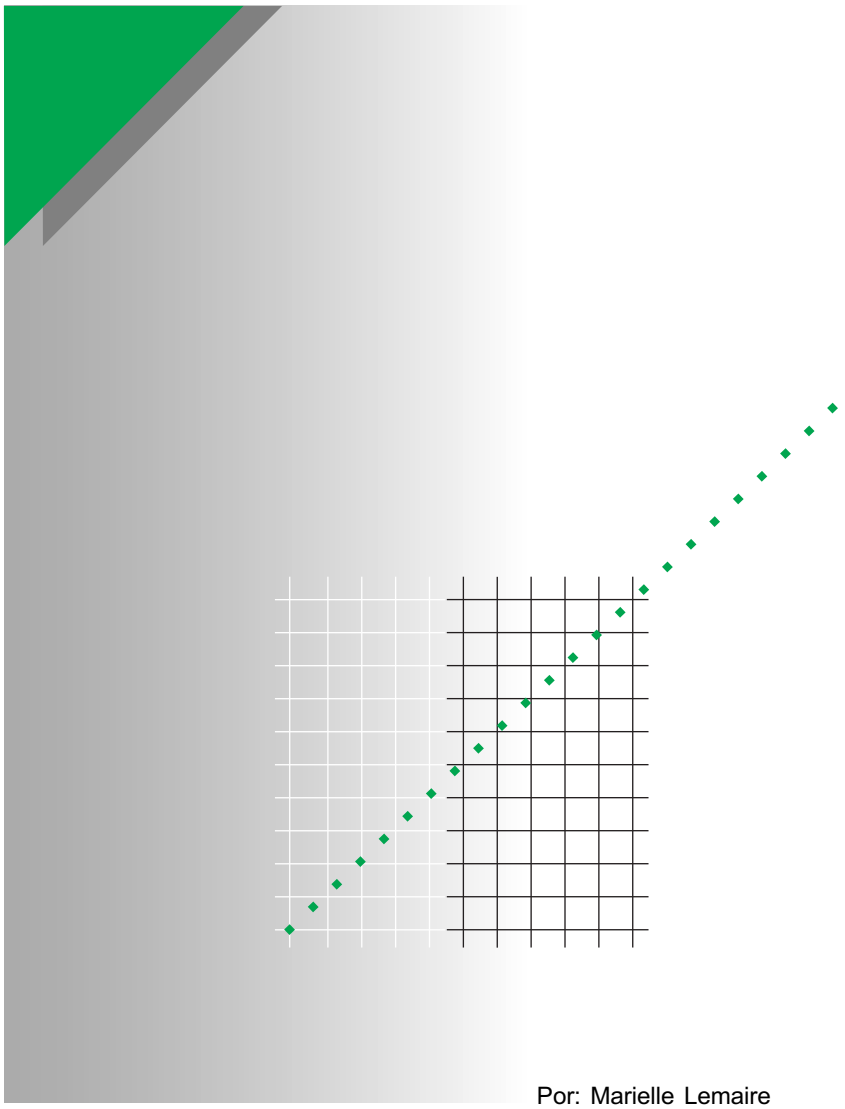
# Cuaderno Técnico nº 175

## Seguridad de las protecciones en MT y AT



Por: Marielle Lemaire

Merlin Gerin
Modicon
Square D
Telemecanique

Schneider Electric

La **Biblioteca Técnica** constituye una colección de títulos que recogen las novedades electrotécnicas y electrónicas. Están destinados a Ingenieros y Técnicos que precisen una información específica o más amplia, que complemente la de los catálogos, guías de producto o noticias técnicas

Estos documentos ayudan a conocer mejor los fenómenos que se presentan en las instalaciones, los sistemas y equipos eléctricos. Cada uno trata en profundidad un tema concreto del campo de las redes eléctricas, protecciones, control y mando y de los automatismos industriales.

Puede accederse a estas publicaciones en Internet:

http://www.schneiderelectric.es

Igualmente pueden solicitarse ejemplares en cualquier delegación comercial de **Schneider Electric España S.A.**, o bien dirigirse a:

Centro de Formación Schneider
C/ Miquel i Badia, 8 bajos
08024 Barcelona

Telf. (93) 285 35 80
Fax: (93) 219 64 40
e-mail: formacion@schneiderelectric.es

La colección de **Cuadernos Técnicos** forma parte de la «Biblioteca Técnica» del **Grupo Schneider**.

**Advertencia**

**Marielle LEMAIRE**

Obtuvo su diploma de Ingeniero IEG, especialidad Física, en 1986.

Después de dos años pasados en un laboratorio de la Universidad de TUCSON (Arizona) entra en Merlin Gerin donde participa en el desarrollo de convertidores estáticos de potencia.

Especialista en la seguridad de funcionamiento, colaboró como experta francesa en el grupo de trabajo WG7 del Comité Técnico «fiabilidad de las protecciones» de la CEI (TC 95). Participa cinco años después, en el desarrollo de sistemas de protección de las instalaciones de media y alta tensión.

# cuaderno técnico nº 175

## Seguridad de las protecciones en MT y AT

Por: Marielle Lemaire
Trad.: J. M. Giró

Edición francesa: marzo 1995
Versión española: febrero 2000

## **Terminología** (nota del traductor)

En este, como en otros Cuadernos Técnicos, la traducción de ciertos términos requiere perífrasis fácilmente aplicables.

Pero la traducción de la terminología técnica no sólo requiere una fidelidad a la idea sino también a las normas y debe de ser válida para los diversos idiomas, en este caso español, francés e inglés.

Por este motivo se adjunta en este punto un pequeño léxico de los términos principales de este cuaderno con su equivalente en francés (idioma del texto original) y en inglés (por su validez internacional).

- Disponibilidad - Disponibilité - Availability: es la probabilidad de que una protección esté en situación de cumplir su misión, en unas condiciones dadas y en un instante determinado.
- Fiabilidad - Fiabilité - Reliability: es la probabilidad de que una protección pueda cumplir con su misión en unas condiciones dadas y en un intervalo de tiempo dado; en concreto y sobre todo, la capacidad de disparar cuando haga falta y la capacidad de no-disparar intempestivamente.
- Mantenibilidad - Maintenibilité - Maintenibility: es la probabilidad de que una operación determinada de mantenimiento activo pueda efectuarse en un intervalo de tiempo dado.
- Seguridad - Sécurité - Satefy: es la probabilidad de que una protección no actúe intempestivamente, en unas condiciones dadas y en un intervalo de tiempo determinado. Tiene un sentido particular.
- Seguridad o garantía de buen funcionamiento - Sûreté - Dependability: tiene el sentido categórico, general o integral de la seguridad.

(Véase especialmente lo indicado en las páginas 8 y 18 de este mismo cuaderno).

# Seguridad de las protecciones en MT y AT

## Índice


| | | |
|---|---|---|
| **1 Introducción** | Objetivo de este cuaderno | p. 6 |
| | Aparamenta de protección | p. 6 |
| | Exigencias de la seguridad de funcionamiento: un compromiso entre dos situaciones extremas indeseables | p. 6 |
| **2 El diseño en función de la seguridad** | Terminología | p. 8 |
| | Las herramientas del especialista en fiabilidad | p. 10 |
| | Los recursos de la seguridad de funcionamiento | p. 10 |
| **3 La seguridad de funcionamiento** | Calidad del software | p. 14 |
| | Calificación de los equipos de protección | p. 14 |
| | Control de calidad | p. 16 |
| **4 Análisis de la información de retorno de la experiencia** | | p. 17 |
| **5 Conclusión** | | p. 17 |
| **6 Anexo** | | p. 18 |
| **7 Bibliografía** | | p. 18 |

# 1 Introducción

## Objetivo de este cuaderno

Este estudio presenta los diversos factores que contribuyen a conseguir un funcionamiento correcto de los equipos de protección de las redes de media y alta tensión, así como los métodos que se pueden utilizar para conseguir estos objetivos de seguridad.

Se desarrollan especialmente:

- el tener en cuenta la seguridad de funcionamiento durante el diseño;
- la búsqueda de la calidad (en el software, en la calificación, en la fabricación) con técnicas adecuadas a los esfuerzos que se presentan en MT y AT;
- el análisis de la información de retorno que da la experiencia.

