

Tercer Ejercicio. Seguridad Nuclear

Tema 3.A.17

Sistemas de instrumentación y control relacionados con la seguridad de las centrales nucleares. Utilización de tecnología analógica y digital.

INDICE

- 1. INTRODUCCIÓN**
- 2. SISTEMAS DE INSTRUMENTACIÓN Y CONTROL RELACIONADOS CON LA SEGURIDAD DE LAS CENTRALES NUCLEARES**
- 3. SISTEMA DE PROTECCIÓN DEL REACTOR**
- 4. SISTEMA DE INSTRUMENTACIÓN POST-ACCIDENTE**
- 5. OTROS SISTEMAS DE CONTROL RELEVANTES**
- 6. UTILIZACIÓN DE TECNOLOGÍA ANALÓGICA Y DIGITAL**
- 7. REFERENCIAS NORMATIVAS PARA SISTEMAS DE INSTRUMENTACIÓN Y CONTROL**

Resumen Ejecutivo:

La finalidad primordial de los sistemas de instrumentación y control de una central nuclear es proporcionar actuación automática y ejercer el adecuado control en el caso de un funcionamiento del reactor inseguro e inadecuado durante operaciones a régimen estacionario y en transitorios de potencia, así como proveer señales de iniciación de actuación de sistemas para mitigar las consecuencias de condiciones de accidentes. La variedad de sistemas de instrumentación y control existentes en una planta es extensa, cabiendo una primera categorización entre sistemas de seguridad y sistemas de no seguridad, y otras categorizaciones derivadas de su funcionalidad (monitorización, control, mitigación).

A lo largo del presente tema se aporta una exposición al respecto de los sistemas de instrumentación y control presentes en el diseño de una central nuclear, su funcionalidad prevista, y una descripción básica de algunos de ellos (sistema de protección del reactor, sistemas de salvaguardias tecnológicas, sistemas de instrumentación neutrónica, sistemas de vigilancia post-accidente y ejemplos de sistemas de control relevantes). En el capítulo 6 del tema se aportan algunas ideas y conceptos básicos en relación con la creciente utilización de tecnología digital frente a la tecnología analógica convencional en los instrumentos, haciendo mención a los nuevos retos y diferencias inherentes a esta nueva tecnología en cuanto a su licenciamiento en contraste con la instrumentación convencional.

Temas relacionados:

“Métodos de medida de presión, temperatura, nivel y caudal. Clasificación y descripción de instrumentación de medición”.

“El sistema de protección del reactor en centrales nucleares”.

TEMA 3.A.16. SISTEMAS DE INSTRUMENTACIÓN Y CONTROL RELACIONADOS CON LA SEGURIDAD DE LAS CENTRALES NUCLEARES. UTILIZACIÓN DE TECNOLOGÍA ANALÓGICA Y DIGITAL

1. INTRODUCCIÓN

Los sistemas de instrumentación y control (sistemas IyC) de las centrales nucleares son utilizados para la realización de funciones de monitorización, control y protección, pudiendo categorizarse en sistemas de Seguridad y sistemas de No Seguridad.

Los sistemas IyC de No Seguridad son utilizados por los operadores para monitorizar y controlar la operación normal de la planta, incluyendo el arranque y la parada, y para mitigar y prevenir transitorios operacionales. Estos sistemas de No Seguridad están apoyados por un conjunto de sistemas de Seguridad, independientes y redundantes, que están diseñados para prevenir y mitigar condiciones de accidente si los operadores y los sistemas de No Seguridad fallan a mantener la planta en las condiciones normales de operación. Estas dos categorías de sistemas, Seguridad y No Seguridad, están pensadas de manera consistente con el concepto de Defensa en Profundidad aplicada a la seguridad. En este sentido, aunque no de manera absoluta, los sistemas de No Seguridad coinciden con los sistemas de monitorización y control y los sistemas de Seguridad con los sistemas de protección.

En base a las funciones citadas, e independientemente de que se trate de tecnología analógica o digital, los sistemas IyC se agrupan, en términos generales, en tres tipos:

- a) *sistemas de monitorización y display* - monitorizan variables de planta y proporcionan datos a otros sistemas y a los operadores para su uso en el control de la operación de la planta. Estos sistemas normalmente también aportan alarmas visuales y sonoras a varias estaciones de control, principalmente la Sala de Control, que notifica al operador de tendencias o valores particulares que requieren la acción del operador para evitar un problema real o una emergencia.
- b) *sistemas de control* - se usan para controlar todas las operaciones normales de la planta, esto es, situaciones de arranque, operación a potencia, parada y transitorios de la planta.
- c) *sistemas de mitigación y protección* - se ubican en un nivel adicional y distinto de los sistemas que monitorizan y controlan las variables de la planta. Estos sistemas se diseñan para detectar situaciones en las que los sistemas de control automático no han sido capaces de mantener la planta en un conjunto de condiciones predefinidas, procediendo a disparar la planta de manera automática, y a arrancar los sistemas necesarios para la mitigación del problema detectado y llevar la planta a una situación segura.

El diseño de centrales KWU-Siemens (como es el caso de CN Trillo) contempla un escalón adicional, constituido por el Sistema de Limitación, que si bien no es de Seguridad está sometido a importantes requisitos de diseño, y cuya actuación se ubica entre las actuaciones de los sistemas de control y de protección con el fin de adelantarse, en caso de perturbaciones en la planta, a las medidas a tomar por el sistema de protección del reactor.

La evaluación de la seguridad de las centrales nucleares está dirigida en primer término hacia los sistemas de mitigación y protección, los cuales están sujetos a los más rigurosos controles reguladores y de licenciamiento, requiriendo un sustancial esfuerzo para el diseño, cualificación, instalación, prueba y mantenimiento. En los análisis de seguridad y de riesgo de las plantas usualmente no se da crédito a los sistemas de control, automático o manual. No obstante, transitorios o fallos en los sistemas de control son considerados con frecuencia sucesos iniciadores para los sistemas de mitigación y protección, y como resultado, pueden asimismo en ocasiones verse sometidos a requerimientos específicos, y contemplados en los análisis para la evaluación del cumplimiento de la planta con los objetivos de seguridad fijados.

El diseño de las plantas nucleares contempla la consideración de una variedad de condiciones de operación. Condiciones en régimen permanente, en transitorios o en accidente son cubiertas por los requerimientos reguladores, los cuales también controlan cómo y en base a qué criterios los transitorios y accidentes deben ser analizados. Estos análisis, por otra parte, especifican los requerimientos operacionales que los equipos y sistemas de la planta deben satisfacer. Para los sistemas IyC estas especificaciones incluyen tanto características del instrumento (tales como rangos de entrada y salida, tiempo de respuesta y precisión) como condiciones ambientales (por ejemplo, temperatura, humedad, efectos de radiación, fluctuaciones de la alimentación eléctrica) bajo las cuales los equipos de IyC son requeridos a operar.

