cahiers techniques 144

introduction to dependability design

P. Bonnefoi

Pascal Bonnefoi earned his engineering degree ESE in 1985. After working for a year in Operational Research for the French Navy he started his work as a reliability analyst for Merlin Gerin in 1986, in the Reliability studies for which he developed a series of special software packages. He aslo taught courses in this field in the industrial and academic worlds. He is presently working as a software engineer for HANDEL, a Merlin Gerin subsidiary.

MERLIN GERIN
service information
38050 Grenoble Cedex
France
tél. : 76.57.60.60

E/CT 144
December 1990

MERLIN GERIN
la maîtrise de l'énergie électrique
GROUPE SCHNEIDER

introduction to dependability design

P. Bonnefoi

Equipment failures, unavailability of a power supply, stoppage of automated equipment and accidents are quickly becoming unacceptable events, be it to the ordinary citizen or industrial manufacturers.
Dependability and its components: reliability, maintainability, availability and safety, have become a science that no designer can afford to ignore.
This technical report presents the basic concepts and an explanation of its basic computational methods.
Some examples and several numerical values are given to complement the formulas and references to the various computer tools usually applied in this field .

Table of contents

1. importance of dependability

Prehistoric men had to depend on their arms for survival. Modern man is surrounded by ever more sophisticated tools and systems on which he depends for safety, efficiency and comfort.

Ordinary citizen are specially concerned in everyday life by:
- the reliability of the TV set,
- the availability of the mains supply,
- the maintainability of freezers and cars,
- the safety of their boiler valves.

Bankers and, in general, service industries give a lot of weight to:
- computer reliability,
- availability of heating,
- maintainability of elevators,
- fire related safety.

In competitive industries it is not possible to tolerate production losses. This is even more so for complex industrial processes. In these cases one vies to obtain the best:
- reliability of command and control systems,
- availability of machine tools,
- maintainability of production tools,
- personnel and invested capital safety.

These characteristics, known under the general term of DEPENDABILITY, are related to the concept of reliance, (to depend upon something). They are quantified in relation to a goal, they are computed in terms of a probability and are obtained by the choice of an architecture and its components. They can be verified by suitable tests or by experience.

For over 20 years Merlin Gerin has pioneered work in the DEPENDABILITY field: in the past, with its contribution to the design of nuclear power plants or the high availability of power supplies used at the launching site of the ARIANE space program, nowadays, by its design of products and systems used worldwide.

2. dependability characteristics

reliability

Light bulbs are used by everyone: individuals, bankers and industrial workers. When turned on, a light bulb is expected to work until turned off. Its reliability is the probability that it works until time *t* and it is a measure of the light bulb's aptitude to function correctly.

Definition:
The reliability of an item is the probability that this item will be able to perform the function it was designed to accomplish under given conditions during a time interval (t_1,t_2); it is written $R(t_1,t_2)$.
This definition follows the one given by the IEC (International Electrotechnical Commission)International Electrotechnical Vocabulary, Chapter 191. There are certain basic concepts used by this definition which must be detailed:

Function: the reliability is a characteristic assigned to the system's function. Knowledge of its hardware architecture is usually not enough. Functional analysis methods must be used to determine the reliability.

Conditions: the environment has a fundamental role in reliability. This is also true for the operating conditions. Hardware aspects are clearly insufficient.

Time interval: we wish to emphasize an interval of time as opposed to a specific instant. Initially, the system is supposed to work. The problem is to determine for how long. In general $t_1=0$ and it is possible to write R(t) for the reliability function.

failure rate

Consider the light bulb example again. Its failure rate at time t, written as $\lambda(t)$, gives the probability that it will suddenly burn out in the interval of time $(t, t+\Delta t)$, given that it kept working until time t. Failure rates are time rates and, as such, their units are inverse time.

Mathematically, the failure rate is written as:

$$\lambda(t) = \lim_{\Delta t \Rightarrow 0} \left(\frac{1}{\Delta t} \frac{R(t) - R(t+\Delta t)}{R(t)} \right)$$

$$= \frac{-1}{R(t)} \frac{d\,R(t)}{dt} \qquad (1)$$

For a human being, the failure rate measures the probability of death occurring in the next hour:
$\lambda(20 \text{ years}) = 10^{-6}$ per hour.
If λ is represented as function of age, one obtains the curve given in figure 1.

After the high values corresponding to the infant mortality period, λ reaches the value of adult age during which it becomes constant since causes of death are mainly accidental and thus, independent of age. After 60 years old, old age causes λ to increase. Experience seems to show that many electronic components follow a similar bathtub curve, from which the same terminology is borrowed: infant mortality, useful life and wearout.

During the useful life, λ is constant and Equation (1) becomes $R(t) = \exp(-\lambda t)$. This is the **exponential** distribution and the shape of the reliability function is given in figure 2.

The exponential distribution is one among many other possibilities. Mechanical devices which are subject to wearout since the beginning of their operating life can follow other distributions, like Weibull's distribution. In this case the failure rate is time dependent. A curve illustrating the time dependency of λ is seen in figure 3, in which no plateau, as in figure 1, exists.

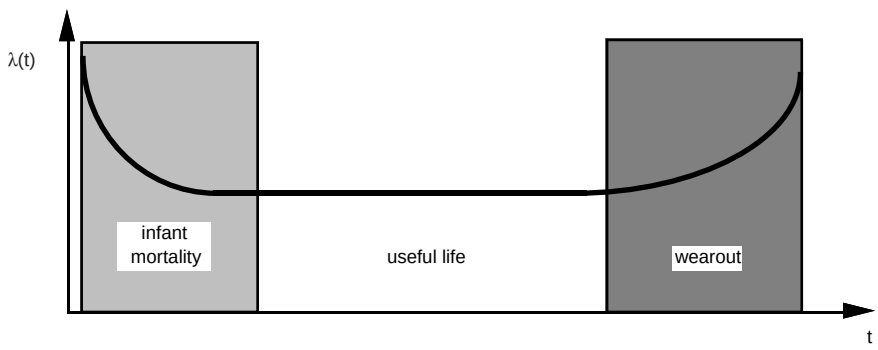


fig. 1: bathtub curve

availability

To illustrate the concept of availability consider the case of an automobile. A vehicle must start and run upon demand. Its past history may be of little relevance. The availability is a measure of its aptitude to run properly at a given instant.

Definition:
The availability of a device is the probability that this device be in such a state so as to perform the function for which it was designed under given conditions and at a given time t, under the assumption that external conditions needed are assured. We will use the symbol A(t).
This definition, inspired by the one given by the IEC, mimicks the one for the reliability. However, its time characteristics are basically different since the concept of interest is an instant of time instead of a time length. For a repairable system, functionning at time t does not necessarily imply functionning between [0,t]. This is the main difference between availability and reliability.

It is possible to plot the availability curve

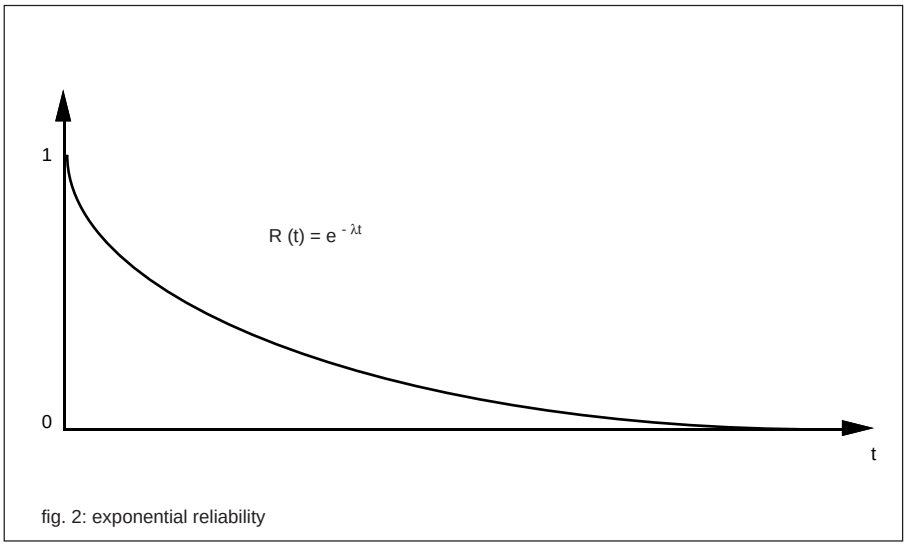


fig. 2: exponential reliability

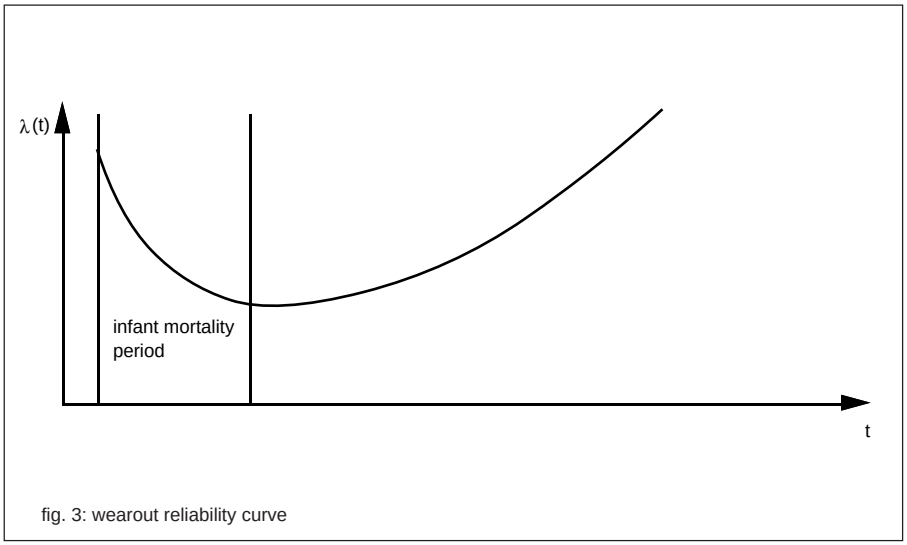


fig. 3: wearout reliability curve

as a function of time for a repairable device, having exponential times to failure and to repair, (see figure 4).
It can be seen that the availability has a limiting value which, by definition, is the asymptotic availability. This limit is reached after a certain time. The limiting reliability is always zero since, eventually, all devices will fail. (This last point is controversial when dealing with software).
Consider again the case of the automobile. Two kinds of cars can have poor availabilities: those with frequent failures and those which do not fail often but instead spend a long time in the garage for repairs. Thus, although the reliability is an important component of the availability, the aptitude to being promptly repaired is also of paramount importance: this is measured by the maintainability.

