n° 175

sûreté des protections en MT et HT

Marielle Lemaire

A obtenu son diplôme d'ingénieur IEG, option génie physique en 1986. Après deux ans passés dans un laboratoire de l'université de TUCSON (Arizona), elle entre chez Merlin Gerin où elle participe au développement de convertisseurs statiques de puissance. Spécialiste de la sûreté de fonctionnement et expert français dans le groupe de travail WG7 du comité technique "fiabilité des protections" de la CEI (TC 95), elle participe depuis 5 ans au développement des systèmes de protection des installations moyenne et haute tension.

CT 175 édition mars 1995

sûreté des protections en MT et HT

sommaire

1. introduction

objectif du document

Ce document présente les différents facteurs contribuant à la sûreté des équipements de protection des réseaux Moyenne et Haute Tension ainsi que les méthodes qui peuvent être mises en œuvre pour répondre aux objectifs de sûreté.

Il développe notamment :
- la prise en compte de la sûreté en conception ;
- l'approche qualité (logiciel, qualification, fabrication) avec des techniques adaptées aux contraintes rencontrées en Moyenne et Haute Tension ;
- l'analyse du retour d'expérience.

Ce document est en accord avec les techniques utilisées dans les années 90 lors de la conception de la nouvelle gamme de protection Sepam.

l'équipement de protection

Un équipement de protection a pour principales missions la détection des défauts du réseau par surveillance de divers paramètres (courant, tension...) et l'émission de l'ordre d'ouverture au disjoncteur en cas de situation anormale. L'équipement de protection est généralement spécialisé pour réaliser la protection d'un des différents composants d'un poste de distribution électrique tels que : arrivée, départ ligne, moteur ou transformateur.

En Moyenne Tension, ces matériels sont souvent intégrés dans la cellule qui contient le disjoncteur (cf. fig. 1). Les contraintes d'environnement sont alors sévères (température, vibration, perturbations électromagnétiques).

Les équipements de protection sont réalisés soit en technologie électromécanique (la plus ancienne), ou bien en technologie électronique (dite statique) analogique ou numérique. Un équipement de protection numérique (à microprocesseur) peut effectuer, en plus de sa mission principale de protection, des fonctions d'automatisme, de mesure, d'auto-surveillance et de communication. Un tel équipement s'insère alors naturellement dans des systèmes de contrôle-commande assurant des fonctions d'automatismes, de consignation d'états, de synoptique (cf. fig. 2).

les besoins en sûreté : un compromis entre deux événements redoutés

Les systèmes de protection associés aux disjoncteurs ont pour mission de **garantir la sécurité de l'installation tout en assurant la meilleure continuité de la distribution de l'énergie.**

Au niveau de la protection, cette mission se traduit par deux événements dont l'occurence doit être nulle en terme d'objectif :

- premier événement redouté : **le non déclenchement de la protection.** Les conséquences d'un défaut non éliminé peuvent être catastrophiques (risque pour les personnes, destruction de postes électriques, perte de production...). Pour la sécurité de l'exploitation, l'équipement de protection doit détecter sélectivement et au plus vite les défauts du réseau électrique. Cet événement peut être évité en améliorant la **disponibilité** de la protection.
- deuxième événement redouté : **le déclenchement intempestif de la protection.**

La continuité de la fourniture d'énergie est impérative aussi bien pour un industriel que pour un distributeur d'électricité. Un déclenchement intempestif dû à la protection peut générer des pertes financières

fig. 1 : équipement de protection intégré dans une cellule Moyenne Tension.

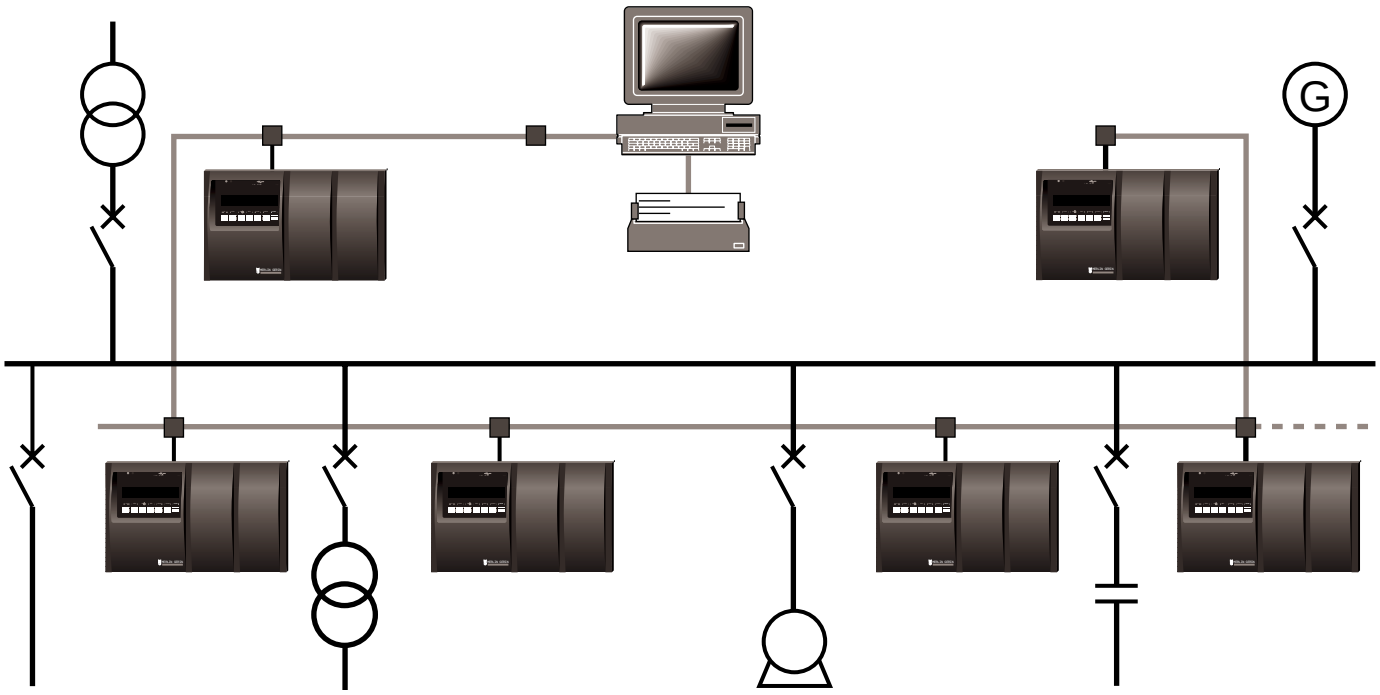

fig. 2 : exemple de système numérique de contrôle-commande d'un poste.

considérables (arrêt de production, coût d'énergie non distribuée...). Cet événement peut être évité en améliorant la **sécurité** de la protection.

Disponibilité et sécurité sont souvent contradictoires.

