

## **TERCER EJERCICIO. SEGURIDAD NUCLEAR**

### **Tema 3-A-10**

#### **El sistema de protección del reactor en centrales nucleares**

##### INDICE

1. Resumen ejecutivo.
2. Relación con otros temas del sumario.
3. Aspectos generales.
4. Circuitos representativos. Estructura.
5. Partes del sistema.
  - 5.1. Nivel de detección.
  - 5.2. Sección analógica.
  - 5.3. Sección lógica.
6. Criterios.  
Bibliografía.

## **1. Resumen ejecutivo**

Este tema comienza considerando los aspectos generales que definen y caracterizan el sistema de protección del reactor (SPR) de las centrales nucleares.

Se incide seguidamente en aspectos descriptivos, a partir de diagramas lógicos sencillos, buscando aproximarse a la estructura general del sistema, partes principales y funciones de los componentes más significativos.

El SPR se subdivide en sistema de disparo, ó parada, del reactor y sistema de actuación de las salvaguardias tecnológicas; con aplicabilidad a ambos, se exponen las características fundamentales de la detección (sensores), sección analógica y sección lógica (que puede ser electrónica, ó de relés), incluyendo en esta parte el nivel de actuación (relés de salida).

En cuanto a criterios, se listan y analizan los que aparecen en la norma IEEE Std 279-1971, "IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations", norma de aplicación obligatoria para los reactores con diseño original de EE.UU., que aporta una buena claridad conceptual acerca de los criterios que se han venido aplicando en el diseño de los sistemas de protección.

## **2. Relación con otros temas del sumario.**

Este tema está relacionado directamente con los temas 23 y 24.

El tema 23 considera todos los sistemas de instrumentación de las centrales, de los cuales el sistema de protección constituye uno de ellos, el más relevante en cuanto a la seguridad.

De dicho tema 23, sus apartados 2.1 y 4 guardan una relación directa con los apartados 3 y 5 de este tema, fundamentalmente con el apartado 5.3 en lo relativo a la sección lógica de los reactores PWR de suministro Westinghouse.

El tema 24 desarrolla los tipos de instrumentos de medida que, en cuanto a las variables más habituales, vigilan éstas a efectos de que, en caso de excederse unos valores de seguridad predeterminados, generen la actuación del sistema de protección. Tales instrumentos forman parte del sistema de protección.

### **3. Aspectos generales**

El sistema de protección del reactor (SPR) tiene por misión la iniciación de las oportunas actuaciones de seguridad para evitar consecuencias en caso de transitorios previstos (sucesos Condición 11, según terminología del suministrador Westinghouse), y mitigarlas en caso de transitorios infrecuentes (sucesos Condición 111) y accidentes base de diseño (sucesos condición IV). Tal y como se refleja en el GDC 20 "Funciones del Sistema de Protección" del Apéndice A del 10CFR50, el sistema deberá ser diseñado para:

- (1) iniciar automáticamente la operación de los sistemas apropiados, incluyendo los sistemas de control de reactividad, para asegurar que los límites de diseño especificados para el combustible no son excedidos como consecuencia de transitorios operacionales previstos, y
- (2) detectar condiciones de accidente e iniciar la operación de sistemas y componentes importantes para la seguridad.

Los requisitos de diseño para el SPR se basan en que este sistema ha de proporcionar la adecuada respuesta para proteger las barreras físicas entre el combustible y el medio ambiente exterior (esto es, las vainas del combustible, la barrera de presión del refrigerante y la integridad del recinto de contención), a fin de garantizar que no se exceden los límites o criterios establecidos para el CLEN (coeficiente del límite de ebullición nucleada), la densidad de potencia, los daños a vainas de combustible y la liberación de material radiactivo, ante cualquiera de los diversos sucesos considerados en los análisis de accidentes.

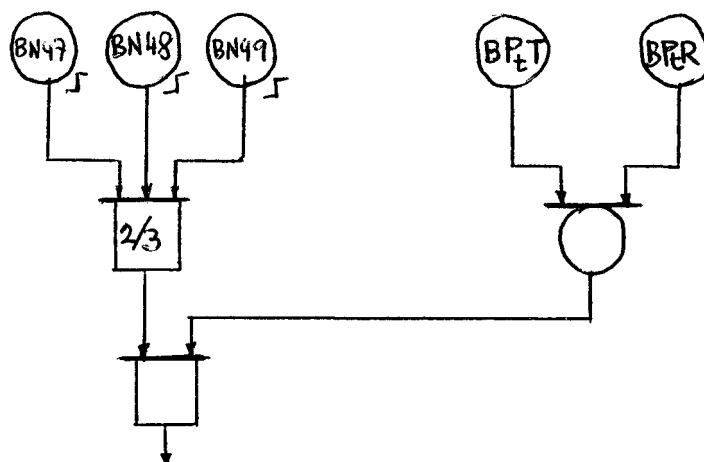
El SPR responde a la necesidad de un sistema de alta fiabilidad capaz de recibir las señales de demanda de acciones de protección generadas en los diversos sistemas de instrumentación que vigilan el proceso (así como por el operador en sala de control), interpretar estas señales aplicándoles los criterios lógicos adecuados a las redundancias existentes para cada una de ellas y, generar las órdenes necesarias para producir las acciones de protección previstas, que en general se engloban en dos: disparo (ó parada rápida, también llamada "scram") del reactor y actuación de salvaguardias tecnológicas. Asimismo, el sistema tiene otras misiones como la de suministrar señales de alarma o informar de las acciones de protección ocurridas.

La descripción detallada del sistema de protección aparece en el capítulo aplicable del Estudio Final de Seguridad, para cada central; el control de su operabilidad se garantiza vía los requisitos contenidos en las Especificaciones de Funcionamiento, que establecen las condiciones autorizadas para mantener a la central operando con el nivel de seguridad requerido.

#### 4. Circuitos representativos. Estructura,

A efectos descriptivos del sistema de protección del reactor, parece conveniente comenzar planteando un diagrama lógico simple, como inicio de la aproximación a la estructura general del sistema.

Consideremos el diagrama lógico siguiente:



Los símbolos utilizados son los siguientes:

**H** Puerta Y (AND): se produce salida cuando están presentes todas las entradas.  
Puerta Y con lógica de coincidencia 2/3 (puerta "2-de-3"): se produce salida cuando están presentes al menos 2 de las 3 entradas.