Este documento se adecúa a las técnicas utilizadas en los años 90 durante el diseño de la nueva gama de protección Sepam.

## Aparamenta de protección

La aparamenta de protección tiene como misiones principales la detección de los defectos de la red, supervisando diversos parámetros (corriente, tensión...) y enviando una orden de apertura al interruptor automático en caso de situación anormal. La aparamenta suele proteger especialmente alguno de los diversos componentes de un centro de distribución eléctrica, como son: una entrada o una salida de líneas, un motor o un transformador.

En MT y AT, estos materiales suelen formar parte de la celda que contiene el interruptor automático (**figura 1**), siendo por tanto considerables los esfuerzos del entorno (temperatura, vibraciones, perturbaciones electromagnéticas).

Los equipos de protección están fabricados o bien con tecnología electromagnética (la más antigua), o bien con tecnología electrónica (también llamada estática), sea analógica o digital. Un equipo de protección digital (basado en el uso de un microprocesador) puede efectuar, además de su misión principal de protección, funciones de automatismo, de medida, de autovigilancia y de comunicación. Un equipo así se integra entonces naturalmente dentro de los sistemas de control y mando, asegurando funciones de automatización, indicación de estado e indicación sinóptica (**figura 2**).

## Exigencias de la seguridad de funcionamiento: un compromiso entre dos situaciones extremas indeseables

Los sistemas de protección asociados a los interruptores automáticos tienen la misión de **garantizar la seguridad de la instalación asegurando al mismo tiempo la mayor continuidad posible del suministro.**

En cuanto a la protección en sí misma, hay dos situaciones extremas posibles que, para que todo vaya bien, nunca deberían de producirse:

- primer extremo indeseable: **que no actúe la protección.**

Las consecuencias de no eliminar inmediatamente un defecto pueden ser catastróficas (riesgo para las personas, destrucción de los centros de transformación, pérdida de producción...). Para la seguridad de la explotación, el equipo de protección debe de detectar selectivamente y lo más rápidamente posible los defectos de la red eléctrica. Esta situación se puede evitar mejorando la disponibilidad de la protección.

- segundo extremo indeseable: **disparo intempestivo de la protección.**

La continuidad del suministro de energía es tan importante para el industrial como para las compañías suministradoras. Un disparo intempestivo debido a la propia protección puede generar pérdidas económicas considerables (parada de la producción, lucro cesante por la energía no distribuida...). Este fenómeno puede evitarse mejorando la **seguridad** de la protección.

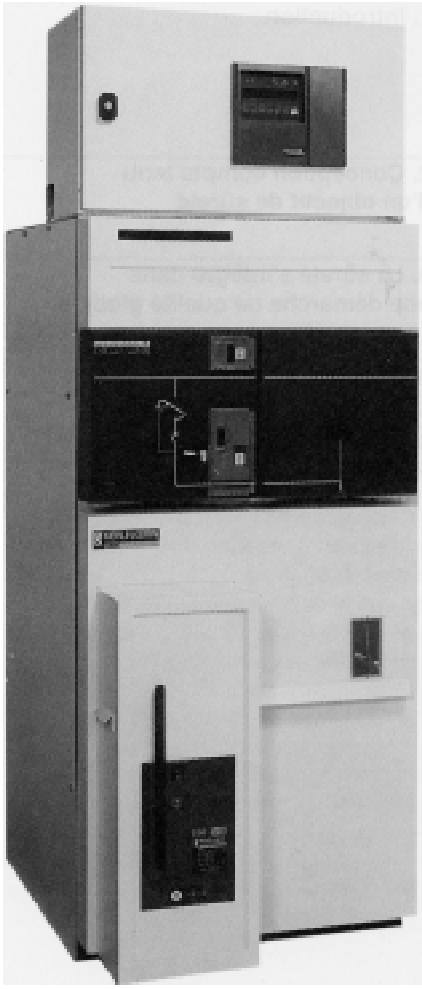


*Fig. 1: Equipo de protección incorporado a una celda de Media Tensión.*

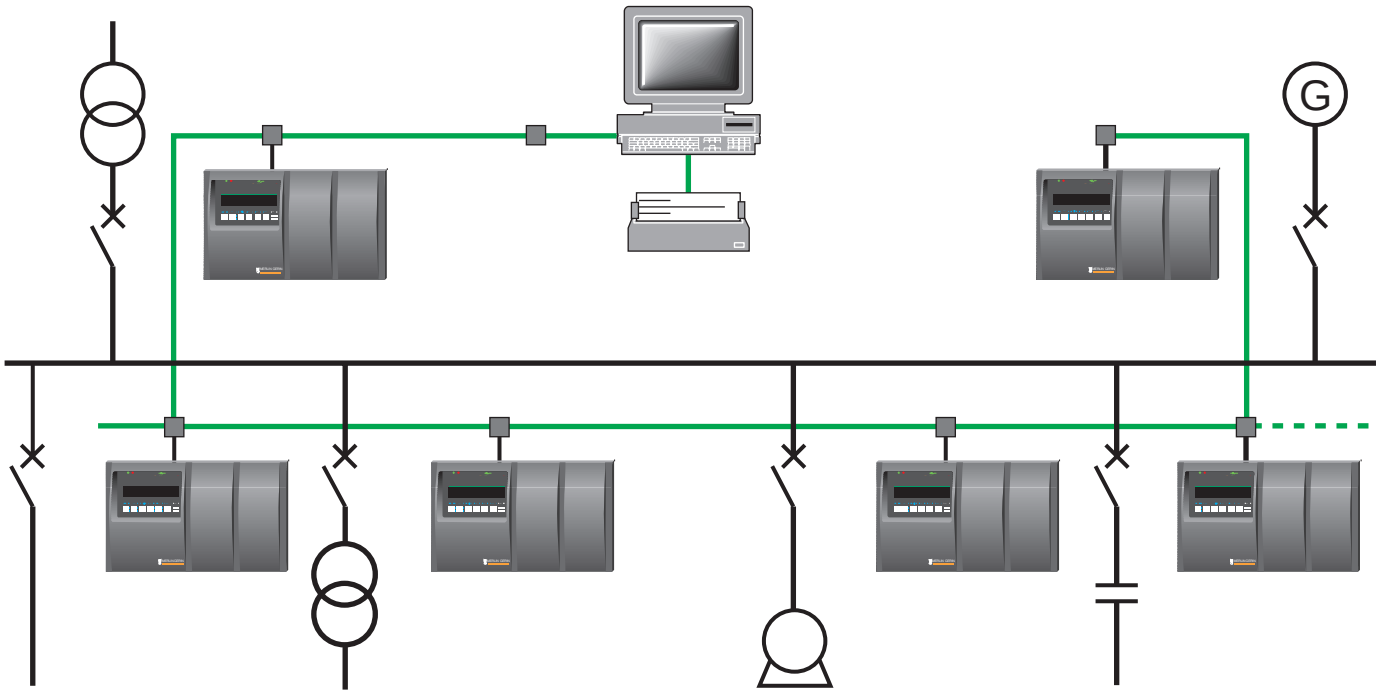



*Fig. 2: Ejemplo de sistema digital de control y mando de un centro de transformación.*

Frecuentemente, la disponibilidad y la seguridad están contrapuestas.

La mejor manera de que un avión no se estrelle es que se quede en tierra. Su seguridad es, entonces, perfecta, ¡pero su disponibilidad, nula! Por el contrario, un avión que vuela en exceso, sin mantenimiento, pone en peligro la vida de las personas. El diseño de cualquier equipo, sea el que sea, obliga a un compromiso entre la disponibilidad y la seguridad.

La disponibilidad y seguridad aumentan al jugar con otras dos componentes de seguridad de buen funcionamiento: la mantenibilidad y la fiabilidad (**figura 3**).

En lo que respecta a los equipos de protección, están sometidos a múltiples agresiones que pueden tender a provocar los citados «fenómenos indeseables», por ejemplo:

- ☐ temperaturas extremas,
- ☐ vibraciones debidas a las maniobras de los interruptores automáticos,
- ☐ atmósferas corrosivas en aplicaciones industriales (industrias químicas, del papel o del cemento...),
- ☐ picos de campos electromagnéticos intensos (hasta varias decenas de kV/m, con un tiempo de rampa de subida del orden de 5 ns, a 1 metro de la celda del interruptor automático.