Le meilleur moyen pour un avion de ne pas s'écraser est de rester au sol. Sa sécurité est alors parfaite mais sa disponibilité est nulle ! Inversement, un avion qui vole trop, sans maintenance, met en danger la sécurité des personnes. La conception d'un équipement, quel qu'il soit, fait appel à un compromis disponibilité / sécurité.

Disponibilité et sécurité sont augmentées en jouant sur les deux autres composantes de la sûreté : la maintenabilité et la fiabilité (cf. fig. 3).

En ce qui concerne les équipements de protection, ceux-ci sont soumis à de multiples agressions qui influent sur les événements redoutés, citons :

- températures extrêmes,
- vibrations dues aux manœuvres des disjoncteurs,
- atmosphères corrosives dans les applications industrielles (chimie, papeteries, cimenteries...),
- champs électromagnétiques impulsionnels intenses (jusqu'à plusieurs dizaines de kV/m à 1 mètre d'une cellule avec des temps de montée de l'ordre de 5 ns).

Cet environnement très sévère, et le fait que les réseaux MT et HT alimentent de nombreux utilisateurs de l'énergie électrique, rendent nécessaires une fiabilité et une maintenabilité maîtrisée et optimale.

Les équipements de protection qui utilisent les micro-processeurs ont permis un progrès important. A titre d'exemple :

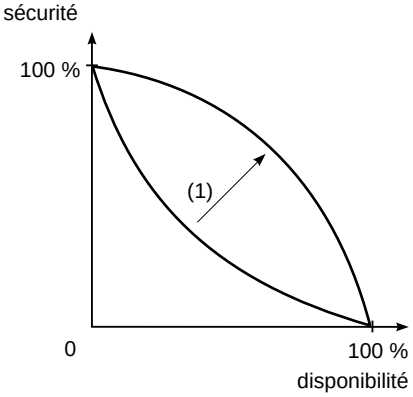

fig. 3 : augmenter la fiabilité et la maintenabilité (1) augmente la disponibilité et la sécurité.

- l'intégration diminue les problèmes de câblage et augmente la fiabilité,
- l'auto-surveillance augmente la disponibilité.

2. conception compte tenu d'un objectif de sûreté

les termes employés

Dès le début de la conception d'un équipement de protection, les objectifs de Fiabilité, Sécurité, Disponibilité et Maintenabilité doivent être pris en compte.

Rappelons les définitions de ces grandeurs :

■ la disponibilité est la probabilité pour une protection d'être en état d'accomplir sa fonction, dans des conditions données, à un instant donné ;

■ la sécurité est la probabilité pour une protection de ne pas avoir de fonctionnement intempestif, dans des conditions données, pour un intervalle de temps donné ;

■ la fiabilité est la probabilité pour que la protection puisse accomplir sa fonction dans des conditions données pour un intervalle de temps donné ; c'est-à-dire principalement l'aptitude à déclencher quand il le faut et l'aptitude à ne pas déclencher intempestivement ;

■ la maintenabilité est la probabilité pour qu'une opération donnée de maintenance active puisse être effectuée dans un intervalle de temps donné.

Ces grandeurs n'ont pas forcément la même signification selon que l'on se place du point de vue de la protection ou de l'installation électrique.

Ainsi, la disponibilité et la maintenabilité de la protection concourent à la sécurité des personnes et des matériels. La sécurité de la protection concourt à la disponibilité de la distribution de l'énergie électrique.

Nota : ces définitions sont cohérentes avec le Vocabulaire Electrotechnique International-VEI 191- et sont d'usage courant. Une norme en préparation (WG 7 du TC 95) relative à la fiabilité des équipements de protection, donne des définitions voisines mais inclut la notion de "sûreté de fonctionnement" dans la fiabilité. Mais la **sûreté** reste le vocable globalisateur.

Les différents états possibles de la protection sont schématisés par la figure 4 avec leurs conséquences pour la distribution électrique.

Le ratio entre le temps passé dans l'état de marche et le temps total de référence est la disponibilité. Le lecteur s'intéressant à la quantification des grandeurs de la sûreté voudra bien se reporter à l'annexe ainsi qu'au Cahier Technique n° 144.

Si l'on revient à la figure 3, l'un des objectifs du concepteur d'équipements de protection est de traiter de manière préventive le maximum de défaillances (maintenabilité) pour augmenter la disponibilité. Un minimum d'événements doivent conduire à la détérioration de la sécurité de la protection (le concept et les moyens d'auto-surveillance seront évoqués dans les chapitres suivants).

S'agissant de protection des réseaux MT et HT, leur sûreté doit être d'un niveau très élevé comparativement à celle de la plupart des équipements BT.

Une Analyse Préliminaire de Risques permet de déterminer les événements redoutés liés aux fonctions remplies par l'équipement de protection (cf. tableau fig. 5).

Une équipe de spécialistes indépendante de l'équipe de conception réalise les études prévisionnelles de sûreté et propose des solutions techniques compatibles avec le niveau spécifié. Une démarche itérative permet de modifier la conception jusqu'à ce que les objectifs soient atteints.

les outils du fiabiliste

Des techniques spécialisées d'évaluation et de modélisation de la sûreté de fonctionnement permettent de décliner les objectifs en contraintes de conception.

■ l'analyse prévisionnelle de la fiabilité détermine le taux de défaillance de chaque composant de l'équipement dans les conditions réelles d'utilisation.

Pour cela, des **bases de données de fiabilité** telles que le Military Handbook 217 (MIL-HDBK-217) (cf. tableaux fig. 6), ou le recueil du CNET (RDF 93) sont utilisées. Elles permettent le calcul de la fiabilité d'un circuit comportant plusieurs composants. Si nécessaire, le concepteur modifie le taux de charge de certains d'entre eux, ou utilise des composants à haute durée de vie garantie (c'est le cas pour les condensateurs chimiques par exemple).

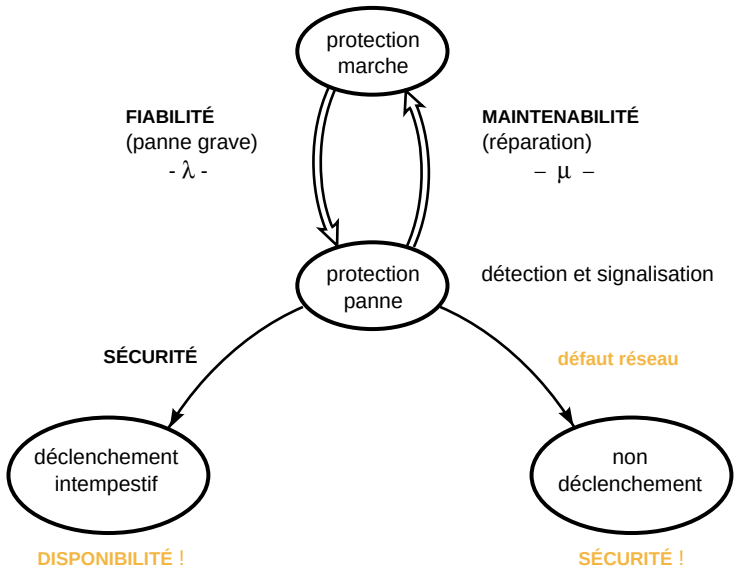

fig. 4 : graphe d'états de la protection et conséquences sur la distribution électrique (en orange).

