10

USE OF EQUIPMENT BUILT-IN AUTOMATIC TESTING, SELF-CHECKING AND MONITORING WITH A VIEW TO IMPROVING RELIABILITY

Study Committee 34 (Protection)

J. GANTNER (Reporter)

October 1986

USE OF EQUIPMENT BUILT-IN AUTOMATIC TESTING, SELF-CHECKING AND MONITORING WITH A VIEW TO IMPROVING RELIABILITY

Study Committee 34 (Protection)

J. GANTNER (Reporter)

with the help of the Working Group

F. Andersson (Sweden), M. Coudray (France), J.P. Lamy (Belgium),
H. Hartmann (Federal Republic of Germany) S. Pettissalo (Finland)

C O N T E N T

1. Introduction (Dependability versus security)

1.1 Principal considerations regarding reliability

The increasing sizes of power networks with increasing transfer of energy and fault current levels have stressed the importance of reliable fault clearing. Great care is taken in circuit design, selection of components, careful production and quality control to assure reliable fault clearing. Nevertheless components in the fault clearing chain will degrade by time or fail suddenly and cause either failure to operate or incorrect operation.
In this study, and in particular in the calculations of chapter 5, the values characterising reliability will include all components of this chain, i.e. also CT's, PT's, auxiliary power sources, trip circuits etc.

Due to the different failure modes - failure to operate and incorrect operation - the fault clearing chain reliability must be divided into dependability and security. The reliability measure, dependability, indicates the ability to perform the requested fault clearing. Security on the other hand indicates the security against incorrect operations (see also chapter 7).

Dependability and security are contradictiory to each other, and a gain in one of the qualities can result in a loss in the other.

The reliability of the components in the fault clearing chain in the new condition is given by the manufacturer. The reliability will however gradually decrease by the time due to degradation of various types. The degree of reliability can be maintained by testing, monitoring and selfchecking and adequate repair when faults or changes are detected.

By different design of the protective scheme utilizing redundant protections the dependability or security can be controlled.

1.2 Power system redundancy

Power systems can, from a reliability point of view, be classified in networks with and without redundancy.

In a network with redundancy at least one network element can be lost and still the necessary power can be generated, transmitted and distributed. A network with a spinning reserve generation for the greatest production unit in operation is an example of full primary redundancy. In a strongly meshed network it may be admissible to lose one or two lines without resulting in network breakdowns or loss of energy to any consumer.

Pure radial networks are examples of the other extreme - a network without any redundancy. There, a loss of a network link like a line will cause an interruption of the power supply to some customers.

Between the two extremes, full and no redundancy, all degrees of primary redundancy will be found in practice. In a network, the degree of redundancy will in general be different for the different parts and elements like lines, generators, transformers and busbars. The degree of primary redundancy will furthermore vary with the load and generation. This means that a meshed network will normally have a very high degree of redundancy at low load operation, so long as no link is out of operation.

The degree of redundancy will decrease with an increase in load, and at peak load the redundancy will normally only cover the loss of one single network link.

Generally a network with redundancy will be a meshed network or a radial one with parallel links, double lines, transformers etc.

1.3 Influence of network design on requirements regarding dependability and security

In a meshed network the different elements are closely tied together. This interlinking gives the network the primary redundancy. On the other hand, an electrical fault in one of the links will have an impact on the adjacent link depending on the degree of meshing. Due to this coupling a failed fault clearing in a meshed network will have very severe consequences.

It is well known that the reach and effectivity of remote back-up functions are limited by the amount of side infeed fault current. The amount of current infeed is a function of the degree of meshing. Thus, in a meshed network the back-up fault clearing will be limited with increasing degree of redundancy.

The meshed network therefore needs primarily a high degree of dependability for local fault clearing.

In a redundant network a single link may be tripped during normal operation without consequences for the consumer. It means that during normal operation, security is of minor interest in a redundant network. A sudden, instantaneous incorrect operation normally has no severe consequences.

However, during system fault conditions, an incorrect tripping of a healthy network link will result in the loss of two links, the healthy one, and the faulty one that caused the system-fault. The probability for incorrect tripping is principally higher during system fault conditions than during non fault conditions. For this reason the network must have a certain degree of redundancy that allows the simultaneous loss of two networks links. This degree of redundancy is in most cases not available during peak load conditions, but only at low load.

In meshed networks the dependability in the fault clearing function must therefore be high and has a higher priority than the security.

In a radial network a failure to clear a fault will normally not have disastrous consequences and jeopardize the whole network operation, thanks to back-up fault clearing functions. Furthermore the remote back-up functions will not be seriously limited due to current infeed effects.

An incorrect operation will cause interruption to the customer both during normal operation and system fault conditions. An incorrect operation can cause loss of generation, but this is mostly of minor importance for the network operation as the loss is taken normally care of by the spinning reserve. Generally, radial networks have no or little redundancy for the loss of lines and transformers but a higher redundancy for loss of generation.

For line and transformer protection in radial networks the security should therefore not be neglected. The dependability clearly must be high, but should not be favoured at the expense of security. Dependability and security have to be balanced in a radial network and in networks with no or a low degree redundancy.

In a non-redundant bus arrangement, tripping of a busbar, either unwanted or at a bus fault, results in a separation of all network links connected to the busbar. Such a trip will cause a "hole" in the net and heavily disturb the operation. Busbar faults can always be cleared by remote back-up functions. Hence, dependability has lower priority than security.

Busbar arrangements with 2- or 1 1/2-breakers are redundant, having two busbars. The benefit of the redundant busbars depends entirely on the dependability of clearing of busbar faults; hence, the dependability must be high. On the other hand, there is only one redundant bus and a false trip of the healthy bus at busbar fault is not acceptable. Therefore both the dependability and security must be high and should be about equal.

1.4 Dependability and security for relay schemes

When the equipment is in a new condition, the fault clearing dependability and security are basically a function of the relay and relay scheme design.

The relay design and the measuring principle determine the reliability and the degree of dependability versus security. Dependability and the security of a relay in its new condition are given to the product by the manufacturer. Reliability and the balance between dependability and security in non redundant relay schemes, is a property of the product since no additional relays are added either to improve the dependability or security.

Although there are many exceptions, particularly at HV and EHV levels, the most common relay applications consist of single protection schemes, and thus the relay manufacturers must balance dependability and security for this application. Generally, neither dependability or security are favoured to any degree (with the exception of some busbar protection design).

In a radial network security is quite important and should be about equal to the dependability. Thereby, a non redundant protection scheme will best suit such a network. To maintain the initial reliability as long as possible, testing, selfchecking and monitoring have to be used. These measures have to be directed towards both the dependability and the security, of course.

With two sets of measuring relays either the dependability or the security can be increased. When the relays are connected in parallel the two relays can perform the trip function independently of each other. In a series connection both relays have to operate simultaneously to perform the trip function.

A scheme with parallel connected measuring relays will have a very low probability for non operation and thus give a high dependability. On the other hand, the likelihood for incorrect function will be the sum of the probabilities for the two relays and thus the security will be low. Series connected measuring relays will, on the contrary, result in a low dependability and high security.

Therefore, when utilizing two sets of measuring relays in a protective scheme either the dependability or the security can be raised compared with the individual relay, depending on the connection of the two relays. When the dependability is raised by parallel connection of the relays, the security of the relay scheme will be lower than any of the individual relays. On the other hand, if the security is raised by series connection, the dependability of the total scheme is lowered.

By utilizing three measuring relays connected in a two out of three connections both the dependability and the security can be raised simultaneously. Such schemes are, in fact, considered for extremely important lines, e.g. for the interconnection between nuclear power plants and the system. In general, however such schemes can hardly be justified economically.

In meshed networks dependability will generally be favoured against security, i.e. a redundant protection scheme with two relays in parallel connection will be best. The necessary degree of security will have to be obtained by testing, selfchecking or monitoring.

Many busbar protections have two measuring relays connected in series to meet the high security. To obtain also the high dependability required (at redundant busbar installations) a parallel connection of two busbar protections may be justified. When two protections with two measuring relays each are connected in parallel the resulting scheme will have both high dependability and security due to the utilizing of four measuring relays.

1.5 Influence of testing, selfchecking and monitoring on the reliability

The probability for a maloperation in a relay protection due to a defective component is increasing with the time. Immediately after the commissioning tests the probability for such a maloperation is practically zero. It is the aim of testing, selfchecking and monitoring (definitions follow in chapter 2) to maintain the initial dependability and security. Thereby, the methods for supervision can be directed towards either dependability or security. If one of the qualities is favoured, the other one will not decrease due to the supervision action. This is unlike the effects in redundant relay schemes utilizing two relays connected in either parallel or series where an increase in one of the quality results in a decrease in the other one.

Figure 1 shows principally the influence of testing, selfchecking and monitoring in different protective schemes. In cases of redundant protections the supervision should preferably be directed towards either dependability or security, considering that the other quality is increased by the parallel or series connection of the measuring relays.

By means of automatic testing, selfchecking and monitoring the loss in security or dependability in redundant protective schemes can be compensated.

In a non redundant scheme, where both dependability and security are of equal importance the supervision has to be directed towards both dependability and security.

Testing, checking or monitoring is necessary both in non redundant and redundant schemes to maintain the initial qualities of the protection scheme.

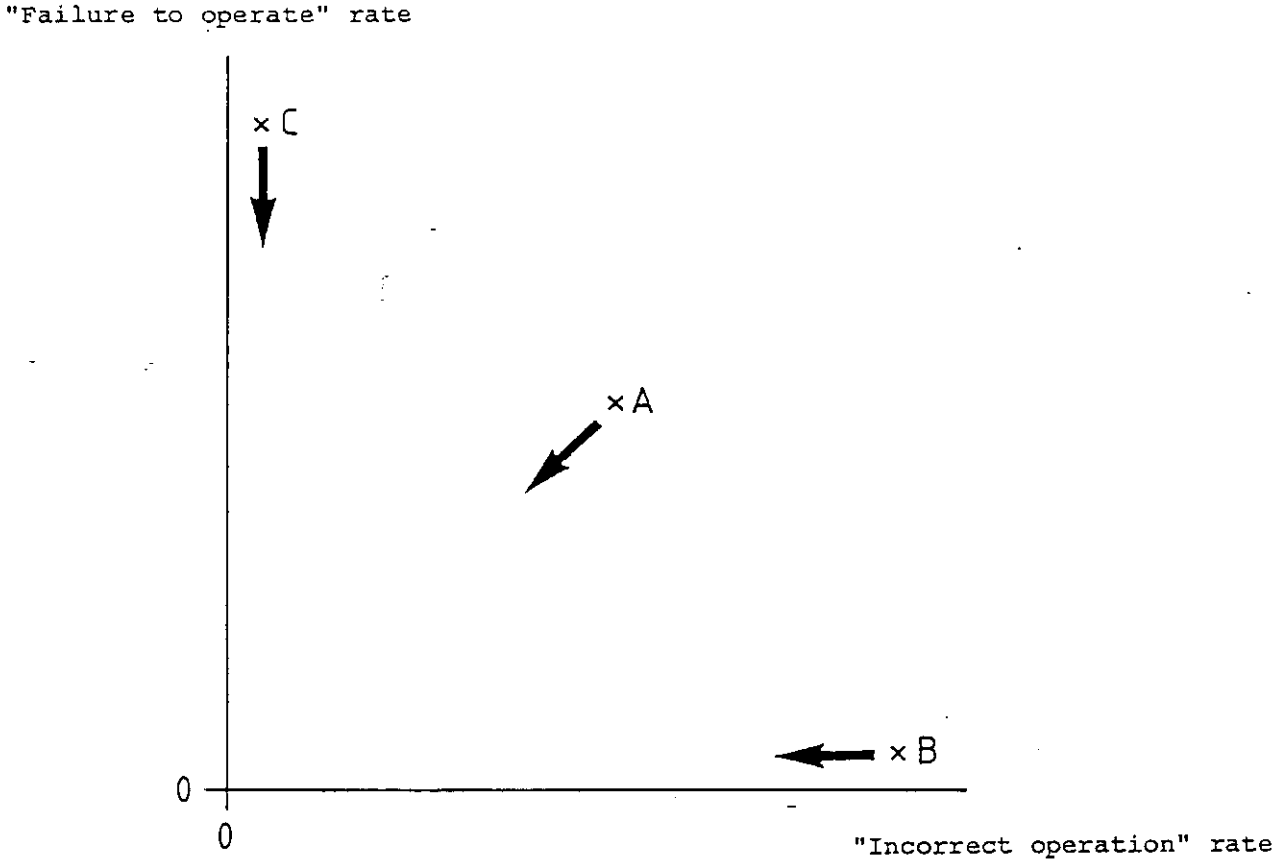


Figure 1: Influence of testing, selfchecking and monitoring on security and dependability

A Non redundant relay scheme

B Redundant relay scheme with two relays in parallel connection

C Redundant relay scheme with two relays in series connection

2. Classification of failure detection methods

Since different terms are used in the various publications on our subject a classification is given below for a consistent use in this report. The following terms are mainly based on the methods used to determine the state of the protection.

A protective scheme will reside in one of the following three states:

a) Successful state, i.e. the protection will not fail to operate nor operate incorrectly

b) Failed state such that the relay tends to restrain, i.e. it will fail to operate when it is expected to do so

c) Failed state such that the relay tends to operate, i.e. it will operate incorrectly. For the purpose of our classification it is useful to further distinguish between:

   c1) Instantaneous incorrect operation, i.e. the failure causes an incorrect operation under healthy load conditions (also called Non-system fault, section 7)

   c2) Potential incorrect operation, i.e. the failure causes an incorrect operation only under abnormal system conditions, such as a power system fault, power swing, switching operation

In order to improve the reliability of the protection it is necessary to reduce the time periods during which is stays in the states b and c2. For this purpose any failure leading to these states should be detected as quickly as possible after it has occurred. Table 1 shows the various methods and summarizes their characteristics.

Manual periodic testing with classical test equipment is made at intervals of typically 0,5 to 2 years (see WG 34-05 report, Madrid 81), whereby the equipment involved is taken out of service for one or more hours. Since it is not limited to purely functional tests but covers also checks of operating values, the chances of detecting degradation failures are good, at least theoretically. There is little information, however, from the field as to how many complete failures have been prevented by detecting degradation at an early stage. Manual testing is, in general, the most complete method and is equally well suited to detect states of failure to operate as of potential incorrect operation, i.e. it improves both dependability and security. Also minor failures such as defective lamps, signals are detected. The main disadvantage is that the protection must be taken out of service for several hours and that for economic reasons the intervals between the tests are relatively long and the time till a hidden (non-self-announcing) fault is discovered may be quite long.

As a new development, manually applied computerised maintenance testing seems to be adopted by an increasing number of utilities. The method is described in detail in reference 1. Its main advantage is that the time required is reduced considerable whereby at the same time the depth of the test may be improved.

