Fault Tree Analysis

A. Palos Teixeira and C. Guedes Soares

IST

Fault Tree Analysis (FTA)

- FTA is a top-down process by which an undesirable event (failure in a project objective or a critical failure that can affect the project), referred to as the top event, is logically decomposed into possible causes in increasing detail to determine the causes or combinations of causes of the top event.
- FTA can yield both **qualitative and quantitative** information about the system under study.
- **Qualitative information** may include failure paths, root causes, and weak areas of the system/project.
- **Quantitative analysis** of a fault tree gives a probabilistic estimation of the top event

FTA Process

1. **Define the system**. The interactions between the system and neighbors, including the human interface, should be fully analyzed to take account of all potential failure causes in the FTA.
2. Understand the **functional relationships** between subsystems and components.
3. **Identify the top-level** fault events of the system, i.e a failure in a project objective or a critical failure that can affect the project objective
4. Construct a fault tree for the selected top event using **event and logic symbols**
5. Identify all single failures and prioritize cut sets by the likelihood of occurrence.

FTA Process

6. If **quantitative** information is needed, **calculate the probability of the top event**
7. Determine whether corrective actions are required. If necessary, develop measures to eradicate fault paths or to minimize the probability of fault occurrence.
8. Document the analysis and then follow up to ensure that the corrective actions proposed have been implemented. Update the analysis whenever a design change takes place.

FTA events and logic symbols

A fault tree is a graphical representation of logical relationships between failure events. Thus, a fault tree may be viewed as a system of event and logic symbols.

Symbol	Gate Name	Causal Relation
	AND Gate	Output event occurs if all input events occur simultaneously
	OR Gate	Output event occurs if only one of the input events occurs.
	Exclusive OR Gate	Output event occurs if one, but not both, of the input events occur.

FTA events and logic symbols

symbol	Gate Name	Causal Relation
m *n inputs*	*m* Out of *n* gate VOTING gate m/n	Output event occurs if at least m of n input events occur.
	Inhibit gate	Input procedures output when conditional event occurs
	Basic Event	Basic Event or failure
	Undeveloped event	Causes are not developed
	Event	Event that can occur normally
	Transfer symbol	Represents an event which comes from another lower-order fault tree or which is to be transferred to a higher-order tree

FTA events and logic symbols

Event symbols

Circle: a basic event that requires no further development. It represents the type of events at the lowest level and thus indicates the termination of tree ramification. Reliability information of the events should be available for quantitative analysis of a fault tree.

Rectangle: an intermediate event that can be developed further. It denotes an event that results from a combination of more basic events through logic gates.

Diamond: an undeveloped event that is not developed further either because it is of insufficient consequence or because information necessary for further development is unavailable.

Triangle: a symbol indicating that the tree is developed further elsewhere (e.g., on another page).

FTA events and logic symbols

Logic symbols

graphically represent the gates used to interconnect the lowlevel events that contribute to the top-level event according to their causal relations. A gate may have one or more input events, but only one output event.

AND gate - An output event is produced if all the input events occur simultaneously.

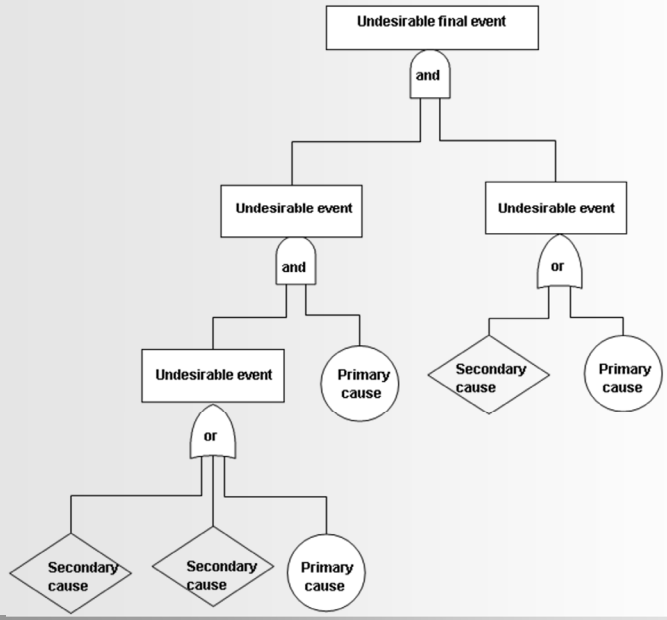
OR gate. An output event is produced if any one or more of the input events occurs.

