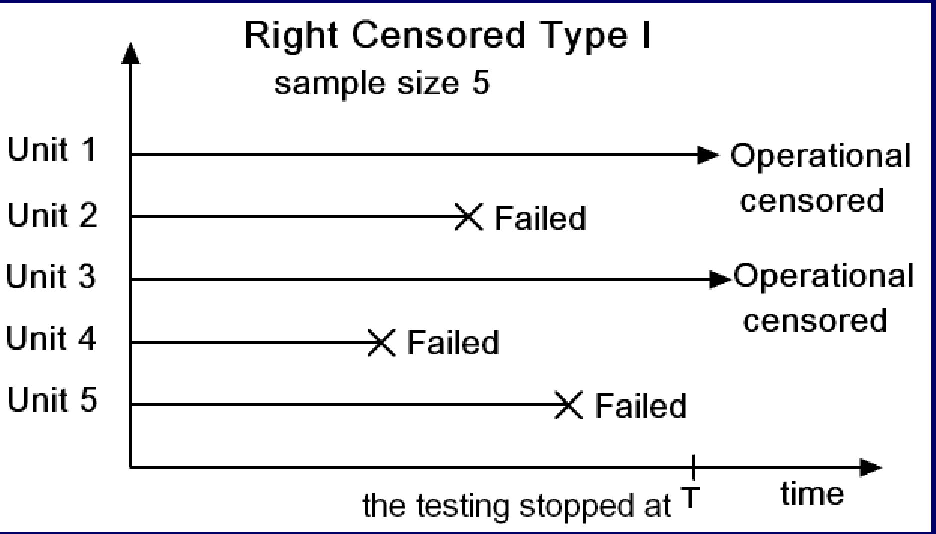
Reliability Data Analysis

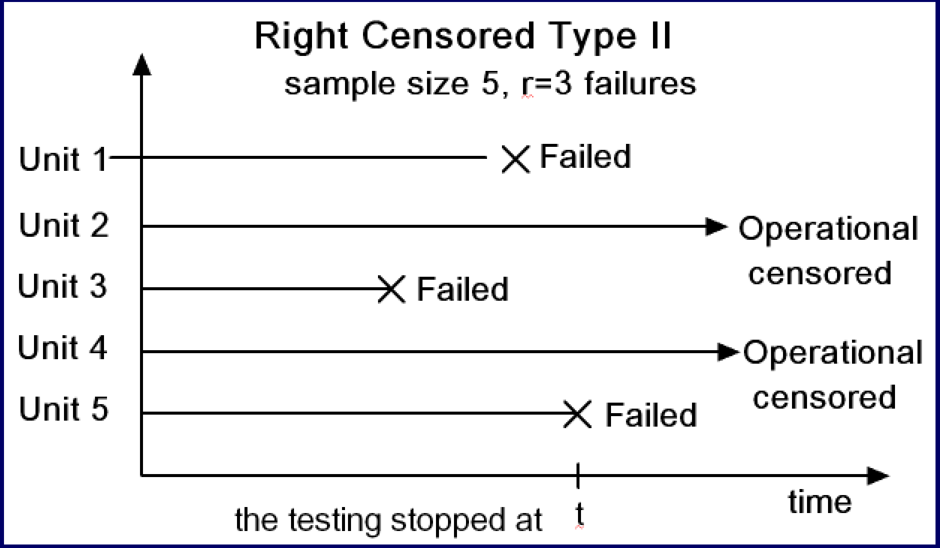
A taxonomy of data

Failure data may be classified as:

- Operational × Test-generated failures
- Grouped × Ungrouped data
- Large samples × Small samples
- Complete × Censored data

- Singly censored data: all units have the same test time.
- Multiply censored data: test time or operating time differ from censored units.
- Left censored: failure time occurs before a specified time.
- Right censored: failure time occurs after a specified time.
  - Type I - right censored: the testing stops at T time units.
  - Type II - right censored: the testing stops when r out n failures occur.





Reliability Data Analysis
Non-parametric approaches

Excel

CI MTTF

Ungrouped Complete Data

Consider $t_1, t_2, \ldots t_n$, where $t_i \le t_{i+1}$ are n ordered failure times.

$$\hat{R}(t_i) = \frac{n-i}{n} = 1 - \frac{i}{n}$$

$$\hat{F}(t_i) = 1 - \hat{R}(t_i) = \frac{i}{n}$$

$$\hat{F}(t_i) = 1 - \hat{R}(t_i) = \frac{i}{n+1}$$

$$\hat{F}(t_i) = 1 - \hat{R}(t_i) = \frac{i-0.3}{n+0.4}$$

$$\hat{f}(t_i) =$$

$$\hat{\lambda}(t_i) = \frac{\hat{f}(t_i}{\hat{R}(t_i}$$

M

Confidence int

bootstrap.

Ungrouped Complete Data	
n =	10
i	Failure times
0	0
1	15.4
2	18.9
3	20.1
4	24.5
5	29.3
6	33.9
7	48.2
8	54.7
9	72
10	86.1

Reliability Data Analysis
Non-parametric approaches

Excel

CI MTTF

Grouped Complete Data

Failures that have occurred into time intervals, their original values are lost.

Consider k time intervals where $t_1, t_2, \ldots t_k$ are the time instants representing the ends of each time interval, such that $t_i \leq t_{i+1}$.

Let $n_1, n_2, \ldots, n_k$ be the number of units that survived at respective ordered time $t_1, t_2, \ldots t_k$, and n the number of units at risk at the beginning of the test.

$$\hat{R}(t_i) = \frac{n_i}{n}, \quad i = 1,2 \ldots, k$$

$$\hat{F}(t_i) = 1 - \hat{R}(t_i)$$

$$\hat{f}(t_i) = -\frac{\hat{R}(t_i + 1) - \hat{R}(t_i)}{t_{i+1} - t_i}$$

$$= \frac{n_i - n_{i+1}}{(t_{i+1} - t_i) \times n}$$

$$\hat{\lambda}(t_i) = \frac{\hat{f}(t_i)}{\hat{R}(t_i)} = \frac{n_i - n_{i+1}}{(t_{i+1} - t_i) \times n_i}$$

$$t_i < t < t_{i+1}$$

Reliability Data Analysis
Non-parametric approaches

Excel

CI MTTF

The $MTTF$ is estimated considering the midpoint of each interval and fraction of units that have failed in each interval.

$$\bar{t_i} = \frac{t_i + t_{i+1}}{2}$$

$$\widehat{MTTF} = \sum_{i=0}^{k-1} \bar{t_i} \frac{n_i - n_{i+1}}{n}$$

$$t_0 = 0, n_0 = n$$

Confidence interval for the $MTTF$: adopt bootstrap.

Time Interval	Number failing	Number surviving
0	0	70
5	3	67
10	7	60
15	8	52
20	9	43
25	13	30
30	18	12
35	12	0

Reliability Data Analysis
Non-parametric approaches

Excel

Ungrouped Censored Data

For singly censored on the right, $R(t), f(t)$, and $\lambda(t)$ may be iteratively estimated from the equation adopted for **Ungrouped Complete Data.**

We know that:

$$\hat{F}(t_i) = 1 - \hat{R}(t_i) = \frac{i}{n+1}$$

So: $$\hat{R}(t_i) = 1 - \frac{i}{n+1} = \frac{n+1-i}{n+1}$$

Therefore:

$$\hat{R}(t_{i-1}) = \frac{n+1-(i-1)}{n+1} = \frac{n+2-i}{n+1}$$

Now, consider:

$\hat{R}(t_i) = \hat{R}(t_{i-1}) \times$

$P(Unit\ will\ not\ fail\ between\ t_i$

$and\ t_{i-1}, given\ it\ has$

$survived\ t_{i-1})$

Reliability Data Analysis
Non-parametric approaches

Excel

Hence:

n =	10		
i	Failure times	δ	R(t)
0	0		1
1	150	1	0.909091
2	340	0	0.909091
3	560	1	0.808081
4	800	1	0.707071
5	1130	0	0.707071
6	1720	1	0.589226
7	2470	0	0.589226
8	4210	0	0.589226
9	5230	1	0.392817
10	6890	1	0.196409

Two events may occur at t_i (since t_i is there, otherwise it is not there): a failure or a censoring. So:

$$\delta_i = \begin{cases} 1 & if\ \ failure\ occurs\ at\ t_i \\ 0 & if\ censoring\ occurs\ at\ t_i \end{cases}$$

Then:

$$\hat{R}(t_i) = \left(\frac{n+1-i}{n+2-i}\right)^{\delta_i} \times \hat{R}(t_{i-1})$$

$$\hat{F}_T(t_i) = 1 - \hat{R}(t_i)$$

$$\hat{F}(t_i) = \left(\frac{i}{i-1}\right)^{\delta} \times \hat{F}(t_{i-1})$$

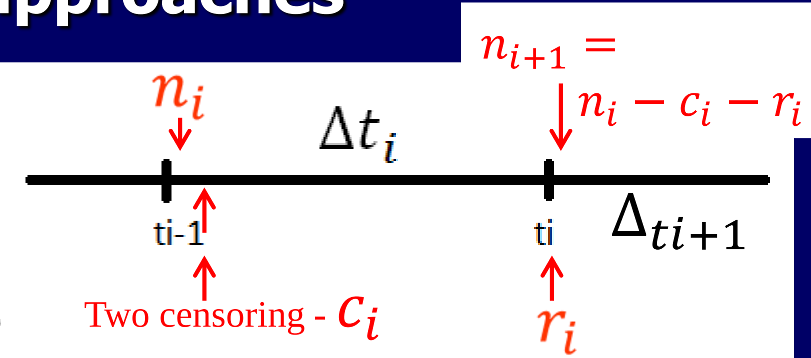
$$\hat{f}(t_i) = \frac{1}{(n+1) \times (t_i - t_{i-1})}$$

$$\hat{\lambda}(t_i) = \frac{1}{(n+1-i) \times (t_i - t_{i-1})}$$

Reliability Data Analysis
Non-parametric approaches

Kaplan-Meier method

for grouped censored data



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

So

$$P(A \cap B) = P(A|B) \times P(B)$$

If A and B are independent, then:

$P(A|B) = P(A)$, so:

$$P(A \cap B) = P(A) \times P(B)$$

Therefore

$$\hat{R}(t_i) = \hat{R}(t_{i-1}) \times \hat{R}(\Delta t_i)$$

where $t_i = t_{i-1} + \Delta t_i$

If at t_i we have r_i failures, then:

$$\hat{R}(\Delta t_i) = 1 - \frac{r_i}{n_i}$$

where n_i is the number of available units at the instant $t_i - \Delta t_i$ without considering the censoring, that is, shortly after t_{i-1}. You should bear in mind that the interval $(t_i - \Delta t_i, t_i]$ is open at the left hand side.

The probability of a subject surviving to any point in time **T** = (**t** + **Δt**) is the product of the cumulative survival probability up to time **t** and the probability of surviving interval **Δt**.

Reliability Data Analysis
Non-parametric approaches

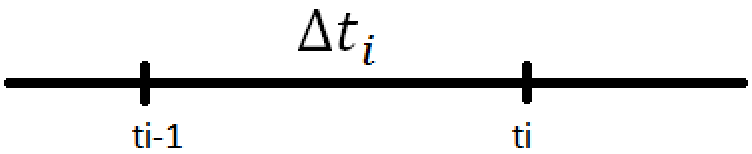
Excel

Mathematica

Kaplan-Meier method

for grouped censored data

For the sake of calculating n_i, it is assumed that censoring occurs shortly after the failures at t_{i-1}.



Therefore: $$\hat{R}(t_2) = \hat{R}(t_1) \times \hat{R}(\Delta t_2)$$

$$\hat{R}(t_2) = \left(1 - \frac{r_1}{n_1}\right) \times \left(1 - \frac{r_2}{n_2}\right)$$

Generalizing:

$$R(t) = \prod_{t \le t_i} \left(1 - \frac{r_i}{n_i}\right)$$

$$i \in (1, m), i \in \mathbb{Z}$$

Reliability Data Analysis
Non-parametric approaches

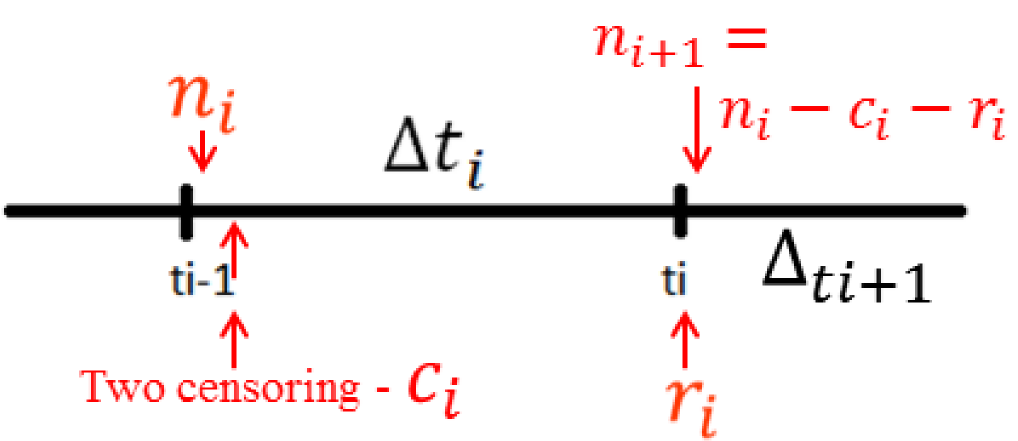
Excel

Mathematica

Kaplan-Meier method summary

Kaplan-Meier method

for grouped censored data



$$\hat{R}(t) = \prod_{t \le t_i} \left(1 - \frac{r_i}{n_i}\right)$$

$$i \in (1, m), i \in \mathbb{Z}$$

$$n_{i+1} = n_i - c_i - r_i$$

Reliability Data Analysis
Non-parametric approaches

Excel

Mathematica

Kaplan-Meier method for grouped censored data

i	TTF or TTS (ti)	ri	ci	ni+1
0		0	0	21
1	9	3	1	17
2	11	1		16
3	13	1	2	13
4	15		1	12
5	17	1		11
6	19			11
7	21			11
8	23	1	1	9
9	25			9
10	27	1	1	7
11	29	1		6
12	31	1		5
13	33		1	4
14	35		2	2
15	37	1		1
16	39		1	0

Reliability Data Analysis
Non-parametric approaches

Excel

Mathematica

Kaplan-Meier method for grouped censored data

i	TTF or TTS (ti)	ri	ci	ni+1	ti - ti-1	1-ri/ni	R(ti)=(1-ri/ni)x (1-ri-1/ni-1)
0		0	0	21		1.000000000	1.000000000
1	9	3	1	17	9	0.857142857	0.857142857
2	11	1		16	2	0.941176471	0.806722689
3	13	1	2	13	2	0.937500000	0.756302521
4	15		1	12	2	1.000000000	0.756302521
5	17	1		11	2	0.916666667	0.693277311
6	19			11	2	1.000000000	0.693277311
7	21			11	2	1.000000000	0.693277311
8	23	1	1	9	2	0.909090909	0.630252101
9	25			9	2	1.000000000	0.630252101
10	27	1	1	7	2	0.888888889	0.560224090
11	29	1		6	2	0.857142857	0.480192077
12	31	1		5	2	0.833333333	0.400160064
13	33		1	4	2	1.000000000	0.400160064
14	35		2	2	2	1.000000000	0.400160064
15	37	1		1	2	0.500000000	0.200080032
16	39		1	0	2	1.000000000	0.200080032
	Total	11	10				
	MTTF						
	19.54545455						

Reliability Data Analysis
Non-parametric approaches

Excel

Kaplan-Meier method
for grouped complete data

i	TTF or TTS (ti)	ri	ci	ni	ti - ti-1	1-ri/ni	(1-ri/ni)x (1-ri-1
0	0	0		70		1.000000000	1.000000000
1	5	3		67	5	0.957142857	0.957142857
2	10	7		60	5	0.895522388	0.857142857
3	15	8		52	5	0.866666667	0.742857143
4	20	9		43	5	0.826923077	0.614285714
5	25	13		30	5	0.697674419	0.428571429
6	30	18		12	5	0.400000000	0.171428571
7	35	12		0	5	0.000000000	0.000000000
	Total	70	0				
	MTTF						
	25.64285714						

Reliability Data Analysis
Non-parametric approaches

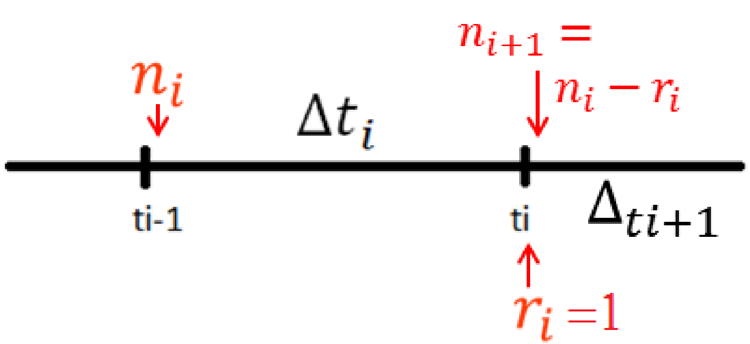
Excel

Kaplan-Meier method summary

Kaplan-Meier method
for ungrouped complete data

As the data set is complete (no censoring), then $c_i = 0, \forall \Delta t_i$.

And since the data set is ungrouped (exact time to failure) $r_i = 1, \forall \Delta t_i$.



Hence:

$$n_{i+1} = n_i - 1$$

Therefore:

$$\hat{R}(t) = \prod_{t \leq t_i} \left(1 - \frac{1}{n_i}\right)$$

$$i \in (1, m), i \in \mathbb{Z}$$

Reliability Data Analysis
Non-parametric approaches

Excel

Kaplan-Meier method for ungrouped complete data

i	TTF or TTS (ti)	ri	ci	ni	ti - ti-1	1-ri/ni	R(ti)=(1-ri/ni)x (1-ri-1/ni-1)
0		0	0	10		1.000000000	1.000000000
1	15.4	1	0	9	15.4	0.900000000	0.900000000
2	18.9	1		8	3.5	0.888888889	0.800000000
3	20.1	1	0	7	1.2	0.875000000	0.700000000
4	24.5	1	0	6	4.4	0.857142857	0.600000000
5	29.3	1	0	5	4.8	0.833333333	0.500000000
6	33.9	1		4	4.6	0.800000000	0.400000000
7	48.2	1		3	14.3	0.750000000	0.300000000
8	54.7	1	0	2	6.5	0.666666667	0.200000000
9	72	1	0	1	17.3	0.500000000	0.100000000
10	86.1	1		0	14.1	0.000000000	0.000000000
	Total	10	0				
	MTTF						
	40.31						

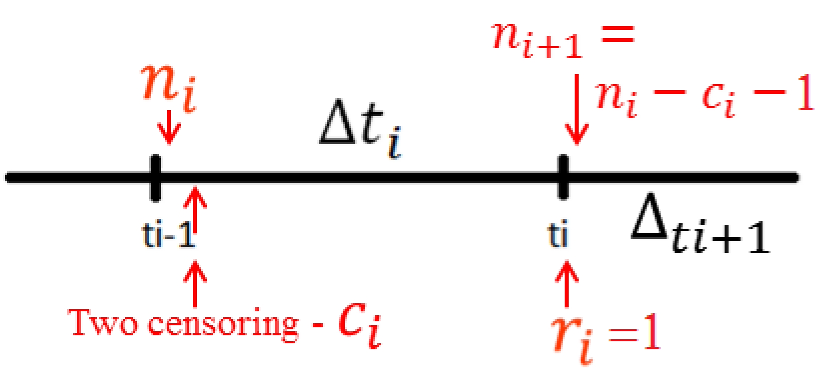
Reliability Data Analysis
Non-parametric approaches

Excel

Kaplan-Meier method summary

Kaplan-Meier method

for ungrouped censored data



Since the data set is ungrouped (exact time to failure) $r_i = 1, \forall \Delta t_i$.

Hence:

$$n_{i+1} = n_i - c_i - 1$$

Therefore:

$$R(t) = \prod_{t \le t_i} \left(1 - \frac{1}{n_i}\right)$$

$$i \in (1, m), i \in \mathbb{Z}$$

Reliability Data Analysis
Non-parametric approaches

Excel

Kaplan-Meier method
for ungrouped censored data

i	TTF or TTS (ti)	ri	ci	ni	ti - ti-1	1-ri/ni	R(ti)=(1-ri/ni)x (1-ri-1/ni-1)	FT(ti)
0				10		1.000000000	1.000000000	0.000000000
1	150	1		9	150	0.900000000	0.900000000	0.100000000
2	340		1	8	190	1.000000000	0.900000000	0.100000000
3	560	1		7	220	0.875000000	0.787500000	0.212500000
4	800	1		6	240	0.857142857	0.675000000	0.325000000
5	1130		1	5	330	1.000000000	0.675000000	0.325000000
6	1720	1		4	590	0.800000000	0.540000000	0.460000000
7	2470		1	3	750	1.000000000	0.540000000	0.460000000
8	4210		1	2	1740	1.000000000	0.540000000	0.460000000
9	5230	1		1	1020	0.500000000	0.270000000	0.730000000
10	6890	1		0	1660	0.000000000	0.000000000	1.000000000
	Total	6	4					
	MTTF							
	2558.333333							

Reliability Data Analysis
Non-parametric approaches

- Other methods:
  - Actuarial method
  - Rank method
  - …

Reliability Data Analysis
Parametric approaches

General process:

- Identifying a theoretical distribution
  - Build graphs and compute statistics, analyze the empirical failure rate, and consider the properties of theoretical distributions
- Estimating the distribution parameters
  - Point estimation
    - Graphical methods
    - Least square method
    - Method of moments
    - Maximum Likelihood Estimation method
  - Confidence interval
- Performing the goodness-of-fit test
  - KS, AD, χ^2...

Reliability Data Analysis
Parametric approaches

Mathematica

Point estimation

Graphical method

A distribution is be transformed into a standard distribution by means of linear transformation. On the graph paper with y axis so calibrated, x and y are linearly related with positive slope, where y represents a cdf F(x) with some scale and location parameters.

Method of Least Squares

The method of least squares fits a curve (or straight line) to a series of data points, by minimizing the sum of squared deviations of the fitted curve and the actual data points.

Method of Matching Moments

The theoretical moments of the distribution are equated with the sample moments.

Method of Maximum Likelihood

The core of this method is selecting as estimate of the distribution parameter a value for which the observed sample is most "likely" to occur.

Reliability Data Analysis
Parametric approaches

Excel

Mathematica

Graphical Methods

i	ti	F(ti)=(i-0.3)/(n+0.4)	Normal(Mean,SD)	Exp(1/Mean)
1	33.644904	0.023026316	0.041458762	0.278184055
2	37.260691	0.055921053	0.050101039	0.303033838
3	46.976141	0.088815789	0.080501834	0.365648018
4	52.532153	0.121710526	0.103256356	0.398893672
5	68.199177	0.154605263	0.191415776	0.483552201
6	74.143111	0.1875	0.234370113	0.512454557
7	75.609671	0.220394737	0.245734482	0.519333339
8	77.992866	0.253289474	0.264815321	0.530305129
9	84.106853	0.286184211	0.316976454	0.557320992
10	85.319391	0.319078947	0.327818003	0.562491275
11	85.616182	0.351973684	0.330494386	0.563747569
12	86.157104	0.384868421	0.335394568	0.566027981
13	89.882303	0.417763158	0.369865514	0.581412209
14	90.282231	0.450657895	0.373635131	0.583031053
15	93.999074	0.483552632	0.409203849	0.597779962
16	98.763826	0.516447368	0.455877347	0.615926604
17	103.34724	0.549342105	0.50136525	0.632609593
18	108.64749	0.582236842	0.553906792	0.651000325
19	112.00697	0.615131579	0.58678315	0.66217736
20	114.62887	0.648026316	0.612037041	0.670651178
21	115.22631	0.680921053	0.617729916	0.672552122
22	118.77664	0.713815789	0.650999795	0.683624529
23	123.39757	0.746710526	0.692589569	0.697476911
24	134.87269	0.779605263	0.785013214	0.729309712
25	139.79835	0.8125	0.819119786	0.741924904
26	141.49929	0.845394737	0.830062916	0.746143219
27	156.02533	0.878289474	0.905996055	0.779471351
28	177.01419	0.911184211	0.967091734	0.820052212
29	183.85396	0.944078947	0.977792953	0.831590865
30	186.71777	0.976973684	0.981308025	0.83619956

1. Obtain data ($\{t_i\}$sample size – $n = |\{t_i\}|$)
2. Sort the data $\{t_i\}$ in ascending order.
3. Compute $FE(t_i) = \dfrac{i-0.3}{n+0.4} \quad \forall\, t_i$ (FE- Empirical distribution)
4. Obtain $FT(t_i)\ \forall\, t_i$ (FT- Theoretical distribution)
5. Create a paper plot:
   - 5.1. Divide the range distance over the x-axis considering the values $FE(t_i)\ \forall\, t_i$.
   - 5.2. Divide the range distance over the y-axis, considering the values $FT(t_i)\ \forall\, t_i$.
6. Plot each point $(FE(t_i), FT(t_i))$ in in the paper.
7. If FT fits the data set $\{t_i\}$, the points should imply a straight line.

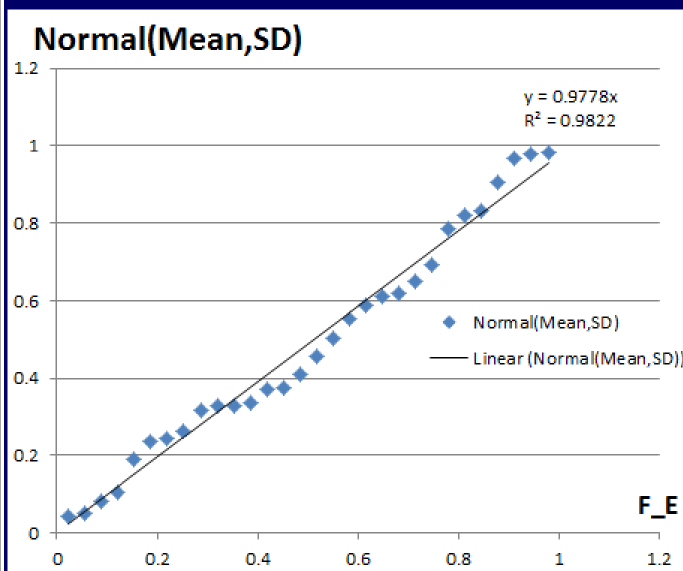
Excel

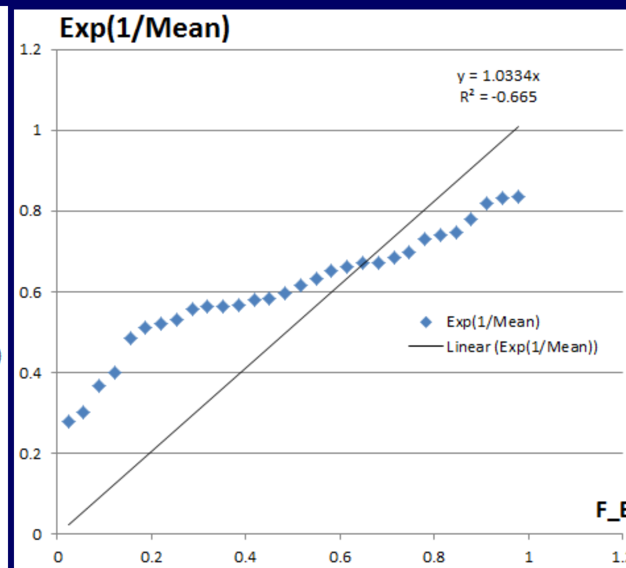
Mathematica

Reliability Data Analysis
Parametric approaches

Graphical Methods

i	ti	F(ti)=(i-0.3)/(n+0.4)	Normal(Mean,SD)	Exp(1/Mean)
1	33.644904	0.023026316	0.041458762	0.278184055
2	37.260691	0.055921053	0.050101039	0.303033838
3	46.976141	0.088815789	0.080501834	0.365648018
4	52.532153	0.121710526	0.103256356	0.398893672
5	68.199177	0.154605263	0.191415776	0.483552201
6	74.143111	0.1875	0.234370113	0.512454557
7	75.609671	0.220394737	0.245734482	0.519333339
8	77.992866	0.253289474	0.264815321	0.530305129
9	84.106853	0.286184211	0.316976454	0.557320992
10	85.319391	0.319078947	0.327818003	0.562491275
11	85.616182	0.351973684	0.330494386	0.563747569
12	86.157104	0.384868421	0.335394568	0.566027981
13	89.882303	0.417763158	0.369865514	0.581412209
14	90.282231	0.450657895	0.373635131	0.583031053
15	93.999074	0.483552632	0.409203849	0.597779962
16	98.763826	0.516447368	0.455877347	0.615926604
17	103.34724	0.549342105	0.50136525	0.632609593
18	108.64749	0.582236842	0.553906792	0.651000325
19	112.00697	0.615131579	0.58678315	0.66217736
20	114.62887	0.648026316	0.612037041	0.670651178
21	115.22631	0.680921053	0.617729916	0.672552122
22	118.77664	0.713815789	0.650999795	0.683624529
23	123.39757	0.746710526	0.692589569	0.697476911
24	134.87269	0.779605263	0.785013214	0.729309712
25	139.79835	0.8125	0.819119786	0.741924904
26	141.49929	0.845394737	0.830062916	0.746143219
27	156.02533	0.878289474	0.905996055	0.779471351
28	177.01419	0.911184211	0.967091734	0.820052212
29	183.85396	0.944078947	0.977792953	0.831590865
30	186.71777	0.976973684	0.981308025	0.83619956

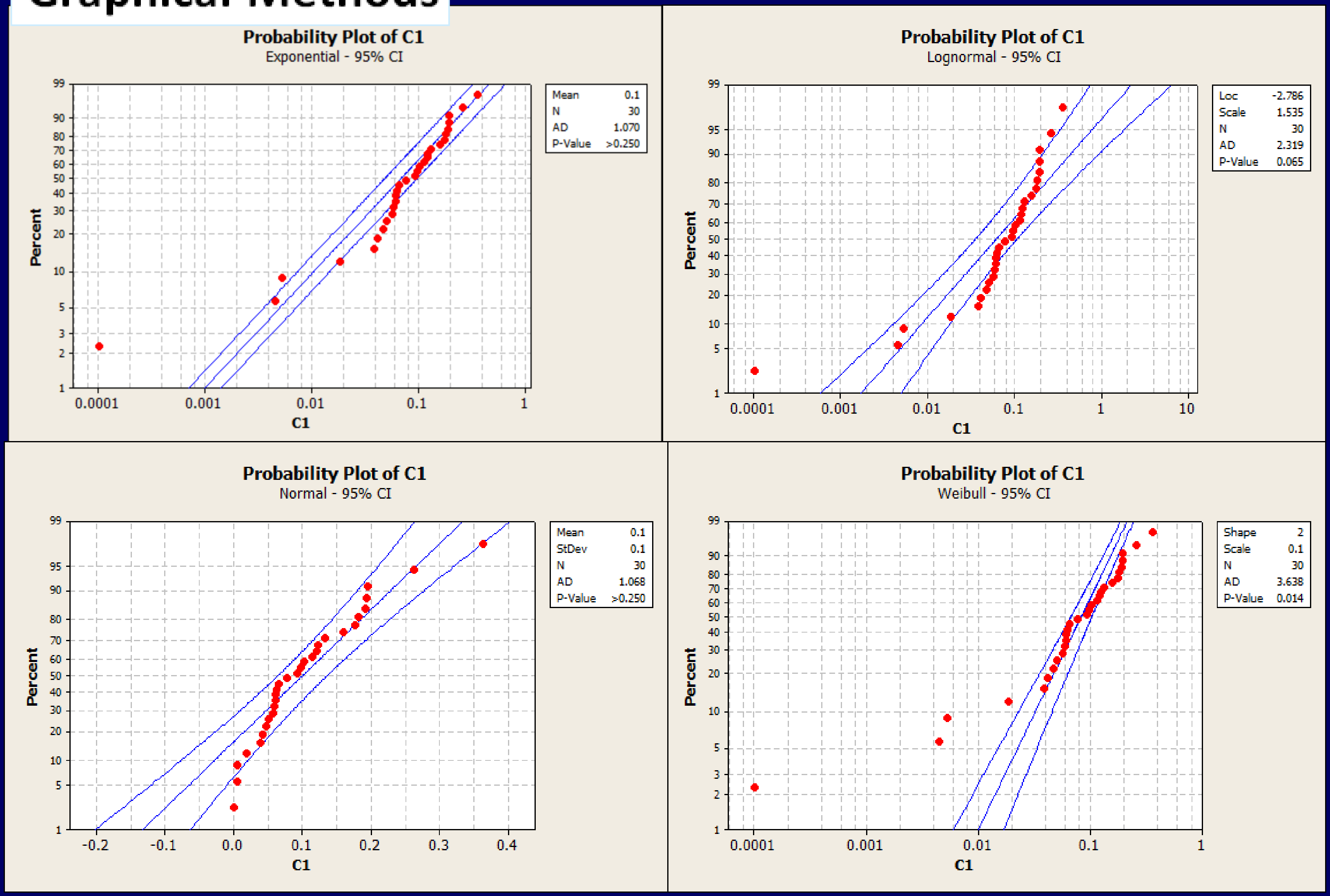




Reliability Data Analysis
Parametric approaches

Mathematica

Graphical Methods



Reliability Data Analysis
Parametric approaches

Mathematica

Method of Matching Moments

THE METHOD OF MOMENTS PROCEDURE

Suppose there are l parameters to be estimated, say $\theta = (\theta_1, \ldots, \theta_l)$.

1. Find l population moments, $\mu'_k, k = 1, 2, \ldots, l$. μ'_k will contain one or more parameters $\theta_1, \ldots, \theta_l$.
2. Find the corresponding l sample moments, $m'_k, k = 1, 2, \ldots, l$. The number of sample moments should equal the number of parameters to be estimated.
3. From the system of equations, $\mu'_k = m'_k, k = 1, 2, \ldots, l$, solve for the parameter $\theta = (\theta_1, \ldots, \theta_l)$; this will be a moment estimator of $\hat{\theta}$.

Reliability Data Analysis
Parametric approaches

Mathematica

Minitab

Method of Matching Moments

Let $X_1, \ldots, X_n$ be a random sample from a Bernoulli population with parameter p.

Find the moment estimator for p.

Tossing a coin 100 times and equating heads to value 1 and tails to value 0, we obtained the following values:

```
{0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0,
 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1,
 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0,
 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1,
 0, 0, 0, 0}
```

Obtain a moment estimate for p, the probability of success (head).

For the Bernoulli random variable, $\mu'_k = E[X] = p$, so we can use m'_1 to estimate p. Thus,

$$m'_1 = \hat{p} = \frac{1}{n}\sum_{i=1}^{n} X_i.$$

Let

$$Y = \sum_{i=1}^{n} X_i.$$

Then, the method of moments estimator for p is $\hat{p} = Y/n$. That is, the ratio of the total number of heads to the total number of tosses will be an estimate of the probability of success.

Note that this experiment results in Bernoulli random variables. Thus, using part (a) with $Y = 33$, we get the moment estimate of p is $\hat{p} = \frac{33}{100} = 0.333\ldots$

Mathematica

Excel

Reliability Data Analysis
Parametric approaches

Method of Matching Moments

Let the distribution of X be $N(\mu, \sigma^2)$.

(a) For a given sample of size n, use the method of moments to estimate μ and σ^2.

(b) The following data (rounded to the third decimal digit) were generated using Minitab from a normal distribution with mean 2 and a standard deviation of 1.5.

```
{1.35902, 3.14884, 0.965424, 2.18839, 2.876, 3.5369, 1.52715, -0.0196308, 1.8647,
 -0.354723, 3.49483, 0.330451, 3.47908, 5.01668, 1.1625, 0.625021, 1.99088,
 2.72912, 3.46589, 1.24573, 1.73628, -0.345712, 3.55427, 4.37219, 1.09182,
 4.28345, -0.378624, 2.63557, 2.10456, 2.36662, 3.01285, 2.74881, 2.85877,
 1.74839, 1.58864, 0.86862, 5.38307, 0.94671, 1.49921, 1.15941, 0.87684, -1.01581,
 0.770395, 0.82342, 0.661982, 2.84892, -2.77245, 1.92475, 2.67788, 3.01776,
 1.51121, 4.61112, 1.35135, 3.60583, 2.78596, 1.4498, -0.796683, 5.37726,
 4.24755, 3.85384, 1.67251, 3.32339, 3.0388, 4.21188, 2.4825, 2.60209, 1.56404,
 2.84462, 3.04684, 1.26248, 3.20472, 3.49371, -0.991947, 2.37858, 2.35186,
 2.59153, 0.873494, 0.232236, 1.90613, 0.693796, 2.0918, -0.198688, 1.28351,
 3.66317, -0.75596, 2.26349, 3.84623, 2.02748, 1.21615, 1.40214, 1.5392, 4.47995,
 0.637378, 0.97747, 1.95484, 3.31798, 0.404918, 1.82952, 1.80883, 2.36095}
```

Reliability Data Analysis
Parametric approaches

Mathematica

Excel

Method of Matching Moments

Let the distribution of X be $N(\mu, \sigma^2)$.

(a) For a given sample of size n, use the method of moments to estimate μ and σ^2.

(b) The following data (rounded to the third decimal digit) were generated using Minitab from a normal distribution with mean 2 and a standard deviation of 1.5.

For the normal distribution, $E(X) = \mu$, *and because* $Var(X) = EX^2 - \mu^2$, *we have the second moment as* $E(X^2) = \sigma^2 + \mu^2$.

Equating sample moments to distribution moments we have

$$\frac{1}{n}\sum_{i=1}^{n} X_i = \mu_1' = \mu$$

and

$$\mu_2' = \frac{1}{n}\sum_{i=1}^{n} X_i^2 = \sigma^2 + \mu^2.$$

Reliability Data Analysis
Parametric approaches

Mathematica

Excel

Method of Matching Moments

For the normal distribution, $E(X) = \mu$, *and because* $Var(X) = EX^2 - \mu^2$, *we have the second moment as* $E(X^2) = \sigma^2 + \mu^2$.

Equating sample moments to distribution moments we have

$$\frac{1}{n}\sum_{i=1}^{n} X_i = \mu'_1 = \mu$$

and

$$\mu'_2 = \frac{1}{n}\sum_{i=1}^{n} X_i^2 = \sigma^2 + \mu^2.$$

Solving for μ *and* σ^2, *we obtain the moment estimators as*

$$\hat{\mu} = \overline{X}$$

and

$$\hat{\sigma}^2 = \frac{1}{n}\sum_{i=1}^{n} X_i^2 - \overline{X}^2 = \frac{1}{n}\sum_{i=1}^{n} (X_i - \overline{X})^2.$$

Because we know that the estimator of the mean is $\hat{\mu} = \overline{X}$ *and the estimator of the variance is* $\hat{\sigma}^2 = (1/n)\sum_{i=1}^{n} X_i^2 - \overline{X}^2$, *from the data the estimates are* $\hat{\mu} = 2.00612$, *and* $\hat{\sigma}^2 = 6.26614 - (2.00612)^2 = 2.24163$

Notice that the true mean is 2 and the true variance is 2.25, which we used to simulate the data.

Mathematica

Excel

Reliability Data Analysis
Parametric approaches

Method of Matching Moments

Let $X_1, \ldots, X_n$ be a random sample from a uniform distribution on the interval $[a, b]$. Obtain method of moment estimators for a and b.

The pdf of a uniform distribution is

$$f(x) = \begin{cases} \dfrac{1}{b-a}, & a \le x \le b \\ 0, & \text{otherwise.} \end{cases}$$

The first two population moments are

$$\mu_1 = E(X) = \int_a^b \frac{x}{b-a}dx = \frac{a+b}{2} \quad \textit{and} \quad \mu_2 = E(X^2) = \int_a^b \frac{x^2}{b-a}dx = \frac{a^2+ab+b^2}{3}.$$

The corresponding sample moments are

$$\hat{\mu}_1 = \overline{X} \quad \textit{and} \quad \hat{\mu}_2 = \frac{1}{n}\sum_{i=1}^{n} X_i^2.$$

Equating the first two sample moments to the corresponding population moments, we have

$$\hat{\mu}_1 = \frac{a+b}{2} \quad \textit{and} \quad \hat{\mu}_2 = \frac{a^2+ab+b^2}{3}$$

Mathematica

Excel

Reliability Data Analysis
Parametric approaches

Method of Matching Moments

As an example, consider the sample:

{65.5507, 1.82501, 54.442, 20.8106, 73.4306, 37.2997, 99.8077, 42.0728, 99.4873, 3.85754, 23.1605, 31.2296, 69.4113, 36.7962, 31.5806, 78.2281, 29.8135, 96.9085, 90.7682, 91.6715, 87.7468, 14.4566, 5.67949, 19.4372, 61.3422, 99.7406, 1.34892, 68.7094, 32.2245, 48.3566, 19.5227, 78.5485, 40.3027, 19.367, 96.7589, 48.1216, 11.5421, 14.3864, 39.5703, 73.7419, 59.4226, 35.8165, 62.3096, 97.7783, 50.6027, 52.2752, 3.29905, 22.6661, 75.5028, 49.3881, 84.9971, 93.0265, 14.3681, 94.0825, 33.6467, 99.1028, 39.494, 90.4233, 24.189, 4.59304, 44.1816, 55.2385, 65.9597, 52.0646, 39.0851, 91.5647, 94.8363, 48.97, 6.58895, 88.0581, 87.4569, 87.4905, 53.7736, 22.5349, 63.1581, 1.29398, 54.677, 97.7355, 89.1812, 12.3295, 22.4311, 87.3989, 54.8723, 70.7633, 1.89215, 20.8777, 30.4361, 41.2275, 23.4138, 84.3135, 75.8812, 38.493, 8.37428, 66.5273, 15.772, 65.6423, 67.1072, 27.8115, 45.4726, 57.9424}

$$\hat{a} = \hat{\mu}_1 - \sqrt{3\left(\hat{\mu}_2 - \hat{\mu}_1^2\right)} \quad \text{and} \quad \hat{b} = \hat{\mu}_1 + \sqrt{3\left(\hat{\mu}_2 - \hat{\mu}_1^2\right)}$$

$$\widehat{\mu_1} = 55.97982$$

$$\widehat{\mu_2} = 3873.881$$

$$\hat{a} = 55.97982 - \sqrt{3 \times (3873.881 \times 55.97982^2)} = 8.858458$$

$$\hat{b} = 55.97982 + \sqrt{3 \times (3873.881 \times 55.97982^2)} = 103.1012$$

Reliability Data Analysis
Parametric approaches

Method of Maximum Likelihood

PROCEDURE TO FIND MLE maximum likelihood estimators (MLEs)

1. Define the likelihood function, $L(\theta)$.
2. Often it is easier to take the natural logarithm (ln) of $L(\theta)$.
3. When applicable, differentiate $\ln L(\theta)$ with respect to θ, and then equate the derivative to zero.
4. Solve for the parameter θ, and we will obtain $\hat{\theta}$.

Reliability Data Analysis
Parametric approaches

Method of Maximum Likelihood

Let $f(x_1, \ldots, x_n; \theta), \theta \in \Theta \subseteq \mathbb{R}^k$, *be the joint probability (or density) function of* n *random variables* $X_1, \ldots, X_n$ *with sample values* $x_1, \ldots, x_n$. *The* **likelihood function** *of the sample is given by* $L(\theta; x_1, \ldots, x_n) = f(x_1, \ldots, x_n; \theta)$, [$= L(\theta)$, *in a briefer notation*].

If $X_1, \ldots, X_n$ are discrete iid random variables with probability function $p(x, \theta)$, then, the likelihood function is given by $L(\theta) = P(X_1 = x_1, \ldots, X_n = x_n)$

$$= \prod_{i=1}^{n} P(X_i = x_i), \quad \text{(by multiplication rule for independent random variables)}$$

$$= \prod_{i=1}^{n} p(x_i, \theta)$$

and in the continuous case, if the density is $f(x, \theta)$, then the likelihood function is

$$L(\theta) = \prod_{i=1}^{n} f(x_i, \theta).$$

We emphasize that L *is a function of* θ *for fixed sample values.*

Reliability Data Analysis
Parametric approaches

Excel

Method of Maximum Likelihood

Suppose $X_1, \ldots, X_n$ are a random sample from a geometric distribution with parameter p, $0 \le p \le 1$. Find MLE $\hat{p}$.

For the geometric distribution, the pmf is given by $f(x, p) = p(1-p)^{x-1}, \quad 0 \le p \le 1, \quad x = 1, 2, 3, \ldots.$

Hence, the likelihood function is

$$L(p) = \prod_{i=1}^{n} \left[p\,(1-p)^{x-1} \right] = p^n\,(1-p)^{-n+\sum_{i=1}^{n} x_i}$$

Taking the natural logarithm of $L(p)$,

$$\ln L = n \ln p + \left(-n + \sum_{i=1}^{n} x_i\right) \ln(1-p)$$

Taking the derivative with respect to p, *we have*

$$\frac{d \ln L}{dp} = \frac{n}{p} - \frac{\left(-n + \sum_{i=1}^{n} x_i\right)}{(1-p)}$$

Equating $\frac{d \ln L(p)}{dp}$ *to zero, we have*

$$\frac{n}{p} - \frac{\left(-n + \sum_{i=1}^{n} x_i\right)}{(1-p)} = 0$$

Solving for p,

$$p = \frac{n}{\sum_{i=1}^{n} x_i} = \frac{1}{\bar{x}}$$

Thus, we obtain a maximum likelihood estimator of p *as*

$$\hat{p} = \frac{n}{\sum_{i=1}^{n} X_i} = \frac{1}{\bar{X}}$$

Reliability Data Analysis
Parametric approaches

Method of Maximum Likelihood

Assume that X denotes the time to failure of device. The time to failureis exponentially distributed with failure rate λ.

$$f(x) = \lambda e^{-\lambda x} \quad \lambda > 0, x > 0$$

We intend to estimate λ from random sample $X_1, X_2, \ldots, X_n$, where $x = (x_1, x_2, \ldots, x_n)$ is the vector representing the observed values of the sample.

$$\hat{\lambda} = \Theta(x)$$

The joint pdf of $X_1, X_2, \ldots, X_n$ is given by

$$L(x, \lambda) = \lambda^n \, e^{-\lambda \sum_{j=1}^{n} x_j}$$

$L(x, \lambda)$is called the likelihood function, which is the function of the unknown parameter λ and the real data x.

The parameter value that maximizes the likelihood function is called the maximum likelihood estimator. The MLE can be interpreted as the parameter value that is most likely to explain the dataset.

The parameter value that maximizes the log-likelihood function will maximize the likelihood function.

$$ln\big(L(x, \lambda)\big) = ln\left(\lambda^n \, e^{-\lambda \sum_{j=1}^{n} x_j}\right)$$

$$ln\big(L(x, \lambda)\big) = ln\, \lambda^n + ln\, e^{-\lambda \sum_{j=1}^{n} x_j}$$

$$ln\big(L(x, \lambda)\big) = n\, ln\, \lambda - \lambda \sum_{j=1}^{n} x_j$$

Reliability Data Analysis
Parametric approaches

Excel

Method of Maximum Likelihood

The function $ln\left(L(x,\lambda)\right)$ can be maximized by deriving it with respect to λ, setting the resulting expression to zero, and solving the equation for λ.

Therefore:

$$\frac{\partial ln\left(L(x,\lambda)\right)}{\partial\lambda} = \frac{n}{\lambda} - \sum_{j=1}^{n} x_j = 0$$

So:

$$\hat{\lambda} = \frac{n}{\sum_{j=1}^{n} x_j}$$

Accelerated life testing

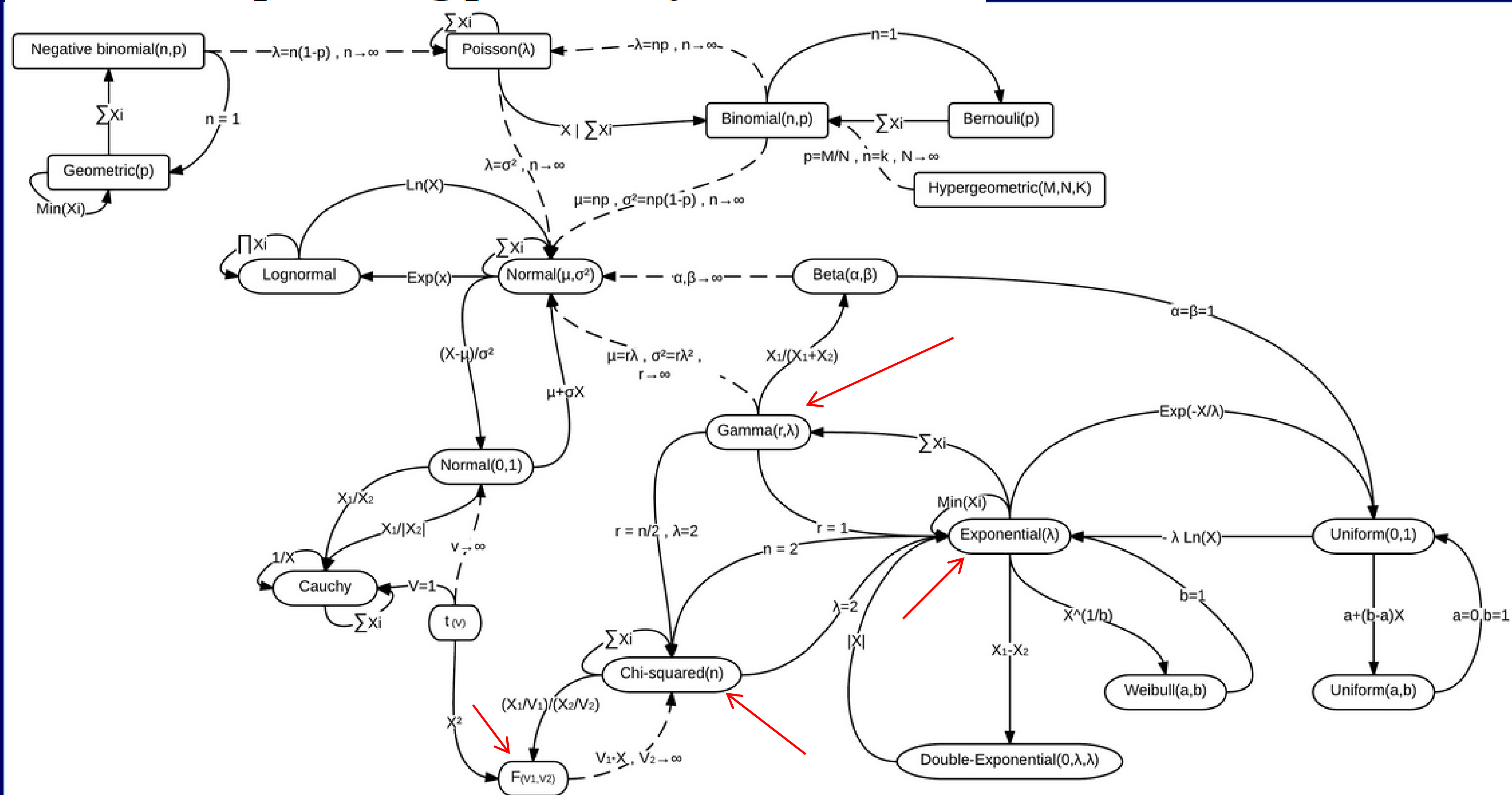
Now assume for a certain system that we observed 60 failures during T = $15\,116\,772.7753$ min hours. Hence:

$$\hat{\lambda} = \frac{60\ failures}{15\,116\,772.7753} = 3.96 \times 10^{-5}\ failures/\min$$

Reliability Data Analysis
Parametric approaches

Excel

Relationships among probability distributions



Consider that we have observed 60 units of a specific type until the respective failures. The failure times were registered and are depicted in the spreadsheet. Assuming the time to failure is exponentially distributed, compute the confidence interval for λ.

lysis

ches

Excel

Mathematica

$$(MTTF_l \quad MTTF_u) = \left(\frac{2S_{n:r}}{\chi^2_{2n,\alpha/}}, \quad \frac{2S_{n:r}}{\chi^2_{2n,1-\alpha/}}\right)$$

Consider a reliability test starts at 0 and that all (n) failures are reported as failures. The test finishes when all fail or after r failures occur (right censoring type II). The confidence for $\hat{\lambda}$ and $\widehat{MTTF}$ can be computed

$$(\lambda_l \quad \lambda_u) = \left(\frac{\chi^2_{2n,1-\alpha/2}}{2S_{n:r}}, \quad \frac{\chi^2_{2n,\alpha}}{2S_n}\right.$$

Now, also consider an accelerated test in which 60 units have been placed. The test was finished when 10 failures occurred. The observed failure times are registered in the spreadsheet. Assuming the time to failure is exponentially distributed, compute the confidence interval for λ.

Reliability Data Analysis
Parametric approaches

Excel

Mathematica

Confidence Interval Exponential Distribution

If right censoring type I is considered, the method still provides a useful approximation.

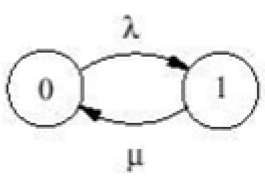
The same process can be applied to estimate the confidence interval for MTTR.

Reliability Data Analysis
Parametric approaches

Excel

Consider now that the units have been repaired. The respective time to repairs are also registered in the spreadsheet. Compute confidence interval for the availability.

The CTMC representing the system:



$$= \frac{}{1+\frac{\lambda}{\mu}}$$

$$A = \frac{1}{1+\rho} \quad \text{where} \quad \rho = \frac{\lambda}{\mu}.$$

re: $\hat{A} = \dfrac{1}{1+\hat{\rho}}$

$$= \frac{\hat{\lambda}}{\hat{\mu}}$$

fidence interval for ρ is $(\rho_l, \quad \rho_u)$,

$$\rho_l = \frac{\hat{\rho}}{f_{2n,2n;{}^{\alpha}/_{2}}} \quad \rho_u = \frac{\hat{\rho}}{f_{2n,2n;{}^{1-\alpha}/_{2}}}$$

he confidence interval for A is $(A_l, \quad A_u)$, where:

$$A_l = \frac{1}{1+\rho_u} \qquad A_u = \frac{1}{1+\rho_l}$$

If T_1 and T_2 are **chi-squared** random variables with n_1 and n_2 degrees of freedom respectively, then $(T_1/n_1)/(T_2/n_2)$ is an $\boldsymbol{F}(n_1, n_2)$ random variable.

