Università
degli Studi di
Messina
DIPARTIMENTO DI INGEGNERIA

Dependable computing modeling and simulation

Unrepairable systems

Master degree in

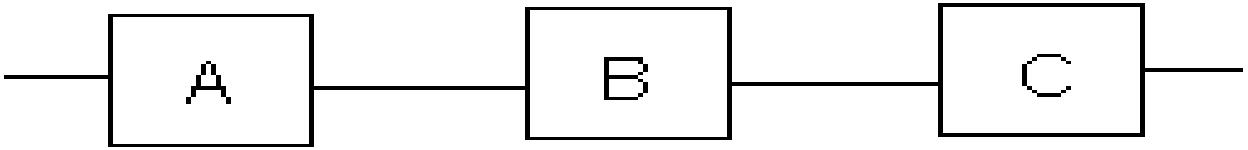
Engineering in Computer Science

Complex system

- It is a system where many sub-systems interact in order to obtain a goal
- We want to evaluate system reliability by knowing sub-systems reliability
- Reliability definition is extended

Series

- System components are connected in such a way all of them are necessary for having a working system
- When one component (*block*) fails the overall system fails



System series

- A logic view: the system is connect as a series
- E. g.:
  - A server made by a power supply, a memory bank, a mother board and a microprocessor (four blocks);
  - The components are not electrically connected in series, but a single component fault (block) threatens the overall system

System reliability

- X_s = *system* failure time
- X_i = *i*-th *block* failure time
- The system works if all the sub-system work
- $R_s(t)=P[X_s>t]=P[X_1>t, X_2>t, \ldots, X_n>t]$
- Statistically independent blocks

$$R_s(t)=P[X_1>t]\cdot P[X_2>t]\cdots P[X_n>t]=\prod_{i=1}^{n} R_i(t)$$

Remarks

$$R_S(t) = \prod_{i=1}^{n} R_i(t)$$

- System reliability is less than the lowest sub-system reliability
- The most fragile sub-system heavily weighs on the system reliability

A series system is less reliable than the reliability of its components

An example

$$R_i(t) = e^{-\lambda_i t}$$

$$R_s(t) = e^{-\lambda_1 t} \cdot e^{-\lambda_2 t} \cdot \ldots \cdot e^{-\lambda_n t} = e^{-(\lambda_1 + \lambda_2 + \ldots + \lambda_n) t} = e^{-\lambda_s t}$$

$$\lambda_s = \lambda_1 + \lambda_2 + \cdots + \lambda_n$$

- The failure time of series system is exponentially distributed

$$MTTF_s = \frac{1}{\lambda_s}$$

Numerical example

- R = memory; $\lambda_R = 2*10^{-6}$ 1/h
- L = processor; $\lambda_L = 5*10^{-6}$ 1/h
- P = power supply; $\lambda_P = 2*10^{-5}$ 1/h
- V = mother board; $\lambda_V = 1*10^{-5}$ 1/h

We want to compute the reliability at one year mission time ($\bar{t}$ = 8760 h)

Numerical example (cont.)

- $R_R(\bar{t}) = \exp(-\lambda_R \bar{t}) = 0{,}983$
- $R_L(\bar{t}) = \exp(-\lambda_L \bar{t}) = 0{,}957$
- $R_V(\bar{t}) = \exp(-\lambda_V \bar{t}) = 0{,}916$
- $R_P(\bar{t}) = \exp(-\lambda_P \bar{t}) = 0{,}839$

- $R_S(\bar{t}) = 0{,}983 * 0{,}957 * 0{,}916 * 0{,}839 = 0{,}723$
- After one year the system worked without faults with a probability equal to 72%
- Note that $R_S(\bar{t})$ is less than $R_P(\bar{t})$

Numerical example (cont.)

- $\lambda_S = \lambda_R + \lambda_L + \lambda_P + \lambda_V = 3.7 * 10^{-5}$ g/h
- $R_S(\bar{t}=8760)=\exp(-\lambda_S \bar{t}) = 0.723$

Reliability improvement

- $R_1(t), R_2(t), \ldots, R_i(t), \ldots, R_n(t)$
- $R_i(t)$ increases of a fixed quantity ΔR_i

$$R_s(t)+\Delta R_s=R_1(t)\cdot R_2(t)\cdot\ldots\cdot(R_i(t)+\Delta R_i)\cdot\ldots\cdot R_n(t)=$$

$$=R_1(t)\cdot R_2(t)\cdot\ldots\cdot R_i(t)\cdot\ldots\cdot R_n(t)+R_1(t)\cdot R_2(t)\cdot\ldots\cdot\Delta R_i\cdot\ldots\cdot R_n(t)\cdot\frac{R_i(t)}{R_i(t)}$$

$$R_s(t)+\Delta R_s=R_s(t)+\frac{R_s(t)\cdot\Delta R_i}{R_i(t)}$$

$$\Delta R_s=\frac{R_s(t)}{R_i(t)}\cdot\Delta R_i$$

How reliability changes

$$\frac{\Delta R_s}{\Delta R_i} = \frac{R_s(t)}{R_i(t)}$$

- *The percentage increase of reliabilty is higher the lower is the reliability of the improved component*

