

D. FERNÁNDEZ

SISTEMAS DIGITALES DE I&C PARA EL CONTROL Y LA SEGURIDAD DE OPERACIÓN DE CENTRALES NUCLEARES

Los sistemas avanzados de I&C para centrales nucleares deben satisfacer exigencias cada vez mayores en materia de seguridad y de disponibilidad. Se deben cumplir además ciertos requisitos específicos que provienen de la cualificación nuclear. Para el tratamiento idóneo de ambos aspectos en el futuro, Siemens ha desarrollado un sistema avanzado de tecnología de I&C que consta de dos sistemas complementarios de I&C: el TELEPERM XP y el TELEPERM XS.

Las características más destacables de estos sistemas son su arquitectura de redundancia adaptable claramente relacionada con las tareas, la consecuente aplicación de estándares para interfaces y comunicación, las herramientas de máximo alcance que simplifican el diseño y el servicio, y una interface hombre-máquina altamente ergonómico, basado en pantallas o dispositivos convencionales.

El apoyo a las tareas de ingeniería está dado por un sistema integrado de ingeniería con capacidad de diseño, prueba y diagnóstico de todas las funciones de I&C y de los equipos que en ellas intervienen. El TELEPERM XP tiene un diseño apto para la ejecución óptima de todas las funciones automáticas que no están sujetas a cualificación nuclear específica. El TELEPERM XS tiene un diseño apto para la ejecución de todas las tareas de control y de protección relacionadas con los sistemas del reactor. Esto expresamente incluye las funciones para iniciar contramedidas automáticas para evitar accidentes o para enfrentarse a ellos.

CONCEPTO

Un sistema de control de proceso que abarque todas las tareas que se llevan a cabo en las centrales nucleares, necesita equipos para las tareas automatización, comunicación, control y supervisión por parte del operador, ingeniería, diagnóstico y mantenimiento. Las prestaciones de este equipo y su forma de intercalarse constituyen las características del sistema de control del proceso. En el futuro, y a consecuencia del permanente acortamiento de los ciclos de innovación en el desarrollo de software y de hardware, los sistemas de control de proceso sólo tendrán cabida en el mercado si se basan en estándares, pues los estándares tienen por lo general un período de vida más prolongado que el de los componentes individuales. Ésta es la razón por la que el uso generalizado de estándares

constituyó el principio fundamental de sustentación del TELEPERM XP y del TELEPERM XS.

INGENIERÍA, MANTENIMIENTO Y DIAGNÓSTICO

La interface central entre el equipo de automatización, las tareas de control y supervisión a car-

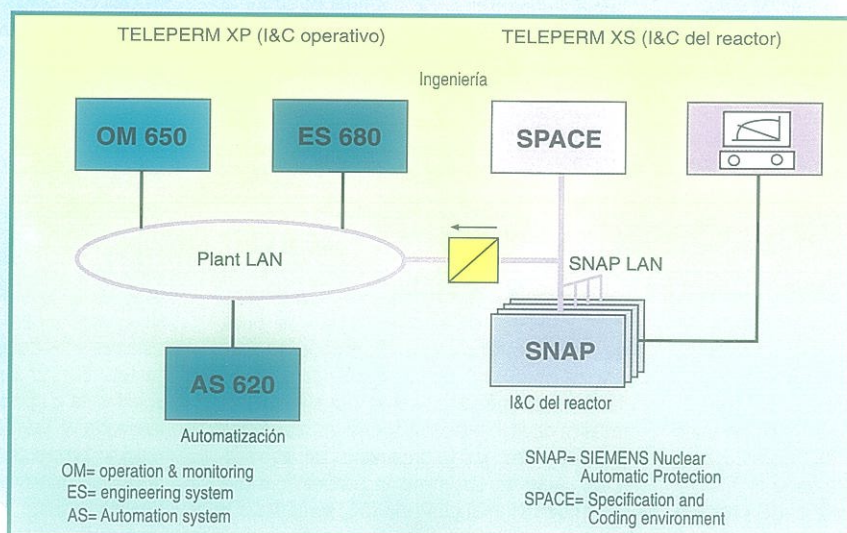
go del operador, la comunicación y el personal responsable del funcionamiento del sistema I&C, es el sistema de ingeniería. Este sistema es una parte integral del sistema de I&C y soporta no sólo las tareas de ingeniería sino también el mantenimiento y diagnóstico de todos los componentes del I&C, es decir, tanto la funcionalidad del software específico de la central para las tareas de automatización,

