n°184

electrical installation dependability studies

Sylvie LOGIACO

**An ISTG Engineer (Institute Scientifique et Technique de Grenoble) graduating in 1987, she was initially involved in risk analysis in the chemicals industry ; at Pechiney, then at Atochem.
With Schneider since 1991, she is part of the centre of excellence for Dependability for which she has carried out a large number of dependability studies on electrical and monitoring and control installations.**

E/CT 184 first issued September 1997

glossary

Availability:
Percentage of time for which the system functions correctly.

Dependability:
Generic term which combines the independent variables of reliability, availability, maintainability and safety.

Hasard analysis:
Based on the functional analysis, this is the analysis of the failures that can occur in a system (in practice it is a synonym for «dependability study»).

Feedback of experience:
Operational reliability data collected during failure of equipment in operation.

Maintainability:
The aptitude of a system to be repaired quickly.

Reliability:
The aptitude of a system to function correctly for as long as possible.

Safety:
The aptitude of a system to not put people in danger.

electrical installation dependability studies

contents

In both the industrial and tertiary sectors, the quality of power supply is of increasing importance. The quality of the electricity product, besides imperfections such as variations in voltage and harmonic distortion, is basically characterised by the availability of the electrical energy. Loss of power is always annoying, but it can be particularly penalising for information systems (computing - monitoring and control); they can even have disastrous consequences for certain processes and in certain cases endanger people's lives.

Dependability studies enable electrical availability requirements to be incorporated in the choice of electrical network to be installed. They also enable two different installation configurations to be compared ... the most expensive one is not always better ...
The aim of this «Cahier Technique» is show how dependability studies are performed: methodology and tools. Two examples of studies are given: that of an electrical network in a factory and that of the monitoring and control system of a high voltage substation. These studies are becoming increasingly easy to perform thanks to computing «tools».

1. introduction

general

The voltage at the terminals of a current consumer can be affected by phenomena originating in the distributor's network, the electrical installation of a subscriber connected to that network or the electrical installation of the user who is suffering the disturbance.

Disturbances in the electricity product

■ the main characteristics of the voltage supplied by both the MV and LV public distribution network are those defined by European standard EN 50160. This details the tolerances that must be guaranteed for both voltage and frequency as well as the disturbance levels that are usually encountered; e.g. harmonic distortion. The table in figure 1 details the standard's recommended values.

At any moment in time therefore, the quality of the energy supplied to the current consumers in an installation can be affected by various disturbances, either imposed by the external supply network or self-generated within the internal distribution network.
The operations of current consumers that are either independent or federated in systems are affected by these disturbances.

■ malfunctions and the type and cost of the damage incurred depend both on the type of current consumers and on the installation's criticality level. Thus, a momentary break in supply to a critical current consumer can have serious consequences on the installation's operation without it being intrinsically affected.

■ in all cases, a study detailing the effects of the suspected disturbances must be performed. Measures must be taken to limit their consequences.

■ the table in figure 2 shows the disturbances that can usually be found in electrical networks, their causes and the solutions that are possible to reduce their effects.

■ the reduction of the effects of harmonics, Flicker, voltage imbalances, frequency variations and overvoltages is achieved by installing equipment suited to each case. The design and choice of connection points for such equipment are decided by performing detailed studies that are outside the scope of this document (see bibliography).

standard EN 50160	**low voltage supply**	
frequency	50 Hz ± 1% for 95% of a week 50 Hz + 4%, - 6% for 100% of a week	
voltage amplitude	for each one week period, 95% of the average effective values over 10 minutes must be within the range of Un ± 10%	
rapid voltage variations	from 5% to 10% of Un (4 to 6% in medium voltage)	
voltage drops (indicative values)	■ amplitude: ■ duration: ■ number:	between 10% and 99% of Un most voltage drops are <60% of Un between 10 ms and 1 minute, most voltage drops < 1s several tens to 1 thousand per year
brief loss of power (indicative values)	■ amplitude: ■ duration: ■ number:	100% of Un up to 3 minutes, 70% are less than 1s several tens to several hundreds per year
long loss of power (indicative values)	■ amplitude: ■ duration: ■ number:	100% of Un over 3 minutes, between 10 and 50 per year

fig. 1: network disturbances : values found in the standard.

Loss of power

For industrial processes and low voltage systems this is increasingly difficult to tolerate since it generates unacceptable costs.

■ immunity to loss of power requires dedicated equipment such as uninterruptible power supplies and independent generator sets. This equipment is generally not enough to resolve all the problems. The network configuration, automatic power restoring control devices, the level of reliability of the equipment, the selectivity of protection devices as well as the maintenance policy, all play an important role in reducing and eliminating down time.
Minimising loss of power requires reliability / dependability studies to be performed that take account of all these factors as well as the frequency and duration of the loss of power that is acceptable to the installation.

These studies enable the best suited configuration and equipment to be determined for the operator's requirements. They generally require the current consumers or systems to be classed according to their sensitivity level as well as distinguishing between:
□ current consumers that accept prolonged stoppage: 1 or more hours (non priority),
□ current consumers accepting stoppages of several minutes long (priority),
□ current consumers which must have the power restored to them after several seconds (essential)
□ current consumers not accepting any break in supply (vital),

As an example, figure 3 shows the simplified diagram of a network in which this distinction has been performed:

□ **vital** current consumers not tolerating the slightest break in supply, are supplied power through an uninterruptible power supply.

□ power is restored to **essential** current consumers a few seconds after network

disturbance	possible causes	main effects	possible solutions
frequency variations	■ supply network ■ grouped operation of independent generators	■ variation in speed of motors ■ malfunctioning of electronic equipment	■ UPS
rapid voltage variations	■ supply network ■ arc furnace ■ welding machine ■ load surge	■ lighting flicker ■ variation in speed of motors	■ increasing short circuit power ■ modifying the installation configuration
voltage drops	■ supply network ■ high load demands ■ external and internal faults	■ extinction of discharge lamps ■ malfunctioning of regulators ■ speed variation, stopping of motors ■ switching of contactors ■ disturbances in digital electronics systems ■ malfunctioning of power electronics	■ UPS ■ increasing short circuit power ■ modifying the installation configuration
brief and long loss of power	■ supply network ■ reclosing operations ■ internal faults ■ source switching	■ equipment stoppage ■ installation stoppage ■ loss of production ■ switching of contactors ■ various malfunctions	■ UPS ■ independent generators ■ modifying the network configuration ■ setting up of a maintenance policy
voltage imbalances	■ supply network ■ many single phase loads	■ overheating of motors and alternators	■ increasing short circuit power ■ modifying the network configuration ■ balancing of single phase loads ■ rebalancing devices
overvoltages	■ lightening ■ switchgear operation ■ insulation fault	■ breakdown of equipment	■ lightening arrestors ■ choice of insulation level ■ control of the resistance of earthing electrodes
harmonics	■ supply network ■ a lot of non linear current consumers	■ overheating and damaging of equipment, mainly motors and capacitors ■ malfunctioning of power electronics	■ increasing short circuit power ■ modifying the installation configuration ■ filtering

fig. 2: disturbances in networks, causes, effects and solutions.

failure, as soon as the voltage and frequency of the generator set have stabilised,

□ power is restored to **priority** current consumers once the essential current consumers have been started up,

□ power is not restored to **non-priority** current consumers, which accept a long break in power supply, until the external network is functioning again.

By appropriate selection of the configuration and the automatic source switching control devices (see. «Cahier Technique» n°161) we can optimise the positioning and dimensioning of back up and replacement supplies in order to meet operating constraints.

It should be remembered that the choice of neutral earthing arrangement is an important factor; it is clearly established that for current consumers requiring a high level of availability, it is highly advisable to use the isolated neutral arrangement since it enables continuity of supply on the occurrence

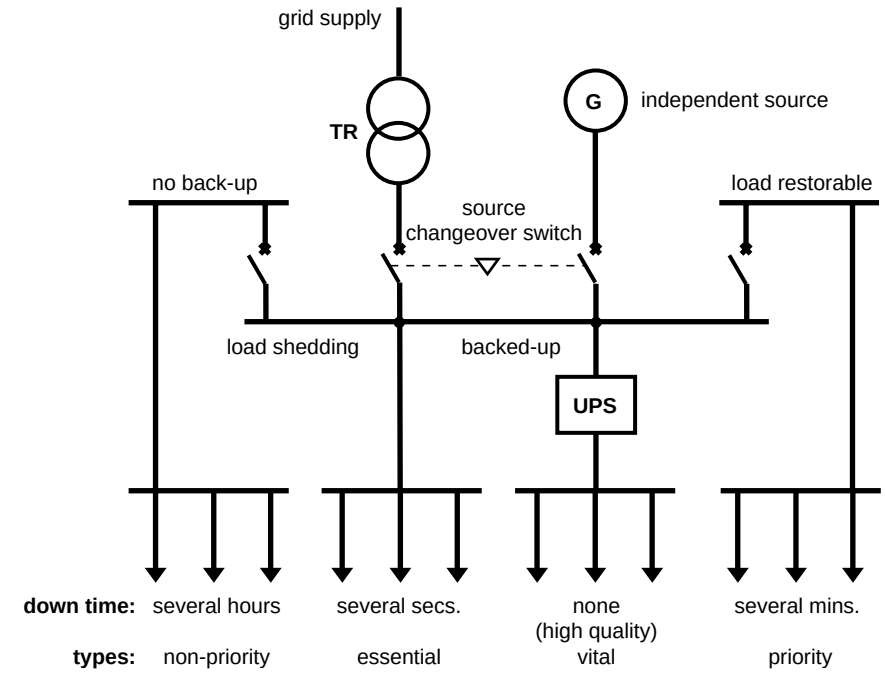


fig. 3: a reliable power supply. Simplified network diagram.

of an initial insulation fault (see. «Cahiers Techniques» n°172 and n°173).

dependability studies

Before looking at electrical network dependability studies, it would be useful to recap on several definitions of the terms used by reliability specialists, even if everyone knows the definitions of the words: reliable, available, maintenance and safety (see fig. 4 and 5).
It is also necessary to detail the applicational scope and general features of such studies.