Reliability Data Analysis
Parametric approaches

Confidence Interval

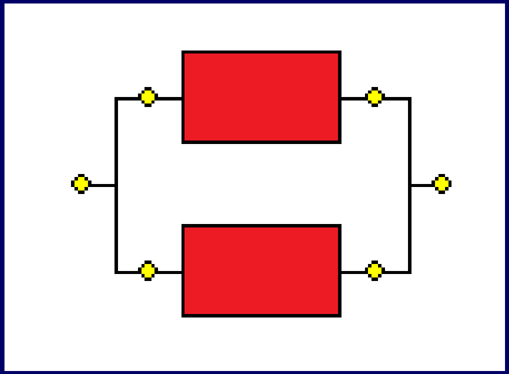
You may also adopt:

- Adopt Bootstrap or Semi-parametric Bootstrap
- If possible, you may also use t-student distribution or
- Central Limit Theorem

REDUNDANCY MECHANISMS

Redundancy Mechanisms

- Parallel Redundancy

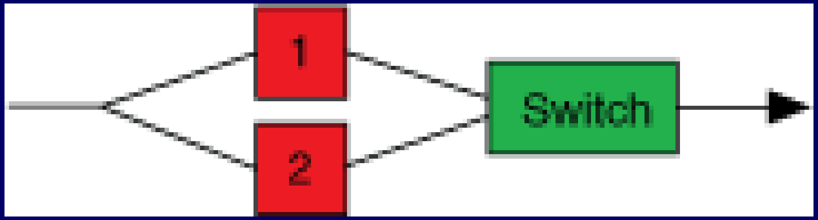


Parallel Redundancy refers to the approach of having multiply units running in parallel. All units are highly synchronized and receive the same input information at the same time.

But because all the units are powered up and actively engaged, the system is at risk of encountering failures in many units.

Redundancy Mechanisms

- Parallel Redundancy

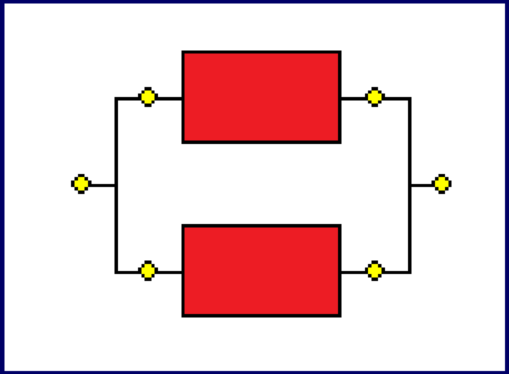


Deciding which unit is correct can be challenging if you only have two units. Sometimes you just have to choose which one you are going to trust the most and it can get complicated.

If you have more than two units the problem is simpler, usually the majority wins or the two that agree win.

Redundancy Mechanisms

- Parallel Redundancy (Active-Active) – load sharing

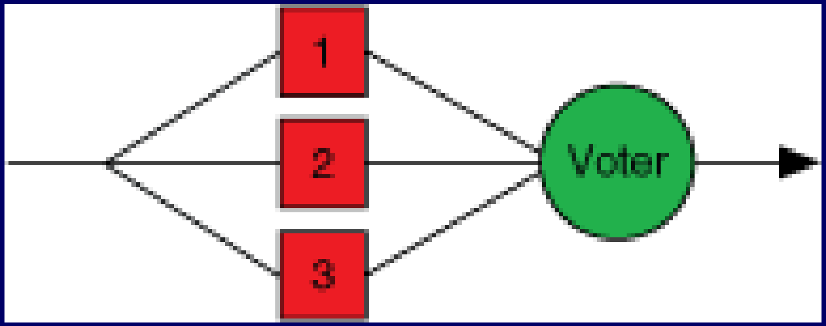


Active-Active refers to the approach of having multiply units sharing the load.

As the units are powered up and actively engaged, the system is at risk of encountering failures in many units.

Redundancy Mechanisms

- Triple Modular Redundancy (TMR)



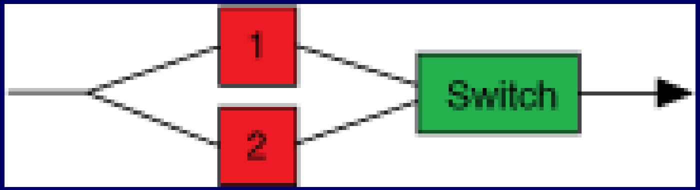
Deciding which unit is correct can be challenging if you only have two units. Sometimes you just have to choose which one you are going to trust the most and it can get complicated.

If you have more than two units the problem is simpler, usually the majority wins or the two that agree win.

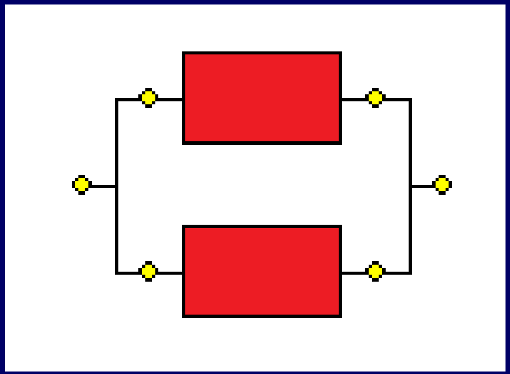
A generalization is named NMR

Redundancy Mechanisms

- Hot Standby In hot standby, the secondary unit is powered up.



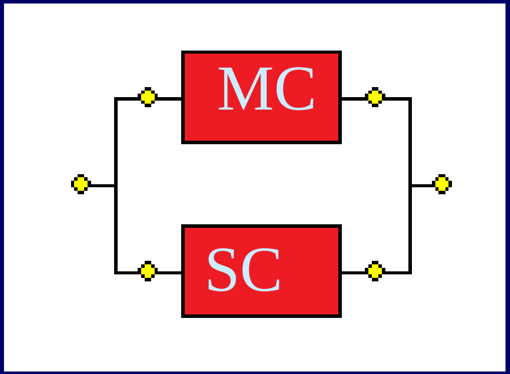
If you use the secondary unit as the watchdog and/or voter to decide when to switch over, you can eliminate the need for a third party to this job.



This design does not preserve the reliability of the standby unit. However, it shortens the downtime, which in turn increases the availability of the system.

Redundancy Mechanisms

- Hot Standby



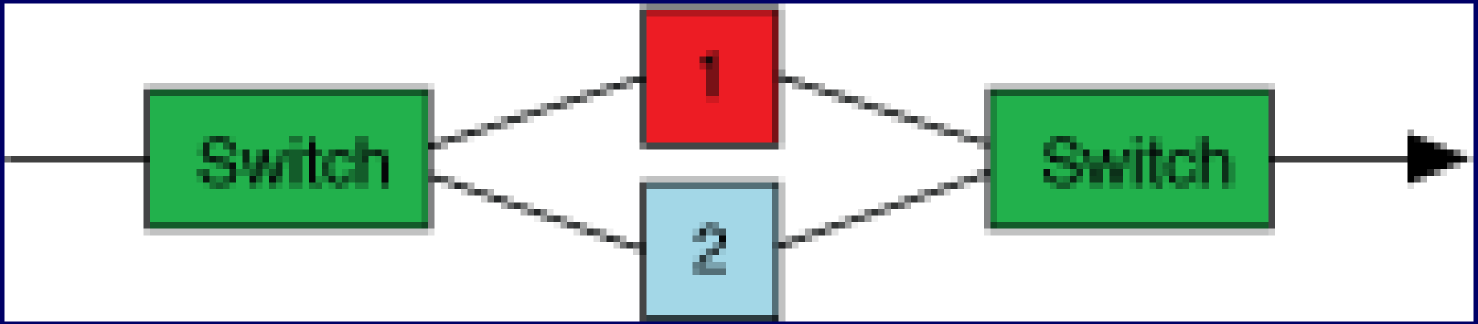
Some flavors of *Hot Standby* are similar to *Parallel Redundancy.*
These naming conventions are commonly interchanged.

For us, Hot Standby and Parallel Redundancy (active-active) are the same mechanism!

But, attention!

Redundancy Mechanisms

- Cold Standby



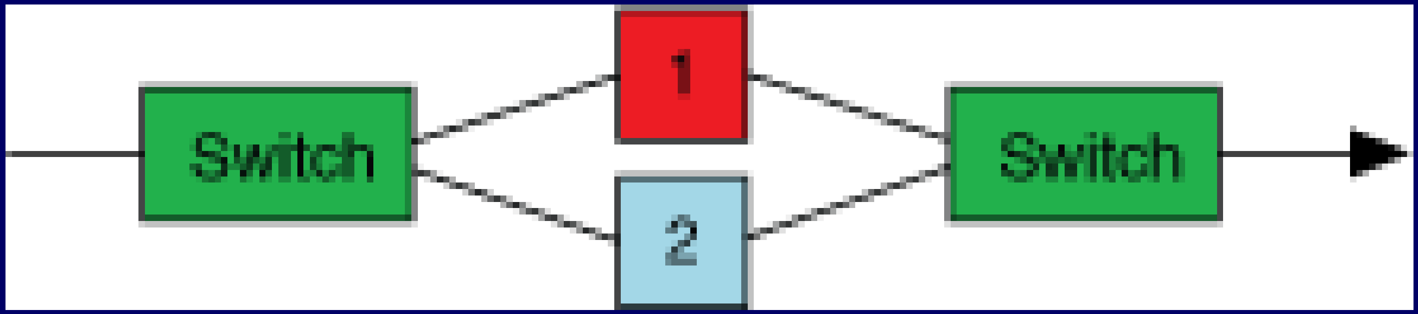
In cold standby, the secondary unit is powered off, thus preserving the reliability of the unit.

The drawback of this design is that standby unit have to power up, since it is initially powered off.

Perfect switching AND non-prefect switching

Redundancy Mechanisms

- Warm Standby



In warm standby, the secondary unit is powered up, but not receiving the workload.

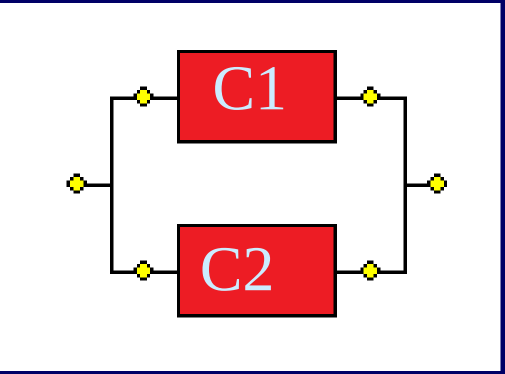
It is common to assume that in such a state the standby component has higher reliability than when receiving the workload (properly working).

When the main component fails, the standby device promptly assumes the task.

Its switching time is shorter than the cold standby's switching time .

Redundancy Mechanisms

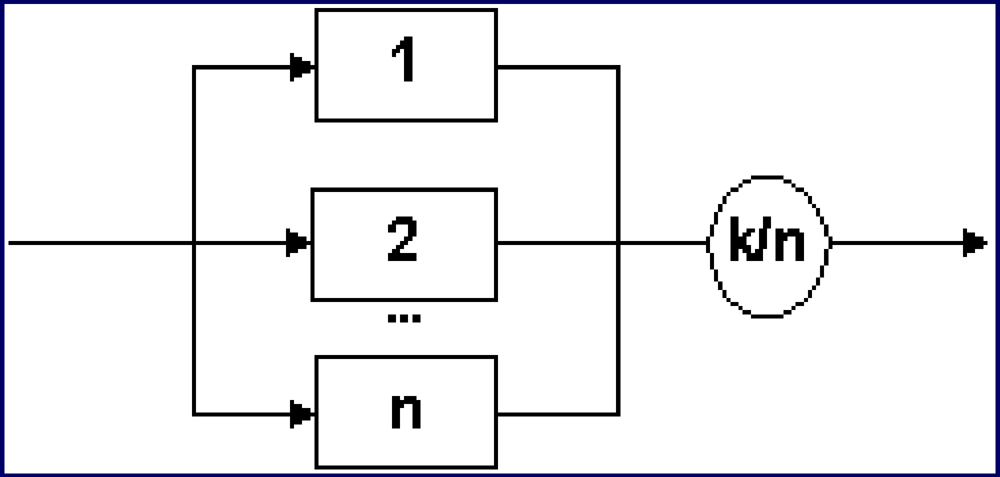
- Active-Active



Active–active redundancy means that workload is shared by two operational units, but workload can be served with acceptable quality by a single unit.

Redundancy Mechanisms

- K out of N



Consider a system composed of n identical and independent components that is operational if at least k out of its n components are working properly.

This sort of redundancy is named *k out of n*

Redundancy Mechanisms

- RAID (redundant array of independent disks)

Many types of RAID have been developed and more will probably come out in the future.

The technology is driven by the variety of methods available for connecting multiple disks as well as various coding techniques, alternative read-and-write strategies, and the flexibility in organization to "tune" the architecture of the system.

Redundancy Mechanisms

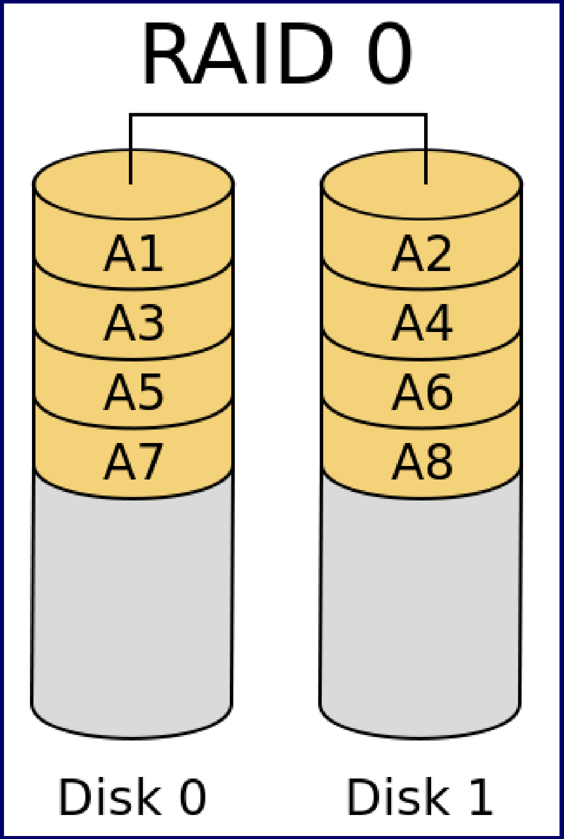
- RAID 0

involves striping, which is the distribution of data across multiple disk drives in equally sized chunks.

For example, a 150 KB file can be striped, or chunked, across ten 15 KB chunks.

The RAID set of striped disks appears as a single, logical disk to the operating system.

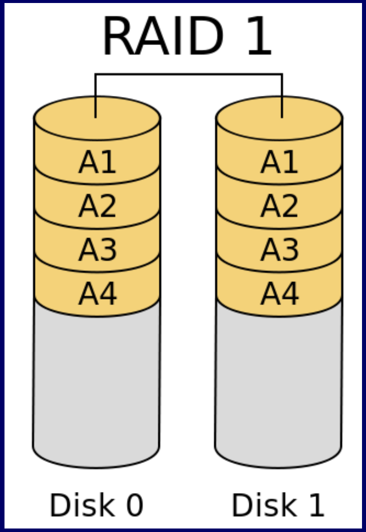
RAID-0 does not provide any data redundancy.



Redundancy Mechanisms

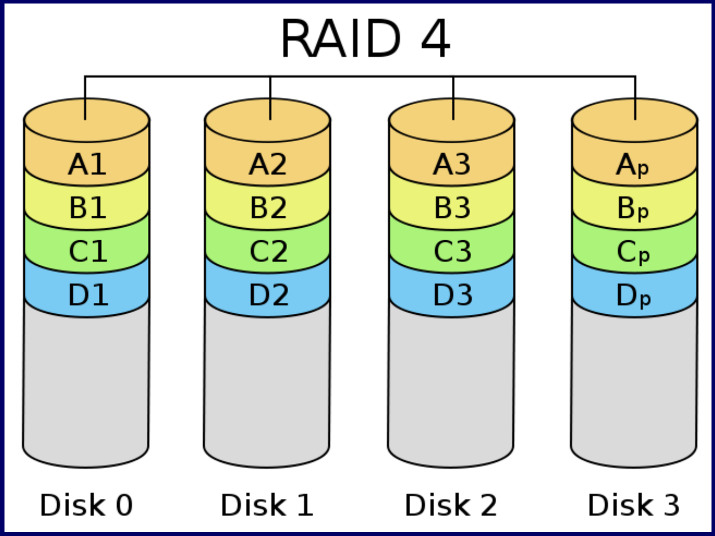
- ## RAID 1

uses mirroring, or shadowing: all data written on a given disk is duplicated on another disk.



- ## RAID 4

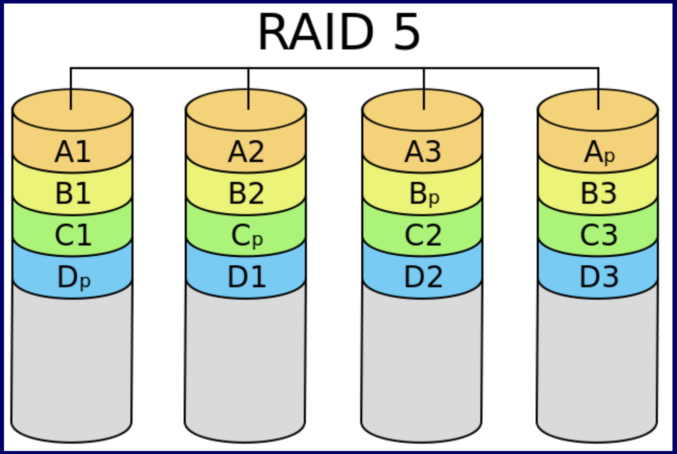
uses block-level striping with a dedicated parity disk.



Redundancy Mechanisms

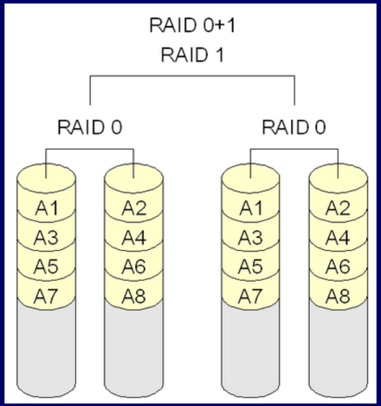
- RAID 5

is similar to RAID 4 except that the parity data is striped across all HDDs instead of written on a dedicated HDD.



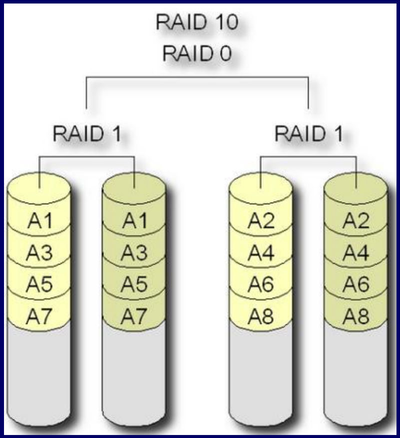
- RAID 0+1

striped sets in a mirrored set.



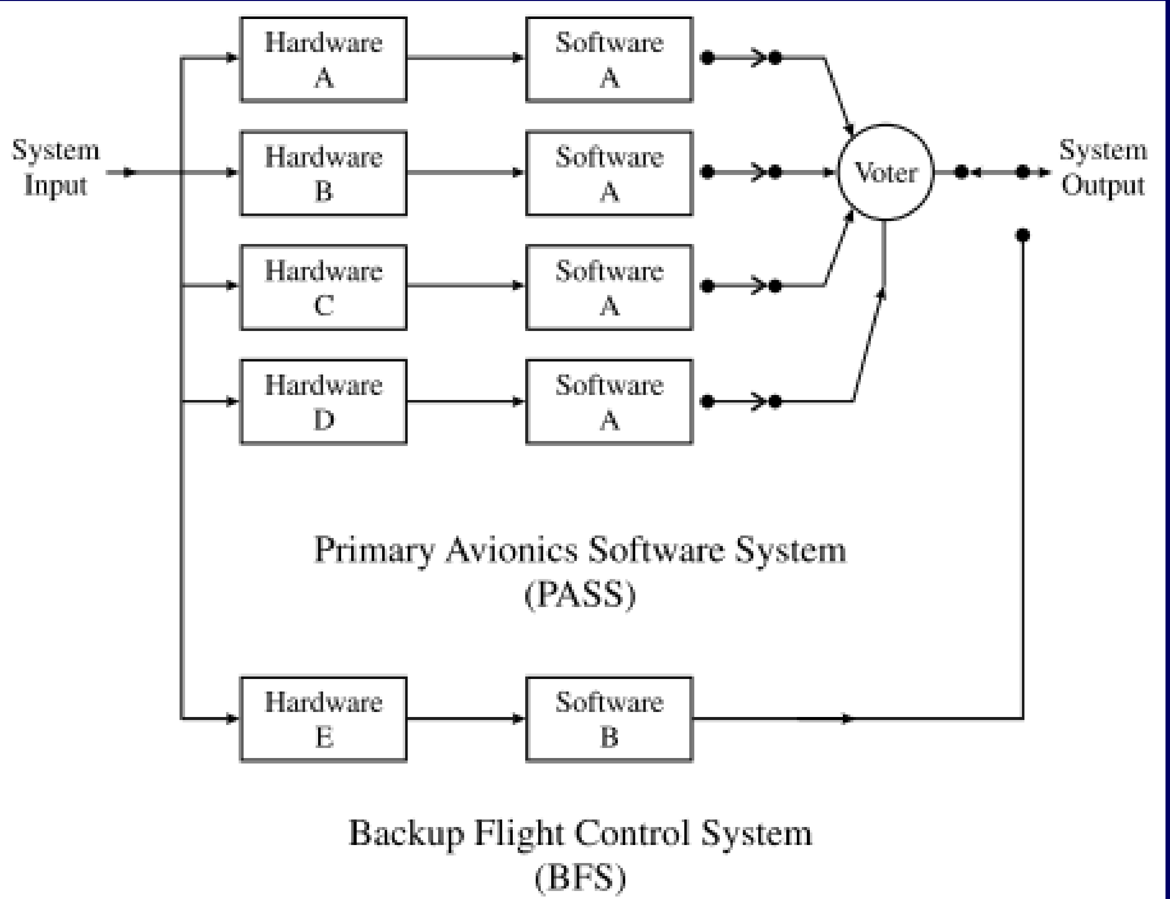
- RAID 1+0 (RAID 10)

mirrored sets in a striped set.



Redundancy Mechanisms

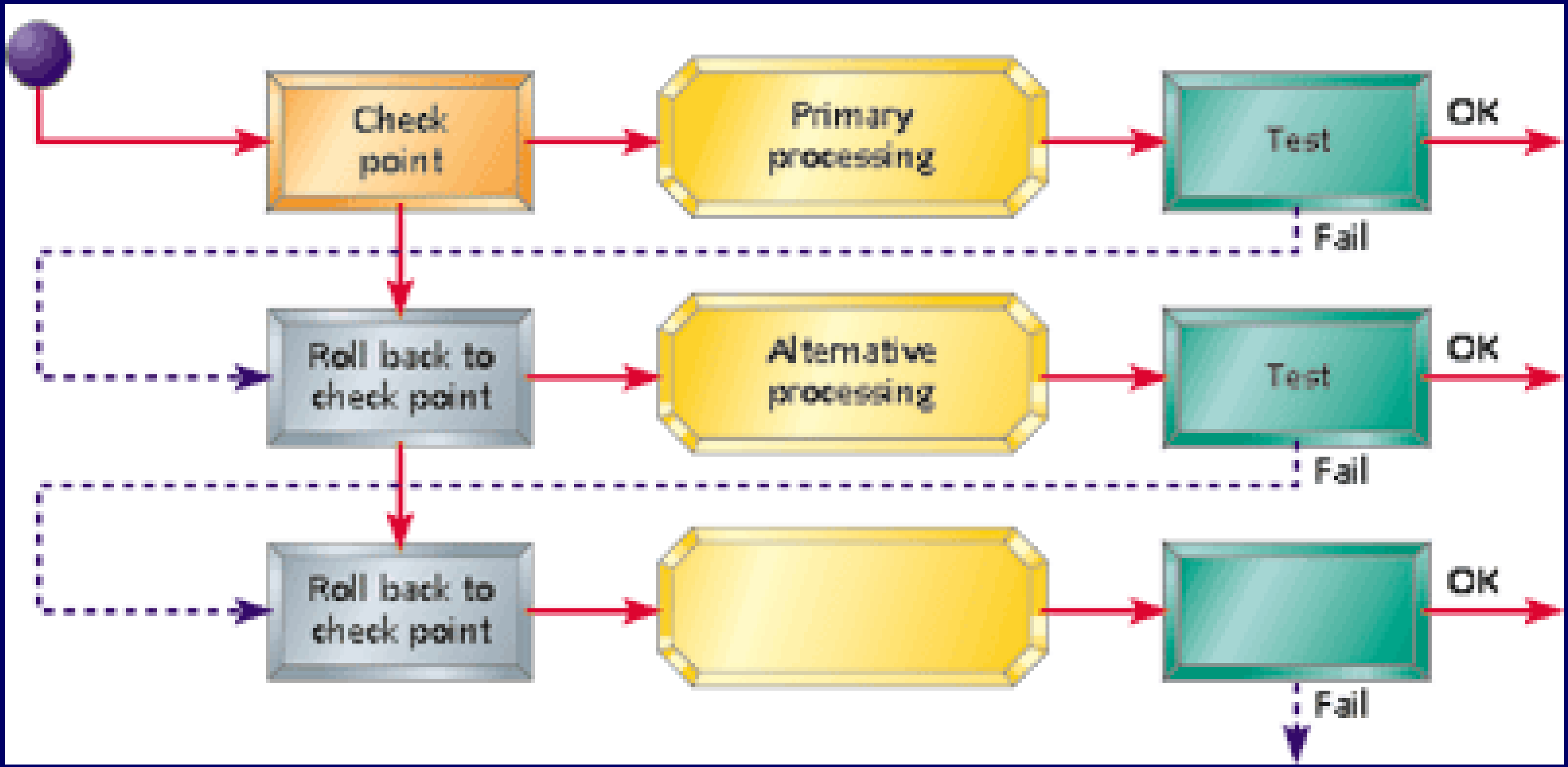
- N-version programming



Hardware and software redundancy in the Space Shuttle's avionics control system.

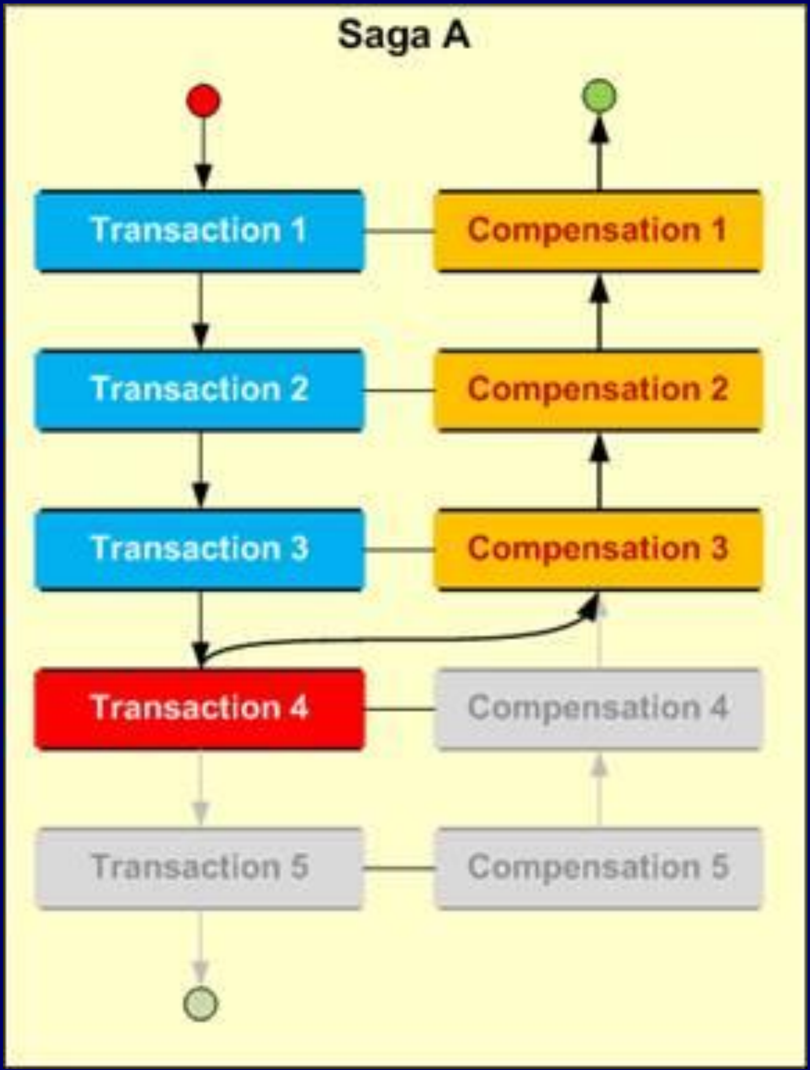
Redundancy Mechanisms

- Checkpoints and recovering



Redundancy Mechanisms

- Backward Recovery



Redundancy Mechanisms

- Reboot

The simplest - but weakest - recovery technique.

From the implementation standpoint is to reboot or restart the system.

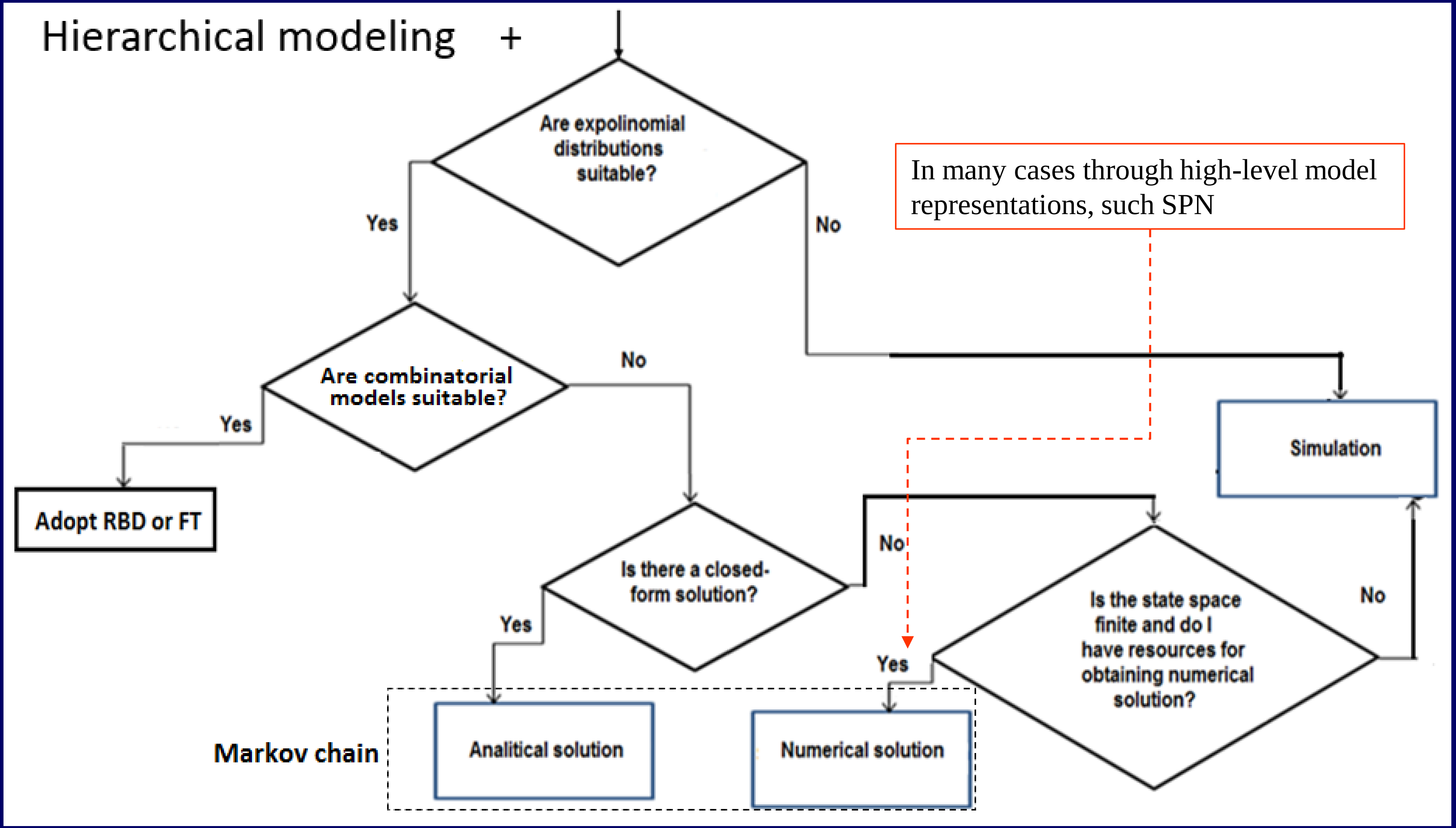
- Journaling - To employ these techniques requires that:

1. a copy of the original database, disk, and filename be stored,
2. all transactions that affect the data must be stored during execution, and
3. the process be backed up to the beginning and the computation be retried.

Clearly, items (2) and (3) require a lot of storage; in practice, journaling can only be executed for a given time period, after which the inputs and the process must be erased and a new journaling time period created.

MODELING

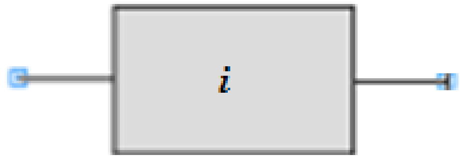
Modeling Strategy

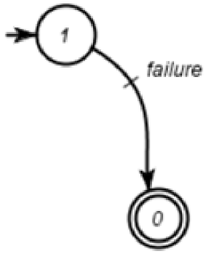


Coherent System

Let x_i be a random variable, and

$$x_i = \begin{cases} 1 & \text{if component } i \text{ functions} \\ 0 & \text{if component } i \text{ fails} \end{cases}$$





Therefore, x_i is a Bernoulli variable.

As **BernoulliDistribution[p]**

PDF	$\begin{cases} 1-p & x_i = 0 \\ p & x_i = 1 \end{cases} \quad x_i \in \{0, 1\}$
DistributionDomain	$x_i \in \{0, 1\}$
DistributionParameterAssumptions	$p \in \mathbb{R} \wedge 0 \le p \le 1$
Mean	p
Variance	$(1-p)\,p$

$$P(x_i = 1) = p_i = E[x_i]$$

Coherent System

Structure Function

Operations

- $\{+,-,\times,\div\}$ – arithmetic operations

Consider a system S composed by a set of components, $C = \{c_i | 1 \leq i \leq n\}$, where the state of the system S and its components could be either operational or failed. Let the discrete random variable x_i indicate the state of component i, thus:

$$x_i = \begin{cases} 0 & \textit{if the component i has failed} \\ 1 & \textit{if the component i is operational} \end{cases}$$

The vector $\mathbf{x} = (x_1, x_2, \ldots, x_i, \ldots, x_n)^1$ represents the state of each component of the system, and it is named state vector. The system state may be represented by a discrete random variable $\phi(\mathbf{x}) = \phi(x_1, x_2, \ldots, x_i, \ldots, x_n)$, such that

$$\phi(\mathbf{x}) = \begin{cases} 0 & \textit{if the system has failed} \\ 1 & \textit{if the system is operational} \end{cases}$$

$\phi(\mathbf{x})$ is called the structure function of the system.

If one is interested in representing the system state at a specific time t, the components' state variables should be interpreted as a random variables at time t. Hence, $\phi(\mathbf{x}(\mathbf{t}))$, where $\mathbf{x}(t) = (x_1(t), x_2(t), \ldots, x_i(t), \ldots, x_n(t))$.

Coherent System

As $\phi(\mathrm{x})$ is also a Bernoulli random variable, then

$$P(\phi(\mathrm{x}) = 1) = E[\phi(\mathrm{x})]$$

If p_i is the reliability of component *i* (at *t*) or its instantaneous availability (at *t*) or its steady-state availability, then $P(\phi(\mathrm{x}) = 1)$ is the respective system measure.

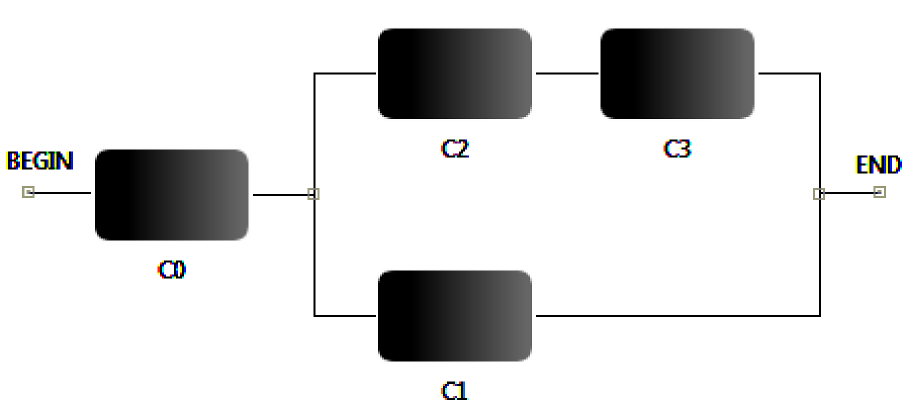
If one is interested in representing the system state at a specific time t, the components' state variables should be interpreted as a random variables at time t. Hence, $\phi(\mathbf{x}(\mathbf{t}))$, where $\mathbf{x}(t) = (x_1(t), x_2(t), \dots, x_i(t), \dots, x_n(t))$.

Coherent System

Excel

- Structure Function $\phi(C_3, C_2, C_1, C_0) = C_0 \times (1 - ((1 - C_2 \times C_3) \times (1 - C_1)))$

C3	C2	C1	C0	ϕ
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	1
0	1	0	0	0
0	1	0	1	0
0	1	1	0	0
0	1	1	1	1
1	0	0	0	0
1	0	0	1	0
1	0	1	0	0
1	0	1	1	1
1	1	0	0	0
1	1	0	1	1
1	1	1	0	0
1	1	1	1	1



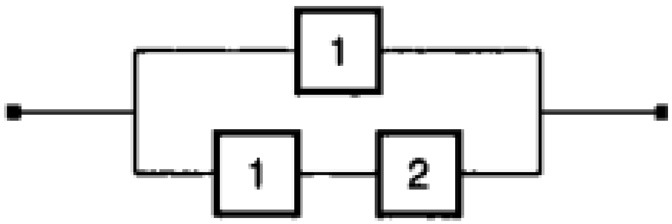
Coherent System

Excel

- Irrelevant Component

A component of a system is irrelevant to the dependability of the system if the state of the system is not affected by the state of the component.

c_i is irrelevant to the structure function if $\phi(1_i, \mathbf{x}) = \phi(0_i, \mathbf{x})$.



Component 2 is irrelevant.

C2	C1	ϕ
0	0	0
0	1	1
1	0	0
1	1	1

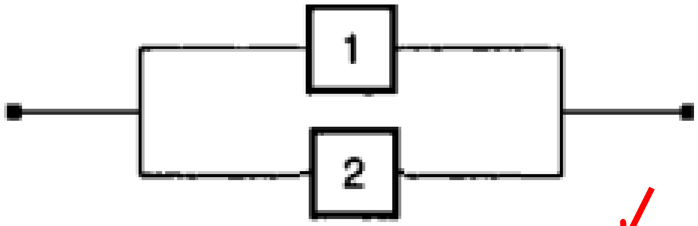
Coherent System

Excel

- Irrelevant Component

A component of a system is irrelevant to the dependability of the system if the state of the system is not affected by the state of the component.

c_i is irrelevant to the structure function if $\phi(1_i, \mathbf{x}) = \phi(0_i, \mathbf{x})$.



Component 2 is relevant.

C2	C1	ϕ
0	0	0
0	1	1
1	0	1
1	1	1

Coherent System

- Structure Function

For any component c_i,

$$\phi(\mathbf{x}) = x_i\,\phi(1_i, \mathbf{x}) + (1 - x_i)\,\phi(0_i, \mathbf{x}),$$

where $\phi(1_i, \mathbf{x}) = \phi(x_1, x_2, \dots, 1_i, \dots, x_n)$ and $\phi(0_i, \mathbf{x}) = \phi(x_1, x_2, \dots, 0_i, \dots, x_n)$.

The first term $(x_i\,\phi(1_i, \mathbf{x}))$ represents a state where the component c_i is operational and the state of the other components are random variables $(\phi(x_1, x_2, \dots, 1_i, \dots, x_n))$. The second term $((1 - x_i)\,\phi(0_i, \mathbf{x}))$, on the other hand, states the condition where the component c_i has failed and the state of the other components are random variables $(\phi(x_1, x_2, \dots, 0_i, \dots, x_n))$.

Equation is known as factoring of the structure function and very useful for studying complex system structures, since through its repeated application, one can eventually reach a subsystem whose structure function is simple to deal with (1).

Coherent System

A system with structure function $\phi(\mathbf{x})$ is said to be **coherent** if and only if $\phi(\mathbf{x})$ is non-decreasing in each x_i and every component c_i is relevant.

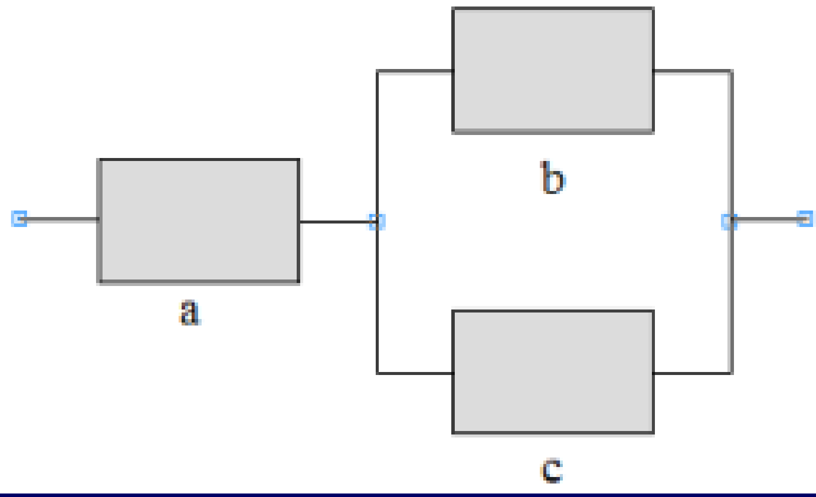
A function $\phi(\mathbf{x})$ is non-decreasing if for every two state vectors $\mathbf{x}$ and $\mathbf{y}$, such that $\mathbf{x} < \mathbf{y}$, then $\phi(\mathbf{x}) \leq \phi(\mathbf{y})$.

Another aspect of coherence that should also be highlighted is that replacing a failed component in working system does not make the system fail. But, it does not also mean that a failed system will work if a failed component is substituted by an operational component.

Coherent System

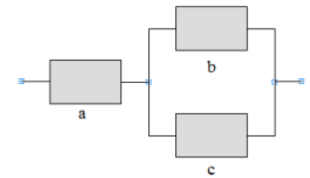
- Example - Structure Function

Consider a coherent system (C, ϕ) composed of three blocks, $C = \{a, b, c\}$



Coherent System

Consider a coherent system (C, ϕ) composed of three blocks, $C = \{a, b, c\}$



Example - Structure Function

factoring on component a, we have:

$$\phi(x_a, x_b, x_c) = x_a\, \phi(1_a, x_b, x_c) + (1 - x_a)\, \phi(0_a, x_b, x_c) = x_a\, \phi(1_a, x_b, x_c).$$

since $\phi(0_a, x_b, x_c) = 0.$

Now factoring $\phi(1_a, x_b, x_c)$ on component b,

$$\phi(1_a, x_b, x_c) = x_b\, \phi(1_a, 1_b, x_c) + (1 - x_b)\, \phi(1_a, 0_b, x_c).$$

As $\phi(1_a, 1_b, x_c) = 1$, thus:

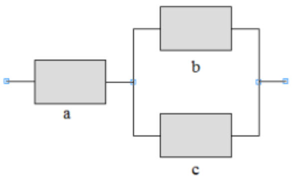
$$\phi(1_a, x_b, x_c) = x_b + (1 - x_b)\, \phi(1_a, 0_b, x_c).$$

Therefore:

$$\phi(x_a, x_b, x_c) = x_a\, \phi(1_a, x_b, x_c) = x_a \times [x_b + (1 - x_b)\, \phi(1_a, 0_b, x_c)].$$

Coherent System

Consider a coherent system (C, ϕ) composed of three blocks, $C = \{a, b, c\}$



- Example - Structure Function

Fact $\phi(1_a, 0_b, x_c)$ on component c to get:

$$\phi(1_a, 0_b, x_c) = x_c\, \phi(1_a, 0_b, 1_c) + (1 - x_c)\, \phi(1_a, 0_b, 0_c).$$

Since $\phi(1_a, 0_b, 1_c) = 1$ and $\phi(1_a, 0_b, 0_c) = 0$, thus:

$$\phi(1_a, 0_b, x_c) = x_c.$$

So

$$\phi(x_a, x_b, x_c) = x_a \times [x_b + (1 - x_b)\, \phi(1_a, 0_b, x_c)] =$$

$$x_a \times [x_b + (1 - x_b)\, x_c] =$$

$$\phi(x_a, x_b, x_c) = x_a x_b + x_a x_c (1 - x_b) =$$

$$\phi(x_a, x_b, x_c) = x_a[1 - (1 - x_b)(1 - x_c)].$$

Coherent System

- Logical Function

Operations

- $\{\wedge, \vee, \neg\}$ – logic operations

$$s_i = \begin{cases} F & \text{if the component } i \text{ has failed} \\ T & \text{if the component } i \text{ is operational} \end{cases}$$

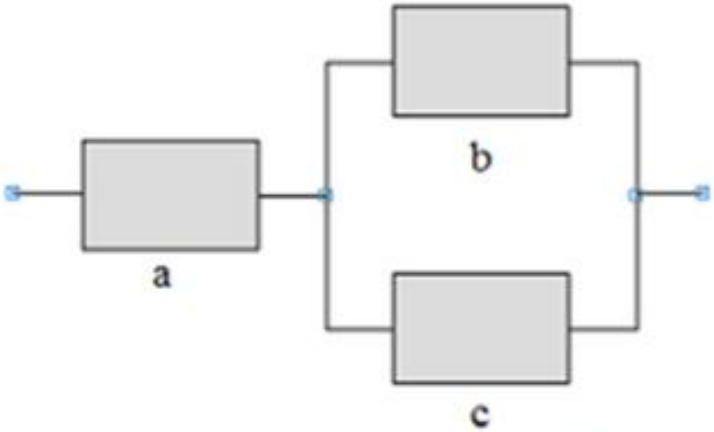
$$\varphi(\mathbf{bs}) = \begin{cases} F & \text{if the system has failed} \\ T & \text{if the system is operational} \end{cases}$$

$\mathbf{bs} = (s_1, s_2, \ldots, s_i, \ldots, s_n)$ represents the Boolean state of each component of the system.
The system state could be either operational or failed.
The operational system state is represented by $\varphi(\mathbf{bs})$, whereas $\overline{\varphi(\mathbf{bs})}$ denotes a faulty system.

Coherent System

- Example – Logical Function

Example: Consider a system (C, ϕ) composed of three blocks, $C = \{a, b, c\}$



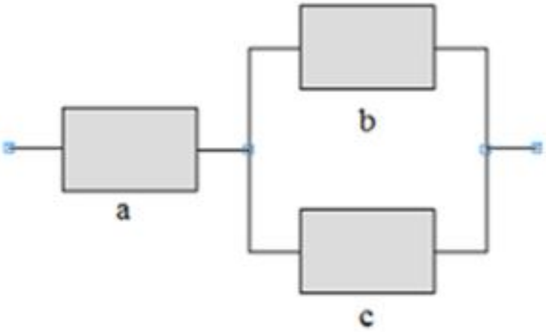
$$\varphi(s_a, s_b, s_c) = s_a \wedge (s_b \vee s_c) = s_a \wedge (\overline{\overline{s_b} \wedge \overline{s_c}})$$

Coherent System

- Example – Converting a Logical Function into a Structure Function

Using the notation described, s_i is equivalent to x_i, $\overline{s_i}$ represents $1 - x_i$, $\varphi(\mathbf{bs})$ is the counterpart of $\phi(\mathbf{x}) = 1$, $\overline{\varphi(\mathbf{bs})}$ depicts $\phi(\mathbf{x}) = 0$, $\wedge$ represents $\times$, and $\vee$ is the respective counterpart of $+$.

Consider a system (C, ϕ) composed of three blocks, $C = \{a, b, c\}$



$$\varphi(s_a, s_b, s_c) = s_a \wedge (\overline{\overline{s_b} \wedge \overline{s_c}}).$$

$$\phi(\mathbf{x}) = x_a \times [1 - (1 - x_b) \times (1 - x_c)]$$

Modeling Techniques

- Classification
  - State-space based models
    - CTMC, SPN, SPA
  - Combinatorial models
    - RBD, FT, RG

Combinatorial models

Reliability Block Diagram

- RBD is success oriented diagram.
- Each component of the system is represented as a block
- RBDs are networks of functional blocks connected such that they affect the functioning of the system
- Failures of individual components are assumed to be independent for easy solution.
- System behavior is represented by connecting the blocks
  - Blocks that are all required are connected in series
  - Blocks among which only one is required are connected in parallel
  - When at least k out of n are required, use k-of-n structure

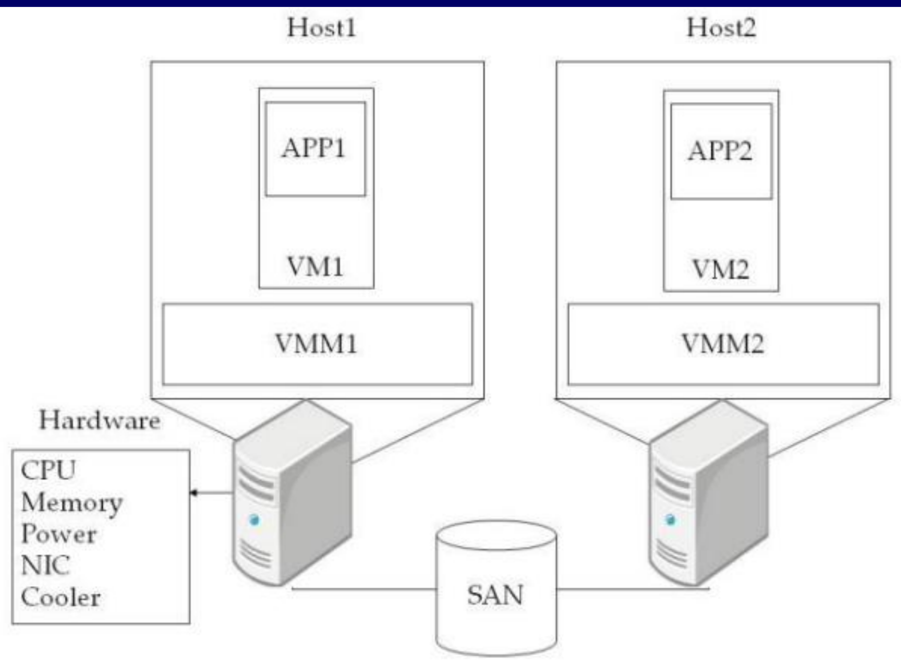
Reliability Block Diagram

- A RBD is not a block schematic diagram of a system, although they might be isomorphic in some particular cases.

- Although RBD was initially proposed as a model for calculating reliability, it has been used for computing availability, maintainability etc.