maintainability

Many designers seek top performance for their products, sometimes neglecting to consider the possibility of failure. When all the effort has been concentrated on having a functionning system, it is difficult to consider what would happen in case of failure. Still, this is a fundamental question to ask. If a system is to have high availability, it should very rarely fail but it should also be possible to quickly repair it. In this context, the repair activity must encompass all the actions leading to system restoration, including logistics. The aptitude of a system to be repaired is therefore measured by its maintainability.

Definition:
The maintainability of an item is the probability that a given active maintenance operation can be accomplished in a given time interval $[t_1,t_2]$. It is written as $M(t_1,t_2)$. This definition also follows closely that of the IEC's international vocabulary. It shows that the maintainability is related to repair in a manner similar to that of reliability and failure. The maintainability M(t) is also defined using the same hypotheses as R(t).
The repair rate $\mu(t)$ is introduced in a way analogous to the failure rate. When it can be considered constant, the implication is an exponential distribution for:

$[M(t) = \exp(-\mu t)]$.

safety

It is possible to distinguish between dangerous failures and safe ones. The difference does not lie so much in the failures themselves but in their consequences. Switching off the light signals in a train station or suddenly switching them from green to red has an impact (all trains stop) but is not functionally dangerous. The situation is totally different if the lights would accidentally turn all to green. Safety is the probability to avoid dangerous events.

The concept of safety is closely linked to that of risk which, in turn, not only depends on the probability of occurrence but also on the criticality of the event. It is possible to accept a life threatening risk (maximum criticality) if the probability of such an event is minimal. If it is just a matter of having a broken limb the acceptable probability might be greater. The curve on figure 5 illustrates the concept of acceptable risk.

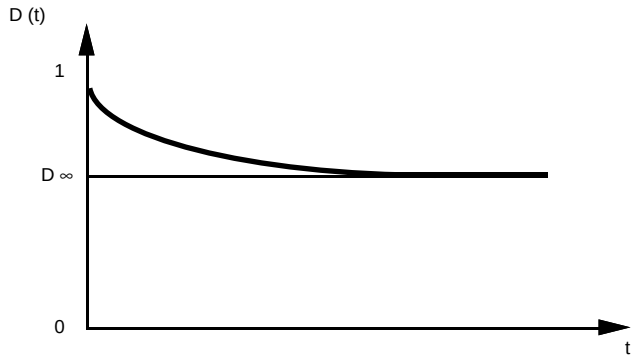


fig. 4: availability as a function of time

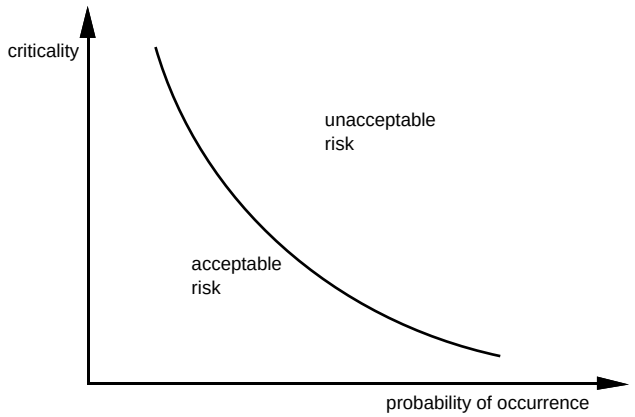


fig. 5: the level of risk is a function of both, criticality and probability of occurrence.

3. dependability characteristics interdependence

interrelated quantities

The examples given so far have shown that the concept of **dependability** is a function of four quantifiable characteristics: these are related to each other in the way shown by figure 6.
These four quantities must be considered in all dependability studies. The dependability is thus often designated in terms of the initials RAMS.
Reliability: probability that the system be failure free in the interval [0,t].
Availability: probability that the system works at time t.
Maintainability: probability that the system be repaired in the interval [0,t].
Safety: probability that a catastrophic event is avoided.

conflicting requirements

Some of the requirements of the dependability can be contradictory.

An improved maintainability can bring about some choices which degrade the reliability, (for example, the addition of components to simplify the assembly-disassembly operations). The availability is therefore a compromise between reliability and maintainability. A dependability study allows the analyst to obtain a numerical estimate of this compromise.

Similarly, safety and availability might conflict with each other.

We have noted that the safety of a system is defined as the probability to avoid a catastrophic event and is often maximum when the system is stopped. In this case, its availability is zero! Such a case arises when a bridge is closed to traffic when there is a risk of collapse. Conversely, to improve the availability of their fleet, certain airlines are known to have neglected their preventive maintenance activities thus diminishing flight safety. In order to ascertain the optimum compromise between safety and availability it is necessary to produce a scientific computation of these characteristics.

A system can be described as being in one of three states, see figure 7. In addition to the normal functionning state, two further failed states can be considered: a failsafe state and a state of dangerous failure. In order to simplify this description we are including in the failed states all modes of degraded performance, labeled “incorrect performance”.

The time spent before leaving state A is characteristic of the reliability. The time spent on state B, after a safe failure, is characteristic of the maintainability. The ratio between the time spent on state A and the total time is characteristic of the availability.
The aptitude of the system to avoid spending any time on state C is a characteristic of safety. It can be seen that state B is acceptable in terms of safety but is a source of unavailability.

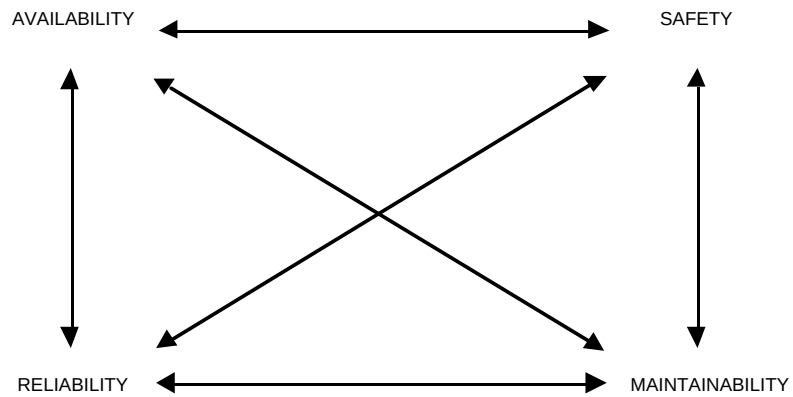


fig. 6: the components of dependability

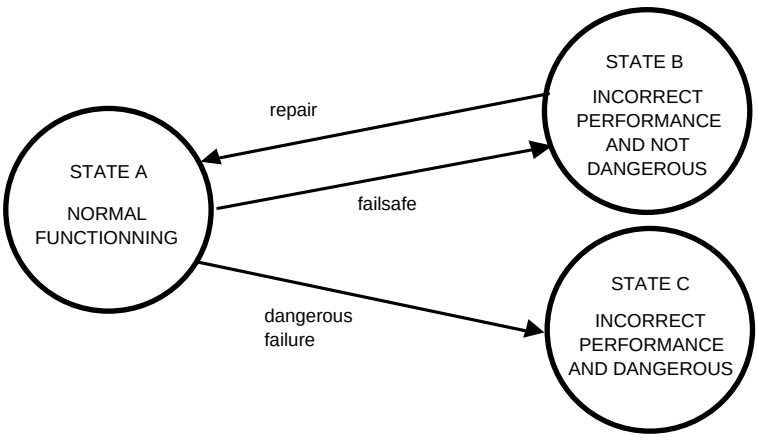


fig. 7: failsafe: availability
dangerous failure: safety

time average related quantities

In addition to the previously mentioned probabilities (reliability, availability, maintainability and safety) of occurrence of events, it is common to use mean times before the ocurrence of events in order to describe the dependability.

Mean times

It is useful to recall here the exact definition of all the mean times as they are often misunderstood. The worst example of abuse is probably the most widely known, the MTBF, which is often confused with lifetime.

On the average, in a homogenous population of items following an exponential distribution, about 2/3 of these items will have failed after a time equal to the MTBF. A single system having a constant failure rate will have a 63% chance of having failed after such a time. The definitions and relative positions of these mean times during the life of a system are given in figure 8.

MTTF or MTFF (Mean Time To First Failure):
the mean time before the occurrence of the first failure.

MTBF (Mean Time Between Failures): mean time between two consecutive failures in a repairable system.

MDT (Mean Down Time):
mean time between the instant of failure and total restoration of the system. It includes the failure detection time, the repair time and the reset time.

MTTR (Mean Time To Repair): mean time to actually restore the system to an operating condition.

MUT (Mean Up Time): mean failure free time.

