Dependability Evaluation through Markovian model

Markovian model

The combinatorial methods are unable to:

- take care easily of the coverage factor

- model the maintenance

The Markov model is an alternative to the combinatorial methods.

Two main concepts:

- state

- state transition

State and state transitions

State: *the state of a system represents all that must be known to describe the system at any given instant of time*

For the reliability/availability models each state represents a distinct combination of faulty and fault-free components

State transitions *govern the changes if state that occur within a system*

For the reliability/availability models each transition takes place when one or more components change state due to an event of a fault or a repair action

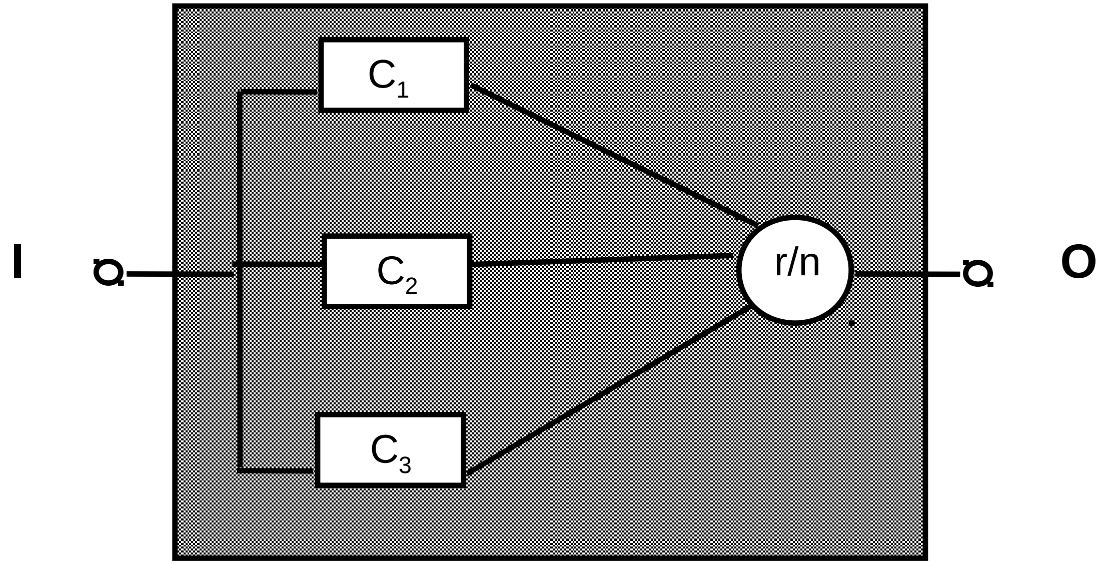
State and state transitions (cnt.)

- *State transitions are characterized by probabilities, such as probability of fault, fault coverage and the probability of repair*

- *The probability of being in any given state, s, at some time,t+Δt depends both:*
  - *the probability that the system was in a state from which it could transit to state state s given that the transition occurs during Δt*
  - *the probability that the system was in state s at instant t and there was no event in the interval time Δt*
- *The initial state should be any state, normally it is that representing all fault-free components*