Reliability Block Diagram

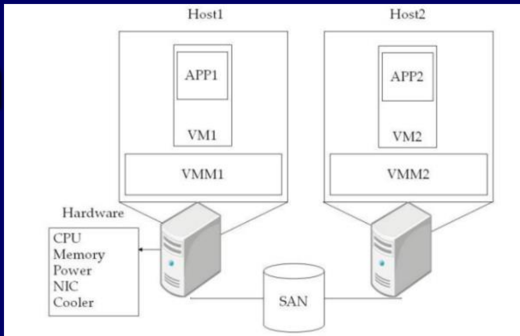
- Series



- Operational Mode

$$OM_1 = App_1 \wedge VMM_1 \wedge VM_1 \wedge H_1 \wedge SAN$$
$$\wedge\, App_2 \wedge VMM_2 \wedge VM_2 \wedge H_2$$

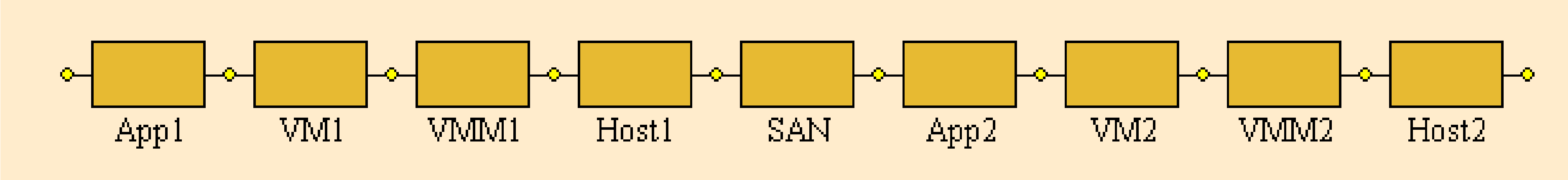
Reliability Block Diagram



Series

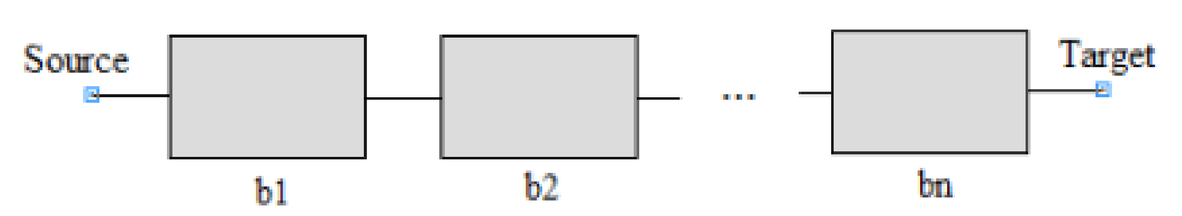
- Operational Mode

$$OM_1 = App_1 \wedge VMM_1 \wedge VM_1 \wedge H_1 \wedge SAN \wedge App_2 \wedge VMM_2 \wedge VM_2 \wedge H_2$$



Reliability Block Diagram

- Series



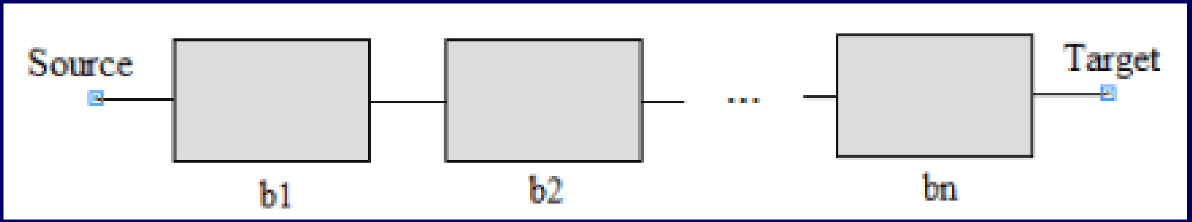
As $\phi(\mathrm{x})$ is also a Bernoulli random variable, then

$$P(\phi(\mathrm{x}) = 1) = E[\phi(\mathrm{x})]$$

If p_i is the reliability of component *i* (at *t*) or its instantaneous availability (at *t*) or its steady-state availability, then $P(\phi(\mathrm{x}) = 1)$ is the respective system measure.

Reliability Block Diagram

- Series



$$P\{\phi(\mathbf{x}) = 1\} = P\{\phi(x_1, x_2, \ldots, x_i, \ldots, x_n) = 1\} = \prod_{i=1}^{n} P\{x_i = 1\} = \prod_{i=1}^{n} p_i = 1.$$

Therefore, the system reliability is

$$R_S(t) = P\{\phi(\mathbf{x}, \mathrm{t}) = 1\} = \prod_{i=1}^{n} P\{x_i(t) = 1\} = \prod_{i=1}^{n} R_i(t),$$

where $R_i(t)$ is the reliability of block b_i.

Likewise, the system instantaneous availability is

$$A_S(t) = P\{\phi(\mathbf{x}, \mathrm{t}) = 1\} = \prod_{i=1}^{n} P\{x_i(t) = 1\} = \prod_{i=1}^{n} A_i(t),$$

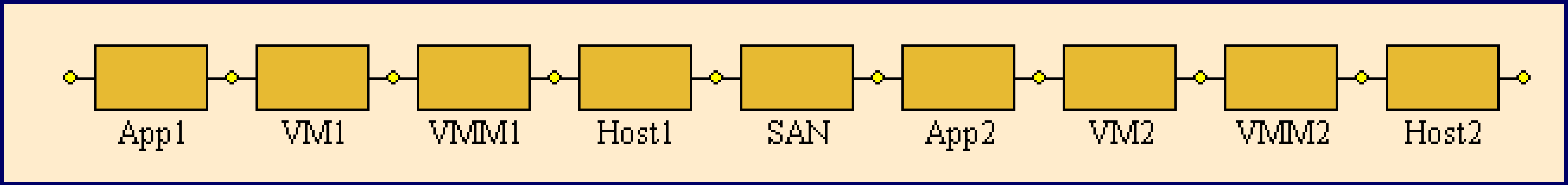
where $A_i(t)$ is the instantaneous availability of block b_i.

The steady state availability is

$$A_S = P\{\phi(\mathbf{x}) = 1\} = \prod_{i=1}^{n} P\{x_i = 1\} = \prod_{i=1}^{n} A_i,$$

where A_i is steady state availability of block b_i.

Computing the Reliability



If for every component i, $TTF_i \overset{\text{def}}{=} EXP(\lambda_i)$, then $R_i(t) = e^{-\lambda_i t}$.

Hence:

$$R(t) = e^{-\lambda_{app1}t} \times e^{-\lambda_{VM1}t} \times e^{-\lambda_{VMM1}t} \times e^{-\lambda_{H1}t} \times e^{-\lambda_{SAN}t} \times e^{-\lambda_{app2}t} \times e^{-\lambda_{VM2}t} \times e^{-\lambda_{VMM2}t} \times e^{-\lambda_{H2}t} =$$

$$e^{-(\lambda_{app1}+\lambda_{VM1}+\lambda_{VMM1}+\lambda_{H1}+\lambda_{SAN}+\lambda_{ap})}$$

$$R(t) = 0.805735302, \qquad t = 0.002 \ tu$$

Reliability Block Diagram

- Series

Series system of n independent components, where the i component has lifetime exponentially distributed with rate λ_i

Thus lifetime of the system is exponentially distributed with parameter $\sum_{i=1}^{n} \lambda_i$

and system MTTF = $1/\sum_{i=1}^{n} \lambda_i$

Reliability Block Diagram

- Series

R.v. X: series system life time

R.v. X_i: i^{th} comp's life time (arbitrary distribution)

$$0 \le E[X] \le min\{E[X_i]\}$$

Case of *weakest link*

$$X = \min\{X_1, X_2, .., X_n\}$$

$$R_X(t) = \prod_{i=1}^{n} R_{X_i}(t) \le \min_i\{R_{X_i}(t)\}, \ (0 \le R_{X_i}(t) \le 1)$$

$$E[X] = \int_0^\infty R_X(t)dt \le \min_i \left\{ \int_0^\infty R_{X_i}(t)dt \right\}$$
$$= \min_i \{E[X_i]\}$$

Reliability Block Diagram

- Example:

Assume that the constant failure rates of web services 1, 2, 3, and 4 of sw system are $\lambda 1 = 0.0001$ failures per hour, $\lambda 2 = 0.0002$ failures per hour, $\lambda 3 = 0.0003$ failures per hour, and $\lambda 4 = 0.0004$ failures per hour, respectively. The sw system cannot work when any one of the web services is down.

a) Calculate the total sw system failure rate.
b) Calculate MTTF of sw system.
c) Calculate the R(t) at 730h

Reliability Block Diagram

- Example:

Assume that the constant failure rates of web services 1, 2, 3, and 4 of sw system are $\lambda 1 = 0.00001$ failures per hour, $\lambda 2 = 0.00002$ failures per hour, $\lambda 3 = 0.00003$ failures per hour, and $\lambda 4 = 0.00004$ failures per hour, respectively. The sw system cannot work when any one of the web services is down.

a) Calculate the total sw system failure rate.

b) Calculate MTTF of sw system.

c) Calculate the R(t) at 730h

Reliability Block Diagram

- Example:

The sw system cannot work when any one of the web services is down.

$\Leftrightarrow$

The sw system only works when all web services work.

$$ws_1 \stackrel{\text{def}}{=} web\ services\ 1\ working$$

$$ws_2 \stackrel{\text{def}}{=} web\ services\ 2\ working$$

$$ws_3 \stackrel{\text{def}}{=} web\ services\ 3\ working$$

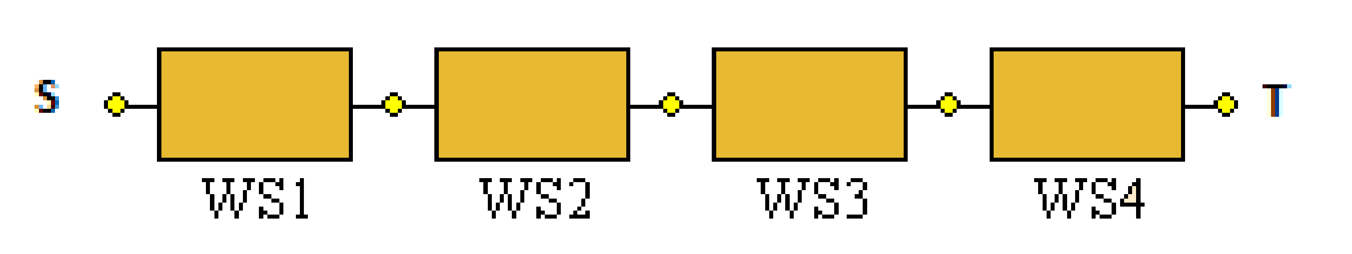
$$ws_4 \stackrel{\text{def}}{=} web\ services\ 4\ working$$

$$\varphi(ws_1, ws_2, ws_3, ws_4) = ws_1 \wedge ws_2 \wedge ws_3 \wedge ws_4$$

Reliability Block Diagram

- Example:

$$\varphi(ws_1, ws_2, ws_3, ws_4) = ws_1 \wedge ws_2 \wedge ws_3 \wedge ws_4$$



  – a) $\sum_{i=1}^{n} \lambda_i$

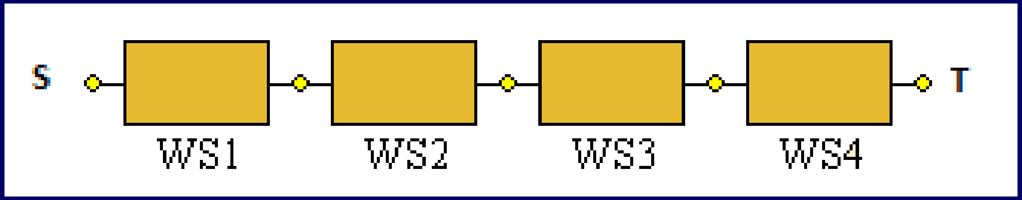
$$\begin{aligned} \lambda_s &= 0.00001 + 0.00002 + 0.00003 + 0.00004 \\ &= 0.0001 \text{ failures per hour} \end{aligned}$$

  – b) MTTF= $1 / \sum_{i=1}^{n} \lambda_i$

$$\mathrm{MTTF}_s = \frac{1}{0.0001} = 10{,}000 \text{ h}$$

Reliability Block Diagram

- Example:
  - c)



$$\phi(x_1,x_2,x_3) = x_1 x_2 x_3 x_4$$

$$P\{\,\phi(x_1,x_2,x_3) = 1\} = E\{\phi(x_1,x_2,x_3)\} = E\{x_1 x_2 x_3 x_4\}$$

If the components are independent, then:

$$P\{\,\phi(x_1,x_2,x_3) = 1\} = E\{x_1\}\,E\{x_2\}\,E\{x_3\}\,E\{x_4\} =$$

As

$P\{\,\phi(x_1,x_2,x_3) = 1\} = R(t)$, then

$$P\{\,\phi(x_1,x_2,x_3) = 1\} = R(t) = r_1(t) r_2(t) r_3(t) r_4(t)$$

And, since $r_i(t) = e^{-\lambda_i t}$, therefore:

$$R(t) = e^{-\lambda_1 t} \times e^{-\lambda_2 t} \times e^{-\lambda_3 t} \times e^{-\lambda_4 t} = e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t}$$

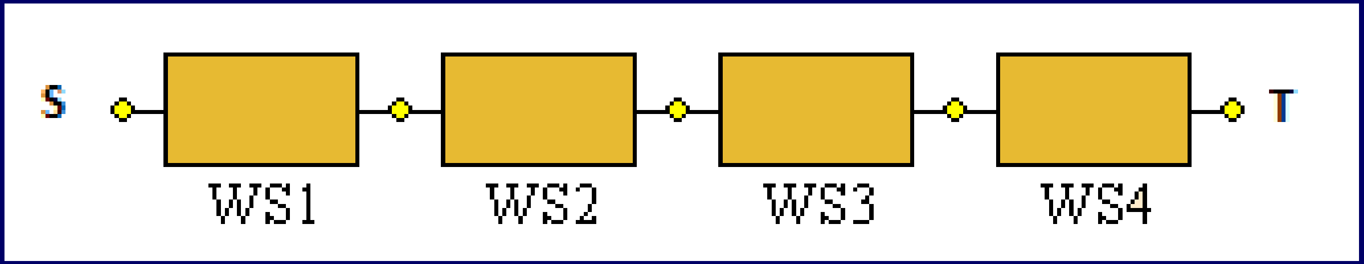
$$R(730h) = e^{-(0.00001+0.00002+0.00003+0.00004)\times 730} = 0.929600830$$

Reliability Block Diagram

- Problem:

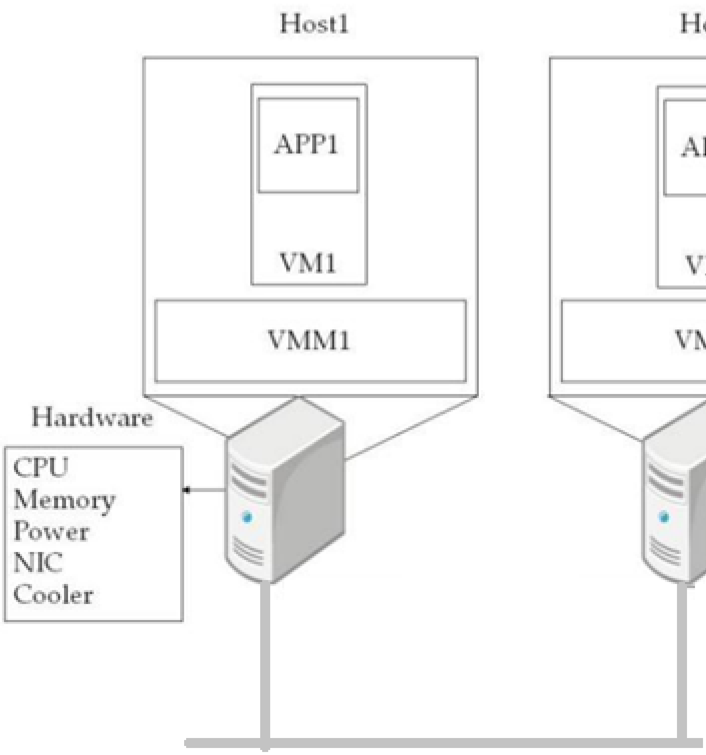
Now, considering the previous example, suppose that the repairing time of each web service is exponentially distributed with average 2h.

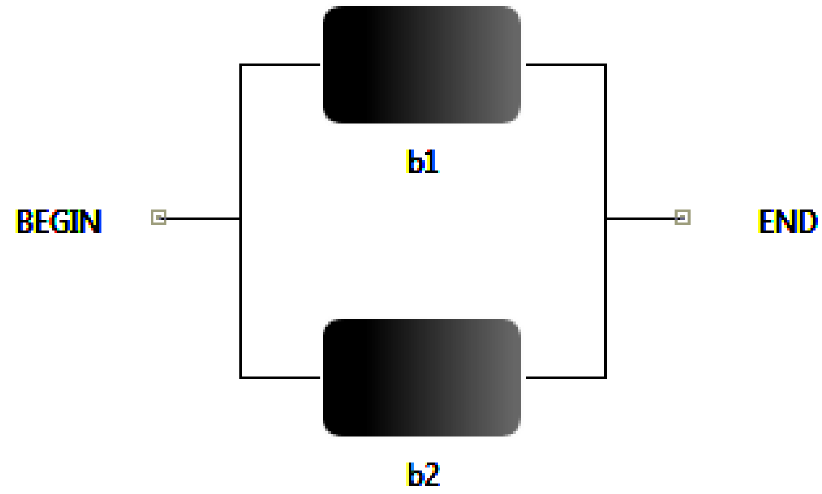
a) Compute the steady state availability.
b) Compute the downtime in minutes in one year period.



Reliability Block Diagram

- Parallel





Operational mode: $OM_3 \stackrel{\text{def}}{=} H_1 \vee H_2$

Logical function: $\varphi(s_{h1}, s_{h2}) = s_{h1} \vee s_{h2}$

Structure function: $\phi(x_{h1}, x_{h2}) = [1 - ((1 - x_{h1}) \times (1 - x_{h2}))]$

Reliability Block Diagram

- Parallel

$$P\{\phi(\mathbf{x})=1\} = P\{\phi(x_1,x_2,\ldots,x_i,\ldots,x_n)=1\} = 1-\prod_{i=1}^{n}P\{x_i=0\} = 1-\prod_{i=1}^{n}(1-P\{x_i=1\}) =$$

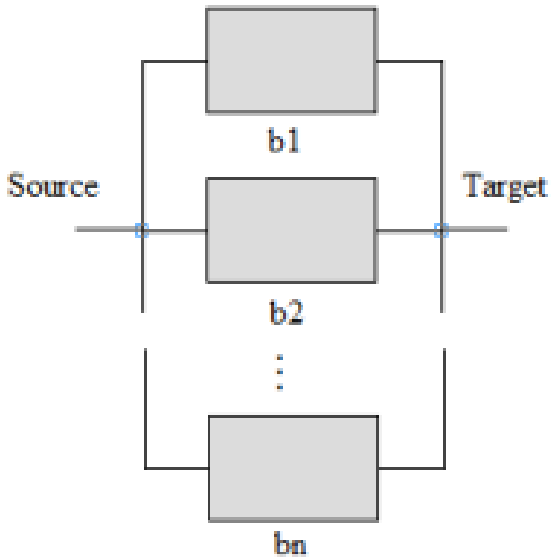
$$P\{\phi(\mathbf{x})=1\} = 1-\prod_{i=1}^{n}(1-p_i).$$

Thus $P\{\phi(\mathbf{x})=1\} = 1-(1-p_i)^n.$

The system reliability is then:

$$R_P(t) = 1-\prod_{i=1}^{n}P\{x_i(t)=0\} = 1-\prod_{i=1}^{n}(1-P\{x_i(t)=1\})$$

$$R_P(t) = 1-\prod_{i=1}^{n}Q_i(t) = 1-\prod_{i=1}^{n}1-R_i(t) \ ,$$



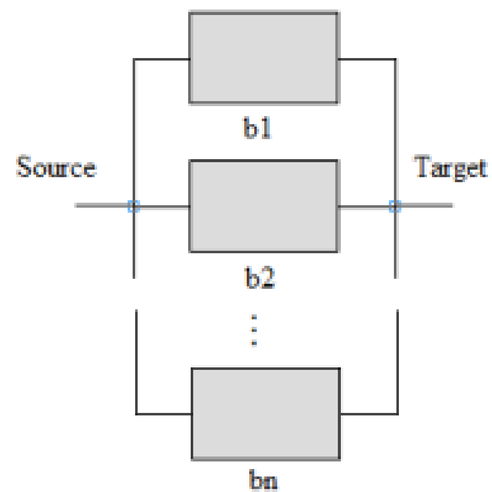
such that,

$$Q_i(t) = P\{x_i(t)=0\} = 1-P\{x_i(t)=1\} = 1-R_i(t),$$

where $R_i(t)$ and $Q_i(t)$ are the reliability and the unreliability of block b_i, respectively.

Reliability Block Diagram

- Parallel



Similarly, the system instantaneous availability is

$$A_P(t) = P\{\phi(\mathbf{x}, \mathrm{t}) = 1\} = 1 - \prod_{i=1}^{n} P\{x_i(t) = 0\} = 1 - \prod_{i=1}^{n} 1 - A_i(t),$$

$$A_P(t) = P\{\phi(\mathbf{x}, \mathrm{t}) = 1\} = 1 - \prod_{i=1}^{n} UA_i(t) = 1 - \prod_{i=1}^{n} 1 - A_i(t),$$

such that, $UA_i(t) = P\{x_i(t) = 0\} = 1 - P\{x_i(t) = 1\} = 1 - A_i(t)$,

where $A_i(t)$ and $UA_i(t)$ are the instantaneous availability and unavailability of block b_i, respectively.

The steady state availability is

$$A_P = P\{\phi(\mathbf{x}) = 1\} = 1 - \prod_{i=1}^{n} UA_i = 1 - \prod_{i=1}^{n} 1 - A_i,$$

where A_i and UA_i are the steady availability and unavailability of block b_i, respectively.

Due to the importance of the parallel structure, the following simplifying notation is adopted:

$$P\{\phi(\mathbf{x}) = 1\} = 1 - \prod_{i=1}^{n}(1 - P\{x_i = 1\}) = \coprod_{i=1}^{n} P\{x_i = 1\} = \coprod_{i=1}^{n} p_i = 1 - (1 - p_i)^n.$$

Reliability Block Diagram

Examples

- Parallel

For a parallel system with n independent and identical components with rate λ

$$R_{\text{ps}}(t) = 1 - (1 - e^{-\lambda t})^n$$

and system

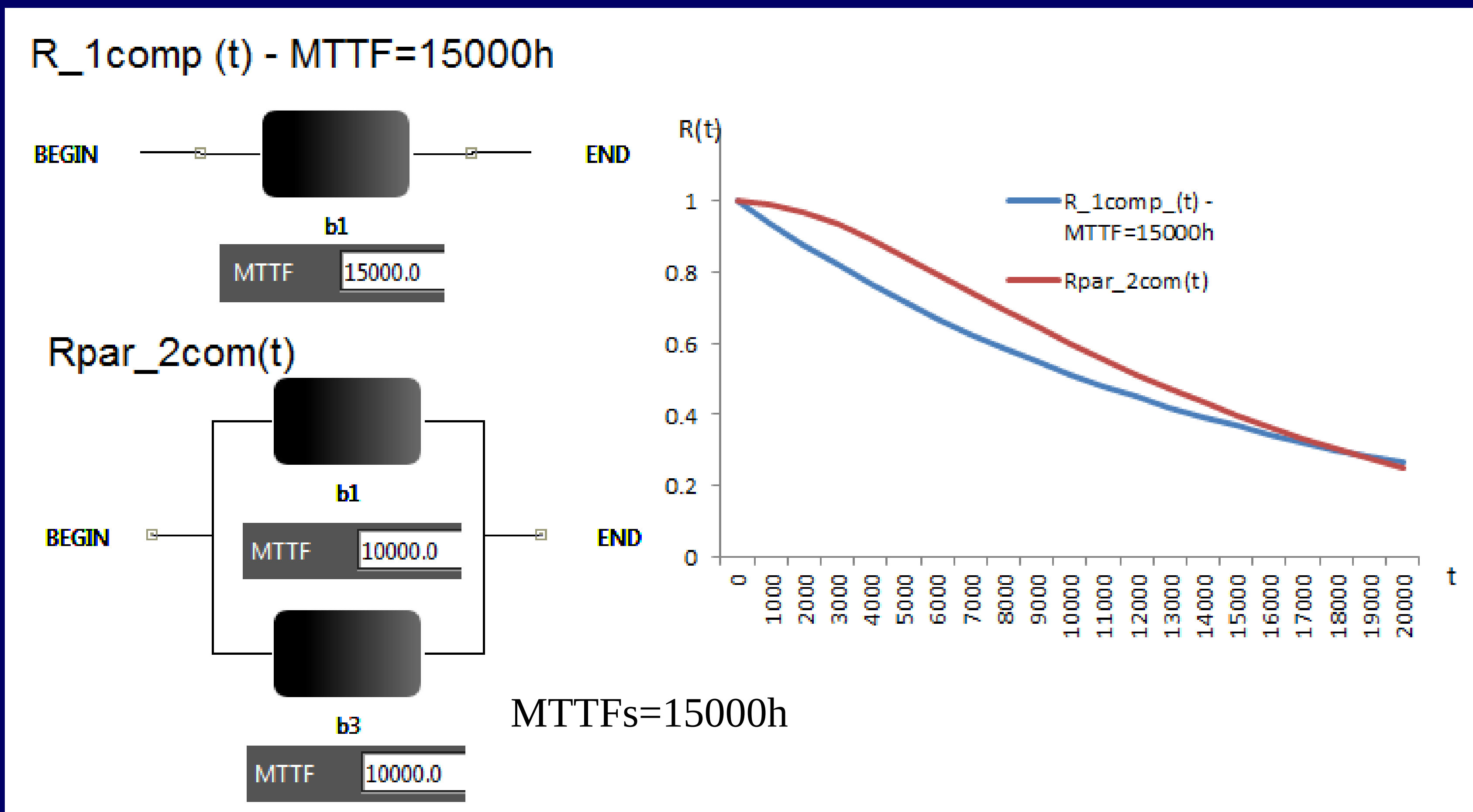
$$MTTF = \int_0^{\infty} R(t) \times dt = \int_0^{\infty} [1 - (1 - e^{-\lambda t})^n] dt = \frac{1}{\lambda} \sum_{i=1}^{n} \frac{1}{i}$$

Comp Excel

Mathematica

Reliability Block Diagram

- Example



Reliability Block Diagram

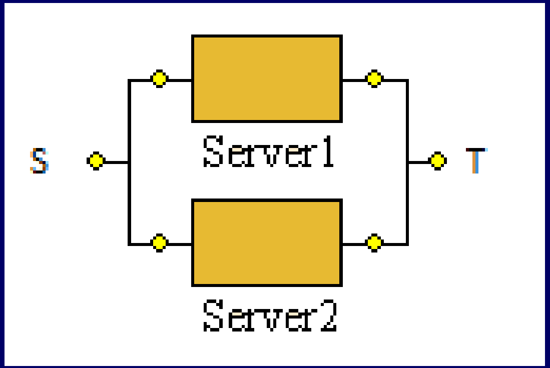
- Example

The system works when at least one server works.

$$s_1 \stackrel{\text{def}}{=} \textit{server 1 working}$$

$$s_2 \stackrel{\text{def}}{=} \textit{server 2 working}$$

$$\varphi(s_1, s_2) = s_1 \vee s_2 \Leftrightarrow \overline{\varphi(s_1, s_2)} = \bar{s_1} \wedge \bar{s_2}$$



We know that

$$P\{\phi(\mathbf{x}) = 1\} = 1 - (1 - p_1)(1 - p_2)$$

As

$P\{\phi(\mathbf{x}) = 1\}$ can be $R(t)$, $A(t)$, A

Reliability Block Diagram

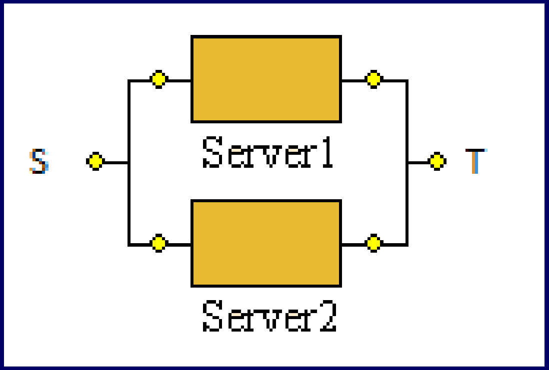
- Example

We know that

$$P\{\phi(\mathbf{x}) = 1\} = 1 - (1 - p_1)(1 - p_2)$$

As

$P\{\phi(\mathbf{x}) = 1\}$ can be $R(t)$, $A(t)$, A



– a)

$$\begin{aligned} R(t) &= 1 - (1 - R_1(t))(1 - R_2(t)) \\ &= R_1(t) + R_2(t) - R_1(t)R_2(t) \\ &= e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1 + \lambda_2)t} \end{aligned}$$

Reliability Block Diagram

Examples

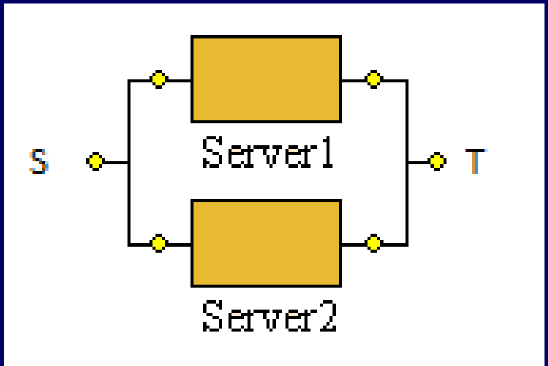
- Example

We know that

$$P\{\phi(\mathbf{x}) = 1\} = 1 - (1 - p_1)(1 - p_2)$$

As

$P\{\phi(\mathbf{x}) = 1\}$ can be $R(t)$, $A(t)$, A



– b)

$$MTTF_p = \int_0^\infty R(t)dt = \int_0^\infty (e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1+\lambda_2)t})dt$$
$$= \frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1 + \lambda_2}$$

– c)

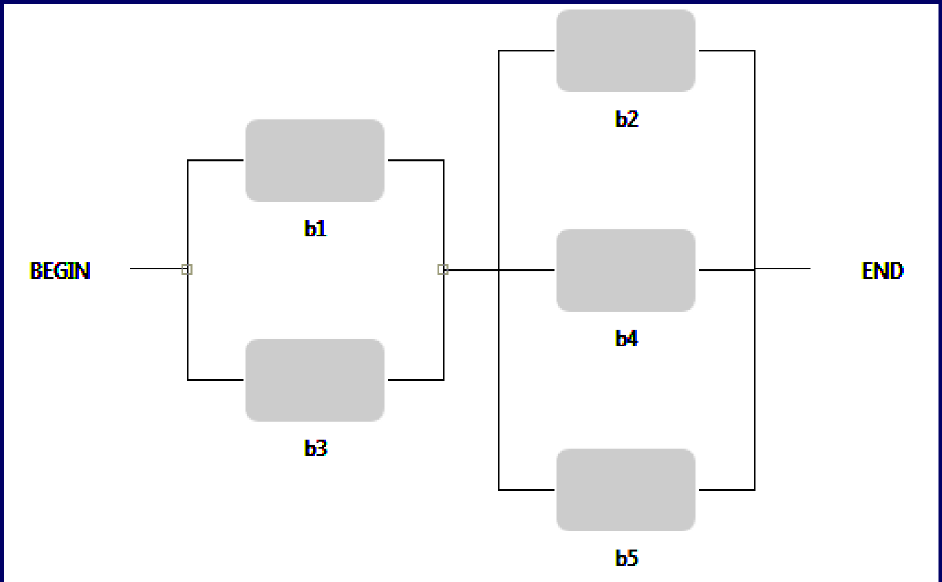
$$R(730h) = 0.9997906870$$

$$MTTF = 105\ 000h$$

Reliability Block Diagram

- Series-Parallel System
  - Series-parallel system: n stages in series, stage i with n_i parallel components.
  - For $i=1,\ldots n$, $R_{ij} = R_j$, $n_i \geq j \geq 1$
  - Reliability of series-parallel system is given by

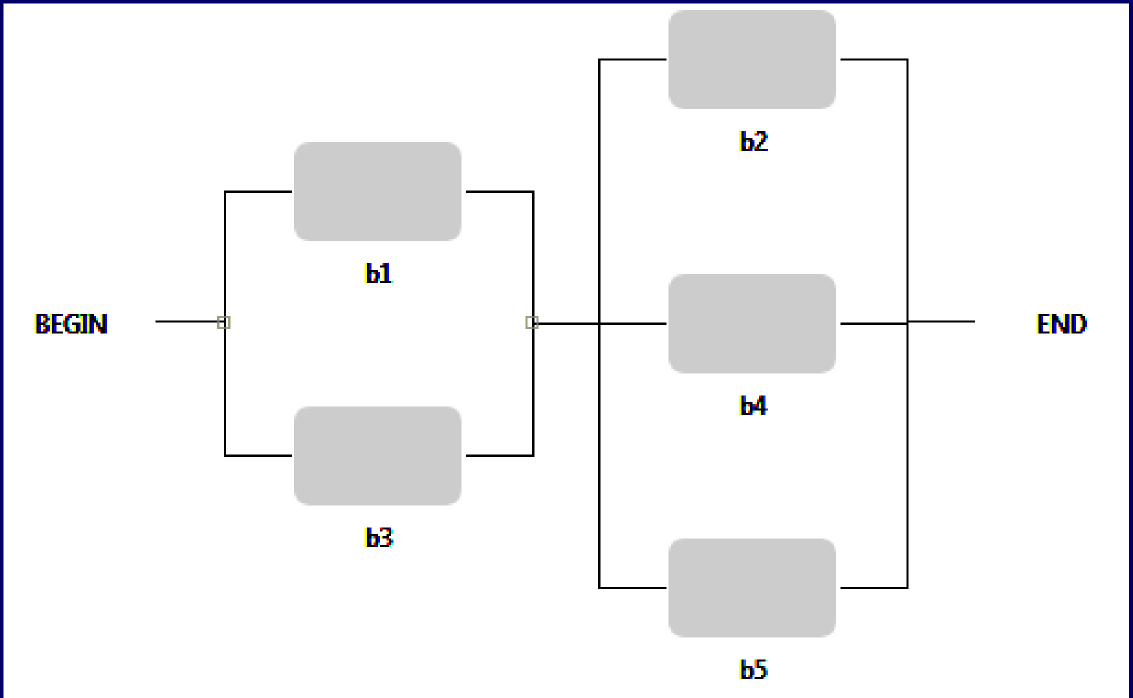
$$R_{sp} = \prod_{i=1}^{n} [1 - (1 - R_i)^{n_i}]$$



Reliability Block Diagram

- Series-Parallel System

Example:

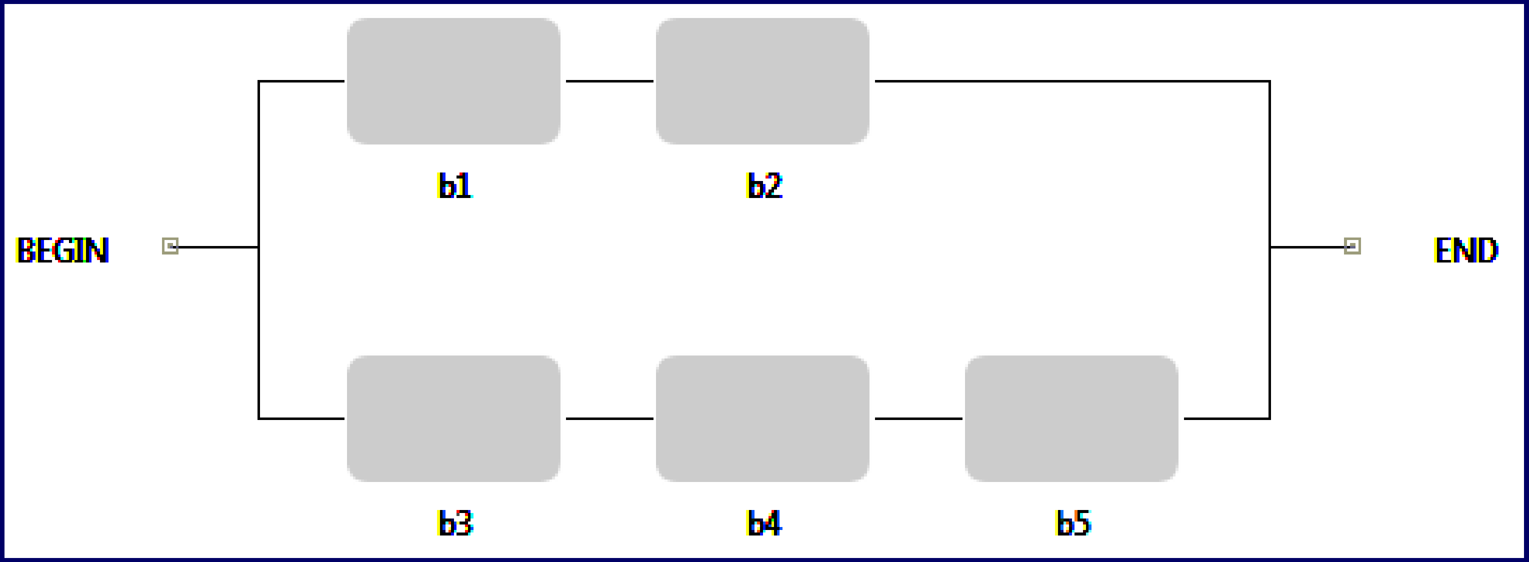


$$P = (1 - (1 - p_1)(1 - p_3)) \times (1 - (1 - p_2)(1 - p_4)(1 - p_5))$$

Reliability Block Diagram

- Series-Parallel System

Example:

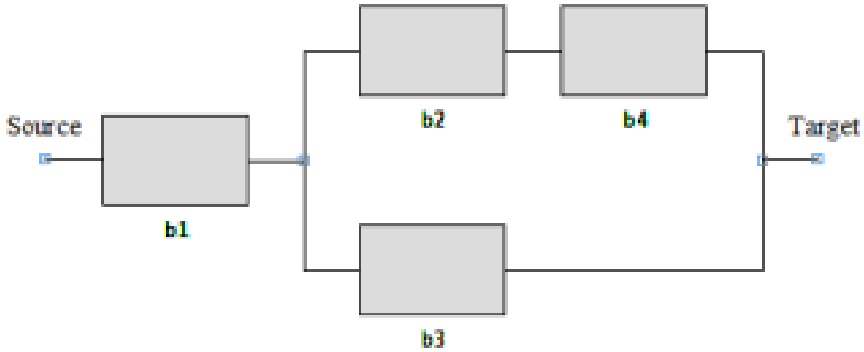


$$P = (1 - (1 - p_1 p_2)(1 - p_3 p_4 p_5))$$

Reliability Block Diagram

- Example:

Consider a system S_1 represented by four blocks (b_1, b_2, b_3, b_4) where each block has r_1, r_2, r_3 and r_4 as their respective reliabilities.



RBD of System S_1

The system reliability of the system S_1 is

$$R_{S_1} = r_1 \times [1 - (1 - r_2 \times r_4) \times (1 - r_3)].$$

Reliability Block Diagram

- Problem

Assume that the constant failure rates of web services 1, 2, 3, and 4 of sw system are $\lambda 1 = 0.00001$ failures per hour, $\lambda 2 = 0.00002$ failures per hour, $\lambda 3 = 0.00003$ failures per hour, and $\lambda 4 = 0.00004$ failures per hour, respectively. The sw system provides the proper service if the web services 1 or 3 are up and the web services 2 or 4 are up.

a) Calculate MTTF of sw system.
b) Calculate the R(t) at 730h

Reliability Block Diagram

- Problem

Now, considering the previous example, suppose that the repairing time of each web service is exponentially distributed with average 2h.

a) Compute the steady state availability.
b) Compute the downtime in hours in one year period.

Reliability Block Diagram

- K out of N

Sequence of Bernoulli trials: n independent repetitions.

- n consecutive executions of an **if-then-else** statement

S_n: sample space of n Bernoulli trials

$$
\begin{aligned}
S_1 &= \{0, 1\} \\
S_2 &= \{(0,0), (0,1), (1,0), (1,1)\} \\
S_n &= \{2^n \ n\text{-tuples of 0s and 1s}\}
\end{aligned}
$$

Reliability Block Diagram

- K out of N

Consider that event
$A \stackrel{\text{def}}{=} Success,$
thus, $\bar{A} \stackrel{\text{def}}{=} Failure.$

A_i is a success at the i^{th} repetition an experiment.

Consider $s \in S_n$, such that, $s = (\underbrace{1, 1, \ldots, 1}_{k}, \underbrace{0, 0, \ldots, 0}_{n-k})$

$$s = A_1 \wedge A_2 \wedge \ \ldots A_k \wedge \overline{A}_{k+1} \wedge \ \ldots \wedge \overline{A}_n$$

$$P(s) = P(A_1)P(A_2)\ldots P(A_k)P(\overline{A}_{k+1})\ldots P(\overline{A}_n)$$

$$= p^k q^{n-k}$$

If each event A_i is independent, and $P(A_i) = p, P(\overline{A}_i) = q$

P(s): Prob. of sequence of *k* successes followed by (*n-k*) failures. What about any sequence of *k* successes out of *n* trials?

Reliability Block Diagram

- K out of N

k 1's can be arranged in $\binom{n}{k}$ different ways,

$$\begin{aligned} p(k) &= P(\text{Exactly } k \text{ successes and } n-k \text{ failures}) \\ &= \binom{n}{k} p^k (1-p)^{n-k} \end{aligned}$$

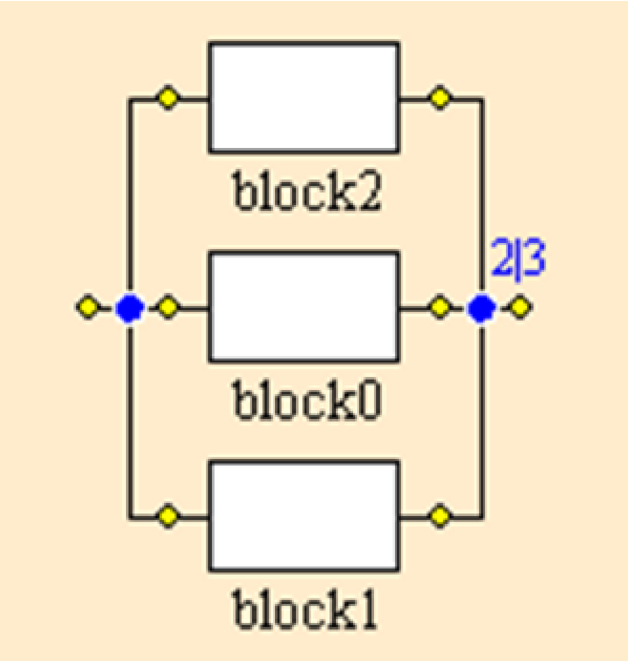
k=*n*, reduces to Series system $p(n) = p^n$

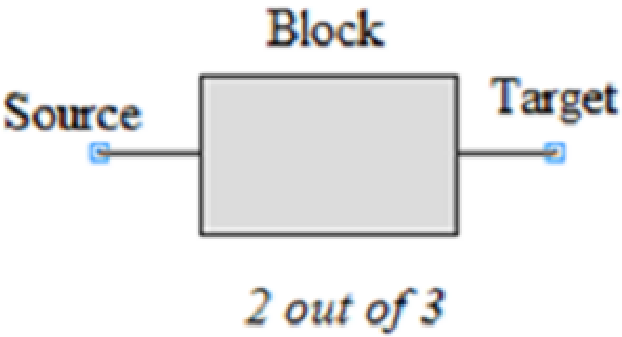
k=*1*, reduces to Parallel system $p(1) = 1-(1-p)^n$

Reliability Block Diagram

Example: 2 out of 3 system

n statistically identical components; also statistically independent



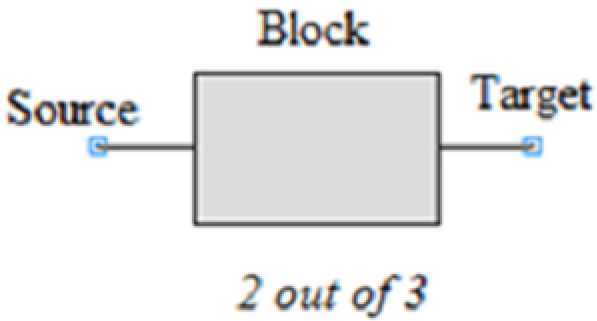


Reliability Block Diagram

Example: 2 out of 3 system

n statistically identical components; also statistically independent

$$\sum_{i=k}^{n} \binom{n}{i} p^i (1-p)^{n-i}$$



If $n = 3$ and $k = 2$, then

$$\sum_{i=2}^{3} \binom{3}{i} p^i (1-p)^{n-i} =$$

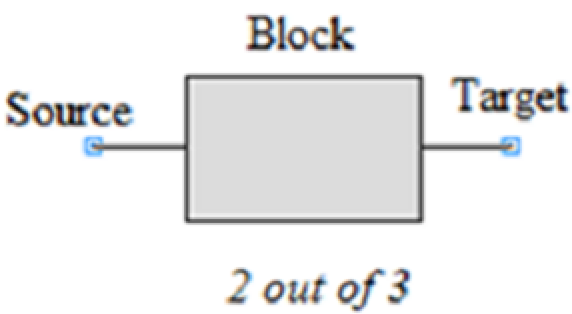
$$\binom{3}{2} p^2 (1-p)^{3-2} + \binom{3}{3} p^3 (1-p)^{3-3} =$$

$$3p^2(1-p) + p^3 = 3p^2 - 2p^3.$$

Reliability Block Diagram

Example: 2 out of 3 system

n statistically identical components; also statistically independent



$$R_S(t) = \sum_{x=k}^{n} \binom{n}{x} e^{-\lambda t x} (1 - e^{-\lambda t})^{n-x}$$

$$\text{MTTF} = \sum_{x=k}^{n} \binom{n}{x} \int_0^{\infty} e^{-\lambda t x} (1 - e^{-\lambda t})^{n-x} \, dt$$

$$\text{MTTF} = \frac{1}{\lambda} \sum_{x=k}^{n} \frac{1}{x}$$

Reliability Block Diagram

Examples

- 2 out of 3

Assume independence and that the reliability of a single component is: $R_{Simplex}(t) = e^{-\lambda t}$

we get: $R_{2oo3}(t) = 3e^{-2\lambda t} - 2e^{-3\lambda t}$

$$E[X] = \int_0^\infty R_{2oo3}(t)dt = \int_0^\infty 3e^{-2\lambda t}dt - \int_0^\infty 2e^{-3\lambda t}dt$$

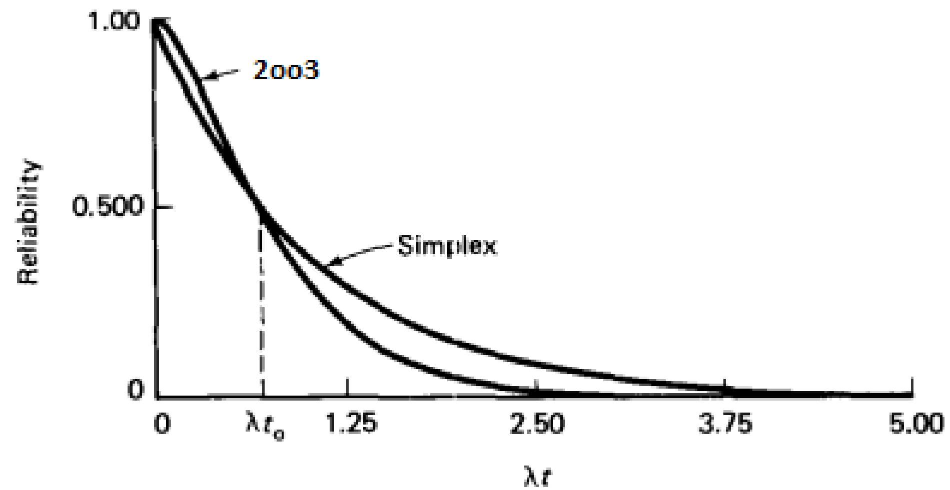
$$= \frac{5}{6\lambda} = MTTF_{2oo3}$$

Comparing with expected life of a single component: $MTTF_{2oo3} = \frac{5}{6\lambda} < \frac{1}{\lambda} = MTTF_{Simplex}$

Reliability Block Diagram

Examples

- 2 out of 3



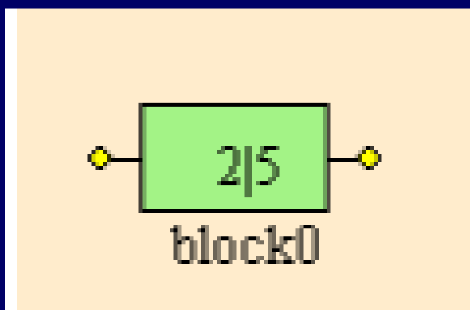
Comparison of 2oo3 and simplex reliabilities

Thus 2oo3 actually reduces (by 16%) the MTTF over the simplex system.

Although 2oo3 has lower MTTF than does Simplex, it has higher reliability than Simplex for “short” missions, defined by mission time $t<(ln2)/\lambda$.

Reliability Block Diagram

- Example: 2 out of 5



$$\lambda = 0.1 \stackrel{\text{def}}{=} a\ component\ failure\ rate$$

$$\mu = 0.9 \stackrel{\text{def}}{=} a\ component\ repair\ rate$$

$$A = \frac{\mu}{(\mu + \lambda)} \stackrel{\text{def}}{=} a\ Componet\ Availability$$

$$A_B = \sum_{i=k}^{n} \binom{n}{i} A^i \times (1-A)^{(n-i)}$$

$$A_B = \sum_{k=2}^{5} \binom{5}{2} \times A^k (1-A)^{5-k}$$

$$= 0.0081 + 0.0729 + 0.32805 + 0.59049 = 0.99954$$

Block Availability =

```
*********  Outputs asked for the model: 2oo5 **************
Steady-State Availability
SS_Avail:   9.99540000e-001
```

Reliability Block Diagram

- Example

For a system with 6 HDDs in a RAID-0 disk set, if the reliability of each HDD at t=3 years is 0.9, the reliability of the RAID set is

$$R_{\text{RAID set}}(t) = \prod_{i=1}^{6} R_{HDD}(t)$$

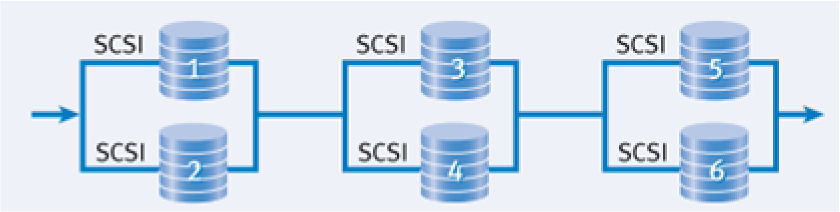
$$R_{\text{RAID set}}(3\ years) = \prod^{6} R_{HDD}(3\ years) =$$

$$R_{\text{RAID set}}(3\ years) = \prod_{i=1}^{6} 0.9 = 0.531441$$

Reliability Block Diagram

- Example

Consider the reliability of each HDD at t=3 years as 0.9. For a storage system with 6 HDDs configured as RAID-1 array, what is the storage system reliability at t= 3 years?



$$R_{\text{RAID}-1\ \text{set}}(t) = \prod_{i=1}^{\#\ of\ RAID\ sets} R_{\text{RAID}-1}{}^{i}(t)$$

$$R_{\text{RAID}-1}(t) = 1 - \left(1 - R_{HDD}(t)\right)^2 = 0.99$$

$$R_{\text{RAID}-1\ \text{set}}(t) = \prod_{i=1}^{3} \left(R_{\text{RAID}-1}{}^{i}(t)\right)$$

$$R_{\text{RAID}-1\ \text{set}}(t) = 0.99 \times 0.99 \times 0.99 = 0.97029899$$

Reliability Block Diagram

RAID-5 can tolerate one HDD failure in an array of n HDDs. For example, if the parity HDD fails, the remaining data HDDs are not affected, but redundancy is lost. If a data HDD fails, the RAID controller uses the remaining data HDDs and the parity HDD to recalculate the missing data on the fly. System performance slightly degrades until the failed HDD is replaced; however, no data is lost.

All data in the RAID set will be lost if another HDD fails before the failed HDD is restored.

The mathematical relationship that evaluates the reliability of n HDDs in a RAID-5 configuration is

$$R_{\text{RAID}-5\text{ set}}(t) = \sum_{j=n-1}^{n} \binom{n}{j} R_{HDD}^{j}(t) \times \left(1 - R_{HDD}^{j}(t)\right)^{n-j}$$

Reliability Block Diagram

- Example

For a storage system with 14 HDDs, one possible configuration is 13 HDDs dedicated to RAID-5 with the remaining HDD available for failover. The reliability for this configuration is (in which 12 of 13 HDDs must operate)

$$R_{\text{RAID}-5\text{ set}}(t) = \sum_{j=12}^{13} \binom{13}{j} R_{HDD}^{j}(t) \times \left(1 - R_{HDD}^{j}(t)\right)^{13-j}$$

$$R_{\text{RAID}-5\text{ set}}(3\ years) = \frac{13!}{12!\,(13-12)!} \times 0.9^{12} \times (1-0.99)^{13-12} + \frac{13!}{13!\,(13-13)!} \times 0.9^{13} \times (1-0.99)^{13-13} =$$

$$R_{\text{RAID}-5\text{ set}}(3\ years) = 0.6213$$

Reliability Block Diagram

- Importance Indices

Reliability Importance

The *reliability importance*, or Birnbaum importance (B-importance), of component i is defined as

$$I_i^B = \frac{\partial R_s(\mathbf{p})}{\partial p_i} \qquad 0 \le p_i \le 1$$

p_i is the reliability of component i, $\mathbf{p}$ is the vector of component reliabilities, and R_s is the reliability of the system.

$$I_i^B = R_s(1_i, \mathbf{p}^i) - R_s(0_i, \mathbf{p}^i),$$

where $\mathbf{p}^i$ represents the component reliability vector with the ith component removed.

$$I_i^B = E(\phi(1_i, \mathbf{x}^i) - \phi(0_i, \mathbf{x}^i)) = \Pr(\phi(1_i, \mathbf{x}^i) - \phi(0_i, \mathbf{x}^i) = 1)$$

where ϕ is the structural function of the system.

Reliability Block Diagram

- Importance Indices

Normalized Reliability Importance

$$I_{n_i}^{B} = \frac{I_i^B}{I_x}$$

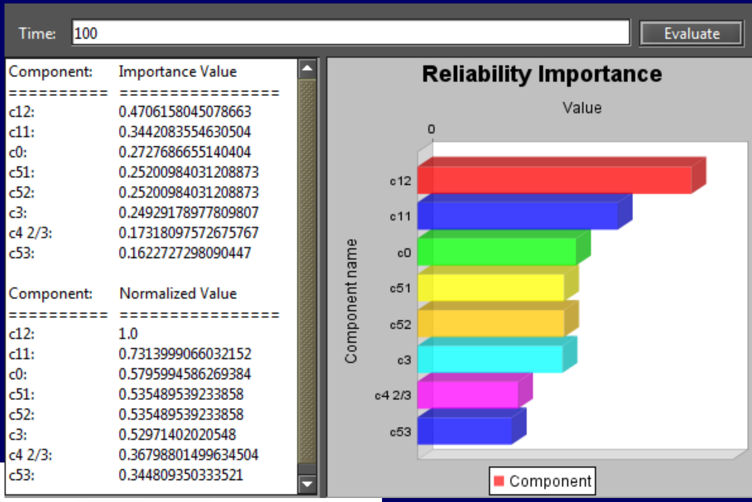
where $I_{n_i}^{B}$ is normalized reliability importance and $I_x = \max_{\forall i}\{I_i^B\}$.