Scope and features of studies

■ applicational scope:
studies are carried out on all types of electrical networks, from low voltage to high voltage, and on their monitoring and control systems.
The networks may be:
□ single feeder

dependability:
Dependability is a generic idea that measures the quality of service, provided by a system, so that the user can have justified confidence in it. Justified confidence is achieved through quantitative and qualitative analyses of the various features of the service provided by the system. These features are based on the probability parameters defined below.

reliability:
the probability that a unit is able accomplish a required function, under given conditions, during a given interval of time [t1,t2] ; written R(t1, t2).

availability:
the probability that a unit is in a state that enables it to accomplish a required function under given conditions and at a given moment in time, t ; written D(t).

maintainability:
the probability that a given maintenance action can be carried out within a given time [t1, t2].

safety:
the probability of avoiding an event with hazardous consequences within a given time [t1,t2].

failure rate:
the probability that a unit loses its ability to accomplish a function during the interval [t, t+dt], knowing that it has not failed between [0, t] ; it is written $\lambda(t)$.

the equivalent failure rate:
the value or a constant failure rate: λ_{eq} for which the reliability of the system in time t is equal to $R(t) - \lambda_{eq}$ is a «constant approximation» of $\lambda(t)$.

MTTF (Mean Time to Failure):
the average time of correct operation before the first failure.

MTBF (Mean Time Between Failure):
the average time between two failures in a repairable system.

MUT (Mean Up Time):
the average time of correct operation between two failures in a repairable system.

MTTR (Mean Time To Repair):
the average time required to repair.

MDT (Mean Down Time):
the average time for which the system is not available. It includes the time to detect the fault, the time for the maintenance service team to get to the fault, the time to get the replacement parts for the equipment to be repaired and the time to repair.

the repair rate:
the inverse of the mean time to repair.

FMEA (Failure Modes and Effects Analysis):
this enables the effects to be analysed of the failure of components on the system.

model:
graphical representation of the combination of failures found during an FMEA and of their maintenance process.

undesirable event:
system failure that must be analysed in order for the user to feel justified confidence in the system. This system failure gauges the quality of service,

fig. 4: definitions.

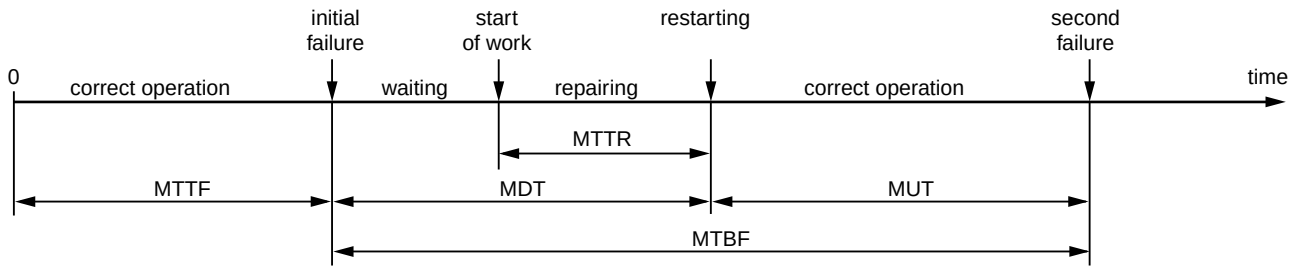
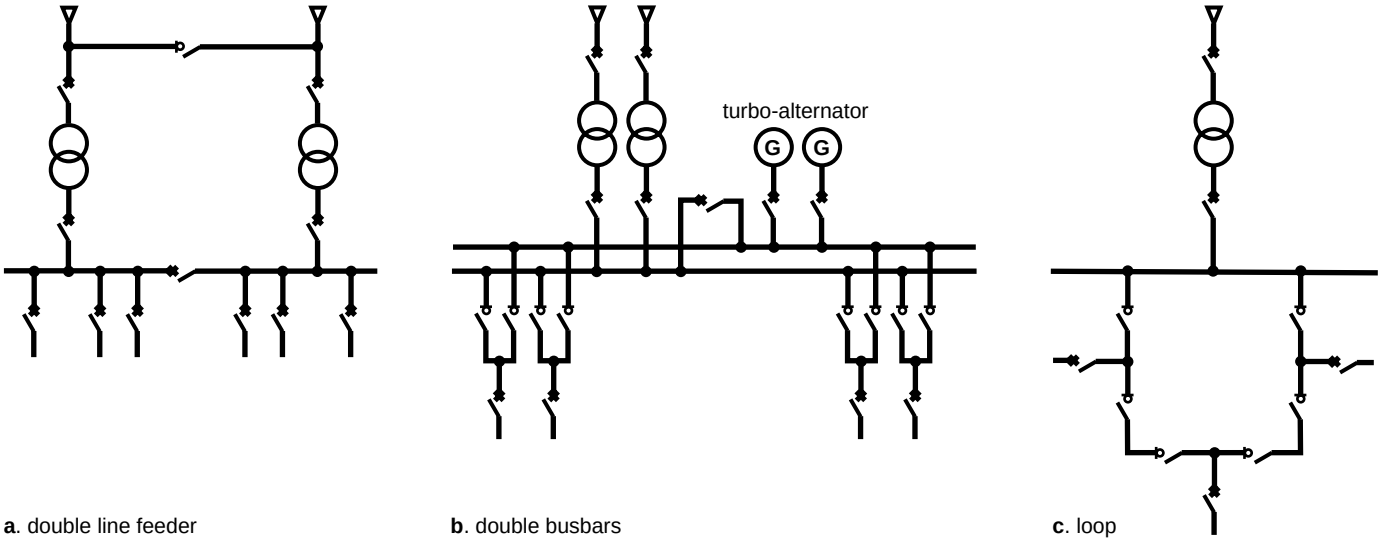


fig. 5: relations between the various values that characterise the reliability, maintainability and availability of a machine.



a. double line feeder **b**. double busbars **c**. loop

fig. 6: network configurations.

	preliminary study	**detailed study**
accuracy of assumptions	1 single failure type (1 frequency, 1 average duration)	failures divided into families according to their effect on the system.
accuracy of modelling	the consequences of the failures are combined into major families	the consequences of the failures are analysed in depth.

fig. 7: differences between a preliminary study and an in-depth study.

□ double feeder (see fig. 6a),
□ double busbar (see fig. 6b),
□ loop (see fig 6c),
□ and with or without reconfiguration or load shedding.

■ characteristic features of studies:
studies are tailor made to take account of the expressed requirements.
They are set up in terms of:
- accuracy of study,
- type of analysis,
- type of dependability criteria,

□ the accuracy of study
(see fig. 7):
- brief or preliminary study: this is a pessimistic study generally used to quickly make technical choices
- very detailed studies that take account of as many factors as possible.
Taking account of all the operating modes, detailed analysis of possible failure modes and their consequences, modelling the malfunctioning behaviour of the system.

□ the types of analysis
- design assistance in assessing the dependability criteria
(see fig. 8),

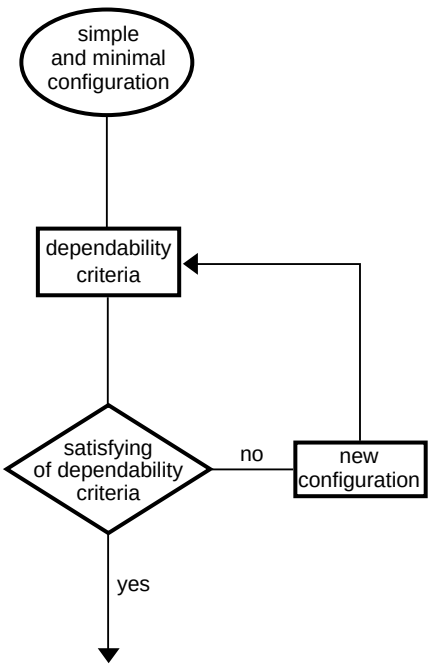


fig. 8: design assistance.

- comparison of configurations (see fig. 9),
- qualitative configuration analysis.

□ the types of criteria to be quantified (see fig. 10)

- the average number of hours that the system functions correctly (MUT):
- the average number of hours that the system functions before not supplying certain current consumers for the first time (MTTF)
- the probability of no longer supplying power to certain current consumers (availability),
- the average number of failures per hour during a year (λ_{eq}),
- an average repair time ($1/\mu_{eq}$),
- the optimal frequency of preventive maintenance,
- the calculation of replacement part kits.

These criteria enable an assessment to be made of the system's performance level and thus to determine the configuration that meets dependability criteria without forgetting economic constraints.

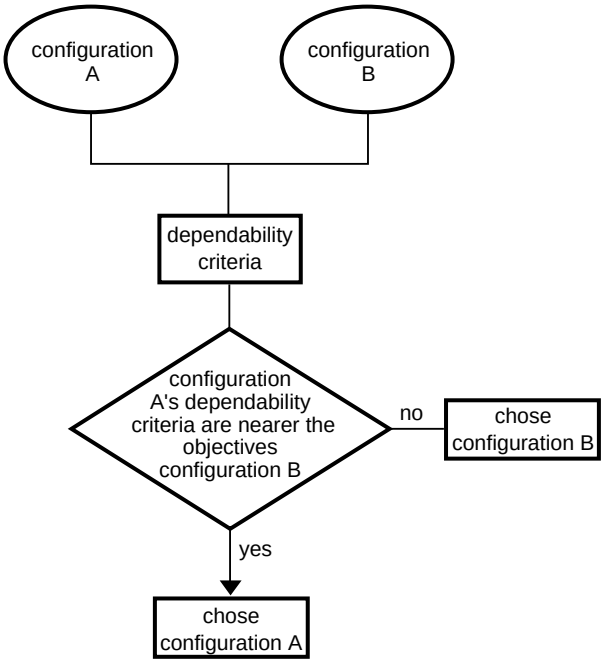
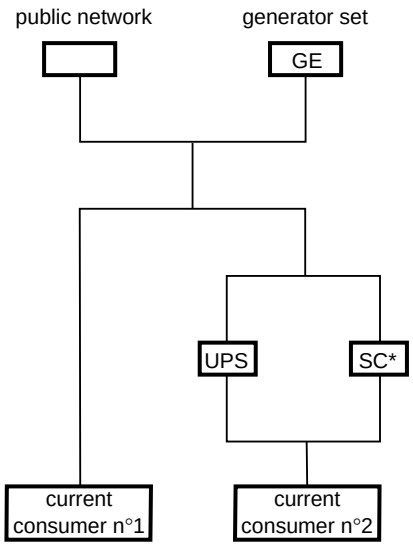


fig. 9: configuration comparison.



we can calculate:

- the probability that GE does not start when power supply is lost.
- the optimum preventive maintenance frequency for the GE.
- the number of minutes a year that current consumer n°1 is not supplied.
- the average number of hours before current consumer n°2 will no longer have power.