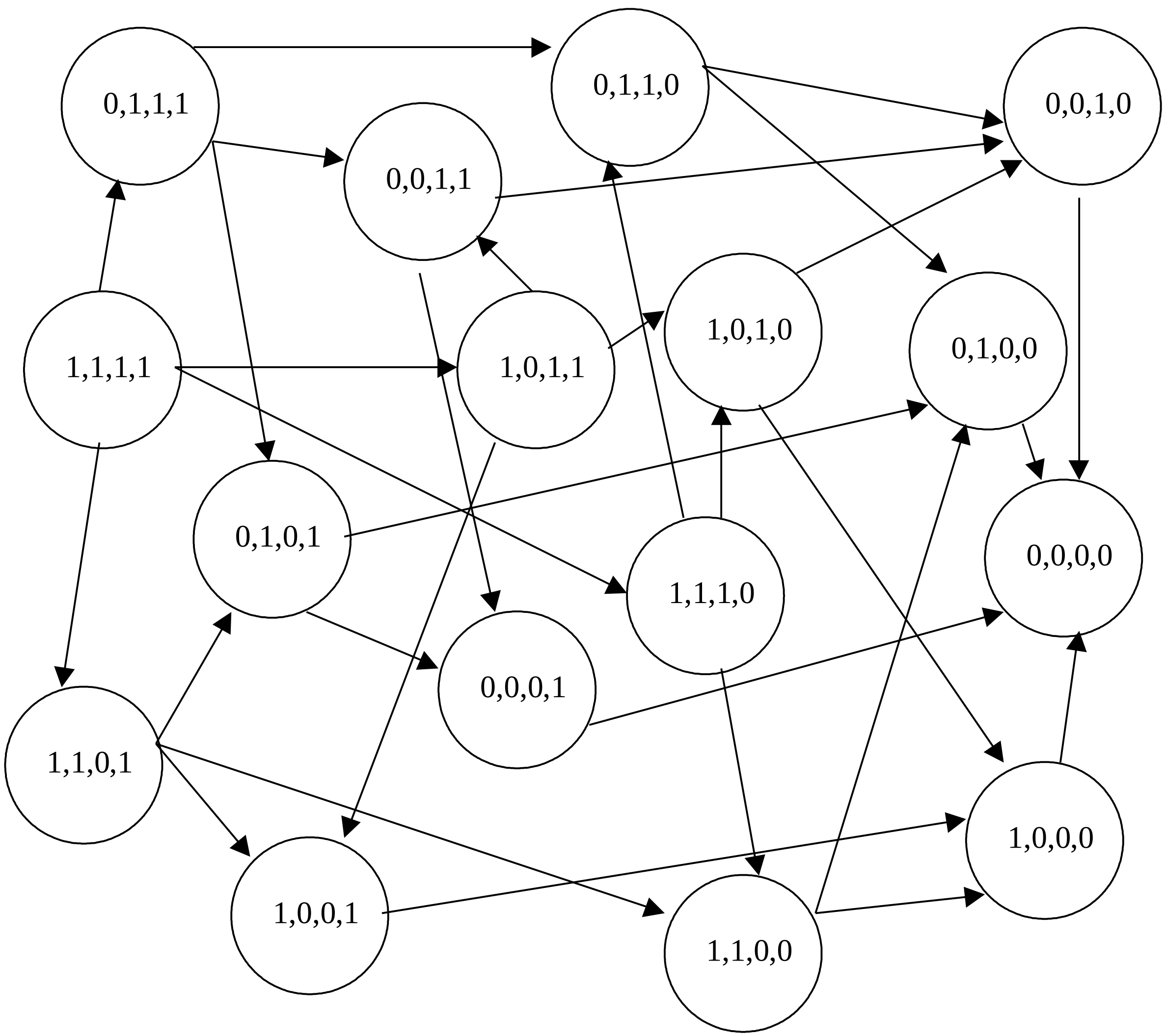
IMPORTANT: IN A MARKOV CHAIN THE PROBABILITY TRANSITION DEPENDS ONLY ON THE ACTUAL STATE (Memoryless Property)

TMR reliability evaluation



- *There are 4 components (1 voter + computation module), therefore each state is represented by 4 bit:*
  - *if the component is fault-free then the bit value is 1*
  - *otherwise the bit value is 0.*
- *For example (1,1,1,1) represents the faut-free state*
- *For example (0,0,0,0) represents all components faulty*

TMR reliability evaluation: states diagram



Markov chain reliability evaluation methodology

- *State transition probability evaluation:*
  - *If the fault occurence of a component is exponentially distributed ($e^{-\lambda t}$) with fault rate equal to (λ), then the probability that the fault-free component at istant t in the interval Δt become faulty is equal to:*
    - *$1 – e^{-\lambda \Delta t}$*