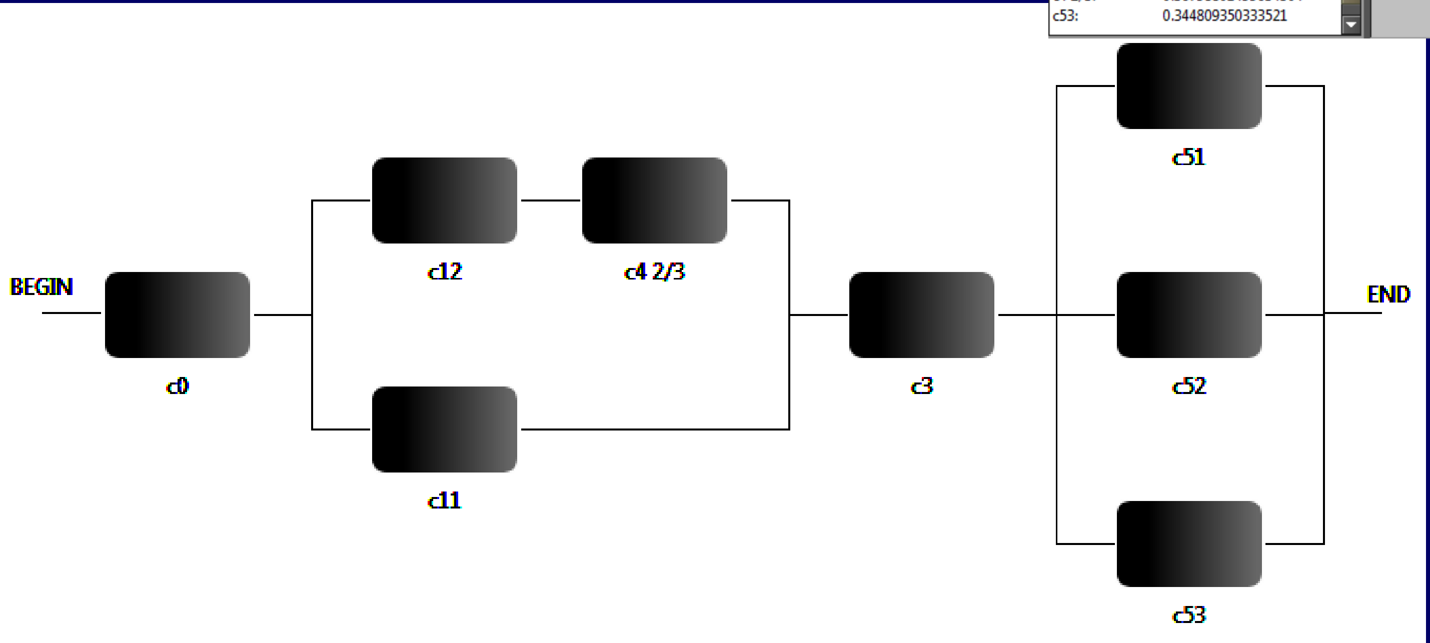
Reliability Block Diagram

- Importance Indices

Excel

Mercury RI_RBD





Component i	C0	C11	C12	C3	C4	C51	C52	C53
Component's failure rate	0.001	0.02	0.01	0.0001	0.01	0.01	0.01	0.04

Reliability Block Diagram

- Importance Indices

Availability Importance

$$I_i^A = A_s(1_i, \mathbf{p}^i) - A_s(0_i, \mathbf{p}^i)$$

Normalized Availability Importance

$$I_{n_i}^A = \frac{I_i^A}{I_x}$$

where $I_{n_i}^A$ is normalized availability importance and $I_x = \max_{\forall i}\{I_i^A\}$.

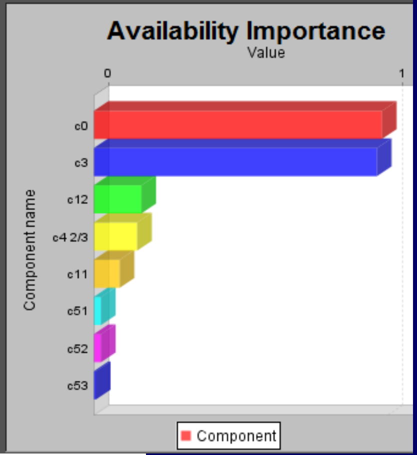
Reliability Block Diagram

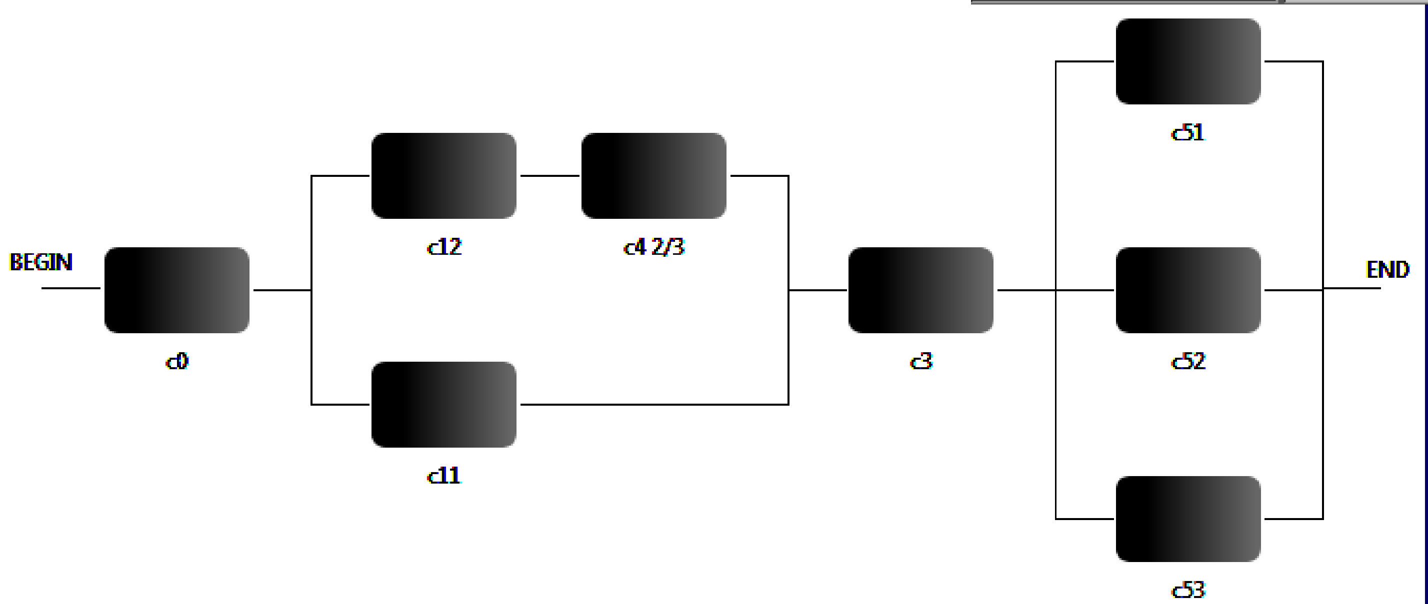
- Importance Indices

Mercury
RI_RBD

Component:	Importance Value
c0:	0.9805600622799777
c3:	0.9632560611809194
c12:	0.16268554669369795
c4 2/3:	0.1478977168822564
c11:	0.08874922218453907
c51:	0.025028798433878063
c52:	0.025028798433878063
c53:	0.00796370859259754

Component:	Normalized Value
c0:	1.0
c3:	0.9823529411764708
c12:	0.16591084315164226
c4 2/3:	0.15082983956981455
c11:	0.09050870578818113
c51:	0.025525002900568503
c52:	0.025525002900568503
c53:	0.008121591831999043





Component i	C0	C11	C12	C3	C4	C51	C52	C53
Component's failure rate	0.001	0.02	0.01	0.0001	0.0001	0.01	0.01	0.04
Component's repair rate	0.05	0.1	0.1	0.05	0.05	0.1	0.1	0.1

Reliability Block Diagram

- Importance Indices

Reliability and Cost Importance

$$I_i^{BC} = I_i^{B} \times \left(1 - \frac{C_i}{C_{Sys}}\right)$$

Availability and Cost Importance

$$I_i^{AC} = I_i^{A} \times \left(1 - \frac{C_i}{C_{Sys}}\right)$$

where C_i is the cost of component *i*, and C_{Sys} is the system cost.

Reliability Block Diagram

- Importance Indices

Normalized Reliability Cost Importance

$$I_{n_i}^{BC} = \frac{I_i^{BC}}{I_x^{BC}}$$

$$I_x^{BC} = \max_{\forall i}\left\{I_i^{BC}\right\}$$

Normalized Availability Cost Importance

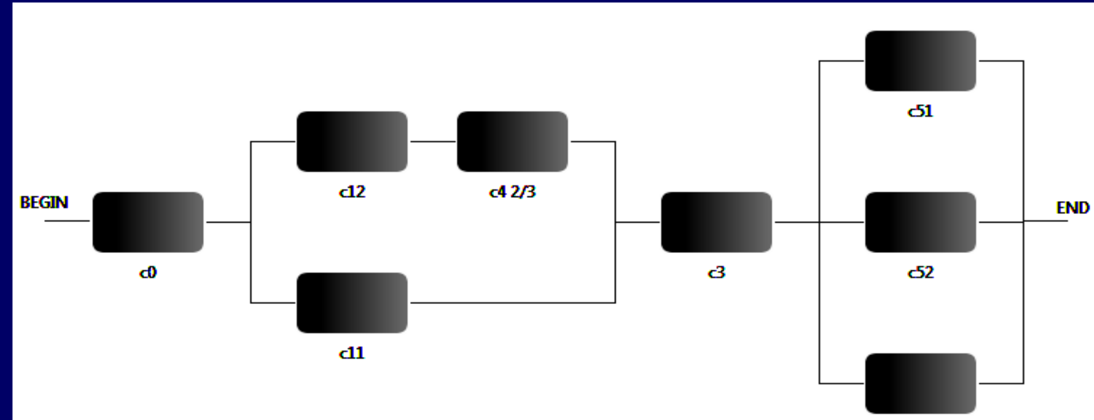
$$I_{n_i}^{AC} = \frac{I_i^{AC}}{I_x^{BC}}$$

$$I_x^{AC} = \max_{\forall i}\left\{I_i^{AC}\right\}$$

Reliability Block Diagram

- Importance Indices

Mercury
RI_RBD



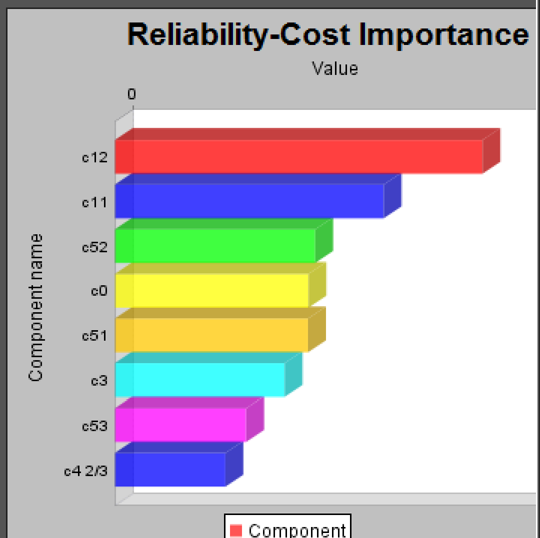
Component i	C0	C11	C12	C3	C4	C51	C52	C53
Component's failure rate	0.001	0.02	0.01	0.0001	0.0001	0.01	0.01	0.04
Component's repair rate	0.05	0.1	0.1	0.05	0.05	0.1	0.1	0.1
Component's cost ($)	1000	500	500	1200	1500	600	400	300

Time: 100

Evaluate

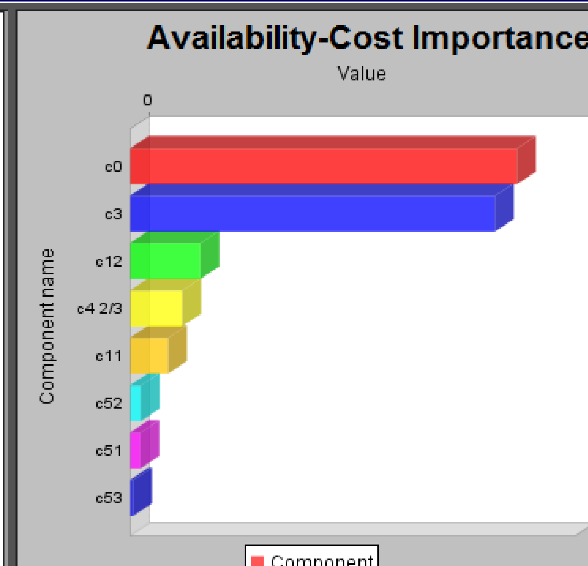
Component:	Importance Value
c12:	0.4313978207988774
c11:	0.3155243258411295
c52:	0.23520918429128282
c0:	0.22730722126170033
c51:	0.22680885628087985
c3:	0.19943343182247847
c53:	0.15415909331859246
c4 2/3:	0.12988573179506824

Component:	Normalized Value
c12:	1.0
c11:	0.7313999066032152
c52:	0.5452257126744737
c0:	0.5269085987517622
c51:	0.5257533657932425
c3:	0.462295872179328
c53:	0.35734787216383085
c4 2/3:	0.30108110317882775



Component:	Importance Value
c0:	0.8171333852333148
c3:	0.7706048489447356
c12:	0.14912841780255645
c4 2/3:	0.1109232876616923
c11:	0.0813534536691608
c52:	0.023360211871619525
c51:	0.022525918590490256
c53:	0.007565523162967663

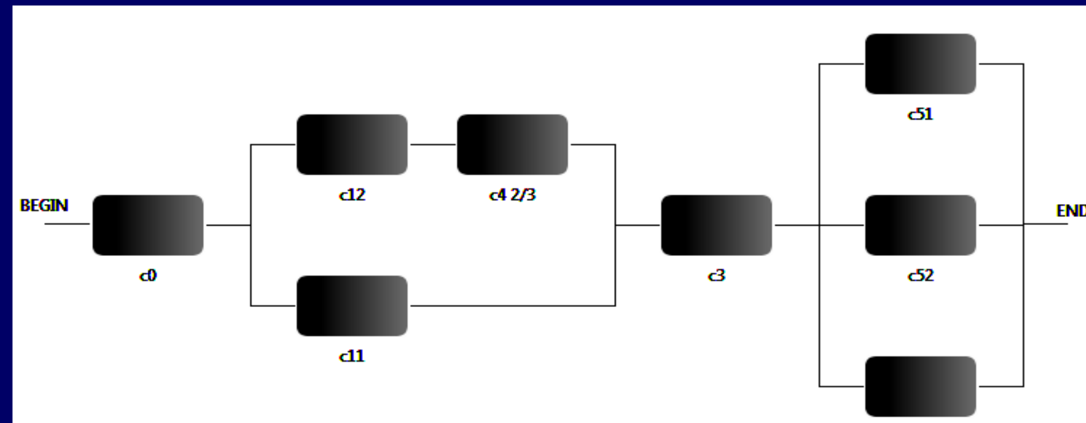
Component:	Normalized Value
c0:	1.0
c3:	0.943058823529412
c12:	0.18250192746680646
c4 2/3:	0.1357468556128331
c11:	0.09955957636699922
c52:	0.028588003248636723
c51:	0.027567003132613982
c53:	0.009258614688847891



Reliability Block Diagram

- Importance Indices

Mercury
RI_RBD

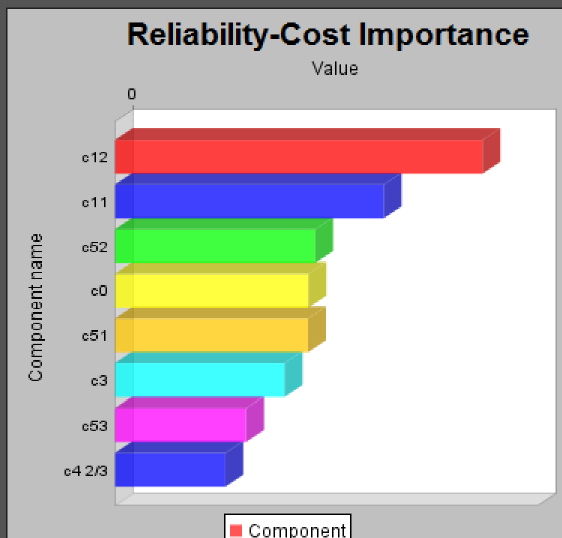


Component i	C0	C11	C12	C3	C4	C51	C52	C53
Component's failure rate	0.001	0.02	0.01	0.0001	0.0001	0.01	0.01	0.04
Component's repair rate	0.05	0.1	0.1	0.05	0.05	0.1	0.1	0.1
Component's cost ($)	1000	500	500	1200	1500	600	400	300

Time: 100 Evaluate

Component:	Importance Value
c12:	0.4313978207988774
c11:	0.3155243258411295
c52:	0.23520918429128282
c0:	0.2273072212617003
c51:	0.22680885628087985
c3:	0.19943343182247847
c53:	0.15415909331859246
c4 2/3:	0.12988573179506824

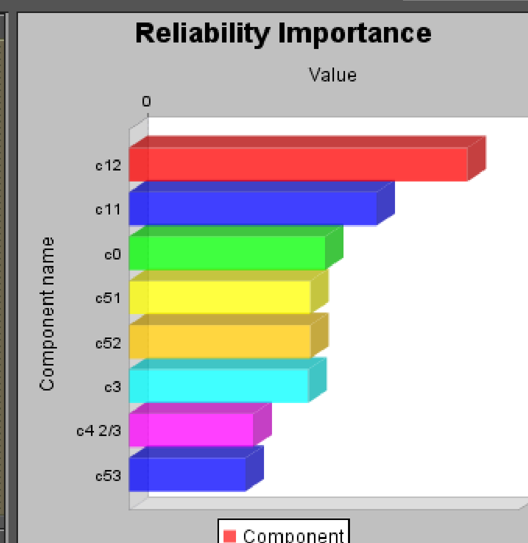
Component:	Normalized Value
c12:	1.0
c11:	0.7313999066032152
c52:	0.5452257126744737
c0:	0.5269085987517622
c51:	0.5257533657932425
c3:	0.462295872179328
c53:	0.35734787216383085
c4 2/3:	0.30108110317882775



Time: 100 Evaluate

Component:	Importance Value
c12:	0.4706158045078663
c11:	0.3442083554630504
c0:	0.2727686655140404
c51:	0.25200984031208873
c52:	0.25200984031208873
c3:	0.24929178977809807
c4 2/3:	0.17318097572675767
c53:	0.1622727298090447

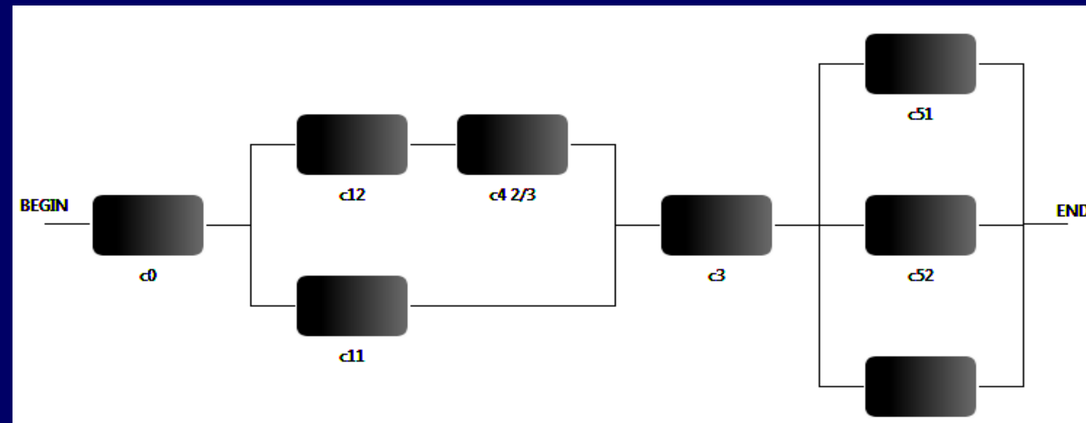
Component:	Normalized Value
c12:	1.0
c11:	0.7313999066032152
c0:	0.5795994586269384
c51:	0.535489539233858
c52:	0.535489539233858
c3:	0.52971402020548
c4 2/3:	0.36798801499634504
c53:	0.344809350333521



Reliability Block Diagram

- Importance Indices

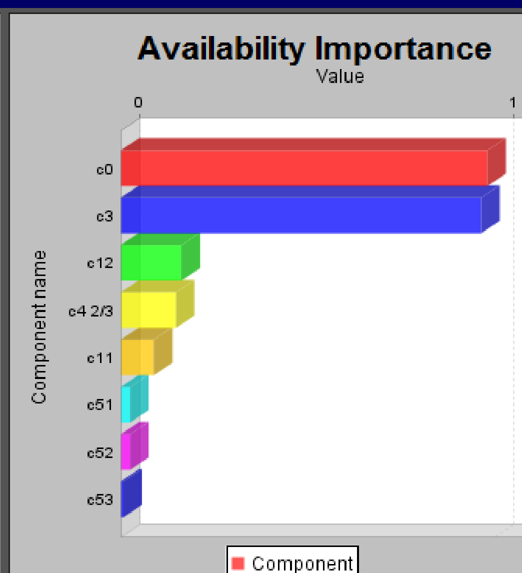
Mercury RI_RBD



Component i	C0	C11	C12	C3	C4	C51	C52	C53
Component's failure rate	0.001	0.02	0.01	0.0001	0.0001	0.01	0.01	0.04
Component's repair rate	0.05	0.1	0.1	0.05	0.05	0.1	0.1	0.1
Component's cost ($)	1000	500	500	1200	1500	600	400	300

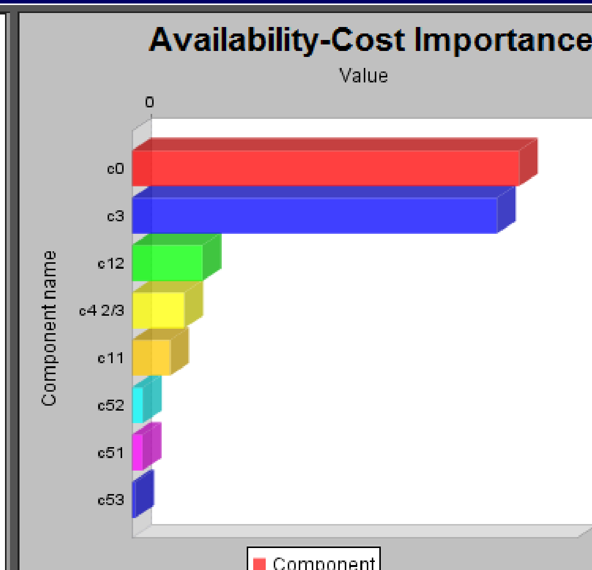
Component:	Importance Value
c0:	0.9805600622799777
c3:	0.9632560611809194
c12:	0.16268554669369795
c4 2/3:	0.1478977168822564
c11:	0.08874922218453907
c51:	0.025028798433878063
c52:	0.025028798433878063
c53:	0.00796370859259754

Component:	Normalized Value
c0:	1.0
c3:	0.9823529411764708
c12:	0.16591084315164226
c4 2/3:	0.15082983956981455
c11:	0.09050870578818113
c51:	0.025525002900568503
c52:	0.025525002900568503
c53:	0.008121591831999043



Component:	Importance Value
c0:	0.8171333852333148
c3:	0.7706048489447356
c12:	0.1491284178025645
c4 2/3:	0.110923287661692 3
c11:	0.081353453669160 8
c52:	0.023360211871619525
c51:	0.022525918590490256
c53:	0.007565523162967663

Component:	Normalized Value
c0:	1.0
c3:	0.943058823529412
c12:	0.18250192746680646
c4 2/3:	0.1357468556128331
c11:	0.09955957636699922
c52:	0.028588003248636723
c51:	0.027567003132613982
c53:	0.00925861468847891



Fault Tree

- FT is failure oriented diagram.
- The system failure is represented by the TOP event.
- The TOP event is caused by lower level events (faults, component's failures etc).
- The term event is somewhat misleading, since it actually represents a state reached by event occurrences.
- The combination of events is described by logic gates.
- The most common FT elements are the TOP event, AND and OR gates, and basic events.
- The events that are not represented by combination of other events are named basic events.

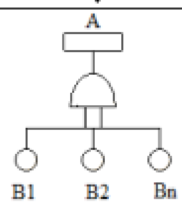
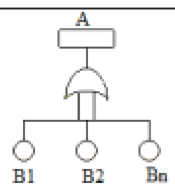
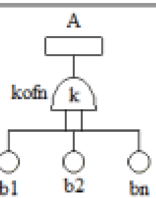
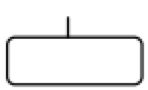
Fault Tree

- Failures of individual components are assumed to be independent for easy solution.
- In FTs, the system state may be described by a Boolean function that is evaluated as true whenever the system fails.
- The system state may also be represented by a structure function, which, opposite to RBDs, represents the system failure.
- If the system has more than one undesirable state, a Boolean function (or a structure function) should be defined for representing each failure mode.
- Many extensions have been proposed which adopt other gates such as XOR, transfer and priority gates.

Fault Tree

- Basic Symbols

Basic Symbols and their description

Symbol	Description
▭	TOP event represents the system failure.
○	Basic event is an event that may cause a system failure.
▽	Basic repeated event.
	AND gate generates an event (A) if All event B_i have occurred.
	OR gate generates an event (A) if at least one event B_i have occurred.
	KOFN gate generates an event (A) if at least K events B_i out of N have occurred.
	The comment rectangle.

Fault Tree

- Structure Function

Consider a system S composed of a set of components, $C = \{c_i | 1 \leq i \leq n\}$. Let the discrete random variable $y_i(t)$ indicate the state of component i, thus:

$$y_i(t) = \begin{cases} 1 & \text{if the component } i \text{ is faulty at time } t \\ 0 & \text{if the component } i \text{ is operational at time } t \end{cases}$$

The vector $\mathbf{y}(t) = (y_1(t), y_2(t), \dots, y_i(t), \dots, y_n(t))$ represents the state of each component of the system, and it is named state vector. The system state may be represented by a discrete random variable $\psi(\mathbf{x}(t)) = \phi(y_1(t), y_2(t), \dots, y_i(t), \dots, y_n(t))$, such that

$$\psi(\mathbf{y}(t)) = \begin{cases} 0 & \text{if the system is operational at time } t \\ 1 & \text{if the system is faulty at time } t \end{cases}$$

$\psi(\mathbf{y}(t))$ is named the Fault Tree structure function of the system.

Fault Tree

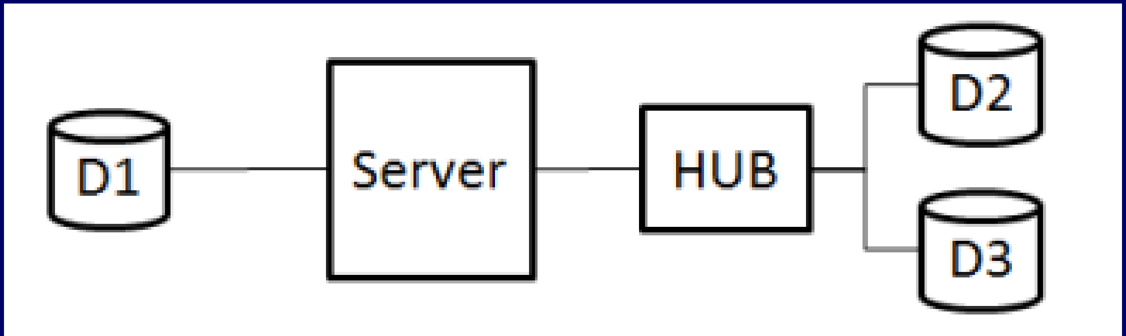
- Logical Function

FT Logic Function Ψ denotes the counterpart that represents the FT structure function (ψ) According to the notation previously introduced, s_i (a Boolean variable) is equivalent to x_i and $\overline{s_i}$ represents $1 - x_i$. The $\Psi(\mathbf{bs})$ (Logical function that describes conditions that cause a system failure) is the counterpart of $\psi(\mathbf{y}(t)) = 1$ (FT structural function – represents system failures), $\overline{\Psi(\mathbf{bs})}$ depicts of $\psi(\mathbf{y}(t)) = 0$, $\wedge$ represents $\times$, and $\vee$ is the respective counterpart of $+$.

Fault Tree

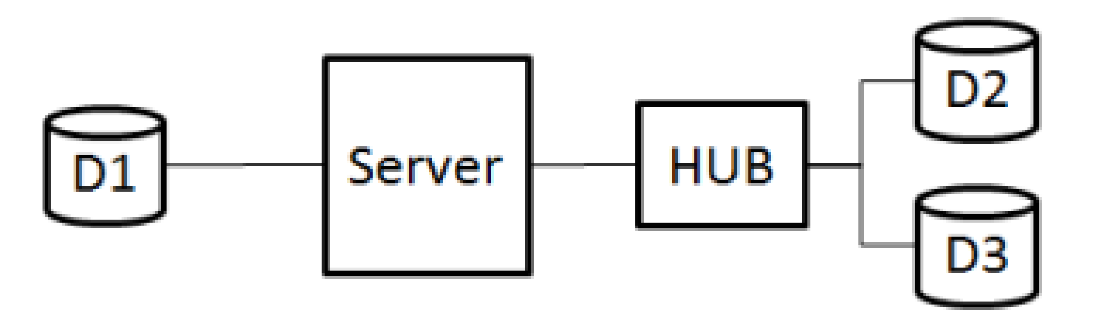
- Example

Consider a system in which software applications read, write and modify the content of the storage device D_1 (source). The system periodically replicates the production data (generated by the software application) of one storage device (D_1) in two storage replicas (targets) so as to allow recovering data in the event of data loss or data corruption. The system is composed of three storage devices (D_1, D_2, D_3), one server and hub that connects the disks D_2 and D_3 to the server



Fault Tree

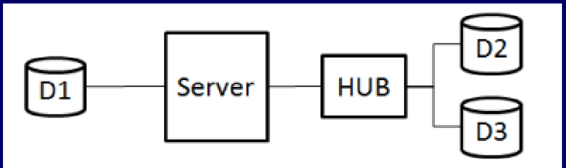
- Example



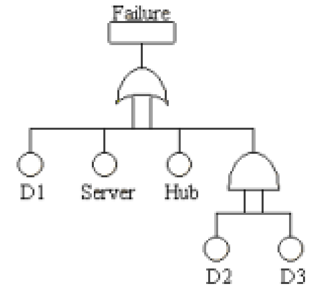
The system is considered to have failed if the hardware infrastructure does not allow the software applications to read, write or modify data on D_1, and if no data replica is available,

Hence, if D_1 or the Server
or the Hub,
or both replica storages (D_2, D_3) have failed.

Fault Tree



- Example



$$\Psi(\mathbf{bs}) = s_0 \vee s_1 \vee s_2 \vee (s_3 \wedge s_4),$$

$$\overline{\overline{s_0 \vee s_1 \vee s_2 \vee (s_3 \wedge s_4)}} =$$

$$\overline{\overline{s_0} \wedge \overline{s_1} \wedge \overline{s_2} \wedge \overline{(s_3 \wedge s_4)}} =$$

The respective FT structure function may be expressed as

$$\psi(\mathbf{y}(t)) = [1 - (1 - y_0(t)) \times (1 - y_1(t)) \times (1 - y_2(t)) \times (1 - y_3(t) \times y_4(t))].$$

if $y_0(t) = 1$ or $y_1(t) = 1$ or $y_2(t) = 1$ or $y_3(t) = y_4(t) = 1$, then $\psi(\mathbf{y}(t)) = 1$, which denotes a system failure.

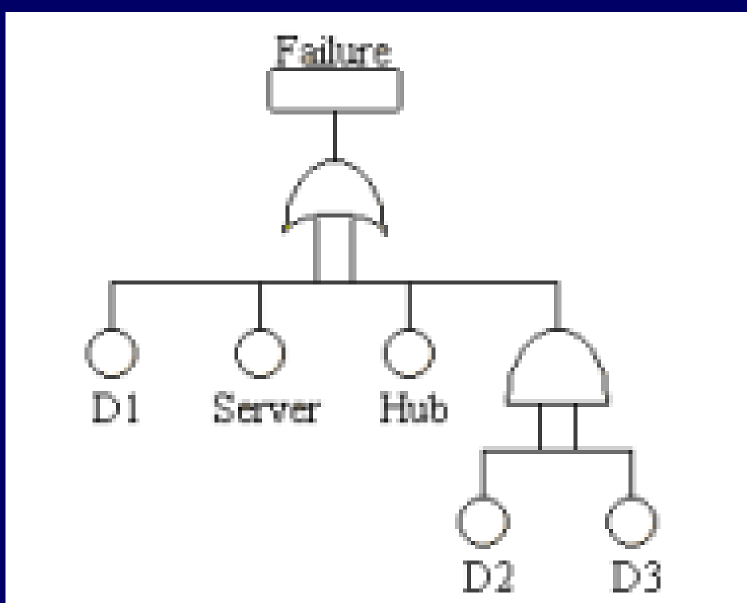
Fault Tree

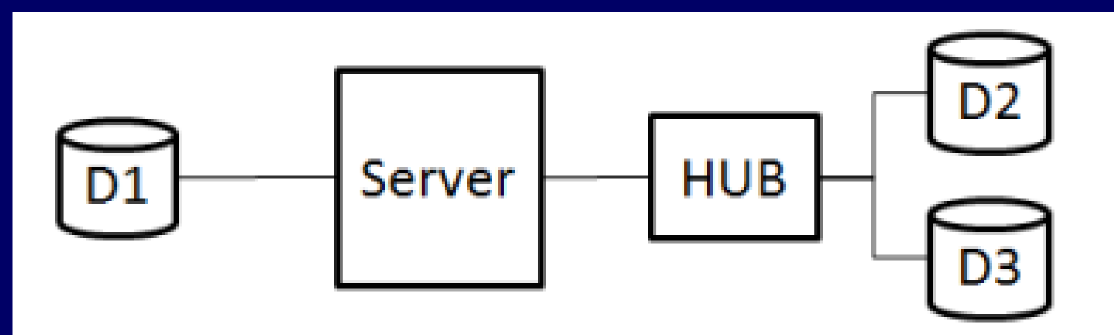
- Problem

Consider that the constant failure rates are λ_S = 0.00002, λ_H = 0.00001, λ_{D1} = 0.00008, λ_{D2} = 0.00009, and λ_{D3} = 0.00007, respectively.

a) Calculate the R(t) at 730h

b) Calculate MTTF of system.





Fault Tree

- Problem

Assume that the constant failure rates of web services 1, 2, 3, and 4 of sw system are $\lambda 1 = 0.00001$ failures per hour, $\lambda 2 = 0.00002$ failures per hour, $\lambda 3 = 0.00003$ failures per hour, and $\lambda 4 = 0.00004$ failures per hour, respectively. The sw system provides the proper service if the web services 1 or 3 are up and the web services 2 or 4 are up.

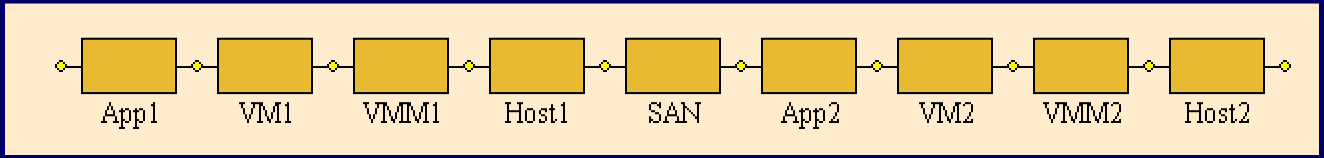
a) Calculate MTTF of sw system.
b) Calculate the R(t) at 730h

ANALYSIS METHODS

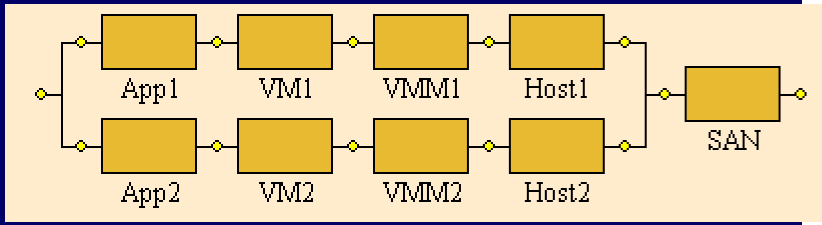
Computing the Reliability

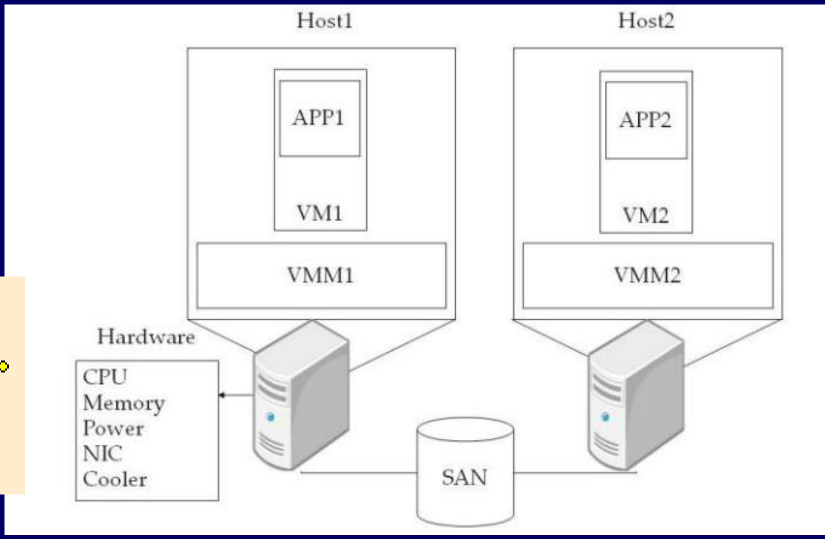
- What is the respective RBD?

This?



Or this?





Analysis by Space Enumeration

- The method by an example

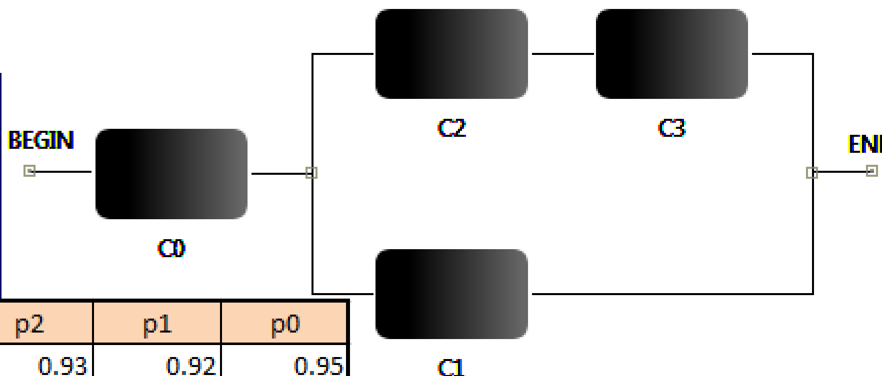
State-space enumeration method proceeds by determining the whole set of state vectors, checking for each one if the system is operational or not.

The whole set of state vectors represents all the combinations where each of the m component can be good or bad, resulting in 2^m combinations.

Each of these combinations is considered as an event E_i. These events are all mutually exclusive (disjoint) and the reliability expression is simply the probability of the union of the subset of events that contain a path between the source and the target nodes.

$$R_{s,t}(S) = \Pr(E_1 \cup E_2 \cup \ldots \cup E_m) = \Pr(E_1) + \Pr(E_2) + \cdots + P(E_m)$$

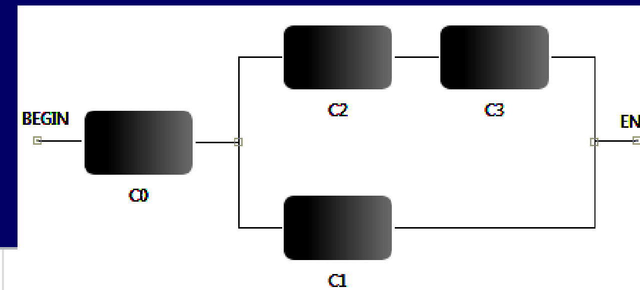
where $E_i \cap E_j = \emptyset \ \forall i, \forall j, i \neq j$



p3	p2	p1	p0
0.96	0.93	0.92	0.95

Analysis by Space Enumeration

- The method by an example



C3	C2	C1	C0	ϕ					
0	0	0	0	0	0.04	0.07	0.08	0.05	0.00000
0	0	0	1	0	0.04	0.07	0.08	0.95	0.00000
0	0	1	0	0	0.04	0.07	0.92	0.05	0.00000
0	0	1	1	1	0.04	0.07	0.92	0.95	0.00245
0	1	0	0	0	0.04	0.93	0.08	0.05	0.00000
0	1	0	1	0	0.04	0.93	0.08	0.95	0.00000
0	1	1	0	0	0.04	0.93	0.92	0.05	0.00000
0	1	1	1	1	0.04	0.93	0.92	0.95	0.03251
1	0	0	0	0	0.96	0.07	0.08	0.05	0.00000
1	0	0	1	0	0.96	0.07	0.08	0.95	0.00000
1	0	1	0	0	0.96	0.07	0.92	0.05	0.00000
1	0	1	1	1	0.96	0.07	0.92	0.95	0.05873
1	1	0	0	0	0.96	0.93	0.08	0.05	0.00000
1	1	0	1	1	0.96	0.93	0.08	0.95	0.06785
1	1	1	0	0	0.96	0.93	0.92	0.05	0.00000
1	1	1	1	1	0.96	0.93	0.92	0.95	0.78031
									0.94185
p3	p2	p1	p0						Ps
0.96	0.93	0.92	0.95						

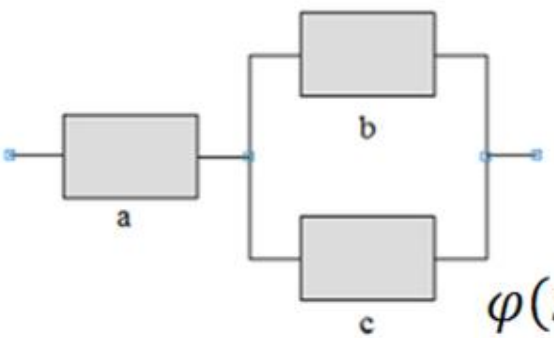
Excel

Mercury Ex.: Rel_ Enumeration

Analysis by Expected Value of the Structure Function

- The method by an example

Consider a system (C, ϕ) composed of three blocks, $C = \{a, b, c\}$



$$\varphi(s_a, s_b, s_c) = s_a \wedge (s_b \vee s_c) = s_a \wedge (\overline{\overline{s_b} \wedge \overline{s_c}})$$

$$\phi(\mathbf{x}) = x_a \times [1 - (1 - x_b) \times (1 - x_c)]$$

$$R_S = P\{\phi(\mathbf{x}) = 1\} = E[\phi(\mathbf{x})] = E\big[x_a \times [1 - (1 - x_b) \times (1 - x_c)]\big] =$$

$$R_S = P\{\phi(\mathbf{x}) = 1\} = E[x_a] \times E[1 - (1 - x_b) \times (1 - x_c)] =$$

$$R_S = P\{\phi(\mathbf{x}) = 1\} = E[x_a] \times [1 - E[(1 - x_b)] \times E[(1 - x_c)] =$$

$$R_S = P\{\phi(\mathbf{x}) = 1\} = E[x_a] \times [1 - (1 - E[x_b]) \times (1 - E[x_c])$$

$$R_S = P\{\phi(\mathbf{x}) = 1\} = p_a \times [1 - (1 - p_b) \times (1 - p_c)] = p_a \times [1 - q_b \times q_c]$$

Analysis by Expected Value of the Structure Function

- Summary of the Process

As x_i is a binary variable, thus ${x_i}^k = x_i$ for any i and k; hence $\phi(\mathbf{x})$ is a polynomial function in which each variable x_i has degree 1.

Summarizing, the main steps for computing the system failure probability, by adopting this method are:

i) obtain the system structure function.

ii) remove the powers of each variable x_i; and

iii) replace each variable x_i by the respective p_i.

Analysis by Expected Value of the Structure Function

- Example

Consider a *2 out of 3* system represented by the RBD in figure. The logical function of the RBD presented in figure is

$$\varphi(\boldsymbol{bs}) = (s_1 \wedge s_2) \vee (s_1 \wedge s_3) \vee (s_2 \wedge s_3)$$

Therefore

$$\overline{\varphi(\boldsymbol{bs})} = \overline{(s_1 \wedge s_2) \vee (s_1 \wedge s_3) \vee (s_2 \wedge s_3)}$$

$$\overline{\varphi(\boldsymbol{bs})} = \overline{(s_1 \wedge s_2)} \wedge \overline{(s_1 \wedge s_3)} \wedge \overline{(s_2 \wedge s_3)}$$

$$\Leftrightarrow$$

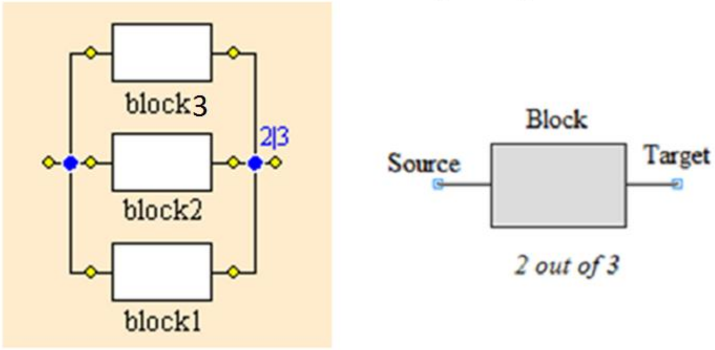
$$\phi(\mathbf{x}) = 1 - (1 - x_1x_2)(1 - x_1x_3)(1 - x_2x_3).$$

Considering that x_i is binary variable, thus $x_i{}^k = x_i$ for any i and k, hence, after simplification

$$\phi(\mathbf{x}) = x_1x_2 + x_1x_3 + x_2x_3 - 2x_1x_2x_3.$$

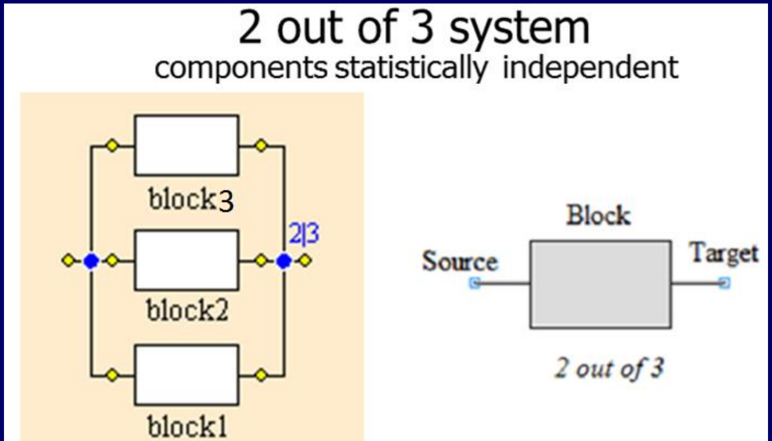
2 out of 3 system

components statistically independent



Analysis by Expected Value of the Structure Function

- Example



Since $\phi(\mathbf{x})$ is Bernoulli random variable, its expected value is equal to $P\{\phi(\mathbf{x}) = 1\}$, that is, $E[\phi(\mathbf{x})] = P\{\phi(\mathbf{x}) = 1\}$, thus

$$P\{\phi(\mathbf{x}) = 1\} = E[\phi(\mathbf{x})] = E[x_1x_2 + x_1x_3 + x_2x_3 - 2x_1x_2x_3] =$$
$$E[x_1x_2] + E[x_1x_3] + E[x_2x_3] - 2 \times E[x_1x_2x_3] =$$
$$E[x_1]\,E[x_2] + E[x_1]\,E[x_3] + E[x_2]\,E[x_3] - 2 \times E[x_1]E[x_2]E[x_3].$$

Therefore

$$P\{\phi(\mathbf{x}) = 1\} = p_1p_2 + p_1p_3 + p_2p_3 - 2 \times p_1p_2p_3.$$

As $p_1 = p_2 = p_3 = p$

$$P\{\phi(\mathbf{x}) = 1\} = 3p^2 - 2p^3$$

Pivotal Decomposition, Factoring or Conditioning

- Method

This method is based on the conditional probability of the system according the states of certain components. Consider the system structure function as depicted in

$$\phi(\mathbf{x}) = x_i\, \phi(1_i, \mathbf{x}) + (1 - x_i)\, \phi(0_i, \mathbf{x})$$

and identify the pivot component i,

then

$$P\{\phi(\mathbf{x}) = 1\} = E[x_i\, \phi(1_i, \mathbf{x}) + (1 - x_i)\, \phi(0_i, \mathbf{x})] = E[x_i\, \phi(1_i, \mathbf{x})] + E[(1 - x_i)\, \phi(0_i, \mathbf{x})]$$

If x_i is independent, then:

$$E[x_i] \times E[\phi(1_i, \mathbf{x})] + E[(1 - x_i)] \times E[\phi(0_i, \mathbf{x})].$$

As x_i is a Bernoulli random variable, thus:

$$P\{\phi(\mathbf{x}) = 1\} = p_i \times E[\phi(1_i, \mathbf{x})] + (1 - p_i) \times E[\phi(0_i, \mathbf{x})].$$

Since $E[\phi(1_i, \mathbf{x})] = P\{\phi(1_i, \mathbf{x}) = 1\}$ and $E[\phi(0_i, \mathbf{x})] = P\{\phi(0_i, \mathbf{x}) = 1\}$,

then:

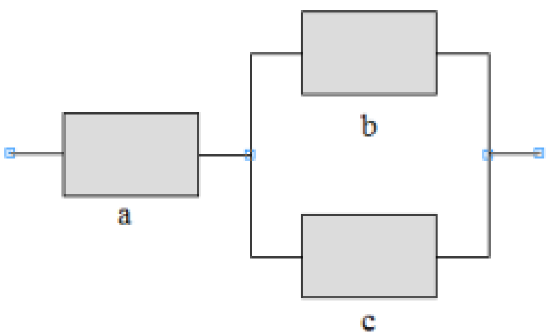
$$P\{\phi(\mathbf{x}) = 1\} = p_i \times P\{\phi(1_i, \mathbf{x}) = 1\} + (1 - p_i) \times P\{\phi(0_i, \mathbf{x}) = 1\}.$$

Pivotal Decomposition, Factoring or Conditioning

- Example

Consider the system composed of three components, a, b and c, depicted in the figure where $\phi(x_a, x_b, x_c)$ denotes the system structure function.