**t7** Puerta O (OR): se produce salida cuando están presentes cualquiera de las entradas, basta con una de ellas.

**t7** Dispositivo biestable: su entrada es una variable continua, esto es, si se la representa en una gráfica de tiempos sigue una curva, y solamente tiene dos salidas posibles, la de su estado normal y la de su estado de seguridad; cambia su salida cuando el valor de la variable de entrada excede un valor de tarado de seguridad prefijado. Se les representa con su identificación (p.e., BN47, biestable de nivel n° 47; LB47, en iniciales en inglés).

En el diagrama, tenemos que cuando al menos dos de los tres biestables de nivel exceden su valor de tarado, cambia el estado de salida de la puerta "2-de-3", tenía un "0" lógico y pasa a tener un "1"; para que ese "1" progrese, ha de haber un "1" a la salida de la puerta O de la derecha, esto es, tendrán que haberse activado al menos uno de los biestables de su entrada (el BPtT, biestable de potencia de turbina, ó el BPtR, biestable de potencia del reactor).

De ser así, tendremos un "1" a la salida de la puerta Y de salida final.

El circuito considerado, por tanto, lo que hace es que cuando el nivel de un tanque ó vasija (p.e., el del presionador de un reactor PWR) excede su valor de tarado de seguridad, se produce orden de actuación de la protección, en este caso el disparo del reactor, si tal subida de nivel ocurre cuando se está en condiciones de operación a potencia; y esto se infiere de que la potencia de la turbina ó la potencia del reactor exceden su valor de tarado (p.e., el 10%). Si la subida de nivel hubiese ocurrido a potencia inferior al 10%, el disparo del reactor no habrá de ocurrir, es una condición operativa que no requiere actuación del sistema de protección.

Con esta introducción como referencia, y buscando ver en qué partes se suele dividir el sistema de protección de cualquier central nuclear, siguiendo un esquema de arriba abajo, esto es, desde sus entradas desde el proceso que se está vigilando hasta sus salidas hacia actuación de la protección, tales partes serían las siguientes:

Nivel de detección (instrumentos de medida y sus líneas de conexión con el proceso, señales de salida de los instrumentos).

En el caso antes dibujado, cada biestable de nivel recibirá señal de un transmisor, y éste tendrá dos conexiones con el proceso, dado que la medida de nivel se hace midiendo presión diferencial (diferencia entre dos presiones); el biestable de alta potencia de turbina recibe señal de un transmisor que mide presión (en la cámara de impulsos de la turbina), lo que precisa solamente de una toma de proceso; en tanto que los biestables de potencia neutrónica reciben señal de detectores que no requieren tomas de proceso, dado que los neutrones del núcleo inciden directamente sobre el detector.

Los medidores de flujo neutrónico no se denominan transmisores, para ellos se emplea el término detector; forman parte de un subsistema dentro del sistema de protección, el sistema de instrumentación nuclear.

Normalmente, existen no uno sino varios detectores de flujo neutrónico (variable de la que se infiere la potencia nuclear del reactor), pues el flujo neutrónico tiene dependencia espacial.

Sección analógica (llegada de la señales a las cabinas de sala de control; acondicionamiento de la señal; cálculos en su caso; salidas hacia control, indicación, registro ó alarma; dispositivos biestables).

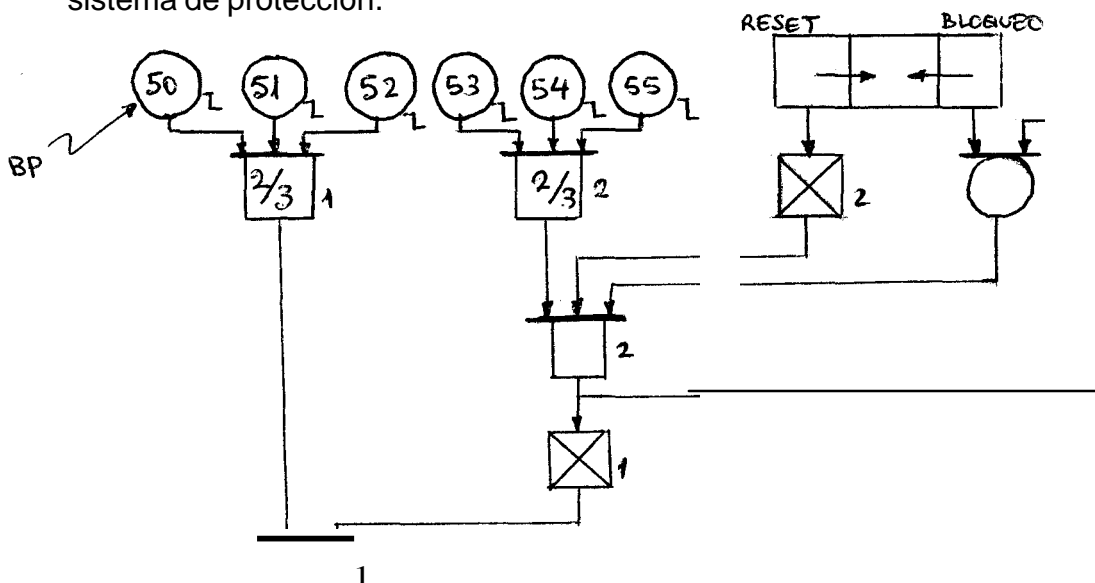
En el caso anterior, los biestables pertenecen, por tanto, a la sección analógica.

Sección lógica, a la que llegan las salidas de los biestables, y hace la combinación de las mismas para formar el nivel de coincidencia requerido, generando una salida hacia el nivel de actuación (bobinas de interruptores, relés), que controlan directamente la actuación de los equipos de seguridad.


En el diagrama antes considerado, los circuitos que conforman el conjunto de las puertas Y, "2-de-3", O, ....., constituiría la sección lógica.

Pasemos a considerar el diagrama lógico de un circuito similar al anterior, pero un poco más complejo pues incorpora la acción del operador de sala de control.

En ese circuito, los biestables (de presión) actúan en el otro sentido, esto es, cambiando estado cuando el valor de la variable, partiendo del valor de operación normal, desciende hasta un valor de tarado prefijado (pasando a tener un "1" en su salida); la acción del operador, de bloqueo del circuito, se podrá realizar por debajo de un valor de la presión intermedio entre el de operación normal, más alto, y el de tarado de seguridad antes aludido. Con dicho bloqueo se evita que, si la presión es baja, ó ha bajado, debido a una condición de operación normal de la planta, tenga lugar la actuación del sistema de protección.



Con respecto al diagrama precedente, se han añadido los siguientes símbolos:

 Dispositivo biestable del tipo que su cambio su estado para generar señal de seguridad tiene lugar cuando el valor de la variable de entrada cae por debajo del valor de tarado.