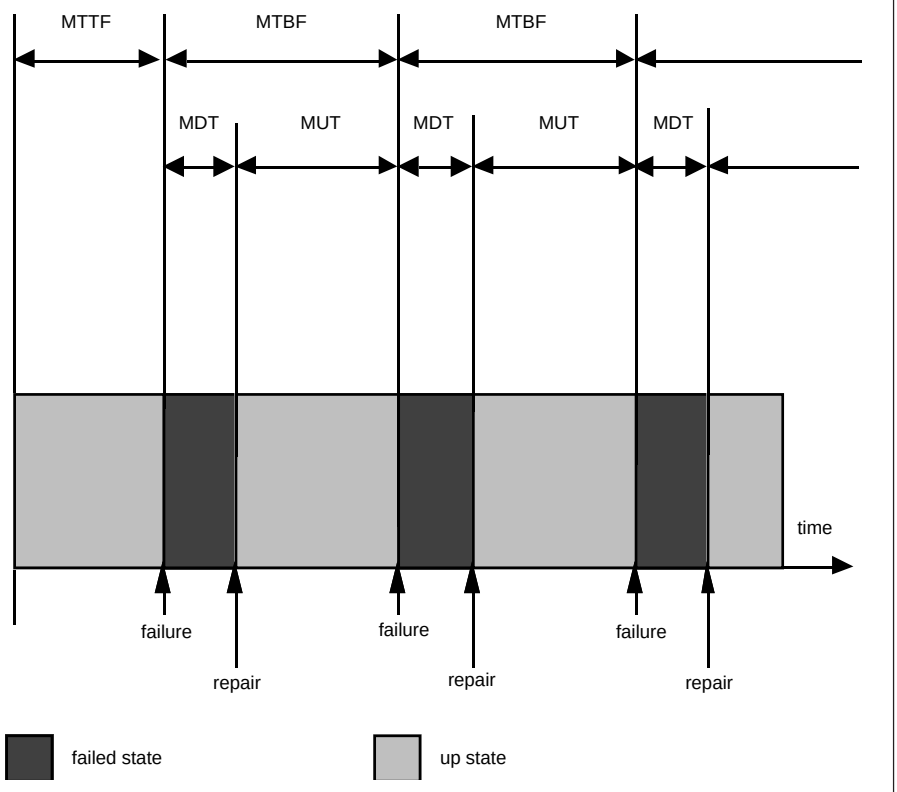


fig. 8: diagram for mean times in the case of a system with no interruptions due to preventive maintenance

Important relations and numerical values

There are many mathematical relations linking the quantities introduced thus far: For an exponential distribution with $R(t) = \exp(-\lambda t)$ one has $MTTF = 1/\lambda$. In this case, for a non repairable system, we have MTBF = MTTF (in fact, in this case, all failures are "first" failures). This explains why the classical formula used for electronic components (non repairable) is: $MTBF = 1/\lambda$.

The above formula is only valid for exponential distributions (constant failure rates) and, strictly speaking, for non repaired items although it is possible to apply it for repaired systems with very small MDTs. Analogously, when repair times obey an exponential distribution, it is possible to show that $MTTR = 1/\mu$.

One also has: MTBF = MUT + MDT. In general it is also true that MDT = MTTR, except for the logistic delay and restart times. Furthermore:

■ **asymptotic availability**

This formula illustrates the assertion given

$$A_\infty = \lim_{t \to +\infty} (A(t)) = \frac{MDT}{MDT + MUT} = \frac{MDT}{MTBF}$$

on page 3 concerning the availability (ratio of correct performance time to total time). This quantity $\frac{MUT}{MTBF}$ corresponds to the asymptotic value given in figure 4, page 4.

■ **asymptotic unavailability**

= 1 - asymptotic availability

$$U_\infty = \lim_{t \to +\infty} (1 - A(t)) = \frac{MUT}{MDT + MUT} = \frac{MUT}{MTBF}$$

The asymptotic unavailability is usually easier to express numerically than the availability: it is much easier to read 10^{-6} than 0.999999.

For exponential distributions, using the equations MUT = $1/\lambda$ and MDT = $1/\mu$ one obtains:

$$U_\infty = \frac{\lambda}{\lambda + \mu} \text{ or } A_\infty = \frac{\mu}{\lambda + \mu}$$

λ is often much smaller than μ since the repair times are much smaller than the times to failure. It is therefore possible to simplify the denominator and write:

$$U_{\infty} = \frac{\lambda}{\mu} = \lambda.MTTR$$

This last formula illustrates, in the case of exponential distributions, the compromise between reliability and maintainability which has to be optimized to improve the availability.
The table of figure 9 gives failure rates and mean times to failure for certain devices belonging to the electronic and electrotechnical fields.

It can be seen that the reliability is degraded when the complexity of the system increases. This corresponds to a well-known rule of dependability design: simplify as much as possible.

The concept of mean time is often misunderstood. For example the next two sentences have, for exponential distributions, the same meanings: "The MTTF is 100 years" and "The odds are one in 100 to observe a failure in the first year". Still, the second sentence seems more worrisome for a manufacturer selling 10 000 devices of this type per year. On the average, about 100 units will fail on the first year.

To illustrate the impact of redundancy on the unavailability, consider the national power grid. One is concerned with the deliverance of energy to the final user. The unavailability is about 10^{-3}. This corresponds to about 9 hours of downtime per year. For a computer room, having a heavily redundant system of Uninterruptible Power Supplies (UPS), it is possible to reduce this figure between 1000 and 10 000 times.

	resistances	micro-proc.	fuses and circuit-breakers, 300 ft. cables, busbars	generator	mains outages
λ(/h)	10^{-9}	10^{-6}	10^{-7} to 10^{-6}	10^{-5}	10^{-2}
MTTF	1000 centuries	100 years	100 to 1000 years	10 years	4 days

fig. 9: failure rates and mean times to failure for certain devices belonging to the electronic and electrotechnical fields

4. types of defects

The design of a system with respect to its dependability goals implies the need to identify and take into account the various possible causes of defects.
One can suggest the following classification:

physical defects

induced by **internal** causes (breakdown of a component) or **external** causes, (electromagnetic interferences, vibrations,...).

design defects

comprising hardware and software design errors.

operating errors

arising from an incorrect use of the equipment:

- hardware being used in an inappropriate environment,
- human operating or maintenance errors,
- sabotage.

The various techniques discussed in this document concern mostly physical defects. Nevertheless, human and software errors are also very important although the state of the art in these fields is not as advanced as for physical defects. Still, within the scope of this document, we feel the following elements are worth mentioning:

Software aspects

- the reliability of a piece of software in which all the inputs are exhaustively tested is equal to 1 forever. Nevertheless, this is unrealistic for real life, complex programs.
- having two redundant programs implies development by different software teams using different algorithms. This is the principle behind fault tolerant software in which a majority vote may be implemented.
- most software reliability models can be split in two major categories:
  - complexity models: based upon a measure of the complexity of the code or algorithm,
  - reliability growth models: based upon previous observed failure history.
- the quantitative evaluation of the

different models does not allow yet for a systematic study of software reliability. The best results are obtained in particular cases and for given environments (language, methods). This is the case for the SPIN (Integrated Digital Protection System) software developped by Merlin Gerin for use in nuclear power plants. Merlin Gerin is also an active participant in different working groups dealing with software reliability (see references). The Technical Paper CT 117 gives further details on this subject. The title is "Methods for developping dependability related software".

Human reliability

Qualitative approaches are predominant in this field. The efforts lie mostly in the modeling of the human operator, task classification and human errors. The most advanced studies belong to the nuclear and aerospace industries. Human behavior is known as much by simulators as by field reports. Both sources can be compared to each other. Some references exist which propose some numerical values. However, these must be used with utmost caution. According to these references it is feasible to assign an error probability depending on the nature of the activity: mechanical, procedure or cognitive action.

Some of the recent major catastrophes have shown that the human factor can have great impact, not only from the operator standpoint but also at the designer's stage. The more freedom of action is given to a human operator the more the risks are increased. This also includes management, as the Challenger Space Shuttle accident has shown: it is possible to go all the way up to the designers of the working structure of the designer's team! Many disciplines are called upon to tackle the problem of human reliability. Among them psychology and ergonomy.

5. from component to system: modeling aspects

data bases for system components

Electronics

Reliability calculations have been widely used in this field for many years. The two best known data bases are the Military Handbook 217 (version E at present) issued in the U.S. and the "Recueil de données de fiabilité", from CNET (French Telecom Center), see figure 11 for an example. Merlin Gerin participates in its updates.

These data bases allow the calculation of the failure rates of electronic components, assumed to be constant. These rates are a function of the application characteristics, environment, load, etc. The type of component is also relevant, e.g., number of gates, value of the resistance, etc. Computation is usually faster with the CNET approach but many specialized computer programs exist to implement either technique with ease.

As an example, let us take a 50 kΩ resistance used in an electronic board and used inside an electric switchboard. It is necessary to consult the table given in figure 11 in order to determine the corresponding correcting values. The environment is "au sol" (fixed, ground) and therefore, the environment corrective factor is:

$\Pi_E = 2.9$

The resistance value gives the corresponding multiplying factor:

$\Pi_R = 1$

This resistance is taken as being "non qualified" which gives the multiplying quality factor

$\Pi_Q = 7.5$

The load factor ρ is a characteristic of the application, as opposed to the other factors which are characteristic of the component itself. If the load factor is 0.7 and the environmental temperature for the board is 90°C, the diagram gives

$\lambda_b = 15$

The global failure rate for this resistance is thus obtained by multiplying all the corrective factors and the base failure rate:

$\lambda = \lambda_b.\Pi_R.\Pi_E\Pi_Q = 0.33 \times 10^{-6}$ / hour

If at the design stage the reliability goals have been integrated, then:

- better thermal designs will allow a lowering of the environment temperature,
- better board designs will lower the load factor ρ.