As $P\{\phi(\mathbf{x}) = 1\} = E[x_i\, \phi(1_i, \mathbf{x}) + (1 - x_i)\, \phi(0_i, \mathbf{x})]$, then:



$$P\{\phi(x_a, x_b, x_c) = 1\} = p_a \times E[\phi(1_a, x_b, x_c)]$$
$$+$$
$$(1 - p_a) \times E[\, \phi(0_a, x_b, x_c)$$

But as $E[\, \phi(0_a, x_b, x_c)] = 0$, so:

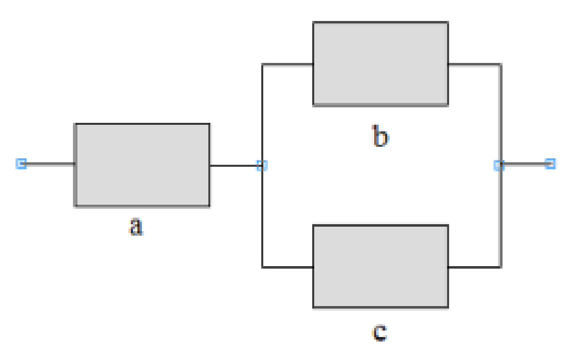
$$P\{\phi(x_a, x_b, x_c) = 1\} = p_a \times E[\phi(1_a, x_b, x_c)].$$

Since

$$E[\phi(1_a, x_b, x_c)] = P\{\phi(1_a, x_b, x_c) = 1\},$$

Pivotal Decomposition, Factoring or Conditioning

- Example



Now factoring on component b,

$$P\{\phi(1_a, x_b, x_c) = 1\} = \begin{array}{l} p_b \times E[\phi(1_a, 1_b, x_c)] \\ + \\ (1 - p_b) \times E[\phi(1_a, 0_b, x_c)], \end{array}$$

then

$$P\{\phi(x_a, x_b, x_c) = 1\} = p_a \times [p_b \times E[\phi(1_a, 1_b, x_c)] + (1 - p_b) \times E[\phi(1_a, 0_b, x_c)]].$$

As $E[\phi(1_a, 1_b, x_c)] = 1$, thus:

$$P\{\phi(x_a, x_b, x_c) = 1\} = p_a \ [p_b + (1 - p_b) \times E[\phi(1_a, 0_b, x_c)]].$$

Now, as we know that

$$E[\phi(1_a, 0_b, x_c)] = P\{\phi(1_a, 0_b, x_c) = 1\}, \text{ and}$$

$$P\{\phi(1_a, 0_b, x_c) = 1\} = E[x_c\, \phi(1_a, 0_b, 1_c) + (1 - x_c)\, \phi(1_a, 0_b, 0_c)],$$

then

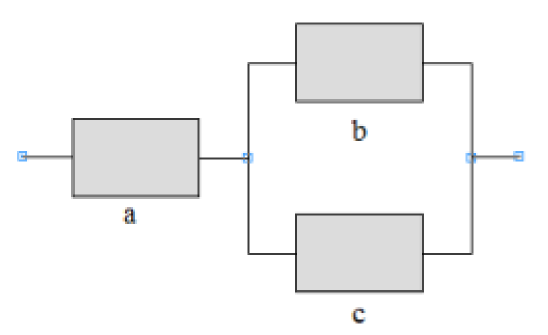
$$E[\phi(1_a, 0_b, x_c)] = E[x_c]\, E[\phi(1_a, 0_b, 1_c)] + E[(1 - x_c)] E[\phi(1_a, 0_b, 0_c)],$$

thus

$$E[\phi(1_a, 0_b, x_c)] = p_c \times E[\phi(1_a, 0_b, 1_c)] + (1 - p_c) \times E[\phi(1_a, 0_b, 0_c)].$$

Pivotal Decomposition, Factoring or Conditioning

- Example



As $E[\phi(1_a,0_b,1_c)] = P\{\phi(1_a,0_b,1_c) = 1\} = 1$

and $E[\phi(1_a,0_b,0_c)] = P\{\phi(1_a,0_b,0_c) = 1\} = 0$,

then

$$E[\phi(1_a,0_b,x_c)] = p_c.$$

Therefore:

$$P\{\phi(x_a,x_b,x_c) = 1\} = p_a\,[p_b + (1-p_b)\times p_c] =$$

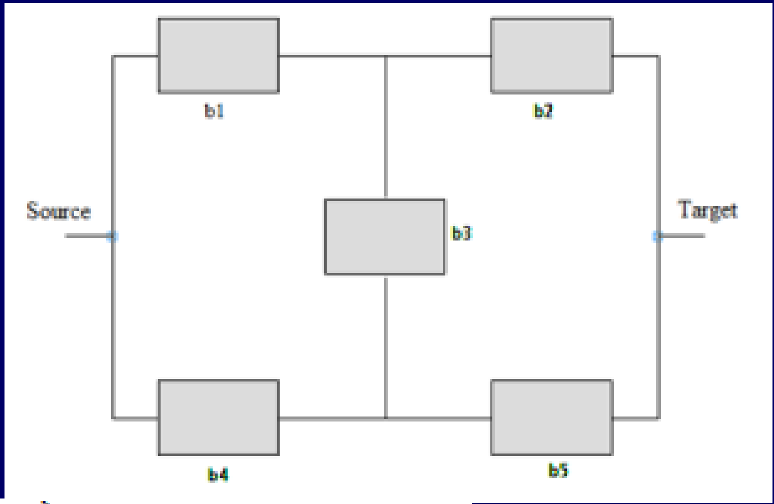
$$P\{\phi(x_a,x_b,x_c) = 1\} = p_a p_b + p_a p_c(1-p_b),$$

which is

$$P\{\phi(x_a,x_b,x_c) = 1\} = p_a[1-(1-p_b)(1-p_c)].$$

Pivotal Decomposition, Factoring or Conditioning

- Example – Bridge Structure



$$\phi(\mathbf{x}) = x_i\,\phi(1_i,\mathbf{x}) + (1-x_i)\,\phi(0_i,\mathbf{x})$$

Factoring on b_3

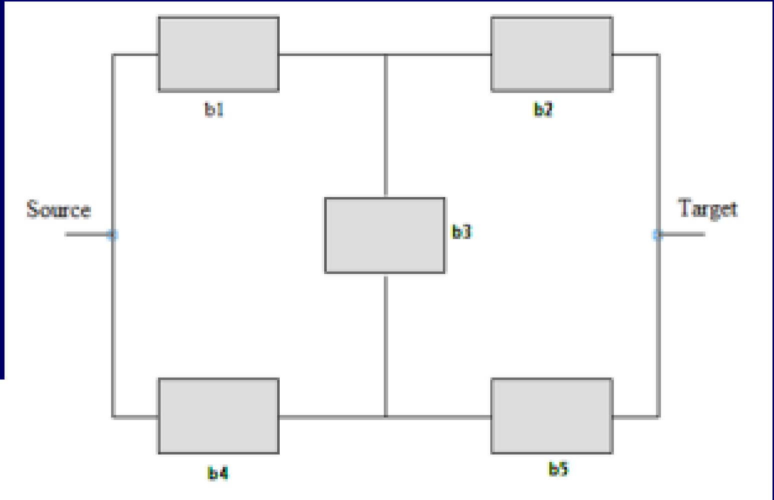
$$\phi(\mathbf{x}) = x_3\,\phi(1_3,\mathbf{x}) + (1-x_3)\,\phi(0_3,\mathbf{x})$$
$$P\{\phi(\mathbf{x})=1\} = E[x_3\,\phi(1_3,\mathbf{x}) + (1-x_3)\,\phi(0_3,\mathbf{x})] =$$
$$P\{\phi(\mathbf{x})=1\} = E[x_3\,\phi(1_3,\mathbf{x})] + E[(1-x_3)\,\phi(0_3,\mathbf{x})] =$$

By independency

$$P\{\phi(\mathbf{x})=1\} = E[x_3]\,E[\phi(1_3,\mathbf{x})] + E[(1-x_3)]\,E[\phi(0_3,\mathbf{x})] =$$
$$P\{\phi(\mathbf{x})=1\} = p_3\,E[\phi(1_3,\mathbf{x})] + (1-p_3)\,E[\phi(0_3,\mathbf{x})] =$$

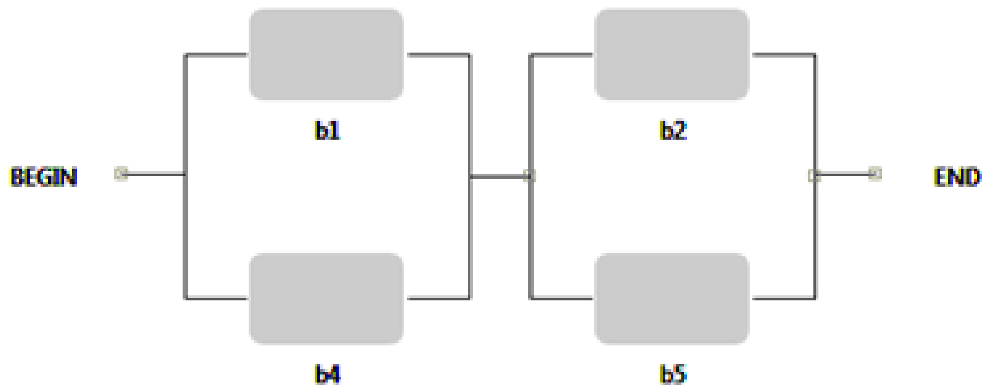
Pivotal Decomposition, Factoring or Conditioning

- Example – Bridge Structure



If $x_3 = 1 \Rightarrow p_3 = 1$, then:

Configuration 1:

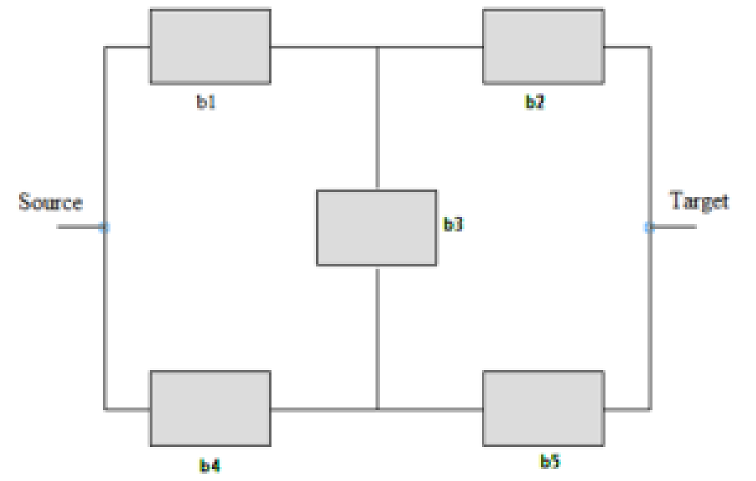


$$P\{\phi(\mathbf{x}) = 1\} = E[\phi(1_3, \mathbf{x})] = P\{\phi(1_3, \mathbf{x}) = 1\}$$

$$P\{\phi(1_3, \mathbf{x}) = 1\} = \big(1 - (1 - p_1)(1 - p_4)\big) \times \big(1 - (1 - p_2)(1 - p_5)\big)$$

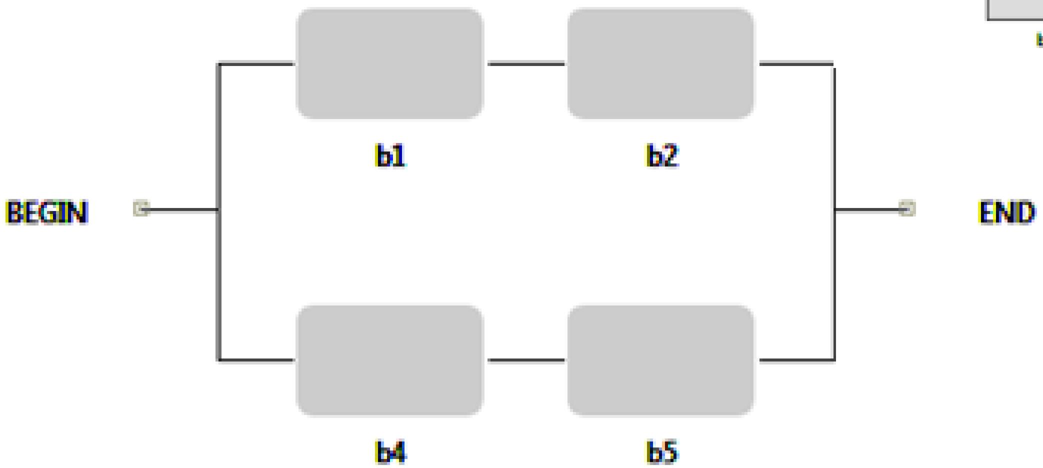
Pivotal Decomposition, Factoring or Conditioning

- Example – Bridge Structure



If $x_3 = 0 \Rightarrow p_3 = 0$, then:

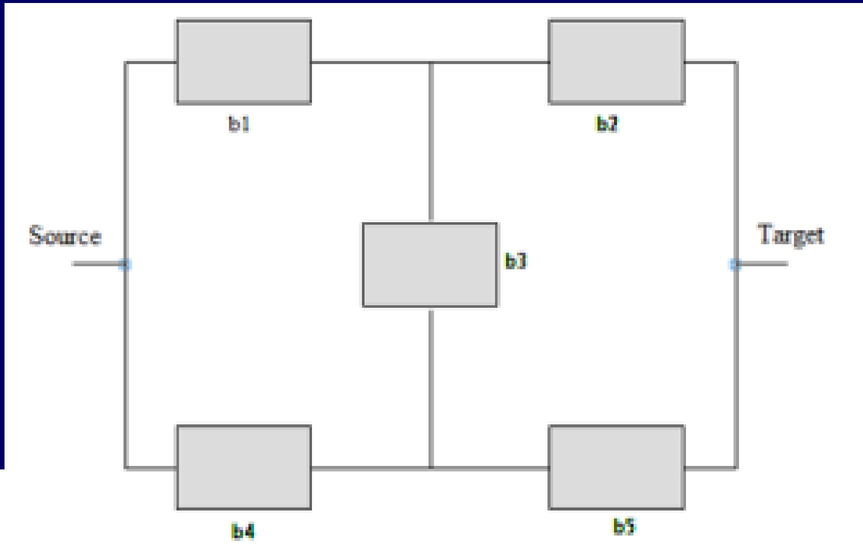
Configuration 2:



$$P\{\phi(\mathbf{x}) = 1\} = E[\phi(0_3, \mathbf{x})] = P\{\phi(0_3, \mathbf{x}) = 1\}$$
$$P\{\phi(0_3, \mathbf{x}) = 1\} = \big(1 - (1 - p_1 p_2)(1 - p_4 p_5)\big)$$

Pivotal Decomposition, Factoring or Conditioning

- Example – Bridge Structure



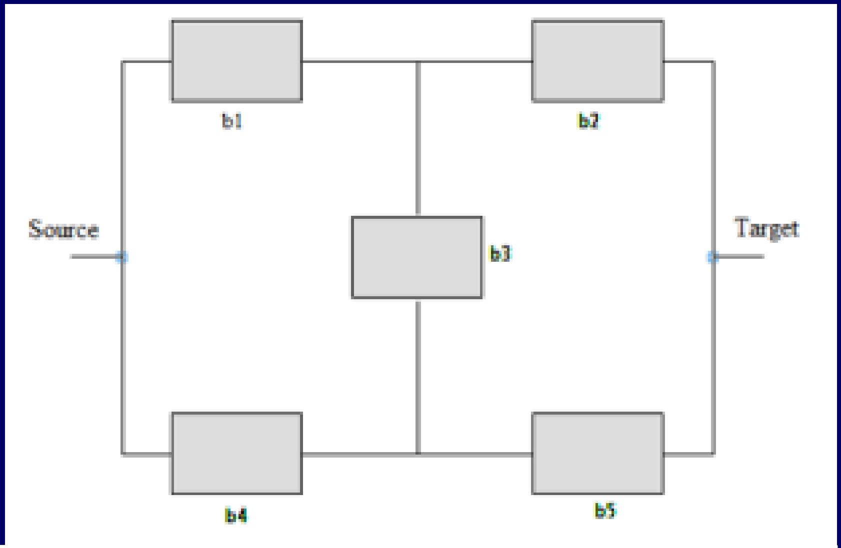
Therefore:

$$P\{\phi(\mathbf{x})=1\} = p_3 \times P\{\phi(1_3,\mathbf{x})=1\} + (1-p_3) \times P\{\phi(0_3,\mathbf{x})=1\}$$

$$P\{\phi(\mathbf{x})=1\} = p_3 \times \Big(\big(1-(1-p_1)(1-p_4)\big) \times \big(1-(1-p_2)(1-p_5)\big)\Big) + (1-p_3)\ \Big(\big(1-(1-p_1)(1-p_4)\big) \times \big(1-(1-p_2)(1-p_5)\big)\Big)$$

Pivotal Decomposition, Factoring or Conditioning

- Example – Bridge Structure



$$R_{bridge}(t) = e^{-(\lambda_2+\lambda_3+\lambda_4)t} - e^{-(\lambda_2+\lambda_3+\lambda_4+\lambda_5)t} + e^{-(\lambda_1+\lambda_3+\lambda_5)t}$$

$$+2e^{-\sum_i \lambda_i t} - e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_5)t} - e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t} - e^{-(\lambda_1+\lambda_3+\lambda_4+\lambda_5)t}$$

$$+e^{-(\lambda_1+\lambda_2)t} + e^{-(\lambda_4+\lambda_5)t} - e^{-(\lambda_1+\lambda_2+\lambda_4+\lambda_5)t}$$

Pivotal Decomposition, Factoring or Conditioning

- Example – Bridge Structure

$$MTTF = \int_0^\infty R_{bridge}(t)dt$$

$$MTTF = \frac{1}{\lambda_1 + \lambda_2} + \frac{1}{\lambda_4 + \lambda_5} + \frac{1}{\lambda_2 + \lambda_3 + \lambda_4} + \frac{2}{\sum_{i=1}^{5} \lambda_i}$$

$$- \frac{1}{\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4} - \frac{1}{\lambda_2 + \lambda_3 + \lambda_4 + \lambda_5} - \frac{1}{\lambda_1 + \lambda_2 + \lambda_3 + \lambda_5}$$

$$- \frac{1}{\lambda_1 + \lambda_3 + \lambda_4 + \lambda_5} - \frac{1}{\lambda_1 + \lambda_3 + \lambda_5} - \frac{1}{\lambda_1 + \lambda_2 + \lambda_4 + \lambda_5}$$

Reductions

The dependability evaluation of complex system structures might be conducted iteratively by indentifying series, parallel, *k out of n* and *bridge* subsystems, evaluating each of those subsystems, and then reducing each subsystem to one respective equivalent block.

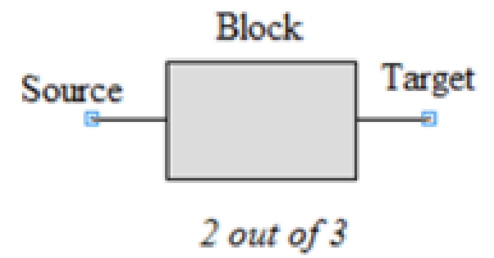
This process may be iteratively applied to the resultant structures until a single block results.

Reductions

- Series reduction
- Parallel reduction

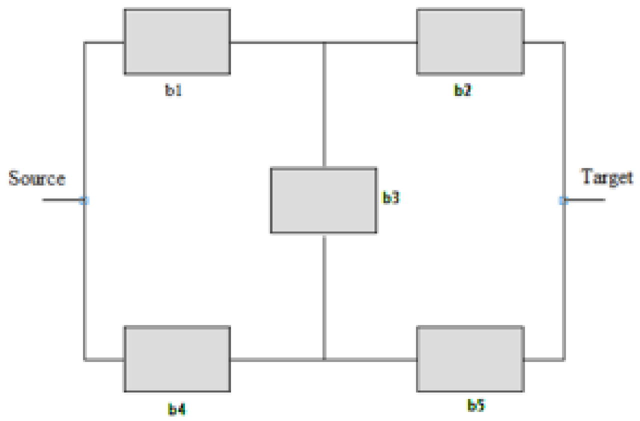
Reductions

- 2 out of 3 reduction



$$P\{\phi(\mathbf{x}) = 1\} = 3p^2 - 2p^3$$

- Bridge reduction

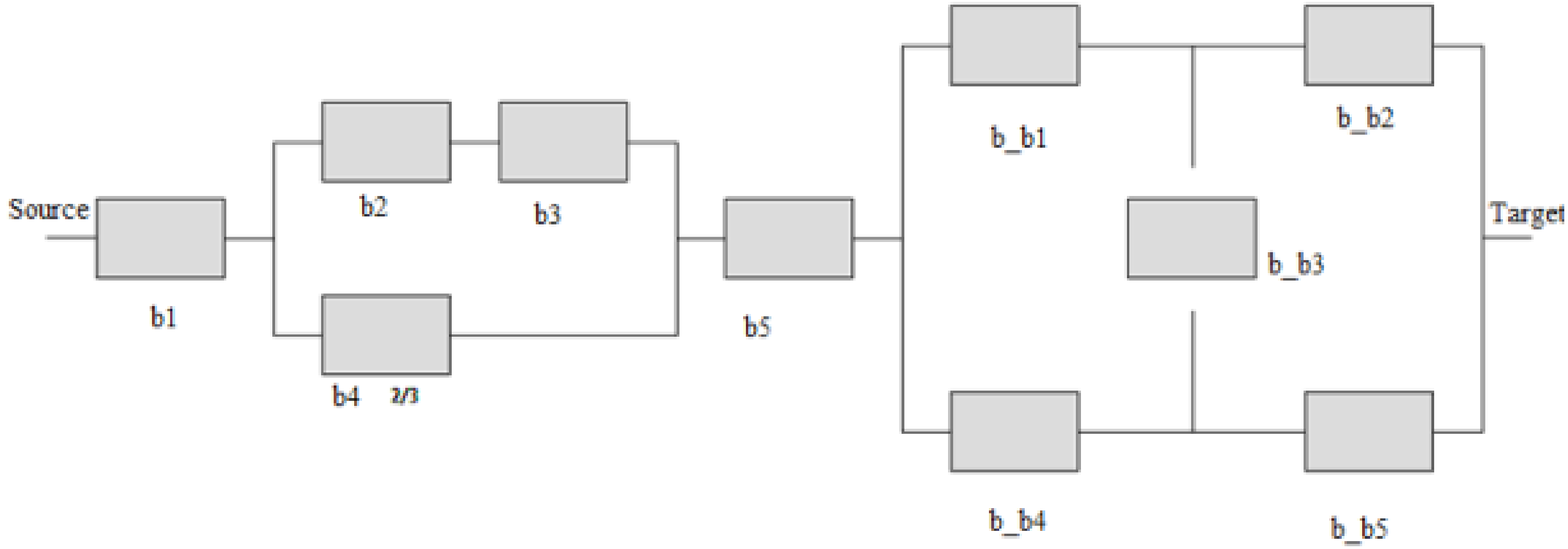


$$P\{\phi(\mathbf{x}) = 1\} = p_3 \times P\{\phi(1_3, \mathbf{x}) = 1\} + (1 - p_3) \times P\{\phi(0_3, \mathbf{x}) = 1\}$$

Reductions

- Example

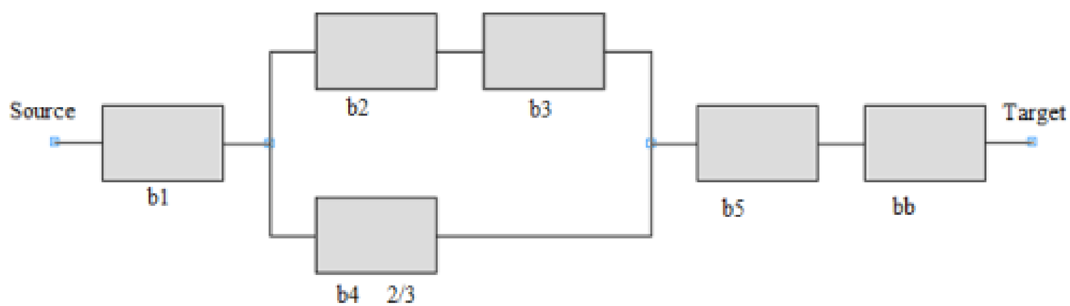
Consider a system composed of four basic blocks (b_1, b_2, b_3, b_5), one *2 out of 3* and one bridge structure. The three components of the *2 out of 3* block are equivalent, that is, the failure probability of each component is the same (p_4). The failure probabilities of components b_1, b_2, b_3, b_5 and the failure probability of the bridge structure are $p_{b1}, p_{b2}, p_{b3}, p_{b4}$ and p_{b5}, respectively.



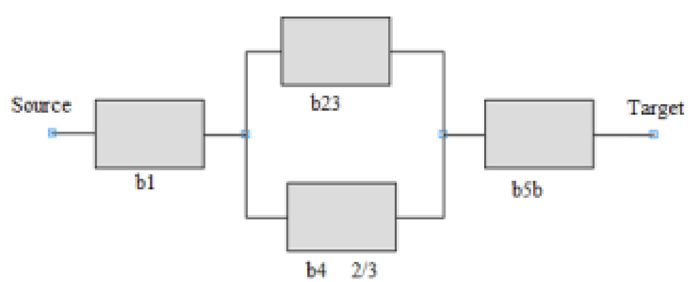
Reductions

- Example

The *2 out of 3* structure can be represented one equivalent block whose reliability is $3p^2 - 2p^3$. The bridge structure can be transformed into one component, b_b, whose failure probability is $p_{bb} = (1-(1-p_{b1}p_{b2})(1-p_{b4}p_{b5})(1-p_{b1}p_{b3}p_{b5})(1-p_{b2}p_{b3}p_{b4}))$.



After that, two series reductions may be applied, one reducing blocks b_2 and b_3 into block b_{23}; and a second that combines blocks b_5 and b_b and reduces it to the block b_{5b}. The reliability of block b_{23} is $p_{23} = p_2 \times p_3$, and the block reliability of block b_{5b} is $p_{5b} = p_5 \times [(1-(1-p_{b1}p_{b2})(1-p_{b4}p_{b5})(1-p_{b1}p_{b3}p_{b5})(1-p_{b2}p_{b3}p_{b4}))]$.



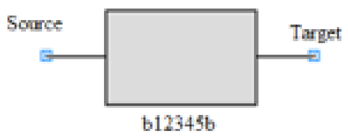
Reductions

- Example

Now a parallel reduction may be applied to merge blocks b_{23} and b_4.
The block b_{234} represents the block b_{23} and b_4 composition, whose reliability is $p_{234} = 1 - (1 - p_2 \times p_3) \times (1 - 3p^2 - 2p^3)$.

Finally, a final series reduction may be applied to RBD and one block RBD is generated, whose reliability is

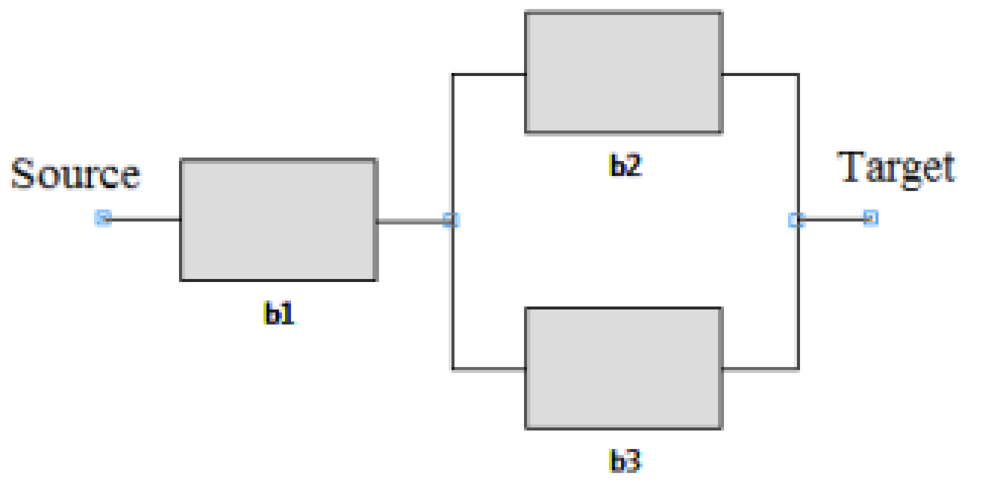
$$p_{12345b} = p_1 \times [1 - (1 - p_2 \times p_3) \times (1 - 3p^2 - 2p^3)] \\ \times \left[p_5 \times \left[\left(1 - (1 - p_{b1}p_{b2})(1 - p_{b4}p_{b5})(1 - p_{b1}p_{b3}p_{b5})(1 - p_{b2}p_{b3}p_{b4})\right)\right]\right].$$



Computation Based on Minimal Paths and Minimal Cuts

- Path and Minimal Path

Consider a system S with n components and its structure function $\phi(\mathbf{x})$, where $SCS = \{c_1, c_2, \dots, c_n\}$ is the set of components. A state vector $\mathbf{x}$ is named a **path vector** if $\phi(\mathbf{x}) = 1$, and the respective set of operational components is defined as **path set**. More formally, the respective path set of a state vector is defined by $PS(\mathbf{x}) = \{c_i | \phi(\mathbf{x}) = 1, x_i = 1, c_i \in SCS\}$. A path vector $\mathbf{x}$ is called **minimal path vector** if $\phi(\mathbf{x}) = 0$, for any $\mathbf{y} < \mathbf{x}$, and the respective path set is named **minimal path set**, that is $MPS(\mathbf{x}) = \{c_i | c_i \in PS(\mathbf{x}), \phi(\mathbf{x}) = 0 \;\; \forall\, \mathbf{y} < \mathbf{x}\}$.



PS_1 is a minimal path set

PS_2 is a minimal path set

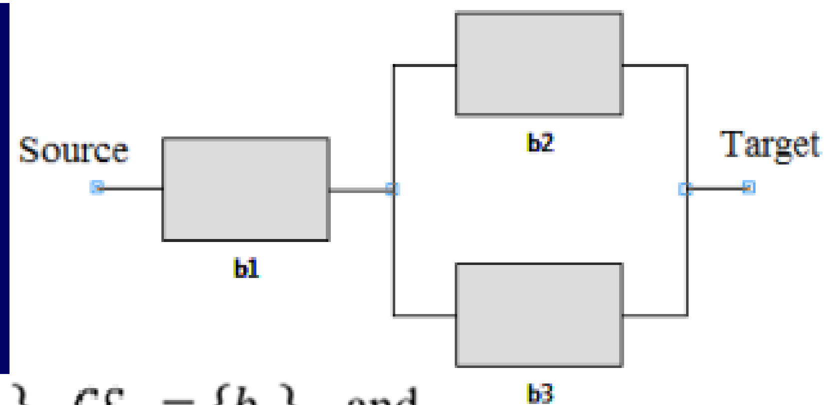
PS_3 is not minimal

$PS_1 = \{b_1, b_2\}$, $PS_2 = \{b_1, b_3\}$ and $PS_3 = \{b_1, b_2, b_3\}$ are path sets

Computation Based on Minimal Paths and Minimal Cuts

- Cut and Minimal Cut

A state vector $\mathbf{x}$ is named a **cut vector** is $\phi(\mathbf{x}) = 0$, and the respective set of faulty components is defined as **cut set**. Therefore, $CS(\mathbf{x}) = \{c_i | \phi(\mathbf{x}) = 0, x_i = 0, c_i \in SCS\}$. A cut vector $\mathbf{x}$ is called **minimal cut vector** if $\phi(\mathbf{x}) = 1$, for any $\mathbf{y} > \mathbf{x}$, and the respective path set is named **minimal cut set**, that is $MCS(\mathbf{x}) = \{c_i | c_i \in CS(\mathbf{x}), \phi(\mathbf{x}) = 1 \ \forall \ \mathbf{y} > \mathbf{x}\}$.

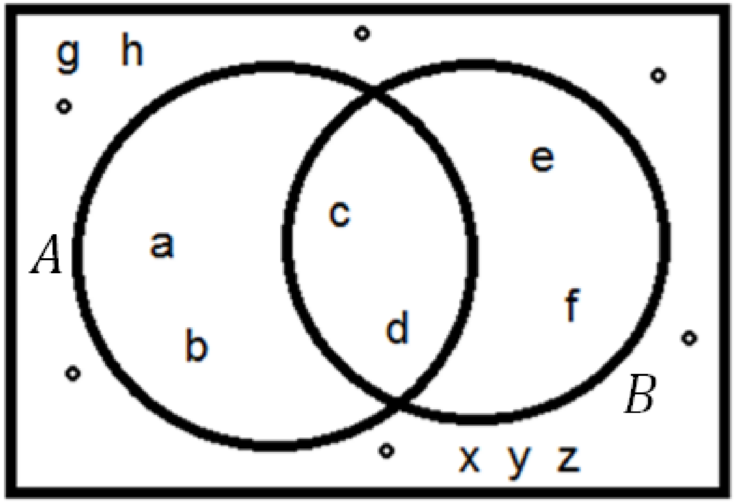


$CS_1 = \{b_1, b_2\}$, $CS_2 = \{b_1, b_3\}$, $CS_3 = \{b_1, b_2, b_3\}$, $CS_4 = \{b_1\}$, and $CS_5 = \{b_2, b_3\}$

CS_4 is a minimal cut set,
CS_5 is a minimal cut set,
The same is not true for CS_1, CS_2, and CS_3.

Sum-of-Disjoint-Products (SDP) method

$$A = \{a, b, c, d\}$$
$$B = \{c, d, e, f\}$$
$$\Omega = \{a, b, c, d, e, f, g, \dots, z\}$$



$$A \cup B = A \cup (A^c \cap B)$$

$$A^c = \{e, f, g, h, \dots, z\}$$

$$A^c \cap B = \{e, f, g, h, \dots, z\} \cap \{c, d, e, f\} =$$

$$A^c \cap B = \{e, f\}$$

$$A \cup B = \{a, b, c, d\} \cup \{e, f\} = \{a, b, c, d, e, f\}$$

$$\Leftrightarrow$$

$$A \cup B = \{a, b, c, d, e, f\} = \{a, b, c, d\} \cup \{c, d, e, f\}$$

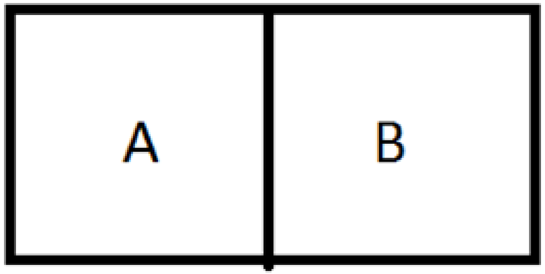
Now, consider $P(A \cup B) = P(A \cup (A^c \cap B))$

As $A \cap (A^c \cap B) = \emptyset$,

since A and $(A^c \cap B)$ are disjoint, then

$$P(A \cup B) = P(A) + P(A^c \cap B)$$

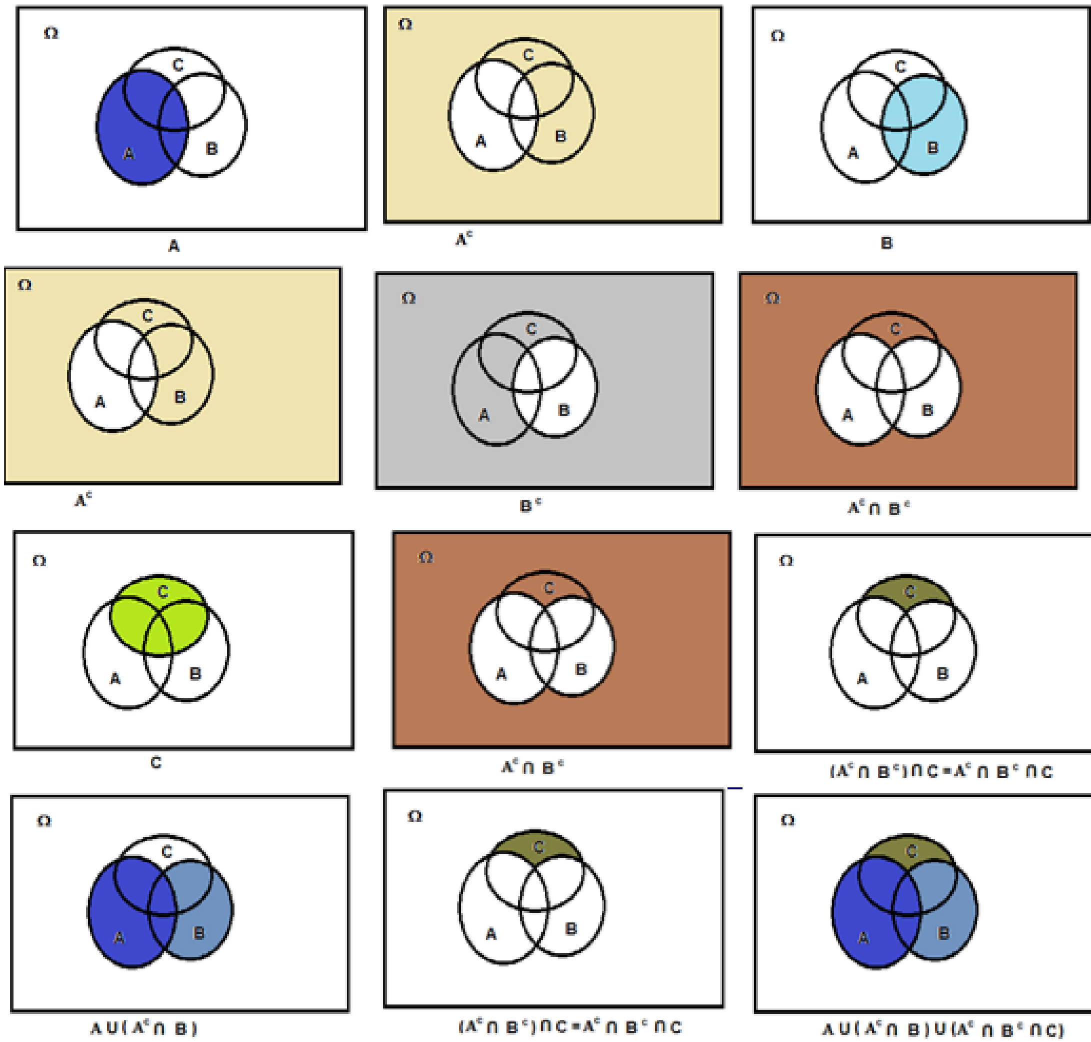
Sum-of-Disjoint-Products (SDP) method



Disjoint Terms: Addition Law The addition law of probabilities is the underlying justification for the SDP method. If two or more events have no elements in common, the probability that at least one of the events will occur is the sum of the probabilities of the individual events. If two events A and B have elements in common, the union of these two events, $A \cup B$, may be expressed as the union of event A with event B, where A^c denotes the complement of A. Then we have the following equation for evaluation of the probability of $A \cup B$:

$$\Pr(A \cup B) = \Pr(A) + \Pr(A^c B).$$

Sum-of-Disjoint-Products (SDP) method



Similarly with three events A, B, and C, we have

$$\Pr(A \cup B \cup C) = \Pr(A) + \Pr(A^c B) + \Pr(A^c B^c C)$$

Sum-of-Disjoint-Products (SDP) method

Similarly with three events A, B, and C, we have

$$\Pr(A \cup B \cup C) = \Pr(A) + \Pr(A^c B) + \Pr(A^c B^c C).$$

With n events $A_1, A_2, \ldots, A_n$, we have

$$\Pr(A_1) + \Pr(A_1^c A_2) + \Pr(A_1^c A_2^c A_3) + \cdots + \Pr(A_1^c \ldots A_{n-1}^c A_n)$$

Sum-of-Disjoint-Products (SDP) method

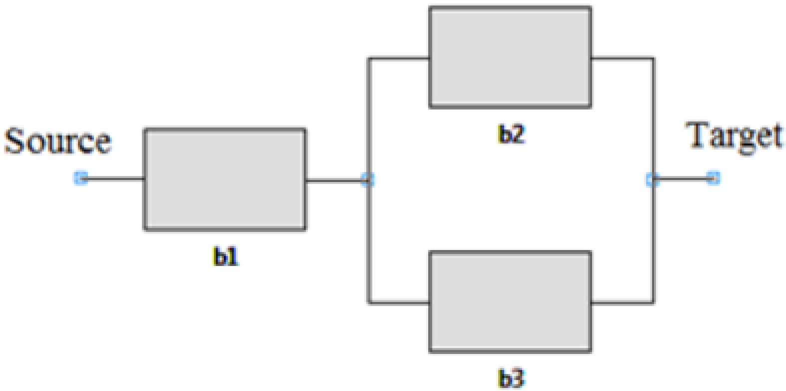
Considering a system composed of three independent components b_1, b_2 and b_3, where the components failure probabilities are p_1, p_2 and p_3, respectively.

The respective RBD logical function is:

$$\varphi(s_1, s_2, s_3) = s_1 \wedge (s_2 \vee s_3)$$

Then define all minimal paths:

$$\varphi(s_1, s_2, s_3) = (s_1 \wedge s_2) \vee (s_1 \wedge s_3)$$



The minimal paths are:

$PS_1 = \{b_1, b_2\}$ and $PS_2 = \{b_1, b_3\}$.

(and $PS_4 = \{b_1\}$, and $PS_5 = \{b_2, b_3\}$ are minimal cut sets)

$$\varphi(s_1, s_2, s_3) \Leftrightarrow \phi(x_1, x_2, x_3) = 1$$

Sum-of-Disjoint-Products (SDP) method

The respective RBD logical function is:

$$\varphi(s_1, s_2, s_3) = s_1 \wedge (s_2 \vee s_3)$$

Then define all minimal paths:

$$\varphi(s_1, s_2, s_3) = (s_1 \wedge s_2) \vee (s_1 \wedge s_3)$$

The minimal paths are:

$$PS_1 = \{b_1, b_2\} \text{ and } PS_2 = \{b_1, b_3\}.$$

(and $PS_4 = \{b_1\}$, and $PS_5 = \{b_2, b_3\}$ are minimal cut sets)

$$\varphi(s_1, s_2, s_3) \Leftrightarrow \phi(x_1, x_2, x_3) = 1$$

Therefore:

$$P\big(\varphi(s_1, s_2, s_3)\big) = P(\phi(x_1, x_2, x_3) = 1).$$

Then, applying the SDP formula:

$$P(A \cup B) = P(A) + P(A^c \cap B)$$

$$P(PS_1 \cup PS_2) = P(PS_1) + P(PS_1{}^c \cap PS_2).$$

Every component within the minimal path PS_1 must properly work for PS_1 being responsible for $\phi(x_1, x_2, x_3) = 1$

Sum-of-Disjoint-Products (SDP) method

So,

$PS_1 \overset{eq}{\Leftrightarrow} s_1 \wedge s_2$ and

$P(PS_1) = P(s_1 \wedge s_2)$.

As $PS_1 \overset{eq}{\Leftrightarrow} s_1 \wedge s_2$, thus:

$PS_1{}^c \overset{eq}{\Leftrightarrow} \overline{s_1 \wedge s_2}$

Since $PS_2 \overset{eq}{\Leftrightarrow} s_1 \wedge s_3$, thus:

$PS_1{}^c \cap PS_2 \overset{eq}{\Leftrightarrow} \overline{s_1 \wedge s_2} \wedge s_1 \wedge s_3$

Therefore:

$P(PS_1{}^c \cap PS_2) = P(\overline{s_1 \wedge s_2} \wedge s_1 \wedge s_3)$

$PS_1{}^c \cap PS_2 \overset{eq}{\Leftrightarrow} \overline{s_1 \wedge s_2} \wedge s_1 \wedge s_3$

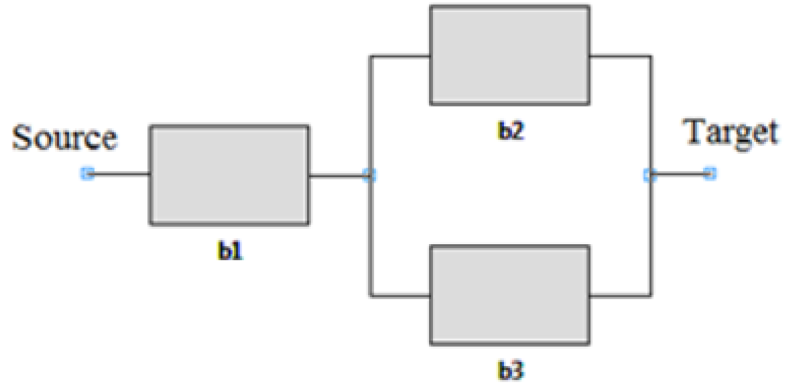
So,

$P(PS_1{}^c \cap PS_2) = P(\overline{s_1 \wedge s_2} \wedge s_1 \wedge s_3)$

Then:

$$P\big(\varphi(s_1, s_2, s_3)\big) = P(s_1 \wedge s_2) + P(\overline{s_1 \wedge s_2} \wedge s_1 \wedge s_3) =$$
$$P(s_1 \wedge s_2) + P((\overline{s_1} \vee \overline{s_2}) \wedge s_1 \wedge s_3) =$$
$$P(s_1 \wedge s_2) + P((\overline{s_1} \wedge s_1 \wedge s_3) \vee (\overline{s_2} \wedge s_1 \wedge s_3)) =$$
$$P(s_1 \wedge s_2) + P(\overline{s_2} \wedge s_1 \wedge s_3) = P(PS_1) + P(PS_1{}^c \cap PS_2)$$

Sum-of-Disjoint-Products (SDP) method



Now,consider $P(x_1) = P(x_2) = P(x_3) = 0.9$

$$P(\phi(x_1, x_2, x_3) = 1) = 0.9 \times 0.9 + (1 - 0.9) \times 0.9 \times 0.9 =$$

$$P(\phi(x_1, x_2, x_3) = 1) = 0.891$$

It is worth noting that:

$$P(\phi(x_1, x_2, x_3) = 1) =$$

$$P(x_1) \times (1 - (1 - P(x_2)) \times (1 - P(x_2)) =$$

$$0.9 \times (1 - (1 - 0.9)) \times (1 - 0.9)) = 0.891$$

State-space based models

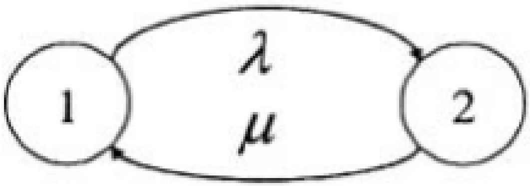
CTMC

Single Component System Availability Model

Consider a system with one component or when the system is considered as a black-box. This systems may have a normal functioning (1) state and a failed state (2).

System

If the TTF and TTR are exponentially distributed with rate λ and μ, respectively, the CTMC that represents the system availability model is



A simple 2-state CTMC

$$\pi_1(0) = 1$$

$$\pi_1(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t}$$

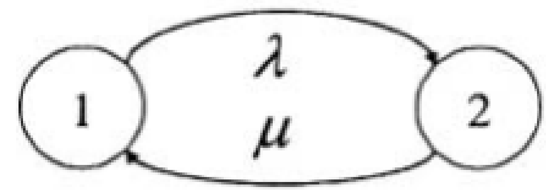
$$\pi_2(t) = \frac{\lambda}{\lambda+\mu} + \frac{\mu}{\lambda+\mu} e^{-(\lambda+\mu)t}$$

$$\pi_1(t) + \pi_2(t) = 1$$

$$A(t) = \pi_1(t)$$

Instantaneous availability

CTMC



A simple 2-state CTMC

Single Component System Availability Model

$$\pi_1(t) = \pi_1 = \frac{\mu}{\lambda + \mu}, t \to \infty$$

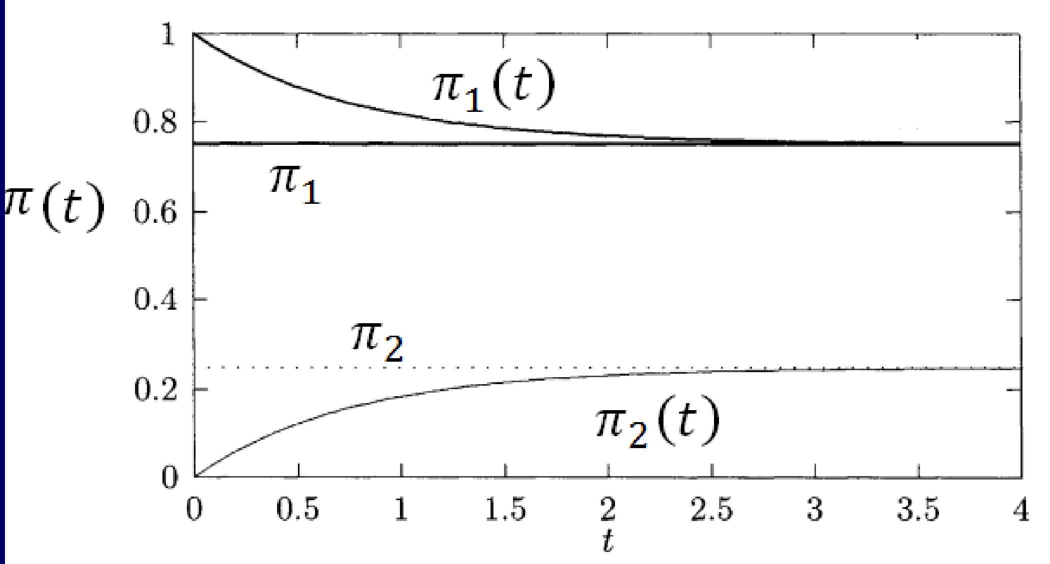
$$\pi_2(t) = \pi_2 = \frac{\lambda}{\lambda + \mu}, t \to \infty$$

$A = \pi_1$

Steady state availability

Figure shows the transient and steady-state behavior of the 2-state CTMC for $3\lambda = \mu = 1$.

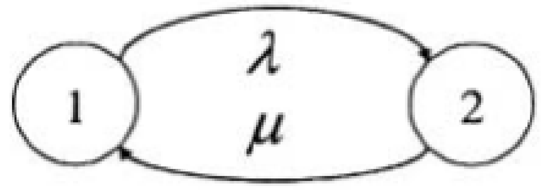
$$\mathbf{Q} = \begin{bmatrix} -\lambda & \lambda \\ \mu & -\mu \end{bmatrix}$$



CTMC

Availability Model

Single Component System Availability Model



A simple 2-state CTMC

$$\pi_1(t) = \pi_1 = \frac{\mu}{\lambda + \mu}, t \to \infty$$

$$\pi_2(t) = \pi_2 = \frac{\lambda}{\lambda + \mu}, t \to \infty$$

$A = \pi_1$

Steady state availability

$DT = (1 - A) \times T$

T – time period

Downtime

$DT = (1 - A) \times 8760h$

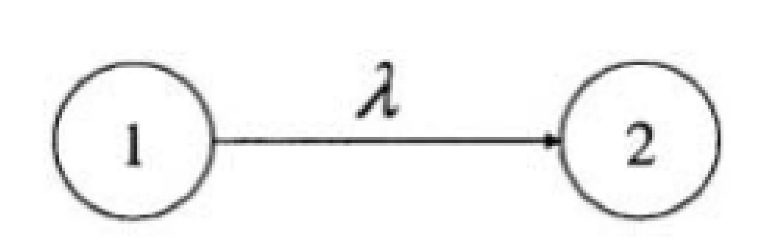
hours in a year

$DT = (1 - A) \times 525{,}600\ min$

minutes in a year

CTMC

Single Component System Reliability Model



$$\pi_1(0) = 1$$

$$\pi_1(t) = e^{-\lambda t}$$

$$\pi_1(t) + \pi_2(t) = 1$$

$$R(t) = \pi_1(t)$$

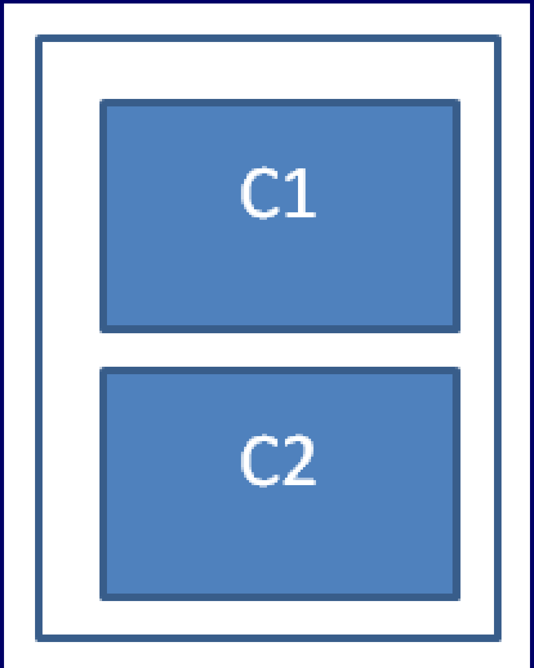
Reliability

$$R(t) = \pi_1(t) = 0, t \to \infty$$

$$MTTF = \int_0^\infty R(t)dt = \int_0^\infty e^{-\lambda t}dt = \frac{1}{\lambda}$$

CTMC

Two Component System - Hot Standby Availability Model



Two-component parallel redundant system with the same repair rate μ and the same failure rate for both components is (λ).

When both the components fail, the system fails.