2. SISTEMAS DE INSTRUMENTACIÓN Y CONTROL RELACIONADOS CON LA SEGURIDAD EN CENTRALES NUCLEARES

Tal y como se expone en el criterio general de diseño GDC-13 "Instrumentation and Control" del Apéndice A al 10CFR50 (Título 10 del Code of Federal Regulations, U.S.A.), el diseño de las centrales nucleares ha de contemplar la apropiada instrumentación para la monitorización de variables y de sistemas en los rangos previstos para la operación normal, transitorios operacionales anticipados y condiciones de accidente, de manera que se asegure la adecuada seguridad, incluyendo aquellas variables y sistemas que pueden afectar al proceso de fisión, la integridad del núcleo del reactor, la barrera de presión del refrigerante del reactor y la contención y sus sistemas asociados. Asimismo, deberán proporcionarse los adecuados controles para mantener variables y sistemas dentro de los rangos de operación previstos.

De acuerdo con lo anterior, la finalidad primordial de los sistemas IyC de una central nuclear es proporcionar actuación automática y ejercer el adecuado control ante un funcionamiento del reactor inseguro e inadecuado durante operaciones a régimen estacionario y en transitorios de potencia, así como proveer señales de iniciación de actuación de sistemas para mitigar las consecuencias de condiciones de accidente. En este sentido, los sistemas de IyC están diseñados para proporcionar protección automática contra funcionamientos anormales y peligrosos del reactor en estado estacionario y durante transitorios de potencia durante las condiciones de operación I, II y III, tal y como se definen en el capítulo 15 del Estudio Final de Seguridad (EFS) de las centrales, así como proporcionan señales iniciadoras de actuación de sistemas para mitigar las consecuencias de situaciones defectuosas

como las incluidas en la condición IV. Entre las perturbaciones que es necesario mantener bajo vigilancia y ejercer el adecuado control se pueden señalar, sin carácter exclusivo:

- a) perturbaciones asociadas a la operación normal, tales como: acumulación y quemado de venenos de fisión, quemado del combustible, excursiones de reactividad.
- b) transitorios operativos previstos, tales como: rechazo completo de carga, parada de emergencia por superación de límites, pérdida de suministro eléctrico.
- c) situaciones de accidente, tales como un accidente con pérdida de refrigerante.

Para llevar a cabo su función, los sistemas IyC de una central nuclear se diseñan para ejercer la vigilancia de diversas variables (presión, temperatura, nivel, caudal, actividad, flujo neutrónico, exposición, etc..) y del estado de los sistemas de la planta, al objeto de identificar las condiciones de operación de la misma, mantener estas condiciones de operación dentro de los rangos previstos, y proporcionar actuación automática cuando se produce una desviación con respecto a las condiciones operativas normales.

Para proporcionar esta funcionalidad, los sistemas IyC incorporados en el diseño de una central nuclear son numerosos y diversos. En una primera aproximación, los sistemas IyC pueden clasificarse, según su función, en sistemas asociados a la generación de energía (No Seguridad) y sistemas de Seguridad. Otra posible clasificación es la contemplada en la Guía Reguladora (RG) 1.70 “Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants” de la USNRC (Nuclear Regulatory Commission), que se corresponde con el tratamiento dado a estos sistemas en la Sección 7 del NUREG-0800 “Standard Review Plan”, según la cual los sistemas IyC se pueden encuadrar en:

- Ø sistemas de disparo del reactor; son aquellos sistemas que inician la inserción rápida de barras de control para mitigar las consecuencias de accidentes base de diseño. El sistema de disparo del reactor y los sistemas de actuación de salvaguardias tecnológicas constituyen los sistemas de protección de la central.
- Ø sistemas de actuación de salvaguardias tecnológicas; son aquellos sistemas que inician y controlan los equipos de seguridad que se encargan de la extracción de calor del reactor o de participar en el mantenimiento de las barreras físicas contra emisiones radiactivas.
- Ø sistemas de parada segura; son aquellos sistemas cuya función es alcanzar y mantener una condición de parada segura en la planta. Incluyen los sistemas de control de reactividad usados para mantener el núcleo del reactor en una condición subcrítica y los sistemas de extracción de calor residual, encargados de proporcionar la adecuada refrigeración para alcanzar y mantener condiciones de parada segura. La configuración específica de estos sistemas depende del tipo de planta (PWR, BWR), las características de diseño específicas de la planta, y las condiciones bajo las cuales la parada segura ha de ser alcanzada y mantenida (parada caliente, parada fría).

Ejemplos típicos de sistemas requeridos para la parada segura son: sistemas de agua de alimentación auxiliar, sistemas de extracción de calor residual, y sistemas de parada segura fuera de Sala de Control (panel de parada remota).

- Ø sistemas de información importantes para la seguridad; son aquellos sistemas que proporcionan información a los operadores de planta para: (1) la evaluación de las condiciones de planta, del comportamiento de sistemas de seguridad y de la toma de decisiones relativa a la respuesta de la planta ante eventos anormales, y (2) la toma de acciones manuales del operador preplaneadas para la mitigación de accidentes. Estos sistemas de información también proporcionan la necesaria información para la toma de las acciones oportunas para mitigar las consecuencias de transitorios operacionales previstos.

Ejemplos de estos sistemas incluyen: sistemas de monitorización post-accidente, indicación de estado inoperable o de bypass de sistemas de seguridad, sistemas de anunciadores (alarmas) de planta, sistema de display de parámetros de seguridad, sistemas de información asociados a instalaciones de respuesta de emergencia.

- Ø sistemas de enclavamientos importantes para la seguridad; son aquellos sistemas que operan para reducir la probabilidad de ocurrencia de eventos específicos o de mantener sistemas de seguridad en un estado que asegure su disponibilidad en un accidente.

Estos sistemas incluyen: enclavamientos para prevenir la sobrepresurización de sistemas de baja presión (por ejemplo, extracción de calor residual) cuando se conectan a sistemas de alta presión (por ejemplo, refrigerante del primario), enclavamientos para prevenir la sobrepresión del sistema de refrigerante primario durante operaciones de baja temperatura de la vasija del reactor, enclavamientos de válvulas para asegurar la disponibilidad de los acumuladores del sistema de refrigeración de emergencia, enclavamientos para aislar los sistemas de seguridad desde sistemas de no seguridad, y enclavamientos para prevenir interconexiones inadvertidas entre sistemas de seguridad diversos o redundantes cuando esas interconexiones pueden existir por motivos de prueba o mantenimiento.

- Ø sistemas de control; en este grupo se incluyen aquellos sistemas usados para la operación normal, a los que no se les da crédito ante accidentes, pero que controlan procesos de la planta que tienen un impacto significativo en la seguridad de la planta. La lista de este tipo de sistemas y funciones de control es específica del diseño de cada planta. Estos sistemas han de ser diseñados de manera que las variables controladas puedan ser mantenidas dentro de los rangos de operación establecidos, y que los efectos de la operación o fallo de estos sistemas estén englobados por los análisis de accidentes del capítulo 15 del EFS.