événement redouté	effets	causes	prévention
déclenchement intempestif	■ ouverture intempestive du disjoncteur ■ indisponibilité d'énergie qui entraîne des pertes financières importantes (arrêt de production...)	■ internes, par exemple : □ détection intempestive d'un défaut, □ actionnement intempestif de la commande... ■ externes, par exemple : □ perturbations électromagnétiques □ saturation des capteurs □ erreur dans la conception du plan de protection...	par exemple : ■ fonctions d'auto-surveillance ■ position de repli ■ compatibilité électromagnétique ■ capteurs amagnétiques
masquage d'un ordre de déclenchement	■ déclenchement d'un niveau amont de protection avec possibilité de destruction locale de matériel ■ destruction importante de matériels (incendie...) s'il n'y a pas de protection amont	■ internes, par exemple : □ non détection d'un défaut □ commande bloquée... ■ externes, par exemple : □ perturbations électromagnétiques □ saturation des capteurs □ perte d'alimentation auxiliaire □ circuit de déclenchement du disjoncteur ouvert □ erreur dans la conception du plan de protection...	par exemple : ■ fonctions d'auto-surveillance ■ compatibilité électromagnétique ■ capteurs amagnétiques ■ module de secours ■ surveillance du circuit de déclenchement ■ sélectivité logique

fig. 5 : événements redoutés relatifs à la fonction protection.

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

$\lambda_p = (C_1 \cdot \pi_T + C_2 \cdot \pi_E)\ \pi_Q \cdot \pi_L$ 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 ⩽ 64 K	.0017
1,001 to 3,000	.040	301 to 1,000	.040	64 K < C ⩽ 256 K	.0034
3,001 to 10,000	.080	1,001 to 10,000	.060	256 K < C ⩽ 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 : exemple de données de fiabilité selon le Military Handbook.

■ l'Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (**AMDEC**), réalisée aussi bien sur le matériel que sur le logiciel, évalue les effets de chaque mode de défaillance connu sur le fonctionnement de l'équipement.

L'AMDEC permet de corriger certains risques de dysfonctionnements et de spécifier les fonctions d'auto-surveillance. Elle peut être faite au niveau d'une fonction générale (la fonction «protection»), d'une fonction élémentaire (la fonction «protection à maximum d'intensité») l'une de ses sous fonctions (cf. tableau fig. 7) jusqu'au niveau le plus bas des composants de base (implantés sur les cartes électroniques).

■ les événements redoutés relatifs à l'équipement de protection sont modélisés par plusieurs techniques :
□ les **arbres de défaillance** décrivent à partir d'un événement redouté toutes les causes possibles de cet événement (cf. tableau fig. 8).
L'arbre de défaillance est une représentation booléenne qui permet de déterminer les chemins les plus critiques pour la réalisation de l'événement.
□ les **graphes de Markov** sont une représentation comportementale où apparaissent les états de marche, marche dégradée et panne de l'équipement. Les transitions entre états sont quantifiées par les taux de défaillance (λ) et de réparation (μ). Ces graphes permettent de calculer les probabilités d'occupation des états de panne (cf. tableau fig. 9).
□ les **réseaux de Petri** ont le même but que les graphes de Markov, c'est-à-dire modéliser les états d'un système. Ils permettent de traiter des systèmes plus complexes dont les transitions entre états n'obéissent pas nécessairement à la loi exponentielle (loi de Weibull par exemple) (cf. tableau fig. 10).
Ces modélisations permettent d'effectuer une simulation quantifiée de la sûreté de fonctionnement et ainsi d'obtenir les probabilités correspondant à la fiabilité, maintenabilité, disponibilité et sécurité de l'équipement de protection.

Le lecteur pourra trouver une description plus précise de ces diverses techniques dans les références [Villemeur] ou [Pages-Gondran].

les moyens de la sûreté

Pour garantir au mieux la sûreté d'une installation électrique, la fiabilité, la sécurité et la maintenabilité des protections doivent être maîtrisées.

Les objectifs liés à ces grandeurs étant fixés, le concepteur de la protection, aidé par le fiabiliste, utilise un certain nombre de moyens pour réussir :
■ grâce au fiabiliste et à ses outils, il maîtrise la fiabilité intrinsèque avant et pendant le développement ;
■ grâce aux moyens d'auto-surveillance, de signalisation des défaillances, et de communication, il peut :
□ améliorer la sûreté avec la mise en position de repli,
□ améliorer la maintenabilité et la disponibilité de la protection.

Examinons les moyens mis en œuvre :
■ l'auto-surveillance
L'efficacité et la pertinence de l'auto-surveillance sont essentielles à la sûreté de la protection. A titre d'exemples, quelques moyens permettent d'accroître la disponibilité et la sécurité :
□ un contrôle d'intégrité des informations contenues dans les boîtiers mémoires «programme» et mémoires «données constantes» doit être effectué à la mise sous tension et cycliquement pendant le fonctionnement. Le contrôle se fait par calcul du Checksum avec retenue sur les zones mémoires utilisées. Le Checksum avec retenue couvre 99,95 % pour 128 octets (99,998 % pour 128 Koctets) des collages de bits d'adresse et de bits mémoire. Pour un volume d'informations à contrôler supérieur à quelques centaines d'octets, le calcul du Checksum avec retenue est plus efficace que le calcul d'un CRC 16 par exemple (cf. référence [INRS]).
□ on doit disposer d'un chien de garde matériel et logiciel afin de détecter tout blocage de l'unité centrale (dû à un défaut composant, un parasite ou à une surcharge du microprocesseur). Il faut aussi s'assurer de la validité du signal de sortie du chien de garde. Le chien de garde doit couvrir les défaillances du quartz ou de l'oscillateur du microprocesseur (cf. fig. 11).
□ le temps de cycle du programme doit être maîtrisé. Si des interruptions sont utilisées pour séquencer les cycles, il faut s'assurer du bon fonctionnement de ces mécanismes.
□ un contrôle de la tension d'alimentation doit être effectué en permanence pour prévenir d'une chute éventuelle de la tension et arrêter «proprement» le microprocesseur (sauvegarde des paramètres).

fonction	mode de défaillance	effet sur la protection	moyens de détection	signalisation
acquérir les courants phase	courant mesuré erroné : niveau continu > seuil de déclenchement	protection activée → déclenchement intempestif	l'algorythme utilisé fonctionne sur le calcul du module du courant à 50 Hz	inhibition « naturelle » de la protection
			détection par le calcul périodique de la composante continue du signal	signaler la défaillance en face avant et par la communication
	courant mesuré erroné : niveau continu < seuil de déclenchement	protection indisponible → non déclenchement sur défaut éventuel	les moyens de détection sont les mêmes	signaler

fig. 7 : tableau d'AMDEC réalisé sur une sous-fonction de la protection à maximum d'intensité.