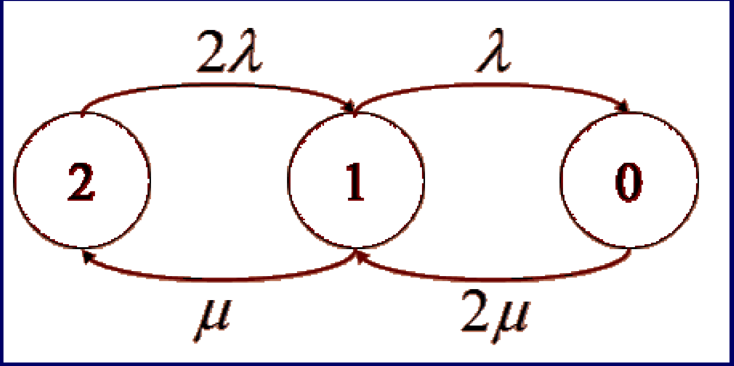
CTMC

2 Machines each with two repair facilities

Two Component System - Hot Standby Availability Model

$$A = \pi_2 + \pi_1 = \frac{\mu(2\lambda + \mu)}{(\lambda + \mu)^2}$$

Steady state availability



$$DT = (1 - A) \times T$$

T – time period

Downtime

Non-shared (independent) repair

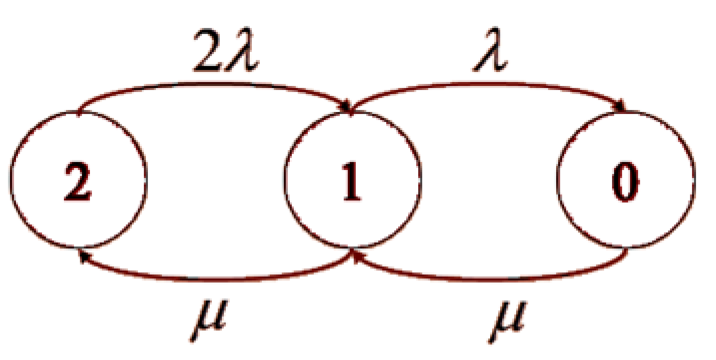
$$A(t) = \pi_2(t) + \pi_1(t)$$

Instantaneous availability

CTMC

2 Machines each with only one repair facility

Two Component System - Hot Standby Availability Model



Shared repair

$A(t) = \pi_2(t) + \pi_1(t)$

Instantaneous availability

$$A = \pi_2 + \pi_1 = \frac{\mu(2\lambda + \mu)}{2\lambda^2 + 2\lambda\mu + \mu^2}$$

Steady state availability

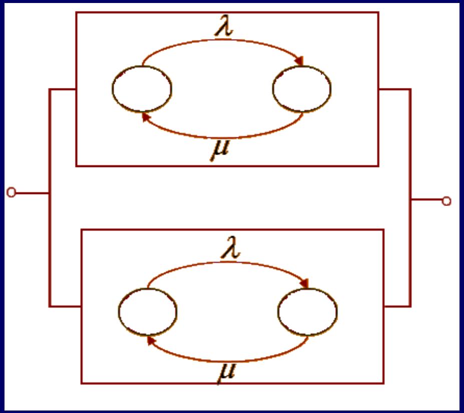
$$DT = (1 - A) \times T$$

T – time period

Downtime

CTMC

Two Component System - Hot Standby Availability Model



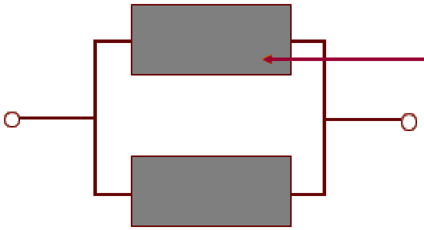
Non-shared case can be modeled & solved using a RBD or a FTREE but shared case needs the use of Markov chains.

$$A_{ss1} = \frac{\mu}{\lambda + \mu} \qquad UA_{ss1} = \frac{\lambda}{\lambda + \mu}$$

$$A_{ss2} = \frac{\mu}{\lambda + \mu} \qquad UA_{ss2} = \frac{\lambda}{\lambda + \mu}$$

$$A_{sys} = 1 - \left(1 - \frac{\mu}{\lambda + \mu}\right)^2 = 1 - \left(\frac{\lambda}{\lambda + \mu}\right)^2$$

$$A_{sys} = \frac{\mu(2\lambda + \mu)}{(\lambda + \mu)^2}$$



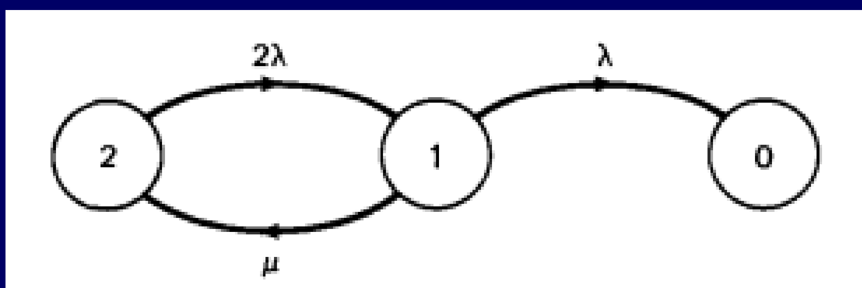
$$A = \frac{\mu}{\lambda + \mu}$$

$$A_{sys} = 1 - (1 - \frac{\mu}{\lambda + \mu})^2$$

CTMC

Reliability and MTTF

Two Component System - Hot Standby Reliability Model



Some authors erroneously claim that reliability models do not admit repair.

$$R(t) = 1 - \pi_0(t)$$

$$MTTF = \int_0^\infty R(t)dt = \frac{3\lambda + \mu}{2\lambda^2}$$

CTMC

M Machines with only one repair facility

- Example – Availability model

Generalization of the two-component system Model with shared repair facility

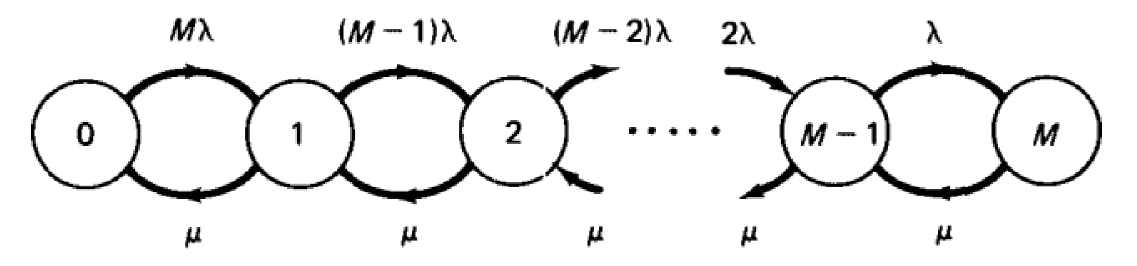
M similar machines independent repair facility.
Hot Standby

Failure rate of each machine is λ

Repair rate is μ

$$A_{sys} = 1 - \frac{\rho^M M!}{\sum_{k=0}^{M} \rho^k \frac{M!}{(M-k)!}}$$

$$\rho = \frac{\lambda}{\mu}$$



CTMC

M Machines each with only M repair facilities

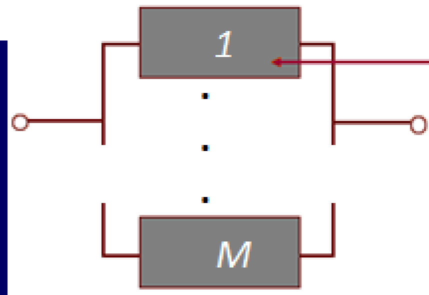
- Example – Availability model

Generalization of the two-component system model with independent repair facility

M similar machines independent repair facility.
Hot Standby

Failure rate of each machine is λ

Repair rate is μ



$$A = \frac{\mu}{\lambda + \mu}$$

$$A_{sys} = 1 - \left(\frac{\rho}{1+\rho}\right)^M$$

$$\rho = \frac{\lambda}{\mu}$$

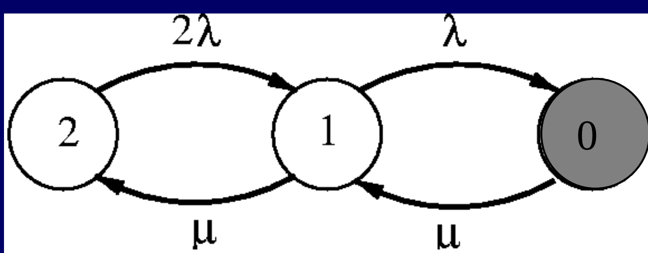
$$A_{sys} = 1 - \left(1 - \frac{\mu}{\lambda + \mu}\right)^M$$

System availability is then computed using a combinatorial approach

CTMC

Hot Standby

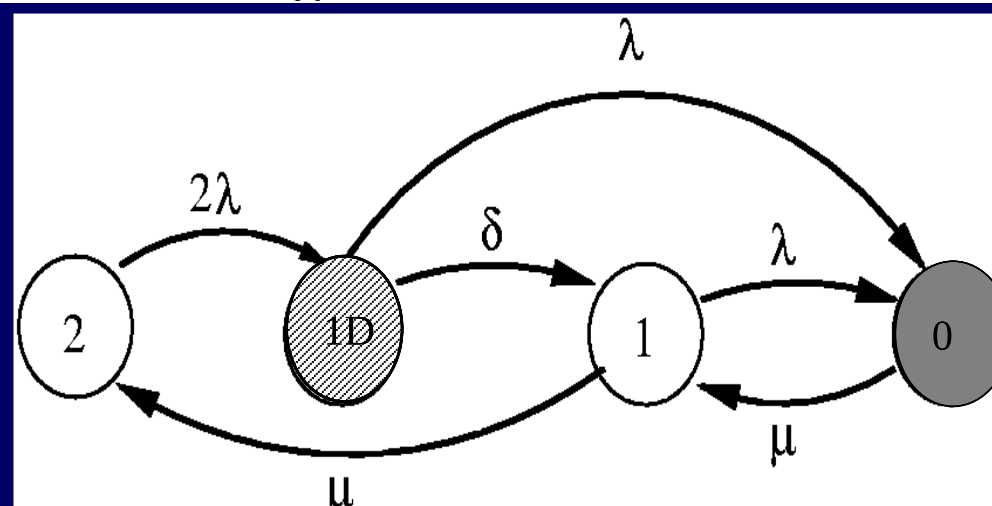
2-equal component availability model with perfect switching



$A_{ss} = 1\text{-}\pi_0$

Hot Standby

2-equal component availability model without perfect switching (with finite detection delay)

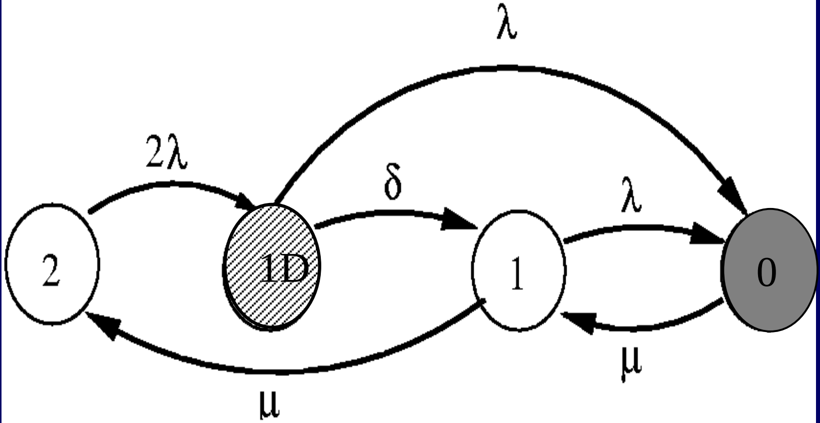


$$A = \pi_2 + \pi_1$$

CTMC

Hot Standby

2-equal component availability model without perfect switching (with finite detection delay)



Then Unavailability is given by

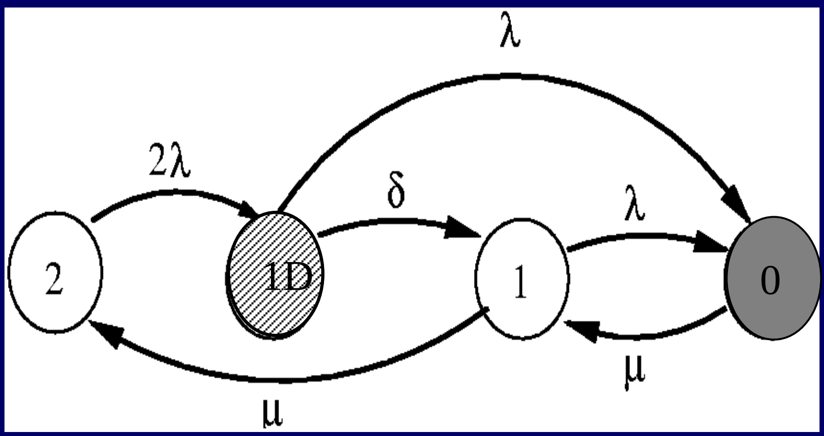
$$UA = \pi_0 + \pi_{1D}$$

$$A = \pi_2 + \pi_1$$

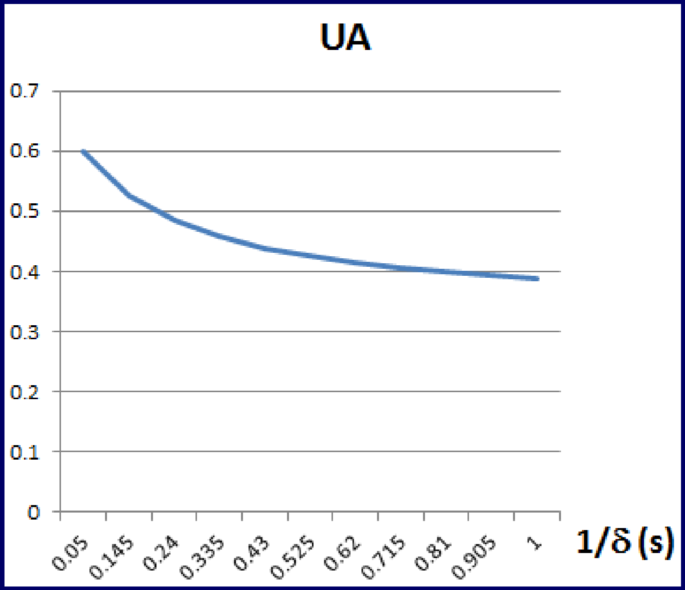
CTMC

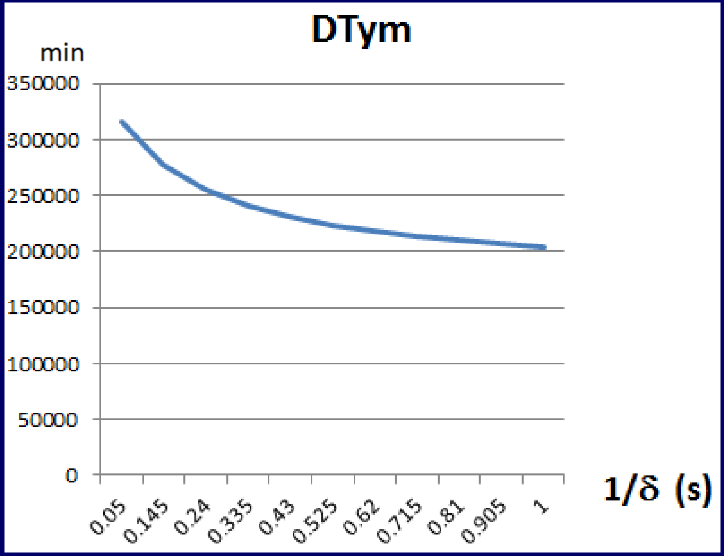
Example

Plot of downtime $D(\delta)$, $D(\delta, t_{th})$, and *D (for 3 state model without state 1D)* as functions of $1/\delta$ (in seconds) for $1/\lambda = 10,000$ h and $1/\mu = 2$ h.



$$UA = \pi_0 + \pi_{1D}$$





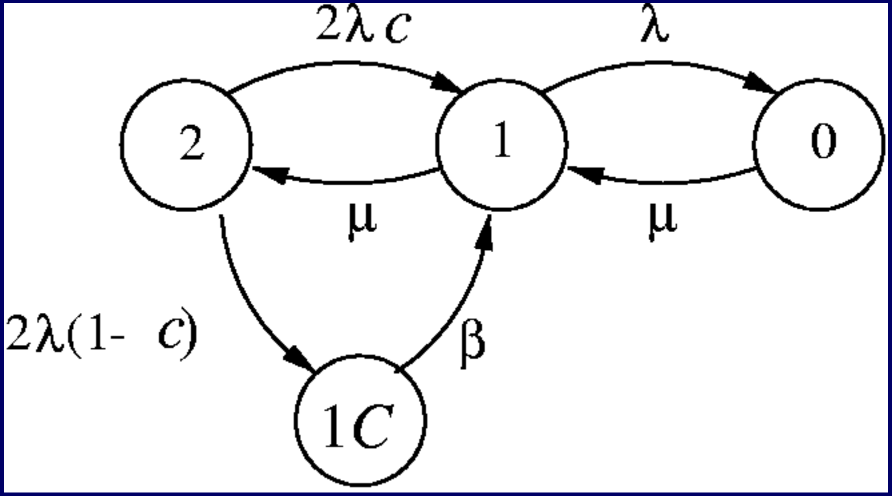
CTMC

Hot Standby

2-equal component without perfect switching with imperfect coverage availability model

Coverage factor = *c* (conditional probability that the fault is correctly handled)

1C state is a reboot (down) state.

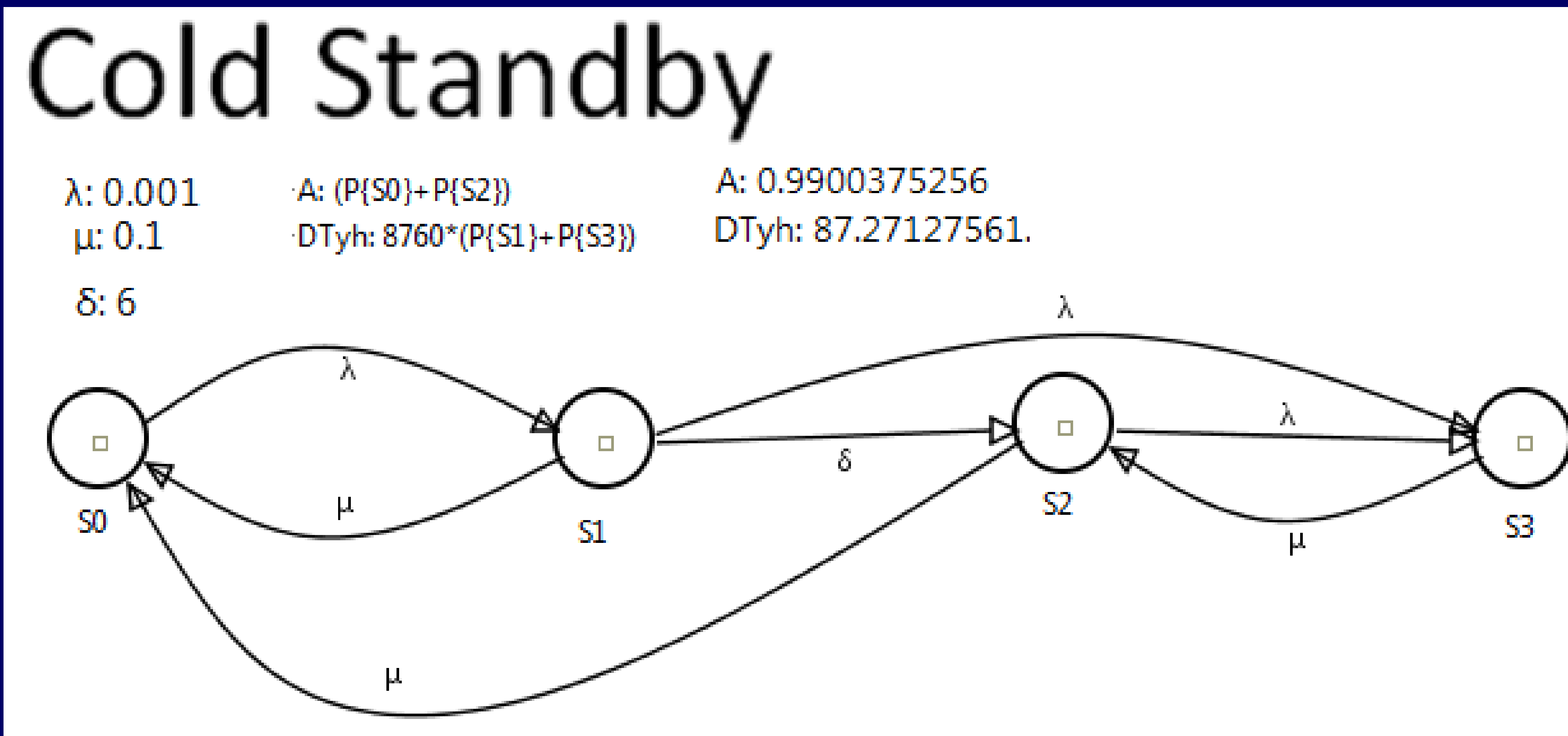


$$U(\beta, c) = \pi_0 + \pi_{1C} = \frac{\lambda\beta + \mu^2(1-c)}{\mu\beta E} \quad (E = \rho\pi_0^{-1})$$

$$D(\beta, c) = U(\beta, c) \times 8760 \times 60 \text{ (down time in min/year)}$$

CTMC

ColdStandbyCTMC_MC

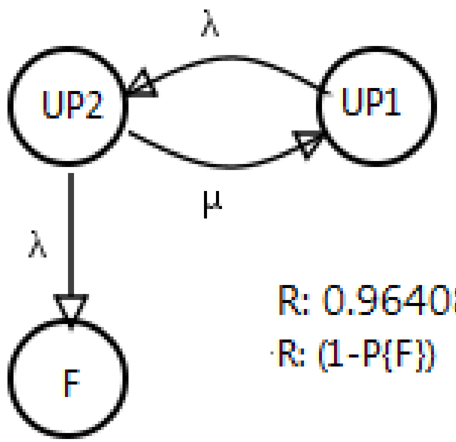


CTMC

Rel_CTMCColdStandby_PS_IC

Cold Standby
Reliability Model with Perfect Switching

λ: 0.001
μ: 0.1



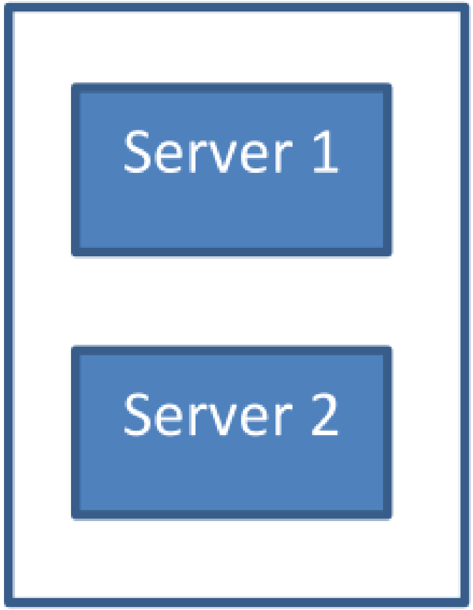
R: 0.9640809
R: (1-P{F})

MTTA: 101999.9999849

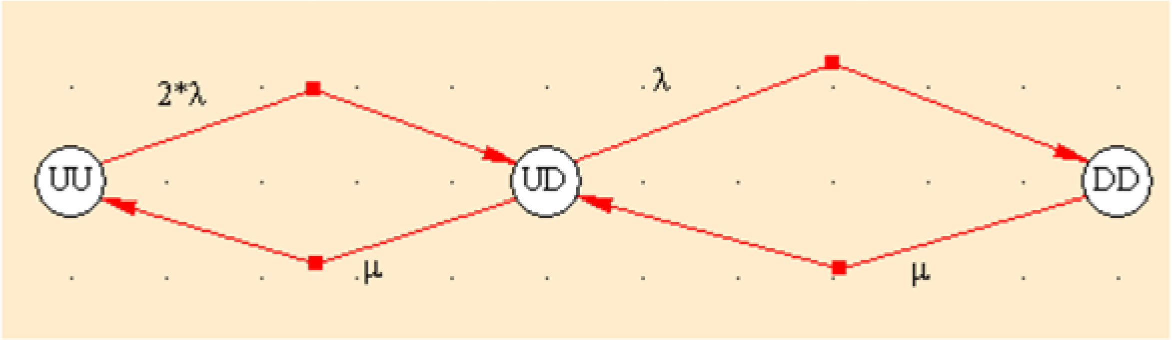
CTMC

Active-Active Redundancy

Consider a system with two parallel servers. The system is considered to be operational if at least one of the servers is operational.



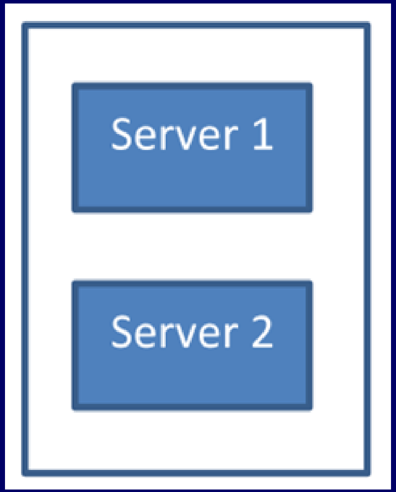
An availability model is represented by the following CTMC:



$$A = \pi(UU) + \pi(UD) = \frac{\mu(2\lambda + \mu)}{2\lambda^2 + 2\lambda\mu + \mu^2}$$

CTMC

Active-Active Redundancy

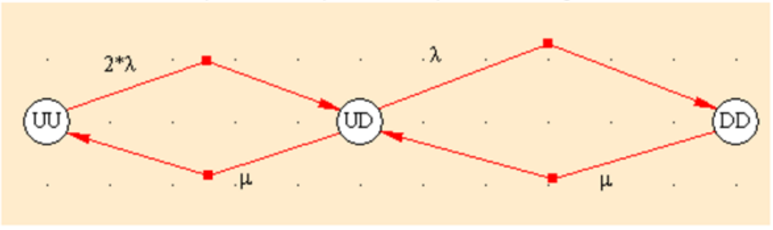


Capacity oriented availability

Now, if the users are interested not as much whether the system is operational or not, but rather in the service capacity the system may deliver. Considering the depicted architecture, it is assumed that if the two servers are operational, the system may deliver its full service capacity. If only one server is operational, the system may deliver only half of it service capacity. And when none of the servers is operational, the system may not deliver the service. Therefore Capacity Oriented Availability (COA) is:

$$COA = (2 \times \pi(UU) + \pi(DU)) / 2$$

An availability model is represented by the following CTMC:



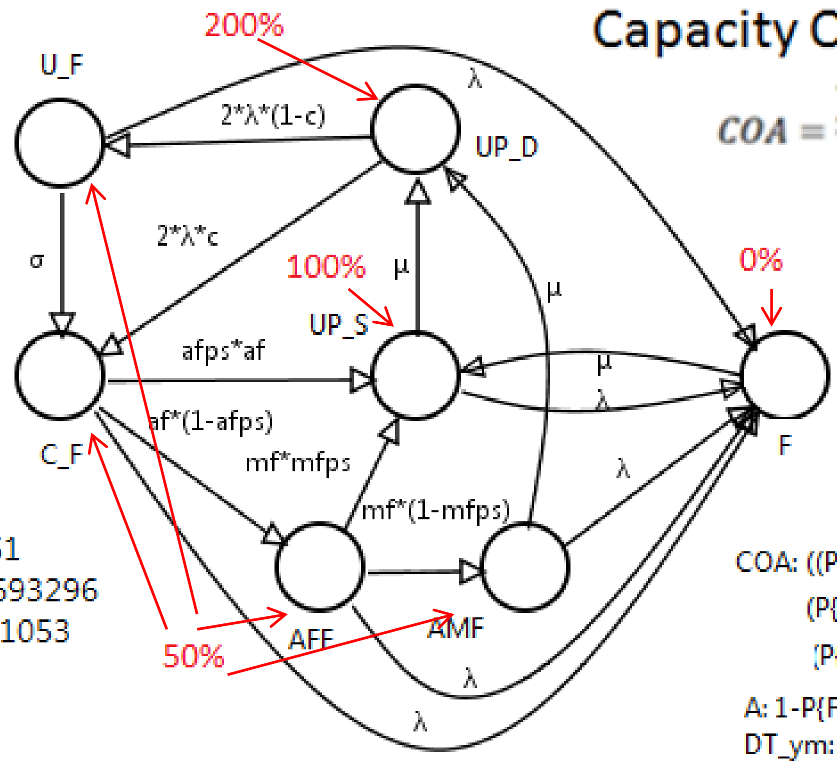
$$COA = \frac{\mu(\lambda + \mu)}{2\lambda^2 + 2\lambda\mu + \mu^2}$$

ActiveActiveF

CTMC

Active-Active system with imperfect fault coverage, automatic and manual failover mechanism

λ: 1/10000
μ: 1/24
σ: 0.25
af: 8
mf: 2
c: 0.99
afps: 0.95
mfps: 0.98
NS: 2



A: 0.9999952351
DT_ym: 6.0793693296
COA: 0.9975661053

Capacity Oriented Availability

$$COA = \frac{\sum_i^n \pi_i \times r_i}{NS}$$

$$r_i := \begin{cases} n_i & if\ i = UP\_D,\quad UP\_S \\ 0.5 \times n_i & if\ i = U\_F,\ C\_F,\ AFF,\ AMF \\ 0 & otherwise \end{cases}$$

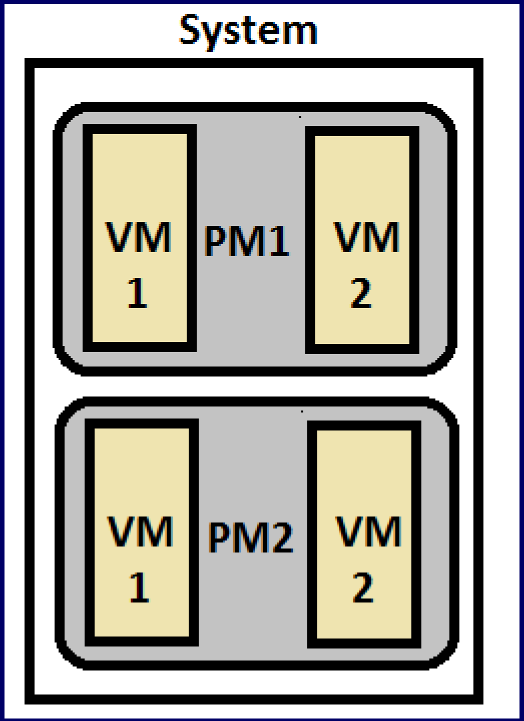
where $n_i \in \mathbb{N}$ is the number of active servers at state i.
NS is the total number of servers.

COA: ((P{UP_D}*R{UP_D})+(P{U_F}*R{U_F})+
(P{C_F}*R{C_F})+(P{UP_S}*R{UP_S})+(P{AFF}*R{AFF})+
(P{AMF}*R{AMF})+(P{F}*R{F}))/(NS)

A: 1-P{F}
DT_ym: ((P{F}*8760)*60)

CTMC

Capacity Oriented Availability in Cloud Systems
A Simple Example



State

$$s_i = (s_{PM_1}, s_{PM_2}, \#vm_{up})$$

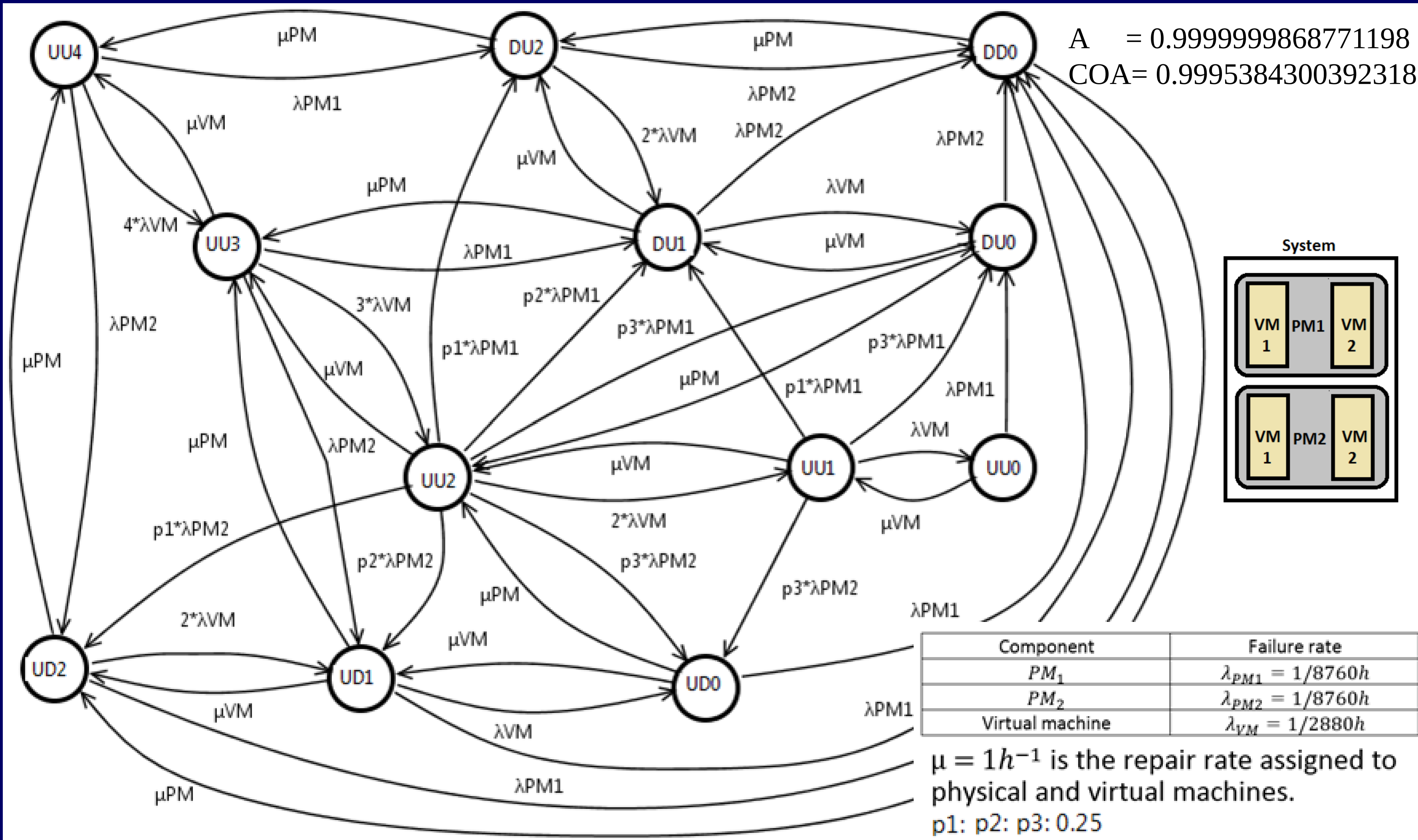
$$s_{PM_i} = \begin{cases} U & - Up \\ D & - Down \end{cases}$$

$$\#vm_{up} = \{1,2,3,4\}$$

Consider a system composed by two physical machines, PM1 and PM2, where each physical machine supports two virtual machines (VMs).

CTMC

Model 1



A = 0.9999999868771198
COA= 0.9995384300392318

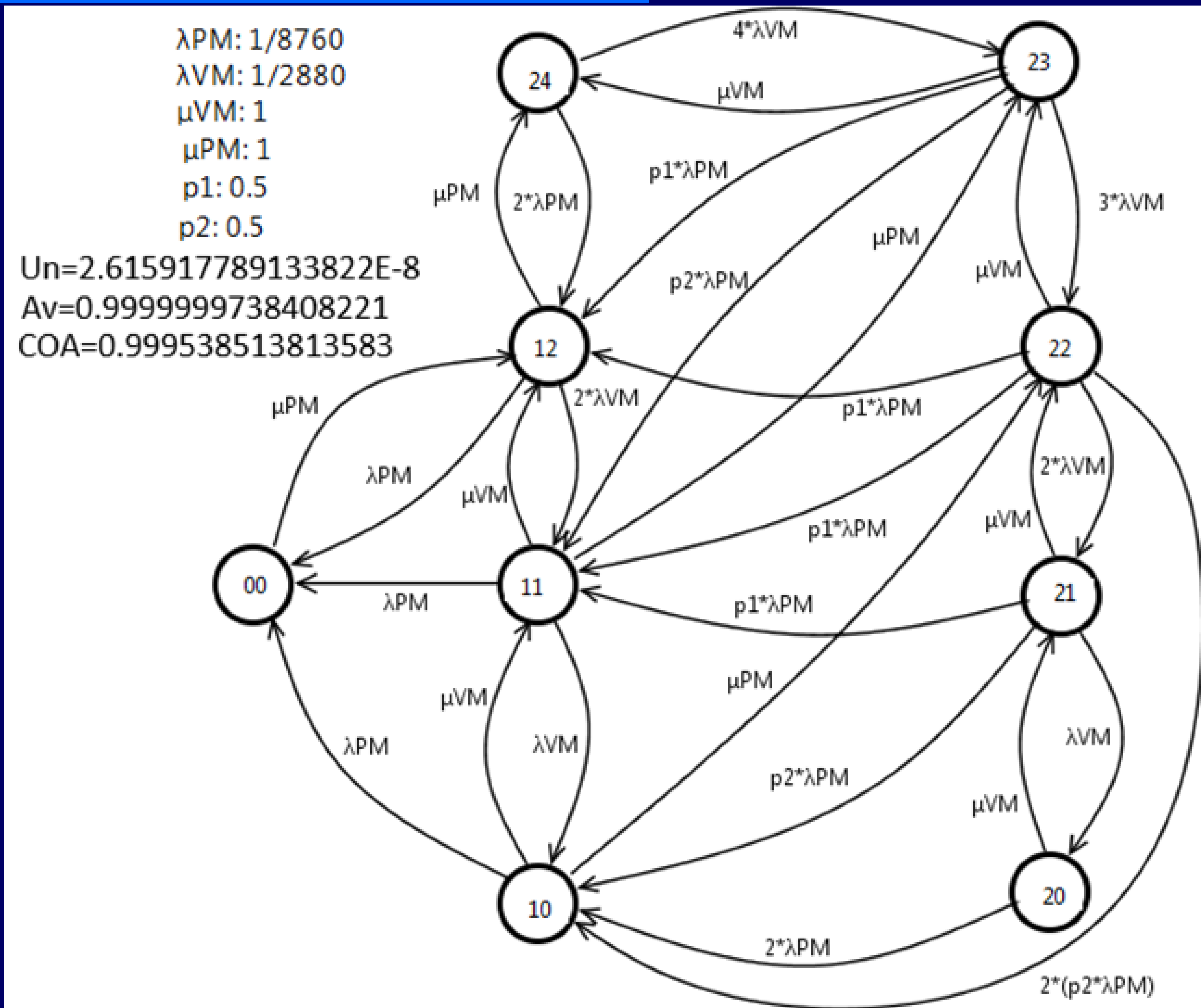
Component	Failure rate
PM_1	$\lambda_{PM1} = 1/8760h$
PM_2	$\lambda_{PM2} = 1/8760h$
Virtual machine	$\lambda_{VM} = 1/2880h$

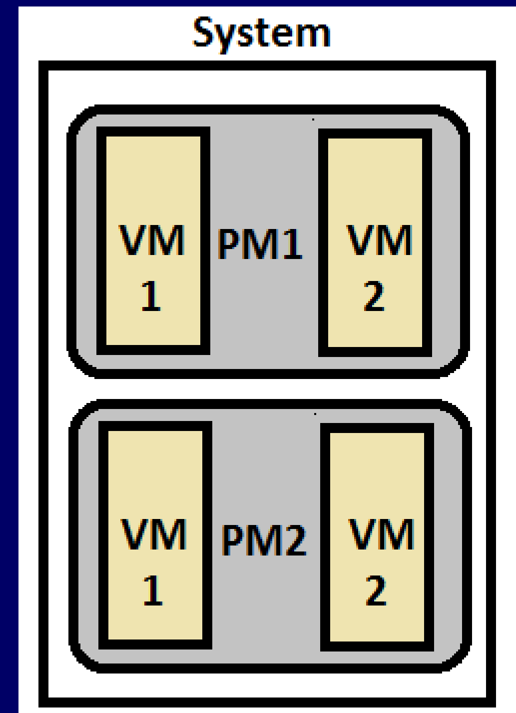
$\mu = 1h^{-1}$ is the repair rate assigned to physical and virtual machines.

p1: p2: p3: 0.25

CTMC

Model 2





$$s_i = (\#pm_{up}, \#vm_{up})$$

$$\#pm_{up} = \{1,2\}$$

$$\#vm_{up} = \{1,2,3,4\}$$

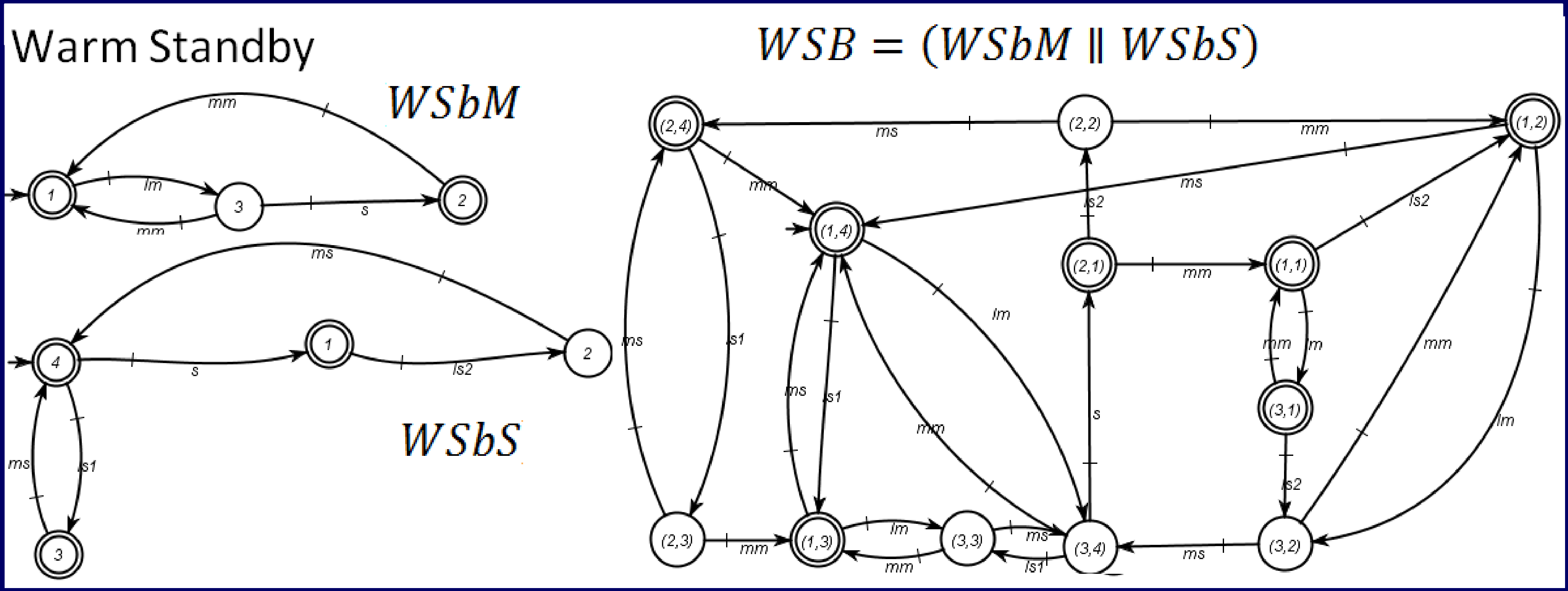
CTMC

Comparison

Model	A	COA
Model 1	0.9999999868771198	0.9995384300392318
Model 2	0.9999999738408221	0.999538513813583
Model 3	0.999999986909146	0.9995387092788293
Model 4	0.999999987	0.9995384342

CTMC

Warmstandby

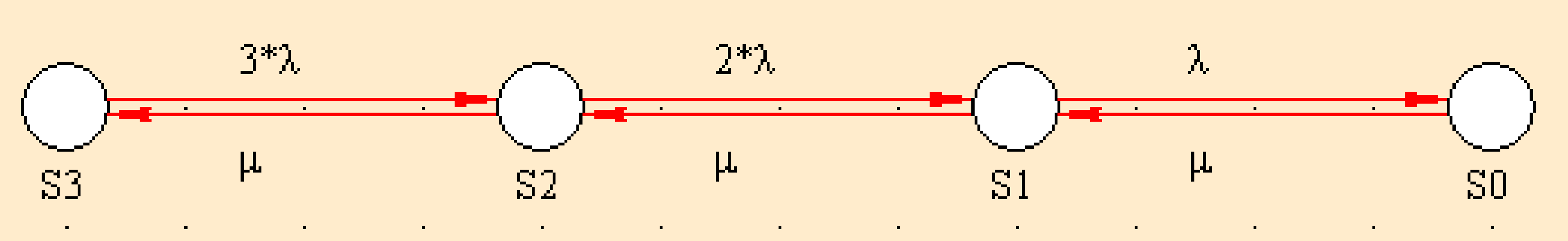


SPN

2 out of 3 with shared repair

Availability Model

The CTMC model:



$$\lambda = \frac{1}{8760}\ h^{-1}$$

$$\mu = \frac{1}{24} h^{-1}$$

Availability=$\pi(S_3) + \pi(S_2) =$ 9.99955210e-001

CTMC

- Example – Availability model

An equivalent 2-state availability model

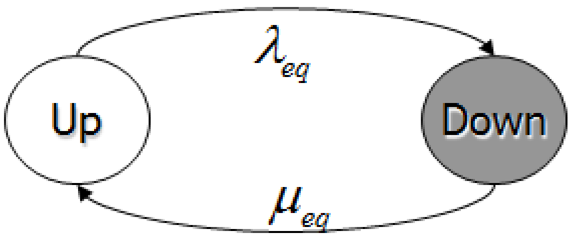
It is interesting to consider an equivalent 2-state availability model that has the same steady state availability as the given multi-state availability model.

To represent system availability in the simple form of equivalent 2-state system, we need to properly define equivalent failure rate λ_{eq} and equivalent repair rate μ_{eq}, such that

$$A = \frac{MTTF_{eq}}{MTTF_{eq} + MTTR_{eq}} = \frac{\mu_{eq}}{\lambda_{eq} + \mu_{eq}}$$

Failure rate of each machine is λ

Repair rate is μ



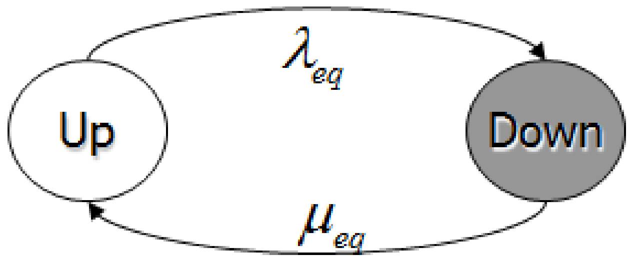
$$\lambda_{eq} = \frac{\lambda \pi_{M-1}}{\pi_0 + \pi_1 + \pi_2 + \ldots + \pi_{M-1}}$$

$$\mu_{eq} = \mu$$

CTMC

- Example – Availability model

An equivalent 2-state availability model



$$\lambda_{eq} = \frac{\lambda \pi_{M-1}}{\pi_0 + \pi_1 + \pi_2 + \ldots + \pi_{M-1}}$$

$$\mu_{eq} = \mu$$

Let *U* be the set of up states, *D* the set of down states, *R* the set of all transitions from *U* to *D*, *G* the set of all transition from *D* to *U*, t_{ij} the transition from state *i* to *j*

$$\lambda_{eq} = \sum_{t_{ij} \in R} P(\text{system in state } i \mid \text{system is up}) \times q_{ij} = \frac{\sum_{t_{ij} \in R} \pi_i \times q_{ij}}{\sum_{k \in U} \pi_k}$$

$$\mu_{eq} = \sum_{t_{ij} \in G} P(\text{system in state } i \mid \text{system is down}) \times q_{ij} = \frac{\sum_{t_{ij} \in G} \pi_i \times q_{ij}}{1 - \sum_{k \in U} \pi_k}$$

CTMC

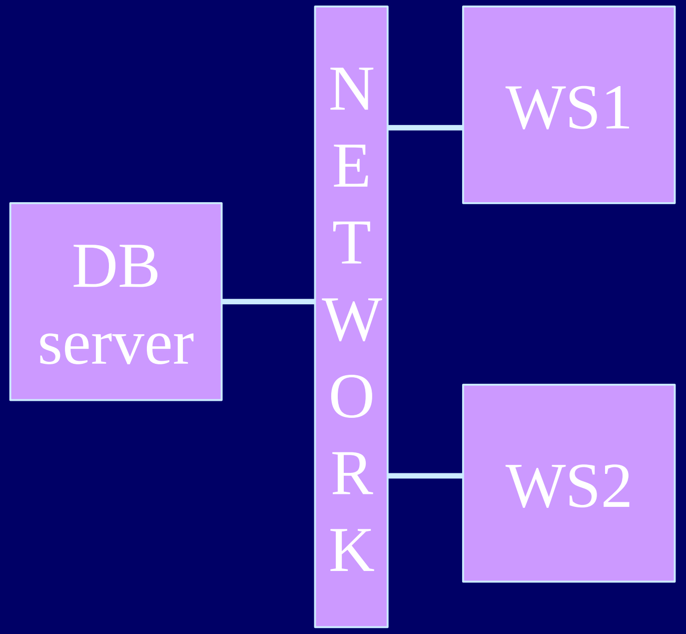
- Example

Consider a system consisting of two web-servers, one database server and a network infrastructure. The system is operational as long as one web-server and the database server are operational. It is assumed that a network infrastructure is fault-free. The database server repairing has priority over the web-servers' repairing activities. The failure rates of the web-servers and of the database server are constant (λ_{ws}, λ_{db} respectively), and the respective time to repair are exponentially distributed with rate μ_{ws} and μ_{db}.

$\lambda_{ws} = 1.14 \times 10^{-4}\ failures\ per\ hour$

$\lambda_{db} = 2.28 \times 10^{-4}\ failures\ per\ hour$

$\mu_{ws} = \mu_{db} = 4.17 \times 10^{-2}\ repairings\ per\ hour$

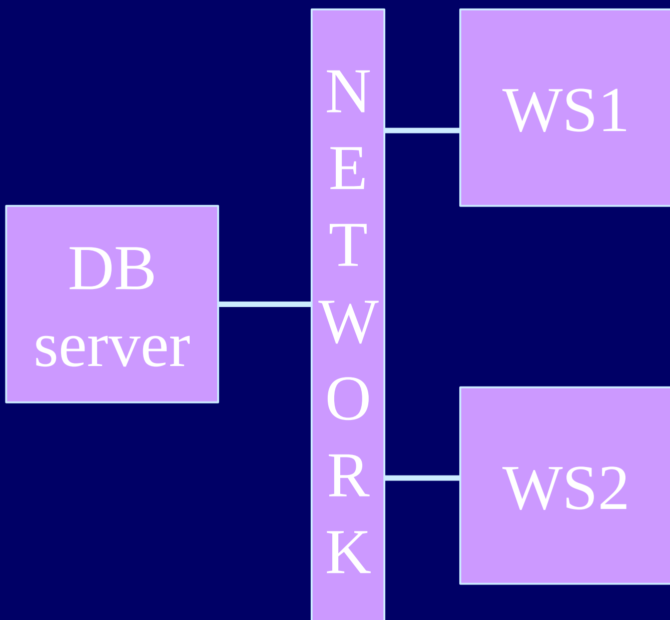


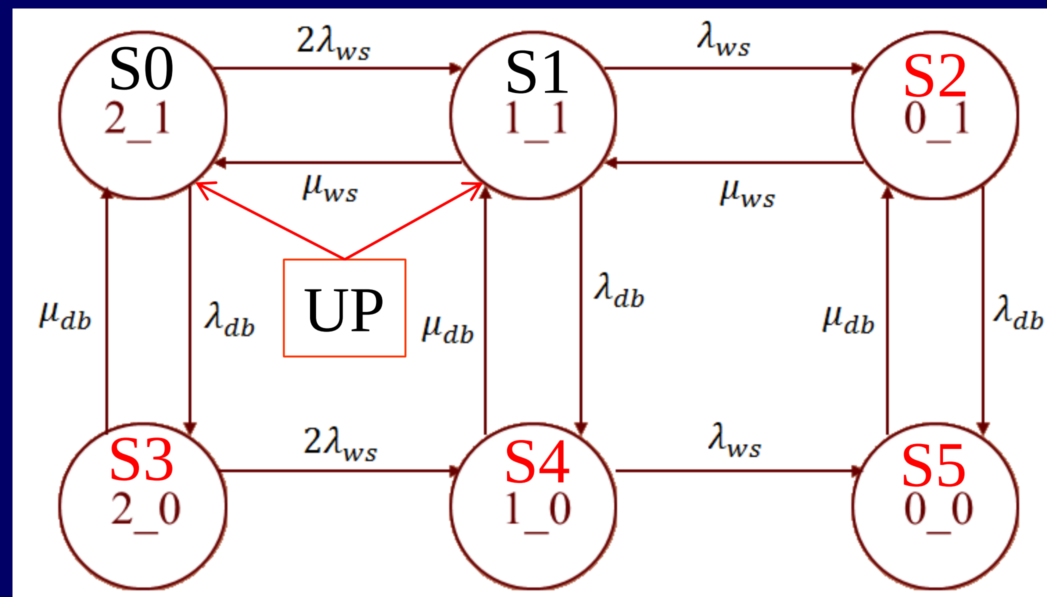
CTMC

ws1ws2dbs

Excel

- Example – Availability model





$\lambda_{ws} = 1.14 \times 10^{-4}$ *failures per hour*

$\lambda_{db} = 2.28 \times 10^{-4}$ *failures per hour*

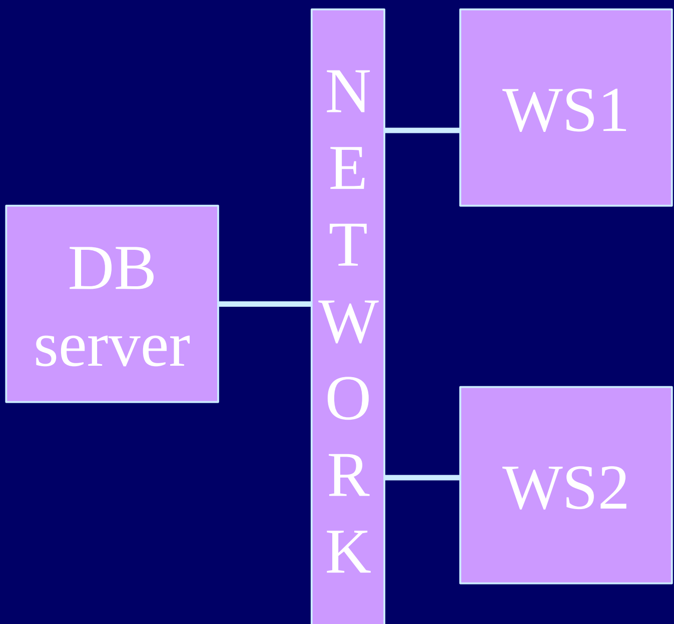
$\mu_{ws} = \mu_{db} = 4.17 \times 10^{-2}$ *repairings per hour*

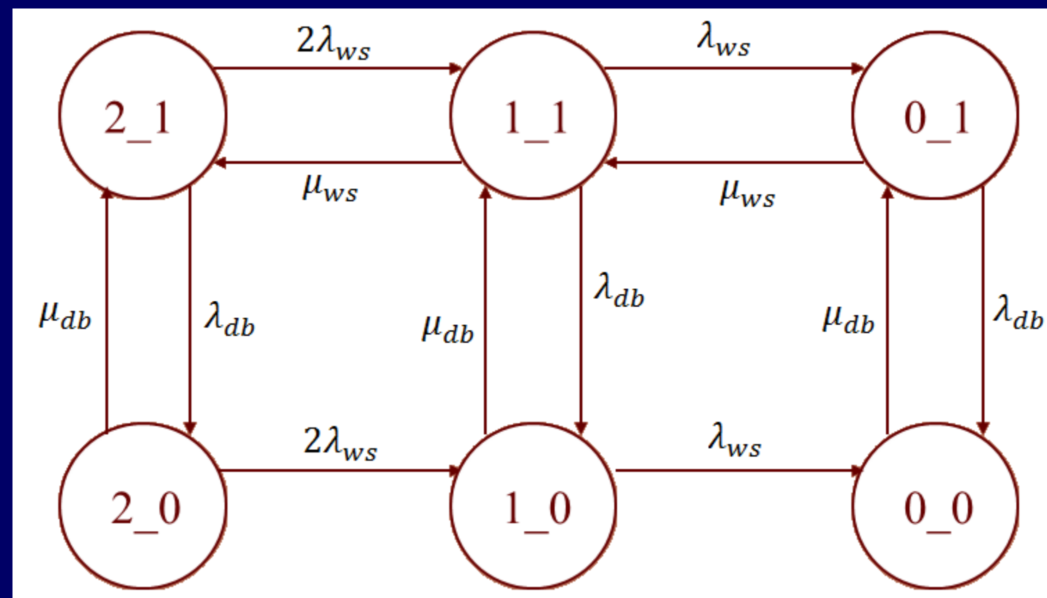
Si	πi	Up/Down
S0	0.98910959199	U
S1	0.00543748939	U
S2	0.00001502574	D
S3	0.00537867258	D
S4	0.00005897750	D
S5	0.00000024281	D
A	0.99454708138	

CTMC

Excel

- Example – Availability model





$\lambda_{ws} = 1.14 \times 10^{-4}$ *failures per hour*

$\lambda_{db} = 2.28 \times 10^{-4}$ *failures per hour*

$\mu_{ws} = \mu_{db} = 4.17 \times 10^{-2}$ *repairings per hour*

$A = \pi_{2\_1} + \pi_{1\_1} = 0.994547080$

$Downtime = (1 - A) \times T = 2866.05467\ minutes$

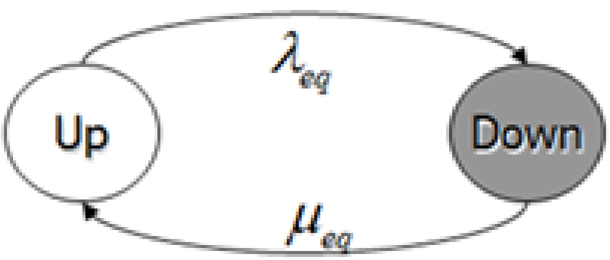
$T = 8760h \times 60min = 525{,}600\ minutes$ in one year.