An example

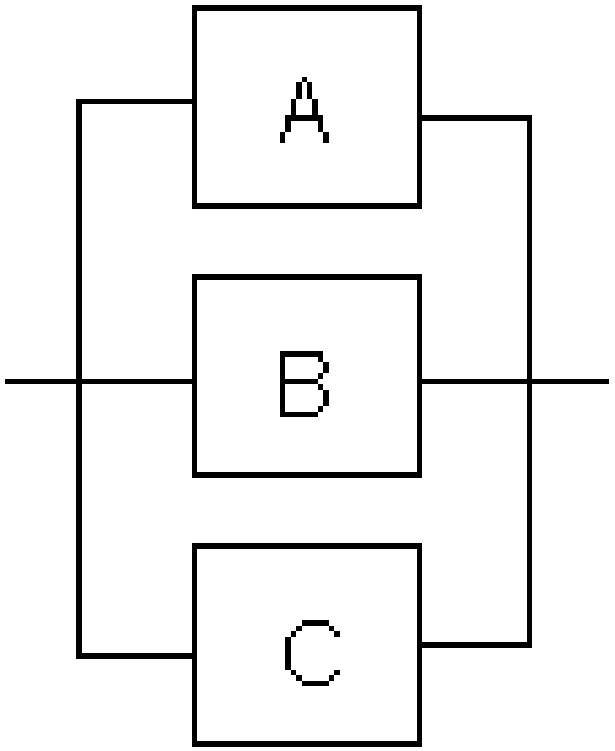
- The reliability of R (memory) is improved of $\Delta R_i = 0.012$
  - $R_s'(t) = (0{,}983 + 0{,}012) \cdot 0{,}957 \cdot 0{,}839 \cdot 0{,}916 = 0{,}732$
- The reliability of P (power supply) of $\Delta R_i = 0.012$
  - $R_s''(t) = 0{,}983 \cdot 0{,}957 \cdot (0{,}839 + 0{,}012) \cdot 0{,}916 = 0{,}733$
- $R_s' < R_s''$

Redundant system

- *A system is said redundant when the failure of an elementary component does not involve the failure of the entire system*

Parallel redundancy

- The same block is replicated in parallel



Unreliability

- Let us consider two components whose *unreliability* is $F_1(t)$ and $F_2(t)$ respectively
- The system does not work if all the two components failed
- $F_S(t)=P[X_S \leq t]=P[X_1 \leq t, X_2 \leq t]$

Unreliability

- Statistically independent components

  $F_S(t) = Pr[X_1 \le t]\ Pr[X_2 \le t] = F_1(t)\ F_2(t)$

  $F_S(t) = 1 - R_S(t) = (1 - R_1(t))\ (1 - R_2(t))$

  $R_S(t) = R_1(t) + R_2(t) - R_1(t)\ R_2(t)$

- In general

$$F_s(t) = 1 - R_s(t) = \prod_{i=1}^{n} (1 - R_i(t))$$

An example

$$R_1(t) = e^{-\lambda_1 \cdot t}$$

$$R_2(t) = e^{-\lambda_2 \cdot t}$$

$$R_s(t) = e^{-\lambda_1 \cdot t} + e^{-\lambda_2 \cdot t} - e^{-(\lambda_1 + \lambda_2)\, t}$$

$$MTTF = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1 + \lambda_2}$$

- The system failure time is **not** exponentially distributed
- Its distribution is said *exponomial*

Series vs Parallel

- The system is faulty if at least one of the components is faulty
- Reliability is **less** than the **smallest** component reliability
- If the components behave exponentially also the system behaves exponentially

- The system is faulty iff all the components are faulty
- System reliability is greater than the reliability of its components
- Although the components behave in an exponential way the system does NOT

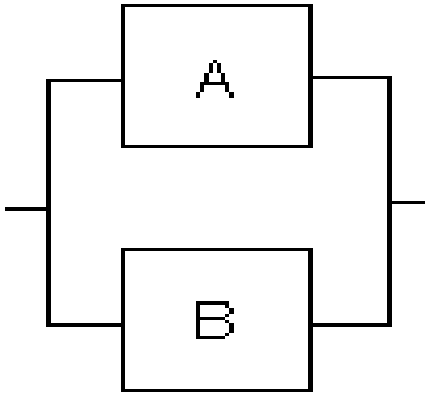
Parallel system

- $R_1(t), R_2(t), \ldots, R_i(t), \ldots, R_n(t)$
- $R_i(t)$ increases of ΔR_i
- Look at the *unreliability*

$$\frac{\Delta R_s}{\Delta R_i} = \frac{1 - R_s(t)}{1 - R_i(t)}$$

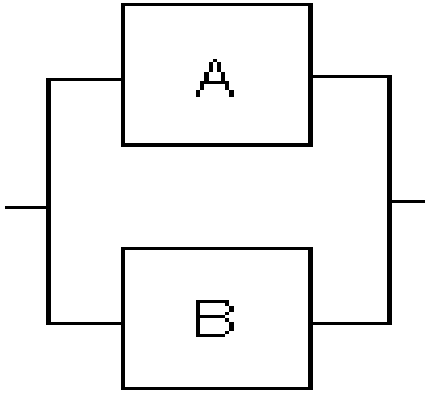
- It is convenient to improve the reliability of the most reliable block