control y supervisión por parte del operador, y comunicación, como la

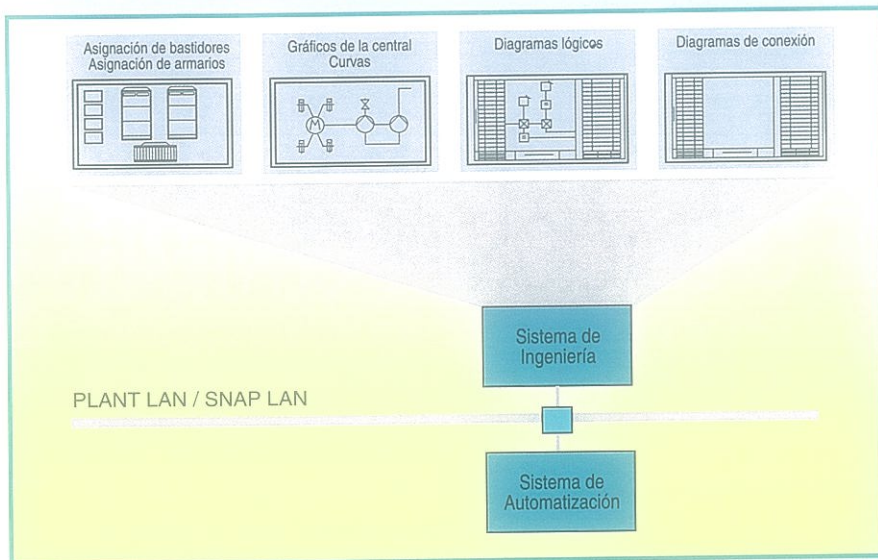
funcionalidad del hardware de todo el sistema de I&C. La característica más importante es que todas las actividades - las de especificación de las funciones de control así como las de diseño de la arquitectura del hardware- se pueden desarrollar a través del mismo interface gráfico de usuario, mediante símbolos estandarizados.

Significa esto que la funcionalidad plena del hardware y del software

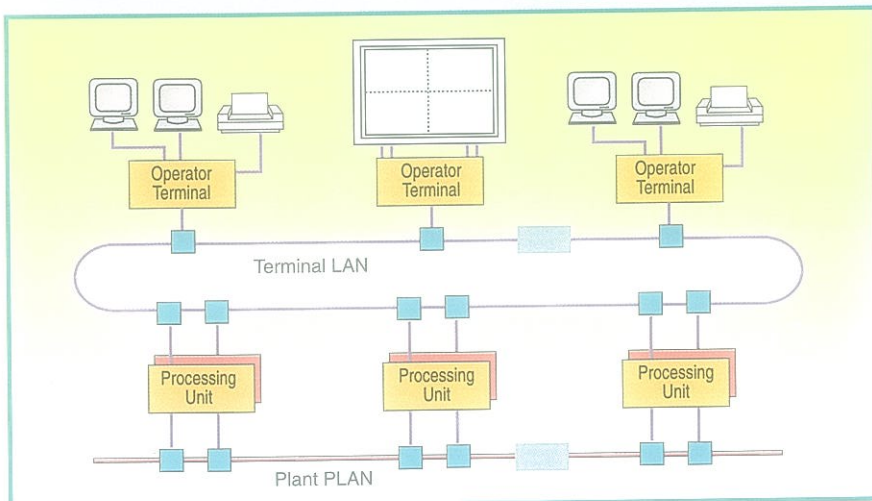
FI - Sistemas Avanzados de I&C para Centrales Nucleares