Probability property

Prob{*there is a fault between* ***t*** *e* ***t+Δt***} =

= ***Prob***{*there is a fault before* ***t+Δt/****the component was fault-free at* ***t***} =

$$= \frac{\textbf{Prob}\{\text{there is a faul before } \mathbf{t+\Delta t} \text{ and the component was fault-free at } \mathbf{t}\}}{\textbf{Prob}\{\text{the component was fault-free at } \mathbf{t}\}}$$

$$= \frac{\textbf{Prob}\{\text{there is a fault before } \mathbf{t+\Delta t}\} - \textbf{Prob}\{\text{there is a fault before } \mathbf{t}\}}{\textbf{Prob}\{\text{the component was fault-free at } \mathbf{t}\}} =$$

$$= \frac{(1 - e^{-\lambda(t+\Delta t)}) - (1 - e^{-\lambda t})}{e^{-\lambda t}} = \frac{1 - e^{-\lambda(t+\Delta t)} - 1 + e^{-\lambda t}}{e^{-\lambda t}}$$

Probability property

$$= \frac{e^{-\lambda t} - e^{-\lambda(t+\Delta t)}}{e^{-\lambda t}} =$$

$$= \frac{e^{-\lambda t}}{e^{-\lambda t}} - \frac{e^{-\lambda(t+\Delta t)}}{e^{-\lambda t}} = 1 - e^{-\lambda\Delta t}$$

If we expand the exponential part we have the following series:

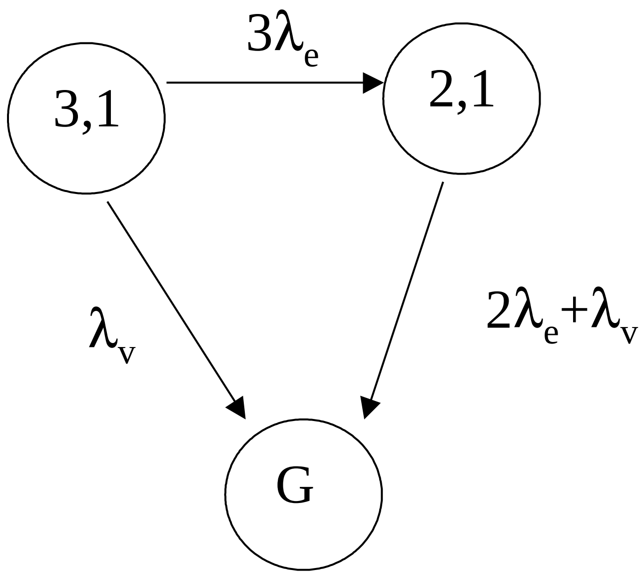
$$1 - e^{-\lambda\Delta t} = 1 - \quad 1 + (-\lambda\Delta t) + \frac{(-\lambda\Delta t)^2}{2!} + \ldots$$

$$= \lambda\Delta t - \frac{(-\lambda\Delta t)^2}{2!} - \ldots$$

For value of $\lambda\Delta t \ll 1$, we have the following good approximation:

$$1 - e^{-\lambda\Delta t} \approx \lambda\Delta t$$

TMR reliability evaluation: reduced states diagram



State (3,1) $\rightarrow$ (1,1,1,1)

State (2,1) $\rightarrow$ (0,1,1,1) + (1,0,1,1) + (1,1,0,1)

State (G) $\rightarrow$ all the other states

Transition probability (in the interval between t and t+Δt):

- *from state (3,1) to state (2,1) -> $3\lambda_e \Delta t$;*
- *from state (3,1) to state (G) -> $\lambda_v \Delta t$;*
- *from state(2,1) to state (G) -> $2\lambda_e \Delta t+\lambda_v \Delta t$.*

TMR reliability evaluation

Given the Markov process properties, i.e.

the probability of being in any given state, s, at some time, t+Δt depends both:

- *the probability that the system was in a state from which it could transit to state state s given that the transition occurs during Δt*
- *the probability that the system was in state s at instant t and there was no event in the interval time Δt*

we have that:

$$P_{(3,1)}(t+\Delta t) = (1-3\lambda_e \Delta t - \lambda_v \Delta t)\, P_{(3,1)}(t)$$

$$P_{(2,1)}(t+\Delta t) = 3\lambda_e \Delta t\, P_{(3,1)}(t) + (1-2\lambda_e \Delta t - \lambda_v \Delta t)\, P_{(2,1)}(t)$$

$$P_{(G)}(t+\Delta t) = \lambda_v \Delta t\, P_{(3,1)}(t) + (2\lambda_e \Delta t + \lambda_v \Delta t)\, P_{(2,1)}(t) + P_{(G)}(t)$$