En la respuesta transitoria de la planta ante cambios normales de carga y transitorios operacionales anticipados, tales como disparo de reactor o disparo de turbina, los sistemas de control son capaces de mantener las variables del sistema dentro de los límites de operación previstos. Las características de control manual y automático facilitan la capacidad para realizar esta función.

Los sistemas de control permiten la toma de acciones para operar la planta de manera segura durante operación normal, incluyendo transitorios operacionales previstos o anticipados, cumpliendo el GDC 19 “Control Room” del Apéndice A al 10CFR50 al respecto de operaciones normales de planta. Los sistemas de control están apropiadamente aislados de los sistemas de seguridad.

Algunos ejemplos típicos de sistemas de control son los siguientes:

Instrumentación de posición de barras

Sistemas de monitorización neutrónica

Sistema de control de caudal de recirculación (BWR)

Sistema de control del turbogenerador y regulador de presión (BWR)

Sistema de control de agua de alimentación

Sistema de computador de proceso

Sistema de control de reactividad (PWR)

Sistema de control de boro (PWR)

Sistema de control de nivel y presión del presionador (PWR)

Sistema de control de nivel de agua en generadores de vapor (PWR)

Otros sistemas de control típicamente incluidos en las otras categorías, pudiendo incluso estar relacionados con la seguridad en algunos casos, son:

Controles del sistema de refrigeración del pozo seco / contención

Controles de calefacción, ventilación, y aire acondicionado

Controles del sistema de purificación de agua del reactor

Controles del sistema de agua de servicios

Controles del sistema de aire de instrumentos

Controles del sistema de protección contra incendios

Control de sistemas de residuos radiactivos (gaseosos, líquidos, sólidos)

- Ø sistemas IyC diversos; son aquellos sistemas expresamente incorporados como respaldo diverso del sistema de protección del reactor y los sistemas de actuación de salvaguardias tecnológicas. Un caso típico es el ATWS, sistema de mitigación de transitorios anticipados sin SCRAM (inserción de barras).
- Ø sistemas de comunicación de datos; son aquellos sistemas que se encargan de la transmisión de señales entre sistemas y entre componentes de sistemas.
- Ø sistemas auxiliares soporte esenciales; son aquellos sistemas que son requeridos para que los sistemas IyC importantes para la seguridad puedan llevar a cabo su función.

Ejemplos típicos son los sistemas de ventilación, calefacción y aire acondicionado, los sistemas de suministro de potencia eléctrica, y los sistemas de agua de refrigeración.

Los sistemas IyC relacionados con la seguridad de una instalación nuclear se diseñan para prevenir y mitigar condiciones de accidente si los operadores y los sistemas de No Seguridad fallan a mantener la planta en las condiciones normales de operación. Tal y como se ha mencionado anteriormente, la evaluación de la seguridad de las centrales nucleares está dirigida primariamente hacia estos sistemas de mitigación y protección, los cuales están sujetos a los más rigurosos controles reguladores y de licenciamiento, requiriendo un sustancial esfuerzo para el diseño, cualificación, instalación, prueba y mantenimiento.

La principal referencia normativa aplicable a los sistemas de instrumentación y control relacionados con la seguridad aparece indicada en el Apéndice A del 10 CFR50, que en su apartado 50.55a(h) específicamente expone que los sistemas de protección de centrales nucleares construidas posteriormente al 1 de enero de 1971 han de cumplir con los requisitos especificados en la norma IEEE Std. 279, "Criteria for Protection Systems for Nuclear Power Generating Stations," o en la norma IEEE Std. 603 "Criteria for Safety Systems for Nuclear Power Generating Stations", que la actualiza y mejora.

Estos documentos constituyen la norma básica de aplicación a los sistemas IyC de Seguridad, y en ellos se definen los criterios básicos que ha de contemplar el diseño de estos sistemas, de los que, entre otros, se podrían citar los siguientes (indicándose entre paréntesis algunas guías reguladoras y documentos de la industria que desarrollan la aplicación de los criterios):

Criterio de fallo simple (RG 1.53, ANSI/IEEE Std 379)

Criterio de completar la acción protectora

Criterios de requisitos de calidad de componentes y módulos

Criterios de requisitos de cualificación de los equipos

Criterios de integridad de canal

Criterios para la interacción de sistemas de control y de protección

Criterios de independencia (RG 1.75 y la IEEE Std. 384)

Criterios de capacidad prueba y calibración (RG 1.22, RG 1.118, IEEE Std. 338)

Criterios de control automático

Criterios de actuación manual (RG 1.62)

Criterios de bypass de canal y de indicación de bypass (RG 1.47)

Criterios de la alimentación eléctrica

De acuerdo con lo establecido en tales normas, los sistemas IyC relacionados con la seguridad presentan, entre otras, una serie de importantes características, tales como:

- son físicamente independientes, de manera que generalmente no comparten software ni hardware con los sistemas de control y operación de la planta.
- están cualificados ambientalmente para las condiciones severas de accidente u operación.
- cuando se demanda su actuación ejecutan completamente la función para la que han sido diseñados.

- generalmente son sistemas de iniciación de actuación de equipos, normalmente no controlando o modulando la operación de los sistemas sobre los que actúan.
- están diseñados para cumplir el criterio de fallo único. Se diseñan con redundancia, de manera que ningún fallo simple impedirá las drásticas acciones tomadas por estos sistemas. Asimismo, permite la prueba completa de un canal con la planta en operación, sin causar o inhibir la función de mitigación y protección.
- adicionalmente a cumplir el criterio de fallo único, estos sistemas tienen otras características que incrementan su fiabilidad y efectividad, como por ejemplo el uso de dos o más señales de iniciación diferentes para cualquier accidente dado. Este tipo de redundancia proporciona protección contra fallos en modo común.

Dada la imposibilidad de tratar en este tema con cierto detalle muchos de estos sistemas IyC, se opta por aportar a continuación, y en la medida de lo posible, algunos conceptos básicos al respecto de algunos de los sistemas IyC importantes para la seguridad más significativos, más concretamente, el sistema de protección del reactor y la instrumentación post-accidente, así como una breve información al respecto de otros sistemas de control que, si bien no relacionados con la seguridad, son relevantes en la correcta operación de la planta.