An example



- $R_P(t) = R_A(t) + R_B(t) - R_A(t) \cdot R_B(t)$
- $R_A(\bar{t}) = 0.5,\ R_B(\bar{t}) = 0.85$
- $R_P(\bar{t}) = 0.5 + 0.85 - (0.5 \cdot 0.85) = 0.925$

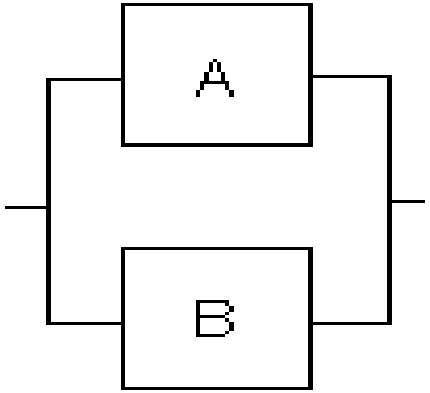
An example (cont.)



- The reliability of component *A* is increased, $\Delta R = 0.10$

- $R'_P(\bar{t}) = [R_A(\bar{t}) + \Delta R] + R_B(\bar{t}) - [(R_A(\bar{t}) + \Delta R) * R_B(\bar{t})] = [0.5 + 0.1] + 0.85 - [(0.5 + 0.1) * 0.85] = 0.940$

An example (cont.)



- The reliability of component B is increased, $\Delta R = 0.10$

- $R''_P(\bar{t}) = R_A(\bar{t}) + [R_B(\bar{t}) + \Delta R] - [R_A(\bar{t}) * (R_B(\bar{t}) + \Delta R)] = 0.5 + [0.85 + 0.1] - [0.5 + (0.85 * 0.1)] = 0.975$

An example (cont.)

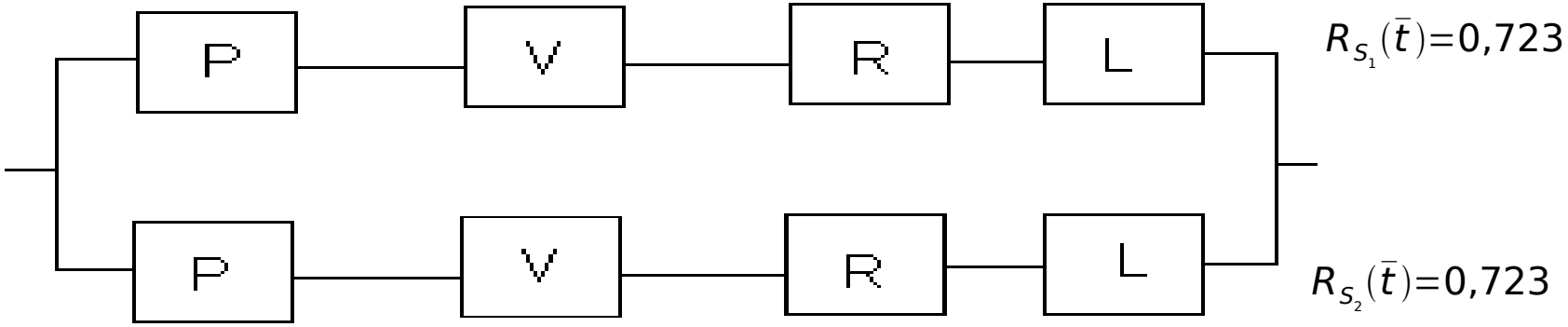
- We can note that

$$R'_P < R''_P$$

- Unlike series systems, it is better to modify the most reliable component in parallel systems
- Anyway, by modifying the less reliable component system reliability increases