Maneta con retorno por muelle a su posición central; si se la desplaza a su posición bloqueo, emite un "1" momentáneo en su salida; idem para el caso que se la accione hacia su posición reset (reposición, ó rearme). Salvo en los instantes en que se actúe la maneta, sus dos salidas de señal son un "0".

**r&J**

Puerta NO: su salida es la contraria que la entrada (p.e., si le llega un "0", su salida será un "1").

(Se han numerado las puertas Y, las "2-de-3" y las NO, al haber dos de cada, y a efectos del texto que sigue).

Con esta disposición, y considerando el caso de que la presión esté descendiendo, cuando llegue al valor de disparo de los biestables 53, 54 y 55 (sería el valor intermedio antes aludido) pasamos a tener un "1" a la salida la puerta "2-de-3" nº 2; desde ese momento el operador, cuando actúe sobre la maneta dando a bloqueo, generará la anulación (bypass operativo) del circuito, dado que llegarían tres señales "1"(\*) a la puerta Y nº 2. Su salida se invertirá en la puerta NO nº 1, y hará que le llegue un "0" a la entrada de la derecha de la puerta Y nº 1. Ello evitará que, de seguir descendiendo la presión y cuando se alcance su tarado de seguridad (la salida de los biestables 50, 51 y 52 pasará a ser un "1"), se produzca la coincidencia de entradas en la puerta ANO nº 1, con lo que la acción del operador habrá evitado la actuación innecesaria del sistema de protección (\*\*).

(\*) Habrá tres señales "1" porque se habrán activado al menos dos de los biestables 53, 54 y/o 55, lo que da un "1" a la salida de la puerta "2-de-3" nº 2; la posición reset de la maneta tiene un "0" en su salida, que pasa a ser un "1" en la puerta NO nº 2; y porque la acción del operador al dar al bloqueo envía un "1" momentáneo que hace que pase un "1" vía la puerta O.

Puede verse, en el diagrama lógico, que la salida de la puerta Y nº 2 tiene una realimentación hacia la puerta O, de modo que el "1", en principio momentáneo, de salida de la dicha puerta llega a la entrada de la derecha de la puerta O y hace que la salida de ésta permanezca con un "1" mantenido, aunque su entrada de la izquierda haya pasado a ser un "0" al haber retornado la maneta de la posición bloqueo hacia la posición central. La señal de bloqueo ha quedado por tanto sellada, ó mantenida.

(\*\*) El bloqueo se elimina cuando ocurre cualquiera de las dos situaciones siguientes:

- a) cuando la presión asciende, y hace que los biestables 53, 54 y 55 dejen de estar disparados, esto es, vuelvan a la condición en que tienen un "0" a la salida, ó
- b) cuando el operador actúa sobre la maneta dándole a reset, ello genera un "1" momentáneo en su salida, que genera un "0" momentáneo en la puerta NO nº 2, y hace que igualmente la puerta Y nº 2 pase a tener un "0", que motiva que su salida pase a ser un "0" permanente debido a que se deshace la realimentación que mantenía un "1" a la salida de la puerta O.

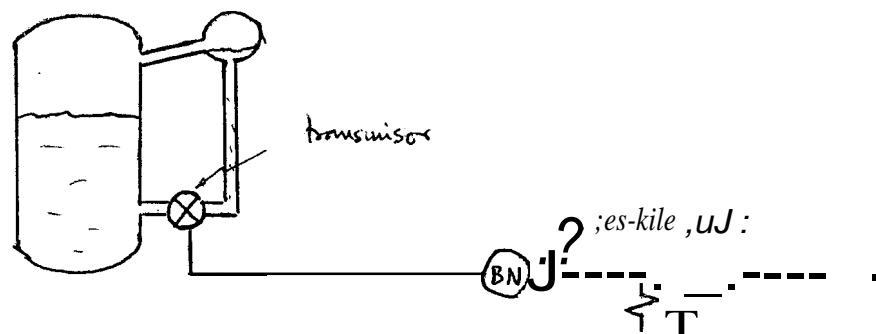
En tales situaciones, y como la salida de la puerta Y nº 2 sería un "0", que pasa a ser un "1" en la puerta NO nº 1, la puerta Y nº 1 se ha devuelto a las condiciones de generar actuación si se produjese la activación de los biestables 50, 51 y/o 52.

Los diagramas lógicos se implantan en el diseño mediante tarjetas electrónicas, empleándose en algunas centrales otra opción, la de utilizar circuitos con relés.

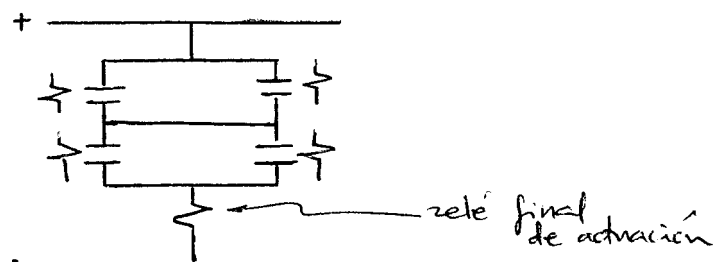
Un relé es un dispositivo interruptor accionado electromagnéticamente, de pequeño tamaño; tiene una bobina, que en función de que esté ó no esté en tensión, produce un cambio de estado de unos contactos, con lo que el circuito de salida cambia su estado, de abierto a cerrado ó viceversa según exista tensión (hay un efecto de atracción electromagnética sobre los contactos que controlan el circuito de salida) ó no exista tensión (los contactos recuperan su posición original por un efecto de resorte que actúa en sentido contrario).

Veamos un ejemplo ilustrativo de la utilización de relés y, esquemáticamente, del conjunto de la cadena de protección. Es el de un sistema que tiene por función la inyección de agua en caso de emergencia, en la vasija de un reactor, para mantener las condiciones de adecuada refrigeración ante una situación de una rotura ó fuga de una tubería primaria.

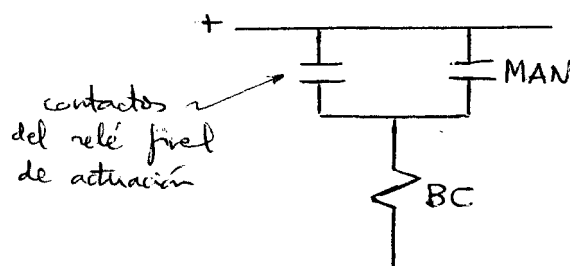
La vasija dispone de un sistema de medida de nivel, en este ejemplo, que consta de cuatro columnas de referencia, con sus correspondientes transmisores y biestables (en la figura se representa esquemáticamente lo relativo a uno de los canales ó redundancias, partiendo de una de las formas de medir el nivel que se considera en el tema 24).