With t = 60°C and ρ = 0.2 the diagram gives:

$\lambda_b = 1.7$

If now a qualified component is selected, we have: $\Pi_Q = 2.5$, which gives $\lambda = 0.012 \times 10^{-6}$, that is an improvement factor of 30.

Knowledge of the reliability of each component provides a means to obtain the reliability of the boards, (which are repairable or replaceable), and therefore that of whole electronic systems. This is done by using the techniques described in the rest of this report.

Mechanics and electromechanics

Data bases in these fields exist although they are not really "standards". Some sources are:

- RAC, NPRD 3: report by the Reliability Analysis Center (RADC, Griffiss AFB), under contract from the US DoD, dealing with non electronic parts.
- IEEE STD 500: field data on reliability of electrical, electronic and mechanical equipment used in nuclear power plants.

In France and the US, some reference books exist that deal specifically with mechanical components.

As an example of data relevant to our activities, figure 10 gives some information concerning circuit breakers. This comes from RAC's NPRD 3-1985. First, there is a failure mode distribution in a pie chart. For example, 34% of all field failures are due to the circuit breaker failing to open when it should. The table in figure 10 gives a point estimate of the failure rate for the thermal function of circuit breakers.

Various information items given are as follows:

- environment: GF, Ground Fixed, industrial conditions.
- failure rate estimate: $0.335\ 10^{-6}\ h^{-1}$
- a 60% confidence interval for the failure rate using the 20% lower and 80% upper bounds.
- the number of records used in this calculation, i.e. 2.
- the number of observed failures: here 3.
- the total number of operating hours: $8.994\ 10^{6}$ h .

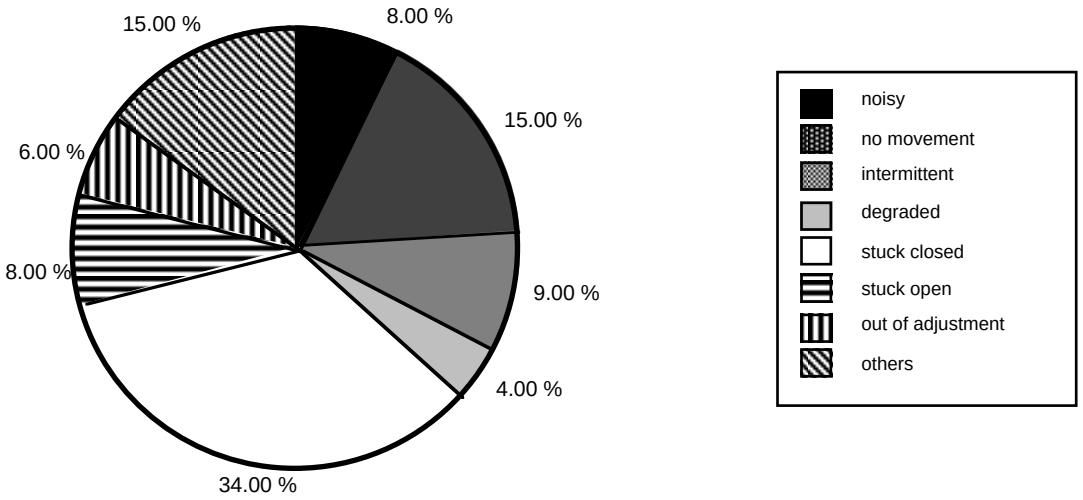
The actual knowledge of the global failure rate and the failure mode distribution allows the calculation of the probability of specific events by using a simple proportionality rule.

For example, for the "stuck closed" mode, we have a corresponding failure rate of:

$$0.335.10^{-6} \times \frac{34}{100} = 1.17.10^{-7}$$

Another approach can sometimes be more relevant: instead of considering the calendar time, the number of make-break operations can be tallied. Then, a test is planned in which a sample is selected and the reliability is estimated using a more realistic model (e.g. Weibull distribution).

Which technique to use is largely a matter of determining the kind of failure one wishes to study: contact wear is related to the number of make and break cycles whereas corrosion is time dependent. Specific use and environment conditions are always important.



component part type	APPL ENV	user code	point estimate	60 % upper single-side	20 % lower internal	80 % upper internal	% of recs	% of fail	operating HRS (E6)
thermal	GF	M	0.335	-	0.171	0.621	2	3	8.944

fig. 10: failure modes and reliability data for circuit breakers

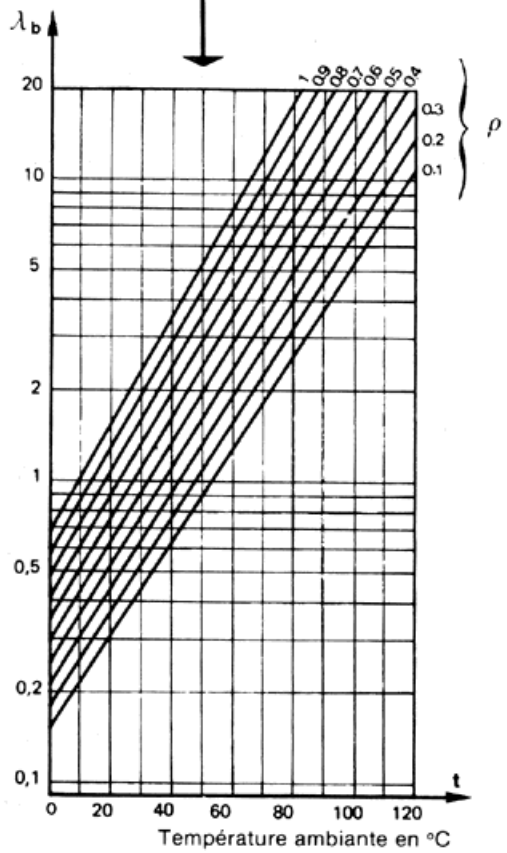
RÉSISTANCES FIXES AGGLOMÉRÉES

CCTU 04 01 A

modèle RA

MIL - R - 11 (RC)
MIL - R - 39 008 (RCR)

$$\lambda = \lambda_b \cdot \pi_R \cdot \pi_E \cdot \pi_Q \cdot 10^{-9}/h$$



λ_b en fonction de la température ambiante t et du facteur de charge ρ

Informations nécessaires		
Température ambiante	t	
Dissipation effective / Dissipation nominale	ρ	
Valeur de la résistance	R	π_R
Environnement		π_E
Classes de qualification		π_Q

Facteur de charge ρ

$$\rho = \frac{\text{Dissipation effective}}{\text{Dissipation nominale}}$$

π_Q Classes de qualification		π_Q
Agrément (PTT,...)	avec CCQ	0,5
	sans CCQ	1
CCQ (UTE/CECC)	sauf usage général	1
	usage général	2,5
Homologation		2,5
Qualification par un client		5
Sans qualification (produit courant)		7,5

π_E Environnement	π_E
Au sol (conditions favorables)	1
Au sol (matériel fixe)	2,9
Au sol (matériel mobile)	8,3
Satellite en orbite	1
Missile (lancement)	29
Avion de transport (zones habitables)	2,8
Avion de transport (zones non habitables)	5,7
Avion de combat (zones habitables)	5,7
Avion de combat (zones non habitables)	11
Bateau (zones protégées)	5,2
Bateau (zones non protégées)	12

π_R Valeur de la résistance	π_R
$R \leqslant 100\ K\Omega$	1
$0,1\ M\Omega < R \leqslant 1\ M\Omega$	1,1
$1\ M\Omega < R \leqslant 10\ M\Omega$	1,6
$R > 10\ M\Omega$	2,5

Répartition des défauts	
Courts-circuits :	0 %
Circuits ouverts :	100 %

Modèle mathématique

$$\lambda_b = 9.10^{-6}.e^{\left[12\left(\frac{t+273}{343}\right) + \left(\frac{\rho}{0.6}\right)\left(\frac{t+273}{273}\right)\right]}$$

information
can refer to American Standard referenced:
MIL HDBK 217 E

fig. 11: example of CNET publications

Failure Modes, Effects and Critically Analysis (FMECA) method

This is a technique to analyse the reliability of a system in terms of the failure modes of its components. The IEC has issued a standard (IEC 812) giving a description of this technique. Each element of the system can, in turn, be analyzed using one of the relevant data bases. The hardware structure of the system as well as its functional characteristics allow the analyst to inductively assess the effect of each and all of the failure modes corresponding to each element and their effects on the system.

An FMECA should also give an estimate of the criticality of each failure mode, see figure 12. This depends on two factors: the probability of occurence of failure and the seriousness of its consequences. Thus an FMECA is a tool to study the influence of the component failures on the system. The main interest of this technique lies in its exhaustiveness. It is nevertheless incomplete in that the combination of effects must be seraparately considered. This can be accomplished using the methods described in the rest of this chapter.

component	function	failure mode	cause	effect	criticality	comments
circuit-breaker	switch	stuck closed	solder	no shedding	2	
«	«	unable to close	mechanical	no power	2	
«	short circuit prot.	unable to open	solder	no protect	4	action
«	current path	sudden open	adjustment	no power	3	
«	«	heat	bad contact	electronic failure	2	

fig. 12: example of FMECA table

Reliability Block Diagram (RBD)

The RBD method is a simple tool to represent a system through its (non-repairable) components. Using the RBD allows the computation of the reliability of systems having series, parallel, bridge and k-out-of-n architectures or any of its combinations. Although it is possible to apply the RBD technique to repairable systems, the implementation is much more difficult.