Este entorno, tan extremadamente duro, y el hecho de que las redes de MT y AT alimenten a numerosos usuarios de la energía eléctrica hacen necesario un perfecto control de la fiabilidad y la mantenibilidad.

Los equipos de protección que utilizan los microprocesadores han permitido un avance considerable. Por ejemplo:

- ☐ con la integración disminuyen los problemas de cableado y aumenta la fiabilidad,
- ☐ con la autovigilancia aumenta la disponibilidad.

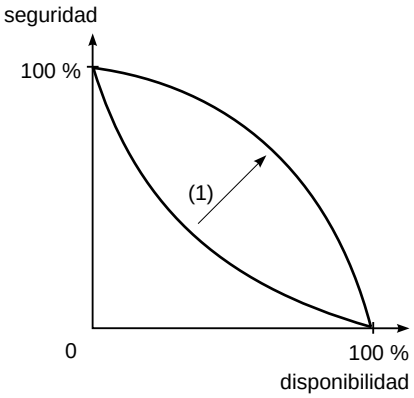



*Fig. 3: Al aumentar la fiabilidad y la mantenibilidad (1) aumenta la disponibilidad y la seguridad.*

# 2 El diseño en función de la seguridad de funcionamiento

## Terminología

Desde que se empieza el diseño de un equipo de protección hay que tener en cuenta los objetivos de Fiabilidad, Seguridad, Disponibilidad y Mantenibilidad.

Recordemos las definiciones de estas magnitudes:

- la disponibilidad es la probabilidad de que una protección esté en situación de cumplir su misión, en unas condiciones dadas y en un instante determinado;
- la seguridad es la probabilidad de que una protección no actúe intempestivamente, en unas condiciones dadas y en un intervalo de tiempo determinado;
- la fiabilidad es la probabilidad de que una protección pueda cumplir con su misión en unas condiciones dadas y en un intervalo de tiempo dado; en concreto y sobre todo, la capacidad de disparar cuando haga falta y la capacidad de no-disparar intempestivamente;
- la mantenibilidad es la probabilidad de que una operación determinada de mantenimiento activo se pueda efectuar en un intervalo de tiempo dado.

Estas magnitudes no tienen necesariamente el mismo significado según se piense en la protección o en la instalación eléctrica.

Así, la disponibilidad y la mantenibilidad de la protección contribuyen a la seguridad de las personas y de los materiales. La seguridad del dispositivo de protección favorece la disponibilidad de la distribución de la energía eléctrica.

Nota: estas definiciones son coherentes con el Vocabulario Electrotécnico Internacional -VEI 191- y se usan frecuentemente. Una norma en preparación (WG 7 del TC 95), relativa a la fiabilidad de los equipos de protección, da definiciones parecidas, incluyendo la noción de «seguridad de funcionamiento» en la fiabilidad. Aquí se usa esta expresión –**seguridad de funcionamiento**– como término que engloba a todos.

Los diversos estados posibles de una protección se esquematizan en la **figura 4** con sus consecuencias para la distribución eléctrica.

La razón entre el tiempo pasado en el estado de marcha y el tiempo total de referencia es la disponibilidad. El lector interesado en la cuantificación de los valores de la seguridad de buen funcionamiento puede leer tanto el anexo como el Cuaderno Técnico n° 144.

Si se observa la **figura 3**, uno de los objetivos del diseñador de equipos de protección es tratar de manera preventiva el máximo número posible de fallos (mantenibilidad) para aumentar la disponibilidad. Sólo un número mínimo de sucesos debe de llevar a la pérdida de seguridad de la protección (el concepto y los mecanismos de autovigilancia se verán en los próximos capítulos).

En cuanto a las protecciones de las redes de MT y AT, su seguridad debe de ser muy buena respecto a la mayoría de equipos de BT.

Un Análisis Preliminar de Riesgos permite determinar las situaciones indeseables relacionadas con las funciones que cumple el equipo de protección (**figura 5**).

Un equipo de especialistas, independiente del equipo de diseño, realiza los estudios previos de seguridad y propone soluciones técnicas compatibles con el nivel especificado. Un conjunto de aproximaciones sucesivas permite modificar el diseño hasta que se consiguen los objetivos buscados.

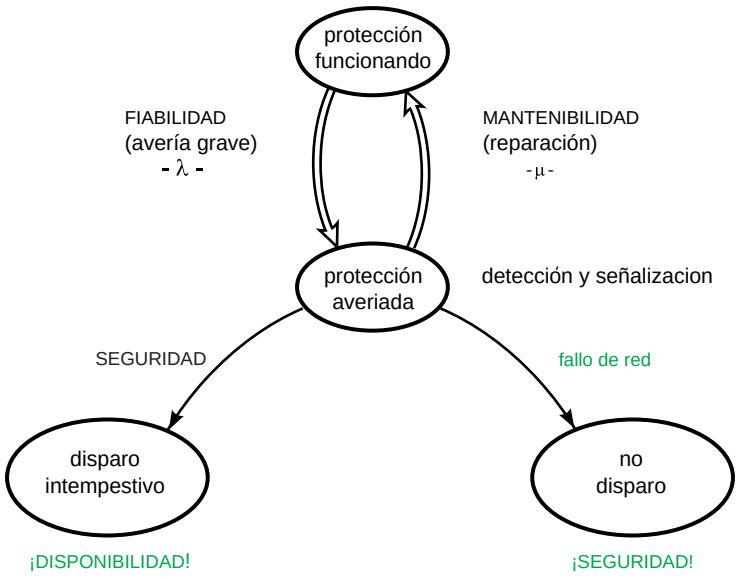



*Fig. 4: Gráfica de los estados de la protección y consecuencias en la distribución eléctrica.*

| fenómenos indeseables | efectos | causas | previsión |
|---|---|---|---|
| disparo intempestivo | ■ apertura intempestiva del interruptor automático<br>■ la energía no está disponible, lo que implica pérdidas económicas importantes (parada de la producción...) | ■ internas, por ejemplo:<br>☐ detección intempestiva de un fallo,<br>☐ accionamiento intempestivo del mando...<br>■ externas, por ejemplo:<br>☐ perturbaciones electromagnéticas<br>☐ saturación de los captadores<br>☐ defectos en el diseño del plan de protección... | por ejemplo:<br>■ funciones de autodiagnóstico<br>■ posición de repliegue<br>■ compatibilidad electromagnética<br>■ captadores amagnéticos |
| enmascaramiento de una orden de disparo | ■ disparo de un nivel aguas arriba de la protección con posibilidad de destrucción local de material<br>■ destrucción importante de materiales (incendio...), si no hay protección aguas arriba | ■ internas, por ejemplo:<br>☐ no detección de un fallo<br>☐ mando bloqueado...<br>■ externas, por ejemplo :<br>☐ perturbaciones electromagnéticas<br>☐ saturación de los captadores<br>☐ fallo de la alimentación auxiliar<br>☐ circuito de disparo del interruptor automático abierto<br>☐ error en el diseño del plan de de protección... | por ejemplo :<br>■ funciones de autodiagnóstico<br>■ compatibilidad electromagnética<br>■ captadores amagnéticos<br>■ módulo de socorro<br>■ supervisión del circuito de disparo<br>■ selectividad lógica |

*Fig. 5: Situaciones indeseables relativas a la función de protección.*

**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 ≤ 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 |
|---|---|
| $\pi_T$ | 5.8 |
| $C_2$ | 5.9 |
| $\pi_E$, $\pi_Q$, $\pi_L$ | 5.10 |

*Fig. 6: Ejemplo de datos de fiabilidad, según el Military Handbook (transcripción literal).*

## Las herramientas del especialista en fiabilidad

Técnicas especializadas de evaluación y de modelización de la seguridad de funcionamiento permiten convertir los objetivos en exigencias de diseño.

■ el análisis provisional de la fiabilidad determina la tasa de fallo de cada componente del equipo en condiciones reales de utilización.