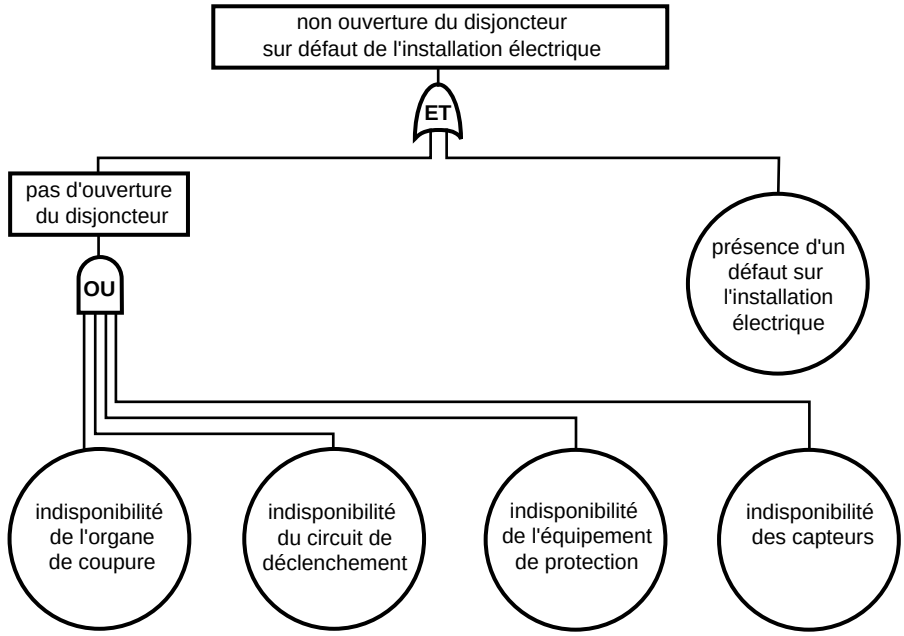

fig. 8 : exemple simple d'arbre de défaillance.

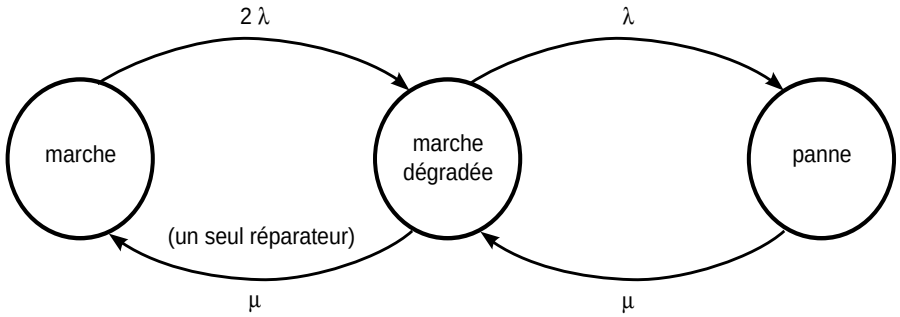

fig. 9 : exemple d'un graphe de Markov pour un système constitué de deux composants redondants et réparables, s'il s'agit de deux composants électroniques (fiabilité exponentielle), a durée moyenne de bon fonctionnement après réparation est $MUT = \frac{1}{2\lambda \cdot \lambda}$

Le réseau de Petri représenté possède deux place (P1, P2), deux transitions (T1, T2) et quatre arcs.
Ce réseau représente le comportement d'un composant réparable en affectant par exemple les significations suivantes aux places et aux transitions :

P1 : le composant est en bon état de marche
P2 : le composant est en panne
T1 : le composant tombe en panne
T2 : le composant finit d'être réparé.

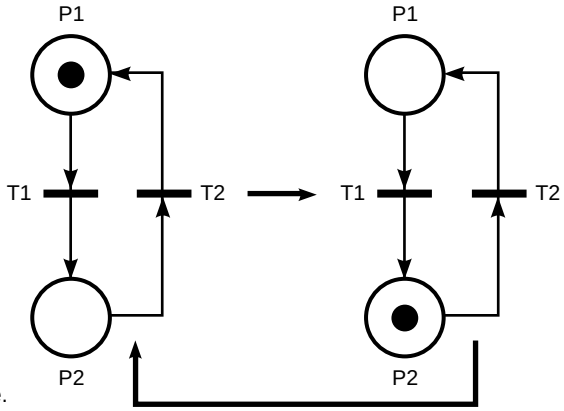

fig. 10 : exemple d'un réseau de Petri pour un système constitué d'un élément réparable.

□ si l'on utilise des mémoires EEPROM, il faut surveiller l'utilisation de ce composant en comptabilisant le nombre d'écritures qui ne doit pas excéder 10 000.
□ il faut éviter de traiter des données numériques erronées à la suite d'une défaillance de la chaîne de conversion analogique digitale. Pour cela un contrôle efficace consiste à vérifier en permanence deux signaux de référence à l'entrée du multiplexeur à deux adresses complémentaires (on détecte ainsi 100 % des pannes du Convertisseur Analogique Numérique et 100 % des collages à 1 ou 0 des bits de sélection du Multiplexeur).

Pour le contrôle de l'intégrité des données

Plusieurs techniques sont utilisables :

■ le contrôle de parité
Il consiste à rendre systématiquement pair le nombre de bits transmis en complétant le message utile par un «bit de parité».
Le récepteur peut ainsi contrôler le message s'il y a une erreur sur un bit ou 3 bits…
L'altération d'un nombre pair de bits n'est pas détectable.

■ le CRC (Cyclic Redundancy Check) consiste à rajouter à l'information utile le reste de sa division par un polynôme normalisé par le CCIT.
Par exemple, le polynome diviseur de degré 16
($X^{16} + X^{15} + X^2 + 1$ = 1100 0000 0000 0011) utilisé pour le «CRC 16» permet la détection de 16 erreurs simultanées.

■ le Checksum constiste à faire la somme binaire des octets et à adjoindre le résultat (tronqué sur un ou plusieurs octets) au message utile.
Le Checksum peut être couplé par exemple au contrôle de parité sur les octets…
Le contrôle de l'intégrité du message par le récepteur est plus facile que pour le CRC et peut être plus efficace.

Pour contrôler la bonne exécution d'un programme

Souvent utilisé en automatisme, la technique du **chien de garde** consiste à exécuter périodiquement une instruction test.

La non exécution de cette instruction, dans un délai fixé, révèle une défaillance et provoque le déclenchement d'une alarme ainsi que la mise en sécurité de l'équipement.

fig. 11 : les moyens d'auto contrôle en numérique.

Beaucoup d'autres mécanismes de détection sont utilisés. Ils sont évidemment très dépendants de la technologie utilisée.