Series-parallel systems

Two components are in series, from the reliability standpoint, if both are necessary to perform a given function. They are in parallel when the system works if at least one of the two components works, see figure 13.

These considerations are easily generalized to more than two components.

Whenever two components are in series and can be considered to be independent, (the failure of one does not modify the probability of failure of the other), the reliability of this sytem can be calculated by multiplying the individual reliabilities together since the first component AND the second must work:

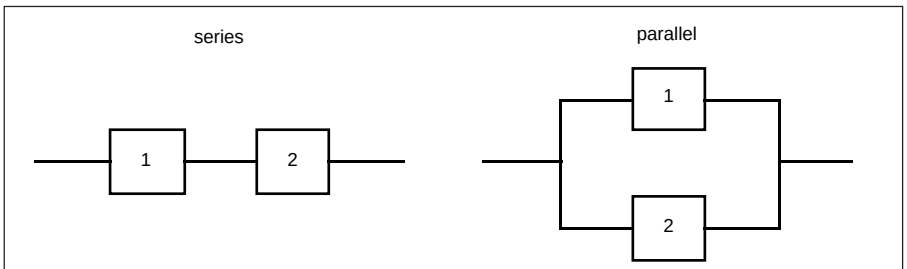


fig. 13: series/parallel systems

$R(t)=R_1(t).R_2(t)$.

In the case of two independent components in parallel, the system works if one OR the other works. It is easy to calculate the unreliability of the system since it is equal to the product of the two component unreliabilities: the system fails if the first component AND the second component fail:

$1 - R(t) =(1 - R_1(t)).(1 - R_2(t))$.

Or equivalently:

$R(t) = R_1(t)+R_2(t) - R_1(t).R_2(t)$.

In this case, components 1 and 2 are said to be in active redundancy. The redundancy would be passive if one of the parallel components is turned on only in the case of failure of the first. This is the case of auxiliary power generators.

For the particular case of non repairable components following an exponential distribution of times to failure, one can write:

For the series case:

$R(t) = \exp(-\lambda_1 t).\exp(-\lambda_2 t) = \exp(-(\lambda_1+\lambda_2)t)$.

It follows that the system's times to failure also follow an exponential distribution, (constant failure rate), since the reliability function is an exponential with:

$\lambda = \lambda_1 + \lambda_2$

For the parallel case:

$R(t) = \exp(-\lambda_1 t)+\exp(-\lambda_2 t)-\exp(-(\lambda_1+\lambda_2)t)$.

Here, the reliability function is not an exponential. Therefore, it can be concluded that the failure rate is not constant.

All these formulas can be generalized to a system with *n* non repairable components, mixing series and parallel architectures.

k-out-of-n redundancies

A k-out-of-n system, or simply K/N, is a n-component system in which k or more components are needed for the system to work properly. We will consider only active redundancies here, see figure 14:

Let us call $R_i(t)$ the reliability of each one of the n components of the system. In some simple cases the reliability of the system can be computed by adding the favourable combinations:

■ **2/3 system:**

$R=R_1.R_2+R_1.R_3+R_2.R_3$

■ **series system (n/n):**

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

■ **parallel system (1/n):**

$$1 - R(t) = \prod_{i=1}^{n} \left(1 - R_i(t)\right)$$

■ **k/n system of identical components**

If we write

$R_i(t) = r(t)$, then,

$$R(t) = \sum_{i=k}^{n} C_n^i \, r(t)^i \left(1 - r(t)\right)^{n-i}$$

Bridge systems

These are systems which cannot be described by simple series-parallel combinations. They can, however, be reduced to series-parallel cases by an iterative procedure, see figure 15.

In order to compute the reliability of this system in terms of the five non repairable component reliabilities it is necessary to apply conditional probabilities:

$R=R_3$.R(given that 3 works)

+ $(1-R_3)$.R(given that 3 has failed).

It is thus possible to derive the system reliability R(t) by decomposing the original bridge system in the two disjoint systems illustrated in figure 16.

Example: reliability of an intrusion detection system.

The system consists of two sensors, a vibration sensor and a photoelectric cell. Each of these sensors could be connected to its specific alarm, as in figure 17, and we would have two independent branches. However, a bridge system would result if each sensor is connected to either one of the two alarms, as in figure 18, through a coupler. We will calculate the reliability improvement due to this modification. Let us also suppose that the mission time of this system is three months, i.e., the maximum expected absence during which the system must function. Furthermore, after each mission, the system is thoroughly checked and maintained and can be considered as good as new when reset. During the mission, there are no repairable elements.

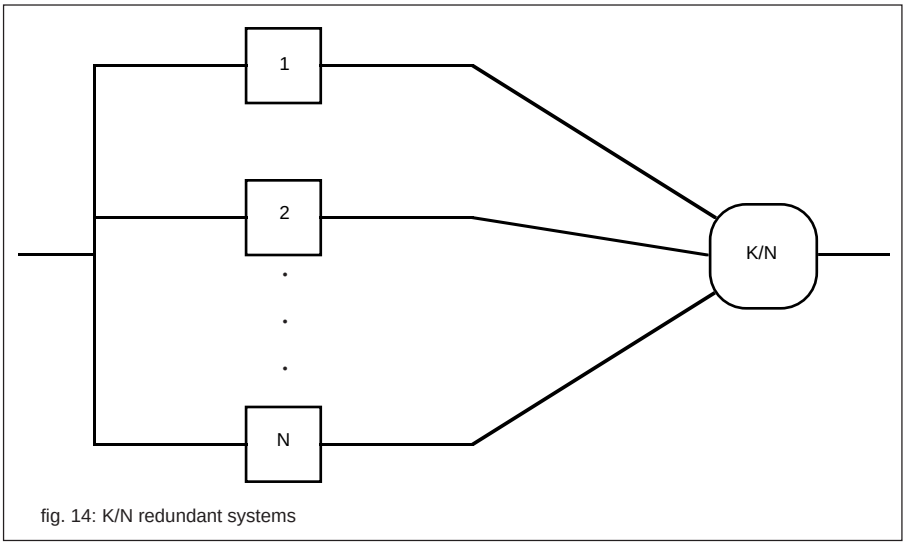


fig. 14: K/N redundant systems

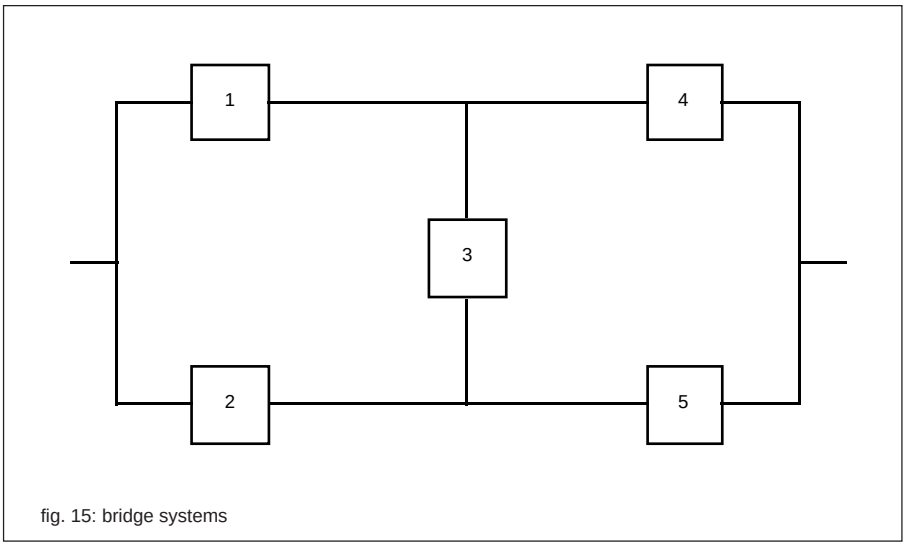


fig. 15: bridge systems

Let us use the following realistic constant failure rates to obtain the different orders of magnitude:

Vibration sensor: $\lambda_1 = 2.10^{-4}$
Photoelectric cell: $\lambda_2 = 10^{-4}$
Coupler: $\lambda_3 = 10^{-5}$
Alarms: $\lambda_4 = \lambda_5 = 4.10^{-4}$

All these failure rates are given in $(\text{hours})^{-1}$

■ **computation for Diagram A of figure 17.**

This is a simple case of two parallel branches, each having two components in series:

Reliability of Branch 1: $R_1(t).R_4(t)$

Reliability of Branch 2: $R_2(t).R_5(t)$

System reliability: $R_A(t) = R_1(t).R_4(t)$

+ $R_2(t).R_5(t) - R_1(t).R_4(t).R_2(t).R_5(t)$

Using $R_i(t) = \exp(-\lambda_i t)$ with t = 3 months = 2190 hours as the mission time one obtains: $R_A(3 \text{ months}) = 0.51$.

