



Telmo GABARAIN es Licenciado en Ciencias Físicas por la Universidad de Navarra. Ingresó en Iberduero en 1976, integrándose en el proyecto de la central de Sayago. En 1977 pasó al grupo de Puesta en Marcha de Lemóniz, primero como responsable del taller de calibraciones y luego al frente de la sección de Instrumentación de PEM. De 1982 a 1991 perteneció a Nuclenor, trabajando en el Departamento de Ingeniería, al cargo de la sección Eléctrica-Instrumentación. En 1991 reingresó en Iberdrola, siendo cedido a UNESA para actuar como residente español en el programa internacional de reactores avanzados que coordina EPRI.

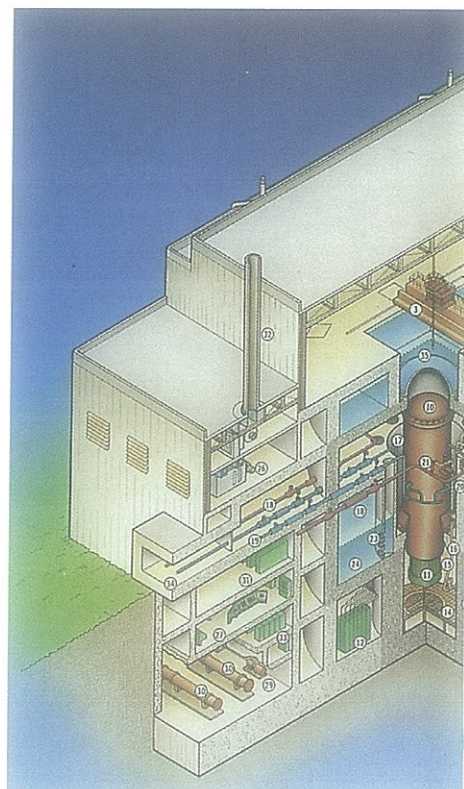
LICENCIAMIENTO DE SISTEMAS DE INSTRUMENTACION Y CONTROL DIGITALES EN CENTRALES AVANZADAS

T. GABARAIN

• Posiblemente el área técnica que experimentará una mayor evolución en las futuras centrales avanzadas respecto a las centrales actuales es la de Instrumentación y Control. La desaparición paulatina del mercado de las tecnologías de control tradicionales y el potencial de los modernos sistemas digitales hacen que exista un amplio acuerdo entre usuarios, fabricantes y reguladores acerca de la conveniencia de utilizar estos últimos en el diseño de centrales futuras, al igual que en la modernización de las actuales. La adopción de esta nueva tecnología trae consigo, sin embargo, algunas incertidumbres en cuestiones de seguridad que han dado lugar a un diálogo complejo y largo entre la industria y la NRC, dentro del contexto de la certificación de los diseños estandarizados de centrales avanzadas.

• El documento de requisitos para reactores avanzados de agua ligera ("Utility Requirements Document" o URD), elaborado por EPRI como una de las primeras etapas del Plan Estratégico para el relanzamiento de programas de construcción de reactores, dedica su capítulo más extenso a establecer los requisitos de diseño para los sistemas de Interfase Hombre-Máquina. Este documento especifica una estructura de control basada totalmente en sistemas digitales, aunque reconoce también la necesidad de prever ciertos modos de fallo, característicos de los sistemas basados en software, que podrían forzar la necesidad de recurrir a equipos alternativos de tecnología clásica como apoyo para determinadas funciones de

seguridad. Sin embargo, el objetivo del URD es conseguir, en la mayor medida posible, una configuración homogénea minimizando el uso de equipos de tecnología tradicional que complicarían el diseño y podrían afectar negativamente a la operación, mantenimiento y gestión de repuestos. Por esta razón, el URD requiere a los fabricantes que



aborden los problemas de fiabilidad a través de un diseño integrado que incluya un plan de ensayos de simulación, pruebas de hardware y programas de verificación-validación de software.

- La fase de Certificación, como se ha dicho al principio, conlleva una intensa interacción entre la industria y la NRC, como consecuencia de la evaluación que esta última debe hacer del URD y de los diseños estandarizados presentados por los fabricantes, Westinghouse, General Electric y ABCE. El Staff tiene una experiencia limitada en la evaluación de seguridad de sistemas de control digitales y actúa con gran prudencia. (Esta actitud es especialmente acusada en las evaluaciones de las reformas de modernización de centrales en operación). La NRC ha formado su criterio a partir de las referencias que proporcionan los diseños más modernos, en particular el de Sizewell de Nuclear Electric, así como de la opinión de expertos en el uso de sistemas digitales para aplicaciones con requisitos de seguridad muy exigentes, como instalaciones médicas y aeronaves.

- En base a estas referencias, la NRC considera que los sistemas digitales de control, aunque sean diseñados con arquitecturas redundantes, son potencialmente vulnerables a modos comunes de fallo si utilizan un mismo tipo de hardware y software. Este tipo de fallos podrían dejar simultáneamente inoperables a varios o a todos los canales redundantes de todo un sistema. Para abordar este problema, la NRC requiere, a semejanza del URD, un minucioso proceso de diseño supervisado por un

sistema de calidad. La NRC considera asimismo necesaria la inclusión de sistemas de control alternativos de apoyo para las situaciones de fallo común mencionadas. Este último requisito preocupa a la industria, no tanto a nivel conceptual, ya que el propio URD describe esta opción, sino por el posible impacto negativo de una aplicación demasiado amplia de esta metodología.