TMR reliability evaluation

With algebric operations:

$$\frac{P_{(3,1)}(t+\Delta t) - P_{(3,1)}(t)}{\Delta t} = -(3\lambda_e + \lambda_v)\, P_{(3,1)}(t) \quad \overset{\Delta t \to 0}{=} \quad \frac{d\, P_{(3,1)}(t)}{dt}$$

$$\frac{P_{(2,1)}(t+\Delta t) - P_{(2,1)}(t)}{\Delta t} = 3\lambda_e P_{(3,1)}(t) - (2\lambda_e + \lambda_v)\, P_{(2,1)}(t) \quad \overset{\Delta t \to 0}{=} \quad \frac{d\, P_{(2,1)}(t)}{dt}$$

$$\frac{P_{(G)}(t+\Delta t) - P_{(G)}(t)}{\Delta t} = \lambda_v\, P_{(3,1)}(t) + (2\lambda_e + \lambda_v)\, P_{(2,1)}(t) \quad \overset{\Delta t \to 0}{=} \quad \frac{d\, P_{(G)}(t)}{dt}$$

TMR reliability evaluation

i.e:

$$P'_{3,1}(t) = -(3\lambda_e + \lambda_v)P_{3,1}(t)$$
$$P'_{2,1}(t) = 3\lambda_e P_{3,1}(t) - (2\lambda_e + \lambda_v)P_{2,1}(t)$$
$$P'_G(t) = \lambda_v P_{3,1}(t) + (2\lambda_e + \lambda_v)P_{2,1}(t)$$

That in matrix notation can be expressed as:

$$\frac{\boldsymbol{\pi}(t)}{dt} = \boldsymbol{\pi}(t)\, Q(t)$$

$$(P'_{3,1} \quad P'_{2,1} \quad P'_G) = (P_{3,1} \quad P_{2,1} \quad P_G) * Q$$

–

TMR reliability evaluation

the reliability is the probability of being in any fault-free state, i.e, in this case of being in state (3,1) or (2,1).

$$R(t) = P_{3,1}(t) + P_{2,1}(t) = 1 - P_G(t)$$

with the initial condition $P_{3,1}(0) = 1$

TMR reliability evaluation

where:

$$Q = \begin{bmatrix} -(3\lambda_e+\lambda_v) & 3\lambda_e & \lambda_v \\ 0 & -(2\lambda_e+\lambda_v) & (2\lambda_e+\lambda_v) \\ 0 & 0 & 0 \end{bmatrix}$$

$$\boldsymbol{P = Q + I} \quad \rightarrow \quad \boldsymbol{Q = P - I}$$

$$P = \begin{bmatrix} 1-(3\lambda_e+\lambda_v) & 3\lambda_e & \lambda_v \\ 0 & 1-(2\lambda_e+\lambda_v) & (2\lambda_e+\lambda_v) \\ 0 & 0 & 1 \end{bmatrix}$$

Properties of Laplace’s transformation

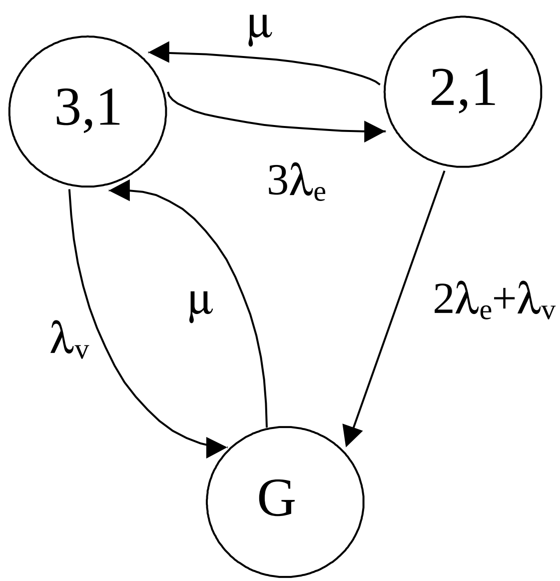
Markov Processes for maintenable systems