F II - Funciones del Sistema de Ingeniería



F III - Control e Información del Proceso



propios de la central está especificada en gráficos que utilizan el sistema de ingeniería y que están almacenados de forma centralizada en una base de datos. Para aportar una mayor claridad, la herramienta de ingeniería soporta estructuras jerárquicas con varios niveles. El conjunto de datos de ingeniería creados como parte del diseño normal de la central sirve como base de referencia para todas las demás actividades. Se utiliza no sólo como punto de partida para la preparación de la documentación de construcción para la fabricación del armario, sino también para la generación automática del código del software específico de toda la central. Constituye además la base de una documentación completa orientada a función y ubicación, con lo que se asegura que la documentación de todos los componentes del sistema de I&C estará siempre actualizada y completa. La interface gráfica de usuario bajo la cual se ocultan los datos y mecanismos específicos del sistema de I&C, constituye en sí mismo un paso importante hacia el futuro y hace posible que el ingeniero de proceso

pueda especificar los requerimientos funcionales del sistema de I&C sin necesitar para ello conocimiento alguno del software. Si bien es cierto que un soporte integrado de ingeniería simplifica la habilitación para la puesta en marcha, la verdadera ventaja de la herramienta de ingeniería se aprecia más adelante, cuando la central ya está operando. La sólida consistencia de la documentación de la planta con la funcionalidad del sistema I&C realmente implementada, cobra particular importancia cuando, durante el tiempo de operación de la central, se deben realizar modificaciones y ampliaciones frecuentes. El sistema de ingeniería se aplica también a tareas de mantenimiento y diagnóstico durante el funcionamiento del sistema de I&C. Así pues, se pueden escanear y visualizar en la interface gráfica de usuario de la herramienta de ingeniería, estados internos como, por ejemplo, las señales de fallo procedentes de los módulos o sencillamente, los valores reales de las variables. Además, las imágenes panorámicas que describen la estructura de I&C, sumadas a la

ergonomía de la interface de usuario, garantizan la rápida y directa identificación de todos los fallos de los módulos con lo cual se pueden tomar a tiempo medidas específicas para remediarlos, y reducir así los costes de reparación.

CONTROL Y SUPERVISIÓN A CARGO DEL OPERADOR

El control y la supervisión del proceso por parte del operador se desarrolla por medio de métodos convencionales o bien, utilizando el sistema de control e información del proceso (TELEPERM XP). Este sistema está caracterizado por un concepto cliente-servidor basado en estándares internacionales que permiten la distribución y representación a escala de la funcionalidad. Clientes y servidores se comunican a través de un bus terminal común, abierto, de modo que toda la información está disponible en todos los puntos. Se pueden así hacer implementaciones adaptadas que van desde las configuraciones mínimas de bajo coste como, por ejemplo, las que se necesitan en las estaciones locales de control, hasta completas salas de control por pantalla con presentación visual panorámica y una o más consolas de control.

Los dispositivos de visualización utilizados son monitores de gráficos de alta calidad y pantallas de gran superficie que hacen posible la visualización gráfica o alfanumérica de la información referida al proceso, a la central y al sistema de control del proceso. Las entradas de operador se introducen a través de un dispositivo de entrada de aplicación generalizada en el mundo del PC: el ratón.

Además de estas funciones clásicas de procesamiento para la información y control del proceso, se pueden incorporar al ordenador servidor otros módulos de función desarrollados con visión de futuro. Un claro ejemplo está dado por el módulo de función "ordenador pronosticador" que calcula por adelantado el comportamiento del sistema sobre la base del estado actual de la central para proporcionar a los operadores información referida a los perfiles de determinadas variables importantes del proceso, con proyección de futuro. Significa esto que se pueden tomar con la debida antelación las medidas necesarias para solucionar fallos, con lo que se mejora la disponibilidad de la central.

COMUNICACIÓN

El objetivo al que apuntan las actividades de determinación de estándares internacionales en la tecnología de la comunicación, es el de alcanzar una comunicación abierta entre los sistemas y los componentes de distintos fabricantes. El estándar más importante para redes abiertas es el modelo de referencia OSI de la International Standardization Organization. Este modelo proporciona una descripción abstracta de la arquitectura de red y de los protocolos asociados. Todos los demás estándares

están basados en funciones definidas en este modelo. Este concepto también resulta aplicable a las redes LAN SINEC (Siemens Network Communication) que utilizan el TELEPERM XP y el TELEPERM XS.