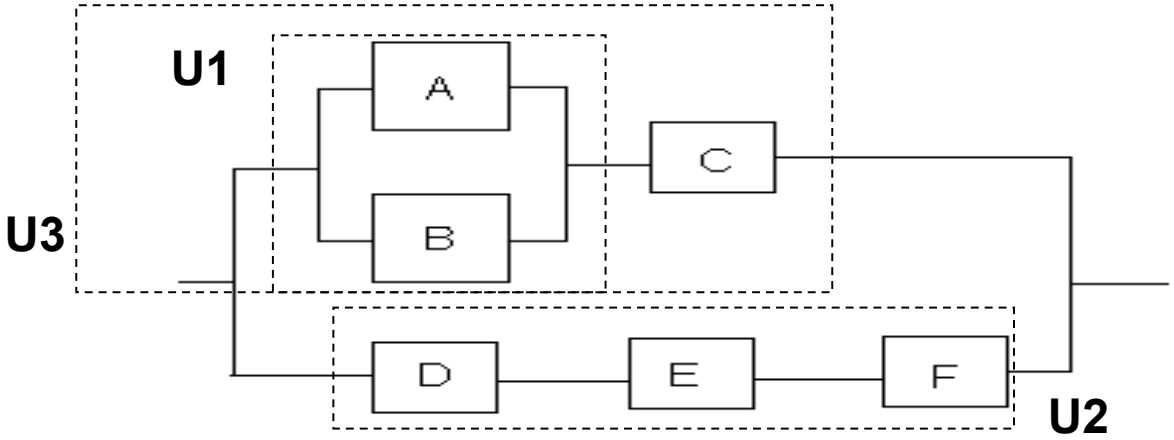
Series-parallel system

- The easiest way is to make all the system (all the components) redundant



$$R_S(\bar{t})=2\cdot 0,723-(0,723)^2=0,923$$

Series/parallel

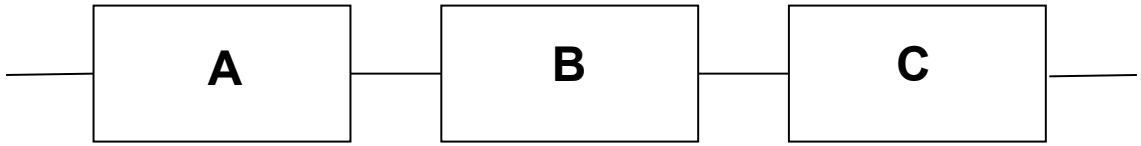


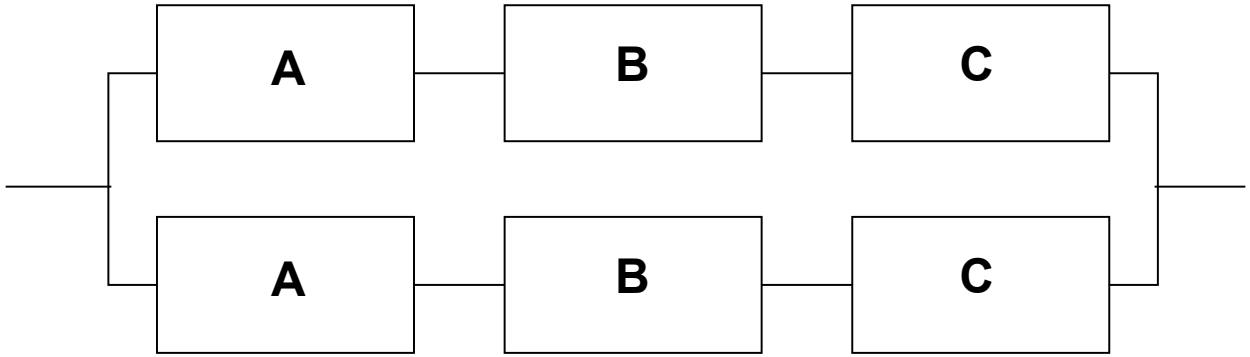
- $R_{U1}=R_A+R_B-R_AR_B$
- $R_{U2}=R_D R_E R_F$
- $R_{U3}=R_{U1}R_C$
- $R_S=R_{U3}+R_{U2}-R_{U3}R_{U2}$

Series/parallel

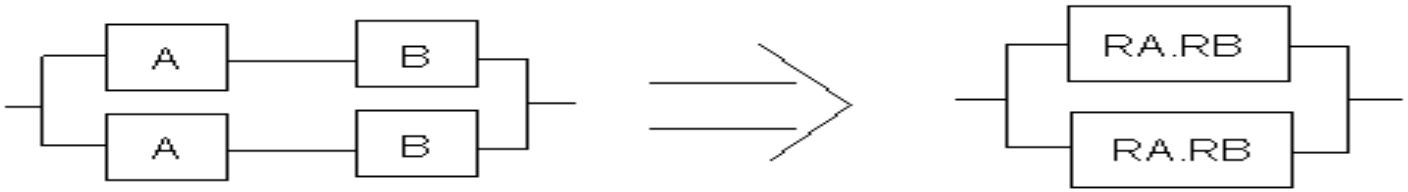
- The more complex logic configurations can be easily resolved by applying simple formulas (but not always)