Automatic periodic testing has so far been used mainly on relatively complex solid-state protective schemes (references 2, 3), which contain a large number of components. Since the probability of a component failure within a period of, say, one year is relatively high, automated testing

with shorter intervals can improve the availability. Most of the checks carried out are functional tests, hence this method is tailored to detect catastrophic failures. However, it is also possible to check a few simple operating values such as delays of timers etc. Short test intervals can give the possibility to detect degradations before they produce a sudden incorrect operation.
Since actual operation of almost all elements can be simulated, most failure-to-operate states are discovered. States of potential incorrect operation (e.g. defect in a stabilising circuit) can also be detected, but, as stated below, this task can in many cases be done more easily by monitoring. Automatic test devices are therefore designed primarily to improve dependability (references 2 and 5).
The additional hardware required for automatic testing not only increases the initial cost, but also the probability of failure of a component (typically 10% to 20% more components). Defects in the automatic test equipment and the effects of wrong diagnostics must, of course, also be considered and will be discussed later on.

Monitoring is continuous. It has been in wide use in protective schemes, in the relay themselves as well as outside. In most cases it monitors the existence of a certain signal or compares two signals, e.g. in a redundant scheme. It detects catastrophic failures immediately and hence may actively be used to prevent some of the instantaneous incorrect operations (e.g. blocking of impedance relay if PT fuse blows).

Monitoring circuits have the advantage that they are relatively simple and consist of few components only; hence their failure rates are much lower than those of the monitored circuits. Most actions (alarm or blocking) have to be delayed by an appropriate time in order to avoid them during transient conditions (e.g. operation of isolators), but these delays are negligible when calculating the unavailability. This latter is practically determined by the mean-time-to repair. Its main disadvantage is that it cannot check the active relay functions such as the operation of a measuring unit or of a tripping amplifier, hence it can hardly detect a state of failure to operate.

The cyclic selfchecking in a microprocessor-based relay can be considered as being continuous for our purpose. Even if the test program occupies a considerable part of the total time and hence the theoretical unavailability is relatively high, this does not matter because the cycles are very short compared to the normal operating time of the protection. It can be so designed to improve both the security and dependability.

Table 1: Classification of Failure Detection Methods

	Time interval between tests	Time during which protection is unavailable	Particularly suited to detect the following states	Particularly suited to detect the following failures	Main Advantages	Main Disadvantages
Manual periodic testing with classical test equipment	0,5 to 2 years	few hours	Failure to operate Potential incorrect operation	Degradation failures Catastrophic failures	-Most complete test -Detects also minor failures -Checking of automatic testing and monitoring	-Protection is unavailable for considerable time -Meantime to detect hidden faults is long -Probability of human error -High operational cost
Manually applied computerised testing	0,5 to 2 years	About 30 minutes	Failure to operate potential incorrect operation	Degradation failures Catastrophic failures	-Very complete tests, can be deeper than manual test -Protection unavailable only for a short time	-Technician may have less encouragement to think for himself -Mean time to detect hidden fault is long -High operational cost
Automatic periodic testing	several hours to several days	5 to 100 ms	Failure to operate	Catastrophic failures Degradation failures	-Meantime to detect hidden faults is relatively short	-Requires additional hardware, hence higher initial co -Somewhat higher failure rate due to additional components
Continuous monitoring in analog and digital circuits	zero	zero	Potential incorrect operation Instantaneous incorrect operation	Catastrophic failures	-Suitable in redundant scheme -Defects are detected immediately -Possibility to prevent instantaneous incorrect trip -Requires little hardware	-Cannot check active operational functions
Programmed cyclic self-checking in MP-based relays	few ms	zero	Potential incorrect operation Instantaneous incorrect operation	Catastrophic failures Soft errors Degradation failures	-Defects are detected immediately -Practically no additional hardware in MP-based relays -Detects also intermittend failures	-Requires additional programme space

3. Various states of the power system and its protection

Since the ultimate aim is the improvement of the power system reliability, we must consider the complete scheme consisting of primary elements, the protection and the built-in testing devices. Although this report shall mainly deal with built-in automatic testing and monitoring equipment, i.e. with the last three lines of table 1, it is clear, that these methods are a part only of all measures to improve the reliability of the power system.

In a first discussion we shall use the simplified state diagram of fig.2. It shows various states in which the power system plus the protection can be. In reality, many more states than shown can be thought of, but for practical purposes only the states which are likely to exist for a reasonable length of time need to be considered.
Therefore, two states are only considered for the power system, a healthy state S and a faulty state $\bar{S}$. The protection may reside in one of the states described previously, and in addition, in states of unavailability due to repair or because it is under test.
It is furthermore assumed that we have one single main protection scheme and some sort of remote back up protection.
The arrows indicate the possible transitions which occur randomly with certain probabilities. At any given moment, the whole system can only be in one state, i.e. the states exclude each other. If the probabilities of the transitions are known, it is possible to calculate - under certain conditions - the probability that at a given instant (t) the system is in a certain state. This method will be used in chapter 5 to calculate some numerical examples.

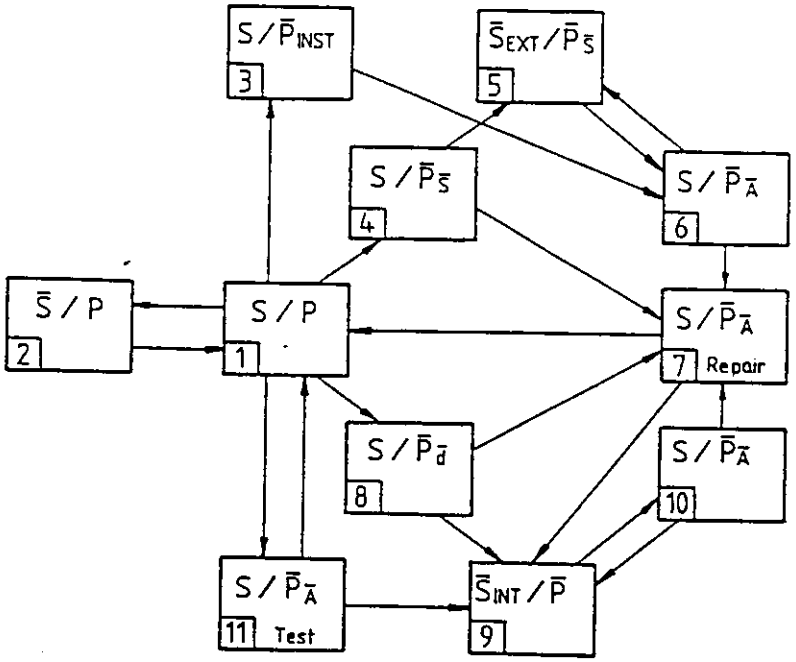


Figure 2: State diagram

States of the power system:

S : System normal
S̄ : System abnormal
$\bar{S}_{INT}$: internal fault
$\bar{S}_{EXT}$: external fault

States of the protection:

P : Protection normal
P̄ : Protection abnormal
$\bar{P}_{INST}$: incorrect instantaneous operation
$\bar{P}_{\bar{S}}$: reduced security, potential incorrect trip
$\bar{P}_{\bar{d}}$: reduced dependability, potential failure to trip
$\bar{P}_{\bar{A}}$: unavailable protection

Combined states of power system plus protection:

1 : Power system healthy, protection healthy
2 : Power system faulty, protection healthy
3 : Incorrect instantaneous operation of protection
4 : Potential incorrect operation state
5 : Incorrect operation during external system fault
6 : Situation after line has been put back in operation, but failure not yet identified
7 : Protection under repair
8 : Potential failure to operate state
9 : Failure to operate during internal fault
10 : Situation after fault has been cleared by back-up protection, but failure not yet identified
11 : Protection not available because being tested

Most of the time, we are in state 1, where the system is healthy and the protection is fully available. In case of a power system fault, we move to state 2, but since the protection is healthy, we return immediately to 1. State 2 is of very short duration and can be neglected in the unavailability calculations which follow later.

A defect in the protection can result in an instantaneous incorrect operation leading to state 3. The probability can be reduced to a certain degree by monitoring, which must act very quickly, however. In many cases, the operators will immediately restore the system to normal, i.e. we move to state 6. It represents the time required to analyse what has happened. It will not take very long to find that the protection was faulty and we proceed to the repair state 7. It must be pointed out, however, that such a quick restoration may not be possible in case of remote controlled stations. If the failed relay system continues to maintain a trip signal, a site visit requiring several hours may be required.
Other types of defects lead to the potential incorrect operation state 4. If the relay is tested before an external fault occurs, we move directly to the repair state, otherwise we will first have a system outage 5 and again a period of analysis 6. The transition rate from 4 to 7 is directly dependent on the frequency of testing. If we test once a year only, and the relay experiences five external faults per year, the probability of a move from 4 to 5 is clearly five times as high as from 4 to 7. If tested once a week the probability of a move to 5 is much smaller of course.

In a similar manner, certain defects will disable the protection, i.e. it will move to the state 8 of potential failure to operate. This state is either detected by testing or by an internal fault. State 9 corresponds to 5 and state 10 to state 6. If a second system fault occurs while we are in states 6 or 10, we will have another failure.

We furthermore have to take into account that during testing the protection considered is unavailable and will not operate for internal faults (state 11).

Many more states can be thought of. We may, e.g., have two failures before detecting any one of them, e.g. we can be in states 4 and 8 simultaneously, which means that we should also define a state $4 \cap 8$. However, the more states, the more complicated the calculation and the interpretation of the results becomes. We must try to keep the diagram simple, by neglecting all those states which are highly unlikely. We then commit a small error only.

One purpose of the diagram is to calculate the probability of state 1, i.e. the availability of the protection. We are of course also interested in the states 5 and 9, i.e. the actual down states of the power system. However, their duration depends entirely on the time needed to restore operation which is very variable. It will be kept as short as possible and the loss of energy will normally be small. Expenses will however also be caused by analysing and repairing. We therefore are interested to know how often we pass through the states 5, 6, 7, 9 and 10.

In order to simplify, we can put stages 5 and 6 together as well as 9 and 10, since it is unlikely to have a second fault occuring before the operator has found that the protection has maloperated.

The above considerations have been made under the assumption that the testing, monitoring or selfchecking devices never fail. If we take such failures into account too, we must consider different failure modes. Since furthermore several of the methods discussed are usually used simultaneously, depending on the complexity of the protective scheme, a complete analysis becomes very involved due to the large number of states.

In reference (7) a total of 52 states have been considered, excluding the states of the power system itself.
For the later discussions it is also useful to define a generic term for all events leading to states 3, 5 or 9, i.e. the forced system outages due to protection failures. We shall call them protection maloperations. They include both failure modes: failure to operate and incorrect operation.

In order to discuss the influence of the built-in test facilities and of the maintenance practice on power system reliability and frequency of protection maloperations we will have to use a suitable model. In chapter 5 we will consider a single line protection and a duplicated parallel protection scheme. In order to arrive at general quantitative conclusions we will have to assume certain MTBF's, time intervals between tests, power system fault rates etc., and to vary them in order to see their influence. Thereby we shall exclude the socalled minor failures for the sake of simplicity.
However, before analysing a complete state diagram, we shall first analyse separately the most important influencing factors in chapter 4.

4. Main factors influencing the availability

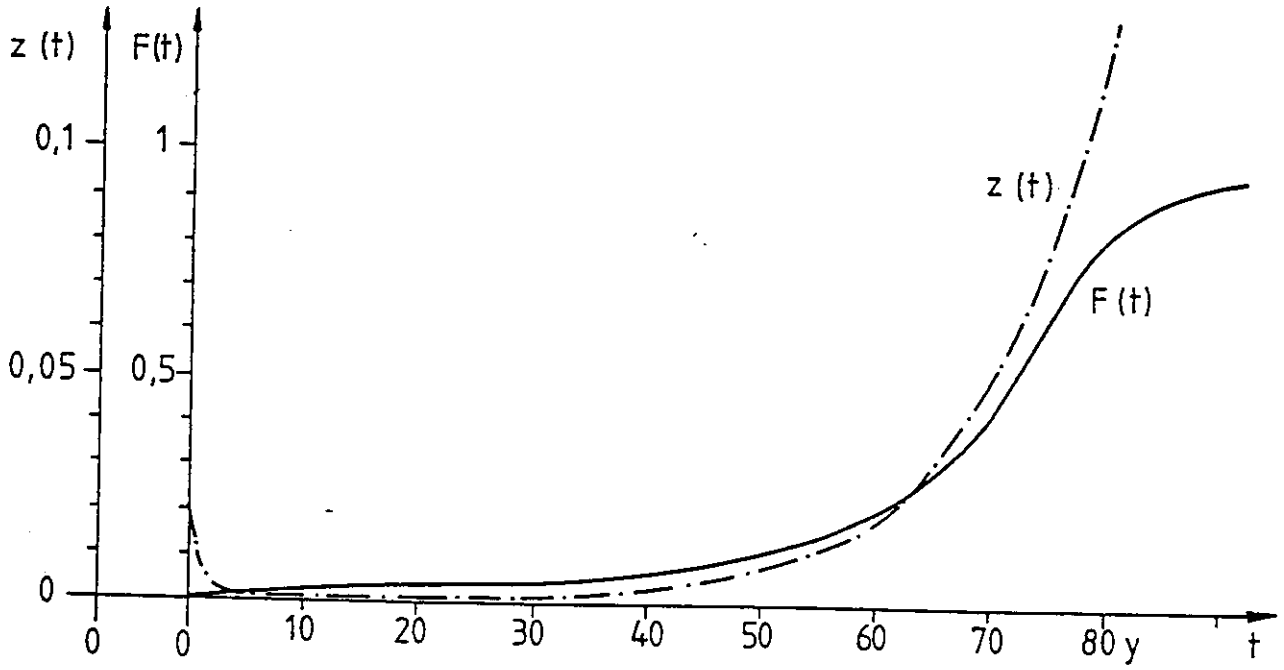
4.1 Effects of maintenance

Reliability is the ability of an item or system to perform a required function under stated conditions for a stated period of time. Let us first assume that the required function is defined and attempt to analyze the influence of testing, maintenance and repair on reliability.

The characteristics defining reliability are functions of time t. The basic terms, defined with more detail in IEC 271, pp.38, are:
- Cumulative distribution function of failures F(t)
- Instantaneous failure rate z(t)

The functions can have very different shapes as will be shown by two examples.

If we observe the failures of a sufficiently homogeneous population of items, starting at t = 0, we will generally find that the number of failures per time unit is not constant. We can plot a curve F(t), indicating the accumulated failures between 0 and t. If the failures are exclusively due to ageing or wear, F(t) will typically be as shown in fig.3 (from a mortality statistics).



As another extreme case, we assume that the failures occur completely randomly, i.e. in a similar way as the decay of radioactivity matter. Z(t) is then a constant, usually denoted by λ , and we obtain an expontential function for F(t) as per fig. 4.