CTMC

Excel

- Example – Availability model

The equivalent two-state model

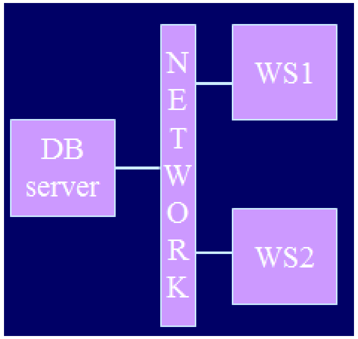


$$\lambda_{eq} = \sum_{t_{ij} \in R} P(\text{system in state } i \mid \text{system is up}) \times q_{ij} = \frac{\sum_{t_{ij} \in R} \pi_i \times q_{ij}}{\sum_{k \in U} \pi_k}$$

$$\mu_{eq} = \sum_{t_{ij} \in G} P(\text{system in state } i \mid \text{system is down}) \times q_{ij} = \frac{\sum_{t_{ij} \in G} \pi_i \times q_{ij}}{1 - \sum_{k \in U} \pi_k}$$

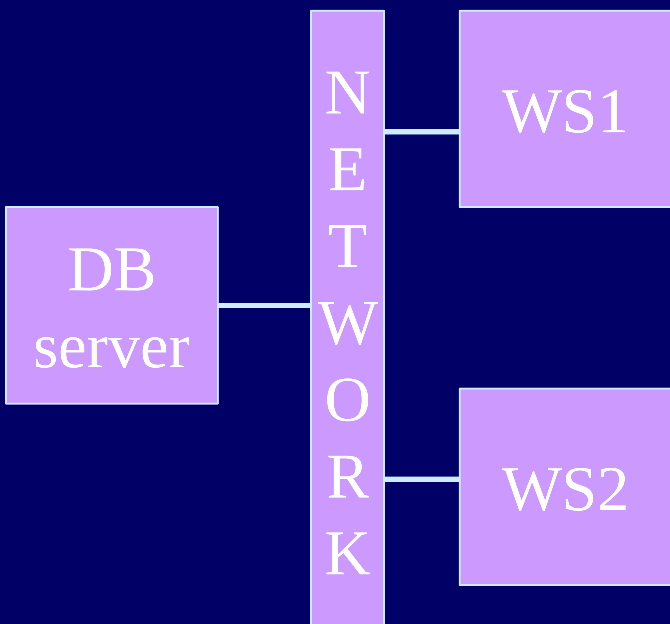
λ_eq	0.000228623
μ_eq	0.041698143

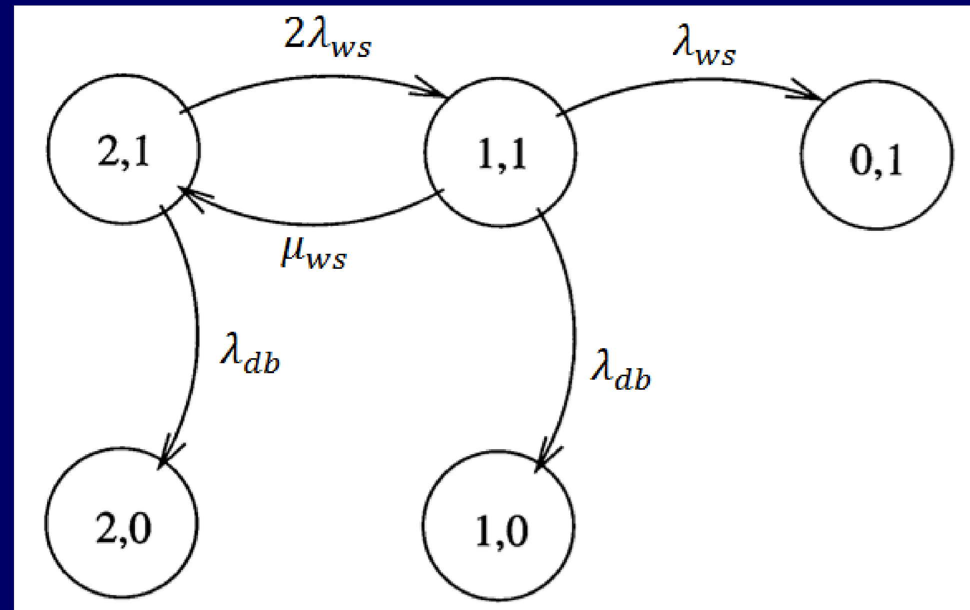
Si	πi
UP	0.99454708138
Down	0.00545291862
A_rm	0.99454708138



CTMC

- Example – Reliability model





States (0,1), (1,0) and (2,0) are absorbing states and (2,1) and (1,1) are transient states.

Absorbing states can be combined into a single one.

$\lambda_{ws} = 1.14 \times 10^{-4}$ *failures per hour*

$\lambda_{db} = 2.28 \times 10^{-4}$ *failures per hour*

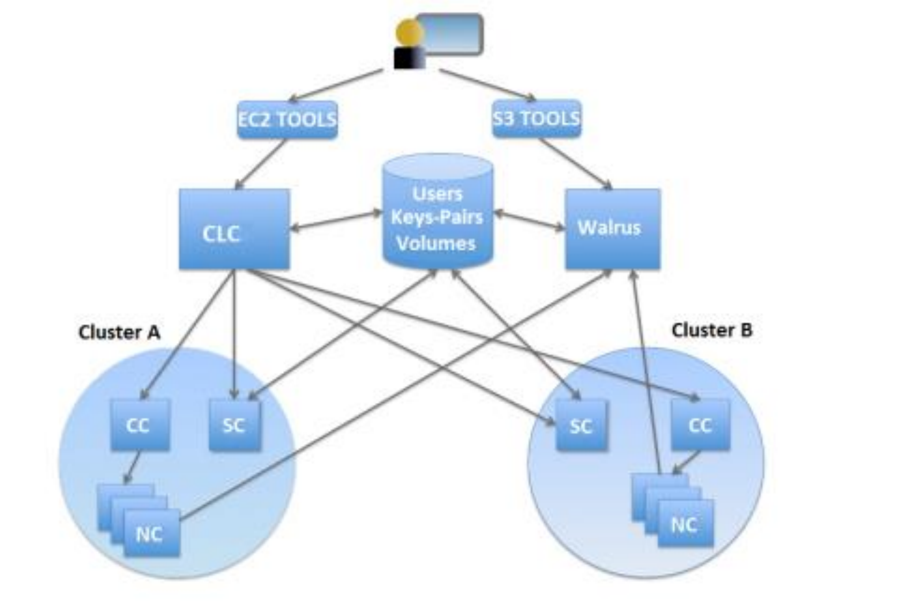
$\mu_{ws} = \mu_{db} = 4.17 \times 10^{-2}$ *repairings per hour*

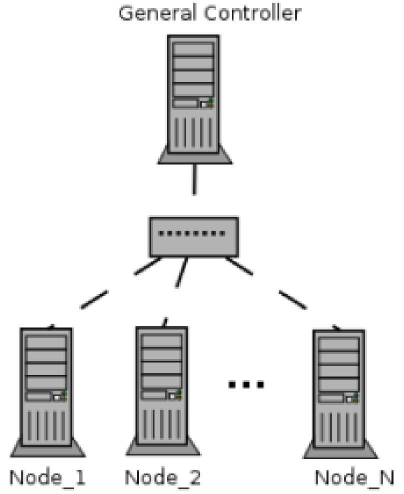
$$R(t) = \pi_{2,1}(t) + \pi_{1,1}(t)$$

CTMC

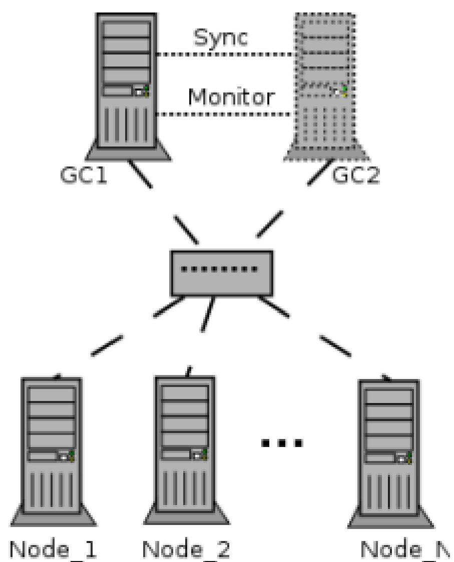
- Example - Availability model

EUCALYPTUS is composed by five high-level components: Cloud Controller, Cluster Controller, Node Controller, Storage Controller, and Walrus. The Cloud Controller (CLC) is responsible for exposing and managing th underlying virtualized resources (servers, network, and storage).





No redundancy

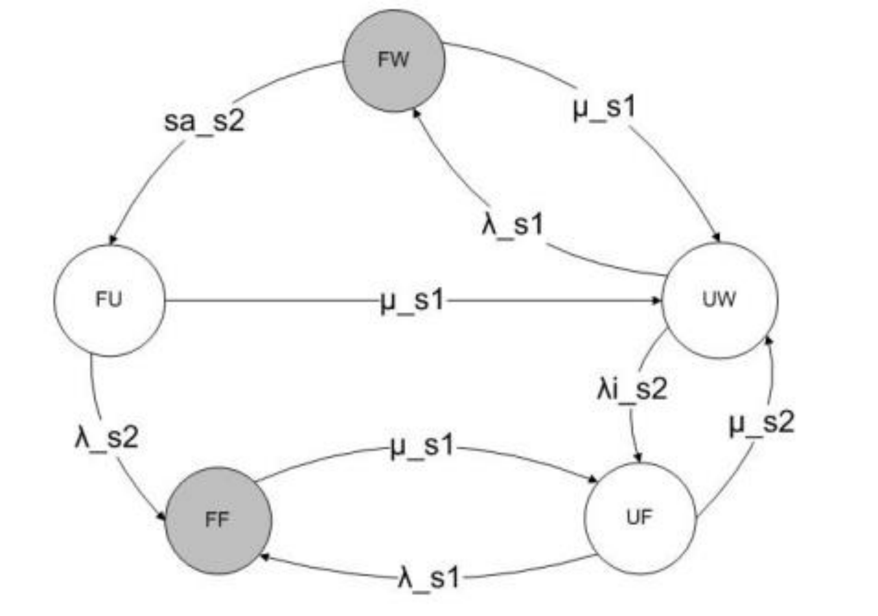


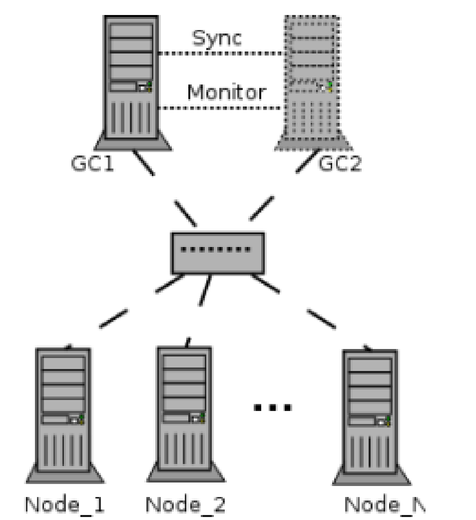
Redundancy in the GC

CTMC

- Example - Availability model

EUCALYPTUS is composed by five high-level components: Cloud Controller, Cluster Controller, Node Controller, Storage Controller, and Walrus. The Cloud Controller (CLC) is responsible for exposing and managing th underlying virtualized resources (servers, network, and storage).





Redundancy in the GC

Parameter	Description	Value
$\lambda\_s1 = \lambda\_s2 = 1/\lambda$	Mean time for host failure	$1/180.721$
$\lambda_i\_s2 = 1/\lambda_i$	Mean time for inactive host failure	$1/216.865$
$\mu\_s1 = \mu\_s2 = 1/\mu$	Mean time for host repair	$1/0.9667$
$sa\_s2 = 1/sa$	Mean time to system activate	$1/0.005$

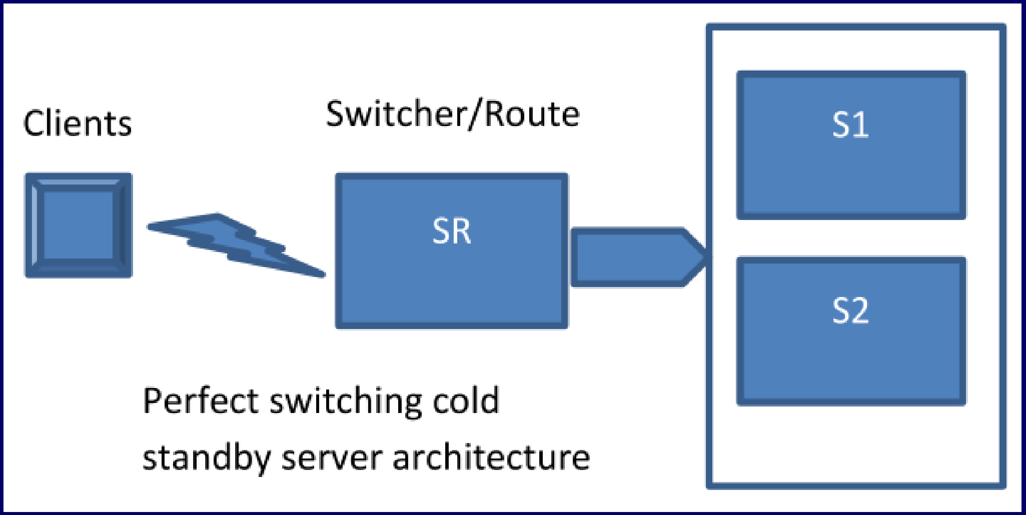
$$A_{GC} = \frac{\mu(\lambda_i(\mu + sa) + \mu^2 + sa(\lambda + \mu))}{\lambda_i(\lambda + \mu)(\mu + sa) + \mu^2(\lambda + \mu) + sa(\lambda^2 + \lambda\mu + \mu^2)}$$

CTMC

- Example – Reliability model

System composed by Two Subsystem:

One Switch/Router and Server Cluster



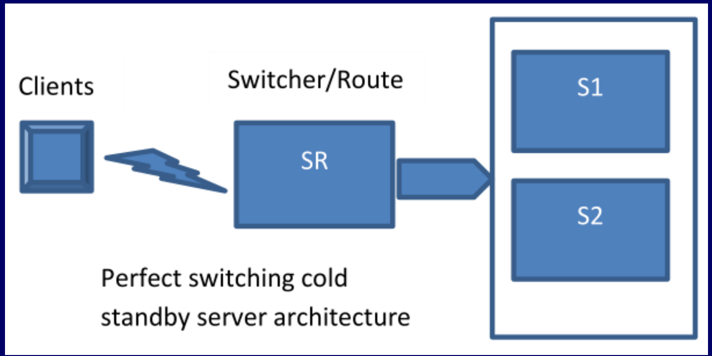
The system is composed by a Switcher/Router and Serve subsystem. The system fails if the Switcher/Router fails OR if the Serve subsystem fails. The Server subsystem is composed by two servers, S1 and S2. S1 is the main server and S2 is the spare server. They are configured in Cold Standby, that is, S2 starts as soon as S1 fails. The start-up time of S2 is zero. This is named perfect switching.

CTMC

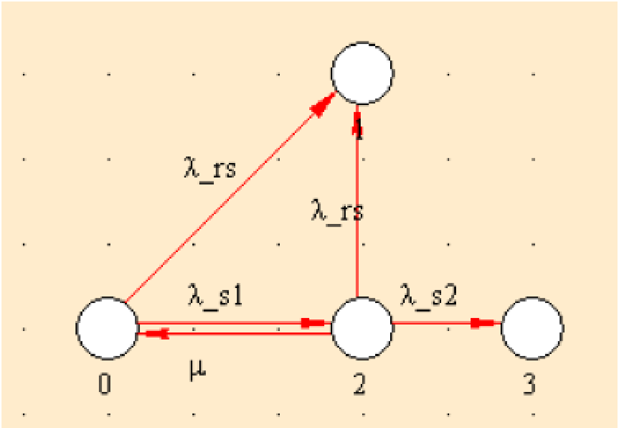
- Example – Reliability model

System composed by Two Subsystem:

One Switch/Router and Server Cluster



The CTMC reliability model



Absorbing states can be combined into a single one

Variable	Value
lambda_rs	1/2000
lambda_s1	1/15000
mu	1/24
lambda_s2	1/15000

The unity of these rates is h^{-1}.

System Unreliability:

UR(4000h)= 0.181615244

System Reliability:

R(4000h) = 0.818384756

λ_{rs} is failure rate of the Switcher/Router.

λ_{s1} is failure rate of the Server 1.

λ_{s2} is failure rate of the Server 2.

μ is the repair rate assigned to Server 1 repair activity.

CTMC

- Preventive Maintenance

Preventive maintenance is useful when the time to failure distribution has an increasing failure rate.

Two main strategies:

Condition-based (inspection-based) PM considered here

Time-Based PM

We model TTF by Hypoexponential HYPO(λ_1, λ_2) distribution.

Time to trigger inspection is assumed to be EXP(λ_{in}),

Time to carry out inspection is EXP(μ_{in}),

Time to repair is EXP(μ),

Time to carry out PM is EXP($y\mu$).

CTMC

- Preventive Maintenance

Preventive maintenance is useful when the time to failure distribution has an increasing failure rate.

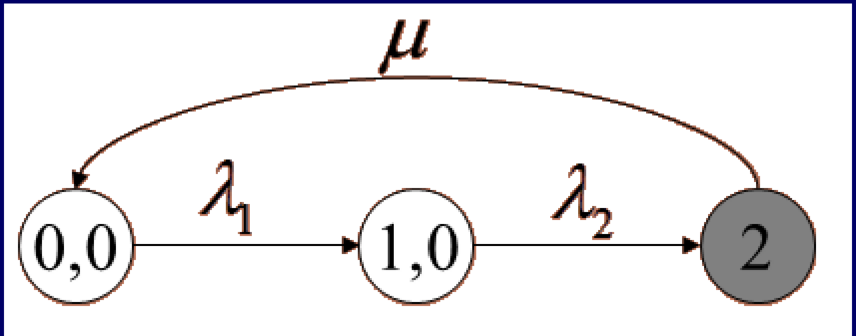
CTMC with corrective maintenance only

Time to failure is HYPO(λ_1, λ_2);

(0,0) & (1,0) are up states;

2 is a down state

Time to corrective maintenance is EXP(μ)



CTMC

- Preventive Maintenance

Preventive maintenance is useful when the time to failure distribution has an increasing failure rate.

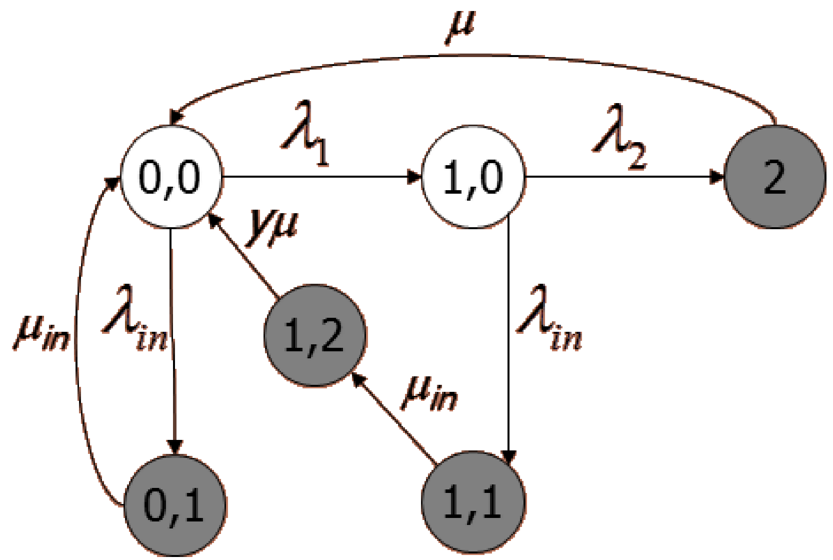
CTMC with preventive maintenance

Inspection triggered after EXP(λ_{in}) intervals

Time to carry out inspection is EXP(μ_{in})

Time to carry out PM is EXP($y\mu$)

PM carried out if inspection finds the system to be in degraded state (1,0)



$$A = \pi_{0,0} + \pi_{1,0}$$

CTMC

- Preventive Maintenance

Preventive maintenance is useful when the time to failure distribution has an increasing failure rate.

$\lambda_1 = 0.001\ h^{-1}$

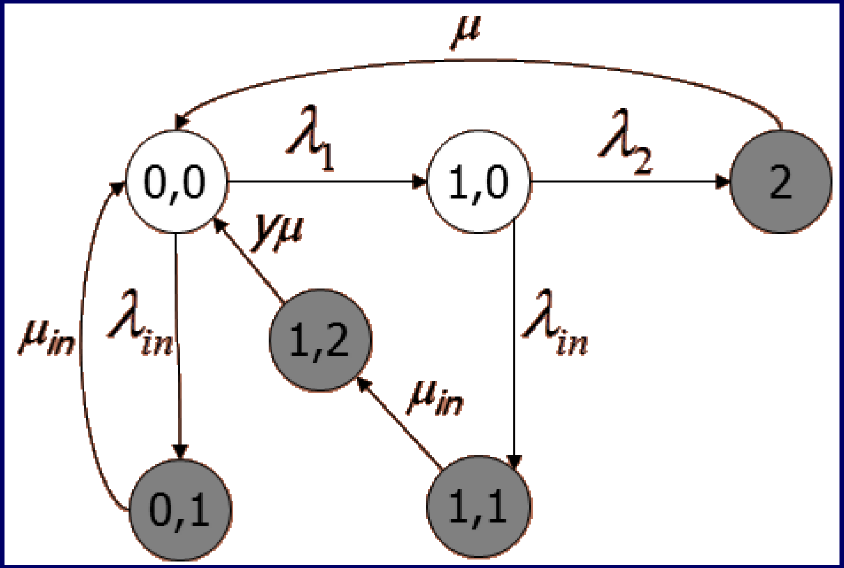
$\lambda_2 = 0.001\ h^{-1}$

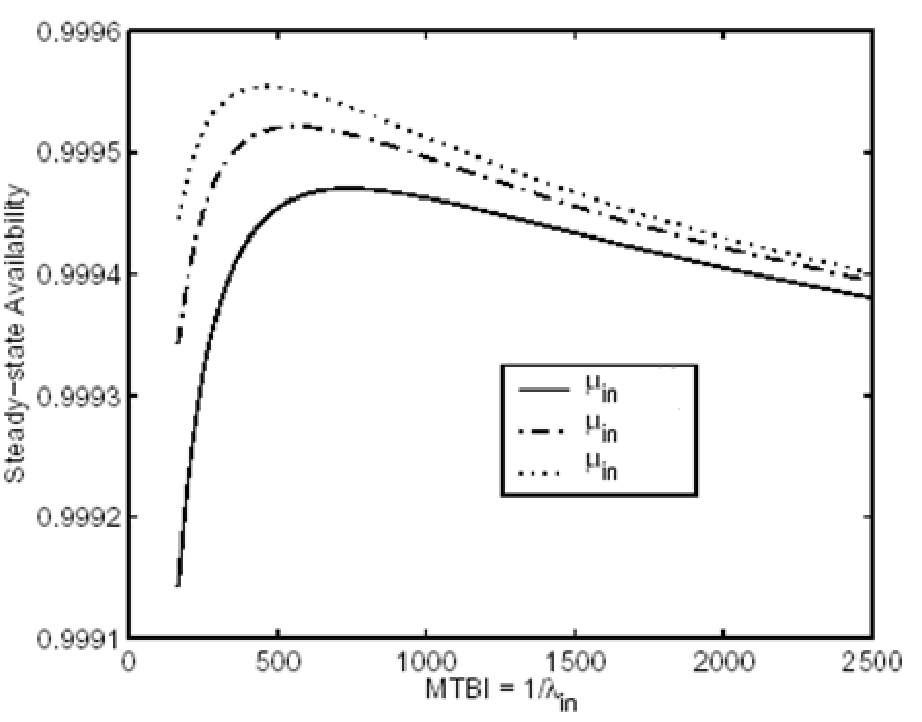
$\mu_{in} = 10\ h^{-1}$

$\mu = 0.1\ h^{-1}$

$y = 5$

$\lambda = 0.0005\ h^{-1}$





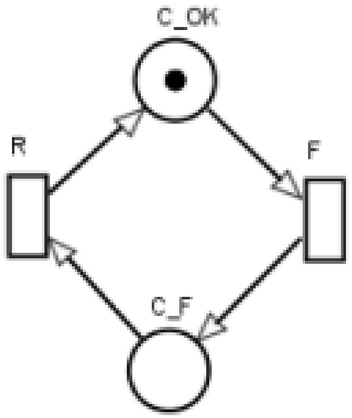
$$A = \pi_{0,0} + \pi_{1,0}$$

MTBI – mean time between inspections

Availability as function of MTBI=$1/\lambda_{in}$

SPN

Single Component System Availability Model



Transition	Time	Time	Type of Service
F	*MTTF*	λ	*single Server*
R	*MTTR*	μ	*single Server*

The instantaneous availiability :

$$A(t) = P\{(m(C\_OK) = 1)(t)\}$$

$$= \sum_{\forall M_i \in RS} r_i \times \pi_i(t) = \frac{\lambda e^{-t(\lambda+\mu)} + \mu}{\lambda + \mu}$$

Downtime in period T :

$$DT = T \times P\{(m(C\_F) = 1)\} = T \times \left(1 - \frac{\lambda}{\lambda+\mu}\right)$$

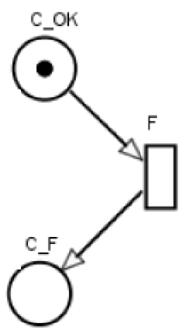
The stationary availability :

$$A = P\{(m(C\_OK) = 1)\} = \sum_{\forall M_i \in RS} r_i \times \pi_i = \frac{\lambda}{\lambda + \mu}$$

$$r_i = \begin{cases} 1 & se\ \ m_i(C\_OK) = 1 \\ 0 & se\ m_i(C\_OK) = 0 \end{cases}$$

SPN

Single Component System Reliability Model



Transition	Time	Time	Type of Service
F	*MTTF*	λ	*single Server*

Although the reliability of the basic component is analytically defined by $R(t) = e^{-t\lambda}$, it is possible to calculate the respective value through numerical transient analysis, once the transiton R. is removed. The reliability can be calculated by:

$$R(t) = P\{(m(C\_OK) = 1)(t)\} = \sum_{\forall M_i \in RS} r_i \times \pi_i\,(t),$$

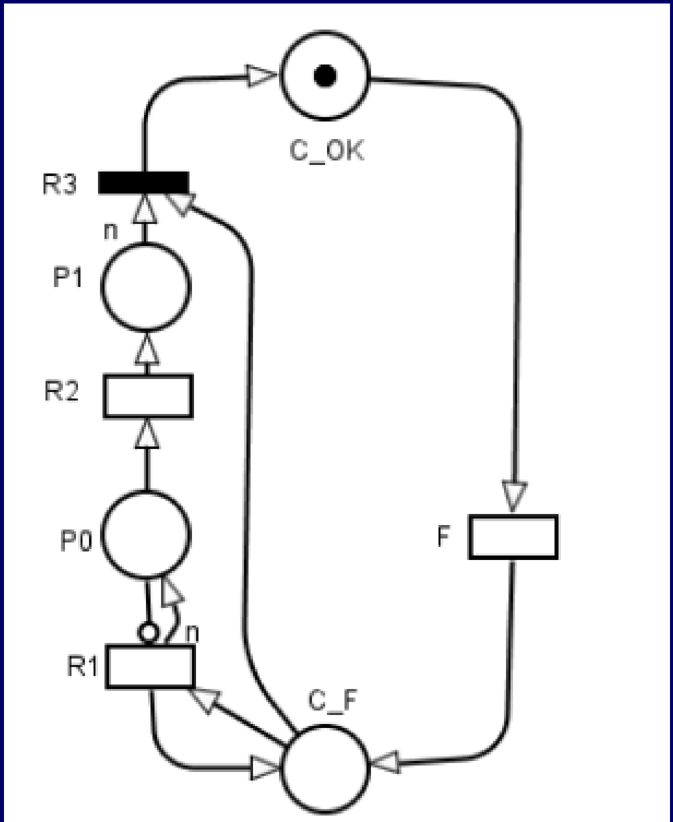
where

$$r_i = \begin{cases} 1 & se\;\; m_i(C\_OK) = 1 \\ 0 & se\; m_i(C\_OK) = 0 \end{cases}$$

SPN

Basic Model with Erlang Distributed Repair Time

Availability Model



$$A = P\{(m(C\_OK) = 1)\} = \sum_{\forall M_i \in RS} r_i \times \pi_i,$$

$$r_i = \begin{cases} 1 & se\ \ m_i(C\_OK) = 1 \\ 0 & se\ m_i(C\_OK) = 0 \end{cases}$$

$$E[T_E] = \overline{X} \quad \text{e} \quad DP[T_E] = SD$$

$$n = \left(\frac{\overline{X}}{DP}\right)^2$$

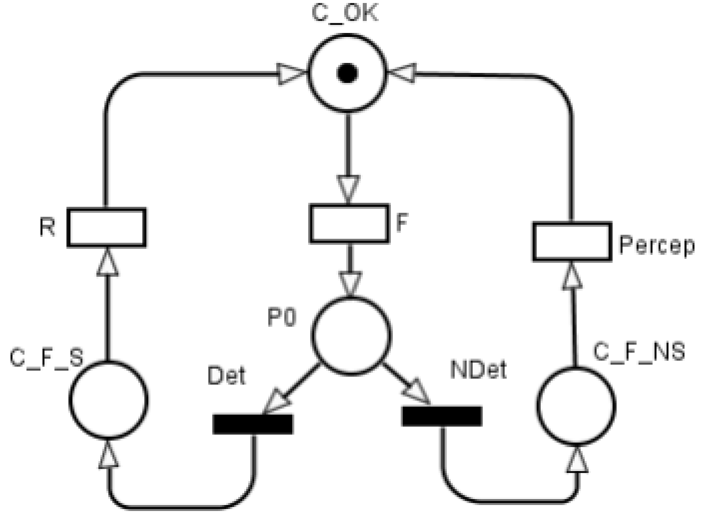
$$\lambda = \frac{n}{\overline{X}}$$

Transition	Type	Time or weight	Rate	Type of service
F	*E*	*MTTF*	$\lambda = \frac{1}{MTTF}$	*single Server*
R1	*E*	*MTTR/n*	$\mu = \frac{n}{MTTR}$	*single Server*
R2	*E*	*MTTR/n*	$\mu = \frac{n}{MTTR}$	*single Server*
R3	*I*	*W=1*		

Basic Model with the Erlang Distributed Repair Time

SPN

Basic Model with imperfect coverage availability model



$$A = P\{(m(C\_OK) = 1)\} = \sum_{\forall M_i \in RS} r_i \times \pi_i$$

$$r_i = \begin{cases} 1 & se\ m_i(C\_OK) = 1 \\ 0 & se\ m_i(C\_OK) = 0 \end{cases}$$

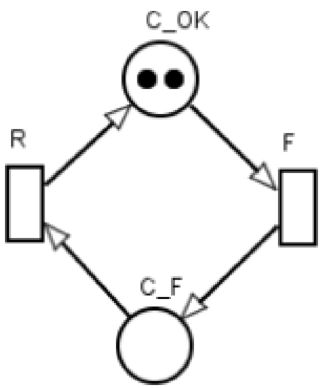
Transition	Type	Time or Wieght	Rate	Type of Service
F	*E*	*MTTF*	λ	*single server*
Det	*I*	W_{Det}		
Ndet	*I*	W_{NDet}		
Percep	*E*	*MTTP*	β	*single server*
R	*E*	*MTTR*	μ	*single server*

Failure Coverage Basic Model

SPN

Hot Standby Model

Availability Model



$$A = P\{(m(C\_OK) = 2) \vee (m(C\_OK) = 1)\}$$

$$= \sum_{\forall M_i \in RS} r_i \times \pi_i = 1 - \frac{2\lambda^2}{2\lambda^2 + 2\lambda\mu + \mu^2},$$

$$r_i = \begin{cases} 1 & se\ \ (m(C_{OK}) = 2) \vee (m(C_{OK}) = 1) \\ 0 & se\ m_i(C\_OK) = 0. \end{cases}$$

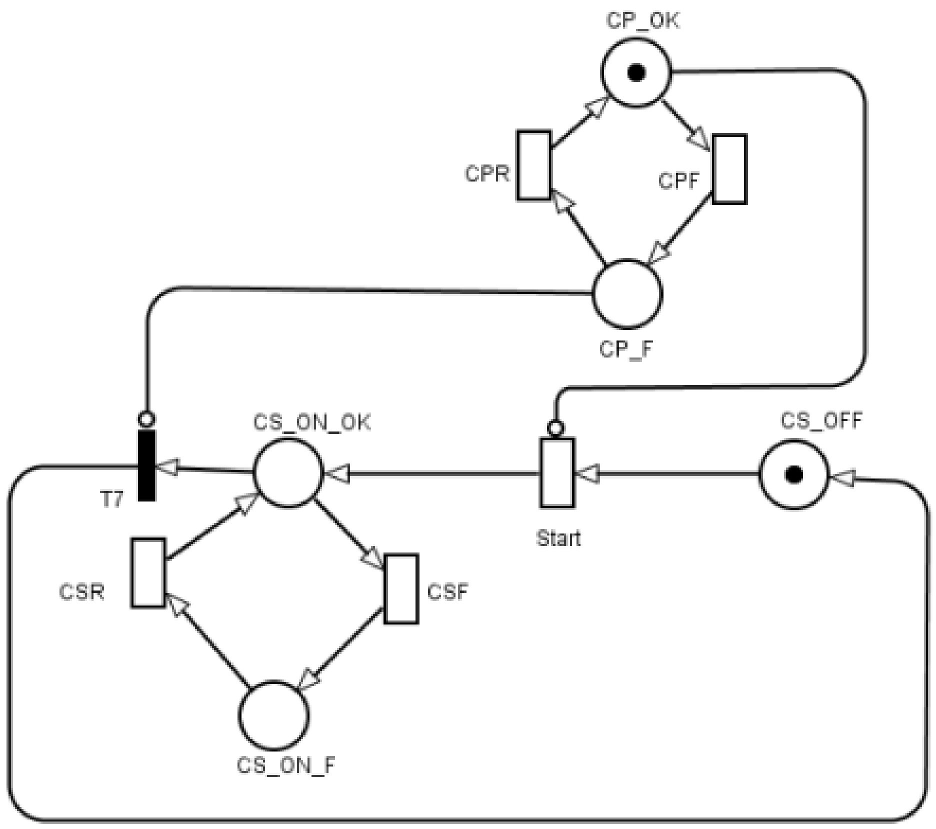
Transition	Type	Rate	Type of Service
F	*MTTF*	λ	*infinity Server*
R	*MTTR*	μ	*single Server*

SPN

Cold Standby

Availability Model

Transition	Type	Time or Weight	Rate	Type of Service
CPF	*E*	*MTTF_CP*	λ	*single server*
CPR	*E*	*MTTR_ CP*	μ	*single server*
CSF	*E*	*MTTF_CS*	α	*single server*
CSR	*E*	*MTTR_ CS*	β	*single server*
Start	*E*	*TTS*	μ	*single server*
T7	*I*	*W=1*		



The stationary availability of the component is calculated by the expression:

$$A = P\{((m(CP\_OK) = 1) \vee (m(CS\_ON\_OK) = 1))\} = \sum_{\forall M_i \in RS} r_i \times \pi_i$$

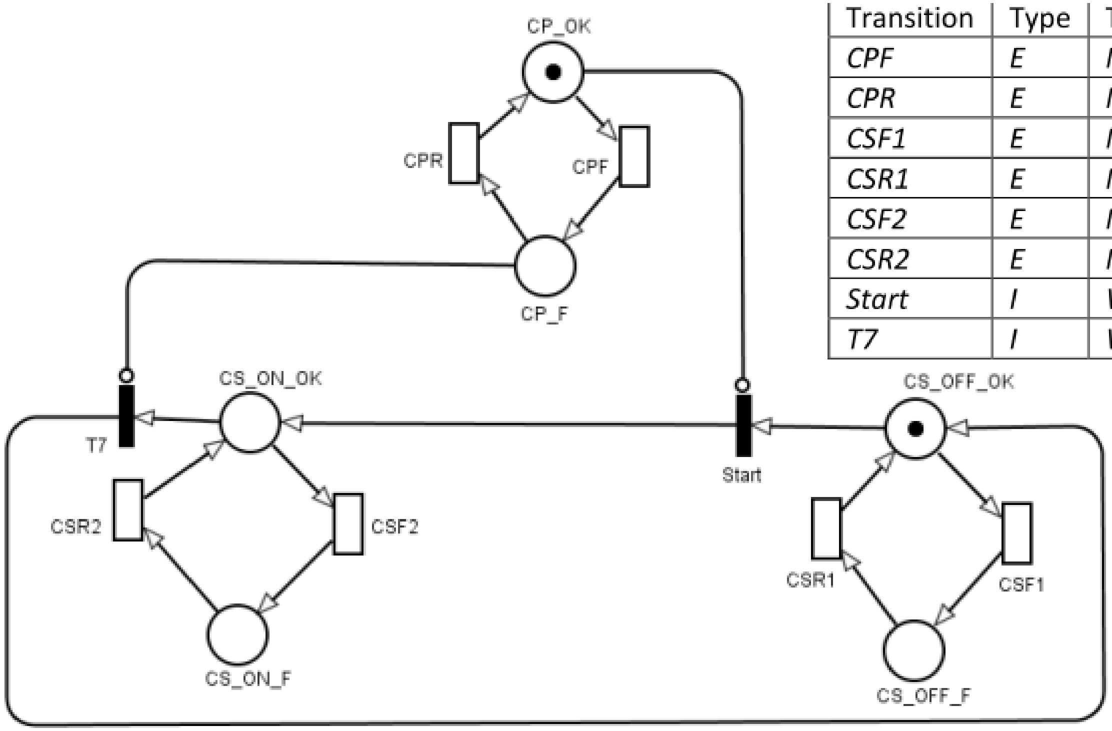
where r_i is a function that

$$r_i = \begin{cases} 1 & se \ (m(CP\_OK) = 1) \vee (m(CS\_ON\_OK) = 1) \\ 0 & se \ (m(CP\_OK) = 0) \wedge (m(CS\_ON\_OK) = 0) \end{cases}$$

SPN

Warm Standby
Availability Model

The *Warm Standby* model is similar to the *Cold Standby* model. However, in a system with *Warm Standby* redundancy, the reserve component remains energized (but inoperative), so that, when the main component fails, the reserve component takes over operations without the delay that occurs in a *Cold Standby* system.



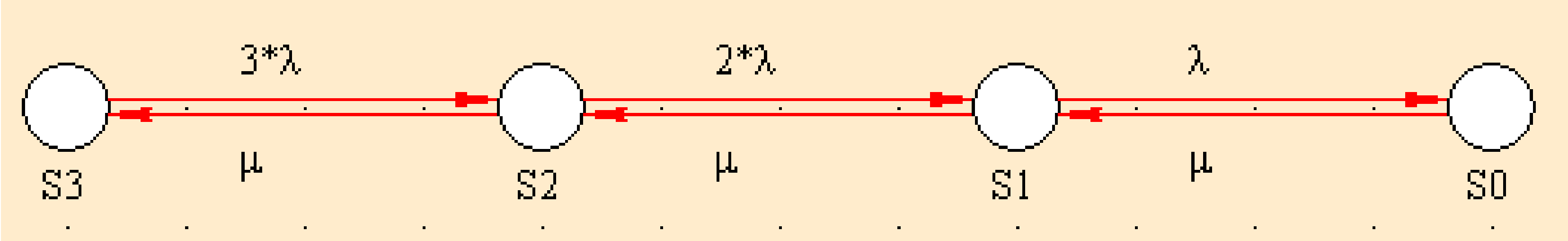
Transition	Type	Time or Weight	Rate	Type of Service	Priority
CPF	*E*	*MTTF_CP*	λ	*single server*	
CPR	*E*	*MTTR_ CP*	μ	*single server*	
CSF1	*E*	*MTTF1_CS*	α	*single server*	
CSR1	*E*	*MTTR1_ CS*	β	*single server*	
CSF2	*E*	*MTTF2_CS*	α	*single server*	
CSR2	*E*	*MTTR2_ CS*	β	*single server*	
Start	*I*	*W=1*			*1*
T7	*I*	*W=1*			*1*

SPN

2 out of 3 with shared repair

Availability Model

The CTMC model:



$$\lambda = \frac{1}{8760}\, h^{-1}$$

$$\mu = \frac{1}{24} h^{-1}$$

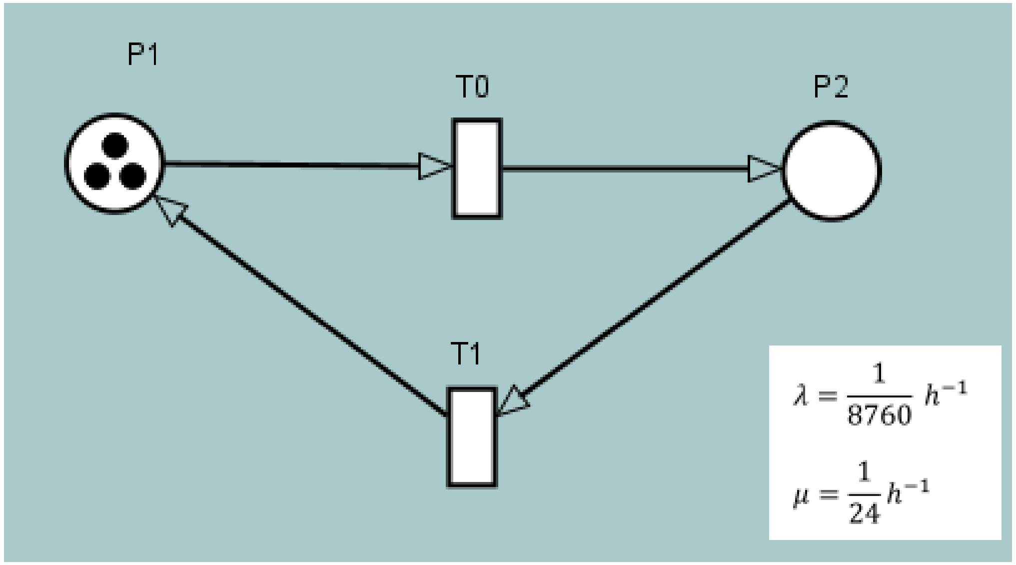
Availability=$\pi(S_3) + \pi(S_2) =$ 9.99955210e-001

SPN

2 out of 3 with shared repair

Availability Model

The equivalent SPN model:

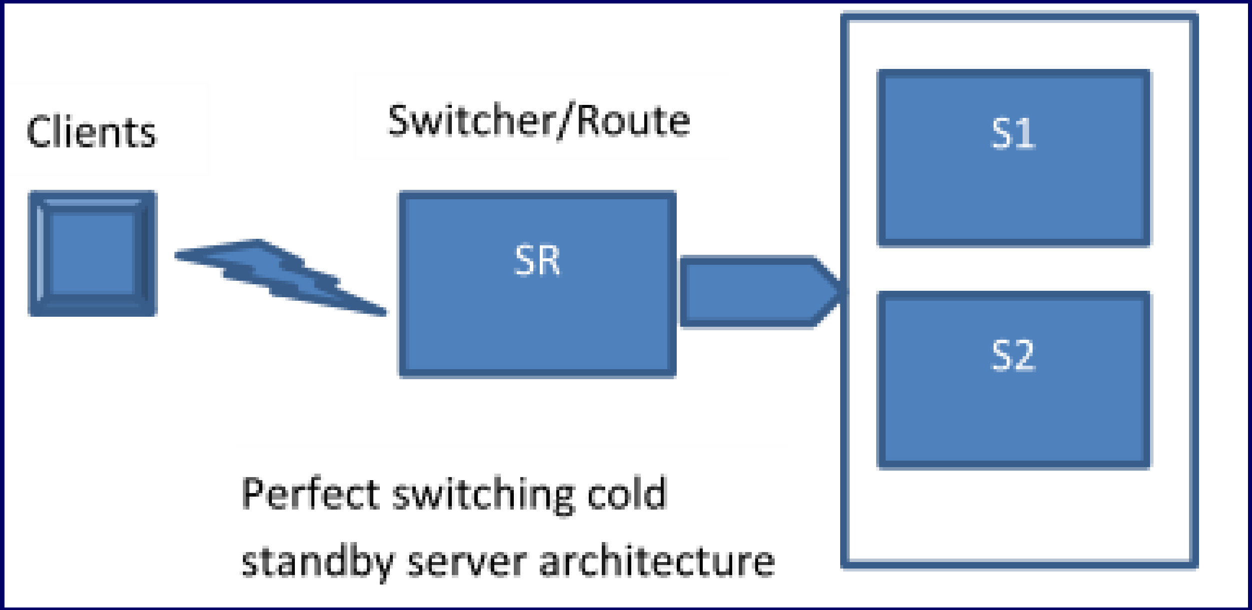


The result obtained through TimeNET:

The Availability = P{#P1≥ 2} = 0.9999552.

SPN

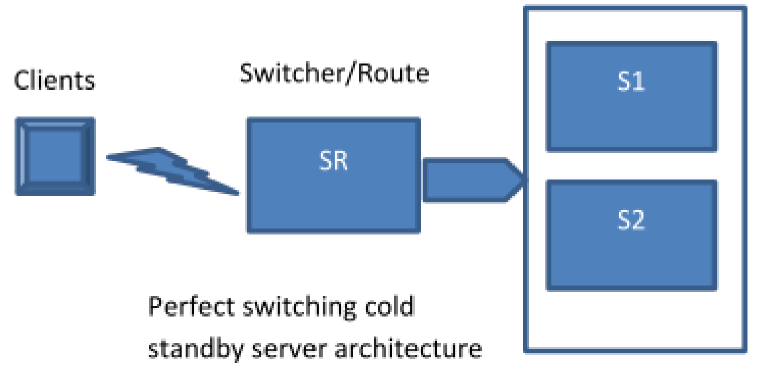
Example



The system is composed by a Switcher/Router and Serve subsystem. The system fails if the Switcher/Router fails OR if the Serve subsystem fails. The Server subsystem is composed by two servers, S1 and S2. S1 is the main server and S2 is the spare server. They are configured in Cold Standby, that is, S2 starts as soon as S1 fails. The start-up time of S2 is zero.

SPN

Example



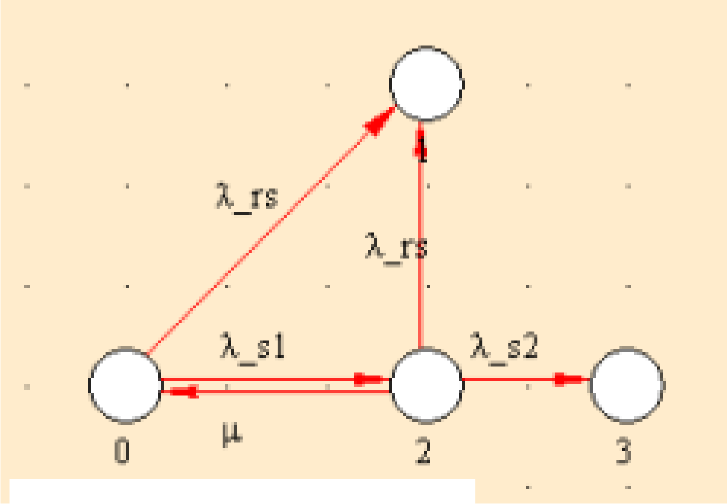
CTMC reliability model

λ_{rs} is failure rate of the Switcher/Router.

λ_{s1} is failure rate of the Server 1.

λ_{s2} is failure rate of the Server 2.

μ is the repair rate assigned to Server 1 repair activity.



Variable	Value
lambda_rs	1/2000
lambda_s1	1/15000
mu	1/24
lambda_s2	1/15000

The unity of these rates is h^{-1}.

