n° 175

dependability of MV and HV protection devices

Marielle Lemaire
Was awarded her IEG engineer's certificate, with an option in physics engineering, in 1986. After two years spent in a laboratory in TUCSON university (Arizona), she joined Merlin Gerin where she contributed to development of static power converters. As dependability specialist and French expert in the WG7 work group of the IEC «reliability of protection devices» technical committee (TC 95), she has been involved in development of protection systems for medium voltage installations for the past 5 years.

ECT 175 (e) first issued august 1995

dependability of MV and HV protection devices

contents

1. introduction

purpose of the document

This document presents the various factors contributing to dependability of protection devices in Medium and High Voltage networks, together with the methods which can be implemented to meet dependability objectives.

It places special emphasis on:
■ taking dependability into consideration at the design stage;
■ the quality approach (software, qualification, manufacture) with techniques adapted to the constraints encountered in Medium and High Voltage;
■ analysis of experience feedback.

This document complies with the techniques used in the nineties for designing the new Sepam protection range.

protection devices

The main functions of a protection device are to detect network faults by monitoring various parameters (current, voltage....) and to transmit a circuit-breaker opening order should an abnormal situation be observed. A protection device generally protects one of the various components of an electrical distribution substation, such as an incomer, a line feeder, a motor or a transformer.

In Medium and High Voltage, these devices are often incorporated in the equipment containing the circuit-breaker (see figure 1). Environmental constraints are then severe (temperature, vibration, electromagnetic disturbances).

Protection devices are produced either using electromechanical technology (the oldest) or analog or digital electronic technology (known as static). A digital protection device (microprocessor based) can perform, in addition to its main protection role, automation, measuring, self-monitoring and communication functions. This device then forms a natural part of control and monitoring systems performing automation, status logging and mimic diagram functions (see fig. 2).

dependability requirements: a compromise between two undesirable events

The function of the protection systems associated with the circuit-breaker is to guarantee installation safety, while ensuring optimum continuity of electrical power distribution.
As regards protection, two undesirable events must never occur if this function is to be fulfilled:

■ first event to be avoided: **failure of the protection device to trip**.
The consequences of a non-eliminated fault can be disastrous (risk for persons, destruction of electrical substations, production loss...). For operational safety, the protection device must detect both selectively and promptly faults in the electrical network. This event can be avoided by increasing **availability** of the protection device.

■ second event to be avoided: **untimely tripping of the protection device**.

Continuity of energy supply is vital both for companies and electricity distributors. Untimely tripping of the protection device can cause considerable financial losses

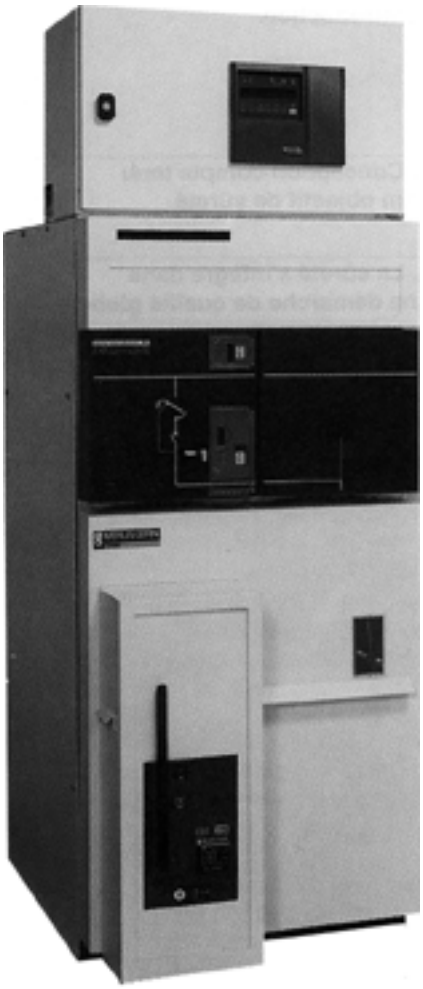

fig. 1: protection device incorporated in a Medium and High Voltage equipment.