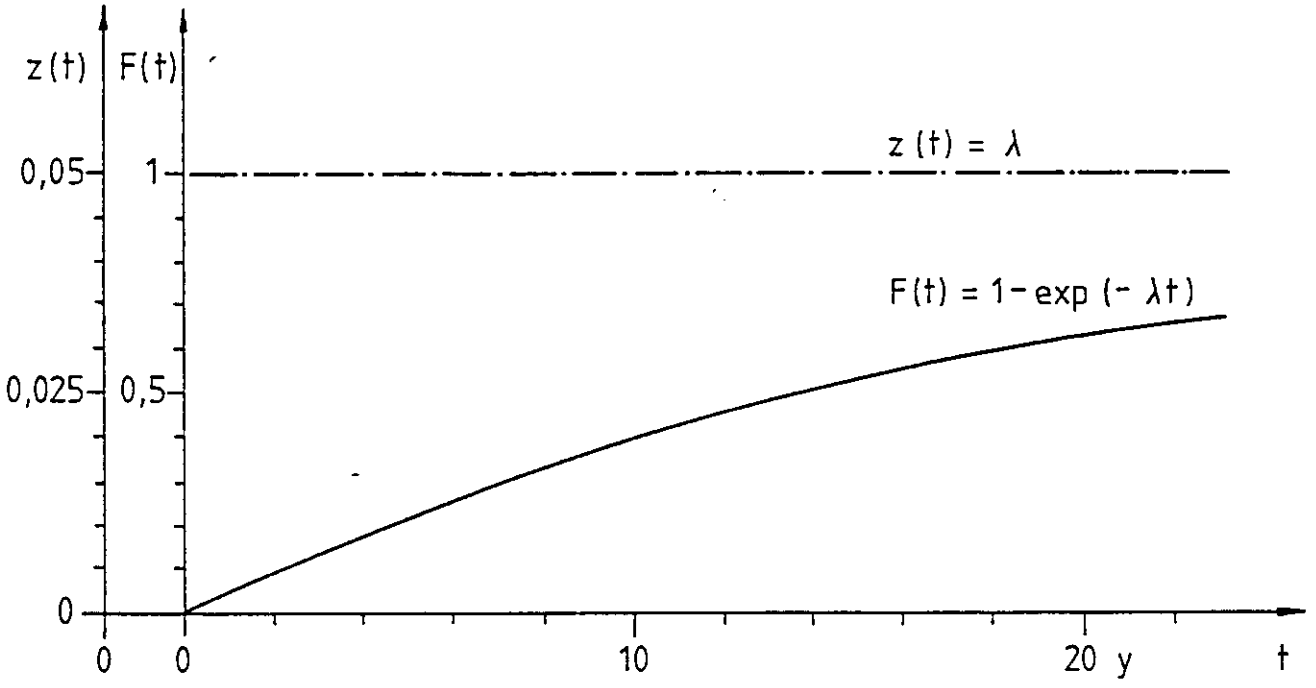


Figure 4

For technical devices, we must expect a combination of the two above extremes. In the specialized literature on reliability a number of other distribution functions are therefore described. It is common to distinguish between three periods, one of early failures, one of a constant failure rate and one of ageing. The curves depend to some degree on the technology considered. In particular, solid state components will generally exhibit a constant failure rate for a very long time. This is probably also true for "soft" errors in MP-based relays.
Irrespective of the distribution, an item will eventually fail if we wait long enough and no intervention takes place. However, if we make an inspection at time T we can influence the curves in different ways. Thereby the results will be different depending on whether preventive maintenance is effective (e.g. electromechanical devices) or useless (solidstate components with constant failure rate).

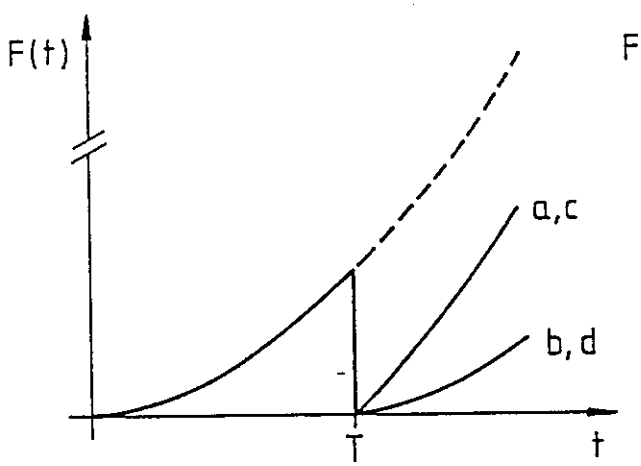


Figure 5a

Preventive maintenance effective, i.e. device with ageing

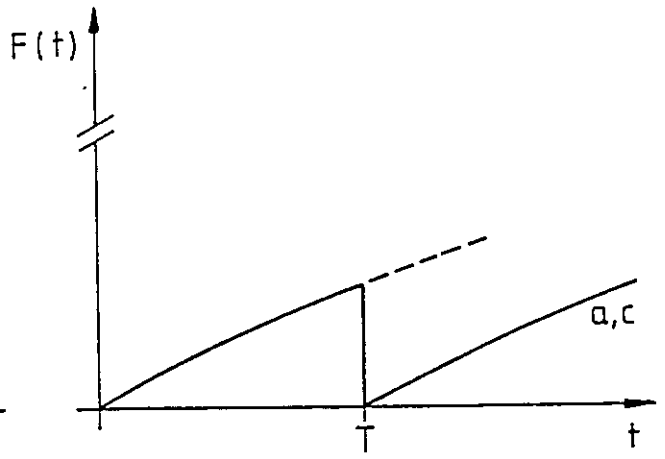


Figure 5b

Preventive maintenance not possible, i.e. constant failure rate

a.) If we find that the item has failed, we repair it. Assuming a 100% reliable inspection and an ideal repair, we thus restore the initial condition at $t = 0$, at least as far as $F(t)$ is concerned: The item has again the ability to perform the required function. Regarding $Z(t)$, it will in general not be the same as with $t = 0$, since some parts of the item are not renewed and hence may show some ageing. (Fig. 5, curve a)

The above repair is equivalent with replacing in a large lot of items the failed ones only by new ones, continuing the operation with a mixture of new and old items.

b.) If the item has failed, we can, in addition to a.) carry out some preventive maintenance, i.e. we try to remove all traces of ageing. This would be normal with an electro mechanical device, where we would check, clean and adjust all the other parts. If we are successful, we have now also restored the initial failure rate.
In a large lot of components, this is equivalent to replacing also those which have not failed.

c.) If the inspection has revealed that the item still has the ability to perform the required function, we may decide to return to normal operation without any further action. We thus continue where we were, except that we know that the item is still alive.

Although we have not really done anything, we will continue on a new curve F(t) simply because of the knowledge gained by the inspection. The failure rate function z(t) will generally not be the same as at the beginning.

d.) In case of c.) we may, however also decide to carry out some preventive maintenance and thus improve also the failure rate as under b.).

As stated before, F(t) indicates the probability that a relay is unable to fulfil a certain function at time t. If we consider a large number of relays, it is useful to define the average unavailability $\bar{A}(T)$ for the time interval $0 < t < T$:

$$\bar{A}(T) = \frac{1}{T} \int_0^T F(t)\, dt$$

It is the complement of the average availability A(T)

$$\bar{A}(T) = 1 - A(T)$$

Although it is possible to take ageing into account in an analytical treatment by using appropriate functions, it leads to considerable complications, and we have to leave it to the specialized literature. We shall assume for our further discussions that $z(t) = \lambda$ is constant and hence $F(t) = 1 - \exp(-\lambda t)$. This simplification will hardly affect the results if we consider the solid-state components, as their ageing begins very late and as they show a relatively long period of a constant λ. A constant λ means that preventive maintenance is useless, i.e. the probability of a solidstate device to fail before or just after a maintenance is the same. The only way to improve the average availability is to reduce the time interval T between inspections.

With electromechanical devices this is quite different. Their rate of failure is very low when the device is new or after maintenance; a reduction of T by using automatic testing is much less effective, since obviously no preventive maintenance can be made with automatic test devices.

4.2 The influence of time intervals between the tests

The effect of T may be illustrated by means of a simple example. Assuming that a relay has a MTBF = $1/\lambda$ of 20 years and that we make a first inspection after one year, the probability F(T) that it has failed before is $1 - \exp(-0{,}05) = 0{,}049$. (For small λ T's we can also use the approximation $F(t) = \lambda T = 0{,}05$).

We are interested to know the average unavailability $\bar{A}$. Since the instants of the actual failures are more or less evenly distributed between t = 0 and t = T, the average time of a hidden fault is about T/2 (half a year) and the total relay-years lost is λ TxT/2 = $\lambda T^2/2$ (0,025 years). If divided by the time period T, we arrive at an average unavailability of $\lambda T/2$ (0,025).

(More mathematical derivations are of course available in the literature,

e.g. $\bar{A}(T) = \frac{1}{T}\int_0^T F(t)dt = 1 - \frac{1}{T\lambda}(1 - e^{-\lambda T}) = 1 - \frac{1}{T\lambda}(\lambda T - \frac{\lambda^2 T^2}{2!} + \frac{\lambda^3 T^3}{3!} - \ldots)$

for $T \ll 1$: $\bar{A}(T) = \frac{\lambda T}{2}$

==========

As shown in fig. 6, the momentary unavailability $\overline{A}(t)$ is a periodical function. Table 2 indicates some values for an MTBF of 20 years. Since the time for inspection and a possible repair are relatively small, we have neglected them.

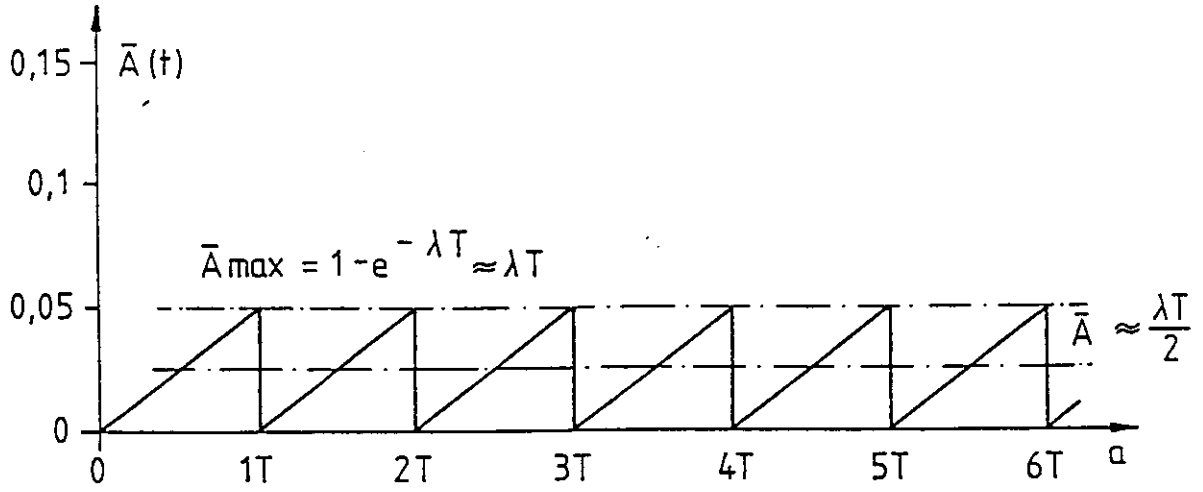


Figure 6: Influence of time interval between tests on unavailability

T	$\overline{A}$	$\overline{A}$*	$P2(oo) = \frac{\lambda}{\lambda+\mu}$
1 week	0,000 481	0,000 481	0,000 481
2 months	0,004 155	0,004 167	0,004 149
4 months	0,008 287	0,008 333	0,008 264
1 year	0,024 588	0,025 000	0,024 390
2 years	0,048 374	0,050 000	0,047 619
3 years	0,071 387	0,075 000	0,069 767

Table 2

Average unavailability for MTBF of 20 years and various test intervals (* using the approximation $\overline{A} = \frac{\lambda T}{2}$. For the meaning P_2 (oo) see below)

Considering a power system with 100 line protections, and 1 fault per year per line, and a test interval of one year, we can expect N = 0,025 x 100 x 1 = 2,5 failures to operate per year. If the test takes place once a week, this will be reduced to less than 0,05 failures.
Similar considerations apply for incorrect operations, whereby we have to take into account however, that for each system fault 5 or may be 10 protections will start and the corresponding probabilities are 5 to 10 times higher if we assume the same MTBF for this failure mode.

Since in section 5, state diagrams will be used for the calculations, we shall illustrate this method too in order to see the difference, using a very simple diagram with two states only:

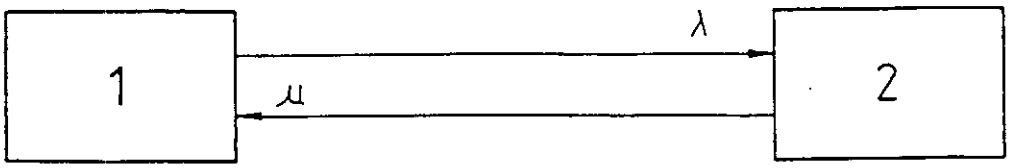


Figure 7: Simple two-state diagram

State 1: No defect in the relay
State 2: Defective component in the relay
λ : Transition rate from 1 to 2, which is the probability that a failure occurs per time unit.
It is the inverse of the mean time to failure or Mean Up Time (MUT)
μ : Transition rate from 2 to 1, which is the probability that a failure is detected and repaired per time unit.
It is the inverse of the mean time to detect and repair or Mean Down Time (MDT). (The times to detect and to repair will be separated later on. For this example we neglect repair time and assume $\mu = \frac{2}{T}$).

Important assumption: Both λ and μ are constant. It can be shown that the behaviour of the relay can then be described by two simple differential equations:

$$s\,P_1(t) = -\lambda P_1(t) + \mu P_2(t)$$
$$s\,P_2(t) = \lambda P_1(t) - \mu P_2(t)$$

whereby s = d/dt operator

$P_1(t)$, $P_2(t)$: Probabilities of states 1 and 2 respectively at time t.
If we assume that the relay is healthy at the beginning we have the initial conditions:

$$P_1(0) = 1 \qquad P_2(0) = 0$$

The solutions are:

$$P_1(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t}$$

$$P_2(t) = \frac{\lambda}{\lambda+\mu} - \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t}$$

$P_2(t)$ is the probability of the state of unavailability. It does not exhibit the periodical nature of fig 5, because it is an average value. If we wait long enough, we obtain the steady state value and the well known formulae:

$$P_2(\infty) = \frac{\lambda}{\lambda+\mu} = \frac{1/\mu}{1/\mu + 1/\lambda} = \frac{MDT}{MDT + MUT}$$

MDT Mean down time
MUT Mean up time

The described method results in slightly different values as shown in table 2, because the assumption of a constant μ is not quite correct.

(the down states do not really have an exponential distribution). It is common, however, to use constant coefficients when applying this method, because the solution of the equations is easier and diagrams with many states can be calculated by a computer.