Por esto, se utilizan **bases de datos de fiabilidad**, como la Military Handbook 217 (MIL-HDBK-217) (**figura 6**), o el folleto CNET (RDF 93). Ambas se usan para calcular la fiabilidad de un circuito constituido por varios componentes. Si es necesario, el diseñador modifica el factor de carga de algunos de ellos, o utiliza componentes que tengan garantía de larga duración (este es el caso, por ejemplo, de los condensadores electrolíticos).

■ El Análisis de los Modos de Fallos, de sus Efectos y de su Criticidad, realizado tanto sobre el hardware como sobre el software, valora los efectos de cada tipo de fallo conocido durante el funcionamiento del equipo.

Asimismo, este Análisis de los Modos de Fallos, de sus Efectos y de su Criticidad se usa para corregir ciertos riesgos de disfunción y especificar las funciones de autovigilancia. Este análisis puede aplicarse a nivel de una función general (la función de «protección»); de una función concreta (la función de «protección contra corriente máxima», por ejemplo); aplicarse simplemente a una de sus subfunciones (**figura 7**); o llegar hasta el nivel más bajo, el de los componentes (los colocados en las tarjetas de circuito impreso).

■ los fenómenos indeseables relativos a los equipos de protección se modelizan con varias técnicas:

□ los **árboles de fallos** describen, a partir de un fenómeno indeseable, todas las causas posibles de este suceso (**figura 8**).

El árbol de fallos es la representación «booleana» que se usa para determinar los caminos más críticos para que se produzca un determinado suceso.

□ las **gráficas de Markov** son una representación del comportamiento donde aparecen los estados de marcha, de marcha degradada y de avería del equipo. La transición de un estado a otro se califica por las tasas de fallo ($\lambda$) y de reparación ($\mu$). Estas gráficas se usan para calcular la probabilidad de permanencia en estado de fallo (**figura 9**).

□ las **redes de Petri** tienen el mismo objeto que las gráficas de Markov, es decir, modelizar los estados de un sistema. Permiten estudiar sistemas más complejos, donde la transición entre estados no sigue necesariamente una ley exponencial –ley o distribución de Weibull, por ejemplo (**figura 10**).

Estos sistemas de modelización se usan para hacer una simulación cuantificada de la seguridad de buen funcionamiento y también para obtener las probabilidades que corresponden a la fiabilidad, mantenibilidad, disponibilidad y seguridad del equipo de protección.

El lector podrá encontrar en la bibliografía, en la referencias [Villemeur] o [Pages-Gondran], una información más precisa de estas técnicas.

## Los recursos de la seguridad de funcionamiento

Para conseguir las máximas garantías de funcionamiento de una instalación eléctrica, deben de controlarse la fiabilidad, la seguridad y la mantenibilidad de la protección.

Fijados los objetivos ligados a estas magnitudes, el diseñador de la protección, ayudado por el técnico en fiabilidad, utiliza un cierto número de medios para conseguirlos:

■ gracias al especialista en fiabilidad y sus herramientas, controla la fiabilidad intrínseca antes y durante el desarrollo;

■ gracias a los medios de autovigilancia, de señalización de los fallos y de la comunicación, puede:

□ mejorar la seguridad de la protección pasándola a la posición de repliegue,

□ mejorar la mantenibilidad y la disponibilidad de la protección.

Examinemos los medios que se usan:

■ autovigilancia.

La eficacia y aplicabilidad de la autovigilancia son vitales para la seguridad de buen funcionamiento

| función | modo de fallo | efecto sobre la protección | medio de detección | señalización |
|---|---|---|---|---|
| medir las corrientes de fase | corriente medida errónea: nivel continuo > umbral de disparo | protección activada → disparo intempestivo | el algoritmo utilizado trabaja sobre el cálculo del módulo de la corriente a 50 Hz | inhibición «natural» de la protección |
| | | | detección por el cálculo periódico de la componente continua de la señal | señalizar el fallo en el panel frontal y a través del sistema de comunicaciones |
| | corriente medida errónea: nivel continuo < umbral de disparo | protección no-disponible → no hay disparo ante un posible fallo | los medios de detección son los mismos | señalizar |

*Fig. 7: Tabla de AMDEC realizada con una subfunción de la protección contra intensidad máxima.*

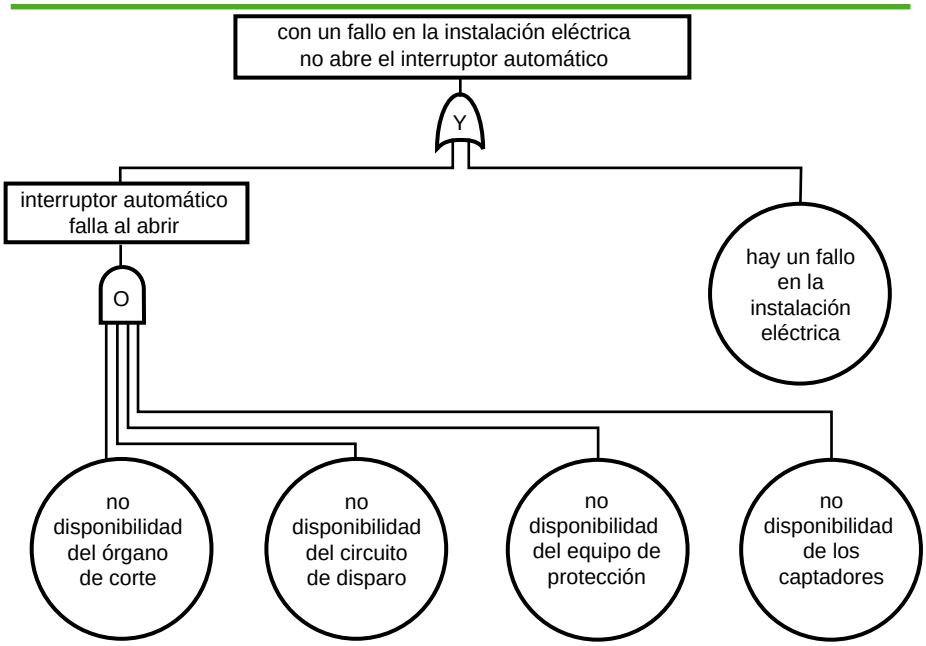



*Fig. 8: Ejemplo simple de árbol de fallos.*

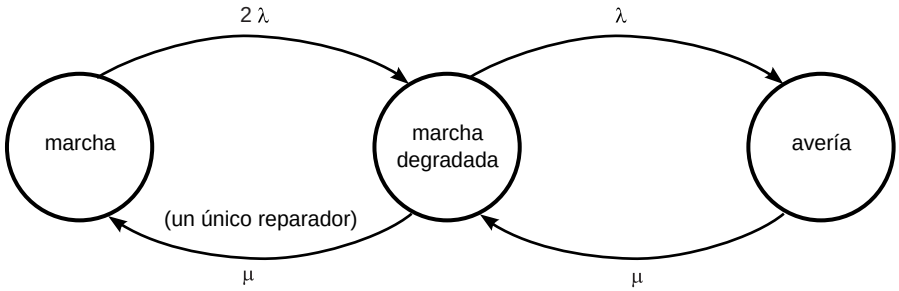



*Fig. 9: Ejemplo de un gráfico de Markov para un sistema constituido por dos componentes redundantes y reparables. Si se trata de dos componentes electrónicos (fiabilidad exponencial), la duración media de buen funcionamiento después de una reparación es* $MUT = \frac{1}{2\lambda . \lambda}$.

La red de Petri representada tiene dos posiciones estables (P1, P2), dos transiciones (T1, T2) y cuatro arcos.
Esta red representa el comportamiento de un componente reparable, al aplicarle, por ejemplo, los significados siguientes a las posiciones estables y transitorias:

P1: el componente está funcionando correctamente,
P2: el componente está averiado,
T1: el componente pasa a avería,
T2: el componente acaba de ser reparado.