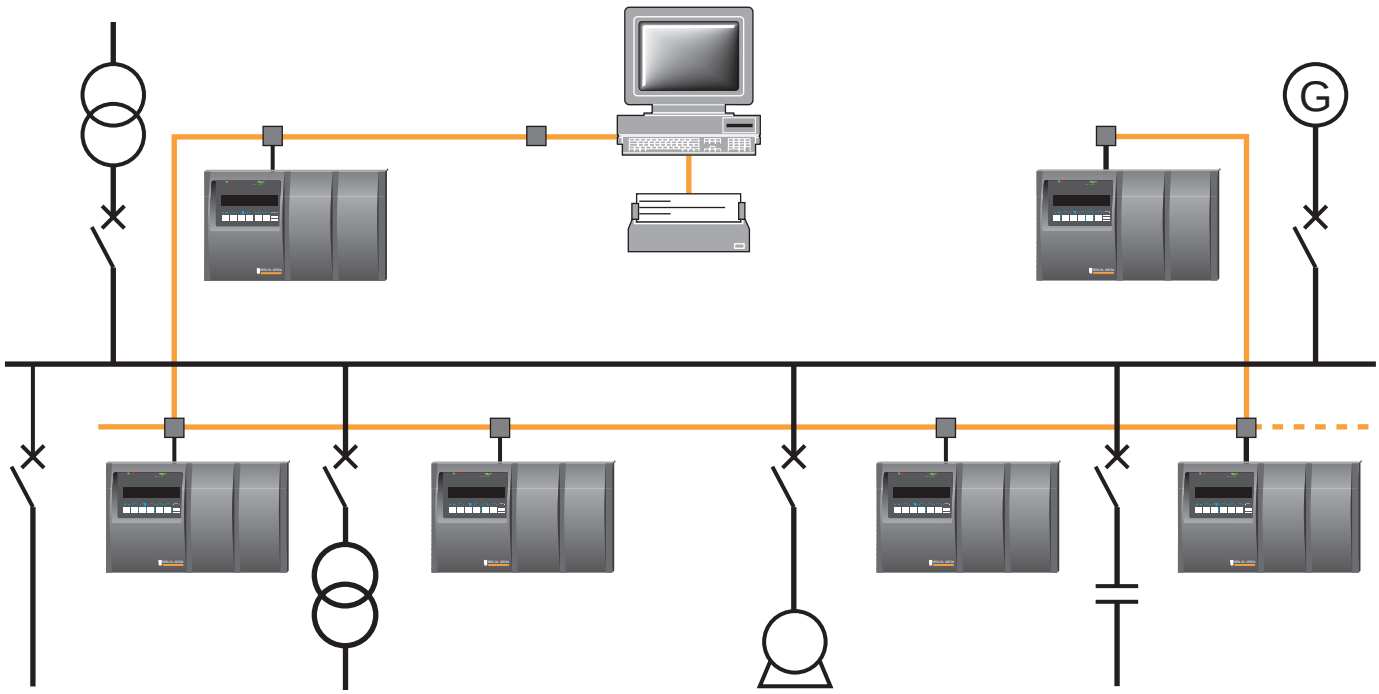

fig. 2: example of a digital control and monitoring system of a substation.

(production shutdown, cost of non-distributed energy...). This event can be avoided by increasing **safety** of the protection device.

Availability and safety are often oposite.

The best way for a plane not to crash is for it to stay on the ground. Its safety is then absolute, but its availability zero! Conversely, a plane which is in the air too often, without maintenance, places people's life in danger. The design of any device calls for a compromise between availability and safety.

Availability and safety are increased by using the other two components of dependability: maintenability and reliability (see fig. 3).

Protection devices are subjected to numerous aggressive factors which affect the undesirable events, e.g.:

☐ extreme temperatures,
☐ vibrations due to circuit breaker operations,
☐ corrosive atmospheres in industrial applications (chemistry, paper mills, cement plants...),
☐ intense electromagnetic pulse fields (up to several dozen kV/m 1 metre from a HV or MV circuit breaker with rise times of the order of 5 ns).

This extremely severe environment and the fact that MV and HV networks supply many electrical power users make controlled, optimised reliability and maintenability an absolute necessity.

Protection devices using microprocessors have enabled considerable headway to be made. For example:

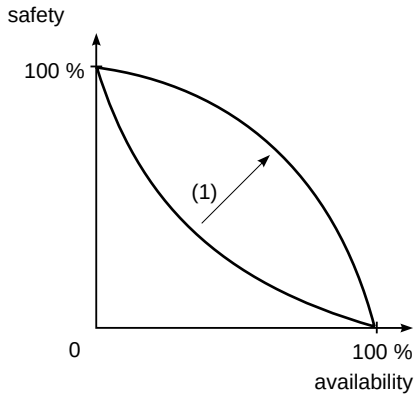

fig. 3: increasing reliability and maintenability (1) increases availability and safety.

☐ integration reduces wiring problems, thus increasing reliability,
☐ self-monitoring increases availability.

2. designing with dependability in mind

the terms used

As from the earliest stage in designing a protection device, the Reliability, Safety, Availability and Maintenability objectives must be taken into account.

These terms are reviewed below:

■ availability is the likelihood that a protection device will be in a state to perform its function, in given conditions, at a given time;

■ safety is the likelihood that a protection device will not trip in an untimely manner, in given conditions, for a given period of time;

■ reliability is the likelihood that a protection device will perform its function in given conditions for a given period of time, i.e. mainly the capacity to trip when required and the capacity not to trip in untimely manner;

■ maintenability is the likelihood that a given active maintenance operation will be performed in a given period of time.

These terms do not necessarily have the same meaning according to the standpoint: the protection device or the electrical installation.

Thus, availability and maintenability of the protection device contribute to safety of persons and equipment.

Safety of the protection device contributes to availability of electrical power distribution.

NB: these definitions comply with the International Electrotechnical Vocabulary-VEI 191- and are commonly used. A standard currently being prepared (WG 7 of TC 95) concerning reliability of protection devices lays down similar definitions, but includes the notion of «functional dependability» in reliability. However **dependability** remains the term englobing the others.

The various possible statuses of the protection device are shown in diagram form in figure 4, together with their consequences for electrical power distribution.

Availability is the ratio between the time spent in the operating status and the total reference time. Readers interested in quantification of dependability values can refer both to the appendix and Cahier Technique n° 144.

To return to figure 3, one of the objectives of the protection device designer is to treat preventively as many failures as possible (maintenability) to increase availability. As few events as possible should result in deterioration of protection device safety (the self-monitoring concept and resources will be described in the following sections).

As the networks to be protected are MV and HV ones, their dependability must be far higher than that of most LV equipment.

A Preliminary Risk Analysis is used to determine the undesirable events linked to the functions performed by the protection device (see fig. 5).

A team of specialists independent from the design team, carries out estimated dependability studies and proposes technical solutions compatible with the specified level. An iterative approach enables design to be modified until objectives are achieved.

the reliability engineer's tools

Specialised techniques for evaluating and modelling operational dependability allow design constraint objectives to be listed.

■ the estimated reliability analysis determines the failure rate of each component of the device in real operating conditions.

Reliability databases such as the Military Handbook 217 (MIL-HDBK-217) (see fig. 6) or the CNET booklet (RDF 93) are used for this purpose and enable reliability of a circuit with several components to be calculated. If necessary, the designer modifies the load rate of some of them, or uses components with a long guaranteed lifetime (e.g. for chemical capacitors).