In both above calculations the unavailability of the protection during the tests has been neglected. For short test intervals, this assumption cannot be maintained anymore. It is obvious that for $T \rightarrow 0$, the unavailability $\overline{A}$ will not become zero, and the formula $\overline{A} = \frac{\lambda T}{2}$ must be replaced by a better one:

$$A = 1 - \overline{A} = \frac{MTTF}{MTBF + MTTR + \frac{T}{2}} \times \frac{T}{T + t}$$

MTTF = $1/\lambda$
MTTR = $1/\mu$
T = test interval
t = time for the test

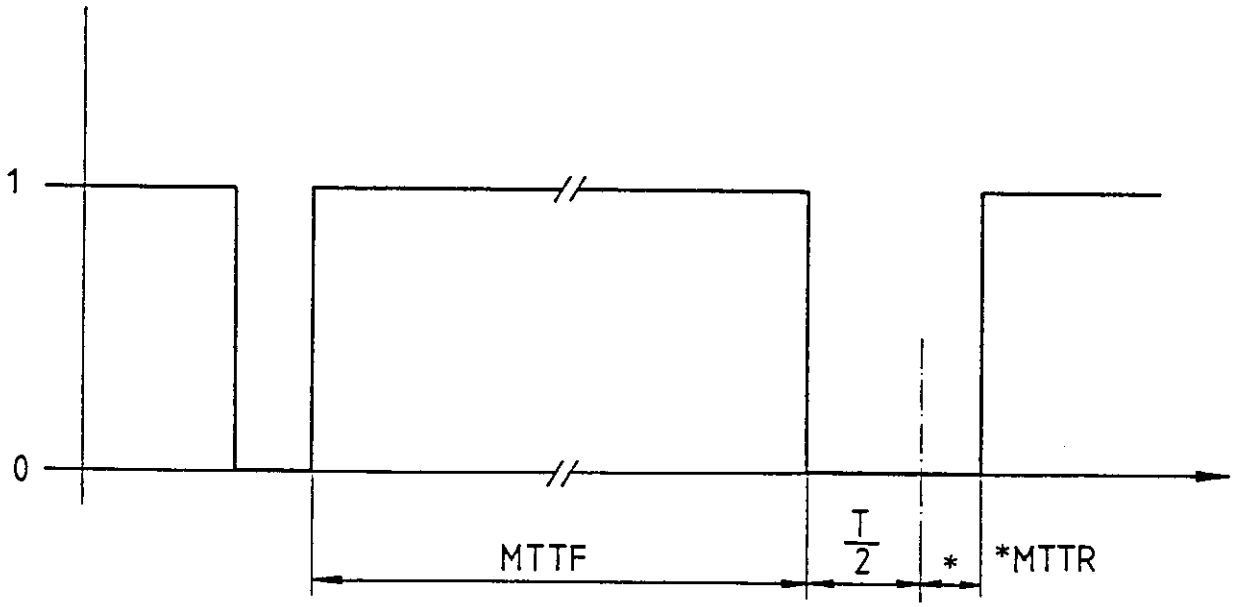


Figure 8

MTTF : Mean time to failure
MTTR : Mean time to repair
1 : Up state of protection
0 : Down state of protection
T : Time interval between tests

The first term can easily be derived from fig. 8. The average time $\frac{T}{2}$ to detect the defect and the repair time have now been separated. The second term takes into account the unavailability during testing.

It is of interest to look for the optimum test interval $T_{opt.}$, by solving the equation

$$\frac{dA}{dT} = 0$$

If we write $f(x) = \frac{a}{b + \frac{x}{2}} \cdot \frac{x}{x + c}$

we obtain $\frac{df(x)}{dx} = \frac{a}{2(b + \frac{x}{2})(x + c)} \underbrace{\left[\frac{c}{x+c} - \frac{x}{2(b + \frac{x}{2})} \right]}_{0} = 0$

and

$$x^2 + xc = 2bc + cx$$

$$T_{opt.} = x = \sqrt{2bc} = \sqrt{2\,(MTTF + MTTR)t}$$

Example:

MTTF : 15 years

MTTR : 24 hours

t : 1 min

$T_{opt.}$ = 66,2 hours

and A = 0,99931405

$\bar{A}$ = 0,00068595

($\frac{\lambda T}{2}$ results in a too optimistic value = 0,00025114)

In the calculations of chapter 5, the times for testing (manual and automatic) will be taken into account.

4.3 Influence of the "depth" of the tests

Since some defects may not be detected during the test, the unavailability will gradually increase and for $t \longrightarrow \infty$ approach 1. We define a fault detection ability factor α using a simple model consisting of the series connection (for the failure to trip mode) of two parts (see also reference 4).

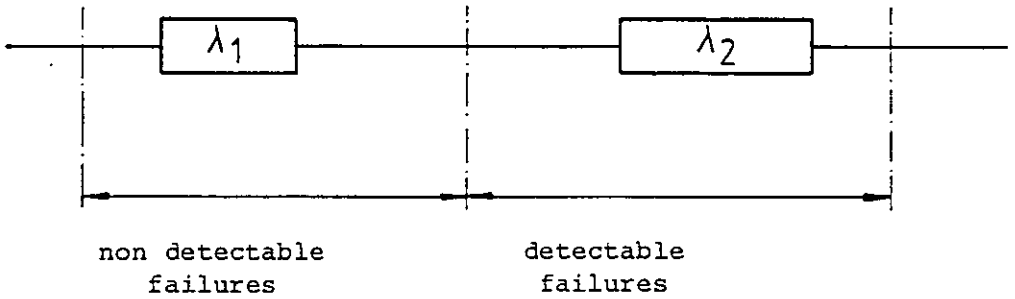


Figure 9

We define $\alpha = \frac{\lambda_2}{\lambda_1 + \lambda_2}$ and $\lambda_1 + \lambda_2 = \lambda$

When the obtain

A (T) just before the first test: $e^{-(\lambda_1 + \lambda_2) T} = e^{-\lambda T}$

A (T) just after the first test: $e^{-\lambda_1 T} = e^{-\lambda(1-\alpha)T}$

The probability that the protection operates also at the end of the second period is the probability that it was healthy at its beginning multiplied by the probability that it did not fail during the second time period:

A (2T) just before the second test: $e^{-\lambda(1-\alpha)T} \cdot e^{-\lambda T}$

and generally

A (nT) just before the n'th test : $e^{-\lambda(1-\alpha)(n-1)T} \cdot e^{-\lambda T}$

The corresponding unavailabilities are the complements to 1.

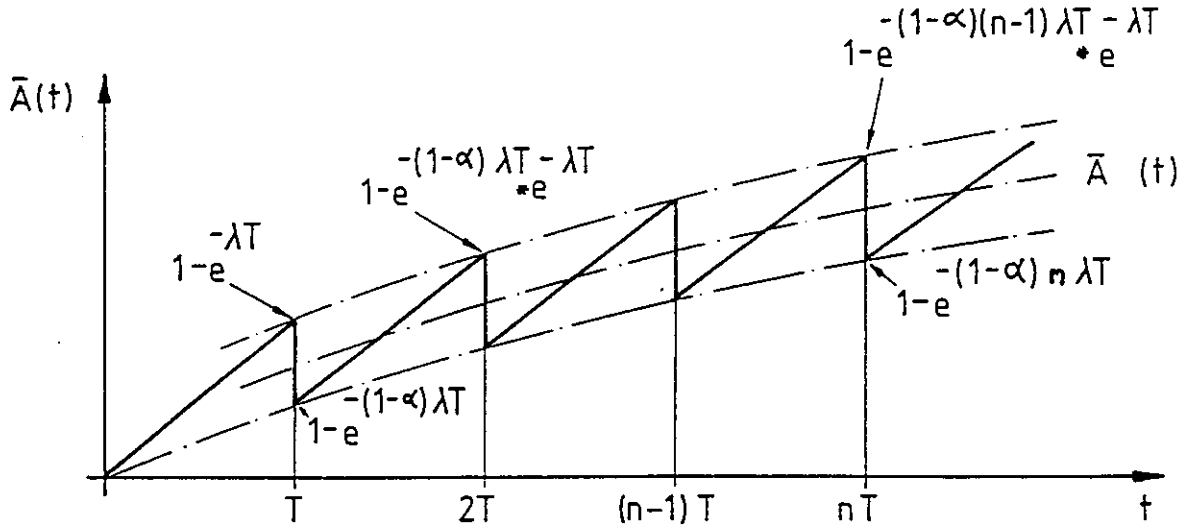


Figure 10: Unavailability for $\alpha < 1$

The average unavailability A(t) is now increasing, as expected. It has been calculated for α = 0,9 and α = 0,98 for the various T's, and for λ = 0,1 (fig. 11) taking the arithmetic mean value of the two curves.

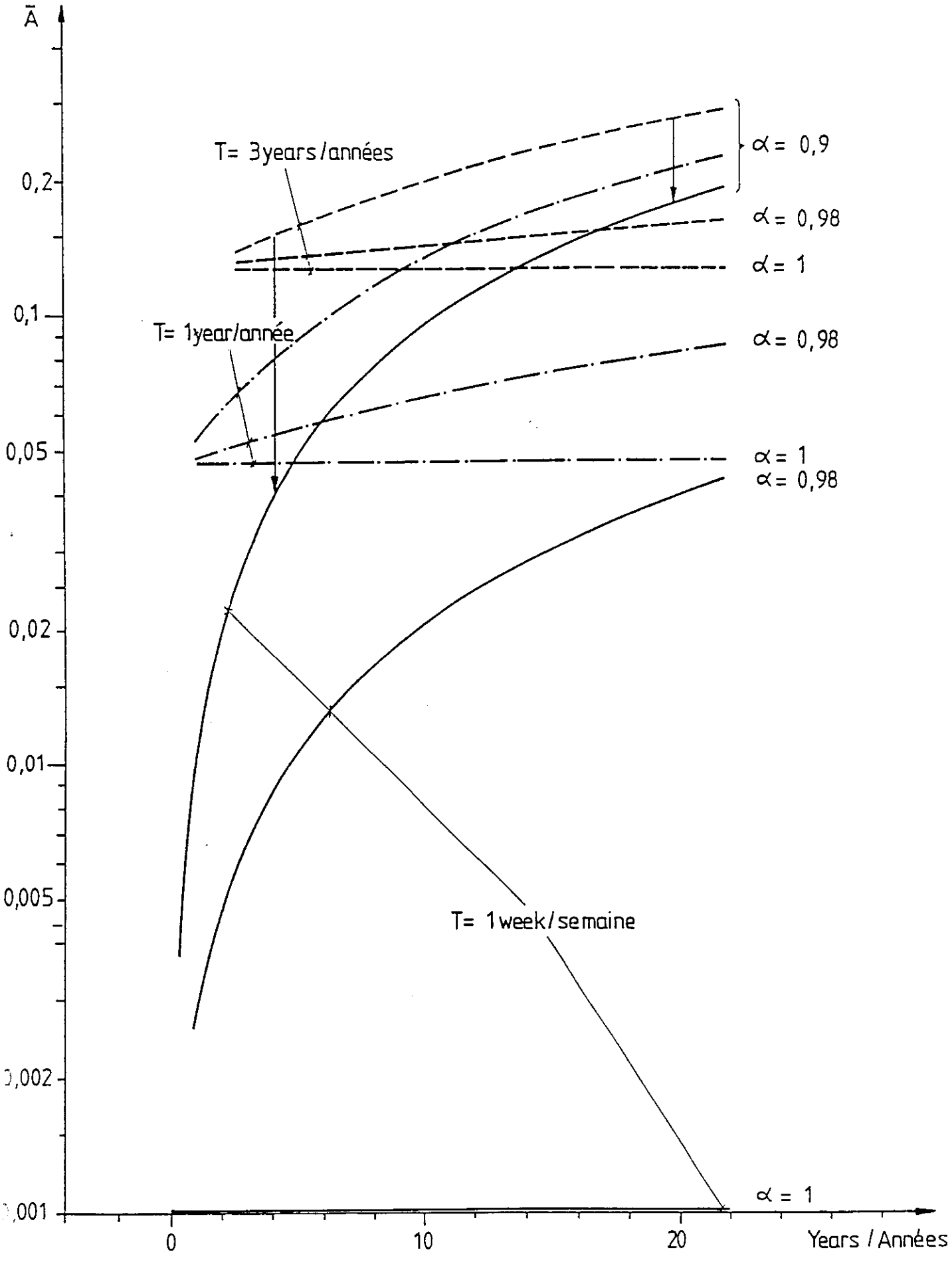


Figure 11: Influence of α and T on unavailability

The unavailability increases continuously and attains relatively high values after 20 years. Whereas the benefit of more frequent testing is quite remarkable at the beginning, e.g. $\bar{A}$ = 0,15 versus 0,04 for α = 0,9 after 2 years, it is much less pronounced after 20 years, namely 0,3 versus 0,2.

In practice, however, this is not so. Each power system fault tests the protection too and reduces the time till recognition of hidden failures (reference 8). The corresponding increase of availability is obtained at the expense of protection maloperations, it is true, but the frequency of protection maloperations is smaller than if the effect is neglected as will be shown in the next section.

4.4 Influences of power system fault rate

In section 4.2 we have estimated the number of protection maloperations by multiplying the primary fault rate with the unavailability of the protection. This is correct if we assume that repairs are only carried out after inspection, but not after a power-system fault:

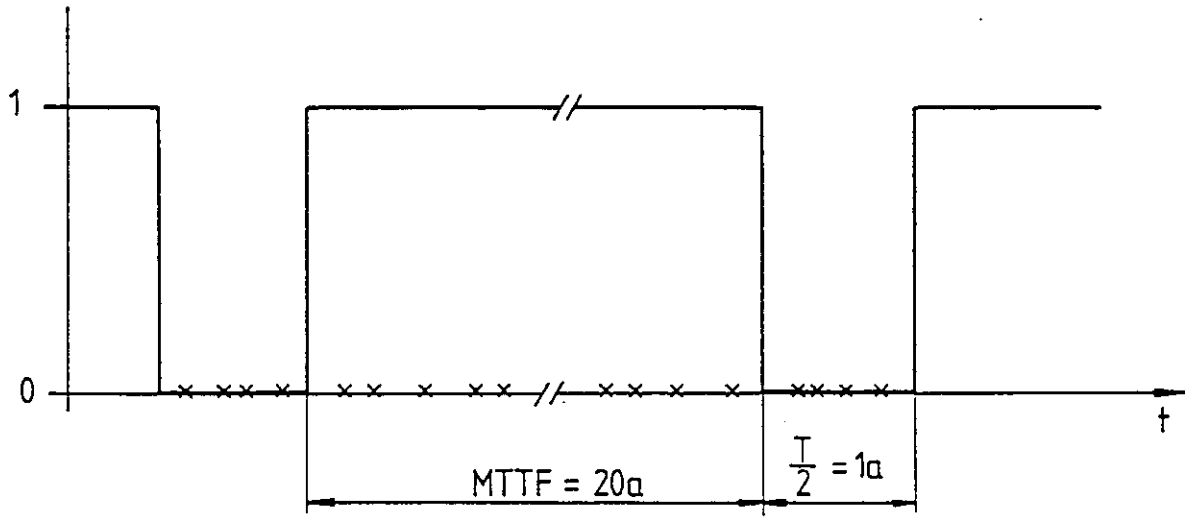


Figure 12: Number of protection maloperations

MTTF: Meantime to failure

x : Power system faults

$\frac{T}{2}$: Average hidden fault time

1 : Up state of protection

0 : Down state of protection

Fig.12 shows that for $\lambda = 0{,}05\ a^{-1}$ and an inspection interval $T = 2a$, five faults will fall into the down state period as an average if we assume a primary system fault rate of $\sigma = 5\ a^{-1}$. We shall thus have five protection maloperations within 21 years, i.e. the corresponding Mean Time is about four years only. We can also use the previous formulae and we obtain for the rate of maloperation:

$$\sigma \cdot \bar{A} = \sigma \frac{\lambda T}{2} = 5 \times 0{,}05 = 0{,}25\ a^{-1}$$

or, in the average $\frac{1}{0{,}25} = 4$ years between two maloperations.

The above assumption is certainly unrealistic, since any maloperation of the protection during a power system fault will lead to a non-scheduled inspection and repair. As already stated in section 3, the time required to identify the case as a protection maloperation (states 6 or 10 in fig. 1) will be short, normally, certainly much shorter than the average time to the next scheduled inspection. It will be neglected in the following section, or considered as part of the repair time.