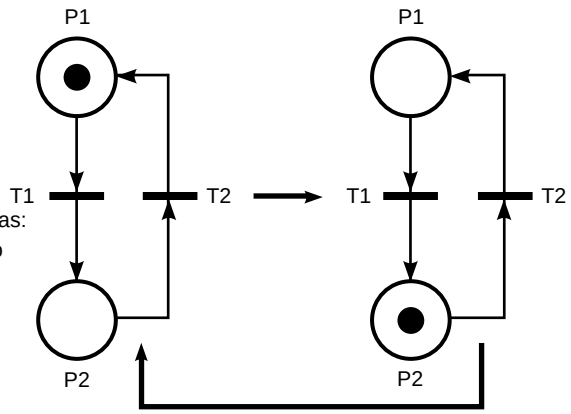



*Fig. 10: Ejemplo de una red de Petri aplicada a un sistema constituido por un elemento reparable.*

de la protección. A modo de ejemplo, se citan algunos medios que pueden aumentar la disponibilidad y la seguridad:

- Al conectar, y después periódicamente, hay que hacer un control de la integridad de los datos contenidos en «programa» y en los «datos constantes». Este control se hace calculando el «checksum» y llevándolo a la parte alta de la memoria utilizada. Este «checksum» arrastrado cubre el 99,95% , para 128 octetos, (99,998% para 128 kilooctetos) del movimiento de los bits de dirección y de los bits de

**Para el control de la integridad de los datos**.

Se pueden utilizar varias técnicas:

- Control de paridad.

Consiste en convertir en par sistemáticamente el número de bits transmitidos, completando el mensaje útil con un «bit de paridad».

De este modo, el receptor puede controlar el mensaje si hay un error de 1 bit o de 3... La alteración de un número par de bits no se puede detectar.

- El CRC (Cyclic Redundancy Check) consiste en adjuntar a la información útil el resto de dividirlo por un polinomio normalizado por el CCIT.

Por ejemplo, el polinomio divisor de grado 16 ($x^{16} + x^{15} + x^2 + 1$ = 1100 0000 0000 0011) utilizado por el «CRC 16» permite la detección de 16 errores simultáneos.

- El Checksum consiste en hacer la suma binaria de los octetos y añadir el resultado (cortando en uno o varios octetos) al mensaje útil.

El Checksum puede añadirse, por ejemplo, al control de paridad en los octetos…

El control de integridad del mensaje por el receptor es más fácil que para el CRC y puede ser más eficaz.

**Para controlar que el programa se ejecute bien**

Usada frecuentemente en automatismos, la técnica del **«perro guardián»** consiste en ejecutar periódicamente una instrucción de prueba.

Si no se ejecuta esta instrucción en un lapso de tiempo determinado, indica que hay un fallo y provoca el disparo de una alarma para que se envíe el equipo de protección a revisar.

*Fig. 11: Los medios digitales de autocontrol.*

memoria. Para controlar un volumen de información mayor de varios centenares de octetos, el cálculo del «checksum» con arrastre es más eficaz que el cálculo de un CRC 16, por ejemplo.

- Hay que disponer de un «perro guardián» de hardware y de software para detectar cualquier bloqueo de la unidad central (debido a un defecto de un componente, a un parásito o a una sobrecarga del microprocesador).

También hay que tener seguridad de la validez de la señal de salida del «perro guardián». El «perro guardián» debe de cubrir incluso los fallos del cristal de cuarzo o del oscilador del microprocesador (**figura 11**).

- Hay que controlar el tiempo de ciclo del programa. Si se usan las interrupciones para secuenciar los ciclos, hay que asegurarse del buen funcionamiento de estos mecanismos.
- Hay que efectuar continuamente un control de la tensión de alimentación para prevenir la caída eventual de la misma y que se quede parado el microprocesador (salvaguardar los parámetros).
- Si se usan memorias EEPROM, hay que supervisar la utilización de este componente, contando el número de grabaciones, que no debe de superar las 10000.
- Hay que evitar tratar los datos digitales erróneos inmediatamente después de un fallo de la cadena de conversión analógico-digital. Un control eficaz para esto es el verificar permanentemente dos señales de referencia a la entrada del multiplexor con dos direcciones complementarias (se consigue así detectar el 100% de fallos del convertidor analógico-digital y el 100% de los cambios a 1 ó a 0 de los bits de selección del multiplexor).

Se usan otros muchos mecanismos de detección, dependiendo sobre todo de la tecnología utilizada.

- la posición de repliegue

Las funciones de autovigilancia detectan el máximo número de fallos que podríamos llamar «mayores». Un fallo se clasifica como de categoría «mayor» si puede provocar un mal funcionamiento de la protección.

Un fallo de este tipo no debe de degenerar en un disparo de la protección. El dispositivo de protección pasa a la posición predeterminada de repliegue para evitar el paso de órdenes aleatorias.

Se informa al usuario del paso a esta «posición de repliegue», y se puede pasar inmediatamente a la posición de mantenimiento para retornar la protección a su plena disponibilidad.

Asimismo, existen fallos llamados «menores», como por ejemplo, el fallo de un periférico (el visor o la consola); se señaliza, pero no afecta a la disponibilidad de la protección.

- la señalización de los fallos

Las funciones de autovigilancia deben de ofrecer medios de diagnóstico adaptados para permitir un retorno rápido al estado de marcha de la protección que ha fallado, es decir:

- dar al usuario una información externa clara y global sobre el estado de la protección,
- dar al fabricante una información interna clara y precisa del estado de la protección, durante una operación de conservación e incluso después del retorno a fábrica de una protección defectuosa.

Por ejemplo, el fallo de la protección se puede señalizar mediante:

- un piloto en el panel frontal,
- una salida del relé «perro guardián»,
- un mensaje en el visor del panel frontal,
- una información que se guarde o grave detallando el origen del fallo,
- un mensaje a través del sistema de comunicación cuando la protección forma parte del sistema de control y mando.

Todo esto es una ventaja importante respecto a protecciones de tecnologías anteriores en las que un dispositivo podía permanecer averiado largo tiempo sin que el usuario se enterara (**figura 12**) y que

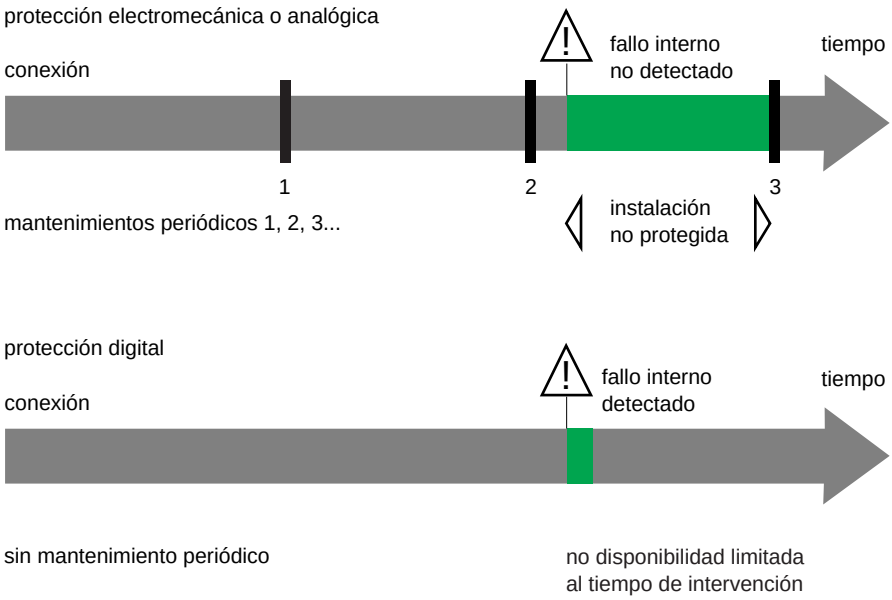



*Fig. 12: La autosupervisión permite reducir el tiempo de no-disponibilidad de la protección y por tanto aumentar la seguridad de la instalación eléctrica.*

además no podía dar ninguna información sobre el origen de la avería...

■ abertura hacia los sistemas de supervisión y de mando y control.

Como ya se ha dicho, la protección digital puede abarcar funciones de automatismo y de comunicación. Se convierte así en un punto de unión del sistema de supervisión con el de mando y control de la instalación eléctrica, lo que facilita la explotación al permitir la vigilancia, la comunicación y la gestión de la red de distribución:

□ vigilancia de los estados y de los valores de las magnitudes eléctricas (medida),

□ vigilancia del estado de los equipos (posición del aparato, temperatura, presión...),

□ tratamiento de alarmas,

□ mando a distancia de los órganos de maniobra,

□ reconfiguración automática de las redes después de un defecto,

□ gestión de la energía consumida en función de la tarificación de las compañías suministradoras,

□ edición de informes de explotación,

□ asignación de los costes de energía a cada uno de los consumidores de la instalación.