* SC= Static contactor

fig. 10 : illustration of dependability assessment criteria.

2. how a study is carried out

the chronological order of phases

Whatever the requirement expressed by the designer or operator of an electrical installation, a dependability study will include the following phases (see fig. 11):

- expression and analysis of the requirements,
- functional analysis of the system,
- failure modes analysis,
- modelling,
- calculation or assessment of dependability criteria.

In most cases, this procedure must be performed several times:

- twice if we want to compare two layouts,
- n times if we want to determine a configuration that is adapted to requirements taking account of technical and economic constraints.

expression and analysis of requirements

As discussed at the end of the previous chapter, the study initiator must detail (see fig. 12):

- what the study involves ; e.g: substation monitoring and control, and provide the design elements that he has in his possession.
- the type of request (type of analysis required), e.g.:
  - a demonstration of the confidence level that we can assign to a power supply for a critical process (orienting us towards a type of study, types of criteria to be assessed),
  - the search for objective criteria making technical and economic analysis possible,
  - the determination of the most suitable configuration to meet requirements (orienting us towards a type of analysis),
  - support for a specific equipment design.

These points can be combined ; in other words a company can search for the configuration best suited to its needs to supply power to a critical process as part of a technical and economic analysis.

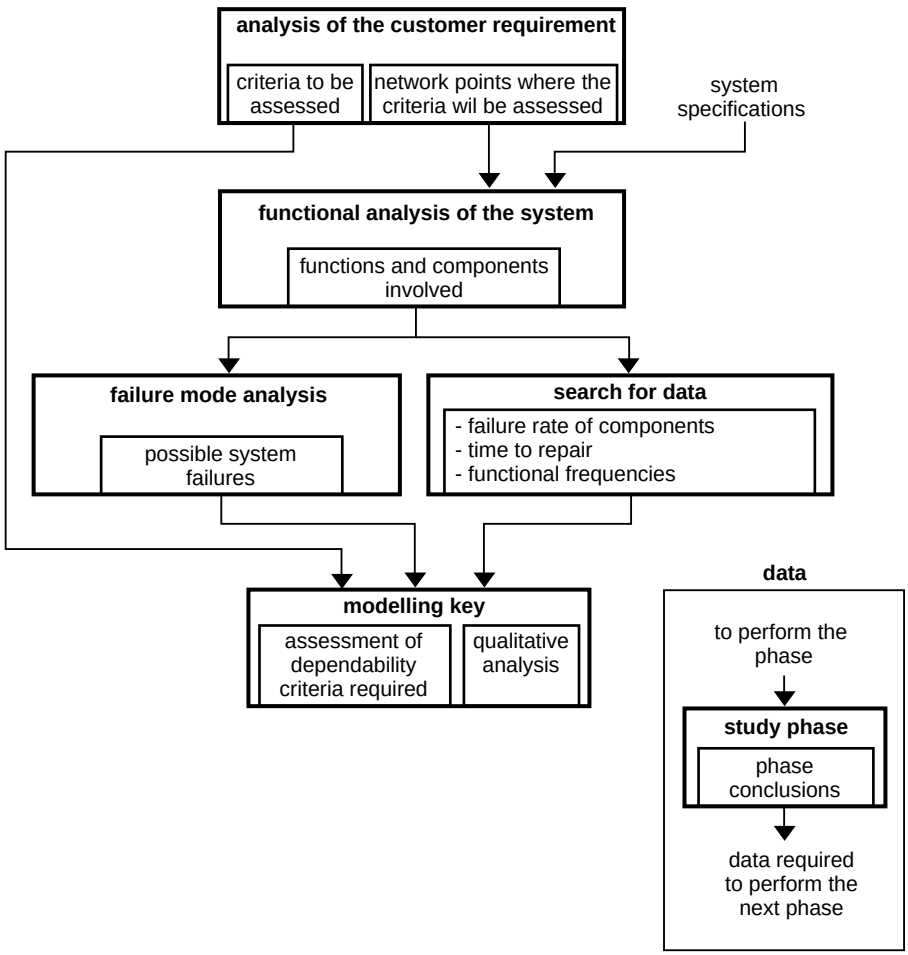


fig. 11: the chronological order of phases in performing a dependability study.

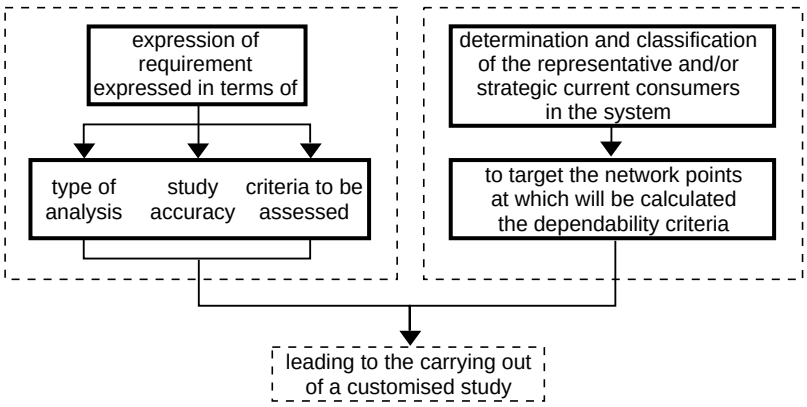


fig. 12: information required for the study.

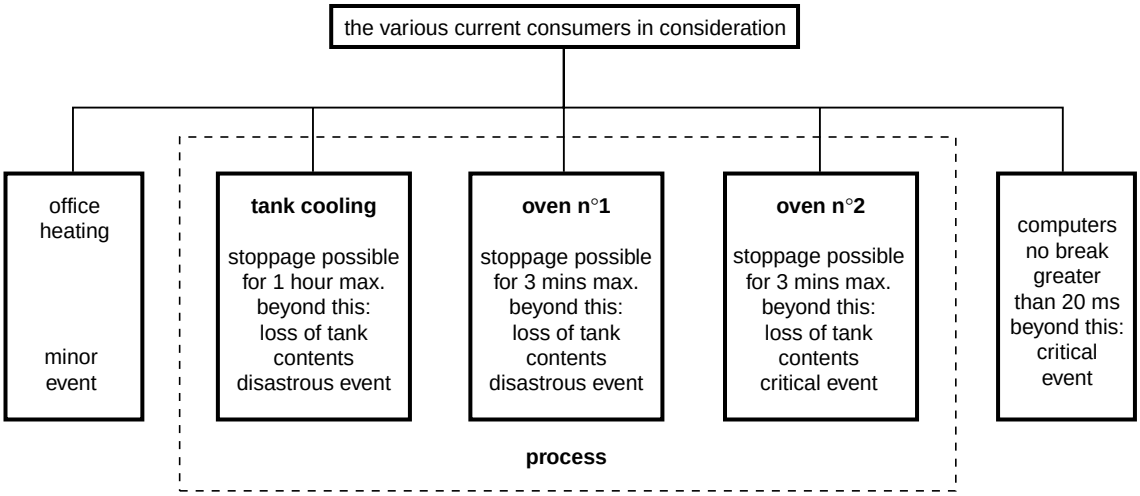


fig. 13: the availability specifications to be provided by the customer.

Faced with the questions: where, to supply what, what is the criticality and the admissible down time, the customer must think in terms of, for example, safety and loss of production or information.

■ the risk:
for an insurance company the idea of risk corresponds to the seriousness (moral, social or economic) of the event in question. In terms of loss of production, the estimate of the risk is quite simple: the product of the probability of the occurrence and the cost of an event gives a good idea of criticity. The assessment of the risk enables the price to pay to be calculated: loss of profits, insurance or optimised electrical installation.

■ formalising of requirements
(see fig. 13): a means of expressing the requirements involves classifying the various current consumers according to the down time that they can withstand (none, a few seconds, a few minutes, a few hours).

functional analysis of the system

Functional analysis describes in both graphical and written terms the role of the network and/or its constituent parts.

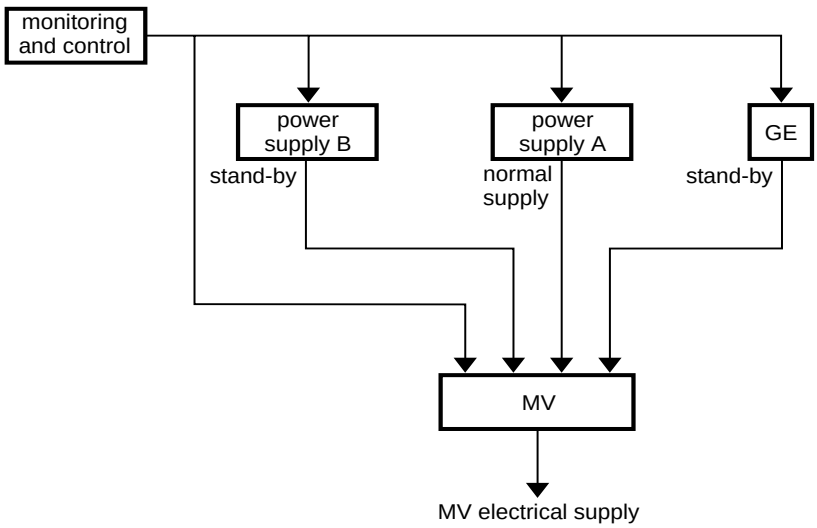


fig. 14: functional block diagrams.