System redundancy



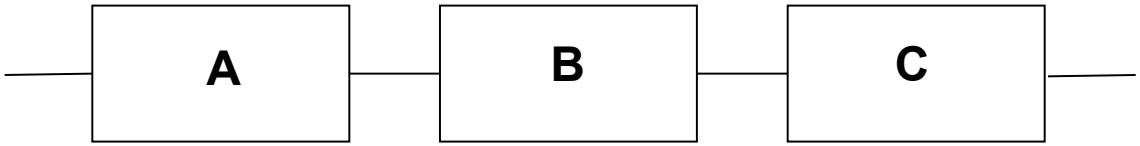


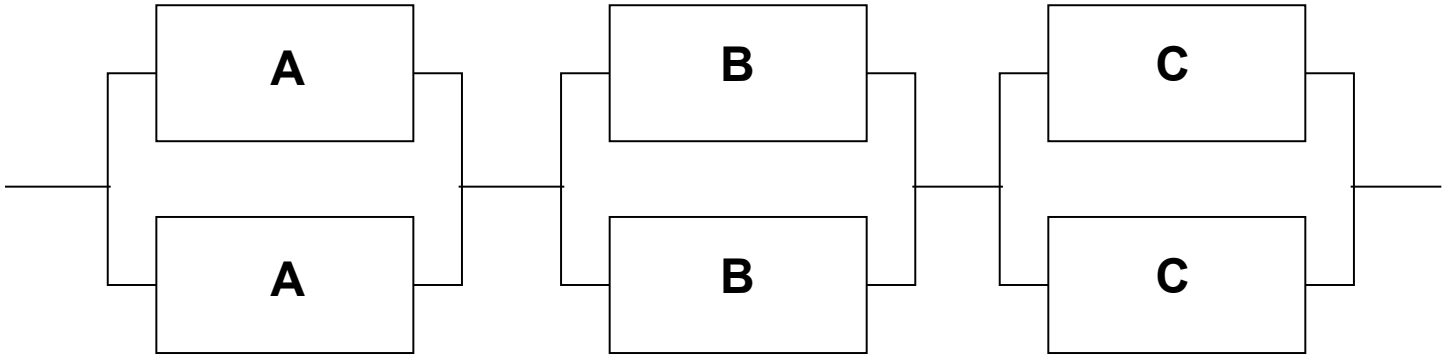
System redundancy



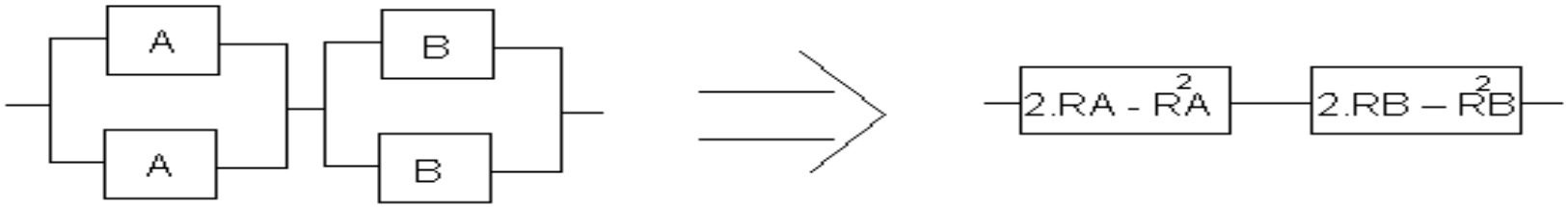
- $R_a = 2 \cdot R_A \cdot R_B - (R_A \cdot R_B)^2 = R_A \cdot R_B \, (2 - R_A \cdot R_B)$

Component redundancy





Component redundancy



$$R_b = (2 \cdot R_A - R_A^2)(2 \cdot R_B - R_B^2)$$

$$R_b = R_A \cdot R_B [\, 4 - 2 \,(R_A + R_B) + R_A \cdot R_B]$$

System vs Component redundancy

$$\frac{R_b}{R_a}=\frac{R_A R_B\left[4-2(R_A+R_B)+R_A R_B\right]}{R_A R_B(2-R_A R_B)}$$

$$=\frac{2+2-2(R_A+R_B)+2\mathrm{R}_A R_B-R_A R_B}{2-R_A R_B}=$$

$$=1+\frac{2-2(R_A+R_B)+2\mathrm{R}_A R_B}{2-R_A R_B}=$$

$$=1+\frac{2(1-R_A)(1-R_B)}{2-R_A R_B}>1$$

Summarising

- The (total) component redundancy is better than the (total) system redundancy
- If a block fails, there is always a path connecting the input and output of the system (as long as two components of the same type do not spoil)
- The component redundancy gives greater reliability but is more expensive by an architectural point of view (more complex architectural choices must be applied to be effective)

Complex structures

- Sometimes it is not possible to have series-parallel structures
- Some elements can appear multiple times, but each element is independent with respect the other

Heuristic method

- It is based on the *total probability theorem*
- Given the events

$$A \in S, \quad B_i \in S \quad i = 1, \ldots, n$$

where $B_1 \cup B_2 \cup \cdots \cup B_n = S, \; B_i \cap B_j = \emptyset, \; \forall i, j$

then

$$P(A) = \sum_{i=1}^{n} P(A|B_i) P(B_i)$$

Event partitioning

- Let us consider the following events
  - E_S="The system is operational in (0, t]"
  - E_{S1}="The component C is operational in (0, t] and the system is operational in (0, t]"
  - E_{S2}="The component C failed in (0, t] and the system is operational in (0, t]"
- Let X_C be the failure time of C