■ la facilidad de mantenimiento

□ la autovigilancia, la señalización y la comunicación facilitan el conocimiento del estado del defecto y de ahí la acción inmediata del personal de mantenimiento,

□ el autodiagnóstico permite al que repara el aparato conocer el origen del fallo y de ahí la rapidez de reparación,

□ las funciones programadas, que personalizan la protección en cuanto a las aplicaciones o funciones que puede realizar, se almacenan en un cartucho removible. Esto facilita la reposición inmediata del servicio después de reemplazar la parte física del aparato (hard), que está estandarizada.

■ casos especiales

La fiabilidad de la protección puede ser insuficiente si sufre agresiones excepcionales o si las necesidades de disponibilidad y seguridad de la distribución eléctrica son excepcionalmente elevadas:

□ entornos severos

Los sistemas de protección están a veces instalados en ambientes excepcionales que sobrepasan las especificaciones de los materiales:

- temperatura,

- vibraciones…

En cada caso, el departamento de diseño debe de identificar claramente las necesidades. De esta forma se proponen soluciones personalizadas:

- ajustes especiales de tarjetas electrónicas,

- contrato de mantenimiento específico.

□ necesidades excepcionales de seguridad

Un módulo auxiliar de emergencia puede asumir la protección en caso de:

- fallo de la alimentación,

- fallo del cableado,

- fallo del relé de disparo,

- protección principal fuera de servicio.

Otra solución consiste en duplicar el equipo de protección, con un circuito «o» en el sistema de mando del órgano de corte. Para la instalación, la seguridad queda muy reforzada y la disponibilidad de la energía no disminuye, cuando se emplean sistemas de protección con la posición de repliegue.

Como solución extrema, se pueden tomar en consideración los sistemas

2/3.

# 3 La seguridad de funcionamiento como una parte de la búsqueda de la calidad total

## Calidad del software

Una parte importante de las prestaciones de los equipos de protección digitales la realiza el software. Por tanto es necesario conseguir un software de calidad para poder lograr los objetivos globales de seguridad.

El control de la calidad del software se consigue siguiendo un riguroso método de trabajo.

Este método, nacido de las recomendaciones establecidas por organismos nacionales e internacionales (IEEE), exige seguir una serie de pasos:

- La división de la aplicación en una sucesión de fases (**figura 13**):
  - especificación,
  - anteproyecto,
  - diseño detallado,
  - codificación,
  - pruebas unitarias,
  - integración y prueba de integración,
  - validación.

A cada una de estas fases se le asocia un conjunto de documentos que se usan y se producen durante ese paso.

Estos documentos contienen los estudios realizados en cada fase y deben de ser validados antes de pasar a la fase siguiente.

- La utilización de reglas y métodos de diseño y codificación que tienen por objetivo el conseguir un alto nivel de estructuración del software (por ejemplo, SADT desarrollado en las herramientas ASA o MACH).
- La utilización de herramientas de gestión de la configuración del software, lo que permite gestionar todos los componentes del programa y especialmente controlar la evolución y las nuevas versiones de todos los componentes (por ejemplo, la herramienta CMS).

Por otra parte, se usan con gran provecho los métodos de revisión de código. Un verificador efectúa una lectura crítica del código y hace sus observaciones. Este análisis «manual» resulta ser en este punto uno de los métodos más eficaces para descubrir los fallos lógicos (los errores de programa).

Finalmente, una vez que cada programa está integrado y validado, una última fase de calificación, dirigida por un equipo independiente del equipo de desarrollo, asegura un control final eficaz.

## Calificación de los equipos de protección

Los equipos de protección, antes de salir al mercado, pasan por un proceso completo de calificación.

Se detallan aquí ciertos criterios de calificación específicos para los entornos de MT y AT:

- la inmunidad a las perturbaciones electromagnéticas (conducidas o radiadas).

Las perturbaciones eléctricas encontradas en los centros de transformación tienen diversos orígenes:

- las descargas de rayo que inciden directamente en las líneas o cerca de los centros de transformación pueden producir sobretensiones de unos centenares de kV y con un frente de subida de orden del microsegundo;
- la maniobra normal de la aparamenta, al abrir y cerrar el órgano de corte de MT o AT, provoca sobretensiones de «maniobra» (onda oscilatoria amortiguada). Estas sobretensiones pueden producir campos eléctricos con crestas del orden de 10 kV/m a 1 metro del interruptor automáticos;
- los operarios pueden provocar descargas electrostáticas que producen sobre el material impulsos de corriente de algunas decenas de amperio y de frente muy rápido, del orden de nanosegundos;

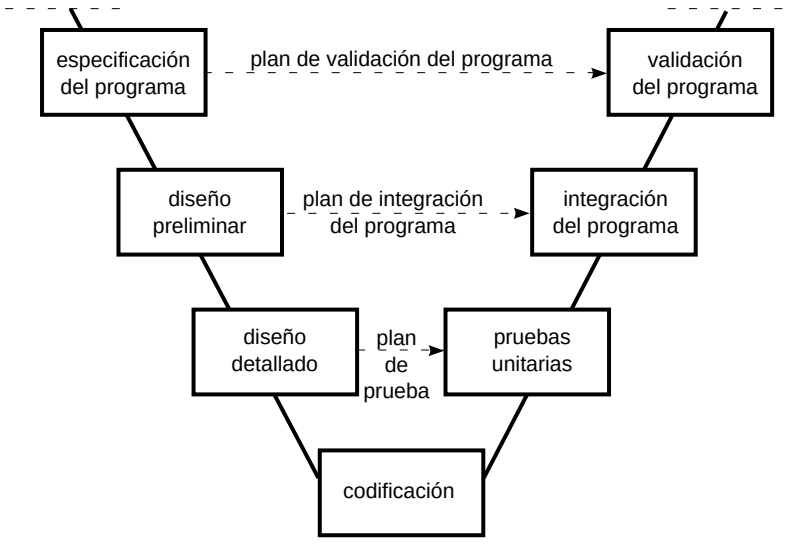



*Fig. 13: Ciclo de desarrollo de un programa (llamado en V).*

- los emisores radioeléctricos (talkies-walkies, por ejemplo) producen campos de varias decenas de V/m a 1 metro.

El lector que desee profundizar en el tema de la Compatibilidad Electromagnética -CEM- puede leer el Cuaderno Técnico nº 149.

Los valores estándar internos de resistencia a los esfuerzos eléctricos definen los niveles de inmunidad necesarios para el funcionamiento de los sistemas de protección en un centro de transformación eléctrico.

Estos niveles corresponden a las resistencias dieléctricas definidas por las normas CEI 255 y, a veces, hasta más severas. Con los ensayos se controla que se respeten los niveles de exigencia definidos. Se realizan cuatro tipos de ensayos:

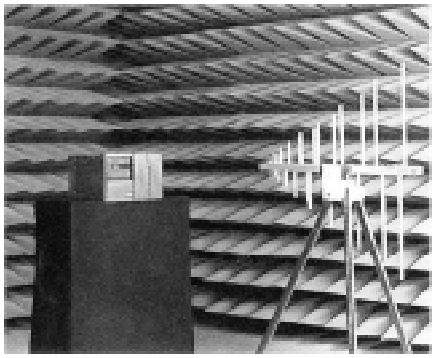


*Fig. 14: Ensayos de perturbaciones electromagnéticas en cámara aneocoica.*

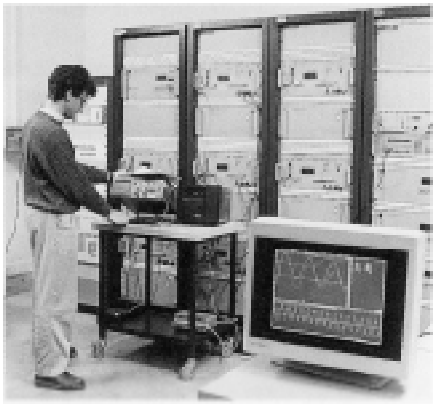


*Fig. 15 : Laboratorio Kirchhoff de ensayos de protecciones.*

- onda oscilatoria amortiguada (CEI 255-22-1)

severidad: clase III, 2,5 kV,

- transitorios rápidos

(CEI-255-22-4)

severidad: clase IV, 4 kV,

- descargas electrostáticas (CEI 255-22-2)

severidad: clase III, 8 kV,

- campos radiados

(CEI-255-22-3)

severidad: mejor que la clase III, 30 V/m (**figura 14**).