3. SISTEMA DE PROTECCIÓN DEL REACTOR

Los sistemas de protección son aquellos sistemas IyC encargados de la iniciación de las oportunas actuaciones de seguridad para mitigar las consecuencias de accidentes base de diseño. Tal y como se refleja en el GDC 20 "Funciones del Sistema de Protección" del Apéndice A del 10CFR50, el sistema de protección del reactor (SPR) 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 aceptables especificados para el combustible no son excedidos como consecuencia de transitorios operacionales anticipados o 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 público (esto es, las vainas del combustible, la barrera de presión del refrigerante y la integridad del recinto de contención), en base a garantizar que no se exceden los límites o criterios establecidos para el CIEN (coeficiente del límite de ebullición nucleada), la densidad de potencia, los daños a vainas de combustible, y la liberación de material radiactivo, ante 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 ordenes necesarias para producir las acciones de protección previstas, que en general se engloban en dos: disparo 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. En base a esta doble funcionalidad se pueden distinguir dos grandes bloques que constituyen el sistema de protección:

- § el sistema de disparo del reactor (SDR), que aporta la función de disparo. El SDR se diseña para limitar las consecuencias de los sucesos de condición II mediante la parada del reactor y la limitación de inserción de reactividad.
- § el sistema de actuación de las salvaguardias tecnológicas (ESFAS), que es el encargado de proporcionar la función de actuación de equipos y sistemas. El sistema ESFAS se diseña para limitar las consecuencias de los sucesos de condición III y IV actuando los sistemas de evacuación de calor, aislando el recinto de contención e iniciando el rociado de contención cuando proceda.

Algunas de las características más relevantes del diseño de un SPR son:

- el sistema puede ser calibrado y probado durante la operación a potencia sin degradar la función de protección.
- toda la información relativa a los parámetros asociados con la seguridad está disponible para el operador en la Sala de Control.
- el sistema se proyecta para que falle en modo seguro. Los canales de disparo se proyectan de modo que un corte de energía origina que éste se vaya a la condición de disparo. Asimismo, la pérdida de tensión en cualquiera de los dos dispositivos de salida disparará el reactor.
- la acción de protección se completa totalmente una vez iniciada, exigiendo la vuelta a operación normal la intervención del operador.
- las operaciones de protección se anulan manual o automáticamente siempre que existan condiciones permisivas que hagan innecesarias dichas acciones.
- el SPR está sometido a requisitos de garantía de calidad, cualificación ambiental y diseño antisísmico (se trata de equipo de Seguridad).
- las fuentes de alimentación eléctrica al SPR son asimismo de Seguridad.

La configuración específica, interacción o interfases de estos sistemas y las peculiaridades funcionales de los sistemas de protección son características del tipo de tecnología de la central (PWR, BWR), e incluso para cada tecnología pueden existir variaciones correspondientes al diseño específico de cada central. A modo de ejemplo, mientras en las centrales PWR-Westinghouse el sistema de actuación de salvaguardias tecnológicas es una función centralizada en cabinas con tarjetas de lógica que generan tanto las señales de disparo como de actuación, en el diseño de centrales BWR las señales de iniciación de sistemas se generan de manera individual para cada uno de los sistemas y la lógica de actuación es realizada para cada sistema en base a relés y contactos. Asimismo, es bastante frecuente en estas centrales la utilización de la terminología de “sistema de protección del reactor” al referirse explícitamente al sistema de disparo de emergencia del reactor.

Teniendo en cuenta que existe un tema exclusivamente dedicado al SPR, y de cara a aportar algunas ideas básicas sobre el funcionamiento y descripción de un SPR, nos centraremos, a modo de ejemplo, en un sistema de protección típico de una central de tecnología PWR de Westinghouse, en el cual se pueden distinguir dos partes de circuitería:

- Ø una parte analógica consistente en cuatro canales de protección analógicos redundantes (donde se encuentran las comúnmente conocidas “cabinas 7300”) que vigilan diversos parámetros de la central, tratando y elaborando las señales procedentes de los transmisores de proceso, y provocan la activación de biestables que generan las correspondientes señales binarias (con tensión/sin tensión) de superación o no del punto de consigna o disparo que van a ser tratadas por el sistema lógico de protección del reactor.
- Ø una parte electrónica, cabinas del Sistema de Protección de Estado Sólido (“cabinas SSPS”), consistente en dos cadenas lógicas redundantes que reciben las señales de los canales de protección analógicos y realizan la lógica de coincidencia necesaria (típicamente 2-de-3 o 2-de-4) para la generación de señales de actuación.

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. Cualquiera de los dos trenes es capaz de realizar la función protectora necesaria.

De las cabinas del SSPS salen dos señales principales:

- Ø *Señal de disparo del reactor.* Cada una de las dos cadenas o trenes de disparo (A o B) es capaz de abrir un disyuntor separado e independiente de disparo del reactor, RTA y RTB respectivamente. Los dos disyuntores de disparo en serie conectan la potencia eléctrica desde los conjuntos motor-generador hacia el accionamiento de barras. En un disparo del reactor, una pérdida de la tensión suministrada a la bobina de mínima tensión libera el dispositivo y al mismo tiempo energiza la bobina de disparo en derivación, y provoca el disparo abriendo el disyuntor. Cuando cualquier de los dos disyuntores abre se interrumpe el suministro de potencia al accionamiento de las barras de control, las cuales entonces caen por gravedad en el núcleo.
- Ø *Señal de actuación de salvaguardias tecnológicas.* Puesto que las salvaguardias tecnológicas comprenden varios sistemas de fluidos, cada uno de los cuales puede ser iniciado de manera independiente por diferentes condiciones de proceso, existen circuitos de iniciación de la actuación separados en dos cadenas de circuitos de actuación de las salvaguardias tecnológicas. La salida de cada uno de los circuitos de iniciación consiste en un relé maestro que actúa sobre relés esclavos para la multiplicación de contactos según se requiera. Los relés lógicos, maestros y esclavos están montados en las dos cabinas SSPS para los elementos duplicados redundantes. Los relés maestro y esclavo actúan sobre mecanismos de puesta en marcha de los diferentes equipos (bombas y ventiladores, válvulas, arranques de emergencia de generadores, etc.)

Sin entrar en los detalles de lógicas específicas y enclavamientos de actuación, se podrían citar algunas actuaciones típicas de disparo contempladas en el diseño de un SDR de una central PWR como el que estamos tratando, tales como:

- Disparos por sobrepotencia nuclear
- Disparos por sobrepotencia térmica del núcleo
- Disparos por presión y nivel de agua en el presionador
- Disparos por bajo caudal en el sistema de refrigerante del reactor
- Disparo de muy bajo nivel de agua en el generador de vapor
- Disparo de turbina y reactor
- Disparo producido por la señal de IS (Inyección de Seguridad)
- Disparo manual

Los puntos de consigna asociados al disparo del reactor (así como para la actuación de salvaguardias) para las diversas variables vigiladas son recogidos en las Especificaciones de Funcionamiento de las centrales nucleares, en las cuales asimismo se establecen los rangos y tiempos de respuesta requeridos para los diversos canales de disparo. En el capítulo 15 del EFS se contempla el análisis de seguridad que demuestra que los puntos de consigna establecidos son conservadores. Mientras que la mayor parte de los puntos de consigna usados son fijos, hay otras variables que son calculadas a través de la correspondiente ecuación, tal y como sucede con el disparo por sobretemperatura y sobrepotencia.