This analysis leads to two complementary descriptions of the network:

■ one description using functional block diagrams (see fig. 14), whose aim is to present the system configuration and the functional links between the various parts of the system.

■ a behavioural description (see fig. 15) whose aim is to describe the sequence of the various possible states.
The main purpose is to identify the events that induce the system to change. The model developed during the course of this analysis notably

highlights the various reconfiguration points in the system.

This second analysis enables account to be taken of functional aspects when they interact with malfunctional aspects.

failure mode analysis

This analysis aims to provide:
■ the list of possible failure modes for each of the items identified in the functional analysis,
■ their causes of occurrence (one cause is enough),
■ the consequences of these failures on the system (also called single events),
■ the failure rate associated with each failure mode as part of a quantitative study.

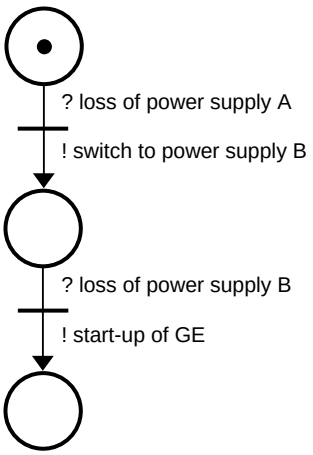
The results are presented in table form (see fig. 16).
This analysis can be considered as the first stage of modelling.

reliability data

As part of a quantitative analysis, it is necessary to have probability data for the failure of the system's equipment.
The probability characteristics are then combined with the failure modes.
These are:
■ the failure rate and how it is broken down according to the failure mode,
■ the average time to repair associated with the frequency of preventive maintenance (see fig. 17).

Failure rates

Remember that this involves quantifying the probability that there will be a failure between [t, t+dt], knowing that there has been no failure before t.
Schneider Electric has a database built up from several sources:
■ internal studies and analysis of equipment returned to the factory after failure,
■ failure statistics observed by utilities companies and other manufacturers,
■ reliability data,
□ for non-electronic components:
- IEEE 500 (feedback of experience from nuclear power stations in the USA),



This Petri network expresses the fact that in the case of loss of power supply A, the network is switched to the power supply B. If power supply B fails, then the GE start-up.

fig. 15: behavioural description in the form of a Petri network.

functions	failure mode	causes	effects on the system
power supply feeder	loss of normal mode	■ power supply failure ■ transformer failure ■ spurious circuit breaker tripping	switch over to stand-by
stand-by	loss of stand-by mode in operation	■ failure of GE in operation ■ spurious circuit breaker tripping ■ transformer failure	loss of electricity supply
	normal mode failure and stand-by mode is not available	■ GE does not start up ■ circuit breaker is blocked open	

fig. 16: failure mode analysis.

equipment	failure mode	failure rate	time to repair, frequency of preventive maintenance
circuit breaker	■ blocked closed ■ spuriously open	λ_1 λ_2	μ_1, —
generator set	■ failure in operation ■ failure on start-up	λ_4 λ_5	μ_2, 6 months
transformer	■ failure in operation	λ_6	μ_3, X months

fig. 17: fictive summary of the reliability data required for a study.

- NPRD91 (feedback of experience from military and non-military systems in the USA),
□ for electronic equipment, the data is generally obtained by calculation from the Military Handbook 217 (F) or from reliability data from the National Centre for Telecommunications Studies.

Some components have a constant failure rate (λ) over time throughout a period of their life. In other words the probability of failure is independent of time ; this is the case of electronic components (exponential law). Electrotechnical components age, or in other words their failure rate is not constant over time. Data most commonly available supposes constant rates.
The use of data that is non-specific to the system being studied and of constant failure rates even if certain components age is, nonetheless, very attractive since it enables valid comparisons to be made between systems.
The fact of finding a configuration that is 10 times more reliable than another, 10 times more available ... means that this configuration is ten times better for the criteria in question ; the relative value is often more important than the absolute value.

Schneider Electric's reliability database has the aim of gathering together as much data as possible. Validity criteria have been set up to guarantee the quality of the data included. We ensure:
■ the way that feedback of data was carried out, on what data it was based,
■ the preliminary calculation method used, the conditions of use, temperature, environment, etc
In time, this work provides us with reliability data to study any installation or to be able to obtain them by extrapolation.

The mean times to repair
depend mainly on the company's maintenance policy. Decisive choices notably include the possibility of inventory, the times when the repair teams are present, the frequency of preventive maintenance, the type of maintenance contract with suppliers, etc.

The impact of the variation of these maintenance policy-based parameters on the system's performance level can be dealt with by a specific analysis.

Functional reconfigurations
In the instance of functional reconfigurations, when functional aspects interact with those that are malfunctional (e.g. in the case of tariff based load shedding) the frequency of these reconfigurations is included in the modelling process.

modelling

The malfunctioning of the network is represented by a model. The model is a graphical representation of the combinations of events determined by the analysis of failure modes which, for example, contribute to the loss of electrical supply for certain current consumers and to their repair procedures.
This model enables:
■ discussions with the customer to validate our understanding of the way the network malfunctions,
■ qualitative analysis of the network performance levels, by the search for common modes, of the simplest combinations which contribute to the event in question,
■ assessment of the network's performance levels by calculating dependability criteria.
Various techniques are available according to the configuration of the system being studied, the undesirable events in question, the criteria to be

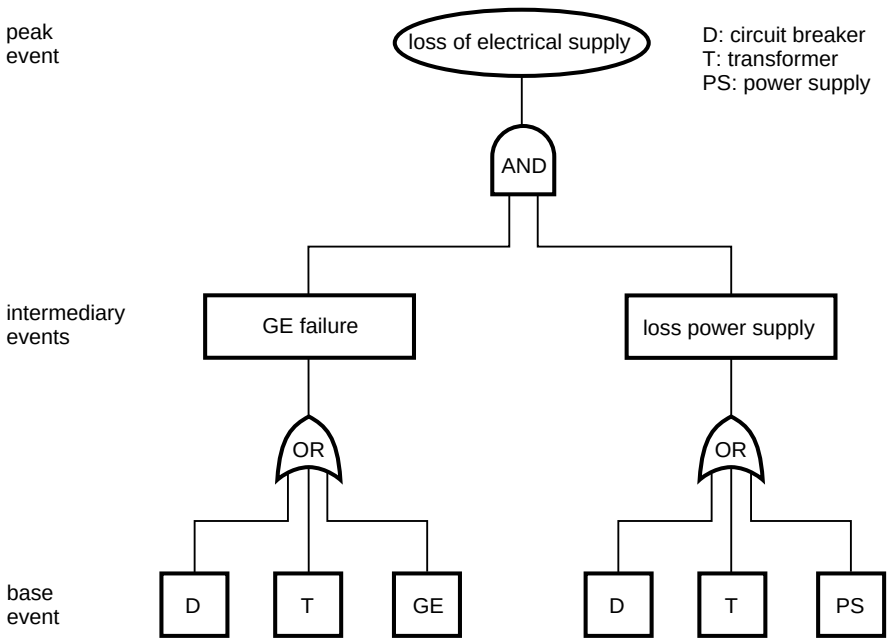


fig. 18: fault tree modelling. The fact that the GE failure only makes sense if there is loss of EDF supply does not initially appear.

assessed and the assumptions taken account of in the model(s).

The main modelling techniques

■ combination:
the combining of single events.
This is the case of fault tree diagrams (see fig. 18).
A fault tree diagram breaks down events into single events.
The immediate causes of the loss of electrical supply are therefore sought, these are intermediary events.
The causes of these intermediary events are then sought in turn.
The break-down continues in this way until it becomes impossible or until it serves no further purpose.
Terminal events are called basic events.
The breaking down of an event into causal events is performed using logical operators or so called gates (the AND gate, the OR gate).
The fault tree diagram in figure 18 expresses the fact that in the given network, there is a total loss of electrical power if there is a loss of «power supply» and loss of the «generator sets».
In this type of modelling exercise, no account is taken of the fact that the failure of the generator sets is only significant if there is loss of «power supply» beforehand.
Networks with reconfiguration possibilities and complex maintenance strategies are difficult to model using the fault tree method.

■ combination and sequential:
the combining of single events whilst taking account of the moment in time when the events occur.

□ Markovian type (see fig. 19).
This type of model is commonly represented by a graph that shows the various possible states in the system.
The arrows that link the system states are quantified by rates, which can be the failure rates, the repair rates or the representative operating mode frequencies.
These rates represent the probability that the system changes status between time t and t+dt.
The graph in figure 19 shows the fact that the system can have any one of four operating status:
- status 1: correct operation,
- status 2: failure of «power supply» and the generator sets have started up,
- status 3: failure of «power supply» and the generator sets have not started up,
- status 4: when the generator sets have failed in operation with the power supply also failed.

Markovian modelling assumes that the frequencies (or rates), which enable passage from one status to another, are constant.
The calculating algorithms associated with this modelling technique can only be applied under these conditions.
This limit leads us to make assumptions and therefore to represent the reality of the situation to a greater or lesser extent.

□ other types.
The procedure used is generally that of a Petri network.
The network is represented by places, transitions and tokens.
The crossing of a transition via a token corresponds to a possible functional or malfunctional system event.
These transitions can be associated with any type of probability law.
Simulation is the only way to enable calculations to be resolved.