La elección del medio de transmisión, cable triaxial y/o fibras ópticas, hace posible el cumplimiento de los requerimientos pertinentes de compatibilidad electromagnética. La elección del tipo de bus, Ethernet (IEEE 802.3) y/o Profibus (DIN 19 245) hace posible el cumplimiento de los requerimientos en cuanto a comportamiento de la transmisión. En aquellas aplicaciones en las que es necesario aportar insensibilidad a las interferencias electromagnéticas, aislamiento galvánico, o en extensiones de bus de hasta 4000 metros, el medio de transmisión utilizado es la fibra óptica.

La enorme importancia de la comunicación entre los componentes del sistema I&C en lo que a seguridad y disponibilidad de la planta se refiere, exige un alto grado de fiabilidad en la transmisión de datos. Para poder satisfacer esta exigencia los buses utilizados deben tener un diseño tolerante a fallos.

TELEPERM XS

Los códigos y los estándares nacionales e internacionales imponen exigencias especiales en cuanto a las tareas de I&C relacionados con la seguridad de una central nuclear. Los aspectos contemplados son:

- Tolerancia a fallos
- Robustez
- Cualificación

Para poder satisfacer plenamente todas estas exigencias sin que por ello las tareas de automatización operativas resulten innecesariamente costosas debido a criterios de excesivo conservadurismo, se desarrolló el sistema de I&C TELEPERM XS como complemento al sistema TELEPERM XP. Está basado en gran medida en dispositivos estándar seleccionados por sus peculiaridades en materia de calidad y adaptados por medio de medidas específicas de diseño. La Cualificación exigida por los códigos y estándares nucleares se logra a través de la realización de pruebas complementarias y de exhaustivas pruebas de fábrica.

PROTECCIÓN DEL REACTOR

La exigencia más importante en materia de sistemas de I&C relacionados con la seguridad en centrales nucleares, concierne al equipo de automatización para la protección del reactor. Las características necesarias en lo que a tolerancia a fallos respecta exigen un sistema distribuido de ordenadores múltiples. Los dispositivos de automatización utilizados deben permitir la implementación y supervisión de estructuras topológicas ampliamente distribuidas.

La superposición del requisito funcional, por el cual algunas acciones de protección se deben iniciar con suma rapidez y plena seguridad para evitar situaciones de riesgo para la central, determina altísimas exigencias de comportamiento.

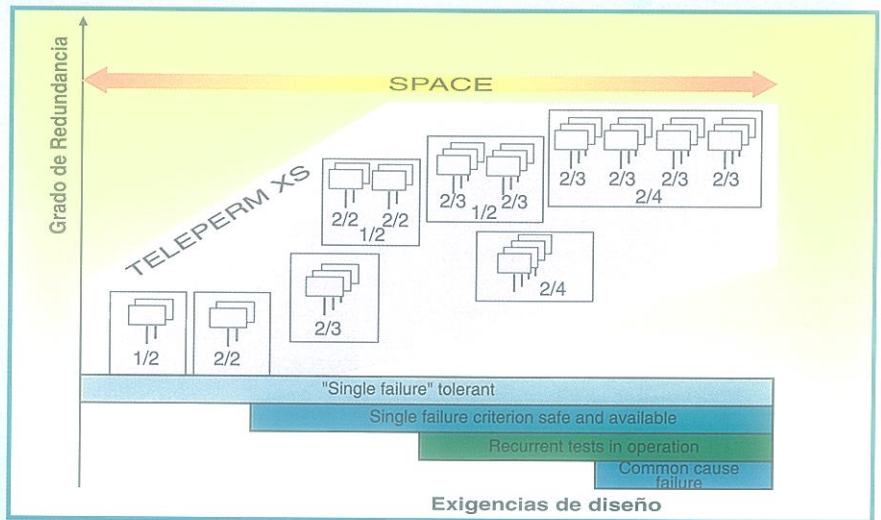
El TELEPERM XS cumple con estas exigencias a la vez que dispone de características del sistema que soportan la implementación y el funcionamiento de arquitecturas altamente redundantes, espacialmente distribuidas. Por ejemplo, se pueden implementar con cada