System Unreliability:

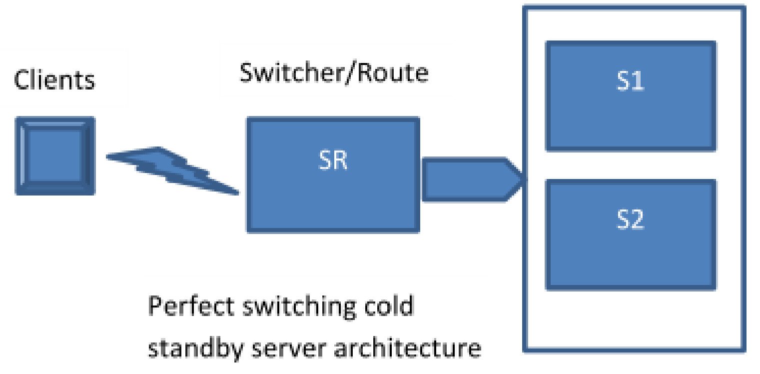
UR(4000h)= 0.181615244

System Reliability:

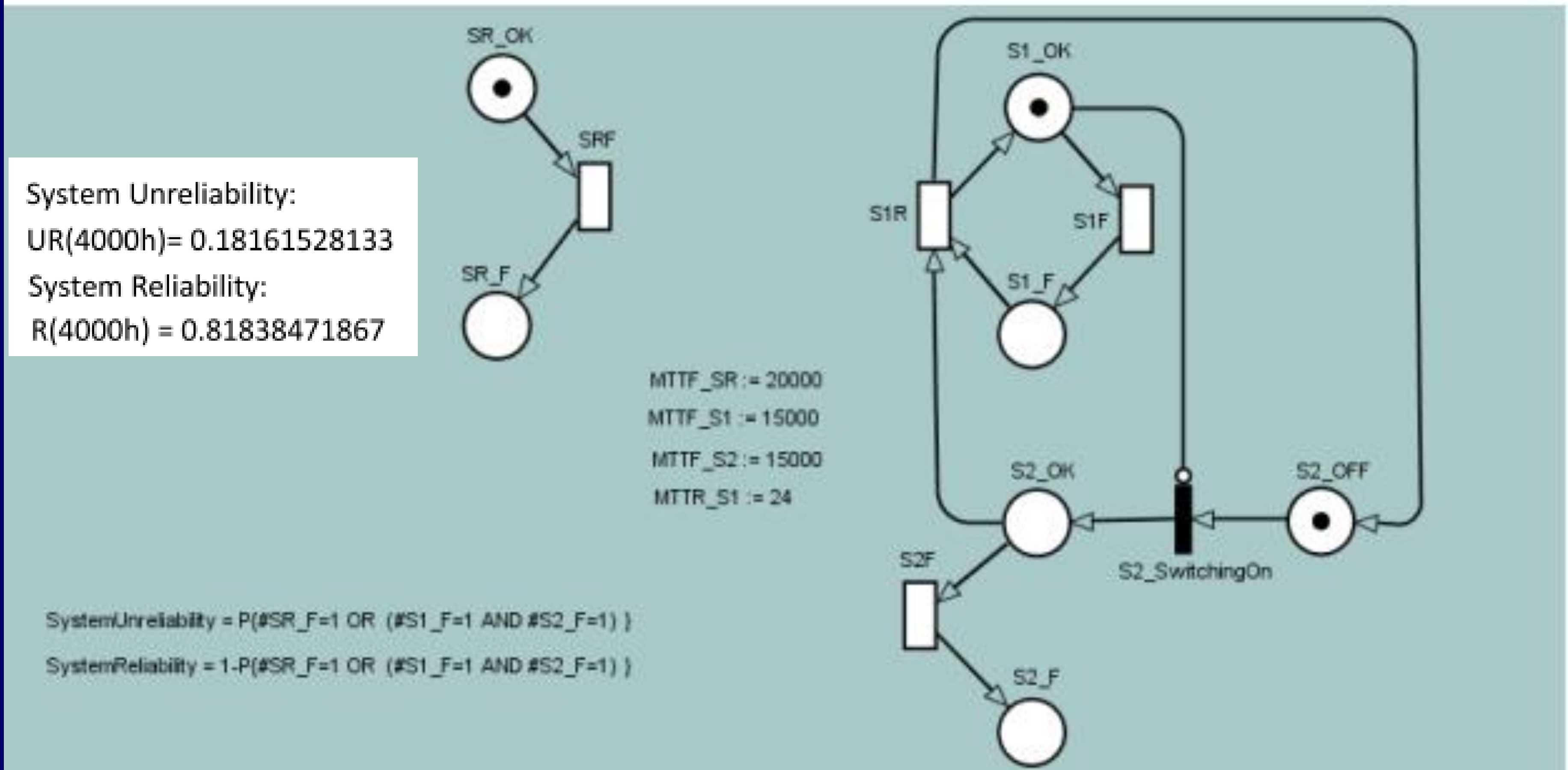
R(4000h) = 0.818384756

SPN

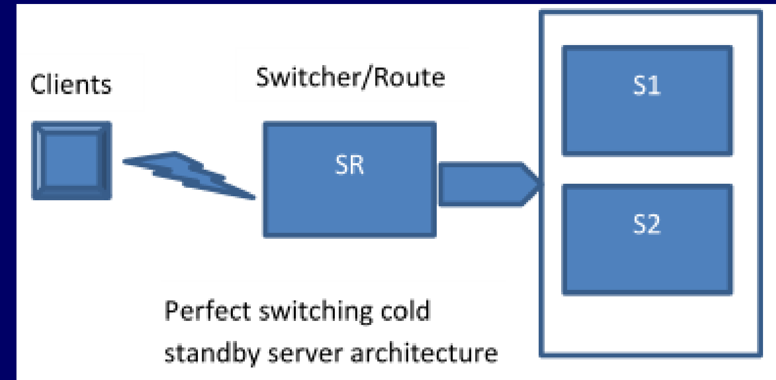
Example



SPN reliability model



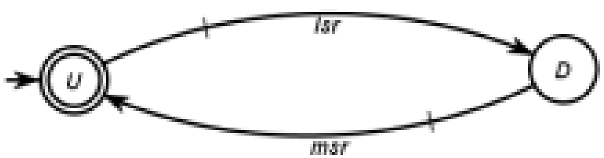
SPN



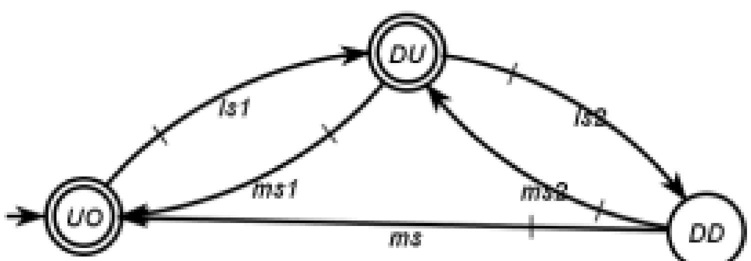
Example **CTMC availability model**

The component's state machines are:

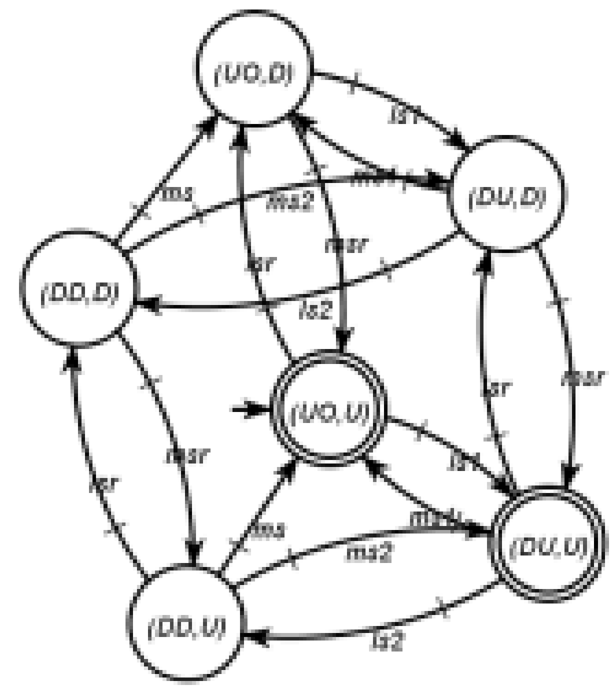
1) SR state machine (SR)



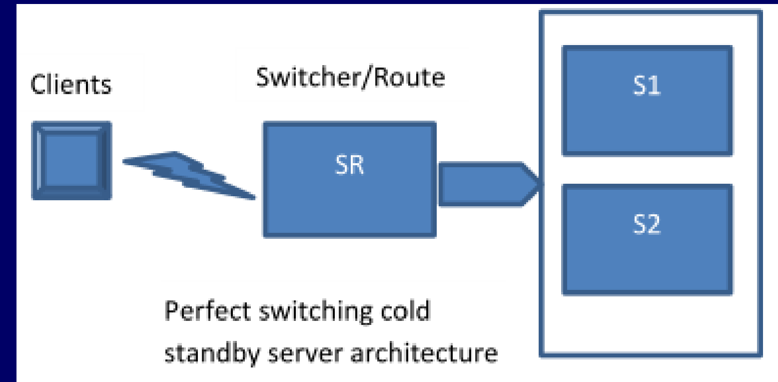
2) Server's state machine (CS)



The respective CSM = Sync(SR,CS) is

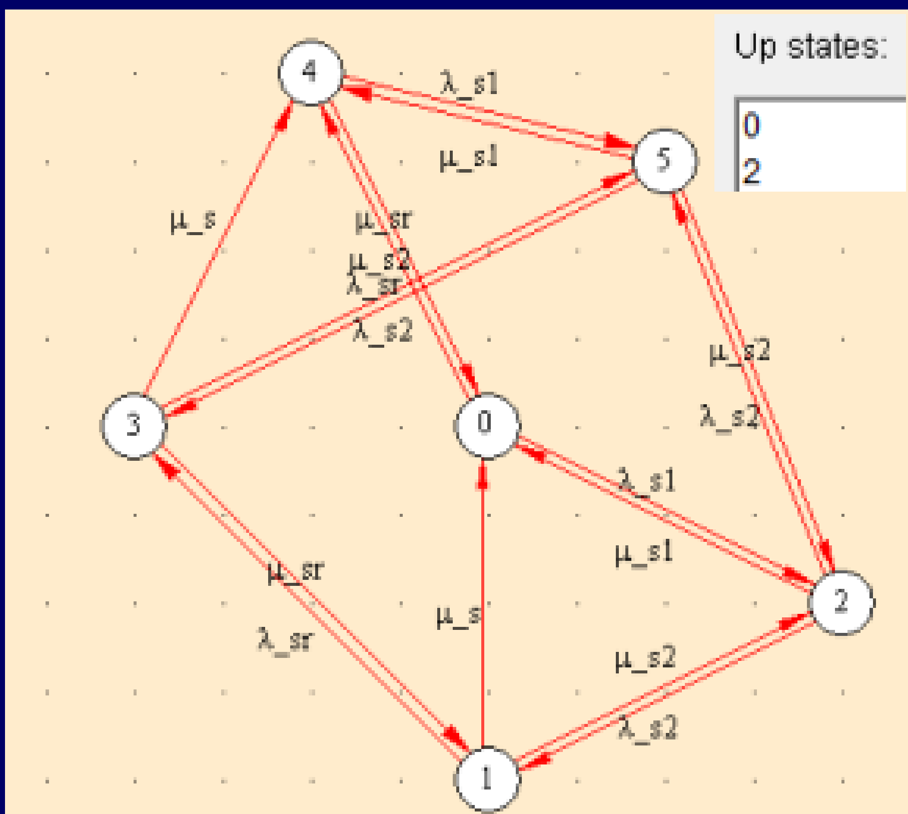


SPN



Example **CTMC availability model**

The respective CTMC availability model is

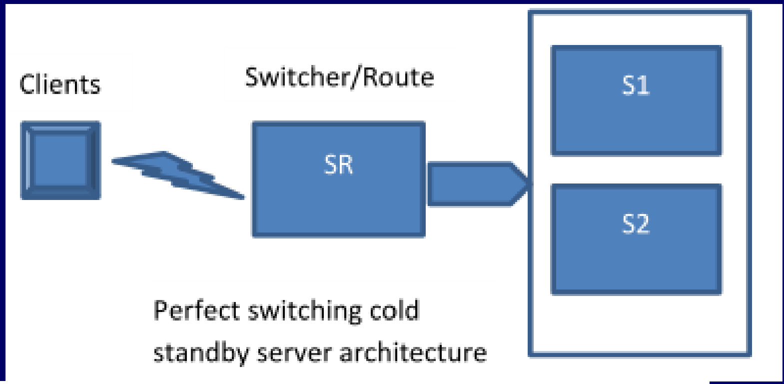


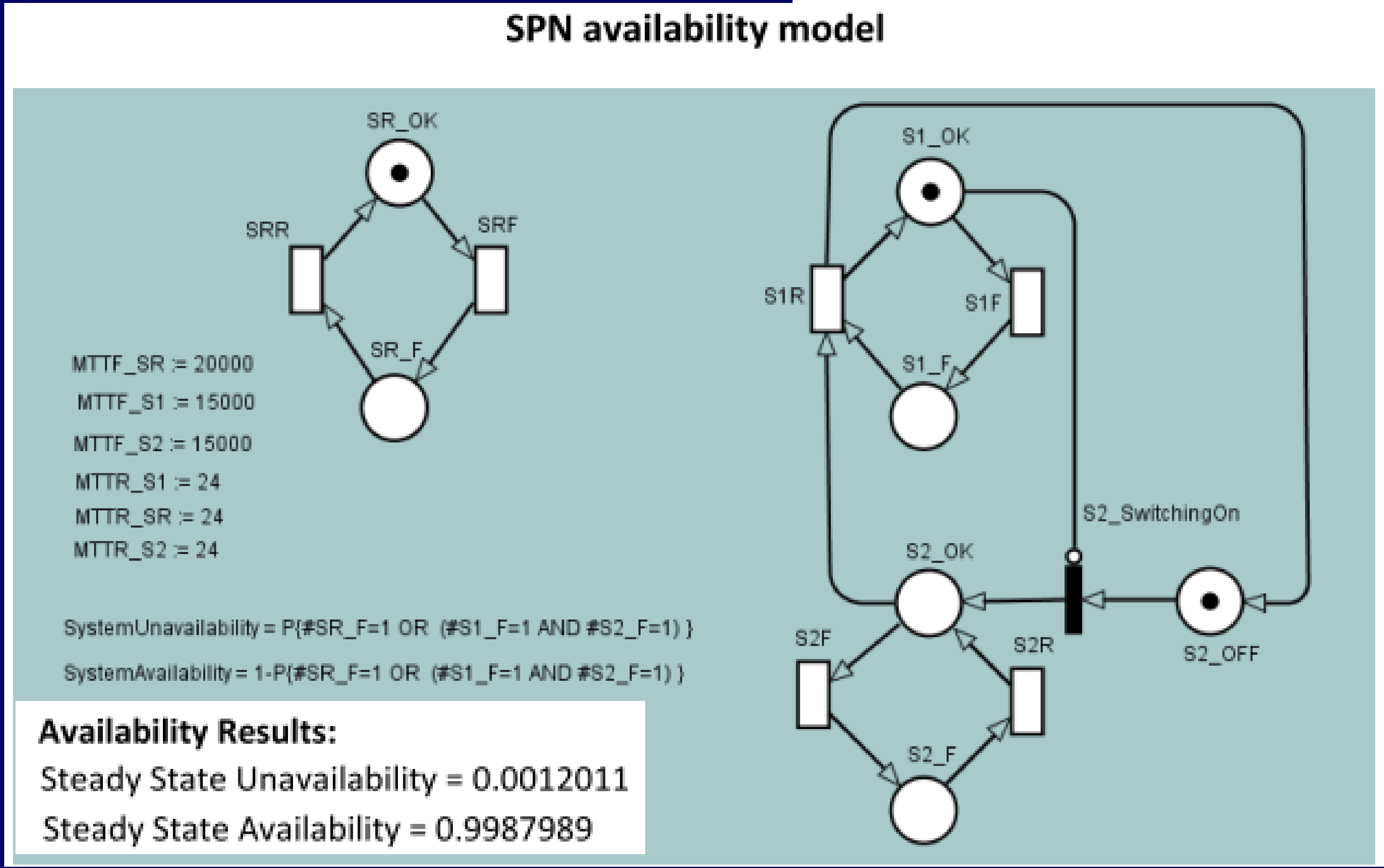
System availability:
A=0.998799526

System unavailability:
UA=0.00120047377

SPN

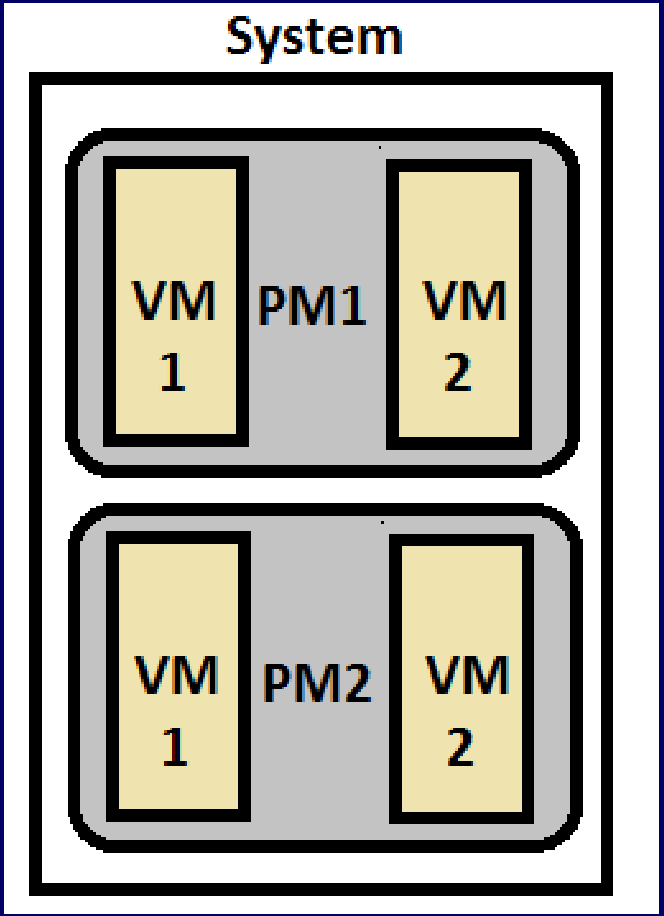
Example


Clients
Switcher/Route
SR
S1
S2
Perfect switching cold
standby server architecture


SPN availability model
SR_OK
SRR
SRF
SR_F
MTTF_SR := 20000
MTTF_S1 := 15000
MTTF_S2 := 15000
MTTR_S1 := 24
MTTR_SR := 24
MTTR_S2 := 24
S1_OK
S1R
S1F
S1_F
S2_SwitchingOn
S2_OK
S2F
S2R
S2_OFF
S2_F
SystemUnavailability = P{#SR_F=1 OR (#S1_F=1 AND #S2_F=1) }
SystemAvailability = 1-P{#SR_F=1 OR (#S1_F=1 AND #S2_F=1) }
Availability Results:
Steady State Unavailability = 0.0012011
Steady State Availability = 0.9987989

SPN

Capacity Oriented Availability in Cloud Systems
A Simple Example



Consider a system composed by two physical machines, PM1 and PM2, where each physical machine supports two virtual machines (VMs).

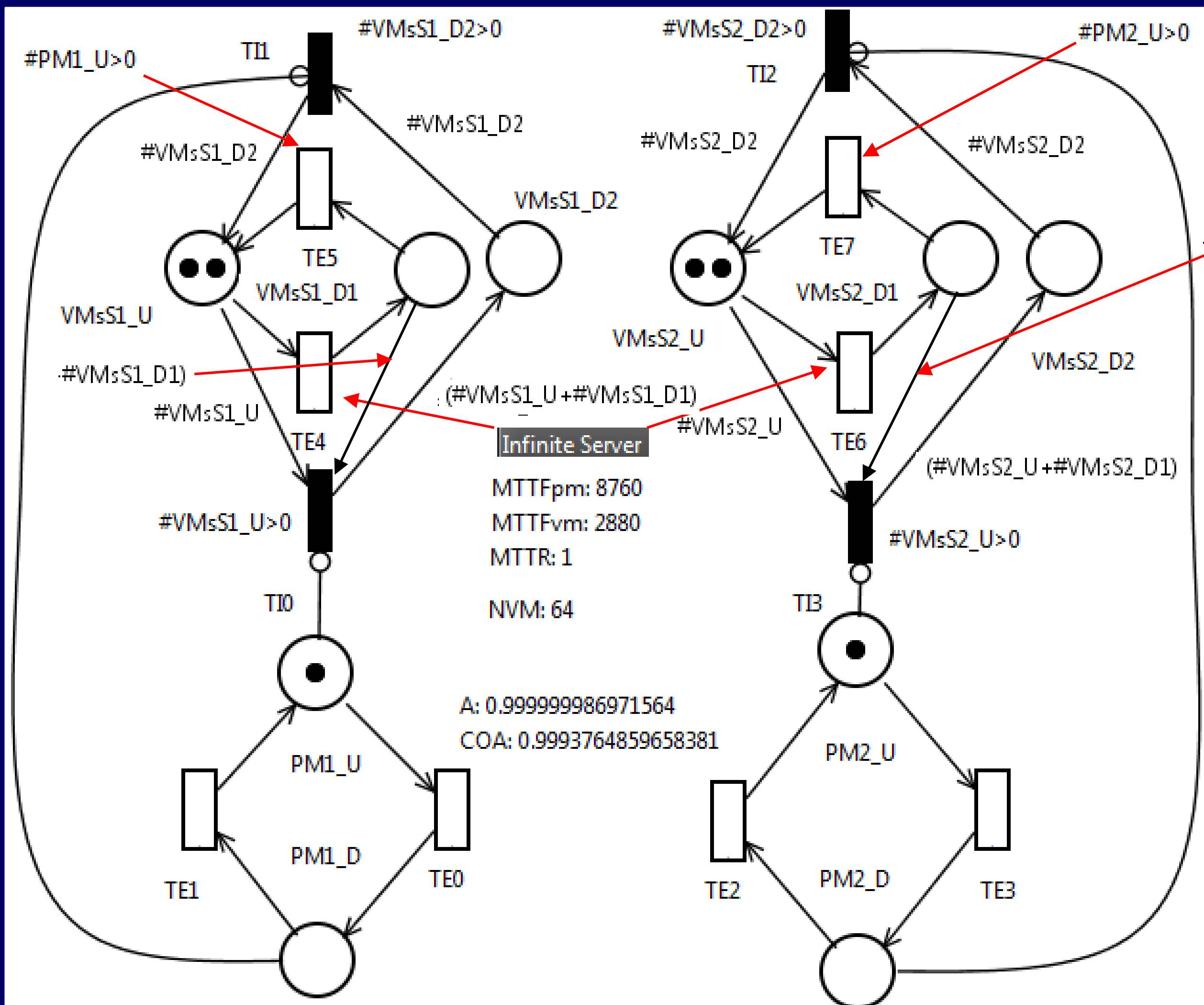
SPN

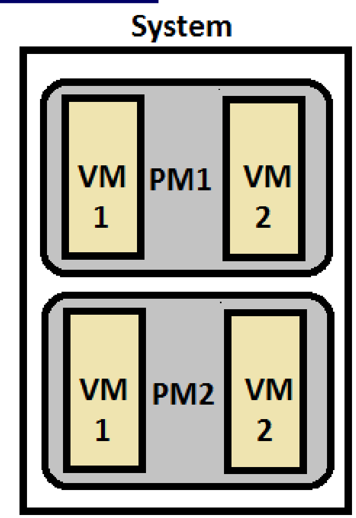
Model 3

NVM=64

#states=4489

~ 5s





A = P{(#VMsS1_U+#VMsS2_U)>0}

COA=
(((P{(#VMsS1_U+#VMsS2_U)=(2*NVM)}*
(2*NVM))
+
(P{(#VMsS1_U+#VMsS2_U)=((2*NVM)-
1)}*((2*NVM)-1))
+
(P{(#VMsS1_U+#VMsS2_U)=((2*NVM)-
2)}*((2*NVM)-2))
+
(P{(#VMsS1_U+#VMsS2_U)=((2*NVM)-
3)}))
/ (2*NVM))

SPN

Comparison

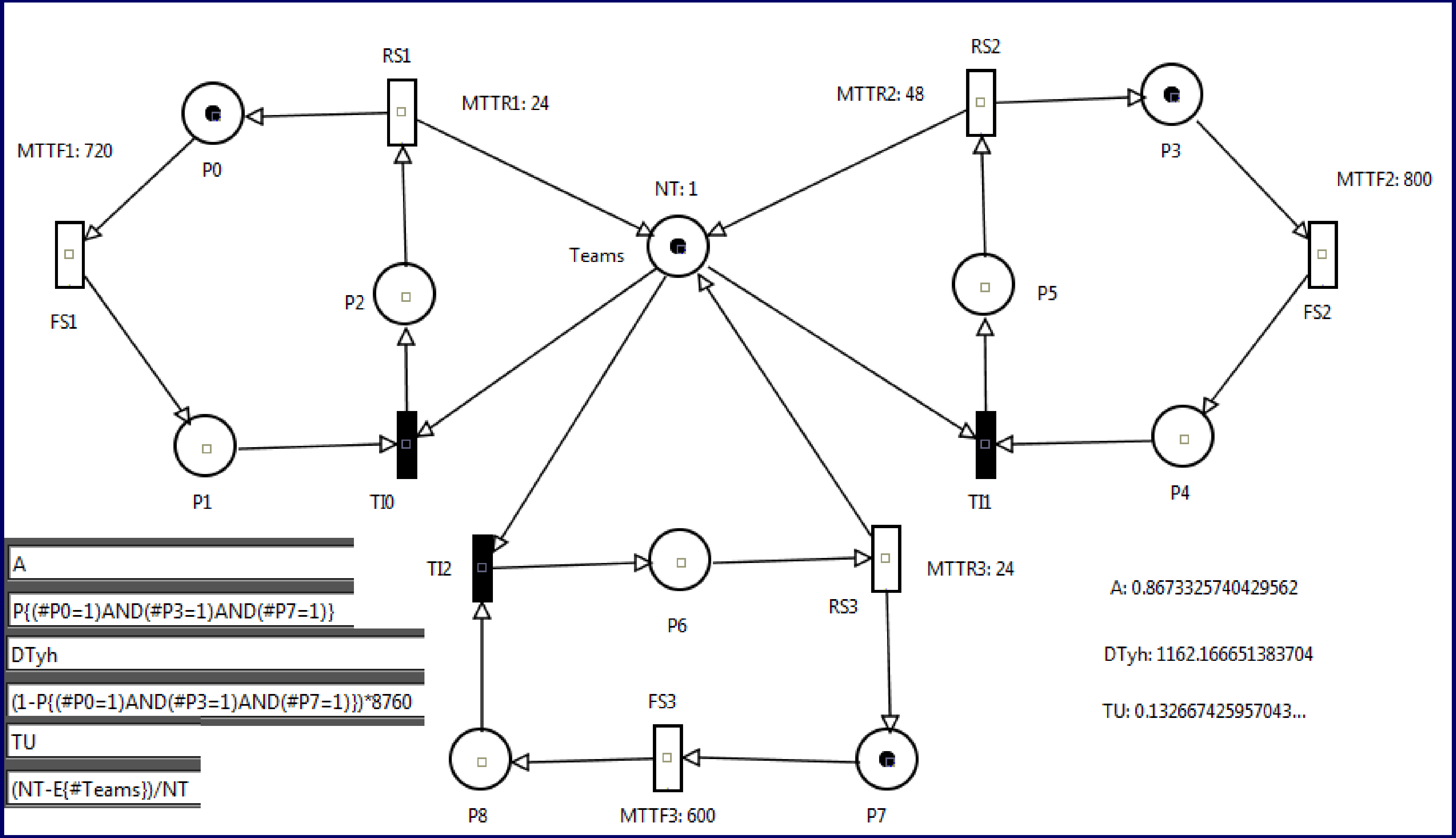
Model	A	COA
Model 1	0.9999999868771198	0.9995384300392318
Model 2	0.9999999738408221	0.999538513813583
Model 3	0.999999986909146	0.9995387092788293
Model 4	0.999999987	0.9995384342

SPN

MERCURY
C:\Users\Paulo\Dropbox\Models\Mercury\
Mercury 4.4.3\Mercury 4.4.3.2\Examples\
SPN_CorrectiveMaintenance.xml

Shared repair

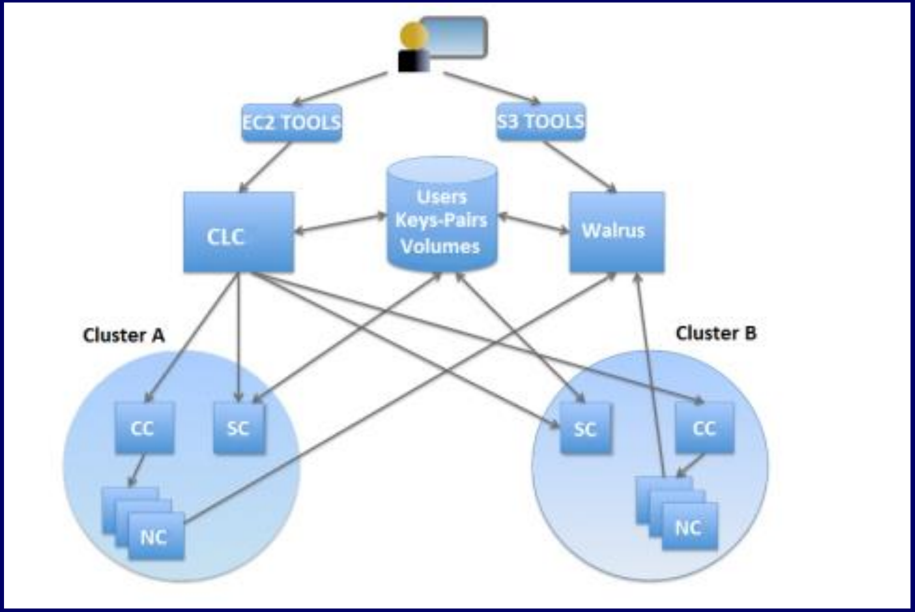
Corrective Maintenance

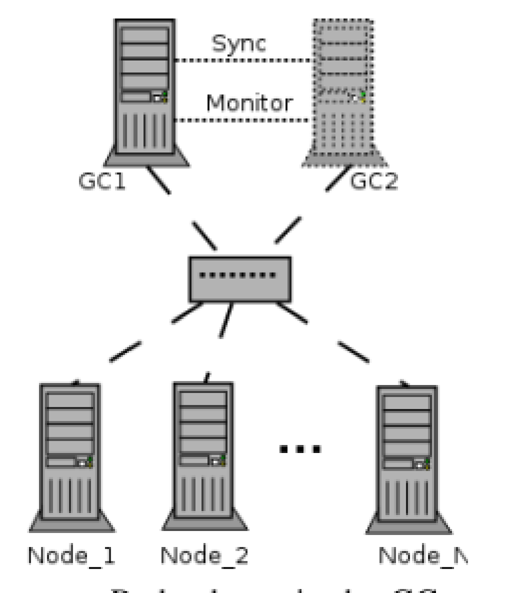


HIERARCHICAL MODELING

Hierarchical Modeling

EUCALYPTUS is composed by five high-level components: Cloud Controller, Cluster Controller, Node Controller, Storage Controller, and Walrus. The Cloud Controller (CLC) is responsible for exposing and managing th underlying virtualized resources (servers, network, and storage).

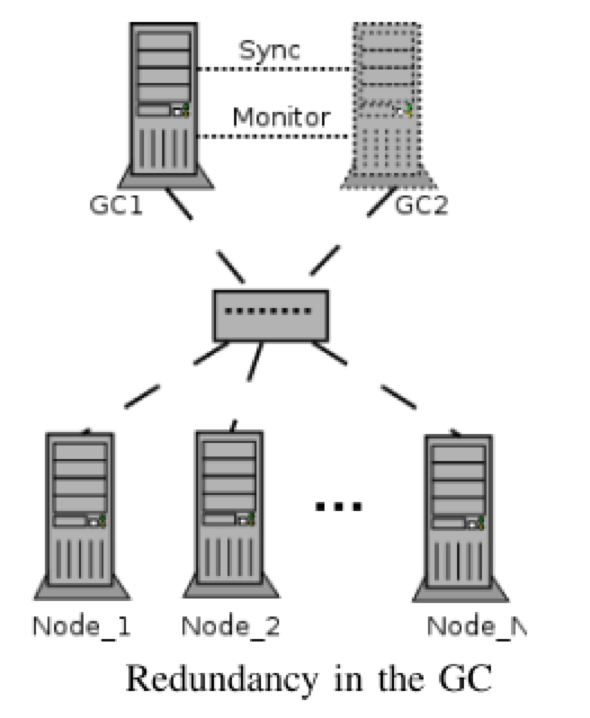


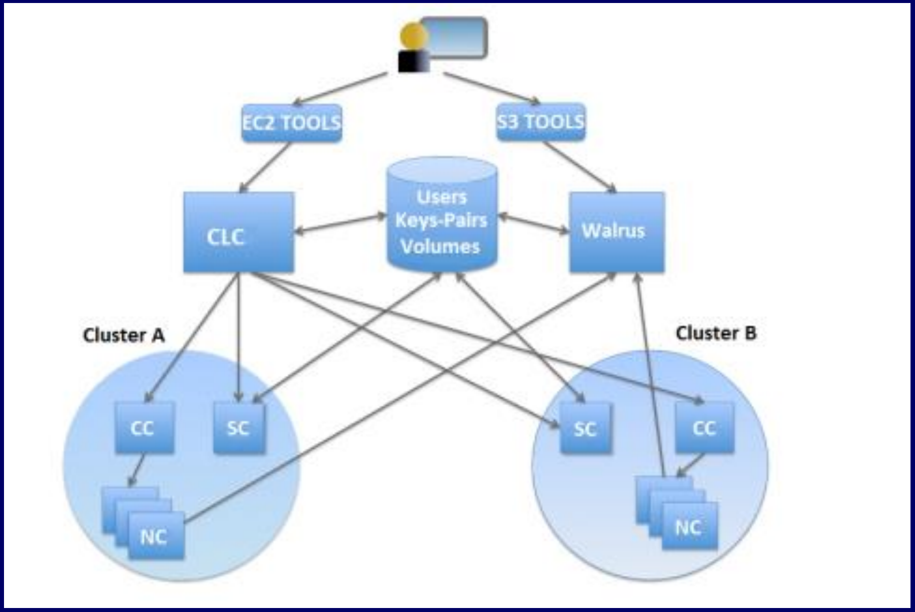


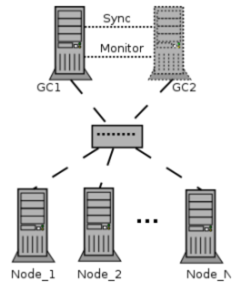
Redundancy in the GC

Hierarchical Modeling

EUCALYPTUS is composed by five high-level components: Cloud Controller, Cluster Controller, Node Controller, Storage Controller, and Walrus. The Cloud Controller (CLC) is responsible for exposing and managing th underlying virtualized resources (servers, network, and storage).







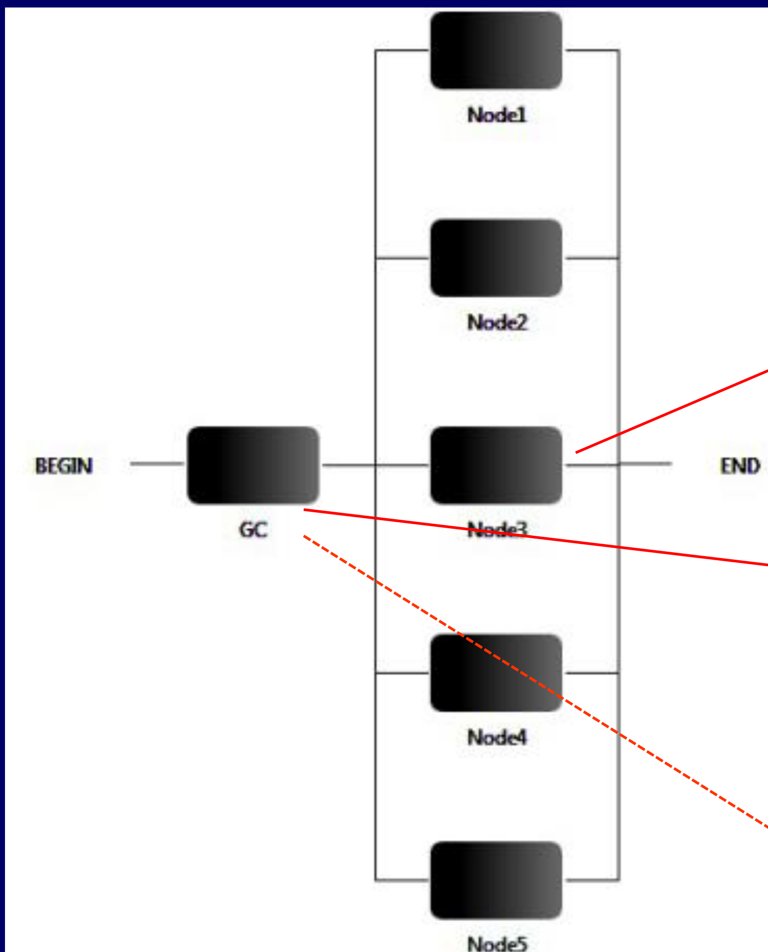
Redundancy in the GC

Hierarchical Modeling

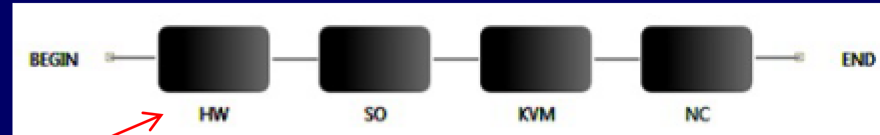
Input Parameters for the nodes

Component	MTTF	MTTR
KVM	2990 h	1 h
NC	788.4 h	1 h

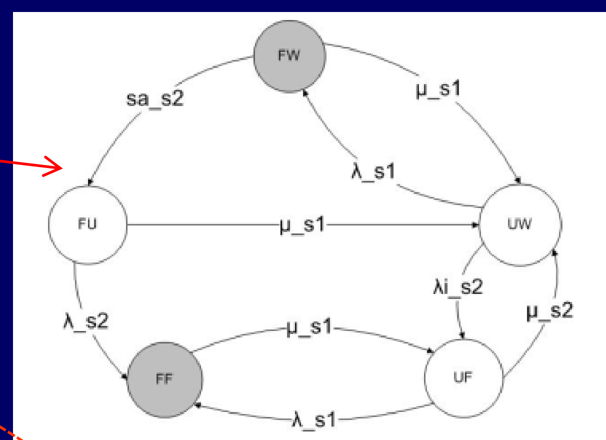
Parameter	Description	Value
$\lambda\_s1 = \lambda\_s2 = 1/\lambda$	Mean time for host failure	$1/180.721$
$\lambda_i\_s2 = 1/\lambda_i$	Mean time for inactive host failure	$1/216.865$
$\mu\_s1 = \mu\_s2 = 1/\mu$	Mean time for host repair	$1/0.9667$
$sa\_s2 = 1/sa$	Mean time to system activate	$1/0.005$



cloud system HLM

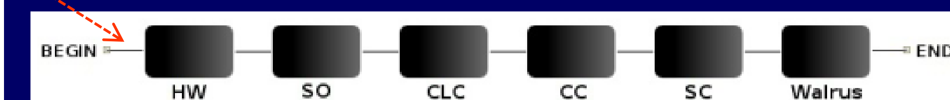


Node subsystem RBD model



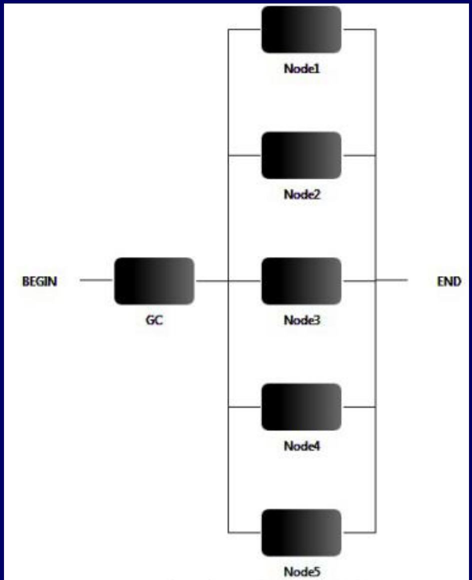
Component	MTTF	MTTR
HW	8760 h	100 min
SO	2893 h	15 min
CLC	788.4 h	1 h
CC	788.4 h	1 h
SC	788.4 h	1 h
Walrus	788.4 h	1 h

Redundant general controller subsystem

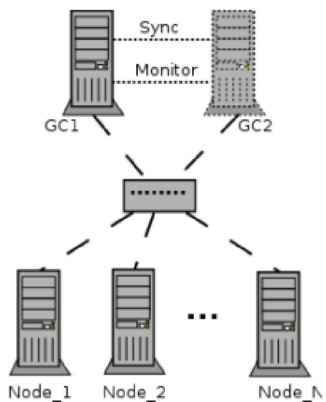


RBD model of the non-redundant General Controller subsystem

Hierarchical Modeling



cloud system **HLM**

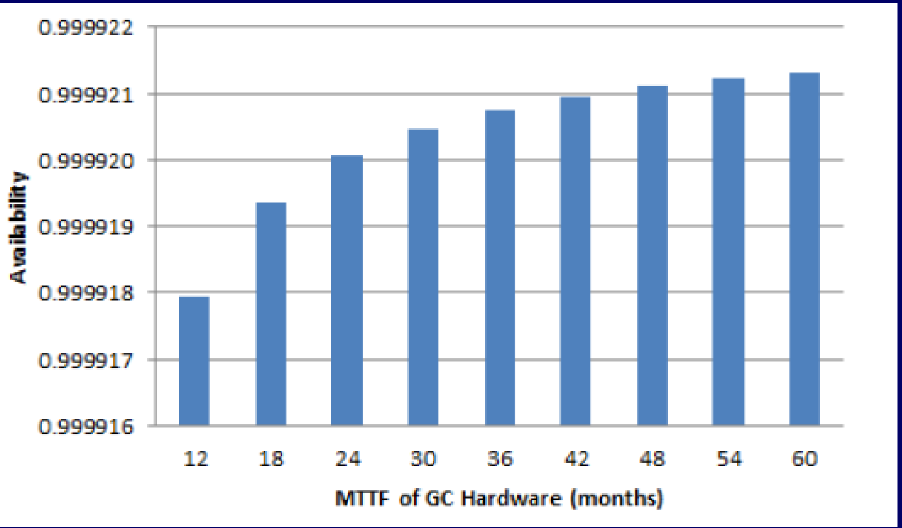


Redundancy in the GC

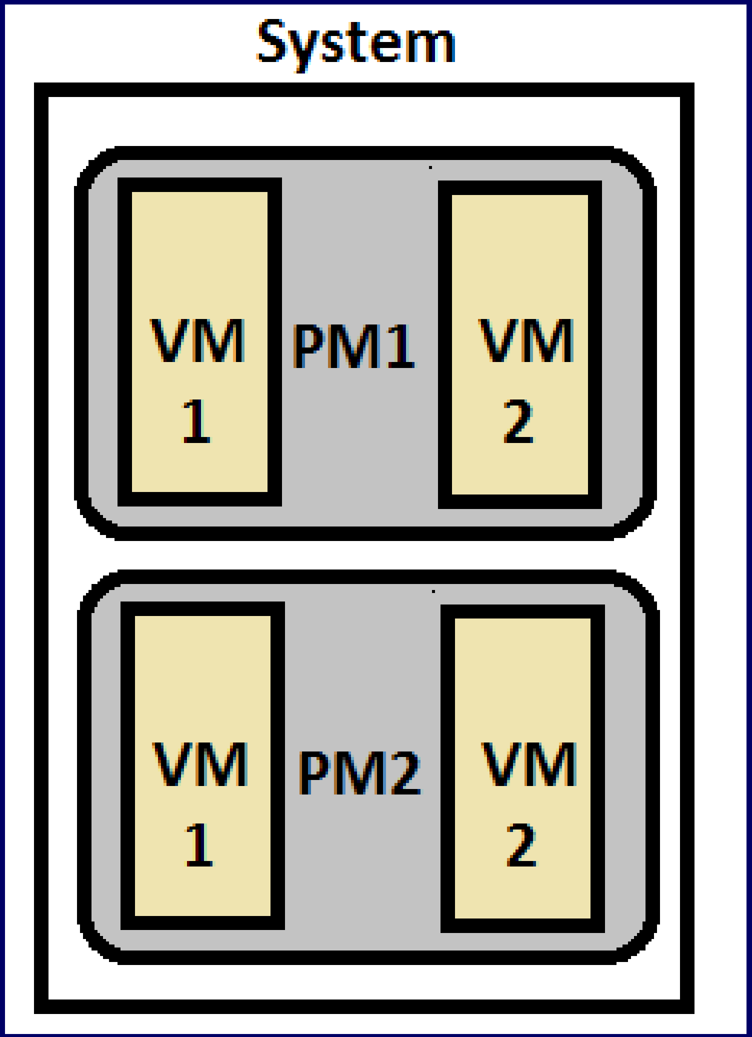
$$A_{GC} = \frac{\mu(\lambda_i(\mu + sa) + \mu^2 + sa(\lambda + \mu))}{\lambda_i(\lambda + \mu)(\mu + sa) + \mu^2(\lambda + \mu) + sa(\lambda^2 + \lambda\mu + \mu^2)}$$

$$A_{cloud} = A_{GC} * (1 - \prod_{i=1}^{n}(1 - A_{Node\_i}))$$

Measure	GC without redundancy	GC with redundancy
Steady-state availability	0.99467823178	0.99991793
Number of 9's	2.273944	4.08581
Annual downtime	46.66 h	0.72 h



Hierarchical Modeling



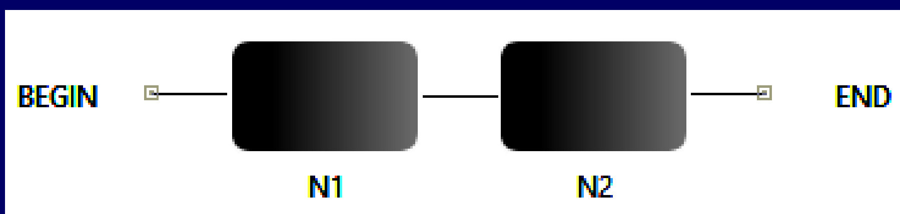
Estimating Capacity Oriented Availability (COA) in Cloud Systems

Consider a system composed by two physical machines, PM1 and PM2, where each physical machine sup-ports two virtual machines (VMs).

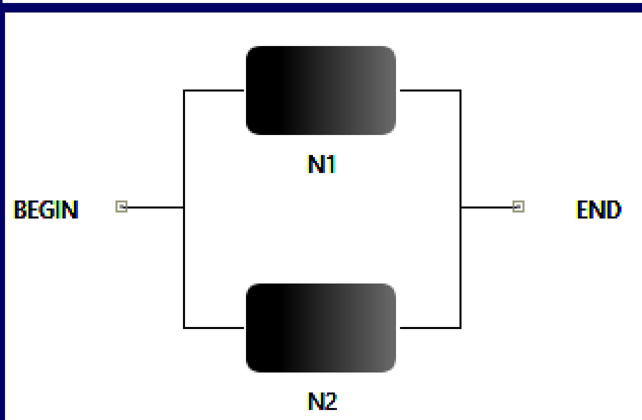
A Simple Example

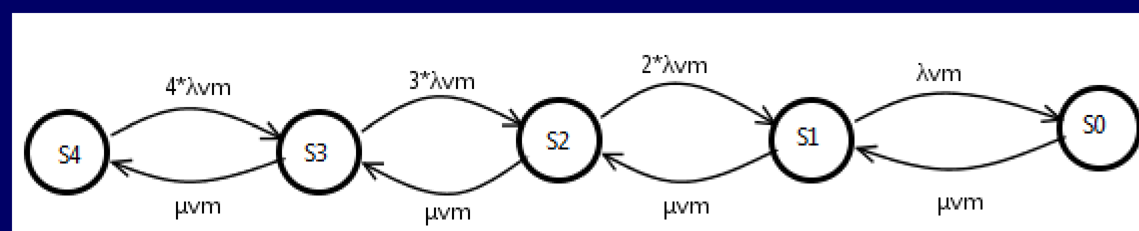
Hierarchical Modeling

- The respective model is represented by RBD and CTMC availability models.



Model 4





Hierarchical Modeling

Model 4

- Availability model

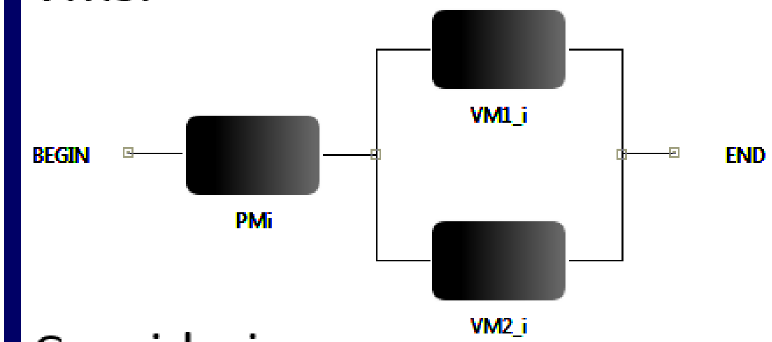
Considering the components of a node are independent and identical, so all the nodes (PM+VM) have the same failure and repair distribution.

Hence, the availability of the system is

$$A_{1oo4} = \sum_{i}^{4} \binom{4}{i} \times A_{PM+VM}^{i} \times (1 - A_{PM+VM})^{n-i}$$

$$A_{1oo4} = \sum_{i=1}^{4} \binom{4}{i} \times A_{PM+VM}^{i} \times (1 - A_{PM+VM})^{4-i}$$

Each node is composed of 1 PM and 2 VMs:



Considering

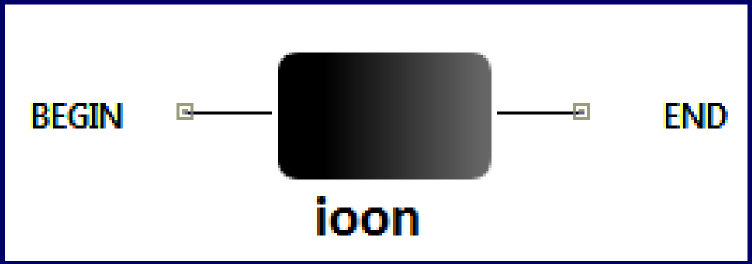
$$MTTR_{PM} = MTTR_{VM} = MTTR$$

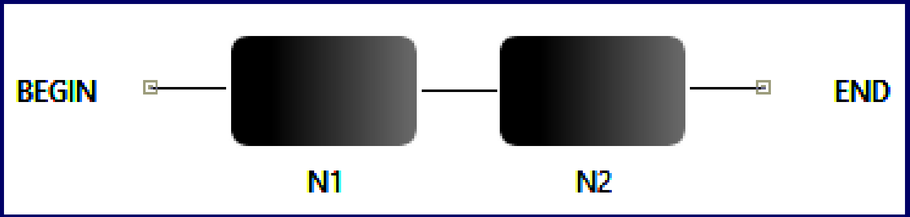
$$A_{PM+VM}^{i} = \frac{MTTF_{PM}}{MTTF_{PM} + MTTR} \times \left(1 - \left(\frac{MTTF_{VM}}{MTTF_{VM} + MTTR}\right)^{2}\right)$$

Hierarchical Modeling

Model 4

- COA model - The respective model is represented by RBDs and CTMC





$$P_{ioon} = \sum_{i}^{n} \binom{n}{i} \times P^i \times (1 - P)^{n-i}$$

$$P(N = 2) = P_{2oo2} = \sum_{i=2}^{2} \binom{2}{i} \times P^i \times (1 - P)^{n-i}$$

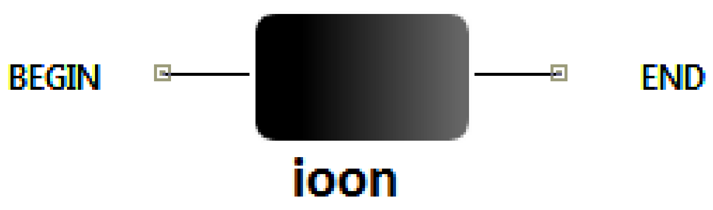
$$P_{2oo2} = 1 \times P^2 \times (1 - P)^0$$

$$P_{2oo2} = P^2$$

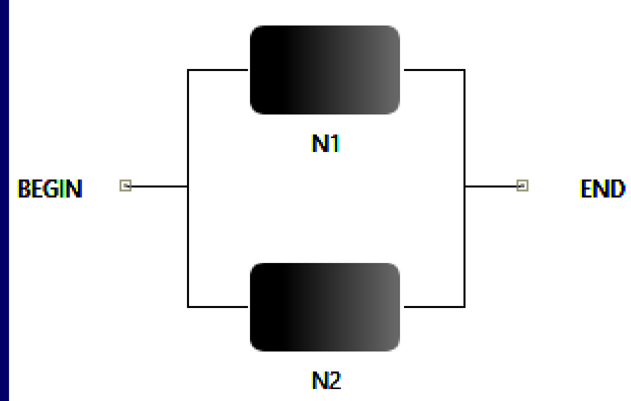
Hierarchical Modeling

- COA model - The respective model is represented by RBDs and CTMC

Model 4



$$P_{ioon} = \sum_{i}^{n} \binom{n}{i} \times P^{i} \times (1-P)^{n-i}$$



$$P(N \geq 1) = P_{1oo2} = \sum_{i=1}^{2} \binom{2}{i} \times P^{i} \times (1-P)^{2-i}$$

$$P_{1oo2} = \binom{2}{1} \times P^{1} \times (1-P)^{1} + \binom{2}{2} \times P^{2} \times (1-P)^{0}$$

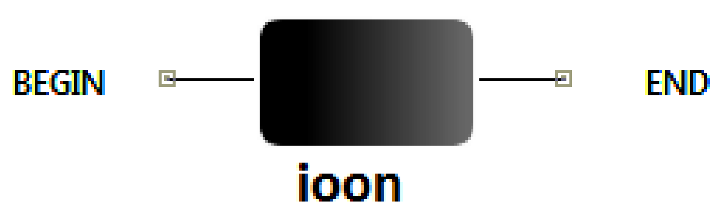
$$P_{1oo2} = 2 \times P \times (1-P) + P^{2}$$

$$P_{1oo2} = 2P - 2P^{2} + P^{2} = 2P - P^{2}$$

Hierarchical Modeling

- COA model - The respective model is represented by RBDs and CTMC

Model 4



$$P_{ioon} = \sum_{i}^{n} \binom{n}{i} \times P^{i} \times (1-P)^{n-i}$$

Hence:

$$P(N=1) = P_1 = P(N \geq 1) - P(N=2)$$

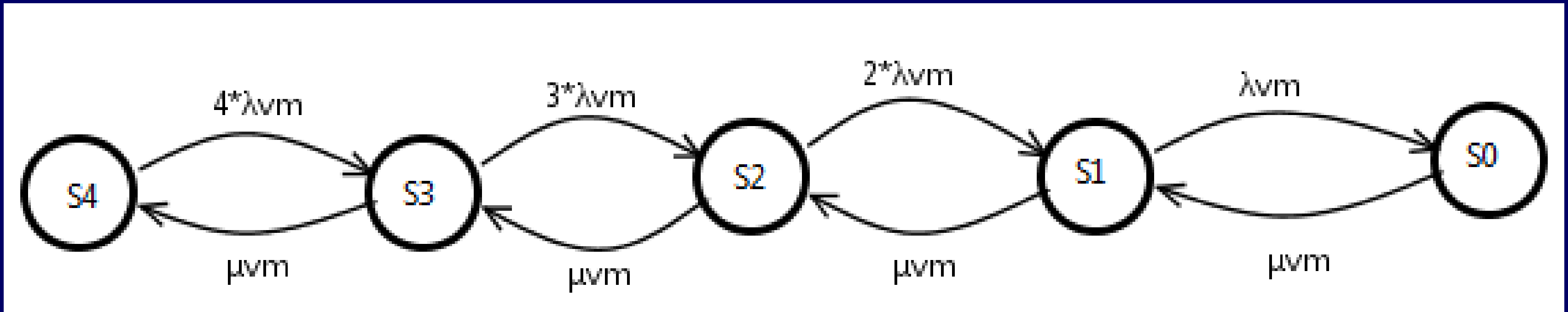
$$P(N=1) = P_1 = 2P - P^2 - P^2$$

$$P(N=1) = P_1 = 2P - 2P^2$$

Hierarchical Modeling

Model 4

- COA model - The respective model is represented by RBDs and CTMC



P4, P3, P2 and P1 represent the probability of being at each state (CTMC model), where P4 is the probability of having four virtual machines running, P3 is the probability of having three virtual machines running, P2 is the probability of having two virtual machines running and P1 is the probability of having only one virtual machines running.

Hierarchical Modeling

Model 4

- COA model - The respective model is represented by RBDs and CTMC

$$COA = \frac{\sum_j^n P(N=j) \times \sum_i^{nmVMjn} iP_i}{m}$$

$$P_i = P_{ioon} - \sum_{j=i+1}^{n} P_j$$

$$nmVMjn$$

$$maximal\ number\ of\ Virtual\ Machines\ for\ j\ PMs$$

Hierarchical Modeling

Model 4

- COA model - The respective model is represented by RBDs and CTMC

- $COA = \dfrac{\left(\left(\frac{\mu_{pm}}{\mu_{pm}+\lambda_{pm}}\right)^2\right)\times([p_4\times 4]+[\ p_3\times 3]+[p_2\times 2]+[p_1])+\left(\frac{2\lambda_{pm}\mu_{pm}}{(\lambda_{pm}+\mu_{pm})^2}\right)\times([p_2\times 2]+[p_1])}{4}$

Where,

P4 = $\dfrac{\mu^4}{24\ \lambda^4 + 24\ \lambda^3\ \mu + 12\ \lambda^2\ \mu^2 + 4\ \lambda\ \mu^3 + \mu^4}$

P2 = $\dfrac{12\ \lambda^2\ \mu^2}{24\ \lambda^4 + 24\ \lambda^3\ \mu + 12\ \lambda^2\ \mu^2 + 4\ \lambda\ \mu^3 + \mu^4}$,

P3 = $\dfrac{4\ \lambda\ \mu^3}{24\ \lambda^4 + 24\ \lambda^3\ \mu + 12\ \lambda^2\ \mu^2 + 4\ \lambda\ \mu^3 + \mu^4}$,

P1 = $\dfrac{24\ \lambda^3\ \mu}{24\ \lambda^4 + 24\ \lambda^3\ \mu + 12\ \lambda^2\ \mu^2 + 4\ \lambda\ \mu^3 + \mu^4}$

Hierarchical Modeling

Comparison

Model	A	COA
Model 1	0.9999999868771198	0.9995384300392318
Model 2	0.9999999738408221	0.999538513813583
Model 3	0.999999986909146	0.9995387092788293
Model 4	0.999999987	0.9995384342

Model 4

Number of physical machine	Number of virtual machine	COA
50	100	0.9998823844
100	200	0.9998841211
500	1000	0.9998855104