Como ya se ha mencionado previamente, la función de los sistemas ESFAS es detectar situaciones de accidente e iniciar la actuación de los dispositivos de salvaguardias tecnológicas necesarias y de sistemas auxiliares soporte esenciales. Sin entrar en detalle al respecto de todas las funciones de actuación, permisivos y enclavamientos, asociados a la actuación de los sistemas ESFAS, se podrían citar a modo de ejemplo ciertos accidentes de una central PWR que exigen una acción protectora, y las variables que iniciarían las señales de actuación de las salvaguardias en cada caso, tales como:

- Importante rotura de tuberías que contienen refrigerante del reactor (accidente por pérdida de refrigerante); la actuación de la Inyección de Seguridad se inicia por baja presión en el presionador.
- Rotura importante del sistema secundario (rotura de tubería de vapor); la actuación de la Inyección de Seguridad se inicia por cualquiera de las siguientes señales: baja presión en el presionador, baja presión en la línea de vapor, alta presión en el recinto de contención.
- Rotura de la tubería de agua de alimentación principal; la actuación de la Inyección de Seguridad se inicia por cualquiera de las siguientes señales: baja presión en el presionador, baja presión en la línea de vapor, alta presión en el recinto de contención.

Ejemplos típicos de sistemas de salvaguardias tecnológicas de centrales nucleares cuya iniciación tiene lugar de manera automática por el sistema ESFAS son:

Sistemas de aislamiento de la vasija del reactor y de la contención
Sistemas de refrigeración de emergencia del núcleo
Sistemas de despresurización y extracción de calor de la contención
Sistemas de agua de alimentación auxiliar de reactores de agua a presión
Sistemas de tratamiento de gases de reserva de reactores de agua en ebullición
Sistemas de limpieza y purificación del aire de la contención
Sistemas de control de gases combustibles en la contención
Sistemas de aislamiento de la sala de control, y de la ventilación, calefacción y aire acondicionado de emergencia

4. SISTEMA DE INSTRUMENTACIÓN POST-ACCIDENTE

Trás el accidente de TMI (Three Miles Island), la USNRC desarrolló un gran número de nuevos requisitos con objeto de incrementar la seguridad de las centrales nucleares. Como es sabido, el accidente de TMI estuvo muy influenciado por el hecho de que los operadores basaron sus decisiones en una información insuficiente e incluso errónea. Para mejorar la capacidad de los operadores en cuanto a hacer frente a situaciones no deseadas se incluyeron requisitos post-TMI de incorporación de nueva instrumentación de monitorización de las condiciones de planta (radiación, integridad de la contención, y refrigeración del reactor) durante condiciones de accidente (Sistema de Instrumentación Post-accidente) y de mejora de la presentación e interpretación de los datos disponibles (Sistema de Monitorización de Parámetros Relacionados con la Seguridad – SPDS).

En lo que concierne a la instrumentación post-accidente, en la RG 1.97 ‘Instrumentation for Light-Water Cooled Nuclear Power Plants to Assess Plant and Environs Condition During and Following an Accident’ de la USNRC se describe la instrumentación necesaria para monitorizar las variables de la planta y los sistemas durante y seguidamente a un accidente con objeto de prevenir y mitigar sus consecuencias, así como los requisitos de diseño que han de cumplir. La RG establece cinco tipos de variables (A,B,C,D,E) necesarias para permitir al personal de operación en Sala de Control la toma de acciones y el conocimiento de la situación de la planta durante el curso de un accidente.

Las variables de cada tipo están explícitamente definidas en la RG, excepto para las de Tipo A que son específicas de cada planta. En función de la importancia de la variable se especifica su categoría (1,2 o 3), de manera que para las variables de categoría 1 están sometidas a los más exigentes requisitos de diseño (redundancia, cualificación sísmica, ambiental, separación física, alimentación eléctrica 1E, etc.), las de categoría 2 requieren cualificación ambiental, y las de categoría 3 son de grado comercial sin requisitos especiales.

La aplicación de esta guía a centrales en operación ha supuesto importantes modificaciones de diseño que han abarcado: implantación de nueva instrumentación (por ejemplo: nivel de la vasija del reactor, analizadores de hidrógeno de la atmósfera de contención), modificaciones de la instrumentación existente

(ampliación de rangos, sustitución de componentes por requisitos de cualificación,...), y modificaciones en Sala de Control (indicación de nuevos indicadores y registros y sustitución de otros por problemas de cualificación sísmica).

5. OTROS SISTEMAS DE CONTROL RELEVANTES

Sistemas de instrumentación nuclear (SIN)

La potencia media de salida de un reactor nuclear es igual al producto del incremento de temperatura del refrigerante por su caudal másico. No obstante, esta forma de determinar la potencia es demasiado lenta a efectos de control del funcionamiento del reactor sin riesgos, por lo que a tal fin se dispone en el reactor de instrumentación neutrónica para la medida del flujo de neutrones en el núcleo, proporcionando con ello una monitorización de la potencia del reactor (proporcional a dicho flujo) y de su evolución en el tiempo.

El diseño de la instrumentación nuclear de una central PWR-Westinghouse contempla dos tipos de instrumentación: Intranuclear (ó In-Core) y Extranuclear (Ex-Core).

El *Sistema de Instrumentación Intranuclear* está diseñado para proporcionar una información fiable sobre la distribución axial de flujo neutrónico y la temperatura del agua de refrigeración del núcleo a la salida de los elementos combustibles, para lo cual consta de termopares fijos y detectores móviles. Los termopares fijos, de Cromel-alumel con vaina de acero inoxidable, se instalan en tubos guía que penetran en la cabeza de la vasija y son ubicados en puntos seleccionados del núcleo para la medición de la temperatura del refrigerante, aportando información para calcular la distribución de potencia radial y la distribución entálpica del refrigerante. Los detectores móviles, cámaras de fisión (U308, con un alto grado de enriquecimiento en U235), están acoplados en los extremos de cables helicoidales y unidades de accionamiento que sirven para su inserción y extracción, moviéndose a lo largo de los elementos combustibles, permitiendo la obtención de información al respecto de la distribución axial del flujo neutrónico.

El *Sistema de Instrumentación Extranuclear* consiste en detectores exteriores colocados adyacentes a la vasija, distribuidos alrededor del reactor en el blindaje primario, los cuales se encargan de: medir y vigilar de modo continuo y en todo el rango de operación del reactor el nivel de potencia del reactor (flujo de neutrones), generar las señales adecuadas de alarma y disparo de protección del reactor en casos de picos de potencia indeseables, generar señales de control para determinados parámetros del reactor, y proporcionar señales audibles y visuales tanto del nivel de potencia como de la velocidad de arranque. Esta instrumentación se calibra con referencia a la intranuclear.