Nota: el ensayo de transitorios rápidos es la transcripción en modo «conducido» de campos electromagnéticos impulsionales «radiados», producidos durante las maniobras de la aparamenta.

Además de los ensayos de CEM, los equipos de protección se someten a ensayos «en situaciones reales».

A título de ejemplo, con el equipo situado en el lado de BT de una celda de MT, se hacen un centenar de maniobras «cerrar-abrir» del interruptor automático. Al hacerlo con poca carga y ser ésta de tipo autoinductivo aparecen importantes

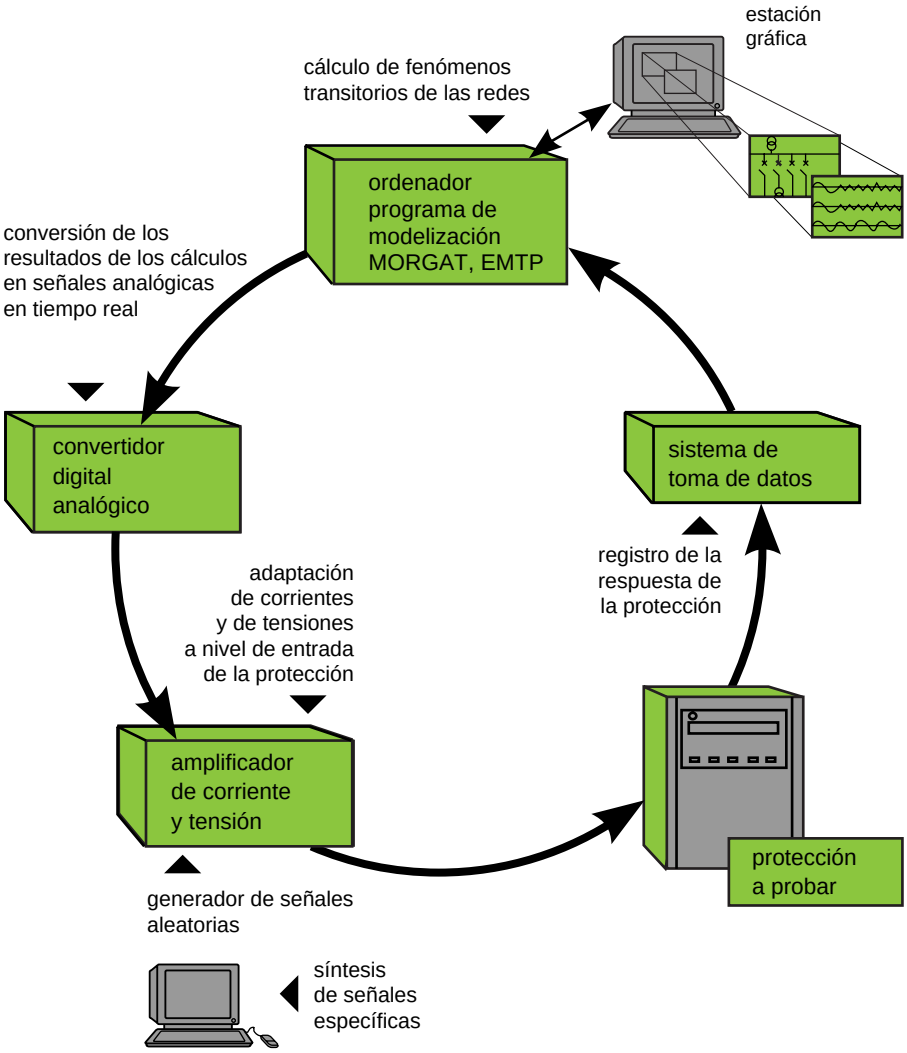



*Fig. 16: Descripción del sistema de ensayos de protecciones.*

sobretensiones de corte de la corriente.

Durante estos ensayos, el equipo de protección no debe de tener ningún fallo intempestivo.

- el laboratorio Kirchhoff: ensayos de protecciones.

Las funciones realizadas por los sistemas de protección son complejas. El buen funcionamiento de las protecciones debe de quedar garantizado para el conjunto de fenómenos susceptibles de producirse en las redes eléctricas. Por tanto, es necesario un laboratorio que realice ensayos de las protecciones (**figura 15**).

El laboratorio Kirchhoff permite reproducir con valores reales los fenómenos tal como aparecen en las redes eléctricas (**figura 16**).

Está equipado con un simulador digital que permite:

- calcular las corrientes y tensiones de red, precisamente en el momento en que se produce un cortocircuito, un defecto de aislamiento o la maniobra de un aparato,
- generar las señales correspondientes y aplicarlas al aparato bajo prueba. Se analiza entonces el comportamiento de las protecciones sometiéndolas a condiciones idénticas a las que se encontrarán en la red real.

La simulación digital de redes eléctricas del laboratorio Kirchhoff usa dos programas:

- EMTP (ElectroMagnetic Transient Program), programa para calcular fenómenos transitorios. Este programa, mundialmente utilizado, permite, a partir de una base de datos con las características de los materiales (transformadores, líneas, máquinas...), elaborar modelos de todo tipo de redes eléctricas, simular un fallo o maniobra de un aparato y calcular con precisión la variación en el tiempo de las corrientes y tensiones;
- MORGAT, simulador de redes eléctricas, desarrollado por la EDF (Electricidad de Francia). Este programa permite simultáneamente analizar con precisión el comportamiento de las redes y controlar el aspecto «tiempo real» en el laboratorio Kirchhoff. Las corrientes y tensiones, calculadas en diversos puntos de la red eléctrica simulada, se convierten en señales analógicas para aplicarlas en la protección que se está probando.

## Control de calidad

Tanto durante la producción como al acabar ésta, los equipos de protección sufren numerosas pruebas de control.

Por ejemplo, las tarjetas electrónicas sufren un primer control en el banco de pruebas dieléctrico que hace los ensayos de aislamiento.

A continuación se les aplica una prueba de funcionamiento «in situ» (**figura 17**).

La prueba «in situ» comprueba el funcionamiento de cada componente de la tarjeta electrónica y además que estén bien implantados. Detecta sobre todo los defectos de fabricación y ciertos defectos de los componentes. Da un diagnóstico implícito y permite una rápida reparación de la tarjeta. A continuación el servicio de calidad analiza los resultados y se consigue detectar rápidamente cualquier desviación en calidad de los componentes o de la fabricación de las tarjetas.

Después de haber pasado por la prueba «in situ», las tarjetas se someten a esfuerzos térmicos y eléctricos combinados. Esta acción elimina los defectos de juventud del material electrónico y permite reducir la duración del período llamado de juventud, consiguiendo que aparezcan los defectos de fabricación antes de que lleguen a la explotación.

Y, además, el servicio de control de calidad también utiliza las estadísticas de defectos para corregir rápidamente cualquier pérdida de calidad de la fabricación.

Las pruebas finales permiten asegurar que las tarjetas que se instalan se comuniquen perfectamente entre ellas y que la configuración que se monta sea la que responda mejor a lo que pide el cliente. Para comprobarlo, se verifica que las señales aplicadas al interfaz del equipo ya montado activa el conjunto de funciones que tiene que prestar el aparato de protección.

Por otra parte, los controles sistemáticos realizados sobre la producción y los test de calidad se hacen periódicamente sobre una muestra representativa de toda la gama del producto.