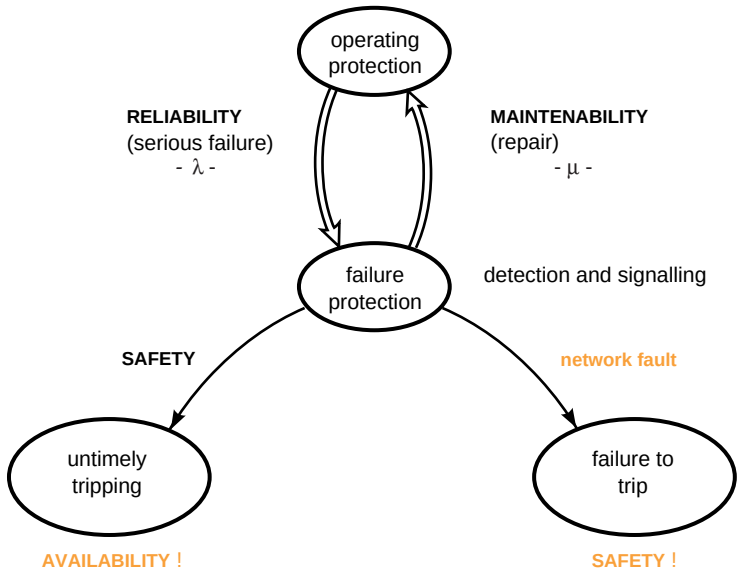

fig. 4: status graph for the protection device and consequences on electrical distribution.

event to be avoided	effects	causes	prevention
untimely tripping	■ untimely opening of circuit-breaker ■ power unavailability causing severe financial losses (production shutdown...)	■ internal, for example: ☐ untimely detection of a fault, ☐ untimely activation of the control mechanism ■ external, for example: ☐ electromagnetic disturbances ☐ sensor saturation ☐ error in protection plan design	for example: ■ self-monitoring functions ■ fall-back position ■ electromagnetic compatibility ■ non-magnetic sensors
masking a tripping order	■ tripping an upstream protection level with possible local destruction of equipment ■ major destruction of equipment (fire...) if there is no upstream protection	■ internal, for example: ☐ failure to detect a fault; ☐ blocked control mechanism ■ external, for example: ☐ electromagnetic disturbances ☐ sensor saturation ☐ loss of auxiliary supply ☐ circuit-breaker tripping circuit open ☐ error in protection plan design	for example: ■ self-monitoring functions ■ electromagnetic compatibility ■ non-magnetic sensors ■ standby module ■ supervision of tripping circuit ■ logic discrimination

fig. 5: undesirable events relating to the protection function.

Microcircuits, gate/logic arrays and microprocessors

Description
1. bipolar devices, digital and linear gate/logic arrays
2. MOS devices, digital and linear gate/logic arrays
3. microprocessors

$\lambda_p = (C_1 . \pi_T + C_2 . \pi_E) \pi_Q . \pi_L$ failures/10^6 hours

bipolar digital and linear gate/logic array die complexity failure rate - C_1

digital		linear		prog. logic array	
no. gates	C_1	no. transistors	C_1	no. gates	C_1
1 to 100	.0025	1 to 100	.010	up to 200	.010
101 to 1,000	.0050	101 to 300	.020	201 to 1,000	.021
1,001 to 3,000	.010	301 to 1,000	.040	1,001 to 5,000	.042
3,001 to 10,000	.020	1,001 to 10,000	.060		
10,001 to 30,000	.040				
30,001 to 60,000	.080				

MOS digital and linear gate/logic array die complexity failure rate - C_1

digital		linear		floating gate prog. logic array	
no. gates	C_1	no. transistor	C_1	no. cells, C	C_1
1 to 100	.010	1 to 100	.010	up to 16 K	.00085
101 to 1,000	.020	101 to 300	.020	16 K < C **i** 64 K	.0017
1,001 to 3,000	.040	301 to 1,000	.040	64 K < C **i** 256 K	.0034
3,001 to 10,000	.080	1,001 to 10,000	.060	256 K < C **i** 1M	.0068
10,001 to 30,000	.16				
30,001 to 60,000	.29				

microprocessor die complexity failure rate - C_1

no. bits	bipolar	MOS
	C_1	C_1
up to 8	.060	.14
up to 16	.12	.28
up to 32	.24	.56

all other model parameters

parameter	section
π_T	5.8
C_2	5.9
π_E, π_Q, π_L	5.10

fig. 6 : example of reliability data as in the Military Handbook.

■ the Failure Modes, their Effects and their Criticity Analysis (FMECA) conducted both on hardware and software, evaluates the effects of each known failure mode on equipment operation.

FMECA is used to correct certain malfunctioning risks and to specify self-monitoring functions. It can be performed at general function level (the «protection» function), at elementary function level («overcurrent protection» function), at one of its subfunctions (see fig. 7) up to the lowest level of the basic components (implanted on the electronic boards).

■ the undesirable events concerning protection devices are modelled using a number of techniques:
□ **failure trees** describe all the possible causes of a particular event to be avoided (see fig. 8).
The failure tree is a boolean representation used to determine the most critical paths to produce the event.
□ **Markov graphs** are a behavioural representation showing operating status, downgraded operation and equipment failure. Transitions between status are quantified by failure λ and repair (μ) rates. These graphs are used to calculate the likelihoods of occupying failure status (see fig. 9).
□ **Petri nets** have the same purpose as Markov graphs, i.e. modelling system status. They enable processing of more complex systems whose transitions between status do not necessarily obey exponential distribution (e.g. Weibull's distribution) (see fig. 10)

These modelling processes enable quantified simulation of operational dependability, thus obtaining likelihoods for reliability, maintenability, availability and safety of protection devices.

Readers can find a more detailed description of these various techniques in the references [Villemeur] or [RGE] or [Pages-Gondran].

dependability resources

Reliability, safety and maintenability of protection devices must be controlled to guarantee optimum dependability of electrical installations.

As the objectives for these values are fixed, the protection device designer, assisted by the reliability engineer, uses a certain number of resources to achieve them:
■ thanks to the reliability engineer and his tools, he controls intrinsic reliability before and during development;
■ thanks to self-monitoring, failure signalling and communication resources, he can:
□ increase dependability by placing in the fall-back position,
□ increase maintenability and availability of the protection device.