λ_a: frequency at which there is loss power supply
λ_b: frequency of GE failure
μ: frequency of repair

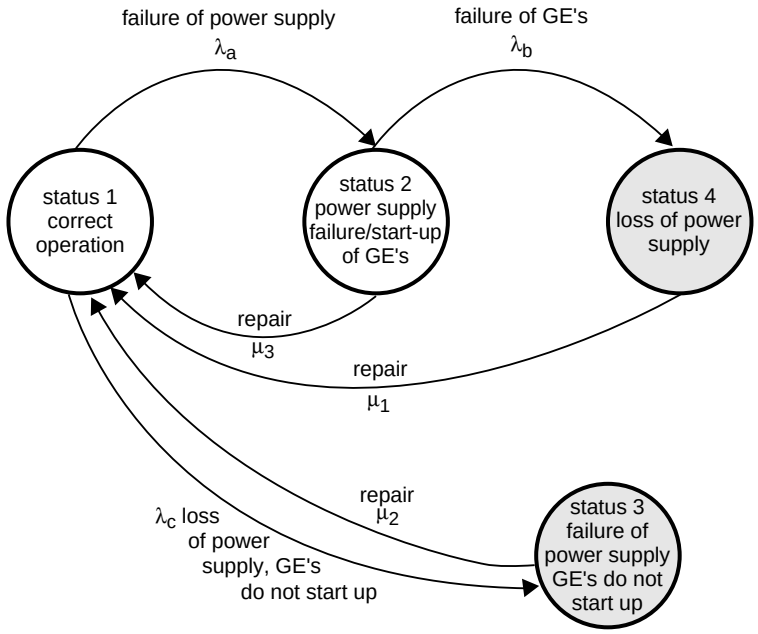


fig. 19: modelling of malfunctions in the form of a Markov diagram λ_a, λ_b and μ are assumed to be constant.

The Pétri network in figure 20 represents the various failure modes that the system may be subject to:
- associated with transition n°1 is the probability of «power supply failure»,
- associated with transition n°2 is the probability of the starting up and the non starting up of the generator sets,
- associated with transition n°3 is the probability of failure of the generator sets in operation.

Criteria used to select a modelling type:

figure 21 shows these modelling techniques in table form.

dependability criteria assessment calculations

Two different techniques can be used.

■ analytical resolution:

□ for states graphs,

□ for fault tree diagrams.

When systems are large or complex, analytical resolution may be impossible.

■ system component behaviour simulation (operation or failure):

□ for Petri networks,

□ for fault tree diagrams.

To achieve accuracy, a large number of simulations must be carried out and the calculation time may be prohibitive if the measurement estimate is related to rare events.

The modelling of a system using a Petri network is the model most closely representing the actual operation of the system being studied. But in view of the limits related to simulation, this technique is not systematically used.

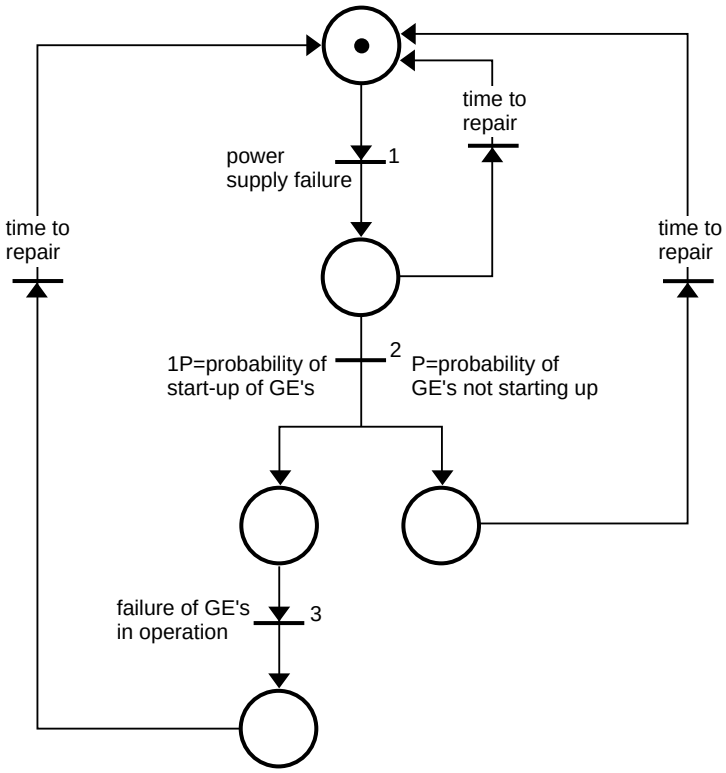


fig. 20: modelling using a Petri network.

selection criteria	fault tree diagram	Markov graph	Pétri network
interaction of the operating mode in modelling	resolution impossible or false depending on the algorithms used	under certain conditions, resolution can be impossible or false depending on the algorithm used	suitable
numerical dispersion of data	resolution impossible or false depending on the algorithms used; no problem if simulation	under certain conditions, resolution can be impossible or false depending on the algorithm used	suitable
the timing of the failures is important	no	suitable	suitable
estimate involving rare events	simulation time which can be prohibitive, no problem in the case of analytical resolution	suitable	simulation time which can be prohibitive
estimate of:			
■ MUT	-	suitable	suitable
■ MTTF	suitable	suitable	suitable
■ D(t)	-	suitable	-
■ D(∞)	suitable (analytical calc.)	suitable	suitable
■ average D at t	suitable (simulation)	-	suitable
■ MTTR	-	suitable	suitable
■ λ_{eq}	-	suitable	suitable

fig. 21: criteria used to select the type of modelling used.

3. examples of studies

comparing two electrical network configurations in a factory

■ presentation of the factory:
A drinking water production plant supplies 100 000 m^3/day at off peak times, 300 jours/year and 200 000 m^3/day at peak times, 65 days a year.
Production of water is performed using 4 production plants, each capable of supplying 100 000 m^3/day.
Each plant is associated with six types of current consumers : R_1, R_2, R_3, R_4, R_5 and R_6 (pumps, disinfectors, etc.) which must work simultaneously in order to ensure production (ref. fig. 22).
The current consumers ensuring the operation of each plant can be distinguished in the following manner:
R_{1a},..., R_{6a} for plant n° 1
R_{1b},..., R_{6b} for plant n° 2
R_{1c},..., R_{6c} for plant n° 3
R_{1d},..., R_{6d} for plant n° 4
To ensure operation at off-peak times, only one plant is required ; during peak times, two plants are required.

■ analysis of the enquiry, the requirements
After two meetings with the customer, the specialists have determined:
□ that the following was required:
- a proposal for a new LV electrical network configuration, the configuration of the MV (5.5 kV) should change very little,
- proof that the proposed layout was at least as good as the old in terms of certain dependability criteria.
□ that the dependability criteria to be assessed were:
- the probability of simultaneously losing electrical supply to current consumers n°1 and n°6,
- the probability of losing electrical supply to current consumers n°3.

■ functional analysis
General considerations concerning the network operation:
□ the site is supplied by two independent power supply feeders. Two generator sets are there on stand-by in the case of failure of the power supply feeders,
□ in normal operation, the site is supplied by the power supply feeder A. If this feeder fails, then the system switches to power supply feeder B. If both power supply feeders fail, the generator sets start up,
□ there are two levels of production, off-peak and peak. In the case of peak production, the power of the generator sets is not sufficient to ensure production.
□ the power supply split between current consumers is such that the availability is

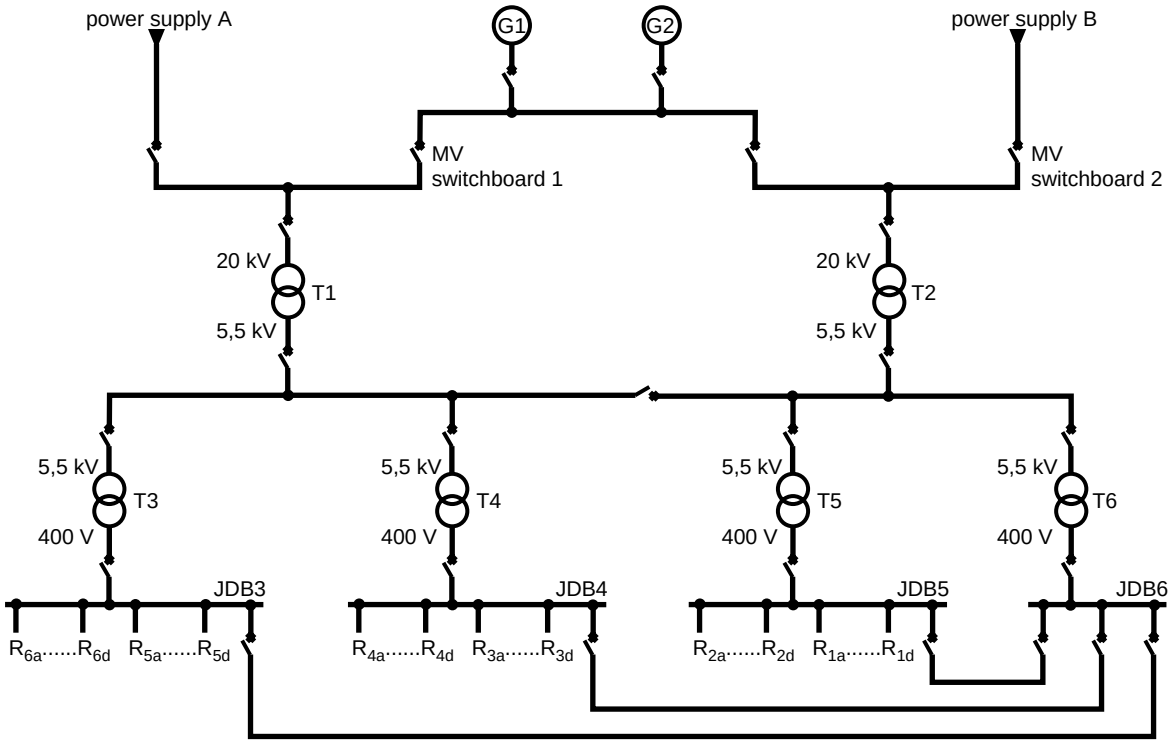


fig. 22: functional diagram of the original installation. Certain penalising common modes are not shown.

not very good. Thus, for example a fault on the busbar JDB3 knocks out all current consumers of type R_5 and R_6. Production is stopped and no other plant can operate,

□ the existing electrical network was such that that there were common mode busbars. A short circuit across these busbars made any reconfigurations inoperative.