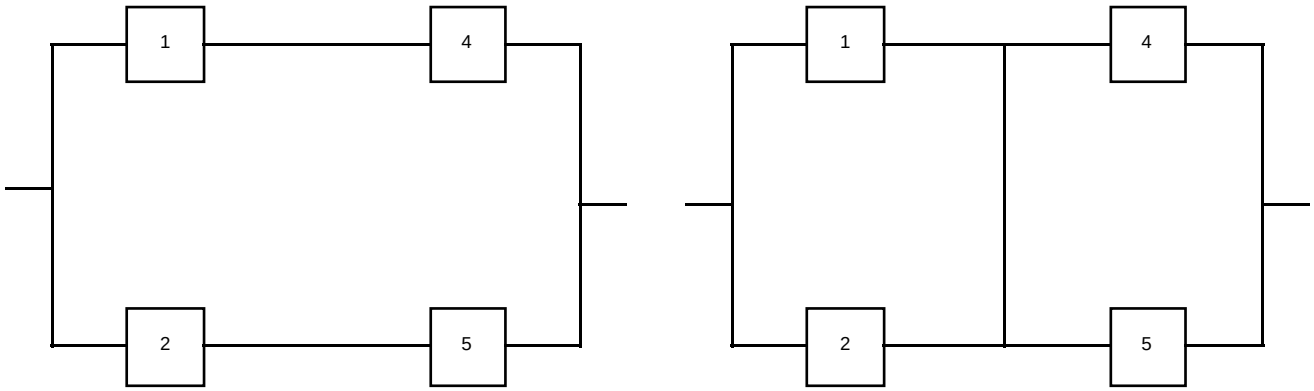


fig. 16: decomposition of a bridge system

■ computation for Diagram B of figure 18

This is the bridge system. Whenever the coupler is failed we are back to the diagram of figure 17. On the other hand, when it works, we have 1 and 2 in parallel, both in series with 4 and 5, themselves in parallel. The system reliability for figure 18 is then:

$R_B = (1-R_3).R+R_3.(R_1+R_2-R_1.R_2).(R_4+R_5-R_4.R_5)$

The numerical computation gives R_B(3 months) = 0.61.

In spite of the excellent reliability of the coupler, the system's reliability is only marginally improved. This numerical example shows, through a simple calculation, that there is not much sense in having a more expensive set-up.

Case of repairable elements

RBD's cannot be used as systematically as before:

■ for two components in parallel, the equation relating R(t) to $R_1(t)$ and $R_2(t)$ is no longer valid. In fact, a working system in the interval [0,t] may correspond to an alternating working condition between 1 and 2, with non repairable components there should be at least one working component in the time interval [0,t] whereas for repairable components both can fail, but not simultaneously.

■ the equation $R(t) = R_1(t).R_2(t)$ remains valid for a two reparaible component series system.

■ in the case of repairable components the main concern is the numerical estimate of the availability. It is possible to use the RBD's with the same formulas as for the reliability calculations:

$A(t) = A_1(t).A_2(t)$ for a series system

$A(t) = A_1(t)+A_2(t)-A_1(t).A_2(t)$ for parallel systems.

These formulas are valid only for simple cases

For instance, the formula $A(t)= A_1(t)+A_2(t) -A_1(t).A_2(t)$ ceases to be valid if only one repairman is available, (instead of as many as necessary). This sequential feature, i.e. having a component waiting to be repaired while the other is being serviced, is not possible to model by a simple RBD. In these cases the State Graphs, to be dealt with later, are adapted to this problem.

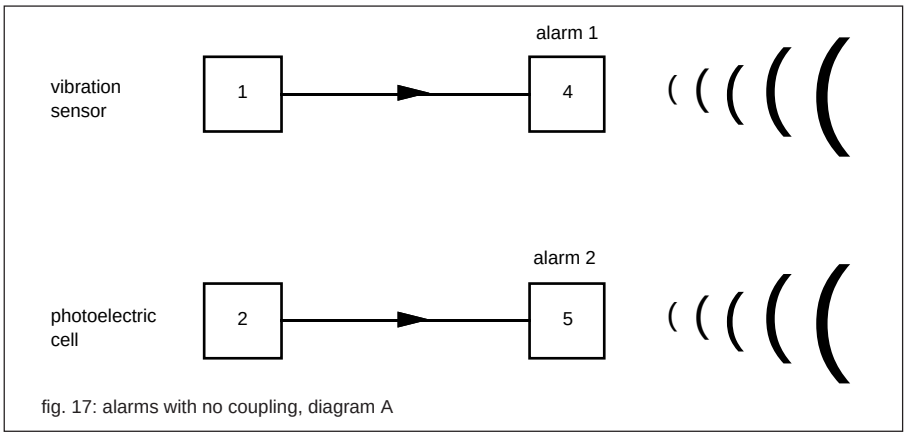


fig. 17: alarms with no coupling, diagram A

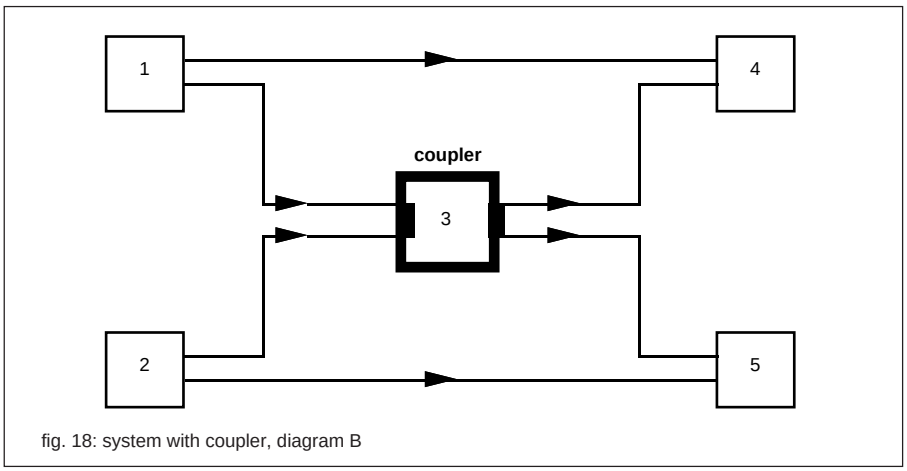


fig. 18: system with coupler, diagram B

fault trees analysis

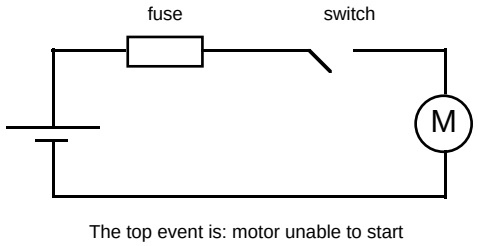
The computation of the system's failure probability is the main goal of this type of analysis. It is based upon a graphical construction representing all the combinations of events, essentially through AND-gates and OR-gates, that may lead to a catastrophic event.
Except for extremely simple cases, computer resources must be used to evaluate the probability of the catastrophic event. It is then possible to modify the structure of the system's design to lower this probability.

Basic procedure
A deep understanding of the system and a clear definition of the "catastrophic event" are essential to build the fault tree. The catastrophic event, sometimes called the "top event", is then analyzed in terms of its immediately preceding causes. Then, each one of these causes is analyzed in terms of their own immediately preceding causes until the basic events are reached. These are supposed to be independent.
A simple example is given in figure 19 and its corresponding fault tree in figure 20. This tree only contains OR-gates connecting the intermediate events (rectangles) and the basic events. The basic events are represented by circles. It is convenient to define a cut-set as a simultaneous combination of basic events that, by themselves, produce the top event.
The analysis proceeds in two phases:

■ **qualitative analysis:** the minimal cut-sets, or min cuts, are obtained. The min cuts are minimal combinations that include basic events that lead to the top event. The order of a min cut is simply the number of basic events it contains.

■ **quantitative analysis:** this is performed using the min cuts and the probability of occurrence of the basic events. This gives an approximate value for the probability of the top event. It is also necessary to validate the accuracy of this approximation in a systematic fashion. Then, depending on the objectives of the analysis, different probabilities are used to compute the system reliability or its availability.

We can illustrate these ideas by two examples:



The top event is: motor unable to start

fig. 19: electrical supply for a motor

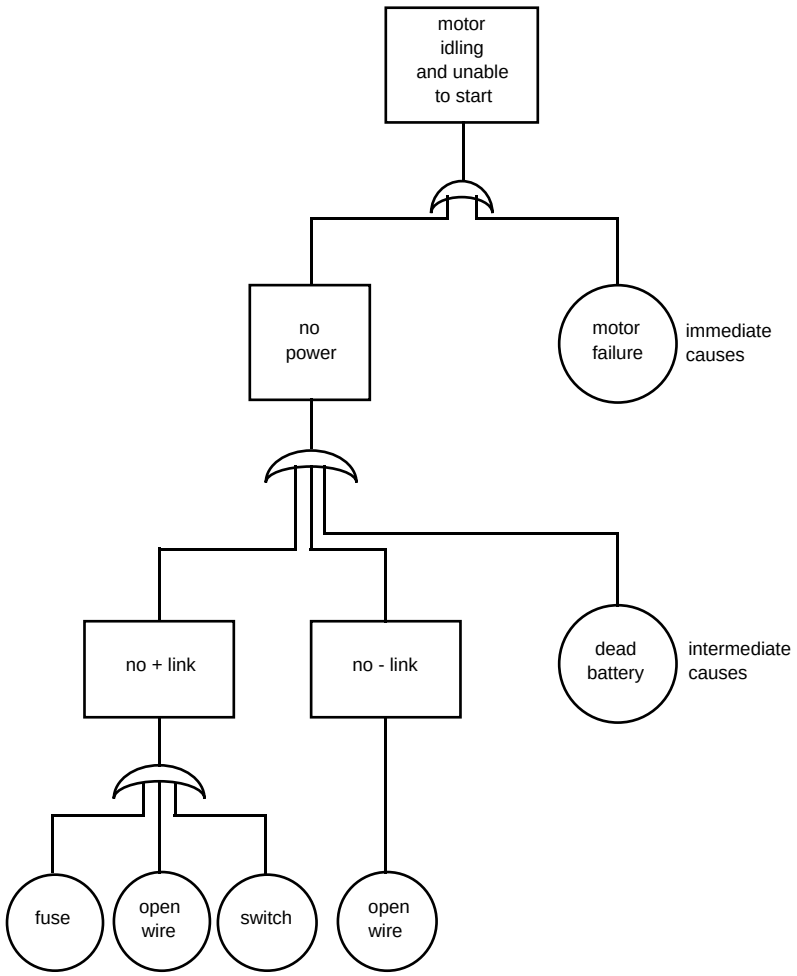


fig. 20: fault tree for fig. 19 circuit

□ an overhead projector with one lamp inside and one spare. The top event is "no working lamp available", see figure 21. A single AND-gate is necessary. The chances of this happening is seen to be 2 in two thousand.