AUTOMATIZACIÓN

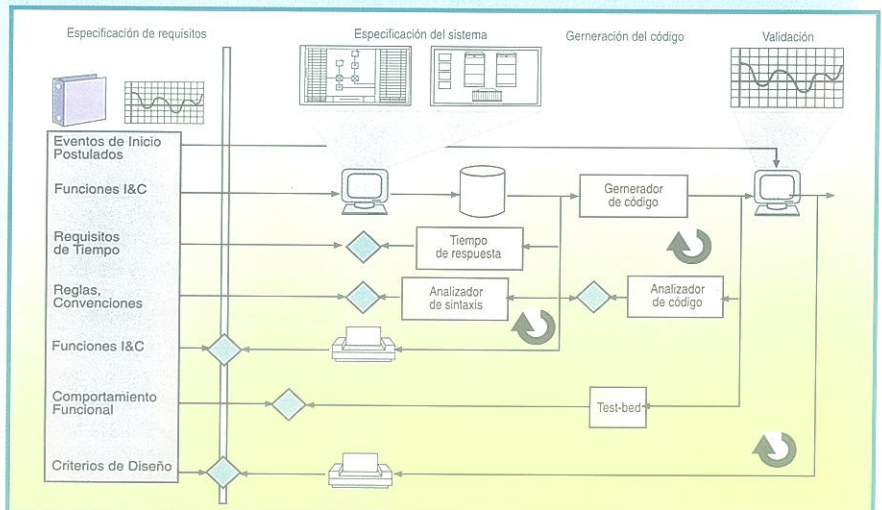
En automatización, se implementan las tareas de I&C de control, de señalización, supervisión y protección. Para lograr esta implementación, el equipo de automatización adquiere señales de medición procedentes del proceso, utilizando módulos de entrada analógica o binaria y ejecutando el necesario procesamiento de datos y los comandos de salida enviados a los actuadores de la central (motores, válvulas, etc.) a través de módulos de salida analógicos o binarios. De esta forma, se implementan secuencias de puesta en marcha y de parada, se hacen cambios de carga, se toman las medidas adecuadas para responder a perturbaciones y, en caso de necesidad, se originan disparos de protección.

Para la implementación económica de un sistema de control de proceso, el poder adaptar la estructura de la automatización a las necesidades de flexibilidad de la central constituye un aspecto de máxima importancia. Significa esto que la automatización debe estar estructurada de forma orientada hacia las tareas. Tanto el TELEPERM XP como el TELEPERM XS brindan libertad para atender estas exigencias de manera económica. La concepción en escala del sistema garantiza que tanto los lazos de control autónomos individuales como los sistemas de mediana capacidad con estaciones de control locales o las centrales nucleares completas, con grandes salas de control por pantalla, se puedan implementar económicamente. Se puede conectar todo el equipo de automatización en una LAN común de la central nuclear, para que toda la información disponible referente al proceso se pueda evaluar de forma centralizada. Esta conexión resulta efectiva para supervisar ininterrumpidamente la consistencia de la información de modo que al operador sólo llegue información validada.

F IV - Ámbito de aplicación



F V - El proceso de diseño del sistema



topología requerida dentro de los trenes de redundancia, sistemas de I&C con un alto grado de fiabilidad y de disponibilidad formados por dos, tres o cuatro trenes de redundancia. El aislamiento eléctrico de las unidades de automatización se logra primordialmente por medio del uso de fibras ópticas para las comunicaciones. Para evitar un acusado estrechamiento en el interface entre los trenes redundantes de I&C y el nivel individual de control, se ha aplicado al procesador asociado con derecho a elección ("voting processor") una arquitectura de máxima fiabilidad y de máxima disponibilidad.

La robustez exige medidas de diseño que afectan tanto al hardware como al software. El uso de un hardware de encapsulado modificado permite al TELEPERM XS tolerar aceleraciones como las que se producen en caso de terremoto o de accidente de aviación. Las adecuadas medidas de blindaje de los armarios aseguran el cumplimiento de las más estrictas exigencias en materia de compatibilidad electromagnética. Además de las medidas de diseño del hardware, también se aplican al software reglas especiales de diseño. Una regla importante exige que el proceso de la central esté efectivamente desacoplado del comportamiento del sistema de I&C pues se debe garantizar que, en caso de perturbación o de accidente en la central, el proceso no pueda bajo ninguna circunstancia afectar a la I&C relacionada con la seguridad. Por este motivo los ordenadores del TELEPERM XS procesan todas las tareas cíclicamente y no utilizan programas controlados por sucesos. Es decir, la lectura de las señales de medición, la formación de señales límite y la salida de comandos de control siguen una secuencia invariable que no está relacionada con lo que pueda ocurrir en la planta ni en los demás ordenadores.