The probability of a busbar short circuit is low, but since the system had high reconfiguring possibilities this failure mode becomes preponderant. The common modes occur at coupling level, during reconfigurations involving transformer T4.

□ for the new network, the current consumers have been separated so that it is possible to supply off-peak demand with the current consumers associated with one single transformer and peak demand with the current consumers associated with two transformers.

Figure 23 presents the proposed network layout and figure 24 its functional analysis.

■ results analysis

The improvement in results obtained with the proposed network is highlighted by giving the improvement ratios, with the existing network being used as a reference.

Besides the probabilities of the simultaneous loss of current consumers 1 and 6 and the loss of current consumers 3, we have assessed their frequency of loss. Also calculated : the optimum maintenance frequency for the generator sets and the contribution of the MV and LV networks to the undesirable events.

Here are the obtained improvements :

□ on the relative probability of simultaneously losing supply to current consumers n° 1 and 6:

- off-peak operation 110
- peak operation 55
- overall 105

□ on the relative probability of losing supply to current consumers n° 3:

- off-peak operation 99
- peak operation 54
- overall 97

Overall, the probability of losing electrical supply to current consumers n°1 and 6 is 100 times greater with the old network than with the proposed network. Indeed, in the old network, there are failures that contribute directly to the loss of electrical power supply.

If this system only worked in off-peak conditions, this ratio would be virtually the same since the system works mostly in off-peak conditions, thus explaining its preponderance in the overall result.

If the system only works in peak conditions, it is around 50 times more probable to lose electrical supply to current consumers 1 and 6 with the old network. In the case of peak conditions, it is MV related faults that predominate and this part of the network cannot be changed very much.

□ on the frequency of loss of supply to current consumers n°1 and 6:

- off-peak operation 22
- peak operation 21
- overall 21

□ on the frequency of loss of supply to current consumers n°3:

- off-peak operation 18
- peak operation 21
- overall 20

The improved performance of the new network is less pronounced in terms of frequency of failure.

Calculation parameters used in a probability of unavailability are the frequency of failure and the time to repair. The failures which directly contribute to the loss of power have an effect on the unavailability time which is proportional to their time to repair.

The new network makes it possible for background preventive maintenance to be carried, in other words without interrupting the plant's normal operation.

■ additional assessments

It seemed interesting to assess some additional criteria to compare the two configurations.

□ the relative probability of losing peak operating conditions

In the case of peak operating conditions, the economic stakes are high. The criteria assessed above do not measure this risk. It is entirely feasible to lose peak production even with current consumers 1, 6 and 3 supplied power.

The probability of losing peak operation is four times less with the new network. The improvement is less pronounced than the other calculated criteria, since the main failures occur in the MV part which remains unmodified.

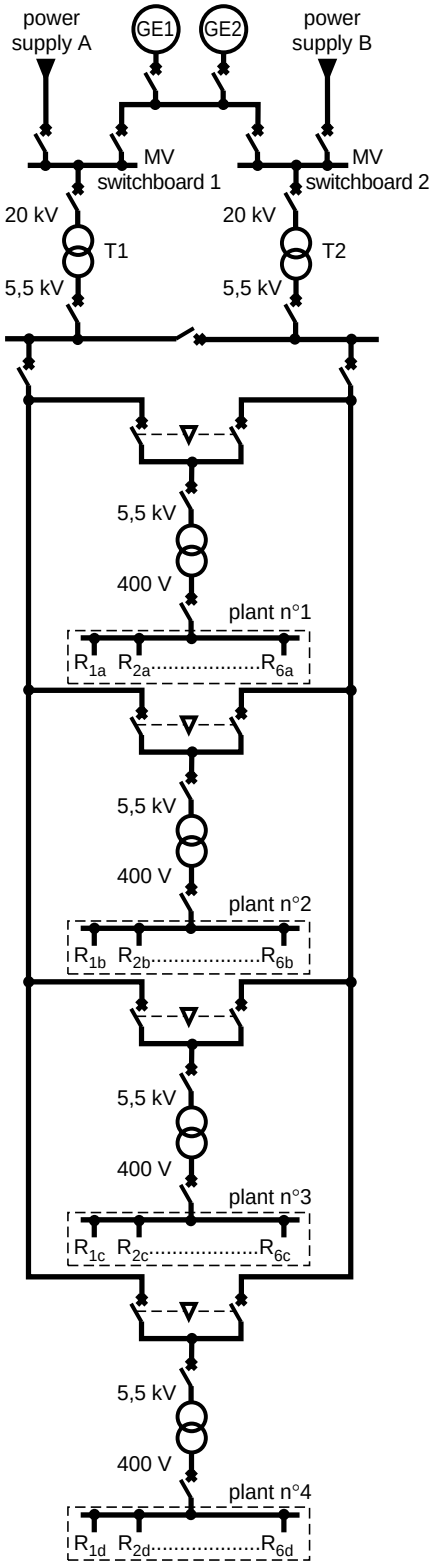


fig. 23: functional diagram of the new configuration.

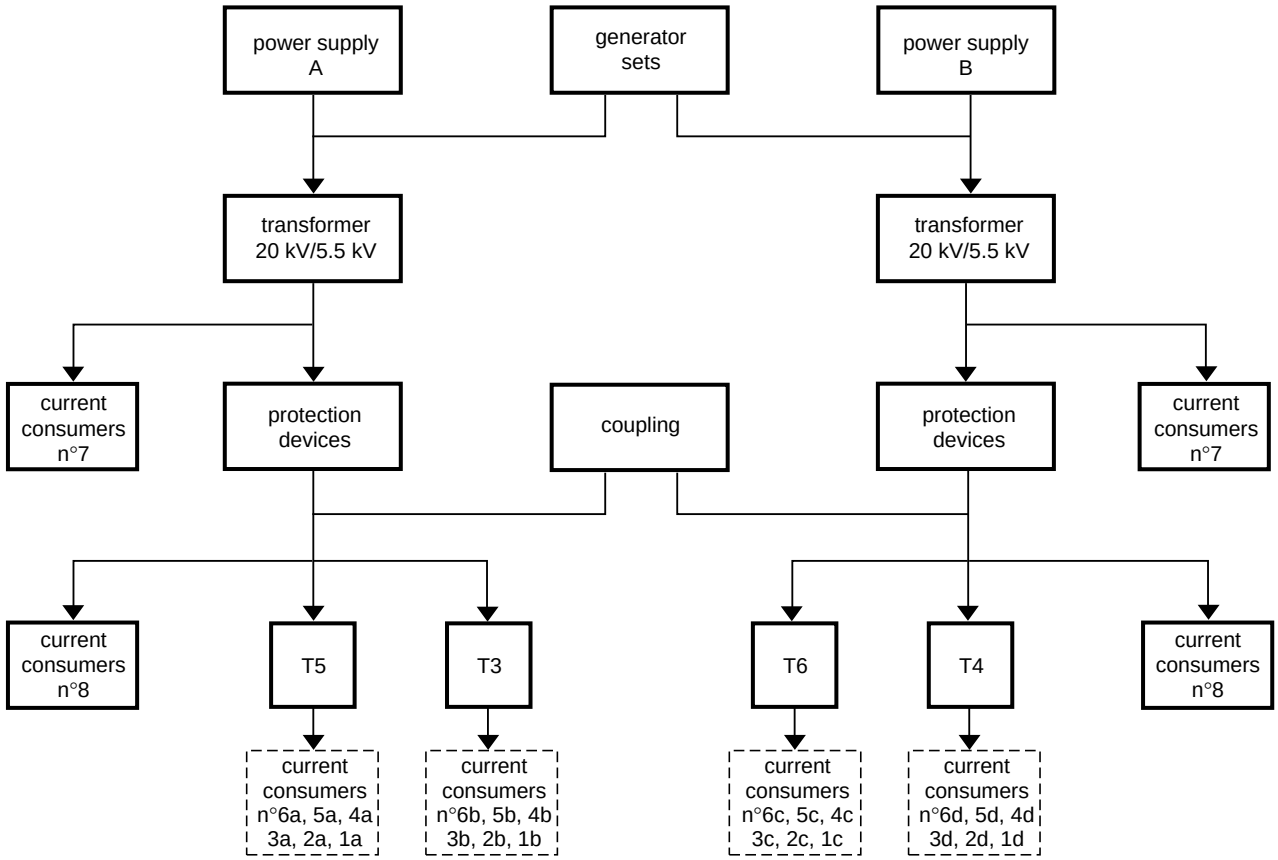


fig. 24: functional analysis of the new configuration.

□ the optimum preventive maintenance frequency

The graph resulting from the calculations (see fig. 25) shows the impact of preventive maintenance frequency of the generator sets on the probability that they will be available when they are required.

For a maintenance frequency of 6 months, the graph shows that there is a trough in the probability of unavailability in the event of a loss of power.

□ contribution of the MV and LV parts to the undesirable events for the proposed network.

The MV part has a much higher contribution than the LV part (around 99.9% compared with 0.1%).

Since the MV network has not been modified, its preventive maintenance must be optimised ; moreover, it would be greatly preferable to have a quality monitoring and control system on the MV network.