System reliability

- The system reliability is

$$R_S(t) = P[E_{S1}] + P[E_{S2}] =$$

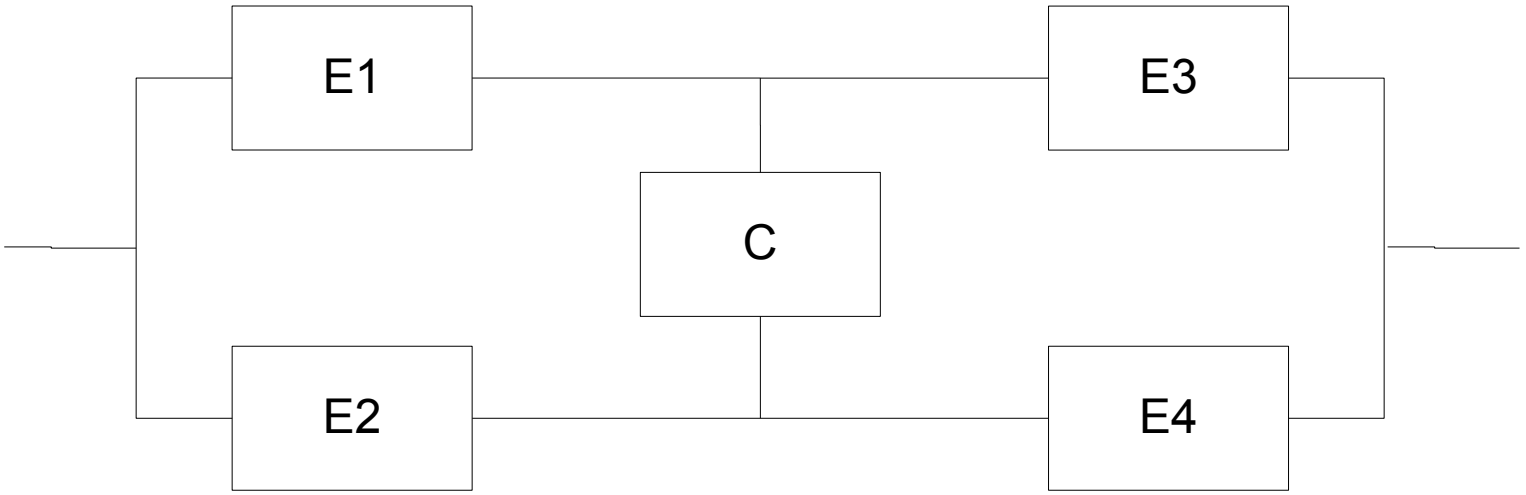
$$= P[X_C > t]\, P[X_S > t | X_C > t] +$$
$$P[X_C \leqslant t]\, P[X_S > t | X_C \leqslant t] =$$

$$= R_C(t)\, R_S(t | X_C > t) + (1 - R_C(t))\, R_S(t | X_C \leqslant t)$$

In practice

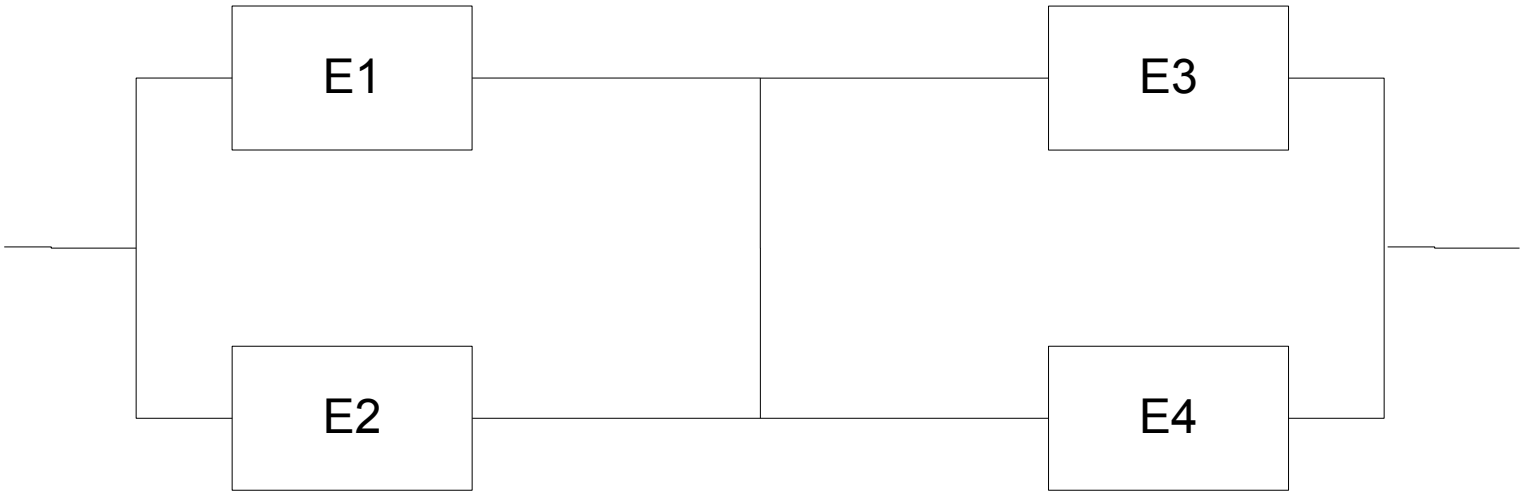
- The component C has to be chosen in such a way the system configures itself as a series/parallel system
- Repeated applications are possible