Esto es, lo arriba representado estaría cuadruplicado. Cada biestable (ó unidad de disparo) controla el estado de energización de un relé, y los contactos de los cuatro relés se combinan para conseguir una lógica determinada; el dibujo muestra el caso de una lógica "1-de-2-dos-veces", a la energización,



La energización del relé de actuación final se produce cuando se han cerrado los contactos de al menos uno de los relés indicados A y C, y los contactos de al menos uno de los dos relés indicados B y D, por eso la lógica se llama "1-de-2-dos-veces". Dicha energización cierra unos contactos en el circuito de la bomba, que se muestra abajo totalmente simplificado a los efectos de este texto, y ello a su vez energiza la bobina de cierre (BC) del interruptor de la bomba, que recibiría así la energía eléctrica necesaria para producir el giro de su motor.





Este circuito final (que se considera que está fuera del sistema de protección, dado que éste terminaría, incluyéndolo, el relé final de actuación) muestra asimismo los contactos que cerrarían el interruptor si fuese el operador quien procediese al arranque manual de la bomba.

Existe también una bobina de apertura, y controles adicionales, y todo ello constituye el circuito de control de la bomba, que aunque no forma parte del sistema de protección del reactor, es un circuito relacionado con la seguridad.

La redundancia de la acción de seguridad se conseguiría por la actuación de otras bombas asignadas a la misma función, con circuitos lógicos idénticos.

## **5. Partes del sistema**

En lo que sigue se consideran sucesivamente las partes del sistema de protección antes mencionadas.

### **5.1 Nivel de detección**

El nivel de detección está constituido por el conjunto de sensores para vigilar las variables de la planta que son significativas para controlar la seguridad. Propiamente, el sensor es el elemento que se usa para percibir la magnitud de la variable, y dicho elemento puede, de por sí, aportar una señal eléctrica representativa del valor de la variable ó bien llevar anexo un componente que realiza dicha conversión, de variable física a variable eléctrica. Tanto en un caso como en el otro, recibe el nombre de transmisor, alusivo a que transmite el resultado de dicha conversión.

Un caso especial de dispositivo sensor son los llamados interruptores; en ellos no existe una conversión de valor físico de la variable en un valor correspondiente en señal eléctrica (esto es, no constituyen un transmisor), sino que cuando la variable ha alcanzado determinada magnitud se cierra, o se abre según el caso, un circuito dispuesto al efecto. A veces tienen nombres específicos, como los presostatos (interruptores de medida de presión) ó los termostatos (ídem para temperatura).

Al conjunto de medidores relativos a presión, nivel, temperatura y caudal se le alude normalmente como instrumentación de proceso.

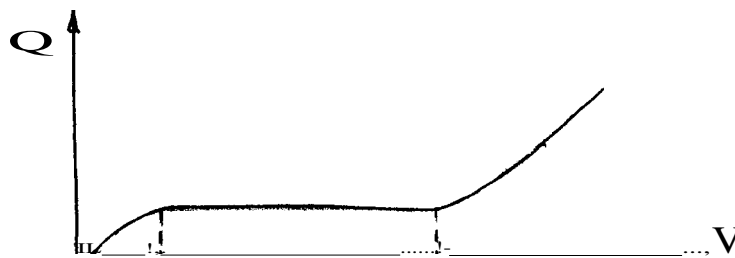
Los procedimientos de medida habituales de éstas variables, y tipos de transmisores representativos, se describen en el tema 24.

Además de las variables citadas, cabe destacar otras de naturaleza eléctrica (tensión, frecuencia,...), y otras dos específicas de los reactores, el flujo neutrónico y la radiación. A los sensores de éstas se les llama normalmente detectores.

La variable flujo neutrónico se usa fundamentalmente para la función de disparo del reactor. Al conjunto de detectores neutrónicos se le denomina sistema de instrumentación nuclear.

En los detectores neutrónicos se mide el grado de ionización producida por los neutrones del núcleo en cámaras, colocadas externamente ó internamente a dicho núcleo según los casos, y cuyo espacio interior tiene un revestimiento; en dicho material de revestimiento los neutrones provocan una reacción secundaria (generan partículas alfa ó beta, ó radiación gamma, que son las que ionizan); los neutrones por sí mismos, al no tener carga eléctrica, no pueden provocar ionizaciones.

El tamaño de los impulsos de ionización es función del voltaje aplicado a la cámara; si dicho tamaño lo representamos en el eje de abcisas de una gráfica en escala logarítmica como  $\log Q$  (logaritmo de la carga eléctrica), tendremos



Los llamados contadores proporcionales trabajan en la zona de la derecha de la gráfica, se suelen usar para el intervalo de fuente, en el que el flujo neutrónico es bajo; su cámara lleva revestimiento de  $B_3F$ .

En la zona de cámara de ionización, que es la parte plana de la gráfica, trabajan las cámaras de ionización no compensada, las cámaras de ionización compensada (ambas llevan boro en el material de revestimiento), y las cámaras de fisión (con revestimiento de material fisionable).

Para una descripción más extensa puede consultarse la referencia 4.

La variable radiación, a efectos del sistema de protección, se usa básicamente para la función de generar aislamiento de sistemas de ventilación.

En los detectores con gas de llenado, el fundamento es análogo a las de las cámaras neutrónicas, con la diferencia de que la ionización es producida directamente por la radiación (en los casos de partículas alfa ó partículas beta), ó bien, en caso de fotones gamma porque éstos interaccionan con el revestimiento de la cámara generando los electrones que provocan ionizaciones en el gas.

Aunque existen más tipos, aquí mencionamos los detectores de semiconductores, generalmente emplean silicio con determinadas impurezas, y se basan en detectar el movimiento de electrones (ó de huecos) generado por la acción de la radiación en materiales semiconductores.

La medida de la radiación se considera asimismo en la referencia 4.

## 5.2 **Sección analógica**

La sección analógica recibe señales, típicamente en el intervalo de 4 a 20 miliamperios, e incluye suministros de potencia, convertidores, indicadores, registradores, dispositivos de actuación de las alarmas, calculadores, controladores, biestables y otros componentes, cuya función conjunta es vigilar en continuo (esto es, en cada instante) los valores de las variables importantes para la seguridad y discernir, bien automáticamente ó por acción del operador, los casos en que tales valores han evolucionado hacia zonas de la operación que aconsejen ó requieran la acción de la protección.