Two kinds of events:

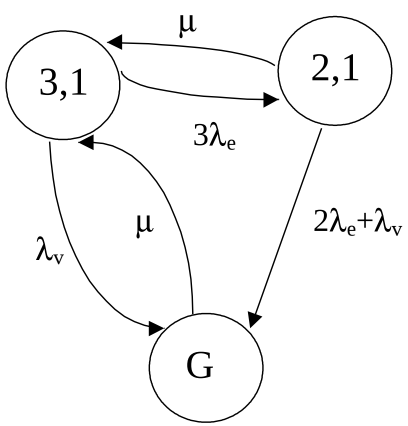
- fault of a component (module or voter)

- repair of the system (of a module or the voter or both)

***Hypothesis**: the maintenance process is exponentially distributed with repair rate equal to* $\boldsymbol{\mu}$



Availability evaluation of TMR system



$$\mathbf{P_{3,1}(t) + P_{2,1}(t) + P_G(t) = 1} \qquad \mathbf{P_{3,1}(0) = 1}$$

$$P'_{3,1}(t) = -(3\lambda_e + \lambda_v)\, P_{3,1}(t) + \mu\, P_{2,1}(t) + \mu\, P_G(t)$$

$$P'_{2,1}(t) = 3\lambda_e\, P_{3,1}(t) - (2\lambda_e + \lambda_v + \mu)\, P_{2,1}(t)$$

$$P'_G(t) = \lambda_v\, P_{3,1}(t) + (2\lambda_e + \lambda_v)\, P_{2,1}(t) - \mu\, P_G(t)$$

$$\frac{d\pi(t)}{dt} = \pi(t)\; Q(t)$$

i.e.

$$(P'_{3,1} \quad P'_{2,1} \quad P'_G) = (P_{3,1} \quad P_{2,1} \quad P_G) * Q$$

-

Availability evaluation of TMR system

		$-(3\lambda_e+\lambda_v)$	$3\lambda_e$	λ_v	
Q	=	μ	$-(2\lambda_e+\lambda_v+\mu)$	$(2\lambda_e+\lambda_v)$	
		μ	0	$-\mu$	

Q = P – I → **P = Q + I**

		$1-(3\lambda_e+\lambda_v)$	$3\lambda_e$	λ_v	
P	=	μ	$1-(2\lambda_e+\lambda_v+\mu)$	$(2\lambda_e+\lambda_v)$	
		μ	0	$1-\mu$	

Istantaneous Availability evaluation of TMR system

The Istantaneous Availability is the probability of being in any fault-free state (in this case: state (3,1) or (2,1)).

$$A(t) = P_{3,1}(t) + P_{2,1}(t) = 1 - P_G(t)$$

with the initial condition $P_{3,1}(0) = 1$

Limiting or steady state Availability evaluation of TMR system

$\mathbf{P_{3,1}(t) + P_{2,1}(t) + P_G(t) = 1}$ $\mathbf{P_{3,1}(0) = 1}$

with $\mathbf{t \rightarrow 00}$ we have that $\mathbf{P'(t) = 0}$

$$P'_{3,1}(t) = \mathbf{0} = -(3\lambda_e + \lambda_v)\, P_{3,1}(t) + \mu\, P_{2,1}(t) + \mu\, P_G(t)$$

$$P'_{2,1}(t) = \mathbf{0} = 3\lambda_e\, P_{3,1}(t) - (2\lambda_e + \lambda_v + \mu)\, P_{2,1}(t)$$

$$P'_G(t) = \mathbf{0} = \lambda_v\, P_{3,1}(t) + (2\lambda_e + \lambda_v)\, P_{2,1}(t) - \mu\, P_G(t)$$