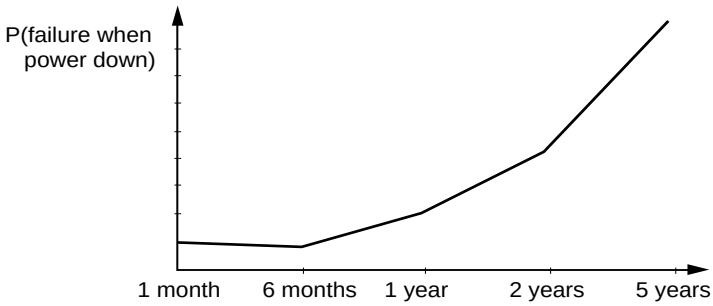


fig. 25: unavailability of a generator set when power is down as a function of the periodicity of maintenance.

the interest of remote monitoring and control in an EHV substation

■ analysis of the enquiry, the requirements

Schneider is carrying out preliminary dependability studies as part of an export monitoring and control offer for an EHV substation. The following preliminary study had to determine which configuration would enable the achievement of dependability objectives that had been set by the customer in terms of the loss of monitoring and control.

The objective was to determine whether it was necessary to incorporate a stand-by remote work station.

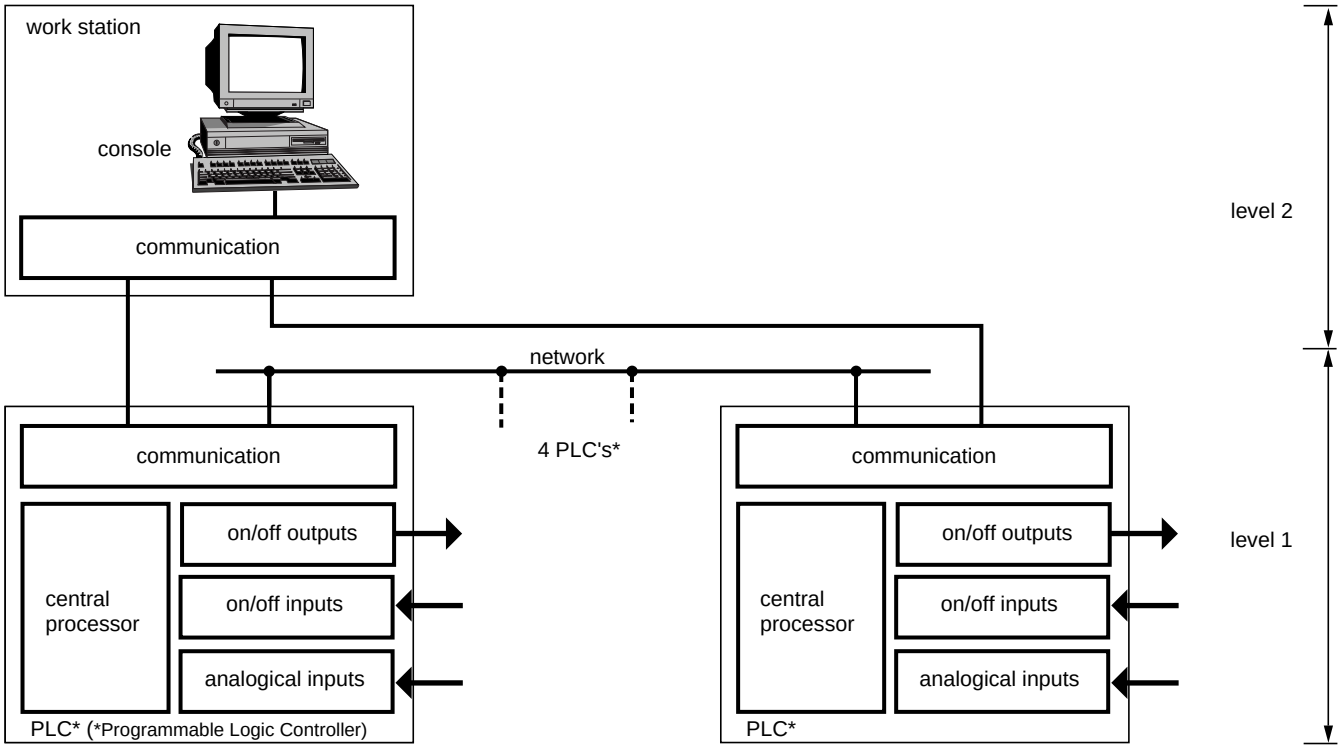


fig. 26: base monitoring and control configuration of an EHV substation.

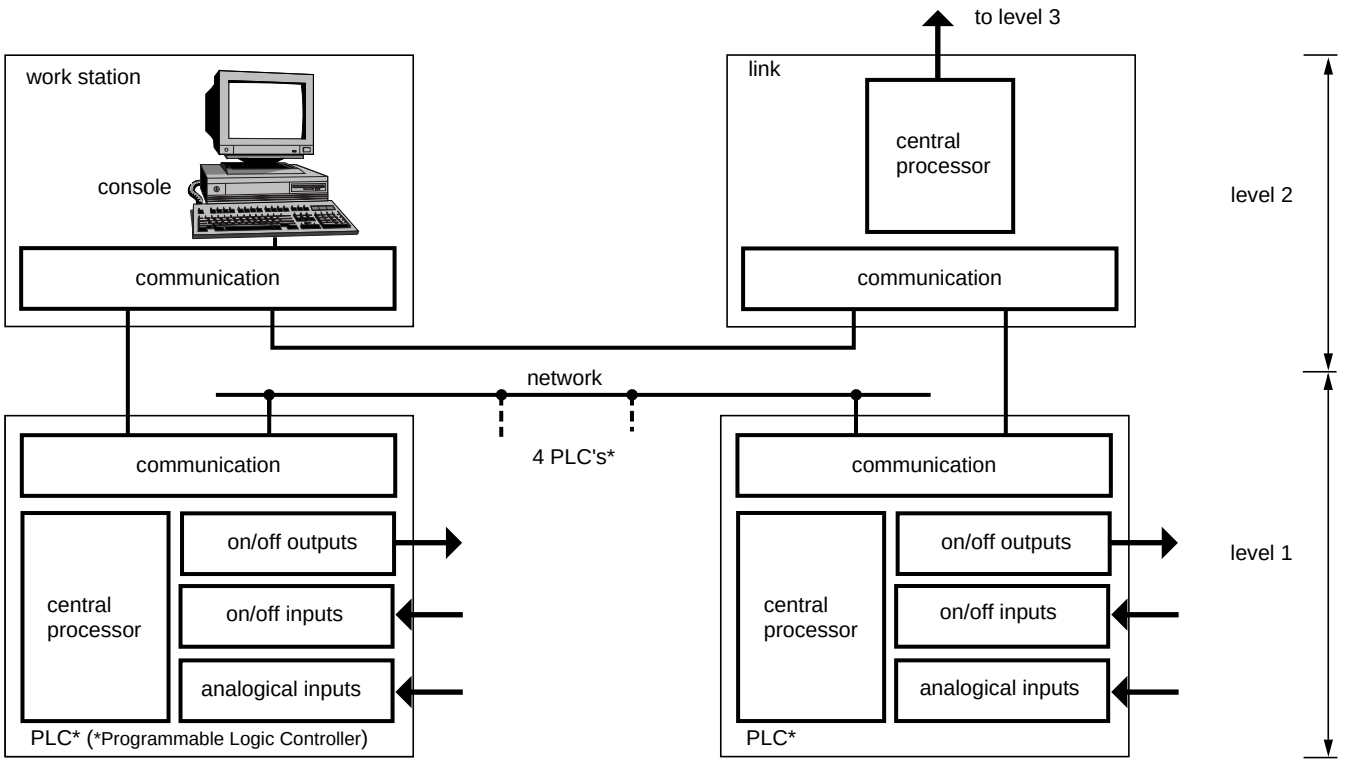


fig. 27: monitoring and control configuration of an EHV substation with access and remote work station.

■ functional analysis
The monitoring and control of the EHV substation in question includes:
□ four plc's which acquire datas on the status of the substation's electrotechnical equipment and which pass on the control orders (level 1),
□ a work station enabling visualisation of the substation's status and the sending of control orders (level 2),
□ and possibly, a remote work station.
The remote workstation is therefore on stand-by with respect to the substation's own work station.
Figure 26 shows the basic solution corresponding to one single level 2 work station.
Figure 27 shows the solution with a link to a remote work station.

■ results analysis
the selected monitoring and control system must have a probability of unavailability of less than 10^{-4} at t=1200 hours. This means the equipment must be non-functional for less than 7 minutes over 1200 hours of operation (50 days).
The undesirable event - loss of monitoring and control - has been broken down into three undesirable events corresponding to calculations of:
□ the probability of totally losing monitoring and control (common mode),
□ the probability of losing at least on/off information,
□ the probability of losing at least analogic information,
or in other words three calculations for each configuration.
The equipment is divided into two classes:
□ equipment for which we have replacement parts (n),
□ equipment for which we do not have replacement parts (s).
Two calculations are performed for each undesirable event, to show the impact of the choice of the average repair time on the end result (see fig. 28).
Hypothesis 2 is the most realistic one; it is these times that will be taken into account to choose between the two solutions.

	MDT for equipment of type n	MDT for equipment of type s
hypothesis 1	1 hour	3 hours
hypothesis 2	4 hours	12 hours

fig. 28: two hypotheses for the average time to repair.

