COMMON CAUSE FAILURES

With the term "Common Causes of Failure" (CCF) are identified events capable of inducing a fault in all components or systems affected.

For example:
- **Functional dependency**. Loss of a common functional input to more components (eg. Power supply, control signal, etc.). This type of dependency can be detected by the logic analysis of tree fault tree or event tree by which they make clear all common events relating to some branches of the tree;

- **External event.** All systems are subject to the same external anomalous event (eg. Flood, fire, etc.), capable of put simultaneously out of service;

- **Causes linked to the supplier.** For example, common defects in more equipment of the same equipment originating from the same vendor;

- **Causes linked to factors affecting operating behavior.** All components are subjected to vibration, high temperatures, etc., ie are subject to maintenance by the same team with the same procedures (therefore potentially subject to the same errors).

Only in some special cases i's possible to study these common effects (extremely important because they can put out of service protective chains otherwise considered redundant) using the direct analysis of the fault tree or of the event tree.
In most cases it is only possible to estimate the influence of these effects by resorting to an approximate quantification of the dependency.

Qualitative analysis

The method consists in showing, with qualitative arguments, that in the project plant have been taken into account adequate measures against the occurrence of CCF.
For example:

- Quality Assurance procedures to avoid mistakes in the project, in the construction and installation;

- tests where are subjected components and systems before commissioning of system at the operational level, to detect possible errors during installation or dimensioning;
- diversification of suppliers, types of components and the materials, to prevent malfunctions due to production errors or defects in the materials;
- A particular care to isolate topologically the different components, to avoid special environmental conditions or incidental act that affect in the same way on components belonging to different redundant channels;
- The use of the Quality Assurance in the maintenance procedures, in order to avoid that an operator not notice the the incorrect positions of switches or valves after the interventions, etc.

Possible identification of CCF

Identified components whose simultaneous failure could result in the Top Event, it is possible to list hese events in a matrix where rows represent the possible categories of common cause failure. Eg .:

Component→	**A**	**B**	**C**
Category↓			
Focalization	L101	L104	L101
Manufacturer	F1	F1	F2
Vibrations	V1	-	-
Temperature	-	T100	T100
Maintenance, ecc.	M1	-	M1

Assigning codes to the different effects it is possible to see which components are potentially subject to common causes (for example: A and C are placed in the same area and L101 are subject to maintenance by the same procedure M1; A and B are manufactured from the same supplier F1; B and C are subject to the same temperature T100.

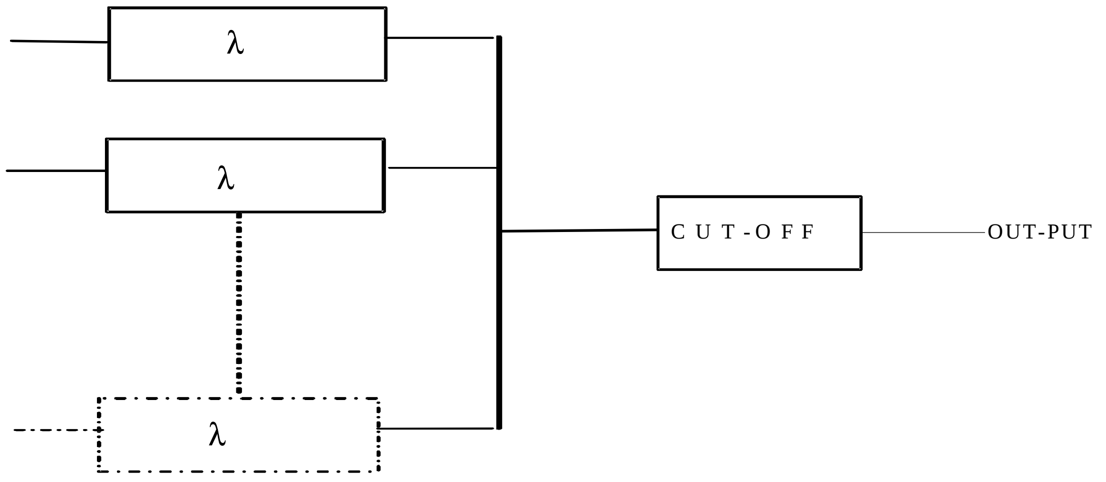
Once identify potential classes of common causes, may occur that are possible determine measures able to avoid these effects and we can estimate the influence of the effects that can not be removed.