■ la position de repli sûre
Les fonctions d'auto-surveillance détectent le maximum de défaillances «majeures». Une défaillance est classée dans la catégorie «majeure» si elle est susceptible d'entraîner un mauvais fonctionnement de la protection.

Une telle défaillance ne doit pas dégénérer en déclenchement intempestif. La protection se met dans une position de repli sûre et prédéterminée afin d'éviter le passage d'ordres aléatoires.

L'exploitant est informé de cette "position de repli", et peut procéder à l'opération de maintenance immédiatement pour redonner à la protection sa disponibilité.
Parallèlement une défaillance dite «mineure», comme par exemple une défaillance de périphériques (affichage ou console de réglage), est signalée mais n'affecte pas la disponibilité de la protection.

■ la signalisation des défaillances
Les fonctions d'auto-surveillance doivent fournir des moyens de diagnostic adaptés afin de permettre un retour rapide à l'état de marche de la protection défaillante, c'est-à-dire :
□ fournir à l'exploitant une information externe claire et globale sur l'état de sa protection,
□ fournir au constructeur, lors d'une opération de maintenance, voire après retour usine de la protection défectueuse, une information interne claire et précise sur l'état de la protection.

Par exemple, la défaillance de la protection peut être signalée par :
□ un voyant en face avant,
□ une sortie relais Chien De Garde,
□ un message sur l'afficheur en face avant,
□ une information sauvegardée en interne détaillant l'origine de la défaillance,
□ un message via la communication lorsque la protection est intégrée dans un système de contrôle-commande.

Ceci est un avantage sensible par rapport aux protections de technologie plus ancienne qui pouvaient rester en panne longtemps sans que l'exploitant en soit conscient (cf. fig. 12) et qui, a fortiori, ne donnaient aucune information sur l'origine de la panne...

■ l'ouverture vers les systèmes de supervision et de contrôle-commande
Comme évoqué précédemment, la protection numérique peut intégrer des fonctions d'automatisme et de communication. Elle devient ainsi un des maillons du système de supervision et de contrôle-commande de l'installation électrique, lequel facilite l'exploitation en permettant la surveillance, la conduite et la gestion du réseau de distribution :
□ surveillance des états et des grandeurs électriques (mesures),
□ surveillance des équipements (position de l'appareillage, température, pression…),
□ traitement des alarmes,
□ commande à distance des organes de manœuvre,
□ reconfiguration automatique des réseaux après défaut,
□ gestion de l'énergie consommée fonction de la tarification du distributeur,
□ édition de bilans d'exploitation,
□ allocation des dépenses d'énergie aux différents consommateurs du site.

■ la facilité de maintenance
□ auto-surveillance, signalisation, communication facilitent la connaissance de l'état de panne, d'où action immédiate de maintenance,
□ l'auto-diagnostic permet au dépanneur de connaître l'origine de la panne, d'où rapidité du dépannage,

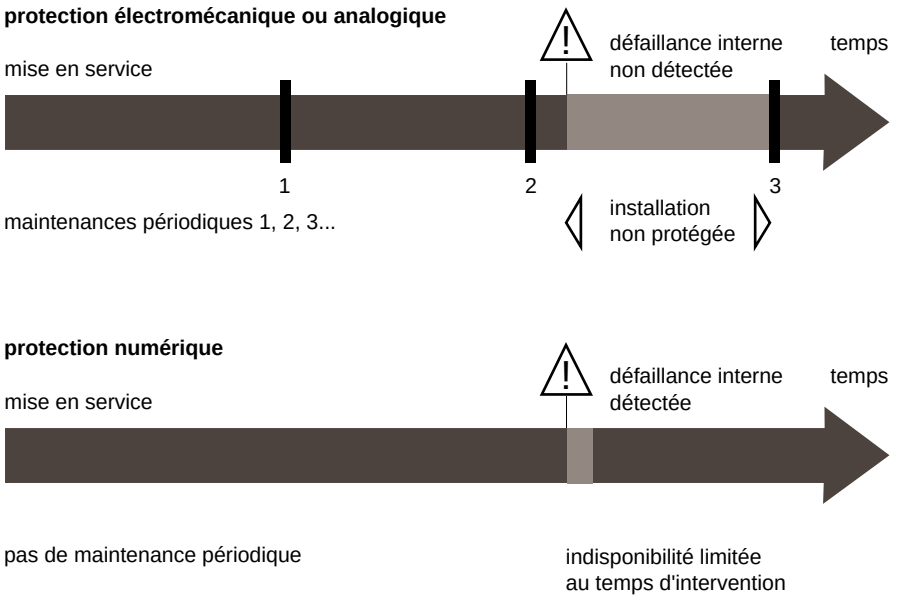

fig. 12 : l'auto-surveillance permet de réduire le temps d'indisponibilité de la protection donc augmente la sûreté de l'installation électrique.

□ les fonctions programmées, qui personnalisent la protection en terme d'application/de fonctions réalisées, sont stockées dans une cartouche amovible. Ceci permet une remise en service immédiate après remplacement de la partie physique (hard) qui est standardisée.

■ cas particuliers

La fiabilité de la protection peut ne pas être suffisante si elle subit des agressions exceptionnelles ou si le besoin de disponibilité et de sécurité de la distribution électrique est exceptionnellement élevé :

□ environnement sévère

Les systèmes de protection sont parfois installés dans des environnements exceptionnels qui dépassent les contraintes spécifiées des matériels :
- température,
- vibration…

Dans chaque cas, les besoins doivent être spécialement identifiés par le bureau d'étude. Une solution personnalisée est alors proposée :
- vernis spécial sur les cartes électroniques,
- contrat de maintenance spécifique.

□ le besoin de sûreté exceptionnel

Un module de secours peut assurer la protection en cas de :
- défaut d'alimentation,
- défaut de la filerie,
- défaut du déclencheur,
- protection principale hors service.

Autre solution, doubler l'équipement de protection avec circuit «ou» dans le circuit de commande de l'organe de coupure. Pour l'installation, la sécurité est fortement augmentée, et la disponibilité de l'énergie n'est pas diminuée, lorsque l'on utilise des systèmes de protection avec position de repli sûre.

A l'extrême des systèmes de vote 2/3 peuvent être envisagés.

3. la sûreté s'intègre dans une démarche de qualité globale

qualité des logiciels

Une part importante des fonctionnalités des équipements de protection numériques est réalisée par le logiciel. Il est donc impératif de maîtriser la qualité du logiciel pour atteindre les objectifs globaux de sûreté.

La maîtrise de la qualité du logiciel est obtenue par la mise en œuvre d'une méthode de développement rigoureuse.

Cette méthode, issue des recommandations établies par les organismes français (AFCIQ) et internationaux (IEEE) impose :

■ le découpage du développement en une succession de phases (cf. fig. 13) :
□ spécification,
□ conception préliminaire,
□ conception détaillée,
□ codage,
□ test unitaires,
□ intégration et tests d'intégration,
□ validation.

A chacune des phases est associé un ensemble de documents utilisés et produits pendant la phase.