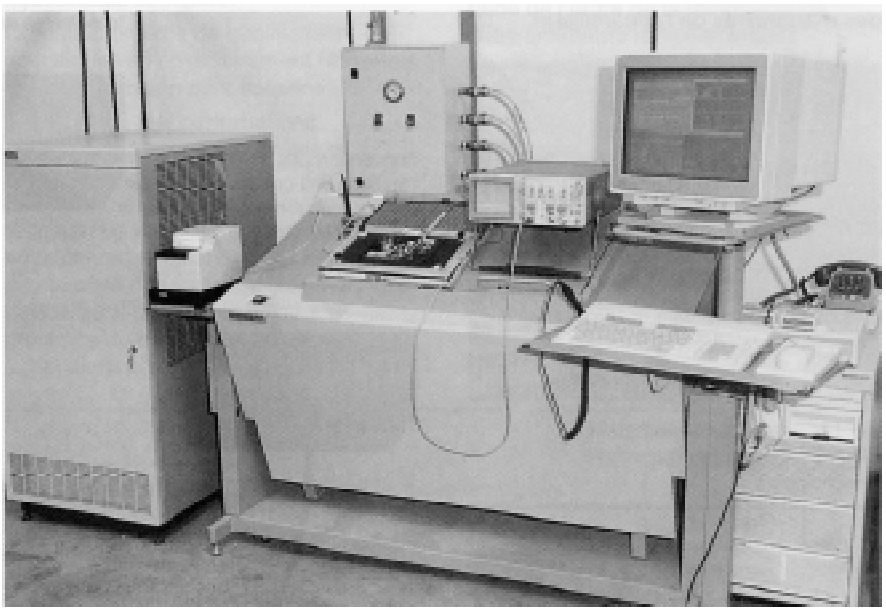


*Fig. 17: Prueba «in situ».*

# 4 Análisis de la información de retorno de la experiencia

Para tener una información de retorno significativa de la explotación de los equipos, es necesario, cuando la fiabilidad es muy buena, tener un parque muy amplio de equipos en servicio. Es entonces cuando se pueden analizar los datos de fallos en explotación. Este análisis de la información de retorno de la explotación es fundamental para:

- medir la fiabilidad operacional de los equipos;
- validar los estudios de seguridad realizados durante el diseño;
- acumular experiencia técnica para progresar;
- disponer de una base de diálogo entre el fabricante y el usuario.

La información de retorno de la experiencia descansa sobre una colección fiable y ordenada de informaciones relativas a los problemas de los clientes. La fiabilidad operacional (calculada con la información de retorno) sólo es útil si el defecto es detectable, detectado y registrado. Los datos de fallos obtenidos de un parque de equipos que no tienen funciones de autovigilancia o cuyo mantenimiento periódico es poco frecuente pueden no ser representativos de la fiabilidad real.

Los datos de fiabilidad operacional obtenidos de un parque de protecciones digitalizadas son muy buenos para hacer una autovigilancia.

Se ha constatado que la fiabilidad operacional era al menos diez veces superior a la previsible (calculada a partir de una muestra de datos MIL-HDBK-217E). Esta diferencia procedía probablemente de una toma de datos de fiabilidad intencionadamente pesimista y a la vez anacrónica (las tecnologías y la calidad de los componentes electrónicos evolucionan muy rápidamente).

Las últimas actualizaciones de tomas de datos de fiabilidad han reducido considerablemente la diferencia entre los resultados de fiabilidad operacional y prevista.

Hoy, el MTBF correspondiente al disparo intempestivo o al no funcionamiento de la protección alcanza varios centenares de años.

# 5 Conclusión

Los equipos de protección de las redes MT y AT garantizan una función de seguridad primordial. Deben de garantizar la protección de materiales y personas asegurando a la vez la disponibilidad de la energía. Sus disfunciones pueden producir a los usuarios pérdidas económicas importantes. Es, por tanto, esencial que respondan a altas exigencias de fiabilidad, seguridad, disponibilidad y mantenibilidad. Para esto, los equipos de protección deben de tener ciertas características técnicas e industriales, de las que, las más significativas, son:

- proteger bien las redes y equipos MT y AT, gracias a algoritmos adaptados a las diversas funciones de protección;
- ser fáciles de instalar, de utilizar y mantener;
- ser fiables en un entorno severo, y además:
  - ser capaces de autovigilarse,
  - tener una posición de repliegue.

Gracias al trabajo de los que durante el diseño estudian la fiabilidad y la calidad, los equipos de protección digitales que hay actualmente en el mercado responden a estas exigencias.

Actualmente, teniendo en cuenta el desarrollo de las comunicaciones digitales (bus) y de la supervisión, la funcionalidad de los equipos de protección llega hasta el dominio del mando y control para una gestión óptima de la distribución eléctrica.

# 6 Anexo

Tiempos medios que caracterizan la seguridad (**figura 18**):

El MTTF (Mean Time To first Failure) es el tiempo medio de buen funcionamiento antes de un fallo.

El MTTR (Mean Time To Repair) es el tiempo medio de reparación.

El MTBF (Mean Time Between Failure) es el tiempo medio entre dos fallos (para un sistema reparable).

El MDT (Mean Down Time) es la duración media de fallo que abarca la detección de la avería, el tiempo de intervención, el tiempo de reparación y el tiempo de volver a dar servicio.

El MUT (Mean Up Time) es la duración media de buen funcionamiento después de una reparación.

El término MTBF se traduce inadecuadamente como la media de tiempos de buen funcionamiento. ¡Esta definición es, de hecho, la del MTTF! La confusión viene del hecho de que frecuentemente el MTTR (del orden de algunas horas) es despreciable respecto al MTTF (del orden de varios miles de horas).

**Las probabilidades**

La Fiabilidad, R(t) (Reliability) es la probabilidad de que un sistema no falle en un tiempo t.

La Mantenibilidad (Maintenability) es la probabilidad de que un sistema pueda repararse en un tiempo t.

La Disponibilidad (Availability) es la probabilidad de que un sistema funcione en un instante t.

La Seguridad (Safety) es la probabilidad de evitar un suceso catastrófico.

En general, se trabaja con una magnitud que es la tasa de fallos $\lambda$ (t). Es la probabilidad de que el sistema falle en el instante siguiente, pensando que el sistema no ha de fallar.

Para un componente electrónico, la tasa de fallos sigue una evolución en el tiempo llamada curva en forma de «bañera». Durante el período llamado «de vida útil», el componente no envejece y su tasa de fallos $\lambda$ se mantiene constante en el tiempo. Se obtienen entonces las eventuales relaciones fundamentales siguientes:

Fiabilidad $R(t) = e^{-\lambda t}$ y $MTTF = 1 / \lambda$.

Ejemplo:

Si un equipo tiene un MTTF de 100 años, su tasa de fallo $\lambda$ = 1/MTTF es de $10^{-2}$ / año. La probabilidad de fallo es, cada año, del 1%.

¡Un MTTF (o MTBF) de 100 años no significa en modo alguno que el sistema no fallará en 100 años! El MTTF no es, por tanto, asimilable ni a la duración garantizada ni a la esperanza de vida...

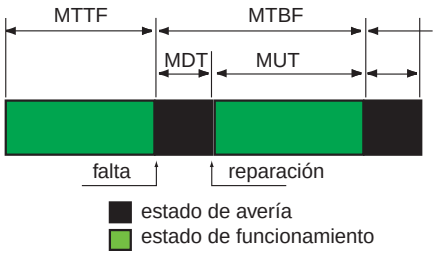



*Fig. 18: diagrama de tiempos medios establecido para un sistema que necesita no interrumpir su funcionamiento para hacer el mantenimiento preventivo.*

# 7 Bibliografía


**Publicaciones diversas**

- Reliability design approach for protection and control equipment for MV distribution networks. Segunda Conferencia internacional de «The Reliability of Transmission and Distribution Equipement». M. LEMAIRE, J. C. TOBIAS. Marzo 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. Enero 1991.
- Military Handbook 217 -F- Department Of Defense, USA.
- Recueils de données de fiabilité des composants électroniques, RDF 93 CNET.
- CEI 191.

**Cuadernos Técnicos Merlin Gerin**

- Introducción al diseño de la seguridad. CT n° 144. P. BONNEFOI
- La CEM: la compatibilidad electromagnética. CT n° 149. F. VAILLANT
- Protecciones de redes de AT-A industriales y terciarias. CT n° 174. A. SASTRÉ