INHIBIT gate. Input produces output only when a certain condition is satisfied. An INHIBIT gate is a special type of AND gate.

EXCLUSIVE OR gate. Input events cause an output event if only one of the input events occurs. The output event will not occur if more than one input event occurs. This gate can be replaced with the combination of AND gates and OR gates.

VOTING gate. Input events produce an output event if at least k of n inputevents occur.

FTA events and logic symbols

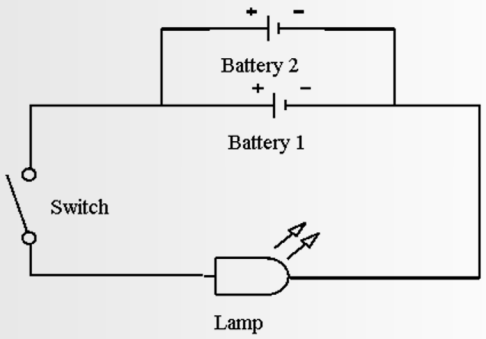


Example: FT

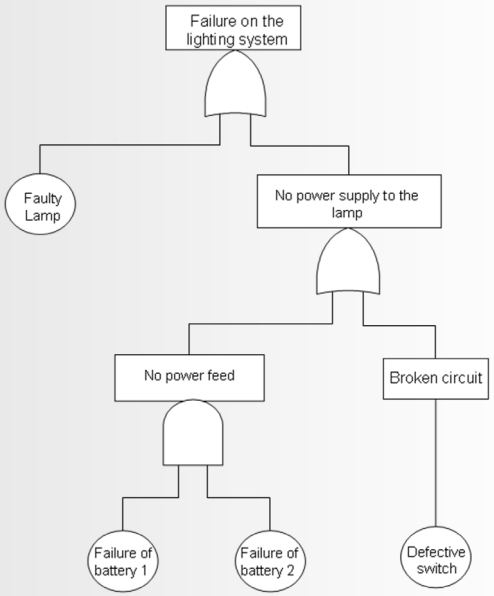
The system represented in the figure illustrates the operation of a lamp fed by two batteries. In order to have energy in the circuit it is enough that one of the batteries works.

Build the fault tree for the event:

" Failure of the lighting system "