Para cubrir todo el rango de medida del flujo de neutrones térmicos existente entre el estado de planta en parada fría y el de planta a plena potencia se disponen tres subsistemas de detectores de neutrones cubriendo diferentes rangos, con el adecuado solape entre los mismos, proporcionando una protección segura y continua. Estos subsistemas son el *Subsistema de Detección de Rango Fuente*, que consta de

dos canales con contadores proporcionales (de BF3) colocados en pozos diametralmente opuestos en la parte inferior del núcleo, y que realizan la medición a niveles bajos de flujo neutrónico (durante paradas, recargas y en los arranques desde subcríticidad hasta un flujo determinado en el rango intermedio); el *Subsistema de Rango Intermedio*, que consta de dos canales cada uno con una cámara de ionización compensada situados coincidiendo con el plano medio del núcleo, y que cubren la medición correspondiente a niveles intermedios entre los niveles de arranque del reactor y los de operación a potencia; y el *Subsistema de Rango de Potencia*, formado por cuatro canales o conjuntos dobles de cámaras de ionización no compensadas, colocados de tal manera que cada cámara vigila un cuadrante (superior e inferior) del reactor, y que cubre los niveles de flujo neutrónico de potencia del reactor hasta el 120 % de la potencia nominal. Las salidas de los canales de rango de potencia se utilizan para la función de control de la velocidad de las barras de control, para alertar al operador de un excesivo desequilibrio axial de la distribución del flujo, para proteger el núcleo contra accidentes de caída de barras de control y de parada, o de extracción de las mismas, y para dar señales de parada del reactor por exceso de potencia.

En el caso de una central de diseño BWR-General Electric la misión del SIN es equivalente a la de los reactores PWR, es decir: medir el flujo de neutrones térmicos en el núcleo durante todos los modos de operación, medir la potencia en diferentes puntos del núcleo con el fin de conseguir una distribución óptima de potencia térmica, medir y registrar la potencia térmica promediada del núcleo, proporcionar señales de disparo y alarma al sistema de protección del reactor cuando el flujo neutrónico o la potencia excedan los valores prefijados, y proporcionar un medio para calibrar los detectores en el rango de potencia.

La diferencia entre el diseño BWR y el PWR es que en el caso de centrales BWR todos los detectores están ubicados en el interior del núcleo. Al igual que en el caso de los PWR, de cara a cubrir todos los rangos de la instrumentación de medida de flujo neutrónico se disponen de subsistemas de detección diversos:

- *detección en el Rango de Fuente* (conocido como SRM), mediante canales conteniendo una cámara de fisión retráctil insertable o extraíble del núcleo.
- *detección en el Rango Intermedio* (IRM), mediante canales conteniendo cámaras de fisión similares a las del rango fuente excepto en el rango de vigilancia.
- *detección en el Rango de Potencia Local* (LPRM), mediante cámaras de fisión fijas y permanentemente instaladas en el núcleo a distintas alturas, que suministran la medida de potencia correspondiente a un flujo neutrónico local.
- *detección de potencia media del núcleo o Rango de Potencia Promediada* (APRM), que consiste únicamente en circuitos electrónicos que reciben las medidas obtenidas por los detectores LPRM y realizan el promediado de las mismas para dar una indicación fiel de la potencia térmica del núcleo, pudiendo generar señales de bloqueo de extracción de barras de control y de SCRAM si el flujo neutrónico sobrepasa un cierto nivel.
- *subsistema de Sonda de Calibración* (TIP - Traversing Incore Probe), que consiste en una serie de mecanismos de accionamiento con detectores de

cámaras de fisión, que se reparten entre los conjuntos de detectores LPRM existentes, obteniendo información de la distribución de flujo neutrónico que comparada con las medidas obtenidas por los LPRMs permite llevar a cabo la calibración de estos.

Sistema de Control del Reactor en centrales PWR

El principio de funcionamiento de los reactores PWR es “reactor siguiendo a turbina”, esto es, el reactor procede a modificar y estabilizar el nivel de potencia generada de manera que se acomode a las alteraciones de la demanda de potencia de la red eléctrica. El encargado de realizar tal función es el Sistema de Control del Reactor, y se basa en el seguimiento de un programa de control de la temperatura media del refrigerante, el cual establece una temperatura media (T_m) creciente linealmente con la potencia de la turbina.

De acuerdo con los criterios generales de diseño, el control del reactor debe efectuarse mediante mecanismos redundantes, independientes y diversos, que en el caso de una central PWR son: posición de las barras de control, que pueden moverse manual o automáticamente, y disolución en el refrigerante de absorbentes neutrónicos (ácido bórico). El sistema de control químico y volumétrico (SCQV), mediante su control manual, es el que regula la concentración del absorbente químico de neutrones en el refrigerante del reactor.

Sistemas de Control de Presión y Nivel del Presionador en centrales PWR

El control de la presión en el primario tiene como objeto garantizar un grado de subenfriamiento adecuado que evite la ebullición en el núcleo y la consiguiente degradación de las condiciones de transferencia de calor. Este control se realiza en el presionador, en el cual se dan condiciones de saturación, de manera que existe un equilibrio agua-vapor que permite controlar la presión gracias a la burbuja de vapor, y se lleva a cabo modificando la temperatura de la interfase agua-vapor.

El control de la presión se realiza mediante calentadores (que se encargan de mantener la temperatura de saturación correspondiente a la presión de operación), duchas (se encargan de aliviar la presión mediante la aportación de agua), y válvulas de alivio (encargadas de limitar la presión del sistema por debajo del punto de tarado del disparo del reactor) y válvulas de seguridad, todos ellos actuados automáticamente por el SPR de la planta.

El control de nivel del presionador se realiza ajustando el caudal de carga desde el SCQV al primario para mantener el programa de T_m de los lazos, mediante actuación sobre la válvula de regulación de carga (en función del incremento de nivel real frente al nivel programado). Tiene por objeto mantener el inventario de la masa en el primario durante la operación normal a potencia.

Sistema de Control e Información de las Barras de Control en centrales BWR

Al igual que en el caso de centrales PWR, las plantas de diseño BWR deberán responder adecuadamente a las demandas de la red, disponiendo de los adecuados

sistemas de control encargados de mantener las diferentes variables dentro de los límites establecidos, evitando la entrada de los sistemas de protección, y establecer las condiciones de operación de la planta con el máximo rendimiento.

En centrales BWR, al utilizar un ciclo directo, el agua que modera y refrigera el núcleo es la misma que experimenta el ciclo termodinámico generador de energía mecánica. Una característica importante de este tipo de centrales es la implantación de las bombas de chorro y del sistema electrohidráulico (EHC) de control de la presión del reactor. El sistema de control del reactor se vale en este caso de un sistema de barras de control y de un sistema de control de reactividad por huecos mediante las bombas de recirculación del reactor. No es aplicable en este caso el control mediante aditivos.

El sistema de control e información de las barra de control consta de un conjunto de subsistemas que permite enviar órdenes a los mecanismos de accionamiento de las barras de control y recibir información del estado y posición de las mismas y de sus mecanismos asociados. Consiste básicamente en un computador de programa fijo materializado en forma de pulsadores y luces indicativas en la consola del operador que dan una información exhaustiva del estado del núcleo y permite asimismo su accionamiento manual.

El subsistema de control de secuencia de barras tiene como función principal obligar al operador a seguir una secuencia de inserción/extracción predeterminada, activando en caso contrario los adecuados bloqueos y alarmas. Esta secuencia es la implantada en el ordenador tras el análisis de la planta y el estudio de reactividad introducida por cada barra.