Let us now look at the resources implemented:
■ self-monitoring
Efficiency and relevance of self-monitoring are vital for dependability of the protection device. Below are examples of some resources enabling availability and safety to be increased:

□ a check on integrity of information contained in the «program» and «constant data» memory boxes must be performed on energising and then cyclically during operation. This check is made by calculating the Checksum with carrying over on the memory zones used. The checksum with carry over covers 99.95 % for 128 bytes (99.998 % for 128 Kbytes) for pasting of address and of memory bits. For volumes of information to be checked exceeding a hundred bytes, calculation of the Checksum with carry over is more efficient than calculation of a CRC 16 for example (see reference [INRS]).
□ a hardware and software watchdog must be fitted to detect blocking of the CPU (due to a component defect, interference or microprocessor overload). The validity of the watchdog output signal must also be checked. The watchdog must cover failure of the microprocessor quartz and oscillator (see fig. 11).
□ program cycle time must be controlled. If interruptions are used to sequence cycles, it must be checked that these mechanisms are operating correctly.
□ a check on supply voltage must be continuously performed to anticipate possible voltage drops and stop the microprocessor «properly» (saving parameters).
□ if EEPROM memories are used, use of this component must be monitored by counting the number of writes which must not exceed 10,000.
□ false digital data must not be processed further to a failure in the analog to digital conversion string.

function	failure mode	effect on protection	detection resources	signalling
acquire the phase currents	false measured current: continuous level > tripping threshold	protection device activated Æ untimely tripping	the algorithm used works on calculation of current module at 50 HZ	"natural" inhibition of protection device
			detection by periodical calculation of signal dc component	signal failure on front panel and by communication
	false measured current: continuous level < tripping threshold	protection device unavailable Æ failure to trip if fault occurs	detection resources are the same	signal

fig. 7: FMECA table performed on a subfunction of the overcurrent protection device.

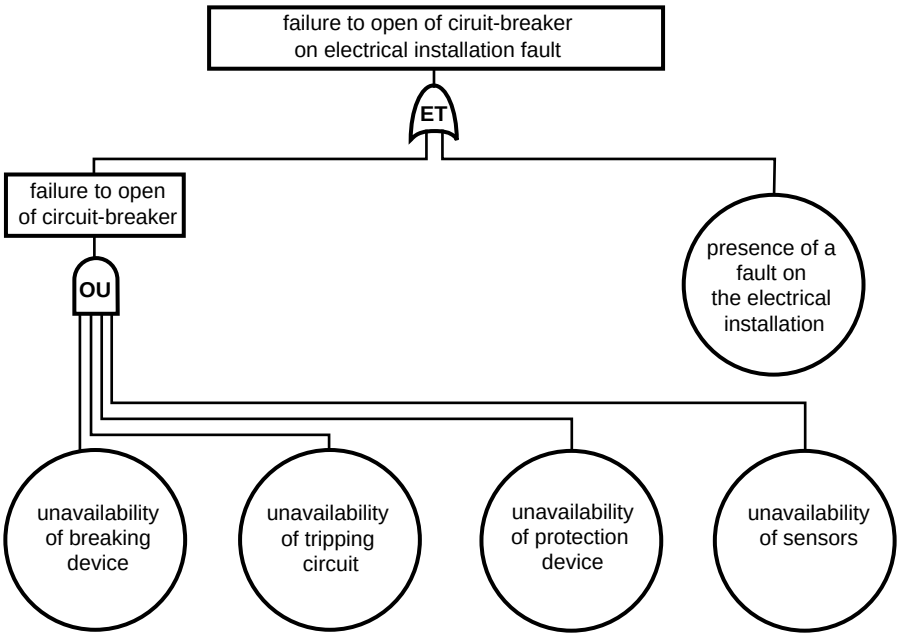

fig. 8: simple example of a failure tree.

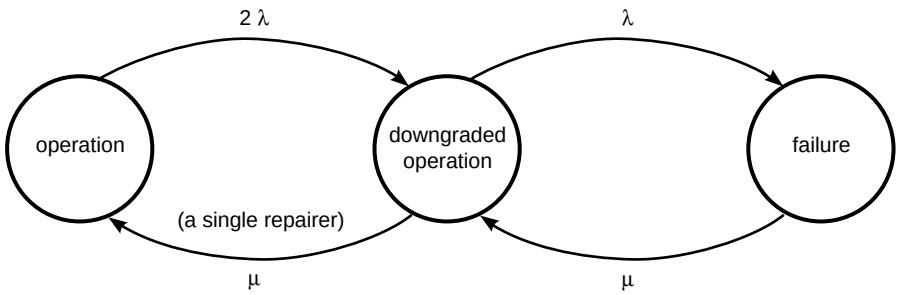

fig. 9: example of a Markov graph for a system consisting of two redundant, repairable components. If they are two electronic components (exponential reliability), the mean proper operating time after repair is $MUT = \frac{1}{2\ \lambda\ \lambda}$

The Petri net represented has two places (P1, P2), two transitions (T1, T2) and four arcs.
This net represents the behaviour of a repairable component, by assigning for example the following meanings to the places and transitions:
P1: the component is in proper operating condition.
P2: the component is not working.
T1: the component has failed.
T2: the component has just been repaired.

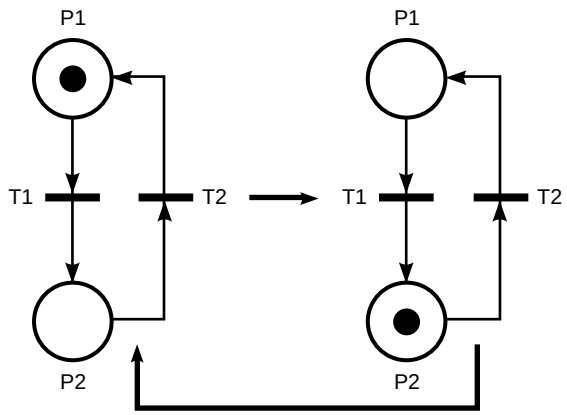

fig. 10: example of a Petri net for a system consisting of two redundant, repairable elements.

An efficient check consists in continuously verifying two reference signals at the input of the multiplexer at two complementary addresses (100 % of failures of the Analog to Digital Converter and 100 % of sticking at 1 or 0 of the Multiplexer selection bits are thus detected).
Many other detection devices are used, which are obviously very dependent on the technology used.

■ the reliable fall-back position
The self-monitoring functions detect as many «major» failures as possible. A failure is said to be «major» if there is a risk of it causing incorrect operation of the protection device.