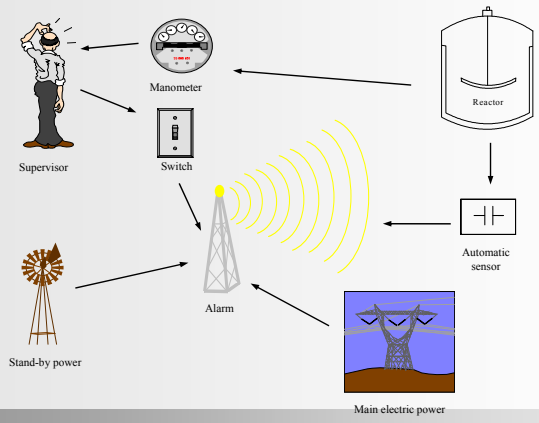


Example: FT

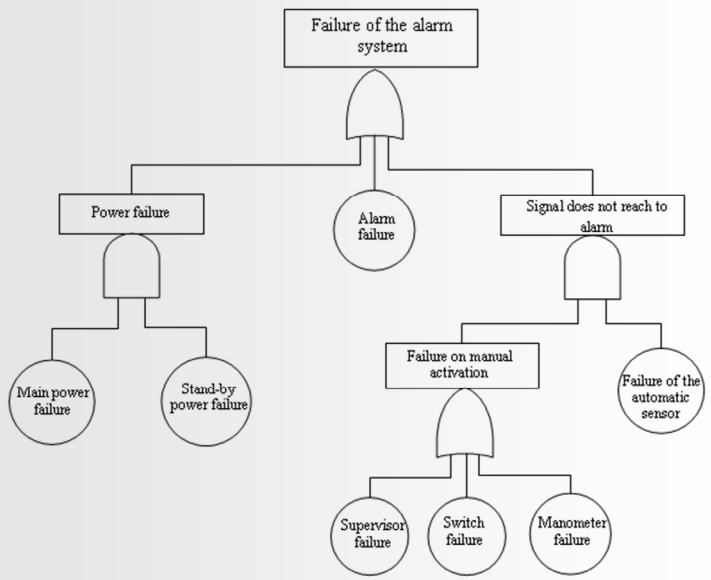


Example: FTA- Over pressure alarme

In the figure bellow a system of alarm of pressure excess in a reactor of a productive system is presented . When the pressure in the reactor reaches a value above the acceptable an alarm is activated manually by the supervisor or automatically for the automatic sensor. The alarm is fed by a line of main energy or, in case of general energy failure, for a stand-by power generator.



Example: FT



Exercise: Offshore gas production installation

Consider the process on an offshore gas production installation. Gas from the various wells is collected in a wellhead manifold and led into two identical process trains. The gas from the process trains is then collected in a compressor manifold and led to the gas pipeline via compressors.

On the inlet pipeline, there are installed two process shutdown (PSD) valves, PSD1 and PSD2 in series. The valves are fail-safe close and are held open by hydraulic pressure.

When activated, the pressure sensors will provide signal to PLC to close the both process shutdown valves PSD1 and PSD2. The PLC employs a 1-out-of-2 voting logic.

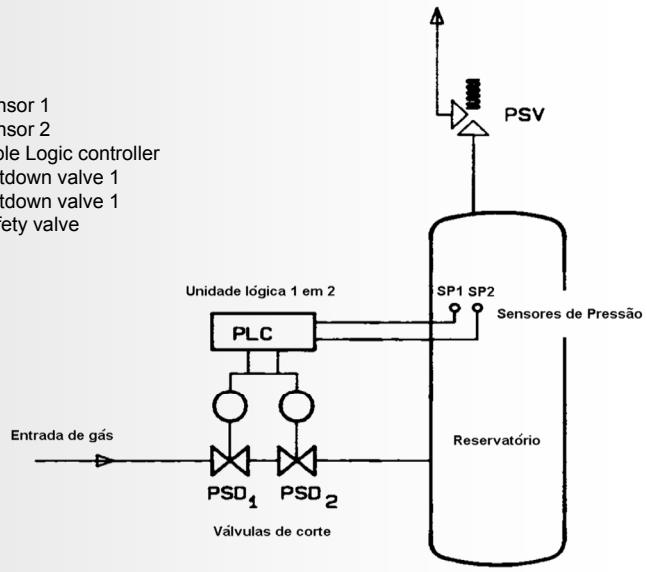
This means that the logical unit sends a signal to close the two valves, PSD1 and PSD2, if at **least one of the sensors** detect that the maximum pressure in the separator was exceeded.

A pressure safety valve PSV is installed to relieve the pressure in the tank in case the pressure increases beyong a specified pressure p.

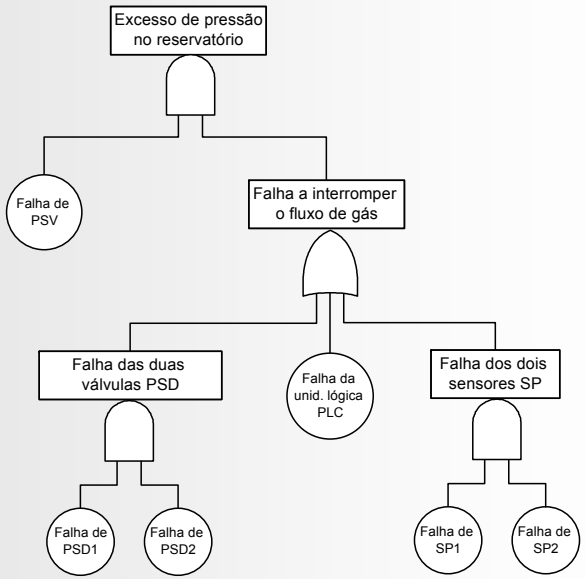
Construct a faul tree where the TOP event is: “Overpressure in the tank”

Example: FT

SP1 - Pressure sensor 1
SP2 - Pressure sensor 2
PLC - Programmable Logic controller
PSD1 - Process shutdown valve 1
PSD2 - Process shutdown valve 1
PSV - Pressure safety valve



Example: FT



Qualitative Analysis of Fault Trees

Minimal cut and path sets

Minimal Cuts and Minimal Paths

Cut Sets

A cut set is defined by:

1) a set of basic events.
2) the top event occurs when all the basic events occur in the cut set.