Ces documents formalisent les études réalisées dans chaque phase et doivent être validés avant de passer à la phase suivante.

■ l'utilisation de règles et méthodes de conception et codage qui ont pour but d'obtenir un haut niveau de structuration du logiciel (par exemple SADT implémenté dans l'outil ASA ou MACH).

■ l'utilisation d'outils de gestion de configuration logiciel qui permettent de gérer tous les constituants d'un logiciel et notamment de maîtriser les évolutions et les versions respectives de tous ces constituants (exemple outil CMS).

Par ailleurs, les méthodes de revues de code sont utilisées avec grand profit. Un vérificateur effectue une lecture critique du code et indique ses observations. Cette analyse «manuelle» reste à ce jour une des méthodes les plus efficaces pour découvrir les erreurs logicielles (les bogues).
Enfin, chaque logiciel étant intégré et validé, une dernière phase de qualification menée par une équipe indépendante de l'équipe de développement permet un contrôle final efficace.

qualification des protections

Les équipements de protection, avant leur mise sur le marché, subissent une qualification complète.

Quelques critères de qualification spécifiques à l'environnement Moyenne et Haute Tension sont détaillés ici.

■ l'immunité aux perturbations électromagnétiques (conduites et rayonnées)
Les perturbations électriques rencontrées dans les postes électriques ont plusieurs origines :
□ les coups de foudre qui interviennent directement sur les lignes ou à proximité du poste peuvent générer des surtensions d'une centaine de kV et de front de montée de l'ordre de la microseconde ;
□ la manœuvre normale de l'appareillage, à l'ouverture et à la fermeture de l'organe de coupure MT ou HT provoque des surtensions de «manœuvre» (onde oscillatoire amortie). Ces surtensions peuvent produire des champs électriques impulsionnels de l'ordre de 10 kV/m à 1 mètre du disjoncteur ;
□ l'opérateur humain peut provoquer des décharges électrostatiques qui se traduisent sur le matériel par des impulsions de courant de quelques dizaines d'ampères et de front très raide de l'ordre de la nanoseconde ;
□ les émetteurs radioélectriques (talkies-walkies par exemple) génèrent des champs de plusieurs dizaines de V/m à 1mètre.

Le lecteur désirant approfondir le sujet Compatibilité Electromagnétique -CEM- peut se procurer le Cahier Technique n° 149.

Des standards internes de tenues aux contraintes électriques définissent les niveaux d'immunité nécessaires au fonctionnement des systèmes de protection dans un poste électrique.

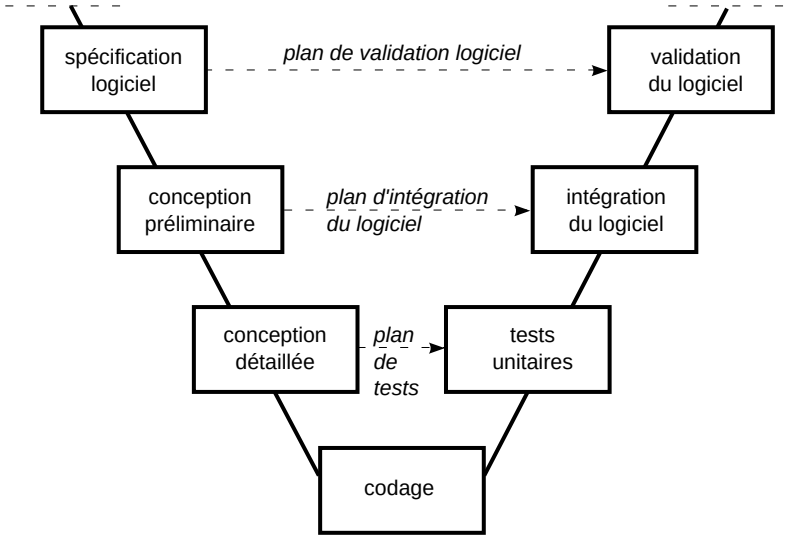

fig. 13 : le cycle de développement logiciel (dit en V).

Ces niveaux correspondent aux tenues définies par les normes CEI 255 voire parfois plus sévères. Le respect du niveau de sévérité défini est contrôlé par des essais. 4 types d'essais sont réalisés :
□ onde oscillatoire amortie
(CEI 255-22-1)
sévérité : classe III, 2,5 kV,
□ transitoires rapides (CEI-255-22-4)
sévérité : classe IV, 4 kV,
□ décharges électrostatiques
(CEI 255-22-2)
sévérité : classe III, 8 kV,
□ champs rayonnés (CEI-255-22-3)
sévérité : supérieur classe III, 30 V/m
(cf. fig. 14).

Note : l'essai aux transitoires rapides est la transcription en mode "conduit" des champs électromagnétiques impulsionnels "rayonnés", générés lors des manœuvres de l'appareillage.

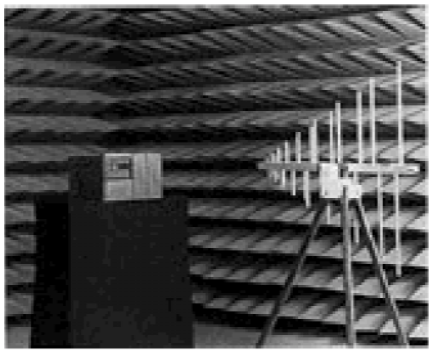

fig. 14 : essais aux perturbations électromagnétiques en chambre anéchoïque.

fig. 15 : laboratoire Kirchhoff d'essais des protections.

Au-delà des essaIs de CEM, les équipements de protection sont soumis à des essais "en situation".
A titre d'exemple, l'équipement étant placé dans le compartiment
Basse Tension d'une cellule Moyenne Tension, une centaine de manœuvres fermeture-ouverture du disjoncteur. La charge faible, et de nature selfique, provoque des surtensions importantes par arrachement de courant.

Durant ces essais, l'équipement de protection ne doit pas connaître de fonctionnement intempestif.

■ le laboratoire Kirchhoff : essai des protections

Les fonctions réalisées par les systèmes de protection sont complexes. Le bon fonctionnement des protections doit être garanti pour l'ensemble des phénomènes susceptibles de se produire sur les réseaux électriques. Un laboratoire performant d'essais des protections, est nécessaire (cf. fig. 15).
Le laboratoire Kirchhoff permet de reproduire en grandeur réelle les phénomènes tels qu'ils apparaissent sur les réseaux électriques (cf. fig. 16).
Il est équipé d'un simulateur numérique qui permet de :
□ calculer les courants et les tensions sur le réseau, au moment où se produit