Junto con la ayuda de sus mecanismos de accionamiento hidráulico, las barras de control sirven para: (1) regular la potencia del reactor adoptando diferentes posiciones, (2) proporcionar un medio seguro de parada rápida y, (3) uniformizar la distribución de flujo neutrónico.

Sistema de Control de Caudal de Recirculación en centrales BWR

El sistema de recirculación proporciona el caudal motriz de las bombas de chorro, cuyo objetivo es aumentar la velocidad de paso de refrigerante a través del núcleo. Consta de dos lazos de recirculación con una bomba cada lazo, que aspira del volumen existente entre la vasija y la envoltura del núcleo y descarga al colector de las bombas de chorro. El caudal de recirculación es $1/3$ del caudal total que atraviesa el núcleo. Este caudal puede variarse regulando la posición de las válvulas controladoras de caudal de que dispone cada lazo, regulando así la potencia térmica generada por el núcleo, función que es realizada por el sistema de control de caudal de recirculación.

El sistema de control de caudal de recirculación consta de circuitos electrónicos para realizar el control de la potencia del reactor según la demanda. Un aumento del caudal de recirculación provoca un efecto de barrido de los huecos del núcleo, desplazando hacia arriba el límite de ebullición (separación fase líquida-vapor). Ello supondrá que un área antes ocupada por huecos ahora contiene líquido, lo que aumentará la moderación en esta zona insertando reactividad positiva en el núcleo.

El aumento de calor en esta zona provoca la ebullición y creación de nuevas burbujas que desplazan hacia abajo el límite de ebullición, insertando reactividad negativa que con el efecto Doppler (temperatura en combustible) detiene el aumento de potencia. El resultado neto es una nueva situación estable con un aumento de potencia térmica del núcleo con una mayor velocidad de formación/extracción de vapor.

Sistema de Control de Presión en centrales BWR

En las centrales BWR las variaciones de la posición de las válvulas de control de la turbina provocan una variación de la presión del reactor que conduce a provocar cambios de potencia opuestos a los deseados. Por ejemplo, el cierre de las válvulas de control como consecuencia de un rechazo de carga genera un aumento de presión que conduce a un incremento de la potencia del reactor. Por ello, estos reactores se diseñan como un elemento que debe trabajar a presión constante, permitiéndose sólo cambios de presión muy pequeños. El sistema que mantiene constante, en todo momento, la presión del reactor es el Sistema de Control Electrohidráulico (EHC).

Este sistema se compone de componentes eléctricos que actúan hidráulicamente sobre las válvulas de control y bypass de turbina, ofreciendo también la posibilidad de regular la potencia del reactor mediante el caudal de recirculación.

6. UTILIZACIÓN DE TECNOLOGÍA ANALÓGICA Y DIGITAL

Las centrales nucleares españolas, y en general todas las que fueron construidas antes del final de la década de los ochenta, utilizaron para el diseño de sus sistemas de instrumentación y control tecnología analógica y electrónica de estado sólido, basada en el uso de sensores analógicos, relés, contactores, biestables, etc. Tan solo sistemas de control muy concretos, y nunca relacionados con la seguridad, así como funciones de información, como el ordenador de planta, fueron confiadas a la tecnología digital basada en el uso de software.

En los últimos años la industria convencional se ha ido dirigiendo hacia el uso de sistemas digitales (a los que con frecuencia se les hace referencia, de manera más adecuada para su diferenciación de la electrónica de estado sólido, por “sistemas basados en microprocesador” o “sistemas basados en software”), y los fabricantes han ido gradualmente disminuyendo el soporte técnico y la presencia de repuestos para los sistemas analógicos. La razón para esta transición hacia sistemas de instrumentación y control digitales radica en importantes ventajas que presentan sobre los sistemas analógicos, tales como que la electrónica digital está esencialmente libre de la deriva que afecta a la analógica (manteniendo mejor la calibración), que la instrumentación digital ha evolucionado notablemente en términos de precisión y capacidad de computación (con mayor capacidad de manejo y almacenamiento de datos) mejorando la medición y muestreo de las condiciones operativas, y que con el adecuado diseño pueden ser más fáciles de manejar y más flexibles en su aplicación. Asimismo, los sistemas digitales contemplan una serie de importantes mejoras potenciales de sus capacidades (por ejemplo, tolerancia al fallo,

autochequeo, validación de la señal, diagnóstico del sistema de proceso, etc.) que pueden constituir la base de nuevos enfoques para alcanzar las especificaciones de calidad requeridas.

Estas ventajas y la transición hacia los sistemas digitales de los fabricantes, en perjuicio del aporte de soporte técnico para sistemas analógicos, es lo que conduce a la tendencia de una sustancial substitución de los sistemas analógicos de instrumentación y control existentes en las centrales nucleares por tecnología digital.

No obstante, la transición hacia los sistemas digitales en centrales nucleares no es un proceso sencillo debido a las dificultades inherentes al licenciamiento de esta nueva tecnología, dando lugar a grandes esfuerzos y a la emisión de elevado número de documentos y normas destinados a la definición de un adecuado marco regulador para el uso de la tecnología digital en aplicaciones de seguridad en centrales nucleares.

Un aspecto diferenciador especialmente destacable de los sistemas digitales frente a los analógicos, y que resulta relevante en cuanto a su licenciamiento, es el hecho de que, por tratarse de componentes de comportamiento discreto, la prueba de un equipo digital sobre una muestra de condiciones de entrada no determina el comportamiento del mismo sobre el rango completo de las mismas. En este sentido, el uso de inspecciones, pruebas tipo y pruebas de aceptación no resulta suficiente para garantizar la adecuada ejecución de la función esperada del equipo y la no presencia de funciones inesperadas.

Puesto que no se puede detectar completamente la presencia de fallos en un equipo digital mediante pruebas, se persigue entonces evitar al máximo posible la introducción de errores durante el proceso de desarrollo del mismo, o en otros términos, alcanzar la máxima fiabilidad del equipo desarrollado, para lo cual la regulación aplicable a estos sistemas establece requerimientos en persecución de un proceso de desarrollo del software altamente disciplinado y de alta calidad.

Este proceso disciplinado y de alta calidad se fundamenta en la estructuración del proceso en etapas claramente definidas, en la preparación y seguimiento de los adecuados planes para la ejecución del mismo, y en el establecimiento de las oportunas medidas de control para la detección de deficiencias o errores que pudiesen ser introducidos durante el desarrollo del sistema, y la comprobación de que el producto final responde a los requisitos establecidos en las especificaciones para el mismo. Estas medidas de control constituyen lo que se denomina proceso de Verificación y Validación, el cual se define como el proceso que permite determinar si los requisitos de un sistema o componente son completos y correctos, si los productos de cada fase de desarrollo cumplen con los requisitos impuestos por la fase previa, y si el sistema o componente final cumple con los requisitos inicialmente especificados.