Minimal Cut Sets

A minimal cut set is defined by:

1) It is a cut set.
2) It is no longer a cut set whenever an event is removed from the set.

The minimal cut set is a necessary and sufficient set of basic events that can cause the top event.

A minimal cut set consisting of a single event is dangerous and should be eliminated by design change

Minimal Cuts and Minimal Paths

Path Sets

A path set is defined by:

1) It is a set of basic events.
2) Top event does not occur when none of the basic events in the set occurs.

Minimal Path Sets

A minimal path set is defined by:

1) It is a path set.
2) It is no longer a path set whenever an event is removed from the set.

The minimal path set is a necessary and sufficient set of basic events that ensure the nonoccurrence of the top event when none of the basic events occurs in the set.

Minimal Cuts and Minimal Paths

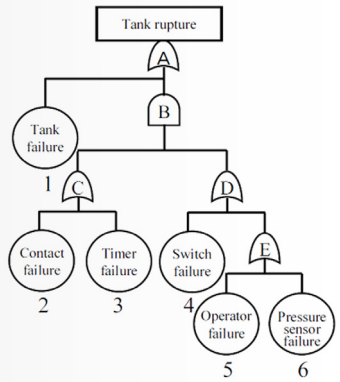
EX:

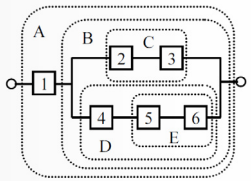
Minimal Cut Sets

$\{1\}, \{2,4\}, \{2,5\}, \{2,6\}, \{3,4\}, \{3,5\}, \{3,6\}$

Minimal Path Sets

$\{1,2,3\}, \{1,4,5,6\}$





Quantitative Analysis of Fault Trees

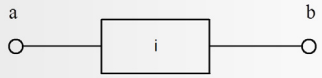
Probabilistic estimation of the top event

Reliability Block Diagrams

Reliability Block Diagrams

A Reliability block diagram or reliability diagram is not more than a combination of basic components that describes the function of the system.

Each component of the system is represented by a rectangle. When the component works we say that the connection is established among the points the *a* and *b*.

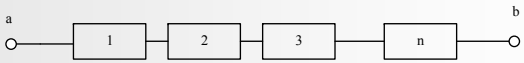


If the system is constituted by n components it is said that the system works if the connection is established among the points *a* and *b*.

Systems of Components

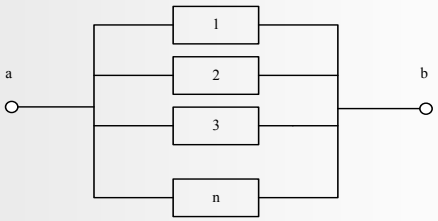
Series configuration

The system works if and only if all the components work.