The *bridge* structure



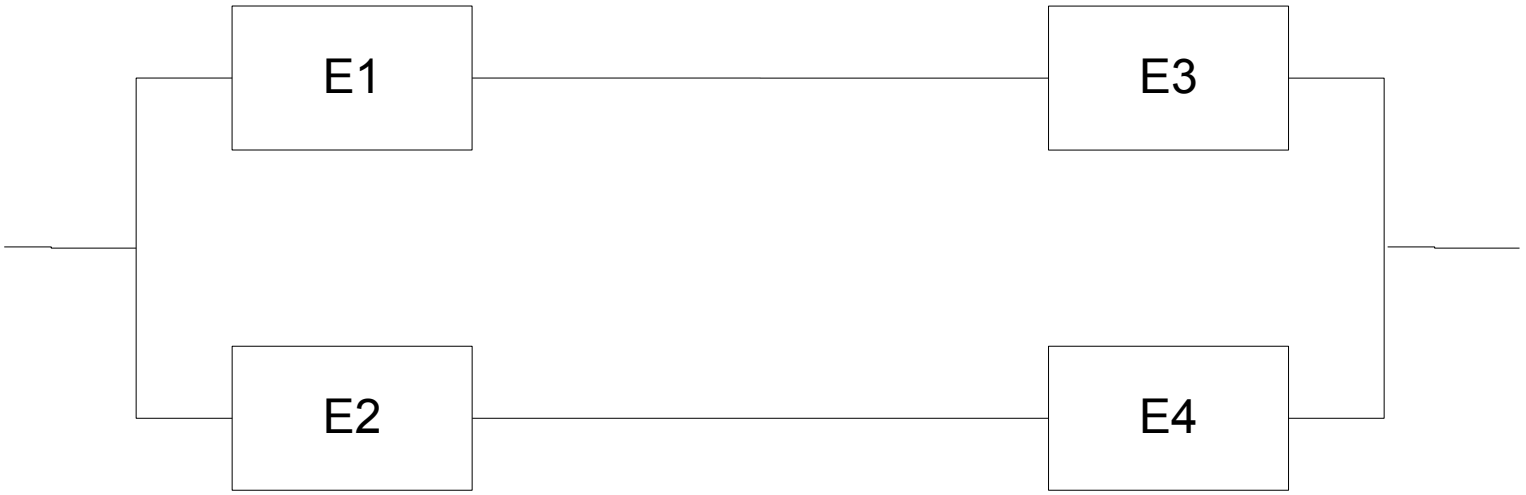
- When C is operational the system remain operational with E_1 and E_4 failed, or E_2 and E_3 failed

Working component



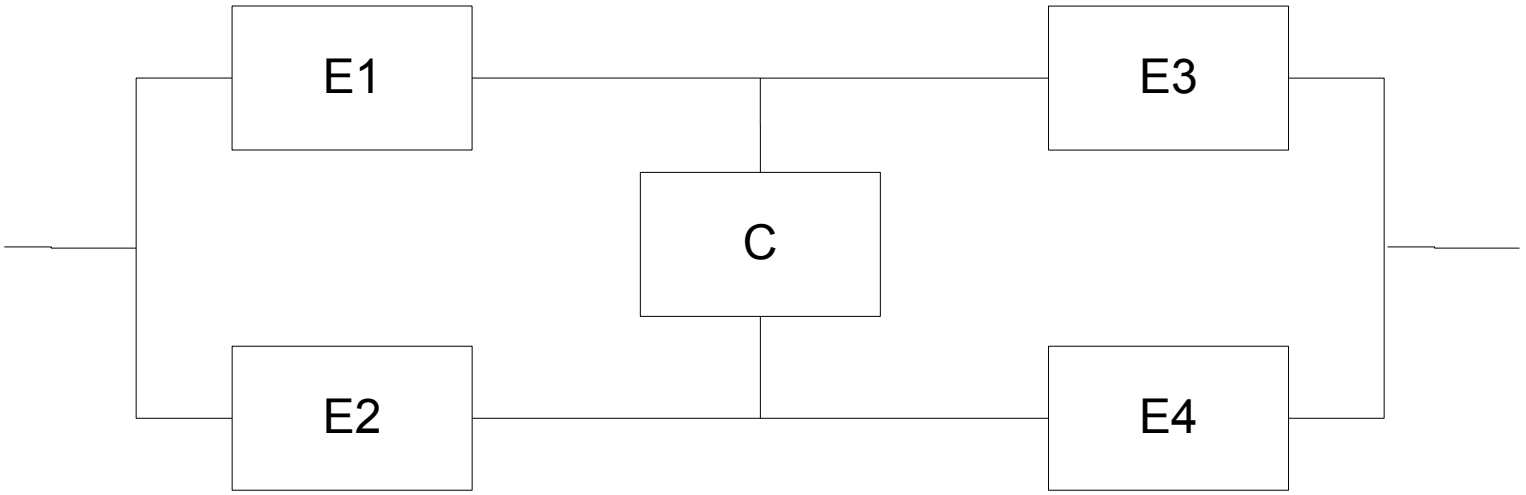
$$R_W = R_S(t \mid X_C > t) = (R_1(t) + R_2(t) - R_1(t)R_2(t)) \cdot \\ \cdot (R_3(t) + R_4(t) - R_3(t)R_4(t))$$