To check data integrity

A number of techniques can be used
■ parity check
This consists in systematically making the number of bits transmitted even by completing the useful message by a «parity bit».
The receiver can thus check the message if there is an error on a bit or 3 bits. Alteration of an even number of bits cannot be detected.
■ the CRC (Cyclic Redundancy Check) consists in adding to the useful information the rest of its division by a polynomial standardised by the CCIT. For example, the degree 16 dividing polynomial
($X^{16} + X^{15} + X^2 + 1$=1100 0000 0000 0011) used for the «CRC 16» can detect 16 simultaneous errors.
■ the Checksum consists in performing the binary sum of bytes and in adding the result (truncated on one or more bytes) to the useful message.
The Checksum can be associated for example with the parity byte check....
Checking message integrity by the receiver is easier than for the CRC and can be more efficient.

To check proper running of a program

Often used in automation systems, the **Watchdog** technique consists in periodically running a test instruction. Non-running of this instruction, within a given time, reveals a failure and causes an alarm and an equipment protection device to trip.

fig. 11: self-monitoring reduces protection device unavailability time.

This type of failure must not degenerate into untimely tripping. The protection device places itself in a reliable, predetermined fall-back position to prevent passage of random orders. The operator is informed of this «fall-back» position and can immediately perform maintenance to restore the availability of the protection device. At the same time, a «minor» failure, for example a peripheral failure (display or setting console) is signalled, but does not affect availability of the protection device.

■ failure signalling
The self-monitoring functions must provide suitable diagnostic resources to enable a prompt resumption of operating status of the faulty protection device, i.e.:
☐ provide the operator with external, clear and global information on the status of his protection device,
☐ provide the manufacturer, during a maintenance operation, or even after return to the works of the faulty protection device, with internal, clear and precise information on the status of the protection device.

For example, failure of the protection device may be signalled by:
☐ a front panel indicator light,
☐ a WatchDog relay output,
☐ a message on the front panel display,
☐ internally saved information detailing failure origin,
☐ a message via the communication system when the protection device is part of a control and monitoring system.

This is a considerable advantage over older protection devices which could remain in a state of failure for long periods of time without the operator being aware of this (see fig. 12) and which thus provided no information on the origin of the failure.

■ a tendency to adopt supervision and control and monitoring systems
As stated earlier, digital protection can incorporate automation and communication functions. It thus becomes one of the links in the supervision and control and monitoring system of the electrical installation, thus simplifying operation by enabling supervision, operation and management of the distribution network:
☐ supervision of status and electrical quantities (measurements),
☐ supervision of devices (switchgear position, temperature, pressure,....)
☐ processing of alarms,
☐ remote control of switching devices,
☐ automatic reconfiguration of networks after fault,
☐ management of consumed energy as a function of distributors' tarifs,
☐ editing operating reports,
☐ allocating energy costs to the various site consumers.

■ ease of maintenance
☐ self-monitoring, signalling, communication facilitate knowledge of failure status, thus allowing immediate maintenance action,
☐ self-diagnostics enable the troubleshooter to know the origin of the failure, thus resulting in rapid troubleshooting,
☐ the programmed functions, customising the protection device in terms of applications/functions performed, are stored in a detachable cartridge. This enables immediate resumption of operation after replacement of the physical part (hard) which is standardised.

■ special cases
Reliability of the protection device may not be sufficient if it is subject to exceptionally aggressive factors or if the availability and safety needs of electrical distribution are exceptionally high:

☐ severe environment
Protection systems are sometimes installed in exceptional environments which exceed specified constraints for equipment:
- temperature,
- vibration...
In each case, needs must be specially identified by the engineering and design department. A customised solution is then proposed:
- special varnish on electronic boards,
- specific maintenance contract,

☐ an exceptional dependability need
A standby module can provide protection in the event of:
- a supply fault,
- a wiring fault,
- a trip release fault,
- main protection device not working.

Another solution is to backup the protection device with an «or» circuit in the breaking device control circuit. Installation safety is considerably increased, and electrical power availability is not reduced when protection systems with reliable fall-back position are used.

As an extreme solution, 2/3 vote systems can be considered.

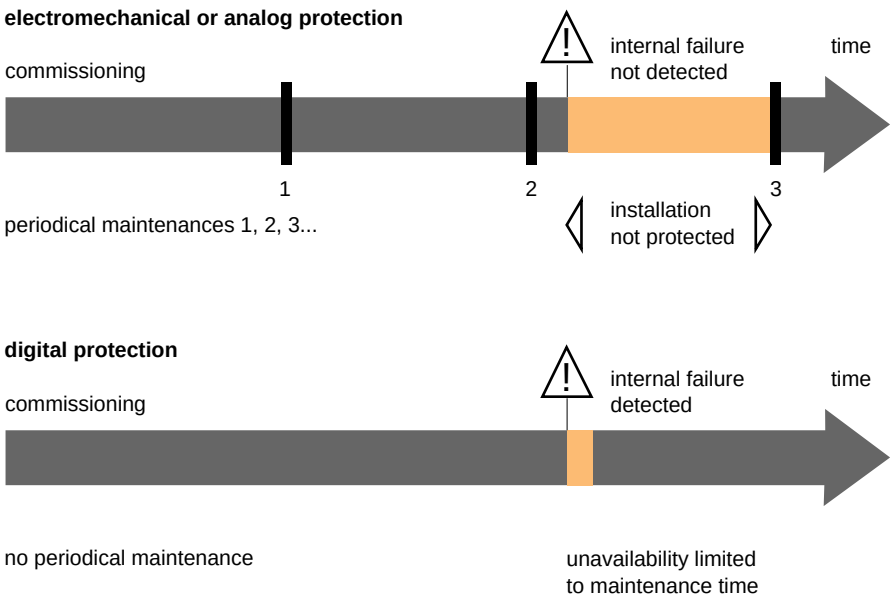

fig. 12: self-monitoring reduces protection device unavailability time.

3. dependability as a part of a global quality approach

software quality

A large part of digital protection device functions are performed by the software. Control of software quality is thus crucial to achieve global dependability objectives.

Software quality is controlled by using a rigorous development method. This method, resulting from the recommendations laid down by French (AFCIQ) and international (IEEE) organisations, stipulates:

■ breakdown of development into a series of phases (see fig.13):
☐ specification,
☐ preliminary design,
☐ detailed design,
☐ coding,
☐ unit tests,
☐ integration and integration tests,
☐ validation.

Each phase has a set of documents used and produced during the phase.