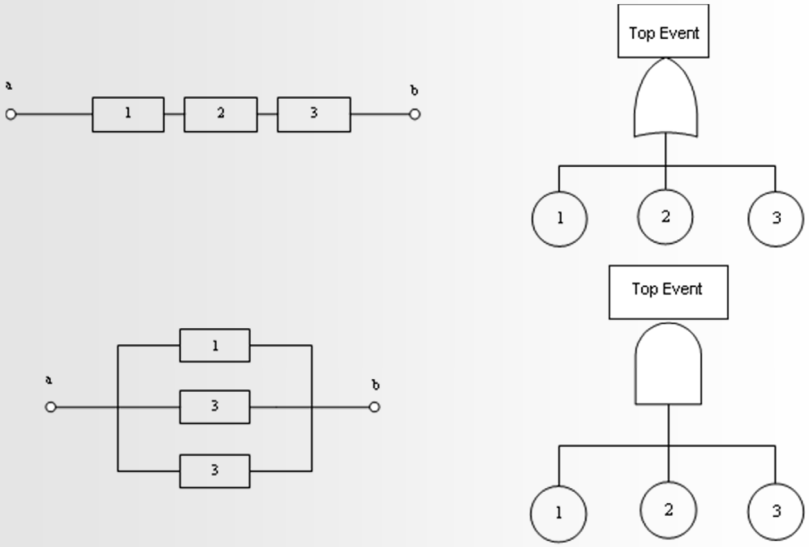


Parallel configuration

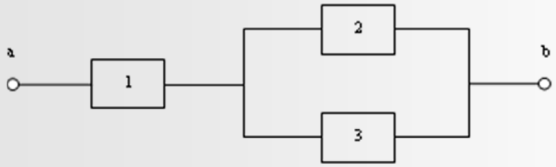
The system works if at least one of its components works.

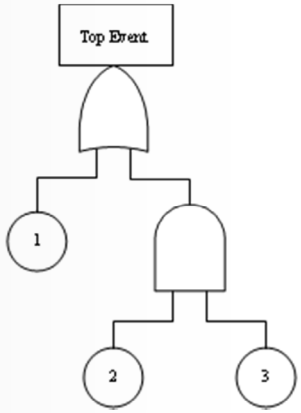


Reliability Diagrams versus Fault Trees

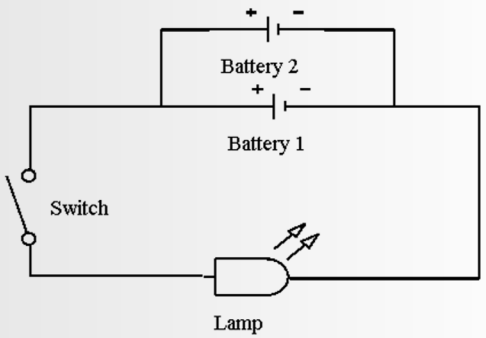


Reliability Diagrams versus Fault Trees (cont.)