Failed component



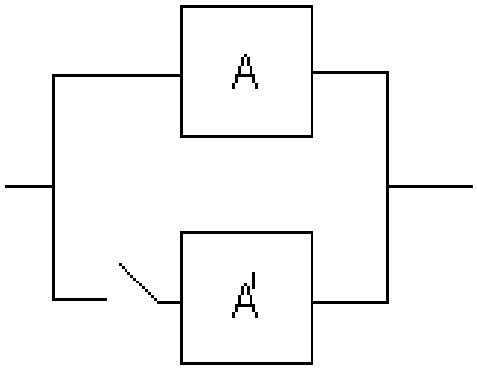
$$R_F = R_S(t|X_C \leqslant t) = R_1(t)R_3(t) + R_2(t)R_4(t) - \\ - R_1(t)R_2(t)R_3(t)R_4(t)$$

System reliability



$$R_S(t) = R_C(t)\,R_W(t) + (1 - R_C(t))\,R_F(t)$$

S*tand-by* redundancy



- A is the main component
- A' is in stand-by mode
- When A fails A' is turned on (automatically o manually)

Stand-by redundancy

- The components are statistically **dependent**
- The system continuously works till time t if:
  a) *A* correctly operates till *t*
  b) *A* failed at time *x* (in *[0, t[*) and *A'* correctly operated from *x* till *t*

Stand-by redundancy (cont.)

- Case a)

$$R_a(t) = R_A(t)$$

- Case b)

$$R_b = \int_0^t R_{A'}(t-x) f_A(x)\, dx$$

$$R_S(t) = R_a(t) + R_b(t)$$

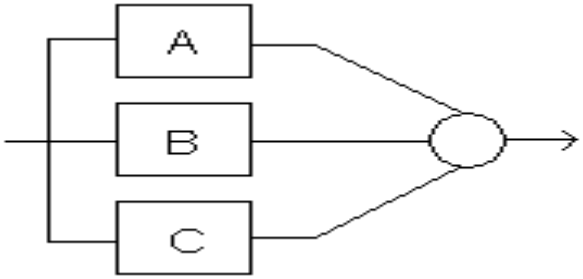
An example

- $R_A(t)=\exp(-\lambda_A t)$, $R_B(t)=\exp(-\lambda_B t)$

$$R_S(t)=\frac{\lambda_A}{\lambda_A-\lambda_B}e^{-\lambda_B t}-\frac{\lambda_B}{\lambda_A-\lambda_B}e^{-\lambda_A t}$$

$$MTTF=\frac{1}{\lambda_A}+\frac{1}{\lambda_B}$$

k out of n system



- The system is operational when half plus one of the components at least are operational
- Probability that *i* components over *n* are operational

$$P[i:n]=\binom{n}{i}R^i(1-R)^{n-i} \qquad \binom{n}{i}=\frac{n!}{i!(n-i)!}$$

k out of n system

- The system works when *i* is greater or equal to *k*:
  - **(k:n): [*k* components out of *n* run, where *k* is greater or equal to *n/2*]**

$$R_{k:n} = \Pr\{k:n\} + \Pr\{k+1:n\} + \ldots + \Pr\{n:n\} =$$

$$= \sum_{i=k}^{n} \Pr\{i:n\} = \sum_{i=k}^{n} \binom{n}{i} R^i (1-R)^{n-i}$$

2 out of 3 system

- Let us consider (k:n) = (2:3)
- All the sub-systems are equal (from the reliability point of view):

$$R_{2:3} = \binom{3}{2} \cdot R^2 \cdot (1-R) + \binom{3}{3} \cdot R^3 \cdot (1-R)^0 =$$
$$= 3(R^2 - R^3) + R^3 = 3 \cdot R^2 - 2 \cdot R^3$$

Common cause failure

- An event that simultaneously involve all the components impairing them
  - Natural causes
  - Accidents: blackout, fire
  - Executive deficiency
- Project diversification