□ a simple light bulb. The top event is “no light”, see figure 22. A single OR-gate is necessary. The probability of the top event is seen to be about 0.001, one in a thousand of not having light. The main cause for this event is the burn out of the light bulb.

In the general case it is often possible to obtain an exact calculation of the probability of the top event using recursivity instead of the min cuts: Boolean probability calculations are performed for each gate in terms of the sub-trees being input to the gate considered. The assumption of independence must be verified but this procedure leads to an exact evaluation of the top event. Thus, the recursive calculation allows a comparison to the min-cut approach. Both methods are complementary.

Application of fault tree using min-cuts to the availability of a low voltage network.

The fault tree corresponding to the network given in figure 23 is shown in figure 24. Power is considerd to be either present or absent. The top event is assumed to be the absence of power at the output, noted E.

In building this tree certain assumptions are made:

■ only two failure modes are considered for the circuit-breakers: sudden contact break and failure to open upon a short-circuit.

■ each transformer line can, by itself, supply voltage to the main network, to which E belongs.

■ the two mains supplies are coming from two different Medium Voltage sources. This reduces the Common Mode failure to the unavailability of the High Voltage supply.

Each event in the Fault Tree will have a certain probability of occurrence associated with it. In this case the probability will be the unavailability. The unavailability associated with the basic events is calculated by the formula: $U \approx \lambda.MTTR$.

λ is the failure rate corresponding to a particular failure mode of a component. It can be obtained from several sources of field data.

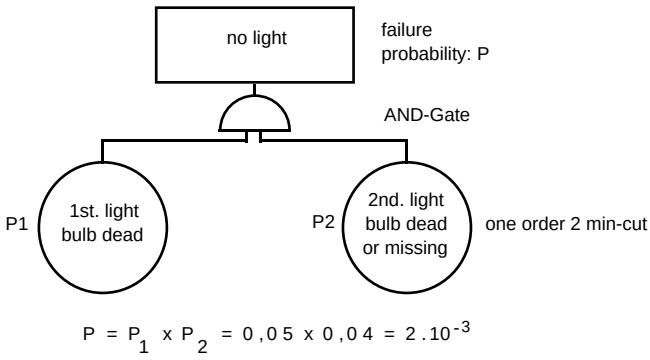


fig. 21: fault tree for an overhead projector

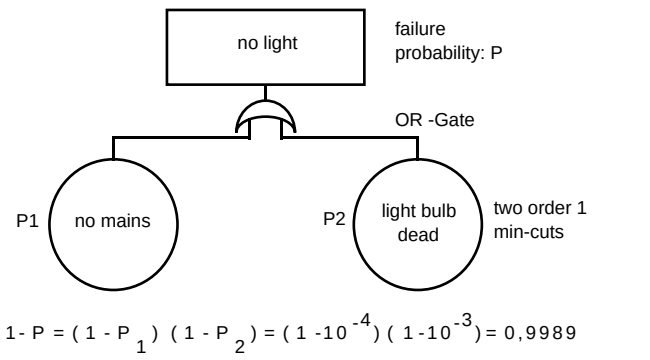


fig. 22: a fault tree for a light bulb

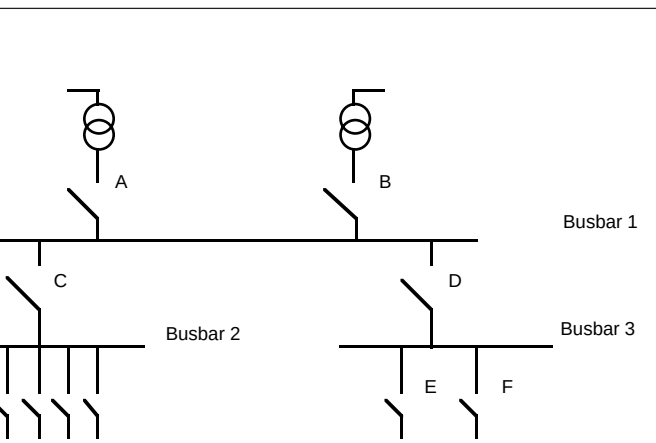


fig. 23: low voltage network

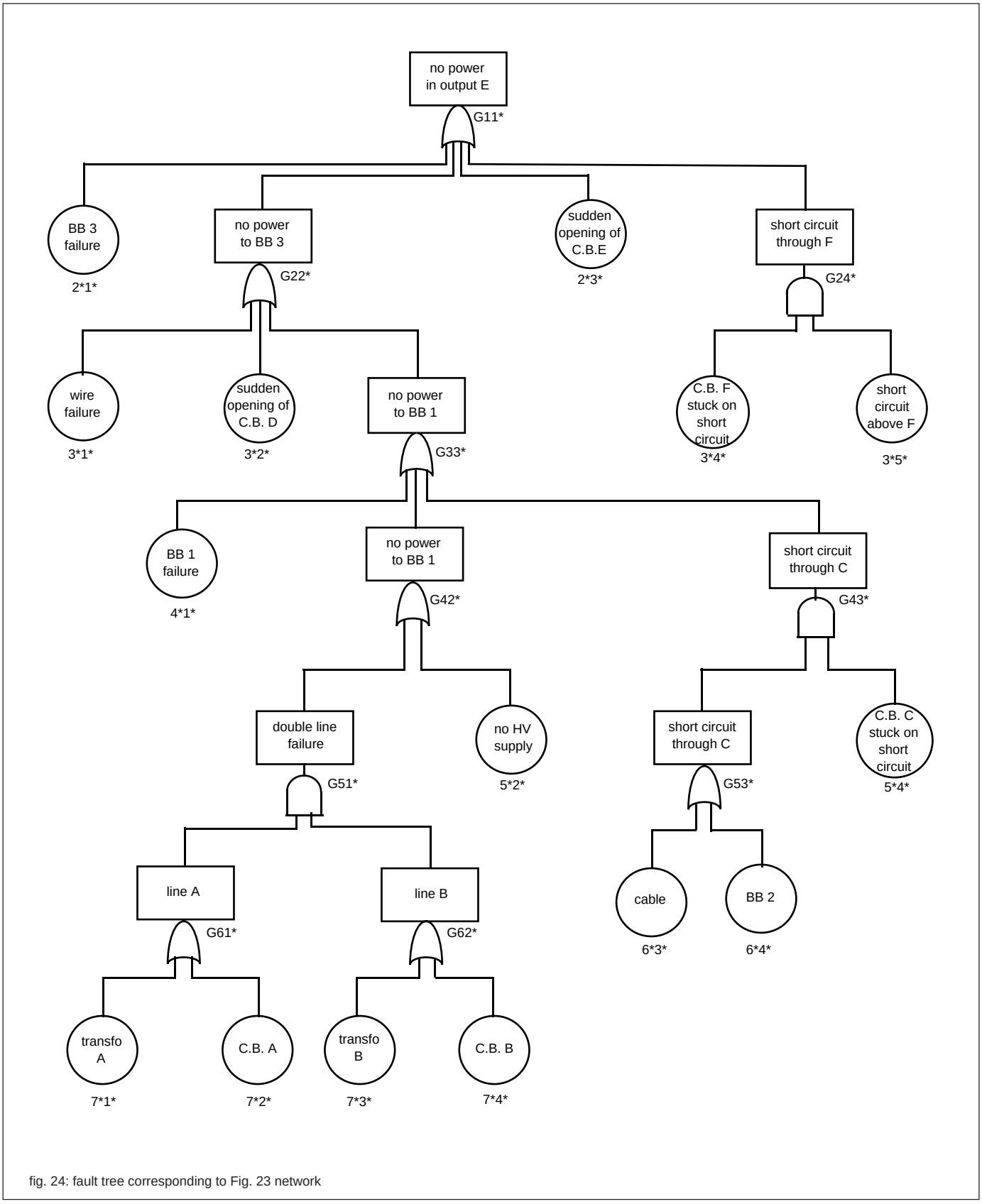


fig. 24: fault tree corresponding to Fig. 23 network

MTTR is the Mean Time to Repair and it depends on the component being considered as well as the particular installation, technology, geographical location, service contract.

In some instances a specific value of a probability is unknown. A worst case situation, or upper bound, is therefore assumed. For example, we have taken the upper bound probability of a short-circuit above F to be 10^{-2}.

The results of the Fault Tree Analysis, shown in figure 25, indicate that the unavailability on output E is 10^{-5} which corresponds to 5 minutes per year. The min cut approach allows, in addition to the calculation of the probability of the top event, the assessment of the weight each min cut carries in producing the top event. Figure 25 also shows this weight, as a percentage of the total unavailability which is possible to attribute to each min cut. This contribution is one measure of the importance of the min cut.

An eyeball examination of the min cuts relative importances shows that the cable linking busbar 1 to busbar 3, (third min cut), is critical. To a lower extent this is also true of the two busbars 1 and 3. If these components were improved, the mains supply then becomes critical. If a further improvement on the overall availability became essential, it would be necessary to incorporate an auxiliary power supply, such as a diesel generator. A detailed study of the availability of an electrical supply is presented in Merlin Gerin's Technical paper "Sureté et distribution électrique" (in French).

state graphs

State graphs, also called Markov graphs, allow a powerful modeling of systems under certain restrictive assumptions. The analysis proceeds from the actual construction of the graph to solving the corresponding equations and, finally to the interpretation of results in terms of reliability and unavailability. Mathematically, a great simplification is obtained by considering only the calculation of time independent quantities.