Above statements may not fully apply to redundant protection systems. A failure to operate of one protection scheme (in a one-out-two scheme) or an incorrect operation (in a two-out-of-two scheme) may not be detected and remain concealed. Such states of reduced dependability or security are of course not desirable. It is however possible to some degree to detect them by monitoring the two systems.

For the next considerations we shall assume one protection scheme only and that repair also takes place after each maloperation. In order to reduce the number of variables we shall furthermore assume for the following analysis that the detection ability factor α is equal to 1.

Under such conditions, the effects of primary system fault rate on the unavailability has been treated in detail in reference 8.

Thereby, a state diagram similar to fig. 13 has been used a basis:

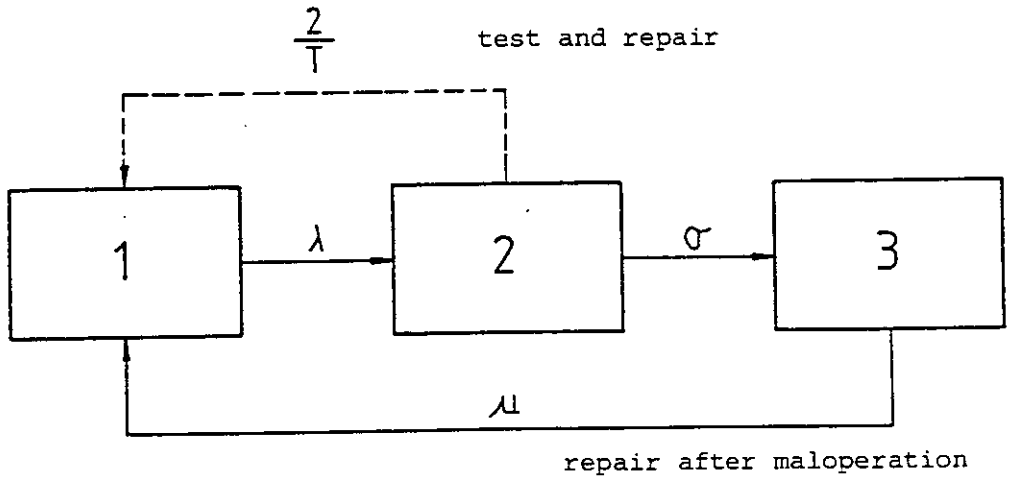


Figure 13: Simple three-state diagram

1 : Healthy state
2 : Protection defective
3 : Maloperation

Fig. 12 helps to analyse the following questions:

a) How often do we have a maloperation ?

b) How often do we have to repair ?

c) What is the influence of λ, σ and T on above mean values ?

The results of such an analysis should help to optimize design of equipment and testing strategy. Thereby, the main objectives are:

- to reduce the risk of a major system disturbance due to a maloperation of the protection. As stated in the introduction, this risk may have different weights for a heavily meshed system than for a radial network. It may also be different for different failure modes

- to reduce the total cost for the equipment (extra cost for auto-test and monitoring devices etc.), for the repairs and the inspections. Obviously, these cost will vary from one utility or country to another.

Before going into a numerical example, we can already make a few qualitative statements.

- Clearly, a high reliability of the equipment, i.e. a low λ firstly results in a low risk of a maloperation. Furthermore, it is the only way to minimize repair cost, since any defect requires a repair, no matter whether it is done after a scheduled test or a maloperation.

- A high power-system fault rate σ tends to increase the frequency of protection maloperation. To bring this risk down again, it is necessary to increase the rate of periodic testing. If e.g., we have five system faults and one test only per year, the chances of a hidden fault being detected by a maloperation is five times higher than during a test.

- The additional complexity due to automatic testing and monitoring will in turn tend to increase the λ. It is very essential that this increase is kept as small as possible. It will further, to a certain degree, increase the number of unnecessary non-scheduled maintenance due to false alarms. (This problem will be dealt with separately and is not shown in fig. 12).

  The state probabilities between the tests as functions of time t are as stated below, assuming that we start from the healthy state after each test:

  $$P_1(t) = A + B\, e^{s_1 t} + C\, e^{s_2 t}$$

  $$P_3(t) = D + E\, e^{s_1 t} + F\, e^{s_2 t}$$

  $$P_2(t) = 1 - P_1(t) - P_3(t)$$

  A, B, C ... E, s_1 and s_2 are functions of λ, μ and σ. Although the diagram is very simple, these functions are already fairly complicated. State diagrams with more states and transitions become very difficult to calculate by hand, but computer programs exist to calculate them.

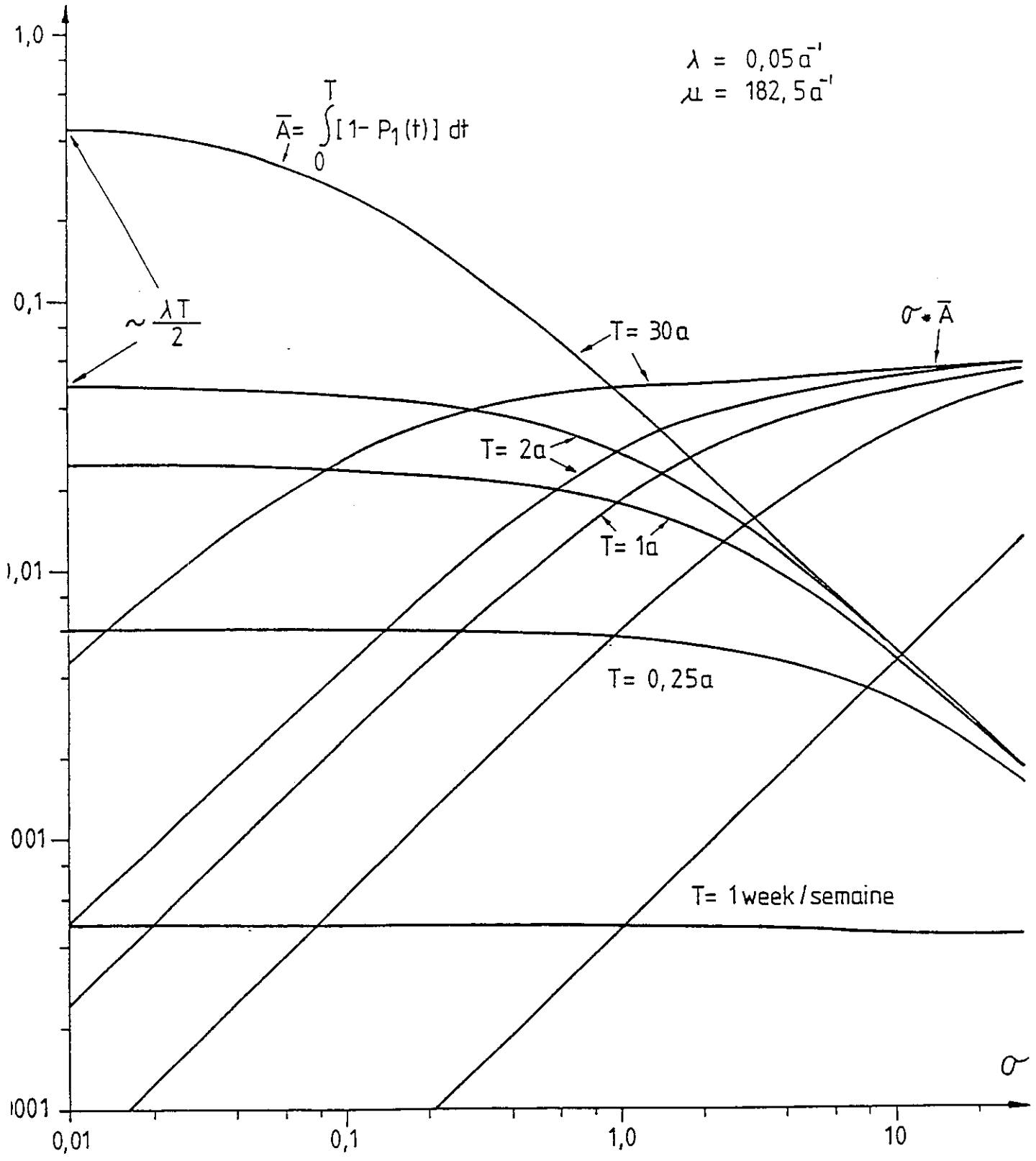


Figure 14: Average unavailability $\bar{A}$, annual number of maloperations $\sigma \cdot \bar{A}$, as a function of annual power system fault rate. Repair on inspection T and after maloperation.

In fig. 14, the average unavailability $\bar{A}$ and the average number of protection maloperations have been plotted against the number of primary system faults. Similar curves have already been published in reference 8 for varying MTBF's, but only for a constant T of 1 year.

For σ = 10 the curves show that for such a high fault rate testing every year or every 30 years does not make much difference !

In the case of frequent testing, i.e. for T about 1 month or shorter, the effect of σ can be neglected. It means, that in case of automatic testing, the rate has practically no influence on the unavailability if we assume a fault detection ability factor α of 1 . However, the effect of both α and σ must be taken into account if we look at Fig. 10. The lower curve will flatten and $\bar{A}(t)$ will stabilize a certain level, because the defects which are not detected by periodic testing will eventually be detected and repaired after a system fault.

As a conclusion we can say that in a complete analysis the rate of primary faults has to be included, considering of course faults within as well as outside the protective zone.

4.5 Failures of the selfchecking or monitoring device

The selfchecking or monitoring circuits can be affected by component failures having different effects. We shall assume in the following two failures modes.

T' : Non-selfannunciating defect with the effect that no signalling is possible. The device is "dead". Defects in the supervised circuits will not be noticed.

T" : Defect with the effect that a false alarm is given at the next test cycle, or immediately in case of continuous monitoring.

We further shall assume as before that all failures of components are independent events.

The question which is often asked is: What is the ratio of false to correct alarms ? This ratio can be surprisingly high, particularly if the supervised circuits have a low failure rate. Reference 6 treats the problem of the quality of diagnostics in detail and arrives at relatively pessimistic values. It is obvious that the quality of the testing device must be much better than that of the supervised relay. As an example we may consider Fig. 15, where R and R represent the probabilities of a truly healthy or defective relay, T' and T" the probabilities of defects in the test device.
The probabilities of combined defects are as follows:

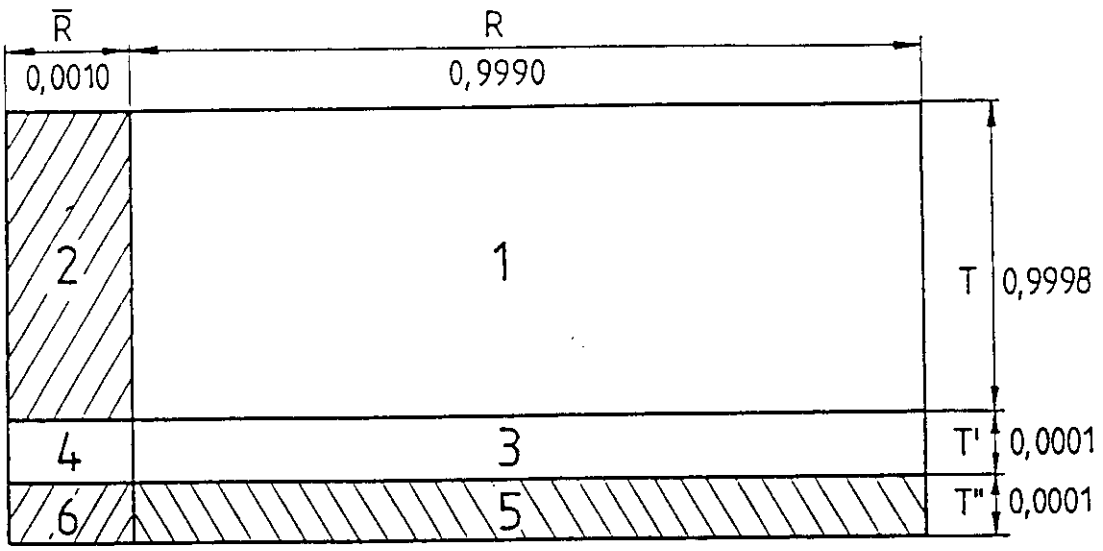


Figure 15

Probabilities:

P(1)	:	Relay healthy, no alarm
P(2)	:	Relay defective, alarm
P(3)	:	Relay healthy, test device defective, no alarm
P(4)	:	Relay defective, test device defective, no alarm
P(5)	:	Relay healthy, test device defective, false alarm
P(6)	:	Relay defective, test device defective, alarm (but probably incorrect diagnostic)

The ratio $\frac{5}{2 \cdot 6 \cdot 5} = \frac{\text{false alarms}}{\text{total number of alarm}}$

may be considererd as a measure of the quality of the test device.

Example:
Relay $\lambda = 0{,}05$
Test device $\lambda'_{AT} = 0{,}005$
$\lambda''_{AT} = 0{,}005$

Assuming that we test every week, the probabilites of a faulty relay or faulty test device after one week are approximately:

$R = 0{,}9990 \qquad \bar{R} = 0{,}0010$
$T = 0{,}9998 \qquad T' = T'' = 0{,}0001$

The above ratio is approximately, as can be seen from fig. 15, equal to

$$\frac{5}{2 \cdot 6 \cdot 5} = \frac{0{,}0001}{0{,}0011} \approx 0{,}09$$

We have approximately one false alarm out of ten. If we relate the false alarms to the total number of tests, however, their probability is fairly low. In a more detailed analysis it is of course necessary to take into account also a possible degradation of the test device with the time (Chapter 5).
Automatic test devices will normally also include means of locating the print or part affected by the component failure, contributing to a faster repair.

5. Combined effect of the various influencing factors

This chapter describes an attempt to set up a model to study the combined effect of the main influencing factors. In practice, the combination of the power system, protection and the supervising devices together forms a very complex system. We must simplify in order to limit the variables to a reasonable number. We therefore consider first a single, non-redundant scheme. On the other hand, it seems important to consider the different failure modes defined in chapter 2.

5.1 Single protection scheme

5.1.1 Main assumptions

A few numerical examples have been calculated based on typical values of failure rates, system fault rates, testing intervals etc. The purpose was, firstly, to check the suitability of the model and, secondly to illustrate some basic trends. The absolute values obtained, however, should be considered with caution. They depend very much on the input values which certainly vary from one application to another.

The model assumes a relatively complex protection scheme, considering the whole chain from the instrument transformers up to the circuit breaker trip coil. Therefore, a comparatively low MTBF of 20 years was taken for each failure mode for the reference case.

The model was drafted having in mind mainly a protective scheme using conventional electronic technology. Whether it is also useful for microprocessor based equipment would have to be investigated later on.

Continuous supervision has been omitted, or considered as a special case of periodic automatic testing. It was found that there is little difference between testing once per week and testing, e.g. every minute, because both invervals are much smaller than those of the other events (defects in protection, system faults). However, it is admitted, that the main reason was to simplify the model. Continuous supervision of many functions can be done easily and with very little additional hardware. The additional failures introduced by monitoring are probably smaller than for automatic testing. It will be desirable to review this point when constructing a model for redundant schemes. There, continuous monitoring of two or more schemes is very important.