These documents formalise the studies conducted in each phase and must be validated before moving on to the next phase.

■ use of design and coding methods and rules aiming at obtaining a high software structuration level (e.g. SADT implemented in the ASA or MACH tool).

■ use of software configuration management tools enabling management of all software components and in particular control of the respective evolutions and versions of all these components (e.g. CMS tool).

Moreover, code reviewing methods are used to great advantage. A reviewer critically reads the code and makes his observations. This «manual» analysis is still one of the most efficient methods for discovering software errors (bugs).

Finally, once each software has been integrated and validated, a final qualification phase conducted by a team other than the development team ensures a last efficient check.

qualification of protection devices

Before protection devices are released on the market, they undergo a complete qualification.

Some qualification criteria specific to the Medium and High Voltage environment are detailed below.

■ immunity to electromagnetic disturbances (conducted and radiated).
The electrical disturbances encountered in electrical substations have a number of origins:
☐ lightning strokes falling directly on lines or close to the substation can generate overvoltages of some hundred kV and rise fronts of the order of a microsecond,
☐ normal operation of switchgear, on opening and closing of the MV and HV breaking device causes «switching operation» overvoltages (damped oscillatory wave). These overvoltages can cause electrical pulse fields of the order of 10 kV/m 1 metre from the circuit-breaker.
☐ the human operator can cause electrostatic discharge resulting on the equipment in current pulses of a few dozen amps and a very steep front of the order of a nanosecond,
☐ radioelectric transmitters (e.g. walkie-talkies) generate fields of several dozen V/m 1 metre away.

Readers wishing to learn more about Electromagnetic Compatibility (EMC) can consult Cahier Technique n° 149.

Internal electrical stress withstand standards define the immunity levels required for operation of protection systems in electrical substations. These levels correspond to the withstands defined by IEC 255 standards or are even more severe. Compliance with the severity level defined is checked by tests. Four types of tests are performed:

☐ damped oscillatory wave (IEC 255-22-1) severity: class III, 2.5 kV,

☐ rapid transients (IEC 255-22-4) severity: class IV, 4 kV,

☐ electrostatic discharge (IEC 255-22-2)severity: class III, 8 kV,

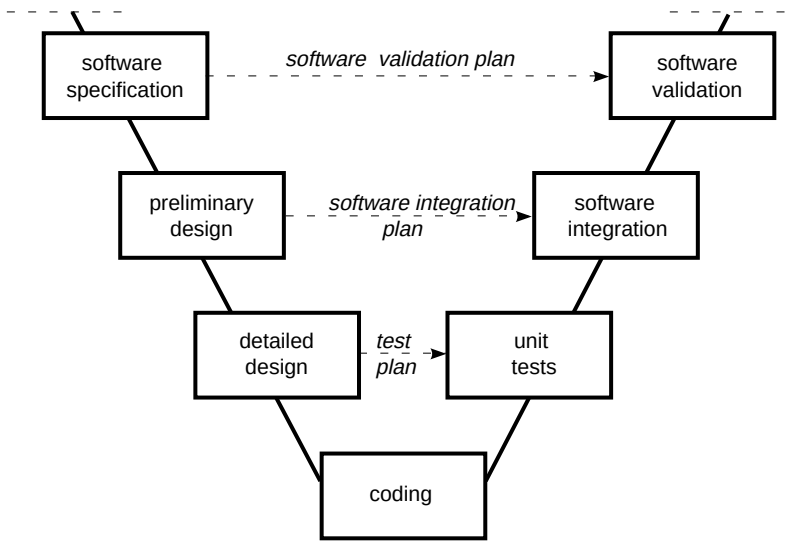

fig. 13: the software development cycle (V-shaped).

☐ radiated fields (IEC -255-22-3) severity: greater than class III, 30 V/m (see fig. 14)

NB: the rapid transient test is the transciption in «conducted» mode of «radiated» electromagnetic pulse fields, generated during switchgear operations.

In addition to EMC tests, protection devices undergo «real-life» situation tests. For example, after placing the device in the Low Voltage compartment of a Medium and High Voltage cubicle, roughly one hundred circuit-breaker opening and closing operations, on a load imposing arc breaking under a small inductive current (switching operation overvoltages due to current pinching) were performed.

During these tests, untimely tripping of the protection device must not occur.

■ the Kirchhoff laboratory: protection device testing

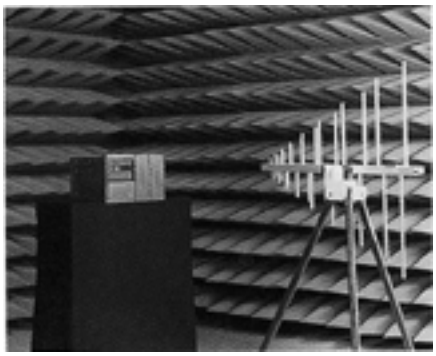

fig. 14: electromagnetic disturbance tests in anechoic chamber.

fig. 15: Kirchhoff protection device testing laboratory.

The functions performed by protection systems are complex. Proper operation of protection devices must be guaranteed for all the phenomena which can occur on electrical networks. An efficient laboratory for performing tests on protection devices is essential (see fig. 15).
The Kirchhoff laboratory enables real life reproduction of phenomena such as they occur on electrical networks (see fig. 16).
This laboratory is equipped with a digital simulator used to:
☐ calculate currents and voltages on the network, when a short-circuit, insulation failure or device switching operation occurs,
☐ generate the corresponding signals and apply them to the protection device to be tested. An analysis is then made of the behaviour of the protection devices subjected to conditions identical to those that they will encounter on the real network.