En algunos documentos se considera que la sección analógica integra asimismo al nivel de detección, si bien a efectos de este texto ha parecido más ilustrativo considerarlo una parte separada.

La sección analógica está básicamente contenida en cabinas, también llamadas armarios (ó "racks"), en sala de control ó ubicaciones anexas. Cada cabina tiene una ó más fuentes de alimentación, de la que se obtiene alimentación, habitualmente de 24 voltios de corriente continua, para los transmisores. Los transmisores generan una señal de corriente de 4-20 mA que tiene una correspondencia biunívoca con el valor de la variable vigilada, señal que llega a las cabinas analógicas.

Las funciones que se realizan internamente a las cabinas son desarrolladas por tarjetas electrónicas.

La señal de corriente antes citada pasa por convertidores que la transforman, asimismo biunívocamente, de 4-20 mA a valores de tensión continua en el intervalo 0-10 voltios.

Los miliamperios tienen ventajas en cuanto a transmisión en distancias comparativamente largas, en tanto que los voltios presentan ventajas para manejo de señal en las cabinas.

Los indicadores aportan el valor instantáneo de la señal, en tanto que los registradores aportan una gráfica. Pueden estar en las propias cabinas, si bien la mayoría están en paneles de la sala de control; la salida de las señales de las cabinas analógicas, hacia paneles, es vía dispositivos que aíslan adecuadamente las salidas, a efectos de que fallos externos no tengan incidencia sobre las cabinas.

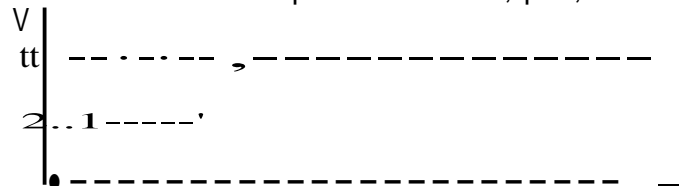
Hay salidas hacia alarmas, las cuales están igualmente en los paneles de sala de control. Existen asimismo salidas hacia ordenadores auxiliares.

Los calculadores ejecutan operaciones sobre la señal (p.e., extraer su raíz cuadrada).

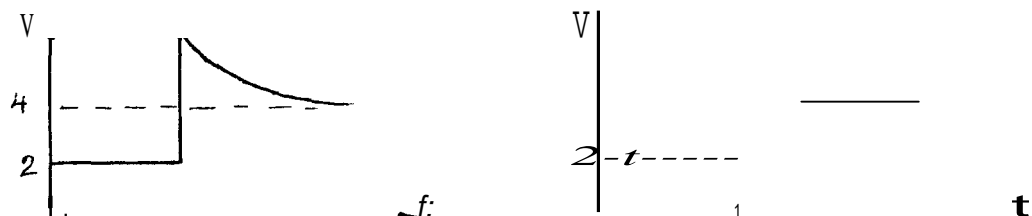
Los cálculos pueden ser de bastante mayor entidad, relacionados con la potencia térmica ó la salida de ebullición nucleada (DNB).

Un caso específico de interés, de calculadores, son los circuitos adelanto/retardo ("lead/lag") y derivada/retardo ("rate/lag"). Lo que hacen estos calculadores es, para una señal dada en la entrada, modificarla de una forma preestablecida, que es función del valor de unas constantes de tiempo ( $\tau_1, \tau_2$ ). La forma de respuesta depende de la de la señal de entrada, y a este efecto es de interés cómo responden estos calculadores ante variaciones en rampa y en escalón (para no extenderse demasiado, el texto que sigue considera solamente las variaciones en escalón).

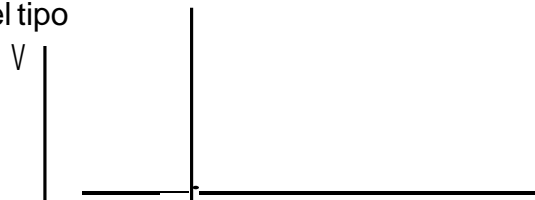
Sea una señal, procedente de un transmisor y ya convertida en voltios, que debido a una perturbación súbita en el proceso cambia, p.e., de 2 V a 4 V.



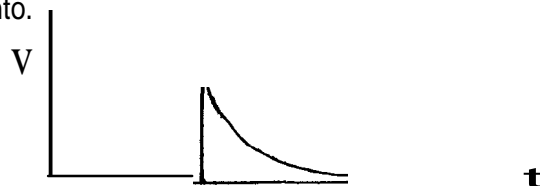
La respuesta del circuito adelanto/retardo es exagerar ó atenuar el escalón, y ello es función de valor relativo de las constantes  $\tau_1$  y  $\tau_2$ .



En cuanto al circuito derivada/retardo, el efecto derivada es obtener ésta en todos los puntos del gráfico de señal, con lo que tendríamos salida para el escalón anterior del tipo



que resulta poco manejable por lo que se consideran, en función de lo que se busque, los valores más adecuados de la constante de derivada ( $\tau_1$ ) y de retardo ( $\tau_2$ ) que hacen que el pico no sea muy alto y que su decaimiento sea más lento.



En cuanto a los controladores, ejecutan una acción sobre el proceso, a efectos de mantenerlo estable, y se basan en controlar adecuadamente un componente que lo regula (tal como una válvula); buscan mantener a una variable en un valor dado, pudiendo tener una acción proporcional, integral y/o derivativa, en función de cómo tratan la perturbación que ha podido tener lugar sobre la variable vigilada.

Los biestables ya han sido aludidos reiteradamente en este texto. Constituyen en el límite de la sección analógica, son la frontera con la parte lógica. En los diseños del suministrador Westinghouse están en las cabinas analógicas, en tanto que en los del suministrador Siemens están en las cabinas lógicas e incorporan un comparador entre los valores de tarado de los biestables redundantes, para aviso de posibles averías.

### 5.3 Sección lógica

La sección lógica está albergada en sus propias cabinas, si bien en otros diseños (en centrales BWR), dado que las señales de iniciación de sistemas se generan de manera individual para cada uno de los éstos, tanto las secciones analógica y lógica correspondientes a dicho sistema como sus relés del nivel de actuación pueden estar ubicados en una misma cabina, la asignada a ese sistema ú subsistema.

La sección lógica, en los diseños existentes, es fundamentalmente de tres tipos: lógica de estado sólido, lógica de relés, lógica dinámica.

La lógica de estado sólido constituye el "Solid State Protection System" (SSPS) en reactores de diseño Westinghouse, que se basa en la utilización de tarjetas electrónicas que combinan señales de presencia/ausencia de determinados niveles de tensión (48 V, 15 V), que cambian de estado cuando se dan determinados grados de coincidencia, en función de las entradas que reciben.