- Quantification of CCF

A number of methods have been proposed to quantify the effect of the common causes failure.
For external events quantifiable (eg. probability of flooding,of fire, of loss of a service or por a common input) is possible to introduce in the event tree the related probability.
For factors not directly quantifiable (eg. manufacturing defects, sensitivity to the same factors to environmental parameters, etc.), for which there is no information from other sources, is possible to make an estimate of the effect. Below are described two very simple methods able to provide an estimate of the effect, based of the influence and the experience of analyst's judgment.

A. Method of cut-off

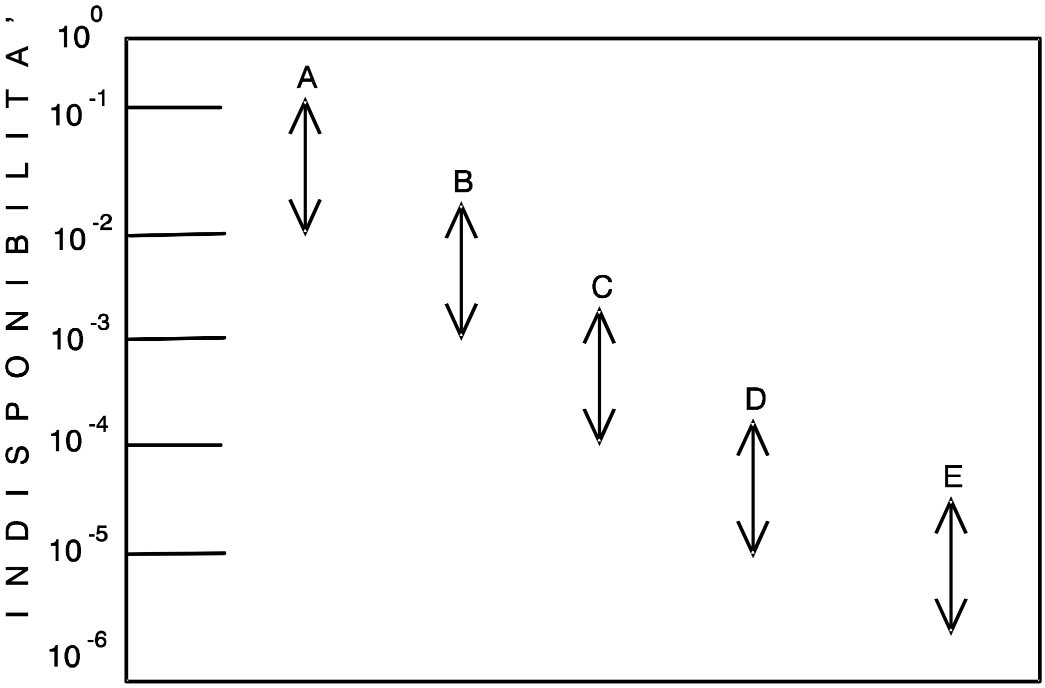
The experience, and common sense, suggest the observation that the process of increasing the redundancy, to improve the reliability, must have a limit; it is impossible to achieve an absolute degree of safety. On this principle is based the the cut-off rule(Fig. XX), that ultimately is equivalent to the application of a criterion of reasonableness and common sense: for each level of quality, for a safety system , there is a minimum value of unavailability that can be reached (cut-off), however difficult to establish.
The application of the rule of the cut-off to a specific project may be carried out only through the use of engineering judgment and of the few data available from past experience, but it not always directly transferable to new type plants.