CONTROL E INFORMACIÓN DE LOS SISTEMAS DE SEGURIDAD

La mayor parte de las tareas de control del operador en las plantas nucleares, son de índole operativo. En los aspectos relacionados con la seguridad, la intervención manual -por ejemplo, la entrada manual al sistema de I&C de seguridad- tiene un ámbito muy limitado. Es más, el bajo potencial del mercado ni siquiera justifica el desarrollo y la Cualificación de interfaces de usuario basadas en pantalla, a través de las cuales se pudiera implementar una intervención manual en materia de seguri-

dad. Por lo tanto, el TELEPERM XS no tiene equipos dedicados para control y supervisión a cargo del operador. En cambio, los dispositivos convencionales de la sala de control se utilizan para la ejecución de comandos manuales relacionados con la seguridad. No obstante, el equipo TELEPERM XP se puede utilizar, por ejemplo, para visualizar o archivar variables del proceso adquiridas a través del sistema de I&C de seguridad como parte del control normal del proceso. Para ello, el sistema de I&C de seguridad se conecta a la LAN de la planta del TELEPERM XP a través de una puerta unidireccional.

INGENIERÍA

En general, se considera que el desarrollo de un software de aplicación específico de la planta, durante la implementación de sistemas de I&C relacionados con la seguridad es la actividad que más induce a cometer errores. Es por esto que para el TELEPERM XS la producción de un software de aplicación está sólidamente formalizada. Se pueden de esa forma evitar los problemas relacionados con los métodos individuales de trabajo del personal. El alto grado de automatización no sólo es aplicable a la producción del software sino que lo es también al proceso de verificación. Además de la función anteriormente descrita, también se integraron en SPACE, o sea, en el sistema de ingeniería del TELEPERM XS, las herramientas necesarias para la verificación y validación.

Con SPACE se utiliza el modelo de proceso que a continuación se detalla para desarrollar un software de aplicación específico de la planta. Las especificaciones de tareas están determinadas principalmente por ingenieros mecánicos, ingenieros de proceso, y físicos -como siempre- en forma de texto, de diagramas, de ecuaciones y de tablas que de esa forma se entregan a los especialistas de I&C. Los especialistas de I&C -es decir, los ingenieros de control, los ingenieros de comunicaciones, los físicos, los ingenieros informáticos y

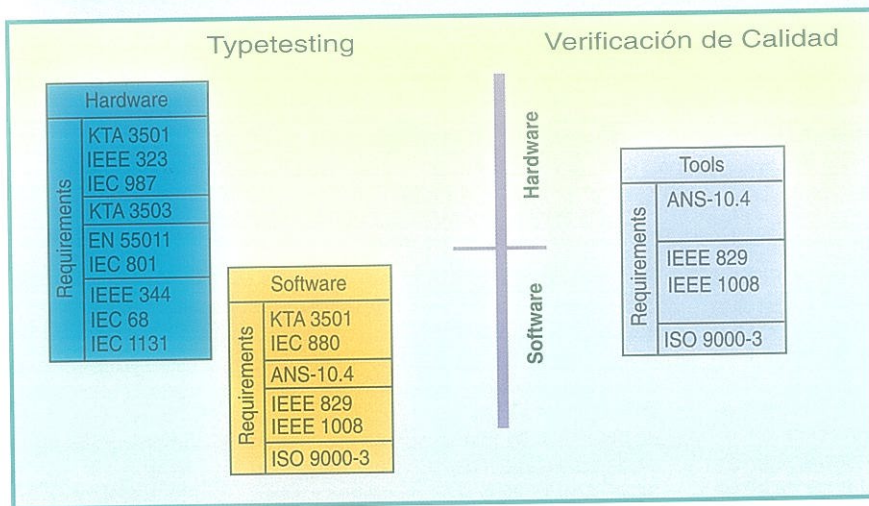
los matemáticos- leen e interpretan estas definiciones de problemas. Las preguntas que surgen para lograr una mayor comprensión dan lugar a discusiones sobre el sistema. Los especialistas de I&C elaboran entonces todos los datos y la información de una forma predefinida antes de utilizar el editor del sistema de ingeniería SPACE para especificar las funciones de I&C en forma de diagramas de función. Estos diagramas funcionales con

signos convencionales de presentación claramente definidos, pueden ser interpretados con fines de verificación por las partes que prepararon las especificaciones de la tarea y sirven además como documentación para los clientes.