Las señales de salida de los biestables, junto con otras señales que llegan a través de los contactos de campo (tales como el disparo de turbina, las señales de baja tensión y baja frecuencia de bombas de refrigeración del reactor), y las procedentes de la instrumentación nuclear y de los monitores de radiación, proporcionan las entradas al citado SSPS.

Las cabinas SSPS se estructuran en dos trenes idénticos y redundantes (A y B) formados por 3 cabinas cada uno: cabina de relés de entrada, cabina lógica y cabina de relés de salida. Además existen otras cabinas adicionales, tales como las de multiplexado/demultiplexado para la transmisión de señales a sala de control y al computador de procesos.

Los relés de entrada a la sección lógica, en este diseño, son accionados por las salidas de los biestables de las señales de protección y están energizados cuando la variable se encuentra en condición segura. Ante condiciones de disparo o actuación de salvaguardias, o pérdida de suministro eléctrico, los biestables interrumpen el paso de corriente, desenergizando el relé, lo que provoca el cierre de sus contactos y el envío de señal al circuito lógico. El rociado de la contención constituye una excepción, energizándose los relés cuando existe una condición insegura, para evitar actuaciones espúreas.

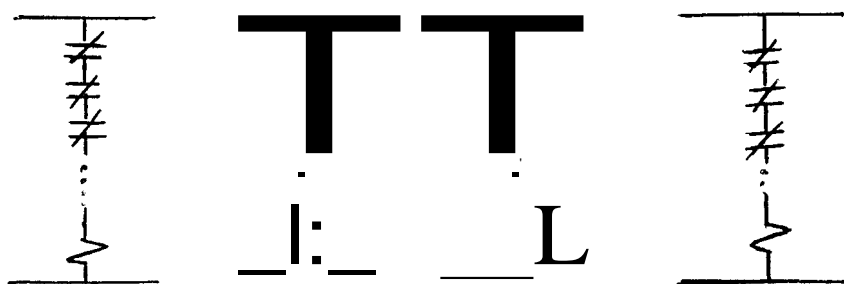
La cabina lógica recibe la señal de los relés de entrada y contiene una serie de tarjetas de procesamiento, entre las que destacan la tarjeta de lógica universal, la tarjeta de mínima tensión y las tarjetas de salvaguardias. La tarjeta de lógica universal contiene los circuitos de decisión de la lógica de coincidencia de

disparo de reactor y de actuación de salvaguardias tecnológicas, determinando la necesidad de estas actuaciones. La tarjeta de mínima tensión recibe la señal de disparo de reactor de la tarjeta de la lógica cuando es requerido, y esta tarjeta se encarga de cortar la alimentación eléctrica de las bobinas de los interruptores de disparo de reactor (con ello, las barras de control caen por efecto de la gravedad, insertándose en el núcleo y deteniendo la reacción nuclear). Las tarjetas de salvaguardia reciben la señal de inyección de seguridad cuando la tarjeta de la lógica determina la necesidad de actuación de salvaguardias, y se encargan entonces de controlar los relés de la cabina de salida. La cabina de relés de salida contiene los relés maestros y esclavos, que envían la señal para la actuación de los diversos equipos de salvaguardia (\*).

(\*) El tema 9 desarrolla más extensamente la información relativa al sistema SSPS de los reactores PWR.

En cuanto a la sección lógica de los reactores BWR, emplea extensivamente la lógica "1-de-2-dos-veces", a base de relés y contactos, lo que la hace más intuitiva. El esquema que, simplificado, suele repetirse en los sistemas de salvaguardas técnicas es semejante al que, en este texto, se ha incluido como ejemplo en el apartado 4, relativo a la actuación de un sistema de seguridad por bajo nivel de la vasija.

El disparo del reactor tiene un esquema algo diferente, basado en cuatro cadenas de contactos de relés, normalmente cerrados, que mantienen energizados unos relés finales de cadena (cada contacto sucesivo de la cadena corresponde a un criterio de disparo diferente, esto es, a una variable vigilada específica).



Cuando se excede el valor de tarado de una variable, abre el contacto a ella asignado en la cadena, y ello desenergiza el correspondiente relé final.

Los contactos de los relés finales se combinan en lógica "1-de-2-dos-veces", de modo que cuando se da el criterio de salida de la lógica, se desenergizan solenoides que, actuando sobre válvulas de un sistema hidráulico, dan origen a la inserción de las barras de control, que en el caso de los reactores BWR se realiza desde abajo, dadas las restricciones que impone disposición general de la vasija y sus componentes internos para que la inserción se pudiera producirse desde arriba por la acción de la gravedad.

En cuanto a los reactores del suministrador Siemens, la sección lógica utiliza una lógica dinámica, conocida como EDM, con electrónica de pulsos, que

realizan ciclos continuos de magnetización de núcleos magnéticos; cuando algún biestable cambia su salida hacia disparo, se produce una perturbación en la secuencia de magnetización, interrumpiendo el flujo de pulsos hacia la salida de las cabinas.

En la salida de las cabinas lógicas hay unos convertidores de pulsos a corriente continua, de modo que si se produce una perturbación en su entrada cambia el estado de su salida (de haber presencia de corriente continua pasa a haber ausencia, ó viceversa según los casos), generándose orden de actuación, bien del disparo del reactor, bien de otras funciones ó sistemas de seguridad.

El número de cabinas lógicas en estos reactores es bastante mayor, en torno a 30, debido a la segregación del sistema en dos zonas y al mayor número de automatismos y complejidad del sistema (dicha multiplicidad de cabinas es extensible a la sección analógica, si bien sus cabinas son más parecidas a las de los reactores de otros suministradores que las cabinas de la sección lógica).

## **6. Criterios**

La norma IEEE Std 279-1971, "IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations", aparece citada en el apartado 10.55a del 10CFR.50 de EE.UU.; en España ha constituido la norma básica para la evaluación del sistema de protección, y a efectos de este texto aporta una adecuada referencia para la exposición de los criterios aplicables al sistema.

Expone las bases de diseño y los requerimientos, ó requisitos.

Por "bases de diseño" se entiende la información que identifica las funciones que ha de realizar una estructura, sistema ó componente (en nuestro caso, un sistema), y los valores, ó rangos de valores, elegidos para controlar los parámetros considerados como límites para el diseño. Tales valores pueden provenir de prácticas generalmente aceptadas y demostradas como válidas, o haber sido deducidos de la evaluación de análisis ó calculos de la evolución de los transitorios operativos ó de los accidentes postulados.