5.1.2 Diagram of the model

The state diagram used is shown in fig. 16. It is based on the diagram of fig. 2 in section 3, adding however the depth of testing, the different failure modes, and the failure of the test devices. It has now 17 states instead of 11, whereby it should be noted, that the numbers do generally not refer to the same states. Three subsystems have been considered: the power system, the protective scheme, the automatic testing device.

States of power system

- $\overline{S}$ No fault
- S_{INT} Fault within protection zone (relay must operate)
- S_{EXT} Fault outside protection zone (relay must restrain)

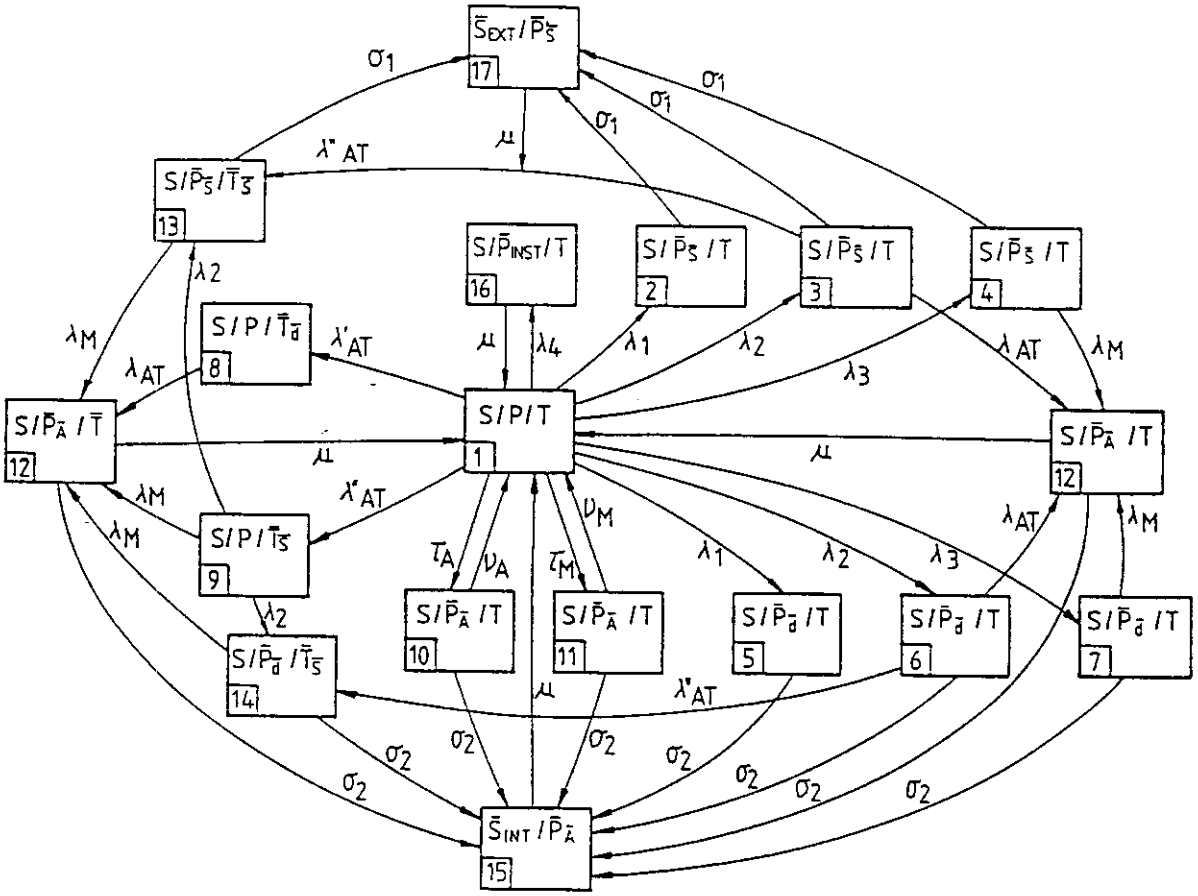


Figure 16: State diagram for a single protection scheme

Symbols

σ_1	:	Rate of external power system faults
σ_2	:	Rate of internal power system faults
λ_1	:	Rate of protection failures, detectable by automatic tests
λ_2	:	Rate of protection failures, detectable by manual test only
λ_3	:	Rate of protection failures, not detectable by testing
λ_4	:	Rate of protection failures, instantaneous incorrect tripping
λ'_{AT}	:	Rate of failure of automatic test equipment; cannot detect any failures
λ''_{AT}	:	Rate of failure of automatic test equipment; gives a false alarm
λ_M	:	Rate of failure detection by manual testing
λ_{AT}	:	Rate of failure detection by automatic testing
τ_M	:	Rate of manual testing
τ_A	:	Rate of automatic testing
ν_M	:	Inverse of meantime for manual testing
ν_A	:	Inverse of meantime for automatic testing
μ	:	Repair rate
α_M	:	Fault detection ability factor for manual tests
α_{AT}	:	Fault detection ability factor for automatic tests

States of protective scheme (excluding automatic testing)

- $\overline{P}$ No defect, fully available (1)
- $\overline{P}_{INST}$ Defects resulting in instantaneous incorrect trip (16)
- $\overline{P}_{\overline{S}}$ Defects resulting in a state of potential incorrect trip (2,3,4,13)
- $\overline{P}_{\overline{d}}$ Defects resulting in a state of potential failures to trip (5,6,7,14)
- $\overline{P}_{\overline{A}}$ Unavailable during testing (10, 11)

States of automatic testing device

- $\overline{T}$ No defect
- $\overline{T}_{\overline{S}}$ Defects resulting in complete inability to detect any component failures (9)
- $\overline{T}_{\overline{d}}$ Defects resulting in a false alarm at the next test cycle (8)

In practice, several other circumstances than those listed above can, of course, be of interest: Power system faults can exert influence on the protection system, e.g. by damaging instrument transformers, by generating surge voltages on wiring and by reducing the level of PLC signals. Furthermore, the test device can have a defect causing a failure of the protective function itself.

Although it is possible to calculate the behaviour of models with many states with the help of a computer (see ref.1), the state diagram finally used was limited to 17 states. It is important to keep in mind that any model is a rough approximation of reality. The absolute values of the results must be interpreted with caution. The main benefit is to see trends in the various availabilities due to automatic testing, selfchecking and monitoring and when changing the main parameters.

Combination of the various states

The state diagram for the complete system consists of combinations of the above states. There would be 45 states, theoretically (or more, if considering multiple defects of components). Many of them are, however, not of interest for our analysis. For example, no defects in the protective scheme, and no defects in the automatic testing device, combined with a power system fault within the protective zone will lead to a normal correct fault clearance. The corresponding state will, however, be of very short duration and can thus be neglected.
The unavailability states 10 and 11 due to testing are also quite short, but still considerably longer, and have thus been maintained.

States 13 and 14 represent combinations of defects in the supervision and in the supervised circuits. Each state obviously can be reached on two different paths, depending on which defect occurs first. Both states are relatively short, whereby state 13 will always be shorter (or more unlikely) because the "drain" is larger, as will be explained. (Readers already familiar with markov chains may skip the explanation which follow).

The diagram, infact, can not only be used for an accurate calculation of the state probabilities by means of the markov technique, but gives a good picture of the behaviour of the system. Incidentally, such diagrams are used to study very different systems (movement of populations, flow of material in a factory, waiting queues, random walks) where a stochastic process takes place.

Thus, it may be helpful to imagine the states as cities and the arrows as rates of emigration and immigration of people. The probability P4 of a person staying in particular city (No.4) is the analogue to the probability of our system being in a state of a non-detected defect in the protection of the potential incorrect operation mode (state 4). The probability of a person moving from 4 to 17 is the product of probability P4 and the rate of transition $\sigma 1$. It is analagous to an incorrect operation for a fault outside the protected zone after a defect of mode 3 has happened.

One important condition is that the states exclude each other and their probabilities add up to 1.

Comparing again states 13 and 14, we realize that the "immigration" is relatively low to both, but the emigration from 13 is higher since $\sigma 1$ has been assumed as 5 times $\sigma 2$. The computer outputs indicate infact for state 13 a probability which is 2.4 to 4.3 times lower than for state 14.

The model yields a lot of information: probability (availability) of each state and frequency of passing through a certain state (e.g. frequency of repairs, outages etc.). The usefulness of the results, of course, depends on the accuracy of the model and of the input data.

Mathematically, the behaviour of the system can be described by a set of linear differential equations (as a continuous process), or by a markov chain (stochastic step-by-step process).

At this point, it is important to mention that the process can be divided into a transient and a steady state part. In our case, e.g. we normally start with a new, fully available system in state 1. It means, that the probability P1 (t = 0) = 1. In case of the population movement process, it means that initially everybody lives in city No. 1. After some time, the distribution of the population will stabilize and remain unchanged, i.e. immigration and emigration to a given city is balanced. Very often, the final, steady state distribution does not depend on the initial state; it is called an ergodic process. This is also the case for our examples.

In our examples, the steady state is attained practically already after 3 to 5 years. The evaluation which follows therefore considers only the steady state for reasons of simplicity (the curves, shown in fig. 14, on the contrary, have been calculated by integrating P(t)).

The meaning of the states 15, 16 and 17 needs some comments. They correspond to states (5 + 6) respectively (9 + 10) in fig. 2, i.e. the situation immediately after a maloperation. While the power system will be restored immediately to normal, either by a back-up protection with autoreclosure or, with a very short delay, manually, the repair of the protection will take longer of course. (In the whole diagram the repair time for all cases has been assumed to be 24 hours.)

The states 15, 16 and 17 therefore do not represent the down time of the power system, and their duration is not so meaningful. It is, however, important to have them in the diagram as separate states, in order to be able to calulate how <u>often</u> we have such outages, in the average.

Two different fault detection ability factors have been defined, in line with section 4.3, using the simple model shown in fig. 17.

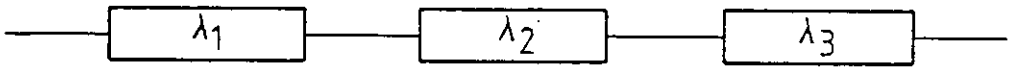


Figure 17

λ_1 : Failures which cannot be detected neither by automatic nor by automatic testing

λ_2 : Failures which can be detected by automatic testing. Since a manual test will always include an automatic test run, these defects will also be detected at each manual test.

λ_3 : Defects which can only be detected by manual testing. It is a measure of the additional depth obtained thanks to the know how and experience of the specialists.

The fault detection ability factors are

$$\text{for automatic testing } \alpha_{AT} = \frac{\lambda_2}{\lambda_1 + \lambda_2 + \lambda_3}$$

$$\text{for manual testing } \alpha_{M} = \frac{\lambda_2 + \lambda_3}{\lambda_1 + \lambda_2 + \lambda_3}$$

The same values have been used for the $\lambda_1, \lambda_2, \lambda_3$ and hence for the α's for both failure modes. This simplification was made as no data were available indicating that there was a general bias towards one of the two. In Reference 7 (section 2.2) , percentages of 42% and 58% are published for the incorrect operation mode and failure to operation mode, which means that our assumption might be quite acceptable for conventional electronic devices. For microprocessor based quipment this assumption must certainly be reviewed.

5.1.3 Selected input rata

For a first set of curves (Fig.18a,b), the average annual numbers of incorrect operations and failures to operate has been plotted against the variable α_{AT}, the fault detection ability factor of automatic testing. Another set of curves (Fig.19a,b) shows the number of component failures detected by power system faults, manual testing and automatic testing. It illustrates the efficiency of manual and automatic testing. The variable is again α_{AT}.

Since the unavailability of the protection is an important measure, the graphs in Fig. 20a,b shows the probabilities of the most important states of the diagram, where the protection is not available for one or another reason.

A reference case has been chosen with the input data (transition rates) as below, and four other curves have been calculated, varying the basic MTBF, the rates of primary system faults and the fault detection ability factor for manual testing, one at the time.

Reference case: (Curve 1)

(all rates per annum):

- External power system faults $\sigma_1 = 5$
- Internal power system faults $\sigma_2 = 1$
- Repair rate (MTTR = 48 h) $\mu = 182.5$
- Rate of automatic testing (once a week) $\tau_{AT} = 52$
- Failure detection rate for automatic testing (average time till detection is half a week) $\lambda_{AT} = 104$
- Inverse of meantime for automatic testing (1 min) $\nu_{AT} = 5{,}3 \cdot 10^5$
- Rate of manual testing (every two years) $\tau_M = 0{,}5$
- Failure detection rate for manual testing $\lambda_M = 1$
- Inverse of meantime for manual testing (8 hours) $\nu_M = 1095$
- Failure rate of protection including CT's, PT's, auxiliary DC, trip circuit etc., for each mode $\lambda_1+\lambda_2+\lambda_3 = 0{,}05$
- Failure rate for instantaneous incorrect operation $\lambda_4 = 0{,}01$
- Fault detection ability factor $\alpha_M = 0{,}9$
- Fault detection ability factor $\alpha_{AT} = 0;0{,}5;0{,}76;0{,}9$

  Failure rates of automatic testing device, both modes $\lambda'_{AT}=\lambda''_{AT} = 0{,}01$

Influence of MTBF (curve 2)

- Failure rate of protection, for each mode
- (Otherwise same as 1) $\lambda_1+\lambda_2+\lambda_3 = 0{,}1$ (instead 0,05)

Influence of power system fault rates (curve 3)

- External power system faults $\sigma_1 = 20$ (instead of 5)
- Internal power system faults $\sigma_2 = 4$ (instead of 1)
- (Otherwise same as 1)

Influence of manual testing interval (curve 4)

- Rate of manual testing interval (every year) $\tau_M = 1$ (instead of 0,5)
- Failure detection rate for manual testing $\lambda_M = 2$ (instead of 1)
- (Otherwise same as 1)

Influence of "depth" of manual testing (curve 5)

- Fault detection ability factor $\alpha_M = 0{,}76$ (instead of 0,9)
- (Otherwise same as 1. Since $\alpha_M \geq \alpha_{AT}$ as stated in section 5.1.2, the curves end at $\alpha_{AT} = 0{,}76$)

5.1.4 Results of the calculations

Fig. 21 shows a printout of the computer for curve 1, α_{AT} = 0,76. It shows the probability of each state in half year intervals, beginning with a fully healthy system P1 = 1. As can be seen, the total system attains an almost steady state after a few years already. The evaluations were made after five years for all points.