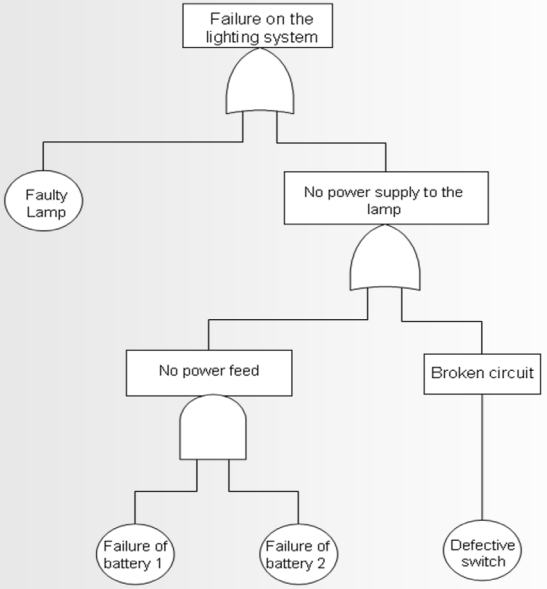


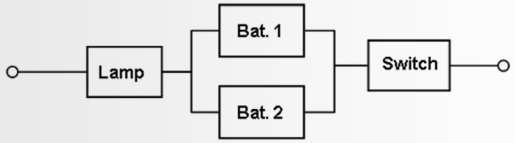


Example: Lighting system

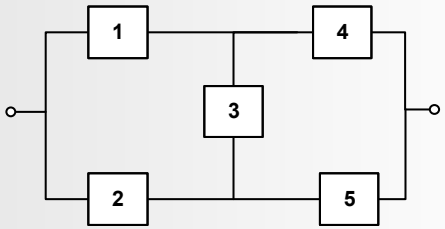


Example: Lighting system

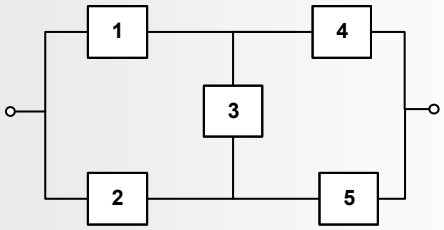




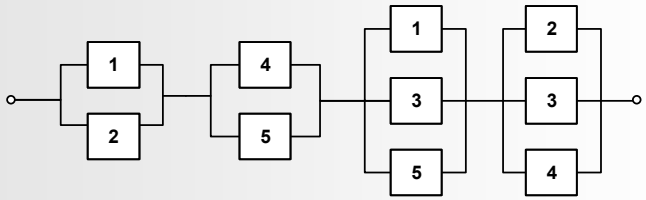
Example of aplication: Bridge System



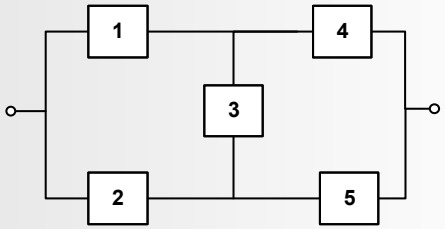
Example of aplication: Bridge System



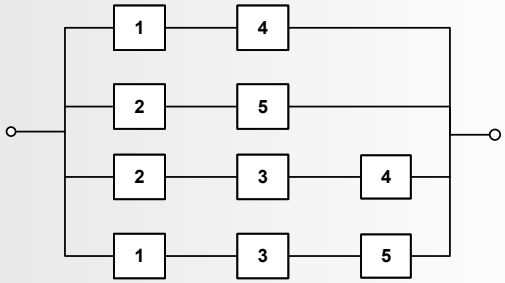
Reliability block diagram considering the cut sets:



Example of aplication: Bridge System



Reliability block diagram considering the path sets:



Probability of failure of systems of components

Basic probability concepts

Probability axioms

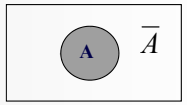
$P(\varnothing) = 0$

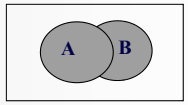
$P(A^c) = 1 - P(A)$

Se $A \subset B$ então $P(A) \leq P(B)$

$0 \leq P(A) \leq 1$

$P(A \cup B) = P(A) + P(B) - P(A \cap B)$





Conditional probability

Def: The conditional probability of the event A given that the event B has occurred is written as $P(A/B) = \frac{P(A \cap B)}{P(B)}$

Def: The event A is said to be statistically independent of the event B

$P(A) = P(A/B)$

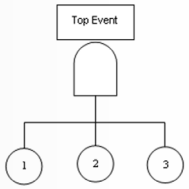
Then $P(A \cap B) = P(A)\,P(B)$

Calculation of the probability of failure of systems of components

Parallel components

In order to the system fail it is necessary that all components fail.

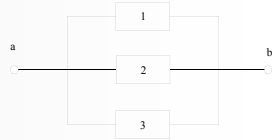
The probability of failure of the system is given by:



$$P[System\ fails] = P[1\ fails \cap 2\ fails \cap 3\ fails]$$

$$P_{fs} = P_{f1} \cdot P_{f2} \cdot P_{f3}$$

or in a general way for *n* elements in parallel,

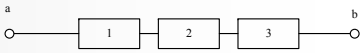


$$P_{fs} = \prod_{i=1}^{n} P_{fi}$$

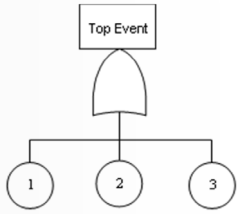
where it was assumed that there was no correlation between the basic elements and therefore the probability of simultaneous occurrence of failure of all components is equal to the product of the probabilities of each component.

Calculation of the probability of failure of systems of components

Series of components



There is failure of the system when one of the components fails or the system works if all its components work:



$$P[System\ works] = P[1\ works \cap 2\ works \cap 3\ works]$$

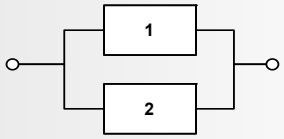
$$R_s = R_1 \cdot R_2 \cdot R_3$$

Or in a general way for *n* elements in series,

$$R_s = \prod_{i=1}^{n} R_i \qquad P_f = 1 - R_s$$

where where it was assumed that there was no correlation between the basic elements.