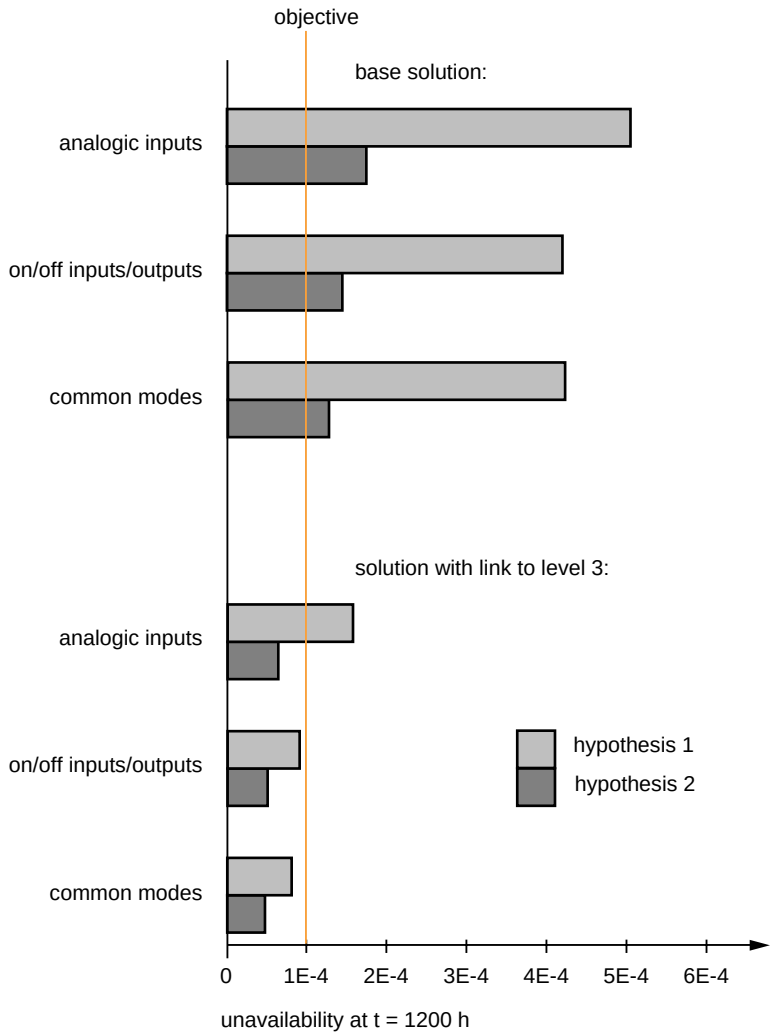


fig. 29: bar chart of the unavailability of the two solutions (the orange line corresponds to the objective to be achieved, it is achieved if the bar chart is to the left of the line).

As figure 29 shows;
□ the solution without the remote station does not enable the required availability to be achieved,
□ the solution with remote monitoring and control enables the objectives to be achieved for on/off inputs and the common modes ; but the probability of losing at least one analogic input remains greater than the target objective.

4. dependability tools

dependability study packages

Certain tools automatically generate a dependability study from the functional analysis of the system and the failure modes of its components.
A model is generated which enables evaluation of the dependability criteria.
These tools are useful for complex systems and/or repetitive systems.
They enable a database to be created on the failure modes of the components and on the consequences of these failures when possible. (see. fig. 30).

modelling tools

Two types of tools (see. fig. 31):
■ simulation tools,
■ analytical calculation tools.
Comment: a Markov graph can very easily be transformed into a Pétri network and be used for simulation. As opposed to a Pétri network, a graph can be associated, but in this case the transitions must be «Markovised»: in a Markov graph the frequency of occurrence of the transitions are necessarily constant.
Schneider currently has a PC graphical interface called PCDM which automatically generates the file defining the Markov graph or the Pétri network that has been drawn (ref. fig. 32).
This provides time savings and improved reliability of data entry.
The Petri network modelling technique is that which currently best approaches the real behaviour of the system. The acceleration of the simulation of Petri networks, notably using MOCA-RP software, is the subject of a thesis whose initial findings have been presented at the ESREL 96 congress (European Safety Reliability).
In the near future, the use of Petri networks will no longer be limited by the simulation time they require.

tool name	modelling technique	calculation resolution technique	main features
Adélia	fault tree	■ analytical ■ simulation	tool developed by Schneider Electric to model the malfunctions in electrical network components. It integrates an electrical network malfunction database. The description of the network and of the undesirable event automatically generates the corresponding fault tree.
Sofia	fault tree	■ analytical (logical polynomial)	tool developed by SGTE Sofrenten. Automatic generation of a fault tree and associated FMEA, by a functional description of the system and the creation of an associated malfunction database.

fig. 30 : two types of tools regularly used by Schneider Electri for dependability study.

modelling type	simulation tool	analytical calculation tool
Markov graph		**super Cab** developed by ELF AQUITAINE
Petri network	**MOCA-RD** developed by Microcab	

fig. 31: the modelling tools.

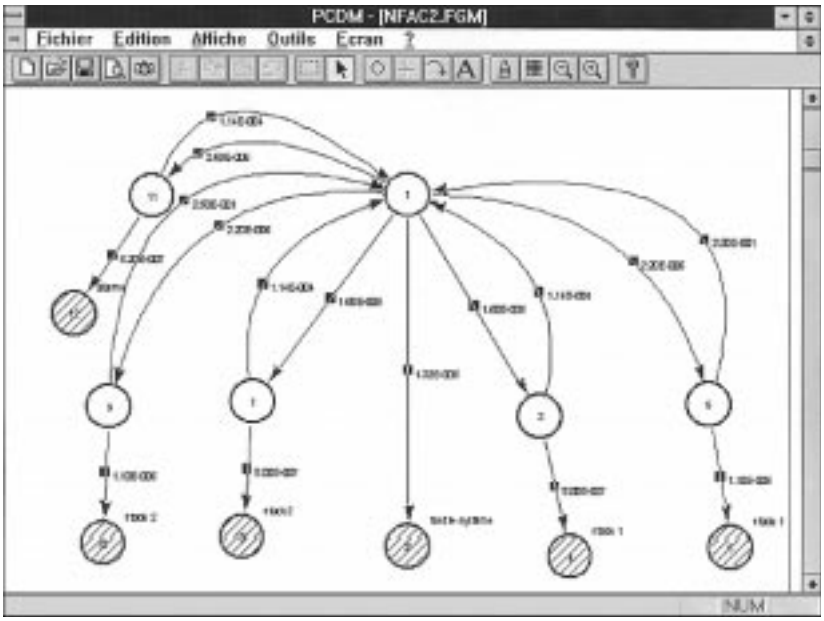


fig. 32: PCDM graphical interface - Markov graph.

5. conclusion

Dependability can be broken down in terms of:
- safety,
- reliability,
- availability,
- maintainability.

Safety requirements initially imposed dependability studies on hazardous applications : rail and air transport, nuclear power stations, etc. If we add the requirements of reliability, availability and maintainability, many other sectors are concerned.

Requirements have progressed in terms of quality of electricity supply. Taking account of the considerable improvements that have been made in methods and equipment, users are entitled today to demand a high level of availability.
To achieve this objective with justified confidence, dependability studies are necessary.

They enable optimisation of
- the configuration of the electrical network,
- of the monitoring and control system,
- of the maintenance policy.

They enable solutions to be chosen that are tailored to achieve the required availability threshold as cost effectively as possible.
Often the study can be limited to a key point in the installation, responsible for the major part of the global unavailability.

In many cases, it is interesting to call in a specialist. The advice they may provide could prove decisive.

bibliography

Standards

■ IEC 50: International electrotechnical vocabulary - general index.

■ IEC 271/UTE C 20310: List of basic terms, definitions and related mathematics for reliability.

■ IEC 300: Reliability and maintainability management.

■ IEC 305/UTE C20321 à 327: Characteristics of string insulator units of the cap and pin type.

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

■ IEC 671: Periodic tests and monitoring of the protection system of nuclear reactors.

■ IEC 706/X 60310 and 60312: Guide on maintainability of equipment.

■ IEC 812/X 60510: Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA).

■ CEI 863/X 60520 : Prévision des caractéristiques de fiabilité, maintenabilité et disponibilité.

■ IEC 880: Software for computers in the safety systems of nuclear power stations.

■ IEC 987: Programmed digital computers important to safety for nuclear power stations.

■ IEC 1165: Application of Markov techniques.

■ IEC 1226: Nuclear power plants ; instrumentation and control systems important for safety ; classification.

■ NF C 71-011 : Sûreté de fonctionnement des logiciels - Généralité

■ NF C 71-012 : Sûreté de fonctionnement des logiciels - Contraintes sur le logiciel.

■ NF C 71-013 : Sûreté de fonctionnement des logiciels - Méthodes appropriées aux analyses de sécurité.

Miscellaneous publications

[1] «Fiabilité des systèmes»
A. Pagès et M. Gondran
Eyrolles 1983

[2] «Sûreté de fonctionnement des systèmes industriels»
A. Villemeur
Eyrolles 1988

[3] Recueils de données de fiabilité :

■ Military Handbook 217 F
Department of Defense (US)

■ Recueil de données de fiabilité du CNET(Centre National d'Etudes des Télécommunications)
1993

■ IEEE 493 et 500 (Institute of Electrical and Electronics Engineers)
1980 et 1984

■ IEEE Guide to the collection and presentation of electronic sensing component, and mechanical equipment reliability data for nuclear-power generating stations

■ Document NPRD91 (Nonelectronics Parts Reliability Data)
du Reliability Analysis Center
(Department of Defense US)

1991

[4] Recommandations:

■ MIL-STD 882 B

■ MIL-STD 1623

Merlin Gerin Cahier Techniques

■ Méthode de développement d'un logiciel de sûreté
Cahier Technique n° 117 -
A. JOURDIL et R. GALERA 1982

■ Introduction to dependability design,
Cahier Technique n° 144
P. BONNEFOI

■ Sûreté et distribution électrique
Cahier Technique n° 148 - G. GATINE

■ High availability and LV switchboards,
Cahier Technique n° 156
O. BOUJU

■ Automatic transfering of power supplies in HV and LV networks
Cahier Technique n° 161
G. THOMASSET

■ Energy-based discrimination for LV protective devices,
Cahier Technique n° CT167
R. MOREL, M. SERPINET

■ Dependability of MV and HV protective devices,
Cahier Technique n° 175
M. LEMAIRE

Schneider's participation in various working groups

■ statistical group of IEC committee 56 (reliability standards),

■ software dependability with the European EWICS-T7 group : computer and critical applications,

■ groupe de travail de l'AFCET sur la sûreté de fonctionnement des systèmes informatiques,

■ participation à la mise à jour du recueil de fiabilité du CNET,

■ IFIP working group 10.4. Dependable computing.

Real.: Sodipe - Valence
DTE - 09-97 - 1500 - Printing: CLERC