Al respecto, se habrán de documentar los aspectos siguientes:

- Las condiciones de la planta que requieren actuación del sistema.
- Las variables que se requiere vigilar para controlar tales condiciones de la planta. Típicamente, la mayor parte son presiones, niveles, temperaturas y/o caudales en diversas localizaciones, además del flujo neutrónico, variable importante en el sistema de disparo del reactor.
- El número mínimo, y localización, de los sensores que vigilan las variables que pueden tener dependencia espacial. Como ejemplo, sería el caso de la vigilancia de la temperatura en una tubería en la que puedan darse condiciones de estratificación.
- Los límites operativos aconsejables para cada variable.

- El margen entre cada límite operativo y el valor que establece el comienzo de las condiciones no seguras.
- Los valores que, cuando se alcanzan, requieren actuación del sistema de protección. A estos valores se les llama habitualmente puntos de tarado, como ya se ha mencionado.
- El rango de valores, para condiciones transitorias, y estacionarias, del suministro de energía (p.e., voltaje, frecuencia) al sistema y de las condiciones ambientales (p.e., temperatura, presión, humedad, vibraciones), tanto en situación normal, transitoria ó accidental, en las que el sistema debe funcionar.
- Las malfunciones, accidentes, u otros sucesos inusuales (p.e., incendios, misiles, inundaciones, sismos) que podrían dañar componentes del sistema ó causar cambios ambientales degradatorios, y para los cuales el diseño ha de incorporar previsiones para mantener su capacidad funcional.
- Los requisitos de funcionamiento mínimos incluyendo lo siguiente:
  - a) Tiempos de respuesta.
  - b) Precisión.
  - e) Rangos de medida para las diferentes condiciones.

En cuanto a los requerimientos, o requisitos, establecen los principios básicos que caracterizan el diseño que ha tener el sistema de protección; varios de ellos ya han aparecido aludidos en apartados anteriores. Son los que aparecen en el texto que sigue, para algunos de ellos se incluye un comentario explicativo, ó aclaratorio de cómo de han aplicado en las centrales.

### 1. Requisito funcional general.

El sistema de protección habrá de actuar automáticamente, iniciando sus actuaciones protectoras cuando las condiciones vigiladas alcancen un nivel preestablecido; típicamente, ello ocurrirá cuando las variables alcancen sus valores de tarado.

### 2. Criterio de fallo único.

No han de existir fallos únicos que, por sí solos, eviten la acción protectora del sistema cuando se la requiera.

Ello lleva a implantar el concepto de redundancia, de modo que una misma función sea realizada por dos ó más subsistemas ó componentes, con lo que el fallo de uno de ellos no evita que se lleve a cabo la función de protección.

### 3. Calidad de componentes y módulos.



Se requiere una calidad que lleve a requerimientos de mantenimiento mínimos, y bajas tasas de fallo; se conseguirán los niveles de calidad mediante la especificación de requerimientos de diseño, sobredimensionado, fabricación, control de calidad, inspección, etc.

#### 4. Cualificación del equipo.

Será vía pruebas de prototipo, ó vía extrapolación adecuadamente fundamentada de datos de otras pruebas, de modo que se verifique que se cumplen, y se mantienen, los requisitos de funcionamiento en las condiciones adversas postuladas.

Típicamente habrán de demostrarse los requisitos de cualificación ambiental y sísmica.

#### 5. Integridad de canal.

Habrá de mantenerse la capacidad funcional frente a las condiciones adversas postuladas ó ante problemas en suministro de energía u otras malfunciones, para todos los canales del sistema de protección.

Por canal se entiende el conjunto de componentes y módulos que, desde el medidor de una variable dada, generan una señal de protección (salida del dispositivo biestable). El concepto aplica a la parte analógica, pues en la parte lógica, donde se establecen las coincidencias para actuación, los canales pierden su individualidad.

#### 6. Independencia de canal.

Los canales que suministran señales para una misma acción protectora habrán de ser independientes y estar separados físicamente de modo que se evite la incidencia simultánea, en varios canales, de los efectos ambientales, transitorios eléctricos y consecuencias de accidentes, reduciendo así igualmente la probabilidad de interacciones entre canales durante operaciones de mantenimiento ó en caso de la malfunción de un canal.

#### 7. Interacciones entre control y protección.

Hay sistemas de instrumentación que tienen funciones de seguridad (tal como el sistema de protección), y sistemas que no tienen funciones de seguridad (de los que se habla genéricamente como de control).

La instrumentación que se use a la vez para protección y para control será considerada que forma parte del sistema de protección y habrá de cumplir los requerimientos de la norma IEEE.

Asimismo, y cuando salen señales desde equipos del sistema de protección para uso en sistemas de control, dicha salida habrá de ser vía dispositivos de aislamiento que serán considerados que forman parte del sistema de

protección y que por tanto habrán de cumplir los requerimientos de la norma IEEE. Con ello, los fallos tras la salida de los dispositivos de aislamiento, esto es, en la parte de control, no repercutirán aguas arriba de éste, o sea, en la parte de protección. Tales fallos podrían ser cortocircuitos, circuitos abiertos, tierras, ó aplicación de las tensiones creíbles, de c.a. ó de c.c.

#### 8. Generación de las entradas hacia el sistema de protección.

Las entradas al sistema, hasta donde sea práctico y factible, serán procedentes de la medida directa de las variables deseadas.

En algunos casos, no obstante y al ser variables no medibles directamente, se incorporan circuitos de cálculo.

#### 9. Capacidad para verificar los sensores.

Habrà de disponerse de medios para verificar, con un alto grado de confianza, la disponibilidad operativa de los sensores durante la operación a potencia.

Ello puede realizarse de varias maneras, tales como:

- a) perturbando la variable monitorizada,
- b) sustituyendo la entrada al sensor por una entrada equivalente, esto es, de la misma naturaleza que la variable medida, ó
- e) por chequeo comparativo de las indicaciones que vigilan una misma variable, ó de las que guardan entre sí una relación conocida.

Básicamente, el método más utilizado a potencia es el de chequeo, conocido normalmente como chequeo de canal.

#### 10. Capacidad para prueba y calibración.

Se habrá de tener capacidad de prueba y de calibración, desde los sensores antes citados hasta las señales de salida de los elementos finales.

El término prueba, si se contrapone a calibración, se refiere a una "prueba funcional", orientada a verificar actuaciones; en tanto que la calibración busca verificar los puntos de tarado, y otros ajustes. Aunque, lógicamente, la calibración no es sino un tipo de prueba.