Digital simulation of electrical networks in the Kirchhoff laboratory uses two softwares:
☐ EMTP (ElectroMagnetic Transient Program), a program for calculating transient phenomena. This international software enables, from an equipment library (transformers, lines, machines,...) modelling of all kinds of electrical networks, simulation of

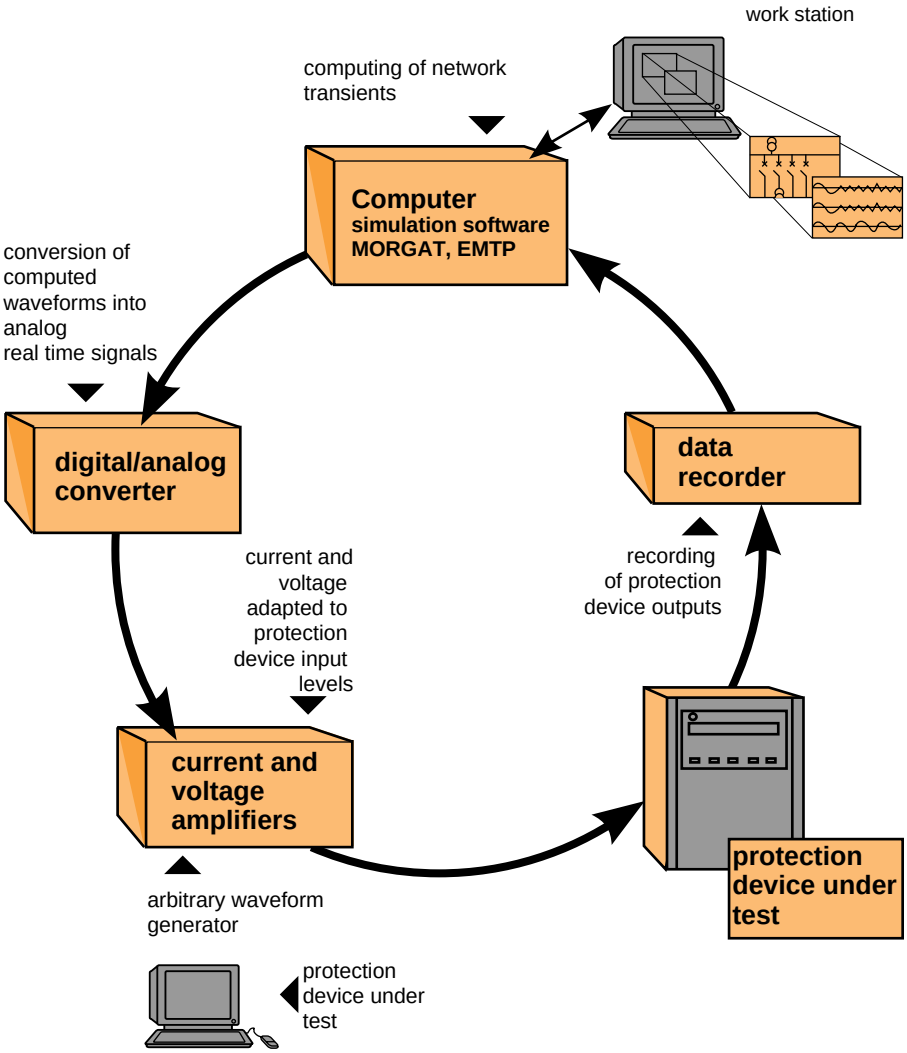

fig. 16: description of the protection device test system.

faults or device switching operation and precise calculation of evolution in current and voltage,
□ MORGAT, an electrical network simulator, developed and distributed by EDF. This software allows both fine analysis of network behaviour and control of the «real time» aspect of the Kirchhoff laboratory. Currents and voltages, calculated at different points of the simulated electrical network, are converted into analog signals for application to the protection device to be tested.

quality control

Protection devices undergo numerous quality control tests during production and at the end of production.
For example electronic boards undergo initial inspection on the dielectric test bay performing insulation tests.
They are then directed to the in-situ tester (see fig. 17).
The in-situ test checks proper operation and implantation of each electronic board component. It indicates mainly manufacturing defects and certain component defects. It provides an implicit dignostics and ensures prompt repair of the board. The results are then used by the quality department and allow rapid detection of any drift in component or board manufacturing quality.

After the in-situ test, the boards are burnt in under combined thermal and electrical stresses. Burn-in eliminates teething faults in electronic equipment and reduces the length of the early period so that these faults appear in manufacture rather than during operation. Likewise, the fault statistics are used by the quality department so that rapid action can be taken for any drift in manufacturing quality.

Final testing ensures that the assembled boards dialogue correctly with each other and that the configuration achieved really does correspond with the customer's order. All the expected functions are thus activated by stimuli applied to the interfaces of the device produced.

In addition to the systematic checks made on production, qualification tests are repeated periodically on a representative sample of the range.

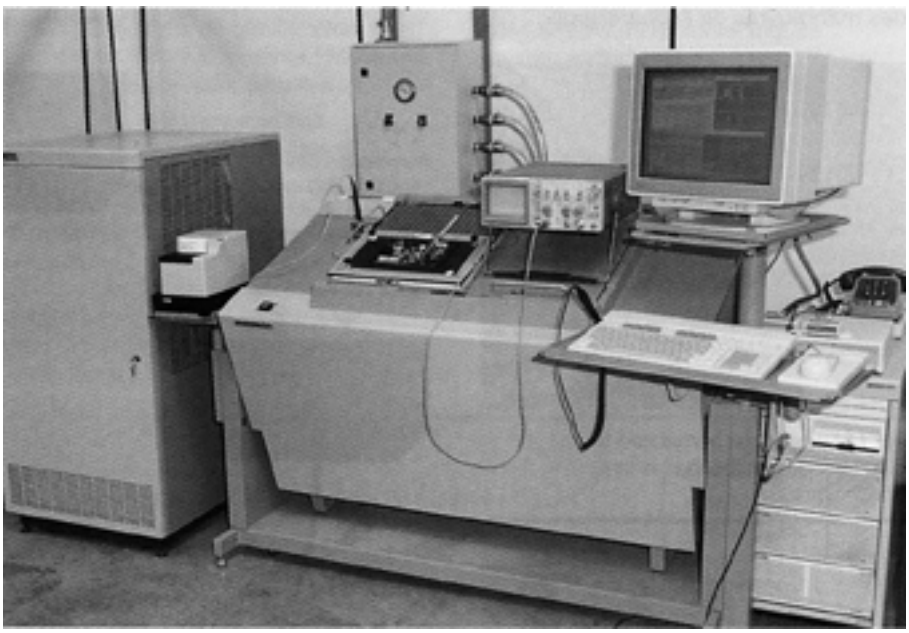

fig. 17: in-situ tester.