Construction of the graph

The graph represents all the possible states of the system as well as the transitions between these states. These transitions correspond to the different events that concern the components of the system. In general, these events are either failures or repairs. As a consequence, the transition rates between states are essentially failure rates or repair rates, eventually weighted by probabilities like that of an equipment refusing to turn on upon demand.

The graph on figure 26 shows the behavior of a system with a single repairable component.

Assumptions

A model is said to be markovian if the following conditions are satisfied:

- the evolution of the system depends only on its present state and not on its past history,
- the transition rates are constant, i.e. only exponential distributions are considered,
- there is a finite number of states,
- at any given time there cannot be more than one transition.

Equations

Under the above hypotheses, the probability of the system being in state E_i at time t+dt can be written as: $P_i(t+dt)$ = P(the system is in state E_i and it stays there) + P(the system comes from another state E_j).

For a graph having n states, n differential equations are obtained which can be written as:

$$\frac{d\Pi(t)}{dt} = \Pi(t).[A]$$

where: $\Pi(t) = [P_1(t), P_2(t), \ldots, P_n(t)]$

[A] is called the transition matrix of the graph.

The solution of this equation in matrix form is performed by computer and gives the probabilities $P_i(t)$, that is the probability of the system being in state i as a function of all the transition rates and the initial state.

Computation of dependability quantities

The availability being the probability of the system being in a working state, it follows:

$$A(T) = \sum_i P_i(t)$$

where $P_i(t)$ = probability of being in working state E_i.

unavailability: 1.01 E -05, i.e. 1.01 10^{-5}
list of min cuts and their importance
min cuts indicated on the fault tree, percent contribution

1	:2*1*	:	9,5
2	:2*3*	:	1,6
3	:3*1*	:	68
4	:3*2*	:	1,6
5	:3*4* , 3*5*	:	,013
6	:4*1*	:	9,5
7	:5*2*	:	9,9
8	:5*4* , 6*3*	:	9,1E - 6
9	:5*4* , 6*4*	:	3,2 E - 6
10	:7*1* , 7*3*	:	,00058
11	:7*1* , 7*4*	:	1,3 E - 5
12	:7*2* , 7*3*	:	1,3 E - 5
13	:7*2* , 7*4*	:	2,7 E - 7

fig. 25: contributions of network components to its unavailability

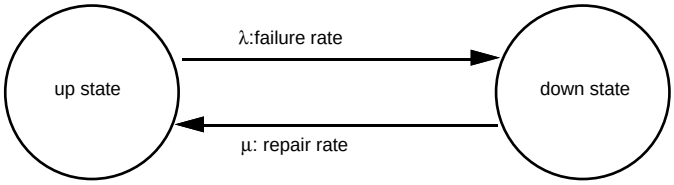


fig. 26: elementary state graph

The reliability is the probability of being in a working state without ever having passed through a down state. A graph is constructed by deleting all transitions going from a failed state to a working state. Once the new probabilities $P_i'(t)$ are obtained, we have:

$$R(t) = \sum_i P_i'(t)$$

There are two other quantities which are very simple to obtain:

■ the meant time of state occupancy:

$$T_i = \frac{1}{\Sigma \text{ (rates of departure from state i)}}$$

■ the occupancy frequency corresponding to state i:

$$f_i = \frac{P_i}{T_i}$$

The characteristic mean times MTTF, MTTR, MUT, MDT, MTBF are calculated using matrix calculus and some of the equations already discussed. For the MTTF, the initial state of the system must be specified in terms of the probabilities of the system being initially in each one of its different states.

Application: Uninterruptible Power Supplies (UPS) in parallel

A UPS is a device which improves the quality of the electrical supply. It is often used for critical applications such as computers and their peripherals. We will consider a typical configuration (Triple Modular Redundancy), i.e. the UPS's constitute a 2/3 redundant system. The unavailability is not the only quantity of interest: the MTTF gives the mean time before the first black-out.

In the construction of the state graph it is here possible to use the fact that the three UPS's are identical and therefore states can be grouped, according to the number of failed UPS's. The failure and repair rates for the UPS's, λ and μ respectively, are given in figure. 27

The number associated with each state corresponds to the number of failed UPS's. Each working UPS in state E_i adds its own exit rate λ towards state E_{i+1}. These exit rates are 3λ, 2λ and λ respectively.

The up states are 0 and 1. We assume that the repair strategy is such that there can be three repairmen working simultaneously on each UPS. Thus, the transition rates corresponding to the repair activity are proportional to the number of failed UPS's in the state being considered. The numerical values are as follows:

$\lambda = 2.10^{-5}\ h^{-1}$; $\mu = 10^{-1}\ h^{-1}$

Figure 28 gives the computed results corresponding to the time independent quantities. It can be seen that the MTTF is here $4.17\ 10^7$ hours whereas the nonredundant case (3/3) has an MTTF equal to $1/3\ \lambda = 1.67\ 10^4$ hours.

For the asymptotic unavailability the change is from $1.19\ 10^{-7}$ for the redundant system to $6\ 10^{-4}$ for the non redundant case (3/3) system. The comparison of these figures is easily visualized through the graph itself: in the redundant case, the unavailability is calculated by summing the probabilities of the two failed states, i.e., $A = P_2+P_3$ while, in the non redundant case, the sum is performed over **three** failed states:
$A = P_1+P_2+P_3$

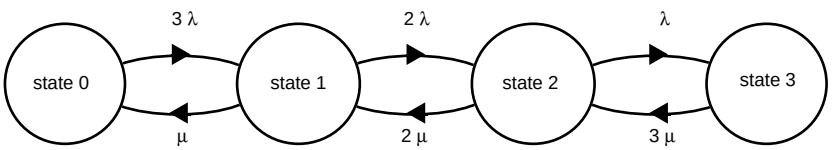


fig. 27: UPS's in parallel

Time independant quantities:

Unavailability:	:	1.199360E-07	Availability	:	9.999999E-01
MTTF	:	4.169167E+07	MTTR	:	8.333667E+00
MUT	:	4.169167E+07	MDT	:	5.000333E+00
MTBF	:	4.169167E+07			

fig. 28: values corresponding to the graph on figure 27

6. conclusion

The dependability is a concept becoming ever more critical for comfort, efficiency and safety. It can be controlled and calculated. It can be designed in, be it for devices, architectures or systems.
Dependability characteristics are now frequently included in specifications and contracts. The existence of computational methods and tools allows the systematic study of the dependability during the design phase and for quality assurance purposes.
An intuitive insight, combined with exact or approximate calculations, allow the comparison of different configurations and thus provide an evaluation of risk associated to a better performance, i.e. performance adapted to clearly specified needs.

7. references and standards

Military Handbook 217E
DoD (U.S.A.)
October 1986.

Recueil de données de fiabilité, CNET
(Centre National d'Etudes des Télécommunications, France)
1983.

IEEE Std. 493 and IEEE Std. 500
(Institute of Electrical and Electronic Engineers)
1980 and 1984.

NPRD document 3
Nonelectronics Parts Reliability Data
Reliability Analysis Center, (RADC)
1985.

A. Pagès, M. Gondran:
"Fiabilité des systèmes"
Eyrolles, France1983.

A. Villemeur:
"Sureté de fonctionnement des systèmes industriels"
Eyrolles, France 1988.

I**nternational Electrotechnical Vocabulary**
VEI 191
International Electrotechnical Commission
June 1988.

Proceedings of the 15th InterRam conference
Portland, Oregon
June 1988.

C. Marcovici, J. C. Ligeron:
"Techniques de fiabilité en mécanique"
Pic, France, 1974.

EPRI document 3593
Electrical Power Research Institute
Hannaman, Spurgin, 1984.

NUREG document 2254
US Nuclear Regulatory Commission
Bell, Swain, 1983.

Merlin Gerin Technical Report 117 :
"Méthode de développement d'un logiciel de sureté"
A. Jourdil, R. Galera 1982.

Merlin GerinTechnical Report 134 :
"Approche industrielle de la sureté de fonctionnement"
H. Krotoff 1985.

Merlin Gerin Technical Report 148 :
"Sureté et distribution électrique"
G. Gatine 1990.

IEC Standard 271
List of basic terms, definitions and related mathematics for reliability.

IEC Standard 300
Reliability and maintainability management.

IEC Standard 362
Guide for the collection of reliability, availability and maintainability data from field performance of electronic items.

IEC Standard 409
Guide for the inclusion of reliability clauses into specifications for components (or parts) for electronic equipment.

IEC Standard 605
Equipment Reliability Testing.

IEC Standard 706
Guide on maintainability of equipment.

IEC Standard 812
Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA).

IEC Standard 863
Presentation of reliability, maintainability and availability predictions.

IEC Standard 1014
Programmes for reliability growth.

Merlin Gerin's dependability experts have published extensively in this field and have presented papers in most international reliability conferences.

Merlin Gerin is also an active participant in several national and international committees dealing with dependability:

- presidence of the French National Committee for IEC TC 56 activities, (dependability) and expert with IEC Working Group 4, TC 56, (statistical methods),
- software dependability with the European Group of EWICS- TC7: computer and critical applications,
- french AFCET Working Group on computer systems dependability,
- updating contributions to the French CNET Electronic components reliability handbook,
- working Group IFIP 10.4 on Dependable Computing.