Dependability Evaluation

Techniques for Dependability Evaluation

The dependability evaluation of a system can be carried out either:

- ***experimentally (heuristic)***: a system prototype is built and empirical statistical data are used to evaluate the system's metrics:
  - by far more expensive and complex than the analytic approach
  - building a system prototype may be impossible
  - experimental evaluation of dependability requires long observation periods

- ***analytical***: dependability metrics are obtained by a mathematical model of the system:
  - mathematical models may not adequately represent the real system's strucure or the behavior of its components
  - simulation models may be a complementary helpful tool

Fundamental Definitions

- ***Failure Function Q(t):***
  - probability that a component fails for the first time in the time interval $(0,t)$
  - it's a cumulative distribution function:

$Q(t) = 0$	for $t = 0$
$0 \leq Q(t) \leq Q(t + \Delta t)$	for $\Delta t \geq 0$
$Q(t) = 1$	for $t \rightarrow +\infty$

Fundamental Definitions (cont'd)

- ***<u>Reliability Function R(t):</u>***
  - probability that a component functions correctly in the time interval *(0,t)*

$R(t) = 1$ for $t = 0$

$1 \geq R(t) \geq R(t + \Delta t)$ for $\Delta t \geq 0$

$R(t) = 0$ for $t \rightarrow +\infty$

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

Fundamental Definitions (cont'd)

- ***Failure probability density function q(t):*** it's the derivative of *Q(t)* when this is a continous function:

$$q(t) = \frac{dQ(t)}{dt}$$

- *R(t)* is continous too and its derivative over time *r(t)* is equal to:

$$r(t) = \frac{dR(t)}{dt} = \frac{d(1-Q(t))}{dt} = -\frac{dQ(t)}{dt} = -q(t)$$

- *R(t)* and *Q(t)* are experimentally evaluated analyzing the behavior of a sufficiently large population and determining the failure rate .

- *N*: population at time *t = 0*
- *n(t):* correct components at time *t*

$$R(t) = \frac{n(t)}{N}$$

Average Failure Frequency

Average failure frequency during the time interval *(t, t + Δt)* :

$$\frac{n(t) - n(t + \Delta t)}{\Delta t}$$

Average failure frequency of a single unit in the time interval *(t, t + Δ t)* :

$$\frac{1}{n(t)} \frac{n(t) - n(t + \Delta t)}{\Delta t}$$

Instantaneous Failure Frequency

If Δt tends to zero each entity at time t is characterized by an ***instantaneous failure frequency*** given by:

$$h(t) = \lim_{\Delta t \to 0} \frac{1}{n(t)} \frac{n(t) - n(t + \Delta t)}{\Delta t} = \frac{1}{n(t)} \left(-\frac{dn(t)}{dt} \right) =$$

$$= \frac{1}{NR(t)} \left(-\frac{dNR(t)}{dt} \right) = -\frac{N}{NR(t)} \frac{dR(t)}{dt} = -\frac{dR(t)}{R(t)} \frac{1}{dt}$$

Being : $$-h(t)dt = \frac{dR(t)}{R(t)}$$

after integration, we obtain the reliability function:

$$R(t) = e^{-\int_0^t h(\tau) d\tau}$$

MTTF (Mean Time To Failure)

- *Index used to evaluate reliability and other dependability metrics.*
- ***MTTF*** (Mean Time To Failure). Expected time before a failure, or expected operational time of a system before the occurrence of the first failure.

$$MTTF = \int_0^\infty t q(t) dt$$

- It can also be calculated (expanding q(t)) as:

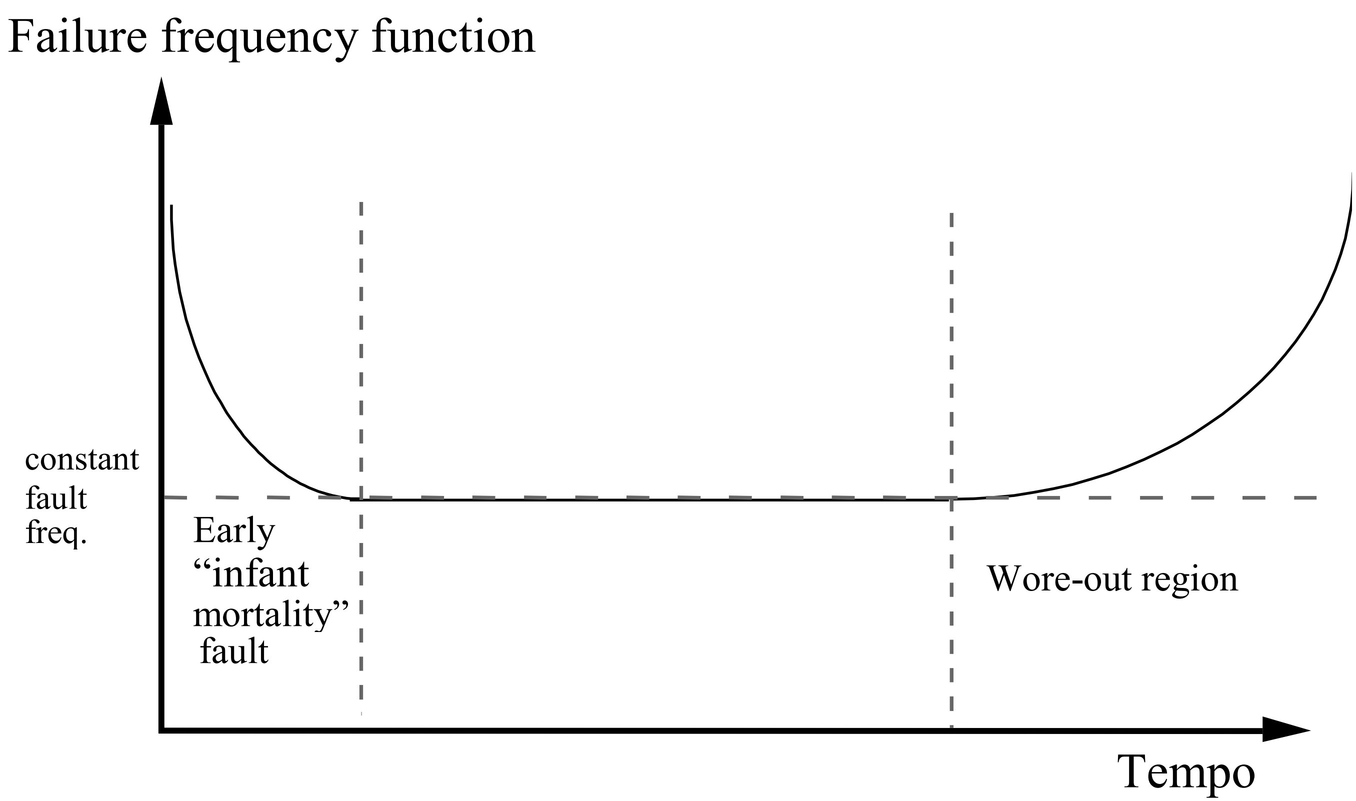
$$MTTF = -\int_0^\infty t \frac{dR(t)}{dt} dt = -\left[tR(t)\right]_0^\infty + \int_0^\infty R(t) dt = \int_0^\infty R(t) dt$$

being

$$\lim_{t\to\infty} tR(t) = \lim_{t\to\infty} te^{-\int_0^\infty h(\tau) d\tau} = 0$$