Limiting or steady state Availability evaluation of TMR system

$\mathbf{P_{3,1}(t) + P_{2,1}(t) + P_G(t) = 1}$ $\mathbf{P_{3,1}(0) = 1}$

with $\mathbf{t} \rightarrow \infty$ we have that $\mathbf{P'(t) = 0}$ and $\mathbf{P(t) = P}$

$$P'_{3,1}(t) = \mathbf{0} = -(3\lambda_e + \lambda_v)\, P_{3,1} + \mu\, P_{2,1} + \mu\, P_G$$

$$P'_{2,1}(t) = \mathbf{0} = 3\lambda_e\, P_{3,1} - (2\lambda_e + \lambda_v + \mu)\, P_{2,1}$$

$$P'_G(t) = \mathbf{0} = \lambda_v\, P_{3,1} + (2\lambda_e + \lambda_v)\, P_{2,1}(t) - \mu\, P_G$$

Limiting or steady state Availability evaluation of TMR system

$$\mathbf{P_{3,1} + P_{2,1} + P_G = 1}$$

$$\mathbf{P_{3,1} =}$$

$$\mathbf{P_{2,1} =}$$

$$\mathbf{P_G =}$$

Safety evaluation

Four types of events:

- fault of a component (module or voter) correcttly diagnoticated

- fault of a component not detected

- correct repair of the system (of a module or the voter or both)

- uncorrect repair of the system

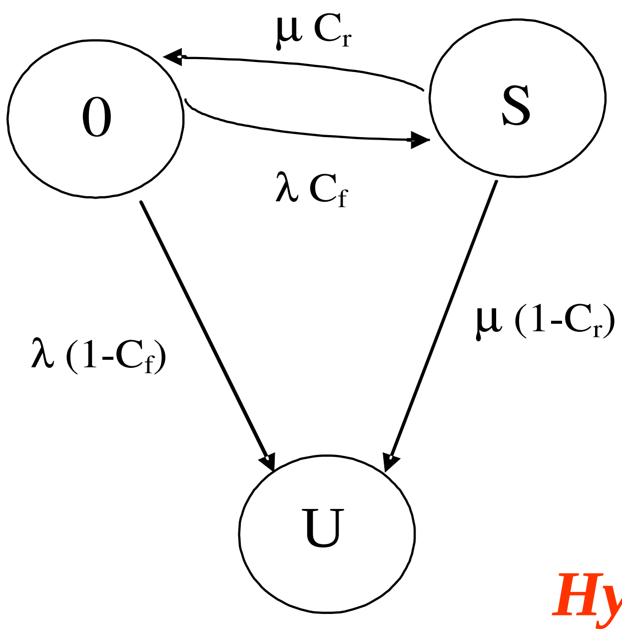
$\lambda \rightarrow$ ***fault rate***

$\mu \rightarrow$ ***repair rate***

$C_g \rightarrow$ ***fault detection coverage factor***

$Cr \rightarrow$ ***correct repair coverage factor***

Single component Safety evaluation



0 → fault free state

S→ safe fault state

U→ unsafe fault state

Hypothesis:

- ***if a fault is not well diagnosticated then it will never be detected***
- ***If a reconfiguration is not wel done then it will be never detected***

Therefore U is an absorbing state

Single component Safety evaluation

Safety = probability to stay in state 0 or GS

$P_O(t) + P_{GS}(t) = 1 - P_{GI}(t)$ $P_O(0) = 1$

$$P'_O(t) = -(\lambda(1 - C_g) + \lambda C_g))\, P_O(t) + \mu C_r\, P_{GS}(t)$$

$$P'_{GS}(t) = \lambda C_g\, P_O(t) - (\mu(1 - C_r) + \mu C_r)\, P_{GS}(t)$$

$$P'_{GI}(t) = \lambda(1 - C_g)\, P_O(t) + (\mu(1 - C_r)P_{GS}(t)$$

Single component Safety evaluation

$$\frac{d\pi(t)}{dt} = \pi(t)\ Q(t)$$

i.e.