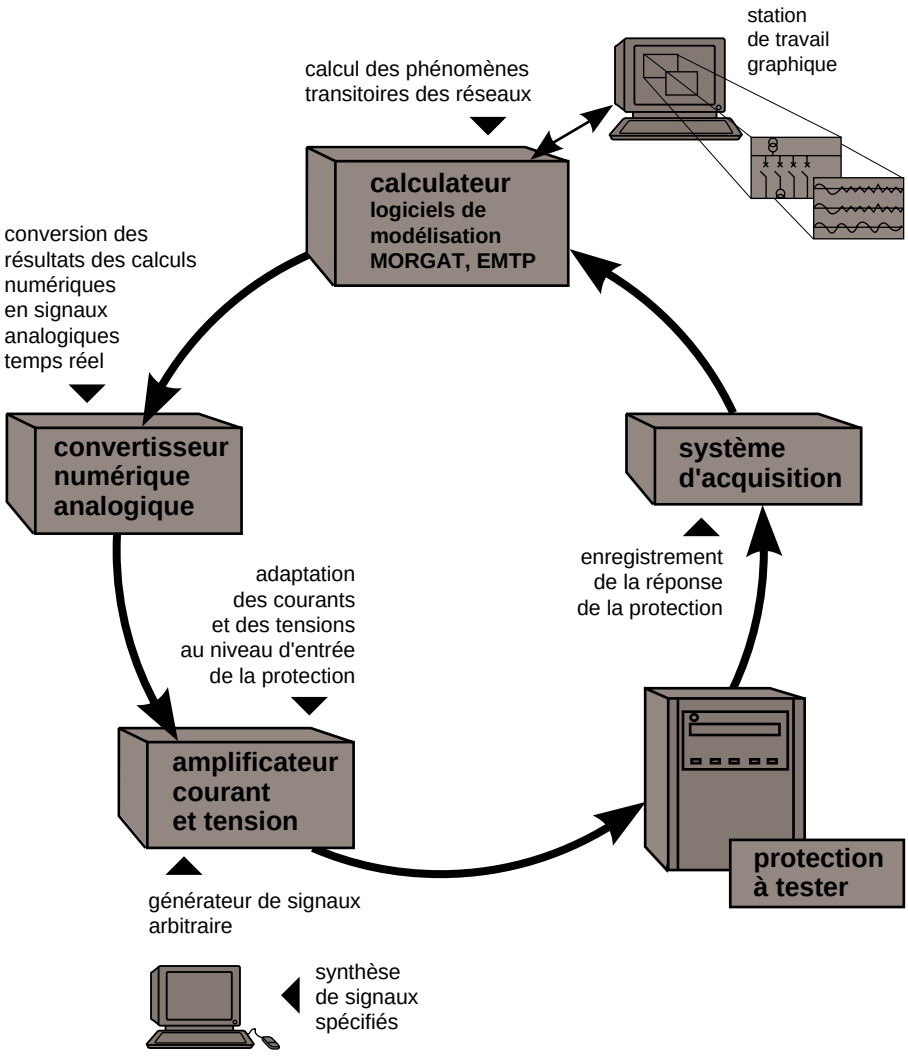

fig. 16 : description du système d'essais des protections.

un court-circuit, une rupture d'isolement ou une manœuvre d'appareil,
□ générer les signaux correspondants et les appliquer à la protection à tester. On analyse alors le comportement des protections soumises à des conditions identiques à celles qu'elles rencontreront sur le réseau réel.

La simulation numérique des réseaux électriques du laboratoire Kirchhoff fait appel à deux logiciels :
□ EMTP (ElectroMagnetic Transient Program), programme de calcul des phénomènes transitoires. Ce logiciel, mondialement utilisé, permet à partir d'une bibliothèque de matériels (transformateurs, lignes, machines...) de modéliser toutes sortes de réseaux électriques, de simuler un défaut ou une manœuvre d'appareil et de calculer précisément l'évolution des courants et tensions ;
□ MORGAT, simulateur de réseaux électriques, développé et distribué par EDF. Ce logiciel permet à la fois l'analyse fine du comportement du réseau et le pilotage de l'aspect «temps réel» du laboratoire Kirchhoff. Les courants et les tensions, calculés en différents points du réseau électrique simulé, sont convertis en signaux analogiques pour être appliqués à la protection à tester.

contrôle qualité

En cours de production, ainsi qu'en fin de production, les équipements de protection subissent de nombreux tests de contrôle.
Par exemple, les cartes électroniques subissent un premier contrôle sur le banc de test diélectrique qui effectue les essais d'isolement.
Elles sont ensuite dirigées vers le testeur in-situ (cf. fig. 17).

Le test in-situ vérifie le bon fonctionnement de chaque composant de la carte électronique ainsi que leur bonne implantation. Il indique principalement les défauts de fabrication et certains défauts de composants. Il donne un diagnostic implicite et permet une réparation rapide de la carte. Les résultats sont ensuite exploités par le service qualité et permettent de détecter rapidement une dérive dans la qualité des composants ou de la fabrication des cartes.

Après être passées par le test in-situ, les cartes sont déverminées sous contraintes thermiques et électriques combinées. Le déverminage élimine les défauts de jeunesse du matériel électronique. Il permet de réduire la durée de la période dite de jeunesse de façon à faire apparaître ces défauts en fabrication plutôt qu'en exploitation.
De la même façon, les statistiques de défauts sont exploitées par le service qualité afin de réagir rapidement à une dérive de qualité de fabrication.

Des tests finals permettent de s'assurer que les cartes assemblées dialoguent correctement entre elles et que la configuration réalisée correspond bien à la commande du client. Pour cela l'ensemble des fonctionnalités attendues sont activées par des stimuli appliqués aux interfaces de l'équipement réalisé.

Outre les contrôles systématiques réalisés sur la production, des tests de qualification sont refaits périodiquement sur un échantillon représentatif de la gamme.

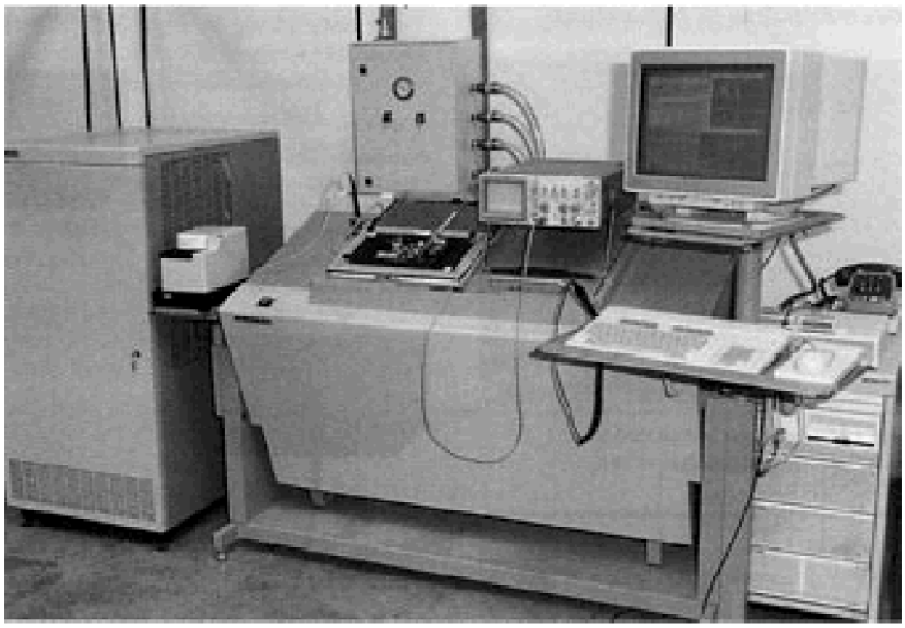

fig. 17 : testeur in-situ.