2 Components in Parallel



$$P_f = P_{f1} \cdot P_{f2}$$

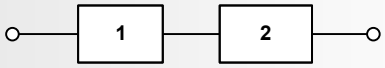
$$R = 1 - P_f$$

$$1 - R_s = (1 - R_1).(1 - R_2)$$

$$\Downarrow$$

$$R_s = P(Comp\ 1\ work \cup Comp\ 2\ work)$$

2 components in Series



$$R_s = R_1 . R_2$$

$$P_f = 1 - R$$

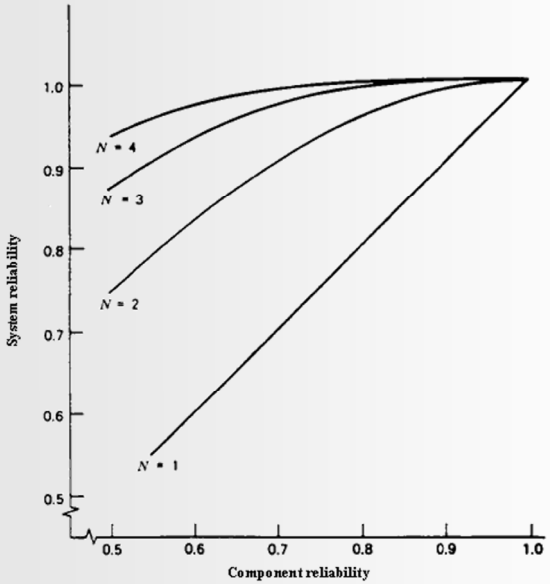
$$1 - P_f = (1 - P_{f1}).(1 - P_{f2})$$

$$P_f = P_{f1} + P_{f2} - P_{f1} \cdot P_{f2}$$

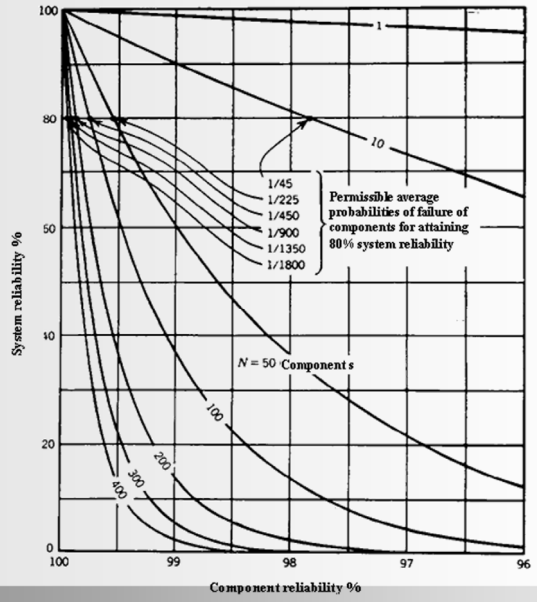
$$\Downarrow$$

$$P_f = P(Comp.\,1\,fail \cup Comp.\,2\,fail)$$

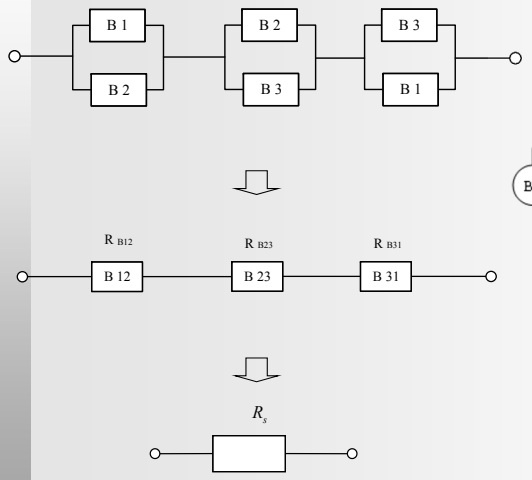
System reliability with parallel components