Adicionalmente a los requisitos sobre el proceso de desarrollo, existen otros aspectos a tener especialmente en cuenta en el caso de utilización de sistemas digitales, tales como la gestión de la configuración del software, el comportamiento determinista, cualificación del equipo (incluyendo compatibilidad electromagnética), la independencia de comunicaciones, el control de acceso, posibilidad de fallos de causa común (requisitos de diversidad), etc.

Al objeto de resolver las dificultades inherentes al licenciamiento de la tecnología digital, y clarificar la aplicación de la normativa internacional existente al respecto, se constituyó en España el Proyecto de Instrumentación Digital, desarrollado en el marco del Plan Coordinado de Investigación establecido entre el CSN y UNESA, emitiéndose como producto del mismo el documento ‘Guía para la implantación de sistemas digitales en centrales nucleares’ (UNESA CEN-6, Rev. 0 Mayo 2002), la cual pretende ser una herramienta para la incorporación de sistemas digitales en centrales nucleares españolas, y contempla los aspectos más relevantes que lleva asociado su licenciamiento para funciones de seguridad, así como define un proceso de licenciamiento por etapas en el cual el CSN se ve involucrado desde las primeras etapas del proceso de desarrollo del nuevo sistema.

Cabría asimismo mencionar, en relación con este tema, el documento ‘Licensing of safety critical software for nuclear reactors. Common position of seven European nuclear regulators and authorised technical support organisations,’ publicado inicialmente en 2007, y posteriormente actualizado mediante la publicación de posteriores revisiones, en el cual se recogen las conclusiones del esfuerzo de organismos reguladores de diversos países en la búsqueda de la armonización de criterios normativos asociados al licenciamiento de sistemas digitales para su uso en centrales nucleares, y en el cual el CSN es parte activa.

7. REFERENCIAS NORMATIVAS PARA SISTEMAS IyC

En la normativa americana, país de origen de la tecnología aplicada en el diseño de la mayoría de las centrales nucleares españolas, se identifica un considerable número de documentos asociados a la regulación del uso de sistemas de instrumentación y control para funciones de seguridad en centrales nucleares. El método de revisión y licenciamiento de estos sistemas por parte de la USNRC aparece contemplado en la Sección 7 “Instrumentation and Controls” del NUREG- 0800 “Standard Review Plan”.

Ante la imposibilidad de hacer referencia a la mayoría de estos documentos se exponen a continuación, adicionalmente a los ya citados a lo largo del tema, algunos de los criterios de aceptación, guías reguladoras y documentos de la industria más relevantes:

- Criterios Generales de Diseño del Apéndice A al 10CFR50; entre otros, se podrían citar para los sistemas IyC los siguientes: GDC - 13 “Instrumentation and Control”, GDC - 19 “Control Room”, GDC - 20 “Protection System Functions”, GDC - 21 “Protection System Reliability and Testability”, GDC - 22 “Protection System Independence”, GDC - 23 “Protection System Failure Modes”, GDC - 24 “Separation of Protection and Control Systems”.
- El apartado 50.55a(h) del 10 CFR específicamente expone que los sistemas de protección de centrales nucleares construidas posteriormente al 1 de enero de 1971 han de cumplir con los requisitos especificados en la norma IEEE Std. 279, "Criteria for Protection Systems for Nuclear Power Generating Stations," o la norma IEEE Std. 603 "Criteria for Safety Systems for Nuclear Power Generating Stations", que la actualiza y mejora. Estos documentos constituyen la norma básica de aplicación a los sistemas IyC de seguridad, y en ellos se definen los

criterios básicos que ha de contemplar el diseño de estos sistemas.

Con respecto a otra normativa internacional asociada a los sistemas IyC en centrales nucleares se podrían citar, entre otros, los siguientes:

- **IEC 1226, “The Classification of Instrumentation and Control Systems Important to Safety for Nuclear Power Plants”.**
- **IEC 231 y el Suplemento IEC 231 A, “General Principles of Nuclear Reactor Instrumentation”.**
- **IAEA Safety Guide, “Protection System and Related Features in Nuclear Power Plants”, IAEA Safety Series N° 50-SG-D3.**

En referencia a su aplicación a CN Trillo, de tecnología KWU-Siemens, se puede destacar la siguiente normativa alemana para los sistemas IyC:

- **KTA - 3501 “Reactor Protection System and Monitoring of Engineered Safeguards”.**
- **KTA - 3502 “Incident Instrumentation”.**

En cuanto a normativa y guías españolas relacionadas con el uso de tecnología digital se podrían añadir las siguientes:

- **UNE 73-404-98 “Garantía de Calidad en los Sistemas Informáticos Aplicados a Instalaciones Nucleares”.**
- **Guía de Seguridad del CSN 1.9 “Garantía de Calidad de las Aplicaciones Informáticas Relacionadas con las Instalaciones Nucleares”.**

A nivel internacional han sido emitidos una considerable cantidad de documentos normativos y de la industria, abarcando los diferentes aspectos asociados al diseño, uso y licenciamiento de sistemas digitales de IyC, pudiendo resaltarse, por ser más genéricos en cuanto a su alcance, los siguientes:

- **IEC Std. 880 “Software for Computer in the Safety Systems of Nuclear Power Stations”.**
- **IEC Std. 987 “Programmed Digital Computers Important to Safety for Nuclear Power Stations”.**
- **USNRC Regulatory Guide 1.152 “Criteria for Programmable Digital Computer System Software in Safety Related Systems of Nuclear Power Plants”, la cual endorsa la IEEE Std 7-4.3.2 “Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations”.**
- **IAEA-IWG-NPPCI-96/3 “Modernization of I&C in Nuclear Power Stations”.**
- **IAEA-IWG-NPPCI-96/1 “Advanced Control Systems to Improve Nuclear Power Plant Reliability and Efficiency”.**
- **EPRI TR-102348 Rev. 1 /NEI 01-01 “Guideline on Licensing Digital Upgrades. A Revisión of EPRI TR-102348 to reflect changes to the 10 CFR50.59 Rule ”.**
- **EUR 18158 “European Nuclear Regulators’ Current Requirements and Practices for the Licensing of Safety Critical Software for Nuclear Reactors”.**

BIBLIOGRAFÍA

Adicionalmente a los documentos ya citados a lo largo del mismo, otras referencias consultadas para la realización del presente tema han sido:

- Estudio Final de Seguridad de C.N. Almaraz; Capítulo 7 “Sistemas de Instrumentación y Control”.
- Estudio Final de Seguridad de C.N. Ascó I; Capítulo 7 “Instrumentación y Control” y Capítulo 15 “Análisis de Accidentes”.
- Estudio de Seguridad de C.N. Cofrentes; Capítulo 7 “Sistemas de Instrumentación y Control”.
- Informe del CSN de referencia CSN/TGE/INEL/9807/904.
- “Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues – Final Report”, National Research Council.
- Documentación del “Curso de Tecnología de Centrales”. Tecnatom S.A.