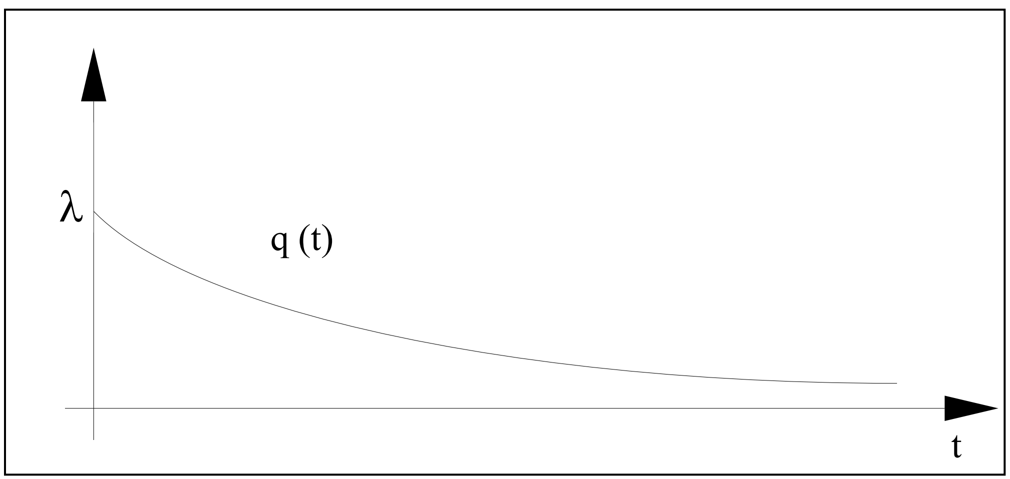
given that *h(t)* is constant or increases over time.

Bathtube curve



Failure Frequency Function

- The first and third region can be excluded assuming to use the entities after the initial testing period and before their aging time.
- Hence, the instantaneous fault frequency function can be assumed constant: $h(t) = \lambda$



$$R(t) = e^{-\int_0^t h(\tau)d\tau} = e^{-\lambda t}$$

$$Q(t) = 1 - e^{-\lambda t}$$

$$r(t) = -\lambda e^{-\lambda t}$$

$$q(t) = \lambda e^{-\lambda t}$$

Repairable Systems

- In the case of *repairable* systems, besides the “fault occurrence” event, the event “repairing” or “replacement” of the faulty components has to be considered:

- ***MTTF*** Mean Time to Fault
- ***MTTR*** (Mean Time To Repair) iThe average time to repair or replace a faulty entity

$\Downarrow$

- **System Availability:**

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

- ***MTBF*** (Mean Time Between Fault) is the average time between two faults, given by the sum of *MTTF* and *MTTR.*

Cover Factor

- Conditional probability that, after the occurrence of a failure, the system returns to function correctly.
- Measure of the system’s ability to reveal a fault, localize it, contain it and restore a consistent and error free state
- For its estimation it’s needed to identify every possible fault, and for each fault, forecast its frequency and the corresponding cover factor.

Limits:

- Hard to determine the probability of every possible fault
- Often it is unrealistic to take into account every possibe fault
- The cover factor is determined considering one fault at a time, whereas one should keep into account the possibility of multiple concurrent faults.

Dependability Evalution

- Dependability evaluation of a complex system can be performed via either:

COMBINATORIAL MODELS

↓

<u>Combinatorial Methods</u>

1. reliability
2. availability

MARKOVIAN MODELS

↓

<u>Markov Processes</u>

1. reliability
2. availability
3. security
4. performability

Combinatorial Models

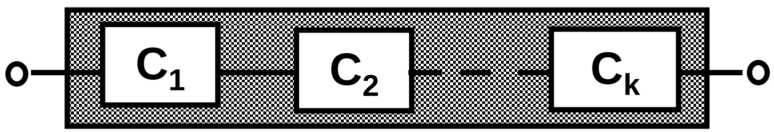
- Availability and reliability of computing systems cosiders the system as composed by a set of interconnected entities.
- ***First step****:* identify availability and reliability of each composing entitiy;
- ***Second step****:* identify the configurations that allow the analyzed system to operate according to the project's specifications;
- ***Third step****:* identify the relation between the faults of each entity and those of the whole system.
- Enitities, in their turn, are made up of components whose dependability metrics depend on:
  - *Components' quality,*
  - *Mainteinance policies,*
  - *Mutual interconnections*

Interconnections

- Typical interconnections are:
  - *Serial*
  - *Parallel*
  - *TMR*
  - *Hybrid M out of N*

Serial Interconnection

- *K* entities are serially inteconnected when the functioning of the system depends on the correct functioning of all the K entities.