Para aquellas partes del sistema cuyo intervalo entre pruebas es más corto que el intervalo normal entre paradas de recarga, se requerirá que exista capacidad de prueba durante la operación a potencia.

Habitualmente, las pruebas del sistema de protección se realizan por tramos, y la funcionalidad del conjunto se garantiza porque en las interfases entre tramos existe solape, esto es, el componente final que se verifica en un tramo es también verificado, como elemento inicial, en la prueba del tramo siguiente.

## 11. Bypass (derivación) de canal ó retirada de operación.

El diseño permitirá que un canal pueda estar en mantenimiento y que, cuando se lo requiera, pueda ser probado ó calibrado durante la operación a potencia, sin que ello dé origen a la iniciación de una actuación del sistema. Durante tales períodos se habrá de cumplir el criterio de fallo único.

Ello implica que, por ejemplo, en un caso de canales con configuración lógica "2-de-3", los mantenimientos ó pruebas se realicen colocando el canal en condición de disparado (actuado). De no hacerlo así, el canal estaría indisponible y la lógica "2-de-3" se habría convertido en una lógica "2-de-2", con lo que no se cumpliría el criterio de fallo único.

## 12. Bypasses (derivaciones) operativos.

Existen casos en que ciertos circuitos de actuación sólo precisan estar activos en determinadas condiciones de la planta. Por ello, pueden ser bloqueados por los operadores de sala de control, si bien, en caso de que cambien las condiciones de la planta, el bloqueo ha de eliminarse automáticamente.

Tal es el caso, ya aludido, de un sistema de emergencia que actúe por baja presión de las tuberías del sistema primario, que ha de actuar si la bajada de presión es consecuencia de un accidente, pero no cuando la bajada de presión es debida a que el reactor está llevando a cabo su secuencia de parada normal; en este caso el operador ha de bloquear (impedir la actuación) del sistema de emergencia. Pero si desaparecen las condiciones que permitían el bloqueo, por ejemplo, si el reactor retorna a operación a potencia, el bloqueo se eliminará automáticamente, esto es, sin la acción del operador.

### 13. Indicación de bypasses (derivaciones)

Cuando algún canal se haya colocado en bypass, ello habrá de aparecer indicado, de forma continua mientras esté en dicha condición, en la sala de control.

## 14. Acceso a los dispositivos de bypass.

Existirán previsiones para controlar la utilización de los dispositivos de bypass, y así garantizar el adecuado control sobre el conjunto del sistema.

## 15. Puntos de tarado múltiples.

El diseño puede incluir que sea preciso cambiar el valor de tarado a otro más restrictivo, si ha cambiado el modo de operación de la planta y el nuevo estado requiere una protección más restrictiva, esto es, que la actuación de la seguridad, de ser requerida, tenga que adelantarse.

Un ejemplo sería el caso de un reactor que, en lugar de operar con los tres lazos de refrigeración, pudiese operar con dos en caso de inoperabilidad de la bomba primaria de ese lazo. Los dispositivos previstos, en estas situaciones, para evitar el uso de tarados inadecuados forman parte del sistema de protección.

#### 16. Finalización de la acción protectora, una vez iniciada.

El criterio considera que, una vez iniciada la acción protectora, ha de completarse, de modo que se alcance una condición segura, o adecuadamente mitigada. El retorno a operación requerirá una acción deliberada del operador.

El diseño, al respecto, permite que para la mayoría de los sistemas de salvaguardias tecnológicas, y con determinados condicionantes (p.e., que haya ocurrido el disparo del reactor, que haya pasado cierto tiempo, ...) el operador pueda proceder a eliminar la orden de actuación automática (lo que no incide en que los sistemas sigan actuando), pero que facilita que puedan ser controlados en manual.

Ello posibilita, p.e., que se pueda detener la actuación de un sistema de inyección de agua a la vasija ó a un tanque si existe peligro de rebose.

#### 17. Iniciación Manual.

El diseño habrá de incluir mandos para la actuación a nivel de cada sistema (p.e, pulsadores ó manetas para el disparo del reactor, idem para el aislamiento de la contención, idem para la inyección de seguridad,...).

Habrà de cumplir el fallo único (ello lleva a la duplicidad de los mandos), y depender de un número mínimo de equipos (esto es, los circuitos de actuación manual habrán de ser simples).

#### 18. Acceso a los ajustes y puntos de prueba.

Habrà de existir un control para acceder a los medios de ajuste de los valores de tarado y otros valores de la calibración, y sobre los puntos de inyección de señales simuladas para las pruebas.

Ello permite el adecuado control sobre la configuración del sistema.

#### 19. Identificación de acciones protectoras.

El diseño permitirá conocer qué acciones protectoras han tenido lugar, no solamente a nivel de sistema, sino de cada canal.

#### 20. Información de monitorización.

Habrà de existir, a disposición de los operadores de sala de control, una información precisa, completa y continua sobre el estado del sistema de

protección, de modo que se tenga conocimiento de cualquier problema ó indisponibilidad.

Se evitará la evolución de situaciones que, pudiendo afectar a medidores, registradores, alarmas,.... lleven a indicaciones que resulten confusas para los operadores.

## 21. Reparaciones.

El diseño habrá de facilitar la localización de posibles averías, y los trabajos de reparación ó sustitución de componentes.

### 22.1 identificación.

Todos los equipos que forman parte del sistema de protección habrán de estar identificados. Los criterios de identificación serán tales que habrán de permitir distinguir claramente a qué redundancia pertenecen tanto los componentes y módulos como los cables de las interconexiones.

En cuanto a los reactores de diseño alemán, la norma más importante relativa al sistema de protección es la KTA 3501, "Reactor Protection System and Monitoring Equipment of the Safety System".

Esta norma incluye un apartado relativo a las funciones del sistema, seguido de otro que detalla los principios del diseño, de desarrollo similar al de requerimientos de la IEEE, añadiendo diversas figuras aclaratorias; le sigue otro apartado, asimismo relativo al diseño, que aparte de criterios adicionales incluye diversos aspectos descriptivos. Finalmente, alude a los sistemas soporte (ventilación, suministro eléctrico) y a las alarmas.

## Referencias

1. Estudio Final de Seguridad de C.N. Aseó.
2. Estudio Final de Seguridad de C.N. Cofrentes.
3. Estudio Final de Seguridad de C.N. Trillo.
4. "Instrumentación Nuclear", de Agustín Tanarro. Madrid, 1979.
5. IEEE Std 279-1971, "IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations".
6. KTA 3501, "Reactor Protection System and Monitoring Equipment of the Safety System".