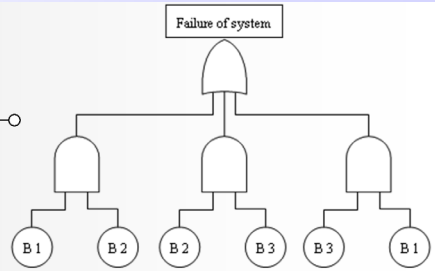


System reliability with series of components



Reliability of combined systems





$$P_{f\,B12} = P_{f\,B1} . P_{f\,B2} \qquad R_{B12} = 1 - P_{f\,B12}$$

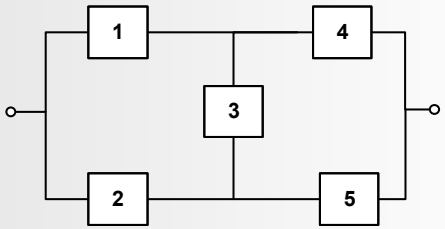
$$P_{f\,B23} = P_{f\,B2} . P_{f\,B3} \qquad R_{B23} = 1 - P_{f\,B23}$$

$$P_{f\,B31} = P_{f\,B3} . P_{f\,B1} \qquad R_{B31} = 1 - P_{f\,B31}$$

$$R_s = R_{B12} . R_{B23} . R_{B31}$$

$$P_{fs} = 1 - R_s$$

Example of aplication: Bridge System

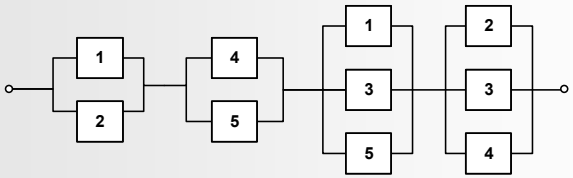


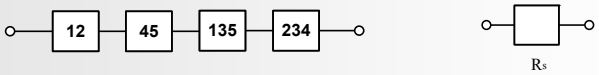
R (minimal cut sets) $\leq R_s \leq$ R (path sets)

Reliability calculation of the bridge system

By the cut sets:

$R_i = 0.800$ (I=1 a 5)





$R_{12}=1-P_{f1}P_{f2} = 1- 0.2 \times 0.2 = 0.960$

$R_{45}=1-P_{f4}P_{f5} = 1- 0.2 \times 0.2 = 0.960$

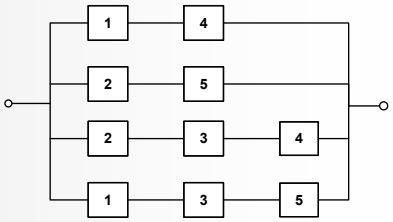
$R_{135}=1-P_{f1}P_{f3}P_{f5}= 1- 0.2 \times 0.2 \times 0.2 = 0.992$

$R_{234}=1-P_{f2}P_{f3}P_{f4}= 1- 0.2 \times 0.2 \times 0.2 = 0.992$

$R_s= R_{12} \times R_{45} \times R_{135} \times R_{234} = 0.960 \times 0.960 \times 0.992 \times 0.992 = 0.907$

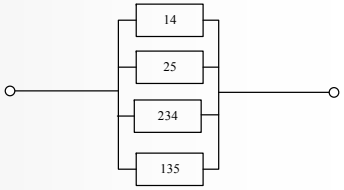
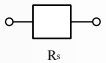
Reliability calculation of the bridge system

By the path sets:



$R_{14}= R_1 \times R_4 = 0.8 \times 0.8 = 0.64$
$R_{25}= R_2 \times R_5 = 0.8 \times 0.8 = 0.64$
$R_{234}= R_2 \times R_3 \times R_4 = 0.8 \times 0.8 \times 0.8 = 0.512$
$R_{135}= R_1 \times R_3 \times R_5 = 0.8 \times 0.8 \times 0.8 = 0.512$

$P_{f\ 14}=1-0.64 = 0.36$
$P_{f\ 25}=1-0.64 = 0.36$
$P_{f\ 234}=1-0.512 = = 0.488$
$P_{f\ 135}=1-0.512 = = 0.488$



$R_s= 1-P_{f142}P_{f3}P_{f4}= 1- 0.36 \times 0.36 \times 0.488 \times 0.488 = 0.969$