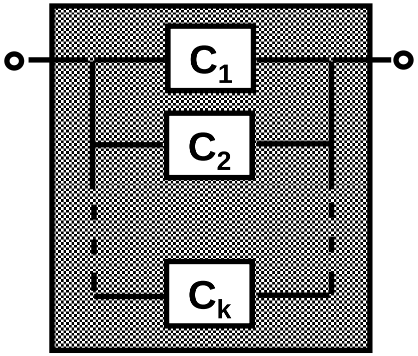
- Given:
  - $R_i(t)$ = reliability of each entity
  - A_i = availability of each entity
- one can derive the following system wide metrics:

$$R(t) = \prod_{i=1}^{K} R_i(t)$$

$$A = \prod_{i=1}^{K} A_i$$

Parallel Interconnection

- *k* entities are inteconnected in parallel when the functioning of the system is guaranteed even if just a single entity works.



- Given:
  - $R_i(t)$ = reliability of each entity
  - A_i = availability of each entity
- we can derive the following system wide metrics:

$$R(t) = 1 - (1 - R_1(t))(1 - R_2(t))\ldots(1 - R_K(t))$$

$$A = 1 - (1 - A_1)(1 - A_2)\ldots(1 - A_K)$$

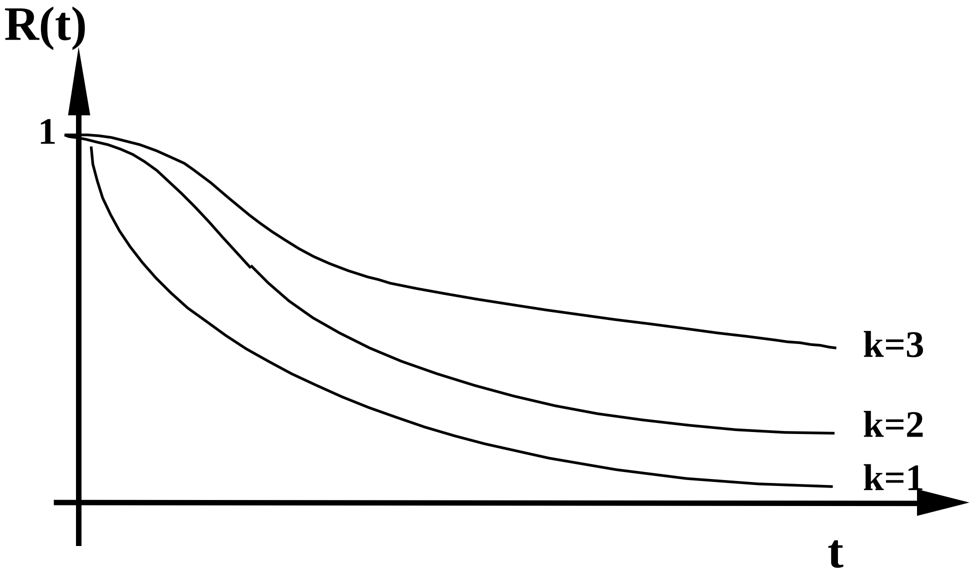
- the system does not work (is unavailable) if all *k* entities fail (are unavailable).