TIME (a)	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
	P11	P12	P13	P14	P15	P16	P17			
0.00	1.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000
	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000			
0.50	0.988058	0.000909	0.000344	0.001098	0.001951	0.000358	0.002193	0.000095	0.003835	0.000020
	0.000451	0.000491	0.000018	0.000030	0.000030	0.000054	0.000065			
1.00	0.983659	0.000979	0.000343	0.001146	0.003122	0.000356	0.002987	0.000095	0.006050	0.000037
	0.000449	0.000506	0.000035	0.000075	0.000042	0.000054	0.000069			
1.50	0.981317	0.000982	0.000342	0.001146	0.003826	0.000355	0.003272	0.000094	0.007331	0.000050
	0.000448	0.000513	0.000045	0.000111	0.000047	0.000054	0.000069			
2.00	0.980008	0.000980	0.000342	0.001144	0.004230	0.000355	0.003373	0.000094	0.008072	0.000060
	0.000447	0.000518	0.000050	0.000136	0.000050	0.000054	0.000069			
2.50	0.979261	0.000980	0.000341	0.001143	0.004505	0.000354	0.003408	0.000094	0.008501	0.000068
	0.000447	0.000520	0.000054	0.000151	0.000052	0.000054	0.000069			
3.00	0.978829	0.000979	0.000341	0.001142	0.004658	0.000354	0.003420	0.000094	0.008750	0.000074
	0.000447	0.000521	0.000056	0.000161	0.000053	0.000054	0.000069			
3.50	0.978577	0.000979	0.000341	0.001142	0.004751	0.000354	0.003423	0.000094	0.008894	0.000079
	0.000446	0.000522	0.000057	0.000166	0.000053	0.000054	0.000069			
4.00	0.978429	0.000978	0.000341	0.001142	0.004806	0.000354	0.003424	0.000094	0.008977	0.000082
	0.000446	0.000522	0.000057	0.000170	0.000054	0.000054	0.000069			
4.50	0.978342	0.000978	0.000341	0.001141	0.004840	0.000354	0.003424	0.000094	0.009025	0.000085
	0.000446	0.000523	0.000058	0.000172	0.000054	0.000054	0.000069			
5.00	0.978290	0.000978	0.000341	0.001141	0.004860	0.000354	0.003424	0.000094	0.009053	0.000088
↓	0.000446	0.000523	0.000058	0.000173	0.000054	0.000054	0.000069			
years										

Figure 21 : Probabilities of states

Fig. 18a shows that the instantaneous incorrect operation remain constant at a value close to 0,01 per annum, as expected, since this type of failure cannot be influenced by testing according to our model.

The incorrect operations for external faults decrease rapidly with increasing depth of the automatic testing which is logical and the same applies to failure to trip operations. Since the fault detection ability factors for both failure modes have been assumed to be the same, this is not surprising. Also the influence of the MTBF is obvious.

It was hoped that a comparison between curves 1 and 5 would give an indication how much manual testing could be simplified by increasing the ability of automatic testing. The trend is correct but not very strong.

Curves 4 show that more frequent manual testing does not yield as much as one may expect, particularly for high α_{AT}. Automatic testing will most likely allow to increase the manual test intervals, as also suggested in Ref. 7.

Generally, the reduction of maloperations due to automatic testing is in the order of 4 to 5 for $\alpha_{AT} = 0,9$.
(Neglecting instantaneous incorrect operations).

In reference 5, (Table 3a) a detailed calculation for a particular distance relay has given reduction factors of about 2 for various types of faults.

In reference 7, on the other hand, the improvements calculated using a very complete state diagram (52 states), are very much higher, i.e. between 17 and 40 for the two modes "failure to trip" and "incorrect operation".

Fig.19a,b give an indication of how many of the component failures are discovered by automatic testing. For $\alpha_{AT} = 0,9$ it is about 75%. Reference 7, section 2.2., indicates a figure of 83% from practical experience.

The uppermost curves are horizontal between $\alpha_{AT} = 0,5$ and 0,9, because we have assumed that the additional failure rates due to the automatic test device do not depend on the test ability factor, for reasons of simplicity.

The failures "detected" by power system faults are remarkably high if there is no automatic testing, because we have assumed relatively high rates compared to the frequence of manual testing. Generally speaking, the curves give the feeling that manual testing is not so efficient. This, is, however largely due to the assumption that no preventive maintenance is possible, which is not quite correct. Furthermore, periodic manual inspections are anyway necessary to detect those hidden defects in the testing device which are not selfannouncing or also the socalled minor failures, as stated in table 1.

Fig.20a,b show unavailabilities, i.e. those periods of time when the protection is unable to perform the required functions. From the point of view of the power system, they are not as serious as the maloperations, but represent periods of severely reduced safety. As already stated, a high fault rate in the system reduces the unavailability, but this is of course not a true improvement, as the maloperations also increase as shown in Fig.18a,b.
The unavailability of the testing device also means a reduction of the safety of the power system, but to a much lower degree. A maloperation will only occur if, in addition, a failure in the protection happens followed by a systen fault.

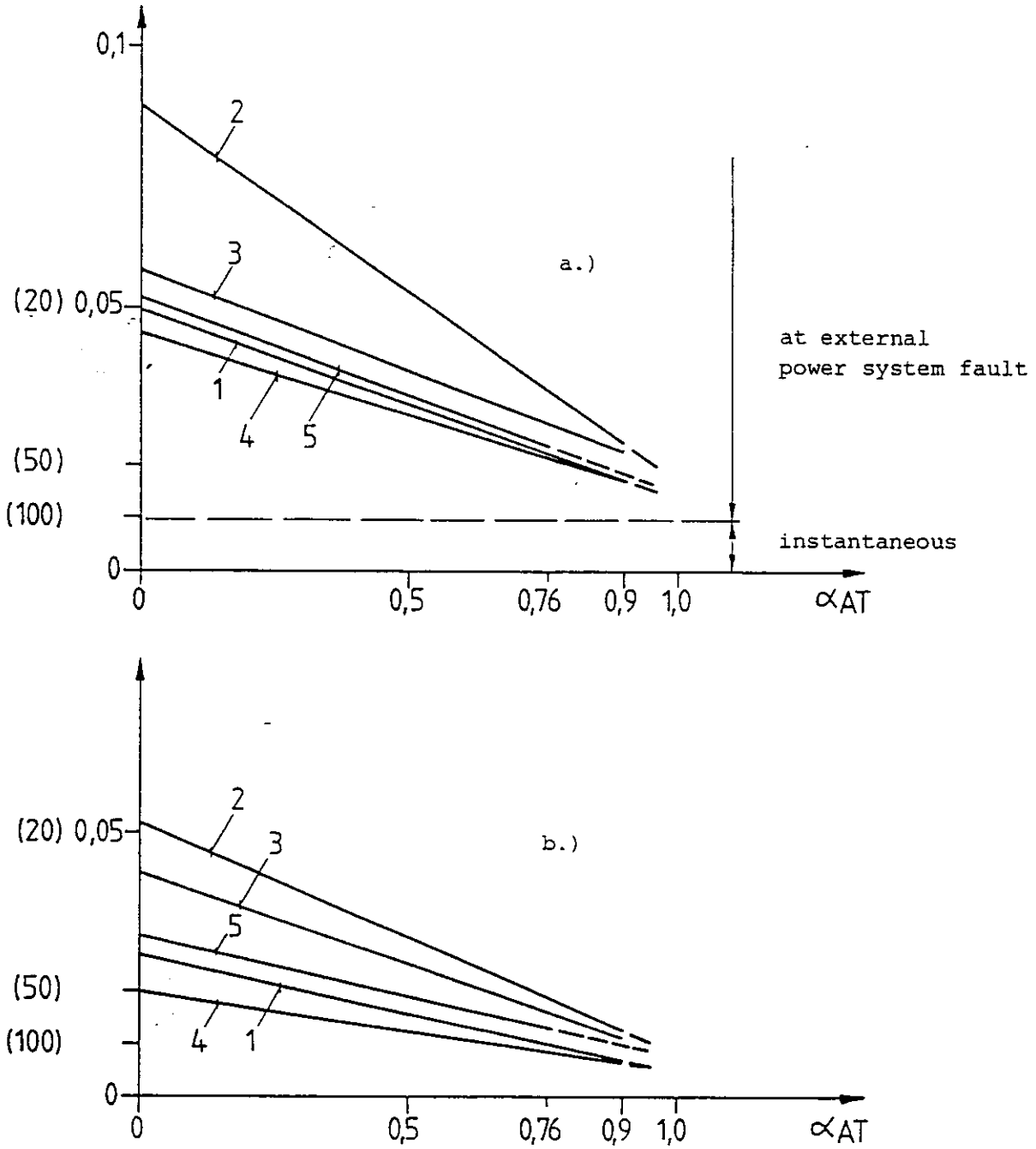


Figure 18: a.) Incorrect operations per annum, or MTBF's (in brackets)
b.) Failures to operate at internal power system fault per annum, or MTBF's (in brackets)
1 : Reference case
2 : MTBF divided by 2
3 : Power system fault rate multiplied by 4
4 : Manual test interval divided by 2
5 : Manual test ability factor 0,76 instead 0,9

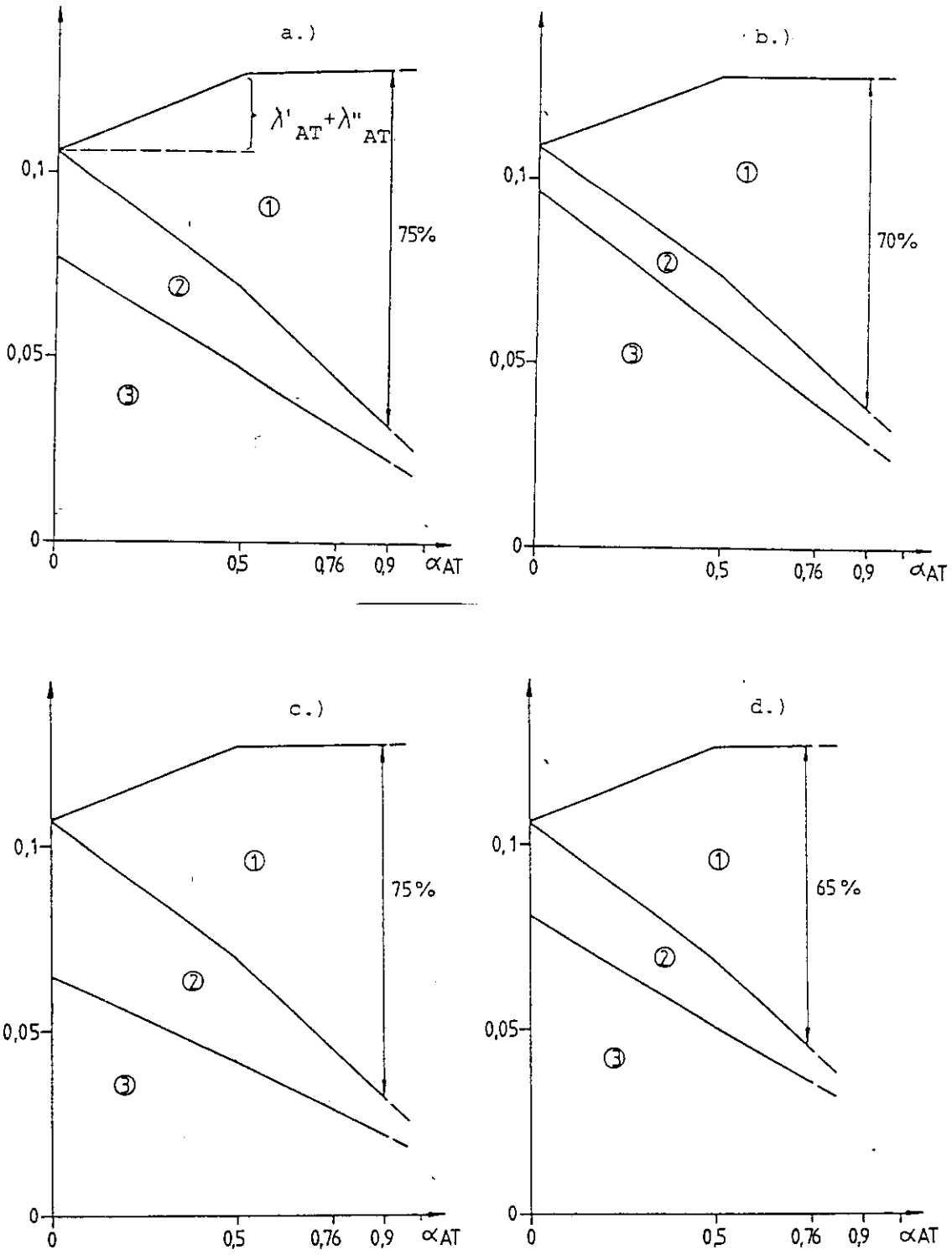


Figure 19: Number of component failures detected per annum
by
1 Automatic test
2 Manual test
3 Power system faults

a.) Reference case
b.) Power system fault rate multiplied by 4
c.) Manual test interval divided by 2
d.) Manual test ability factor of 0,76 instead 0,9
$\lambda'_{AT}+\lambda''_{AT}$: Additional failures due to automatic test device

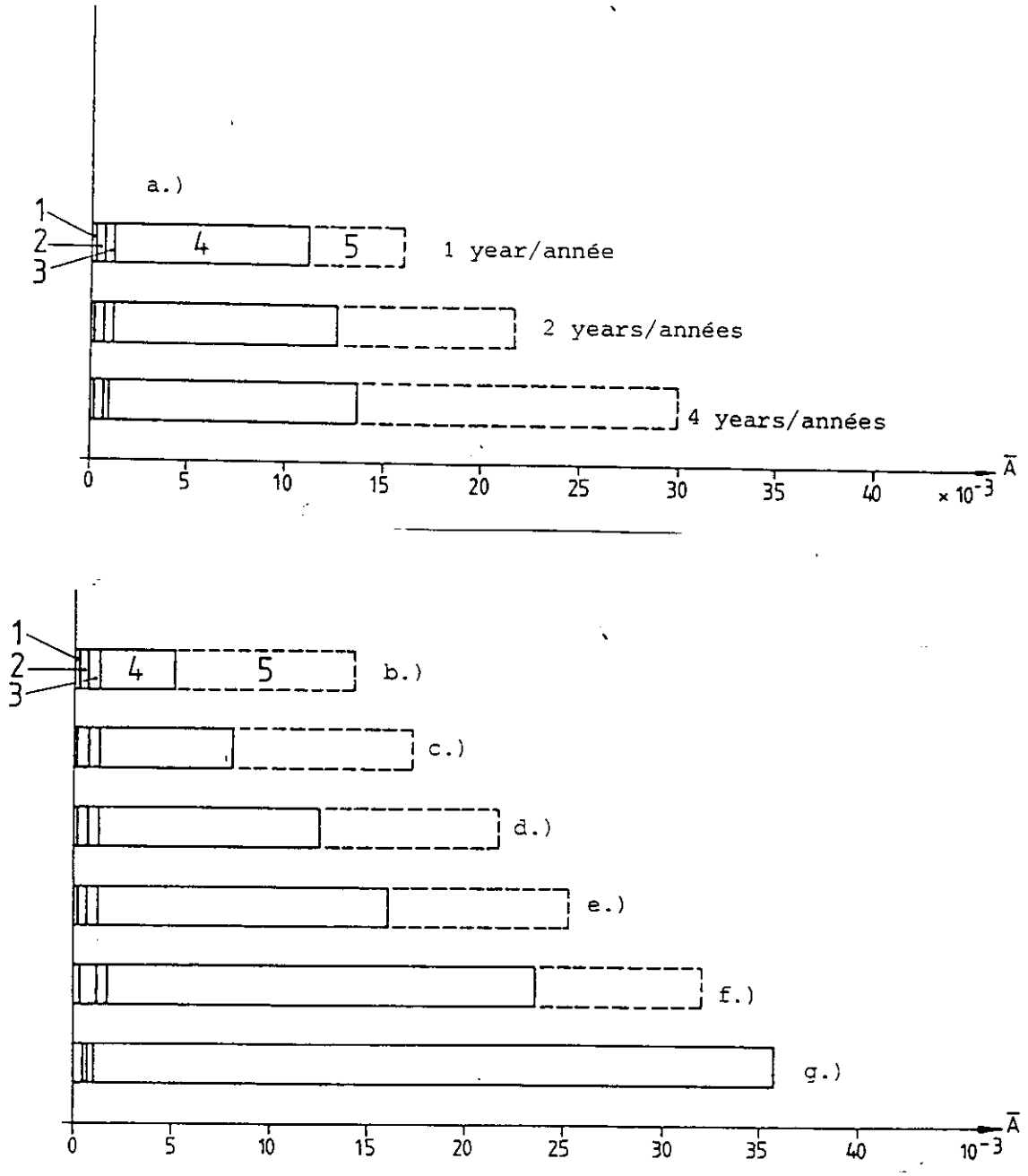


Figure 20: Influence of some factors on various unavailabilities of the protection scheme