4. analyse du retour d’expérience

Pour avoir un retour d’expérience significatif, il est nécessaire, lorsque la fiablité est très bonne, d’avoir un parc très important d’équipements mis en service. Il est alors possible d’analyser les données de défaillance en exploitation. Cette analyse du retour d’expériences est fondamentale pour :
- mesurer la fiabilité opérationnelle des équipements ;
- valider les études de sûreté réalisées pendant la conception ;
- cumuler l’expérience technique pour progresser ;
- disposer d’une base de dialogue entre le constructeur et l’exploitant.

Le retour d’expérience repose sur une collecte fiable et ordonnée des informations relatives aux incidents en clientèle. La fiabilité opérationnelle (calculée sur le retour d’expérience) n’est pertinente que si la défaillance est détectable, détectée et enregistrée. Les données de défaillance, issues d’un parc d’équipements qui n’ont pas de fonctions d’auto-surveillance ou dont la maintenance périodique est peu fréquente, peuvent ne pas être représentatives de la fiabilité réelle.

Les données de fiabilité opérationnelle sur un parc de protections numériques sont pertinentes du fait de l’auto-surveillance.

Il a été constaté que la fiabilité opérationnelle était au moins supérieure d’un facteur 10 à la fiabilité prévisionnelle (calculée à partir du recueil de données MIL-HDBK-217E). Cet écart provenait vraisemblablement des recueils de données de fiabilité volontairement pessimistes et parfois anachroniques (les technologies et la qualité des composants électroniques évoluant très rapidement).

Les dernières mises à jour des recueils de données de fiabilité ont considérablement réduit l’écart entre les résultats de fiabilité opérationnelle et prévisionnelle.

Aujourd’hui, le MTBF correspondant au déclenchement intempestif ou au non fonctionnement de la protection atteint plusieurs centaines d’années.

5. conclusion

Les équipements de protection des réseaux Moyenne et Haute Tension assurent une fonction de sûreté primordiale. Ils doivent garantir la protection des matériels et des personnes tout en assurant la disponibilité de l’énergie. Leurs dysfonctionnements peuvent infliger aux exploitants des pertes financières élevées. Il est donc essentiel qu’ils répondent à de hautes exigences de fiabilité, sécurité, disponibillité et maintenabilité.

Pour cela les équipements de protection doivent remplir certaines caractéristiques techniques et industrielles dont les plus significatives sont :
- bien protéger les réseaux et les équipements MT et HT, grâce à des algorithmes adaptés aux diverses fonctions de protection ;
- être simples à mettre en œuvre, à exploiter et à maintenir ;
- être fiables dans un environnement sévère, mais en plus :
  - être capables de s’auto-surveiller,
  - posséder une position de repli sûre.

Grâce au travail des fiabilistes et des qualiticiens, en cours de conception, les équipements de protection numérique, actuellement sur le marché, répondent à ces exigences.

Aujourd’hui, tirant parti du développement des communications numériques (bus) et de la supervision, la fonctionnalité des équipements de protection s’étend dans le domaine du contrôle-commande pour une gestion optimisée de la distribution électrique.

6. annexe

Les temps moyens qui caractérisent la sûreté (cf. fig. 18) :
Le MTTF (Mean Time To first Failure) est le temps moyen de bon fonctionnement avant défaillance.
Le MTTR (Mean Time To Repair) est le temps moyen de réparation.
Le MTBF (Mean Time Between Failure) est le temps moyen entre deux défaillances (pour un système réparable).
Le MDT (Mean Down Time) est la durée moyenne de défaillance comprenant la détection de la panne, la durée d'intervention, le temps de la réparation et le temps de remise en service.
Le MUT (Mean Up Time) est la durée moyenne de bon fonctionnement après réparation.
Le terme de MTBF est traduit à tort comme la moyenne des temps de bon fonctionnement. Cette définition est en fait celle du MTTF ! La confusion vient du fait que souvent le MTTR (de l'ordre de quelques heures) est négligeable devant le MTTF (de l'ordre de plusieurs milliers d'heures).

Les probabilités
La Fiabilité, R(t) (Reliability) est la probabilité que le système soit non défaillant sur une durée t.
La Maintenabilité (Maintenability) est la probabilité que le système soit réparé sur une durée t.
La Disponibilité (Availability) est la probabilité que le système fonctionne à un instant t.
La Sécurité (Safety) est la probabilité d'éviter un événement catastrophique.

En général, on travaille avec une grandeur qui est le taux de défaillance λ (t). C'est la probabilité de tomber en panne dans l'instant qui suit sachant que le système n'a pas eu de défaillance.

Pour un composant électronique, le taux de défaillance suit une évolution dans le temps appelée la courbe «en baignoire». Pendant la période dite «de vie utile», le composant ne vieillit pas et son taux de défaillance λ est constant dans le temps. On a alors les éventuelles relations fondamentales suivantes :
Fiabilité $R(t) = e^{-\lambda t}$ et $MTTF = 1 / \lambda$.

Exemple :
Si un équipement a un MTTF de 100 ans, son taux de défaillance $\lambda = 1 / MTTF$ est de 10^{-2} / an. La probabilité de panne chaque année est donc de 1 %.

Un MTTF (ou MTBF) de 100 ans ne signifie surtout pas que le système sera non défaillant pendant 100 ans ! Le MTTF n'est donc assimilable ni à une durée de garantie, ni à une durée de vie...

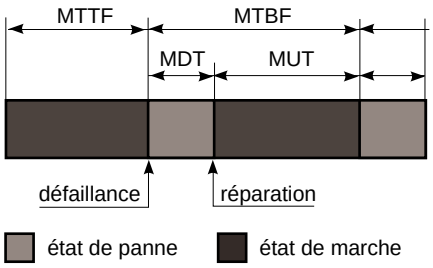

fig. 18 : diagramme des temps moyens, établi pour un système ne nécessitant pas d'interruption de fonctionnement pour maintenance préventive.

7. bibliographie

Publications diverses

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

■ Sûreté de fonctionnement des systèmes industriels
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

■ VEI 191

Cahiers techniques Merlin Gerin

■ Introduction à la conception de la sûreté,
Cahier Technique n° 144
P. BONNEFOI

■ La CEM : la compatibilité électromagnétique,
Cahier Technique n° 149
F. VAILLANT

■ Protections des réseaux HTA industriels et tertiaires,
Cahier Technique n° 174
A. SASTRÉ

Réal. : Illustration Technique - Lyon - Photo. : Merlin Gerin
DTE - 03-95 - 2500 - Imp. : Clerc