4. analysis of experience feedback

To ensure significant experience feedback, a very large installed equipment base must be in operation when reliability is excellent. Operating failure data can then be analysed. Analysis of experience feedback is vital to:

■ assess operational reliability of equipment;
■ validate the dependability studies conducted during design;
■ cumulate technical experience to progress;
■ possess a dialogue basis between the manufacturer and the operator.

Experience feedback relies on reliable and orderly gathering of information relating to incidents occurring at customers' premises. Operational reliability (calculated on experience feedback) is only relevant if failure can be detected, is detected and recorded. Failure data, resulting from an installed equipment base which has no self-monitoring functions and in frequent periodical maintenance, may not be representative of real reliability.

Operational reliability data on an installed base of digital protection devices are relevant due to the self-monitoring function.

It has been observed that operational reliability is at least greater by a factor 10 than estimated reliability (calculated from the data book MIL-HDBK-217E). This difference was probably the result of deliberately pessimistic and sometimes anachronistic reliability data books (electronic component technologies and quality evolve at a great pace).

Recent updates to reliability data books have considerably reduced the difference between the operational and estimated reliability results.

Today, the MTBF corresponding to untimely tripping or failure to trip of the protection device is several hundred years.

5. conclusion

Medium and High Voltage network protection devices perform a vital dependability function. They have to guarantee protection of persons and equipment, while ensuring availability of electrical power. Their malfunctions can inflict severe financial losses on operators. It is thus of prime importance that they meet high reliability, safety, availability and maintenability standards.

Consequently, protection devices must meet certain technical and industrial characteristics, of which the most significant are:

■ proper protection of MV and HV equipment and networks, by algorithms adapted to the various protection functions;
■ simplicity of implemenation, operation and maintenance;
■ reliability in severe environments, as well as:
□ ability to perform self-monitoring,
□ possession of a reliable fall-back position.

The work of reliability and quality engineers, at the design stage, ensures that the digital protection devices out on the market today meet all these requirements.

Today, taking advantage from development of digital communications (bus) and supervision, the functions of protection devices extend to the control and monitoring domain for optimised management of electrical power distribution.

6. appendix

Mean times characterising dependability (see fig. 18):

The MTTF (Mean Time To first Failure) is the mean time a device operates properly before failure.

The MTTR (Mean Time To Repair) is the mean repair time.

The MTBF (Mean Time Between Failure) is the mean time between two failures (for a repairable system).

The MDT (Mean Down Time) is the mean failure time including detection of failure, intervention time, repair time and resumption of operation time.

The MUP (Mean Up Time) is the mean time a device operates properly after repair.

The MTBF term is wrongly translated as the mean proper operation time. This definition actually belongs to the MTTF! The confusion stems from the fact that the MTTR (of the order of a few hours) is often tiny compared with the MTTF (of the order of several thousand hours).

The likelihoods

Reliability, R(t) is the likelihood that the system will not fail over a time t.

Maintenability is the likelihood that the system will be repaired in a time t.

Availability is the likelihood that the system will operate at a time t.

Safety is the likelihood that a disastrous event will be avoided.

A quantity which is the failure rate λ (t) is normally used for working purposes. This is the likelihood to break down in the next instant, bearing in mind that the system has not failed.

For electronic components, the failure rate follows an evolution in time known as the «bathtub» curve. During the «useful life» period, the component does not age and its failure rate is constant in time. The following fundamental relationships are then obtained:

Reliability $R(t) = e^{\lambda t}$ and $MTTF = 1 / \lambda$.

Example:

If a device has a MTTF of a 100 years, its failure rate $\lambda = 1 / MTTF$ is 10^{-2}/ year. The likelihood of failure each year is thus 1 %. This also means that out of 100 devices in operation, on average 1 device will break down each year!

A MTTF (or MTBF) of a 100 years on no account means that the system will not fail for 100 years. The MTTF cannot therefore be compared to a guarantee period or to a lifetime...

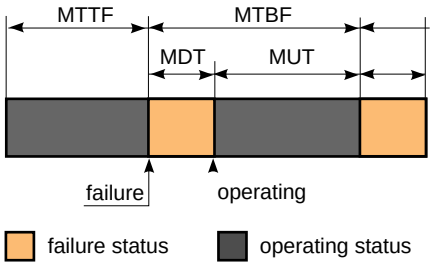

fig. 18: diagram of mean times, established for a system requiring no interruption in operation for preventive maintenance.

7. bibliography

Publications

■ Reliability design approach for protection and control equipment for MV distribution networks.
Second International Conference on the Reliability of Transmission and Distribution Equipment,
M. LEMAIRE, J.C. TOBIAS,
march 1995.

■ Electrical disturbance tests for measuring relays and protection equipment.
Part 1: 1 MHz burst disturbance tests.
Eyrolles EDF.
A. VILLEMEUR, 1988.

■ Fiabilité des systèmes
Eyrolles EDF
A. PAGES, M. GONDRAN, 1980.

■ Autotest d'une mémoire programme : deux solutions
Electronique n° 4, janvier 1991.

■ Military Handbook 217 -F-
Department Of Defense, USA.

■ Recueils de données de fiabilité des composants électroniques, RDF 93
CNET.

Standards

■ **IEC 255**
Electrical relays
□ **part 22:** Electrical disturbance tests for measuring relayus and protection equipment.
- section 1: 1 MHz burst disturbance tests,
- section 2: Electrostatic discharge tests,
- section 3: Radiated electromagnetic field disturbance tests,
- section 4: Fast transient disturbance test.

■ VEI 191.

Merlin Gerin's Cahiers Techniques

■ Introduction to dependability design
Cahier Technique n° 144
P. BONNEFOI 1991.

■ EMC: electromagnetic compatibility
Cahier Technique n° 149
F. VAILLANT 1991.

■ MV public distribution networks worldwide
Cahier Technique n° 155
C. PURE 1991.

■ Design of industrial networks in HV
Cahier Technique n° 169
G. THOMASSET.

■ Protection devices of industrial and tertiary HVA networks
Cahier Technique n° 174
A. SASTRE.

Réal. : Illustration Technique Lyon -
DTE - 08/95 - 2 500 - Imprimeur : Clerc