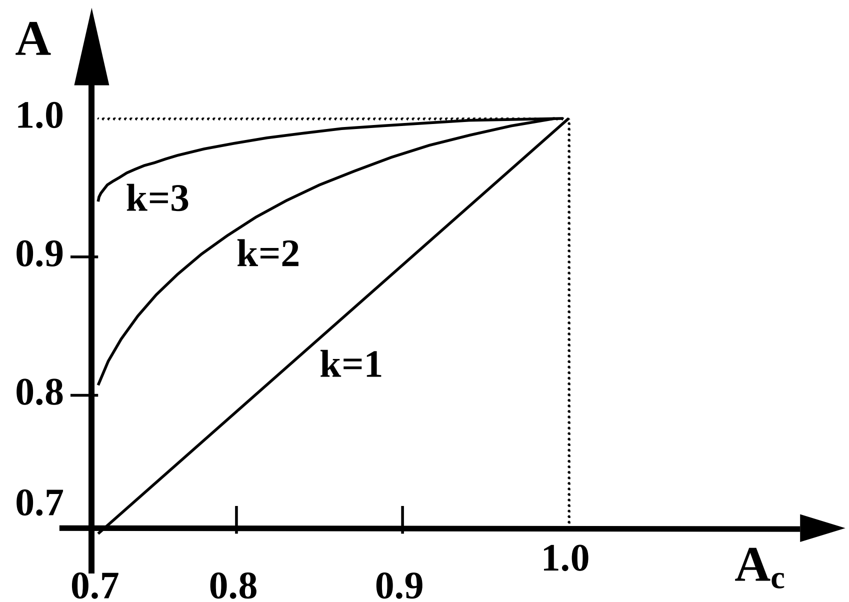
Parallel Interconnection (cont'd)

- In the case of entities having the same reliability $R_C(t)$ or availability A_C we get that:

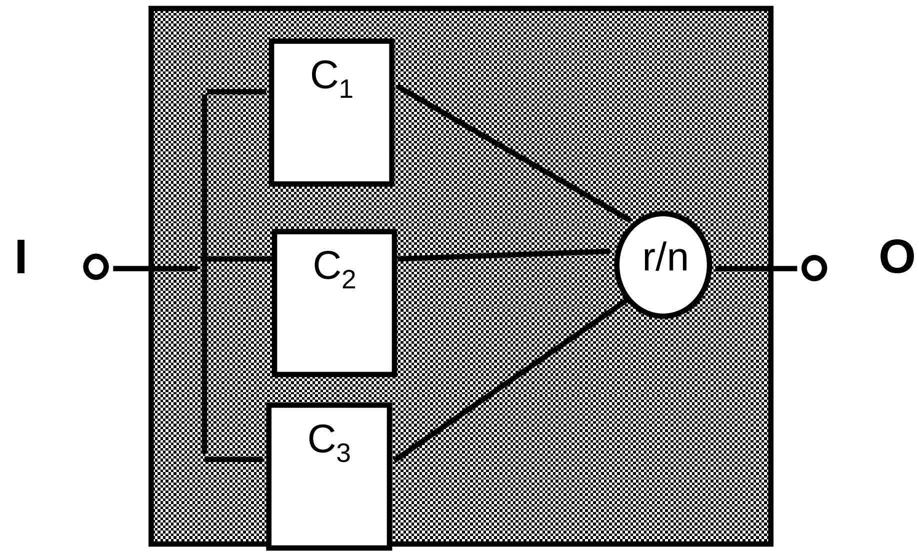
$$R(t) = 1 - (1 - R_C(t))^K$$

$$A = 1 - (1 - A_C)^K$$





TMR Interconnection

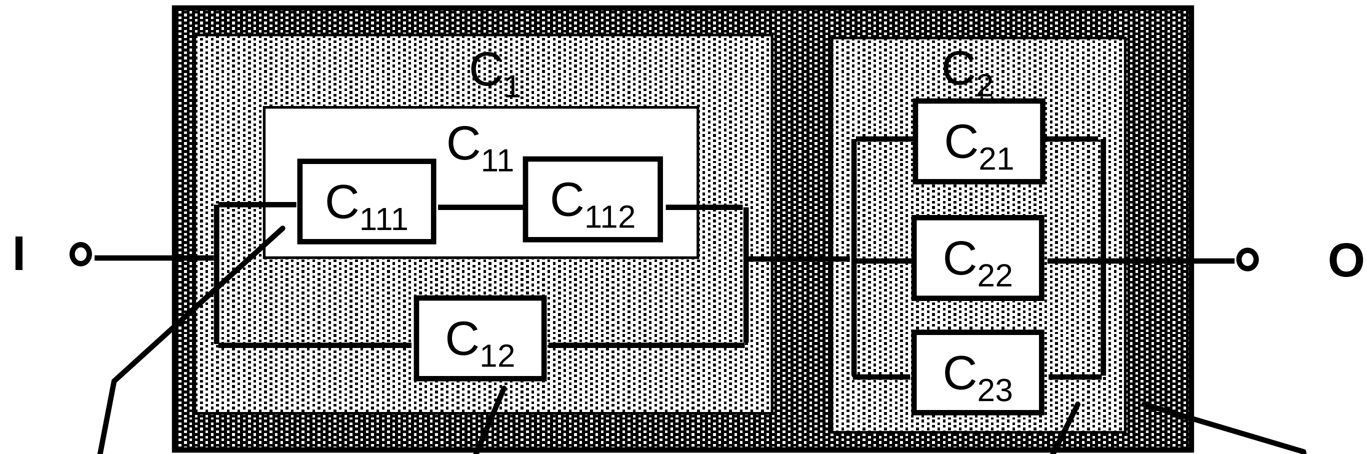


- The system fails or is not available when two entities are simultaneously faulty/unavailable or when the voter is faulty/unavailable:

$$R(t) = \left[R_C(t)^3 + 3R_C(t)^2(1 - R_C(t))\right]R_{VOTER}(t)$$

$$A = \left[A_C{}^3 + 3A_C{}^2(1 - A_C)\right]A_{VOTER}$$

Parallel/Serial Interconnections



$R_{11} = R_{111} \cdot R_{112}$

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

$R = R_1 \cdot R_2$

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

Hybrid M out of N interconnection

- The system works as long as there are at least *M* correct entities, namely at most $K = N - M$ entities fail.
- Given:
  - $R_i(t)$ = reliability of each entity
  - A_i = availability of each entity
- one can derive the following system wide metrics:

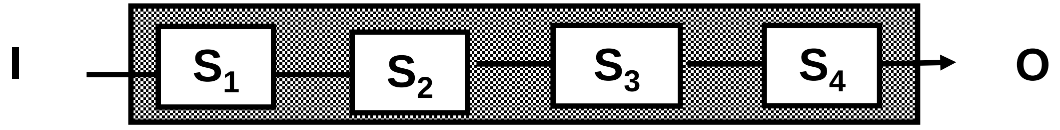
$$R(t) = \sum_{i=0}^{K} \binom{N}{i} R_C^{N-i}(t)(1 - R_C(t))^i$$

$$A = \sum_{i=0}^{K} \binom{N}{i} A_C^{N-i}(1 - A_C)^i$$

- Infact, the probability that:
  - N entities are correct is: $R_C^N(t)$
  - N-1 entities are correct: $NR_C^{N-1}(t)(1 - R_C(t))$
  - N-2 entities are correct: $\binom{N}{2} R_C^{N-2}(t)(1 - R_C(t))^2$
  - N-K entities are correct: $\binom{N}{K} R_C^{N-K}(t)(1 - R_C(t))^K$

Evaluation Examples

- Let us consider a non-redundant system composed of 4 serially connected entities:

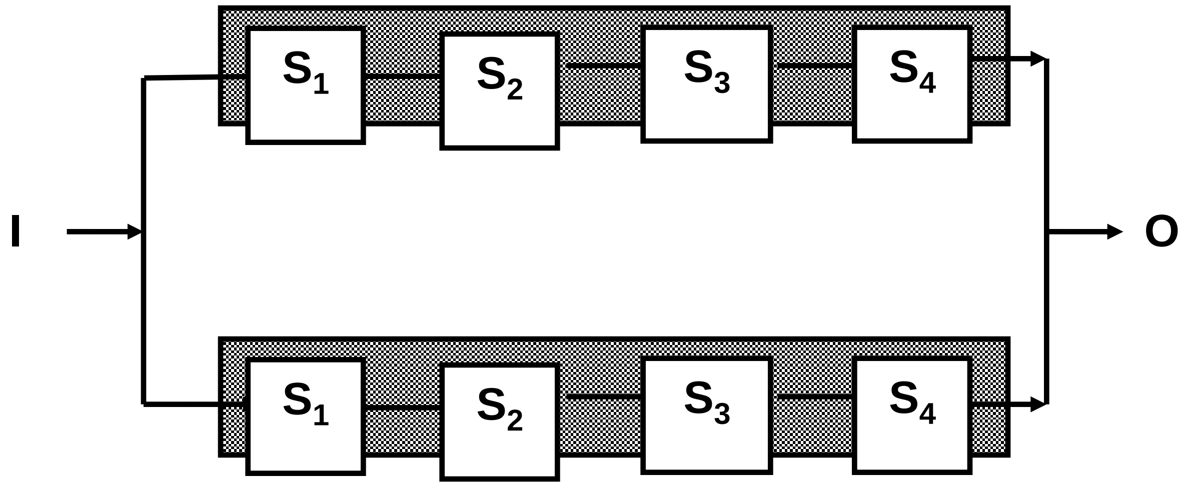


$$R(t) = R_1(t)R_2(t)R_3(t)R_4(t)$$

$$A = A_1 A_2 A_3 A_4$$

- How can I increase the system’s dependability?

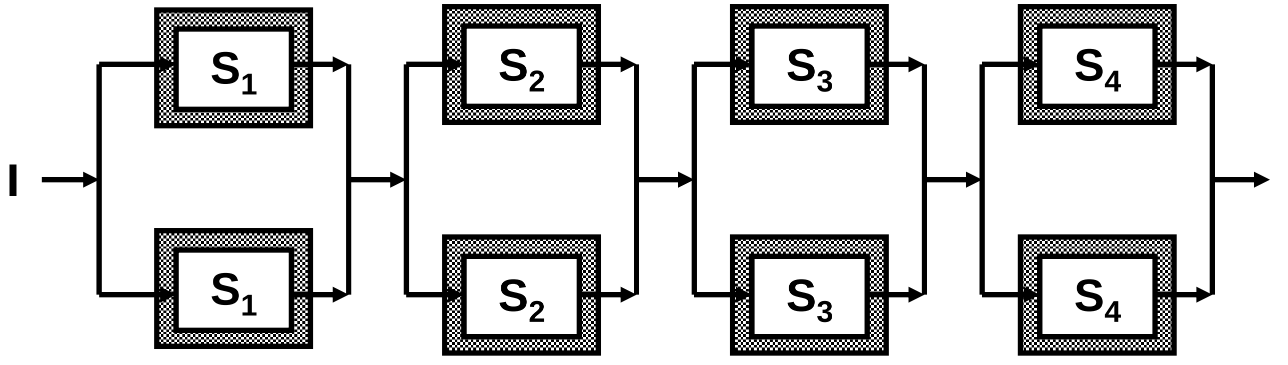
Pair with a duplicated system



$$R_{d1}(t) = 1 - (1 - R(t))^2$$

$$A_{d1} = 1 - (1 - A)^2$$

Duplicate Each Component



$$R_{d2}(t) = R_{1d}(t)R_{2d}(t)R_{3d}(t)R_{4d}(t)$$

$$A_{d2} = A_{1d}A_{2d}A_{3d}A_{4d}$$

where:

$$R_{id}(t) = 1-(1-R_i(t))^2$$

$$A_{id} = 1-(1-A_i)^2$$

Quantifying the dependability of the considered configurations

- Assuming, e.g., that each $A_i = 0,9$, the system's availability in the three cases is, respectively:
  - $A = 0,6561$
  - $A_{d1} = 0,8817$
  - $A_{d2} = 0,9606$