Unavailability states:

1 : Repair after maloperation (states 15,16, 17)
2 : Repair after component failure detection (state 12)
3 : Testing periods (states 10, 11)
4 : Hidden failures (states 2,3,4,5,6,7,13,14)
5 : Only automatic test device unavailable (states 8,9)

a.) Influence of manual test intervals
b.) Power system fault rate multiplied by 4
c.) Automatic test ability factor α_{AT} = 0,76 instead 0,9
d.) Reference case α_{AT} = 0,76
e.) Manual test ability factor α_{M} = 0,76 instead 0,9
f.) MTTF divided by 2
g.) No automatic testing

5.1.5 Conclusions

The state diagram used yields results which seem to be reasonable and shows that automatic testing can substantially reduce the number of maloperations. This applies of course also to continuous monitoring. Thereby, the fault detection ability factor must be high enough, without, however, raising the failure rates λ'_{AT} and λ''_{AT} too much. In practice, it will be difficult to calculate this ability factor. It will also be different for the different failure modes. Considering that we have included also CT's, PT's, trip circuits etc. in the whole chain, the α_{AT} of 0.9 used in the reference case is probably too optimistic and 0.76 maybe closer to reality.
Furthermore, the rates for the failure modes of the testing device itself have only been roughly estimated. The rate λ''_{AT} of non-selfannouncing failures is rather pessimistic, since it can be assumed that most component failures would be detected at the next test cycle rather than at the next manual test. There is also the question whether these rates depend on the "depth" of the test device.

It becomes evident, therefore, that automatic testing and monitoring can yield very positive results even though the actual improvement cannot be quantified. It is also apparent that the traditional parameter to evaluate reliability, i.e. MTTF, is no longer sufficient. The MTTF itself is not improved. The ability, however, to establish that a failure has occurred, and to correct it before the scheme or device has had an opportunity to operate incorrectly, improves the availability. This, then, becomes the more important parameter. Availability depends, as shown, also on several other factors. It may, therefore, be necessary to find new ways to specify the reliability.

The method could also be applied to redundant scheme, e.g. two protection in parallel. However, the number of possible states would increase considerably and the treatment might require a lot of additional effort which is difficult to estimate. It depends very much whether the diagram could be simplified without becoming too inaccurate. Inasmuch as the advantages of self-checking and monitoring would be similar to the single protection scheme, the precise figures would add very little to the evaluation.

6. Economical aspects of automatic testing, monitoring and selfchecking

6.1 Maintenance cost

The cost for manual periodic testing varies from country to country and from utility to utility. It can be assumed that the cost for testing one high voltage line protection will be between 100 and 1000 USD if all the periodic tests for a whole station are coordinated into a single occasion. As an example, we shall take a high voltage line protection, considering the large number of line protections in a network.

In order to obtain a complete picture, the cost has to be capitalized taking into account the test intervals and the interests. Figure 22 shows the present value of the cost for the maintenance tests during a 20 year period. With an interest rate of 10%, and assuming testing every second year, the present value for these tests during a 20 year period will be 4,2 times the cost for each individual test. The present value for the test of the line protection above will be 420-4200 USD. Assuming that by automatic testing, selfchecking and monitoring the need for manual testing can be reduced to 50% of the present value, there will be a saving of 50%. Thus, the cost reduction for manual periodic testing can justify an investment for automatic testing of 210 - 2.100 USD in each line protection.

6.2 Outage cost

The value of an increased reliability in the fault clearing function can be evaluated using the cost for outages. One European state power board evaluates lost delivery to the consumer to 0,38 USD/kW and 1,38 USD/kwh.

This includes the cost for the utility and the losses for the consumer due to the outages. By using this cost an an example and assuming an average outage time of 3 minutes the outage cost will be for example:

$$0{,}38 + \frac{3}{60} \cdot 1{,}38 = 0{,}45 \text{ USD/kw.}$$

Assuming an average load of 550 MW and 100 MW on a 400 kV respectively 150 kV overhead line the outage cost for the line will be 247.500 USD resp. 45.000 USD.

However, not every failure to trip or incorrect tripping of a single relay protection will lead to an outage for the consumers. Assuming that only one out of five cases will result in outages the cost will be 49.500 USD respective 9.000 USD for a maloperation of a 400 kV resp. 150 kV line protection.

Assuming a primary fault rate of 1 fault/year and line together with 1% rate of failure to trip and 3% of incorrect tripping the number of maloperation will be:

$$\frac{(1 + 3)}{100} \cdot 1 \cdot 20 = 0{,}8 \text{ over a 20 year period.}$$

The cost associated with the maloperations over the 20 year period will be 39.600 USD and 7.200 USD for the 400 kV and the 150 kV line respectively.

Assuming that by automatic testing, selfchecking and monitoring the rate of maloperation can be decreased by 50% the outage cost over the 20 year period will be reduced by 19.800 USD to 3.600 USD for a 400 kV to a 150 kV line, respectively.

The reduced cost above over the 20 year period will with a 10% interest rate justify an investment of 0,426 . 19.800 = 8.400 USD to 0,426 . 3.600 = 1.500 USD.

It is clear, that a calculation as shown above will always be very schematic and, to some degree, a guess work, but it may give a rough indication of the cost involved.

From the above we can conclude that if the rate of maloperation of the line protection can be substantially decreased the lower outage cost can pay-off relatively expensive equipment for automatic testing, selfchecking and monitoring on extra high voltage lines.

The above statement is valid on highly loaded lines. For other types of protection like transformer and generator protection, the economical benefit is highly dependent on the directly available spare capacity. Big transformers and generators are mostly equipped with redundant protections connected in parallel. These protective schemes have a very high dependability and an economical benefit from a further increase in dependability due to automatic testing, selfchecking and monitoring is doubtful. The economical benefit would have to be justified by the increased security and reduced number of incorrect trippings. Since, however, full and directly available spare capacity exists in most cases, the economical benefit will be limited.

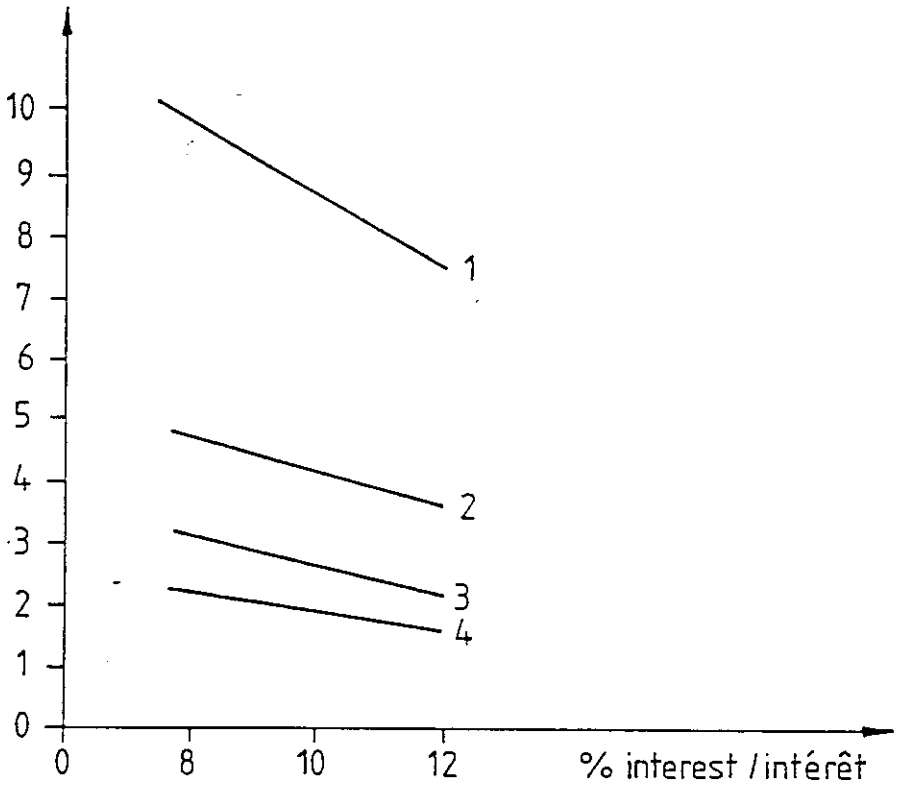


Figure 22 : present value of cost for periodic manual testing

7. Definitions of terms and symbols used

Terms

The following definitions are partly taken from IEC publications 271 and 271a, partly from the report 1 WG 34-05, Madrid 1981.

Power-System Fault (WG 34-05)

A power-system fault is defined as any fault or power-system abnormality which involves or is the result of failure of a primary-system circuit or item of primary-system plant or equipment and which requires the disconnection of the faulted circuit, plant or equipment from the power-system by the automatic tripping of the appropriate circuit brakers. Simultaneous power-system faults at different points on the power system are counted as separat incidents as are faults resulting from manual or automatic reclosure on to persistent power-system faults.

Non-System Fault (WG 34-05)

A non-system fault is defined as any incident which results in unwanted circuit breaker tripping as a consequence of a cause other than an power-system fault condition, such as the unwanted operation of protection in the absence of a power-system fault condition or the tripping of a circuit breaker due to some other secondary equipment failure or to human error.

Failure to Operate (WG 34-05)

An equipment is considered to have failed to operate if, when called upon to operate under the stated conditions, it fails to so or fails to do so within its specified maximum operating time.

Incorrect Operation (WG 34-05)

The operation of an equipment is considered incorrect if such operation occurs when it should not. Such incorrect operations, or maloperations, may occur under system-fault conditions or non-system fault conditions.

Maloperation

Failure to operate or/and incorrect operation

Dependability (WG 34-05)

Dependability is defined as the probability that a device, an equipment, or a system, will operate correctly.

Security (WG 34-05)

Security is defined as the probability that a device, an equipment, or a system, will not operate incorrectly.

Availability (WG 34-05)

Availability is defined as the proportion of time, considering a suitable period, in which a device, an equipment, or a system, is in service in a healthy state, to perform its intended function. Considering a suitable period, therefore, the availability is given by the ratio:

$$A = \frac{\text{Up time}}{\text{Up Time + Down Time}}$$

where Up Time = time in service in a healthy state

and Down Time = time out of service as a consequence of defects, including time spent in routine and remedial maintenance.

The availability may thus be defined in terms of the mean time to failure (MTTF) and the mean time to repair (MTTR) as the ratio:-

$$\frac{MTTF}{MTTF+MTTR}$$

Failure mode

The effect by which a failure is observed.
Note: For example, an open or short-circuit condition or a gain change.

Sudden failure

Failure that could not be anticipated by prior examination or monitoring.

Gradual failure

Failure that could be anticipated by prior examination or monitoring.

Catastrophic failure

Failure which is both sudden and complete.

Degradation failure

Failure which is both gradual and partial.
Note: In time, such a failure may develop into a complete failure.

Intermittent failure

Failure of an item for a limited period of time, following which the item recovers its ability to perform its required function without being subjected to any external corrective action.
Note: Such a failure is often recurrent.

Critical failure

Failure which is likely to cause injury to persons or significant damage to material.

Major failure

Failure, other than a critical failure, which is likely to reduce the ability of a more complex item to perform its required function.

Minor failure

Failure, other than a critical failure, which does not reduce the ability of a more complex item to perform its required function.

Redundancy

In an item, the existence of more than one means for performing a given function.

Active redundancy

That redundancy wherein all means for performing a given function are operating simultaneously.

Standby redundancy

That redundancy wherein the alternative means for performing a given function are inoperative until needed.

Symbols

σ_1	:	Rate of external power system faults
σ_2	:	Rate of internal power system faults
λ_1	:	Rate of protection failures, detectable by automatic tests
λ_2	:	Rate of protection failures, detectable by manual test only
λ_3	:	Rate of protection failures, not detectable by testing
λ_4	:	Rate of protection failures, instantaneous incorrect tripping
λ'_{AT}	:	Rate of failure of automatic test equipment; cannot detect any failures
λ''_{AT}	:	Rate of failure of automatic test equipment; gives a false alarm
λ_M	:	Rate of failure detection by manual testing
λ_{AT}	:	Rate of failure detection by automatic testing
τ_M	:	Rate of manual testing
τ_A	:	Rate of automatic testing
ν_M	:	Inverse of meantime for manual testing
ν_A	:	Inverse of meantime for automatic testing
μ	:	Repair rate
α_M	:	Fault detection ability factor for manual tests
α_{AT}	:	Fault detection ability factor for automatic tests

8. References

1 Bennett A., Webb A.C.: Computer techniques for the monitoring and testing of modern protection relays. CIGRE report 34-02, 1984

2 Kimura S., Okumara M., Andow F., Mitani J.: Automatic test facilities built into protective equipment and service history. CIGRE report 34-03, 1980

3 Fiorentzis M.: New Fully Automatic Means for testing Generator Protection Equipment. Brown Boveri Review No.2, 1977

4 Lohage L., Axelson G. : Detection of faults on protection systems. CIGRE Report 34-01, 1984

5 Yip H.T., Weller G.C., Allan R.N.: Reliability Evaluation of protection devices in electrical power systems, Fourth National Reliability Conference - Reliability 83.

6 Malcolm J.G., Foreman G.L.: The need: Improved diagnostics - rather than improved R. 1984 Proceedings annual reliability and maintainability supervision.

7 Yaguchi T., Oura Y., Tsuboi A., Andow F.: In-service experience and reliability evaluation of protective relay systems with built-in automatic testing and supervision devices CIGRE report 34-05, 1984.

8 G.Brauner, B.Koetzold: Influence of relay reliability on power system availability, CIGRE SC 37 report No. 83 CE 08 B of meeting June 1983 in Oslo.

Le CIGRÉ a apporté le plus grand soin à la réalisation de cette brochure thématique numérique afin de vous fournir une information complète et fiable.

Cependant, le CIGRÉ ne pourra en aucun cas être tenu responsable des préjudices ou dommages de quelque nature que ce soit pouvant résulter d'une mauvaise utilisation des informations contenues dans cette brochure.

Publié par le CIGRÉ
21, rue d'Artois
FR-75 008 PARIS
Tél. : +33 1 53 89 12 90
Fax : +33 1 53 89 12 99

The greatest care has been taken by CIGRE to produce this digital technical brochure so as to provide you with full and reliable information.

However, CIGRE could in any case be held responsible for any damage resulting from any misuse of the information contained therein.

Published by CIGRE
21, rue d'Artois
FR-75 008 PARIS
Tel : +33 1 53 89 12 90
Fax : +33 1 53 89 12 99