IDIPENDENT FOULT DEPENDENT FOULT

Fig. XX - Cut-Off Method

A user guide of the cut-off method is given in Fig. XY, which is based on the experience accumulated by the Safety and Reliability Directorate of the UKAEA, through the analysis of data coming from plants, both nuclear and industrial.



TIPY OF SYSTEM

System Type:

A simple, single system

B simple, redundant system

C partially diversified system

D completely diversified system

E two separate systems, each diversified

Fig. XY - Guide to the possible intervals of unavailability of safety systems.

B. The Beta Coefficient Method

The cut-off technique does not attempt to represent the factors which determine the dependencies. A further step in the development of models, is to try to describe how some important characteristic influencing the contribution of the dependencies failures in relation of the overall system reliability. The model, called "Coefficient β", assumes that the failure rate of the individual components as a significant feature of the project. Assuming that the total failure rate (λ) for each unit (component/system redundant) is composed of the contributions of the dependent faults and the independent ones:

$\lambda = \lambda_i + \lambda_c$

where:

– λ_i is the failure rate for independent failures

– λ_C is the failure rate for dependent failures

The factor β is defined as:

$\beta = \lambda c/(\lambda c+\lambda i)=\lambda c/\lambda$

and it represents the relative contribution of dependent failure to component/system failures (see Fig. YY).

The reliability of the system can be expressed in terms of l and b. The crucial assumption is that the factor b is obtained for conditions of existing plants is still valid for the design of new installations. Data from operating experience can be used to calculate the values of l and b. From the experience of American nuclear reactors, for example, it has been obtained for the pumps a value of β = 0.15; for other types of components as have been used values of β = 0.01 - 0.1. The data to be used include all of the examples of multiple defects, regardless of whether or not these are followed by failure of the system. This use of the data is done due the scarcity of the same data, but also because the model does not distinguish between different levels of redundancy.

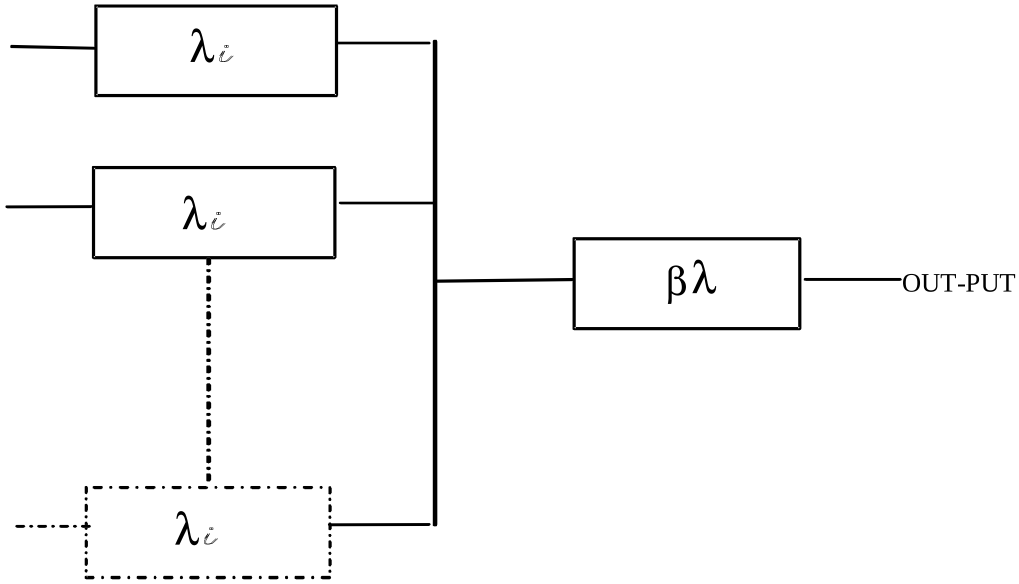


Fig.YY - β Method