- Tras evaluar la propuesta del Staff contenida en el SECY 93-087,

los comentarios del ACRS, de fabricantes y de representantes de las empresas eléctricas (EPRI y NUMARC), la posición de la Comisión es la siguiente:

1. El solicitante (de certificación de diseño) deberá demostrar que su sistema de Instrumentación y Control posee unas características de diversidad adecuadas para compensar la vulnerabilidad de sus sistemas de control a modos comunes de fallo. Un método aceptable de análisis es el que recoge el NUREG-0493 que aplica a la evaluación del ABWR de GE.

2. Este análisis deberá considerar todos los accidentes descritos en el capítulo 15 del SSAR y, para cada uno de ellos, todos los modos comunes de fallo postulados. En todos los casos, deberá demostrarse que el diseño incluye diversidad para las funciones requeridas en cada uno de dichos escenarios.

3. Si un modo común de fallo inutiliza una función de seguridad del sistema de control, deberá existir un dispositivo de control alternativo para ejecutar la misma función. Este podrá ser un sistema digital no relacionado con la seguridad, siempre que se demuestre su independencia del modo de fallo que afecta al sistema al que apoya y su inmunidad a las condiciones creadas por el accidente. El sistema alternativo puede ser manual (como el que se requiere en el punto 4), siempre que se demuestre que hay un margen de tiempo suficiente para permitir la correspondiente actuación del operador (del orden de una hora).

4. Además de los sistemas de control digital, el diseño deberá contar con un conjunto de elementos de control y monitorización en Sala de Control que permitan las actuaciones manuales necesarias para llevar la central a parada caliente, incluyendo las funciones de control de reactividad, extracción de calor residual, aportación de agua al reactor y aislamiento e integridad de contención. Estos dispositivos, que la NRC entiende como un subconjunto de los descritos en el punto anterior, estarán clasificados como componentes no relacionados con la seguridad y estarán cableados hasta el nivel más próximo a los componentes de los sistemas que sea práctico. Este último requisito persigue que esta actuación manual se procese con independencia del sistema digital de superior jerarquía, pero permitiría, en una arquitectura de control distribuido por ejemplo, que los elementos de control estuvieran cableados hasta los controladores digitales locales, que elaboran las señales de control de los dispositivos electromecánicos que actúan los componentes del sistema. Estos controles podrían utilizarse para cumplir con el requisito del punto 3, siempre que se disponga de tiempo para dar crédito a la acción manual.

- Con esta formulación, se ha resuelto la interacción entre EPRI y la NRC por lo que respecta a la evaluación del

URD. La materialización de estos criterios en los diseños específicos se analiza dentro de la certificación de cada uno de ellos. Los términos de la posición del NRC son en general satisfactorios para la industria, aunque hay algunas opiniones que los consideran excesivamente conservadores y susceptibles de repercutir negativamente en el coste y en la complejidad del diseño, tanto en centrales avanzadas como en las reformas para modernización de las centrales actuales.

- Realmente, la posición de la NRC es muy genérica y podría implementarse con arreglo a un amplio abanico de interpretaciones que, a su vez, darían lugar a diferentes configuraciones. Incluso dentro de la propia NRC, no hay un criterio único acerca de cuestiones tales como modos de fallo que deban postularse o qué se considera el "máximo nivel que sea práctico" para el cableado local de los controles alternativos en el punto 4. En cualquier caso, el postular fallos comunes de software es razonable si se pretende, como es el caso, llegar a configuraciones basadas en soportes informáticos (hardware y software) de grado comercial. Diseñar totalmente un sistema digital de control bajo un sistema de calidad de grado nuclear podría llevar aparejada la exigencia de aplicar la filosofía de 10CFR50 Apéndice B, entre otros, a elementos tales como sistemas operativos o compiladores de lenguajes de alto nivel. Este requisito implicaría exigencias complejas y costosas de verificación-validación del software inicial y de sus actualizaciones posteriores.

Una opción sería desarrollar herramientas informáticas simplificadas para facilitar su control y revisión; esto, sin embargo, tendría el inconveniente de tener que renunciar al uso de productos comerciales estandarizados y ampliamente contrastados, lo cual es asimismo un requisito del URD. El uso de herramientas estandarizadas, aunque obligue a postular modos de fallos común, tiene grandes ventajas de cara a comunicaciones en sistemas abiertos, actualizaciones e, incluso, de cara a la fiabilidad, por cuanto son susceptibles de perfeccionarse con las mejoras realimentadas a través de su utilización en un gran espectro de aplicaciones. Así pues, la posición expresada por la NRC puede considerarse como apropiada, habida cuenta del estado actual de la tecnología digital, siendo compatible con un diseño armónico, si no ideal, de los sistemas de Instrumentación y Control de las centrales avanzadas. En cualquier caso, la industria deberá seguir muy de cerca, durante las fases de certificación y de desarrollo de la ingeniería de detalle (FOAKE), la implementación de estos criterios en los diseños específicos para asegurar una aplicación óptima de los mismos.