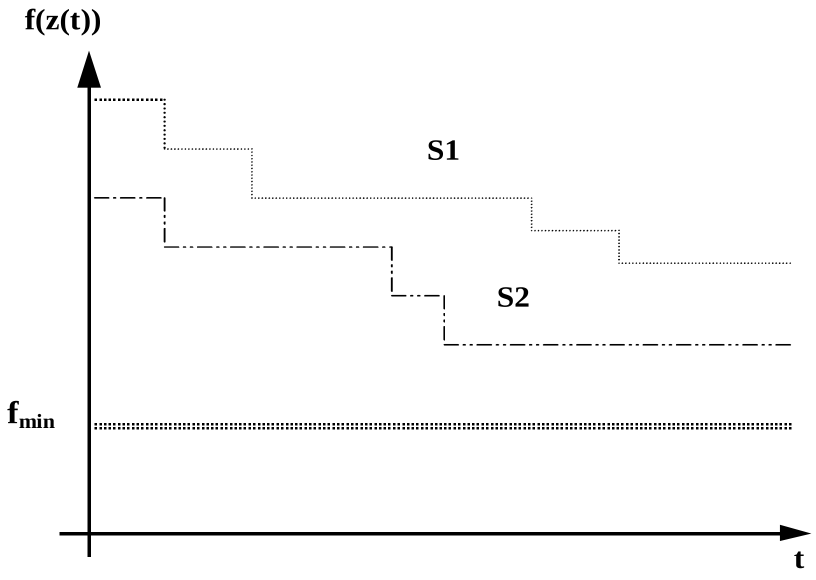
$$(P'_{3,1} \quad P'_{2,1} \quad P'_G) = (P_{3,1} \quad P_{2,1} \quad P_G) * Q$$

-

		$-\lambda$	λC_g	$\lambda(1-C_g)$	
Q	=	μC_r	μ	$\mu\ (1-C_r)$	
		0	0	0	

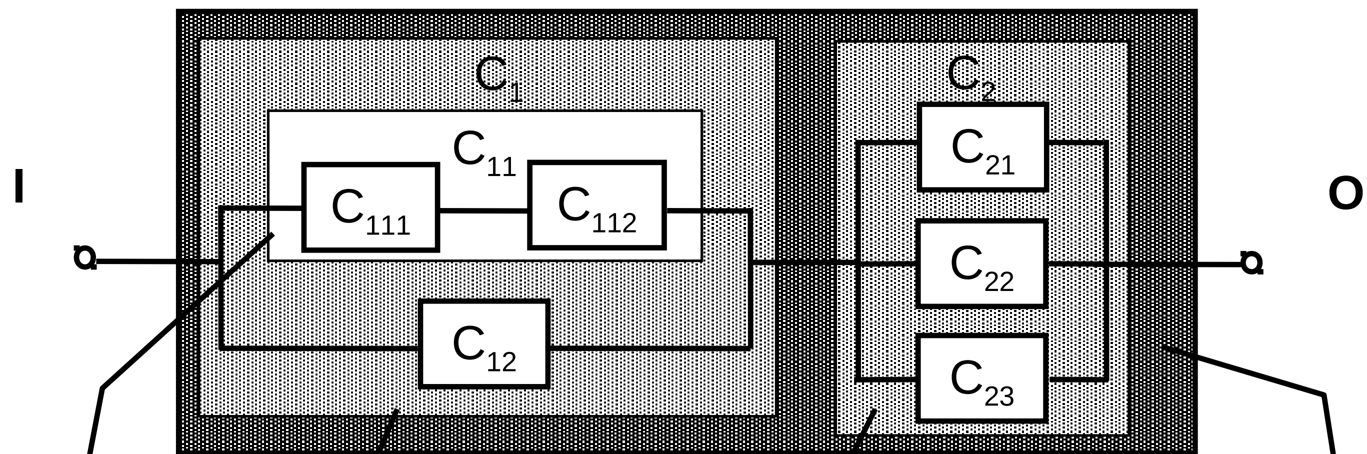
Performability

Index taking into account even the performance of the system given its state (related to the number of fault-free components)



We will discuss it when we will know how evaluate the performance of a system

Reliability/Availability/Safety evaluation of complex system



$R_{11} = R_{111} . R_{112}$

$R_1 = 1 - (1 - R_{11}) . (1 - R_{12})$

$R_2 = 1 - (1 - R_{21}) . (1 - R_{22}) . (1 - R_{23})$

$R = R_1 . R_2$