Una vez que la especificación está completa, se puede verificar automáticamente según varios criterios, utilizando herramientas de análisis. Este análisis incluye características tan importantes como verificación de integridad y ausencia de ambigüedades. Esta verificación sólo se ha podido materializar a través del uso de métodos rigurosamente formales. Entonces, se entrega la verificación formalmente correcta a quienes originaron la especificación de ese requerimiento, que son a la vez los responsables de su versión. Con miras a lograr la máxima calidad del software de aplicación, el hecho de que el software de aplicación derive automáticamente de la especificación formal aportada por los especialistas constituye un hecho importante. Como el software fue generado por una herramienta automática, se puede verificar la consistencia del código generado con la especificación formal utilizando para ello una segunda herramienta informática. Una de las consecuencias de este método es que la verificación de la calidad del generador de código se puede mantener a niveles viables desde el punto de vista económico.

Una vez concluida esta etapa de verificación, el código está listo para ser sometido a prueba. A modo de opción para facilitar la prueba, se puede generar un entorno de prueba por medio del generador del código. Este generador aporta todas las ayudas necesarias para la eficiencia de la prueba. Por ejemplo, se pueden generar transitorios arbitrarios de señal para provocar respuestas específicas en todas las señales internas y se puede acceder a las memorias con el fin de evaluar su comportamiento funcional.

Si se pide al sistema una retroalimentación realista para evaluar el comportamiento funcional, el código generado se puede enlazar a un simulador de área parcial. En esas pruebas



funcionales, el simulador de área parcial simula el proceso termohidráulico de la central y proporciona la función de I&C con la medición de datos solicitada. La función de I&C - o sea, el objeto de la prueba- responde a esta medición de datos enviando comandos a los elementos finales de control que, a su vez, afectan el proceso termohidráulico de la central. En caso necesario, el simulador de área parcial puede simular transitorios de potencia, fallos de funcionamiento o accidentes.

CUALIFICACIÓN

Es especialmente durante el desarrollo de sistemas de nueva tecnología destinados a desempeñar importantes funciones de seguridad, cuando la cuidadosa observancia de las exigencias de seguridad desde el principio mismo cobra importancia como forma de evitar problemas que, en las etapas posteriores del proceso de desarrollo, pueden derivar en costosas modificaciones o, inclusive, en nuevos diseños. Se ha optado por lo tanto por una valoración paralela al desarrollo.

GRS ISTec, en representación del ente Bávaro de licenciamiento (BStMLU) llevó a cabo, desde 1988, evaluaciones continuas de los desarrollos. En Junio de 1992 concedió su aceptación al concepto de realización del sistema de I&C para funciones de seguridad de máxima categoría.

Pruebas de Homologación

La prueba de homologación tiene como fin demostrar que los módulos cumplen debidamente con los datos especificados en la correspondiente hoja de datos. Se compone de una parte teórica y de otra parte práctica. Los aspectos esenciales de la valoración teórica son el análisis del efecto de fallos, el análisis de carga crítica y el programa para las pruebas prácticas que comprende las pruebas funcionales y las pruebas de robustez (Influencias/acostecimientos internos y externos). La función de especialista autorizado (instituto independiente) es la valoración de los documentos elaborados por el fabricante, la evaluación del programa de pruebas prácticas, la participación en la realización de las pruebas prácticas (en la medida en que se considere necesaria) y la valoración de los resultados de la prueba.

Las pruebas de homologación de software se desarrollaron de igual forma que las pruebas de homologación de hardware. Esto es posible dado que, como regla general, nos encontramos con sistemas distribuidos con módulos de software reutilizables a los que se puede asignar configuración y parámetros de acuerdo con la aplicación a la que estén destinados.

PRUEBA DE HOMOLOGACIÓN DE LOS MÓDULOS DE SOFTWARE

Se contrataron desde octubre de 1992 con GRS ISTec, filial de TÜV-Nord. En junio de 1996 se concluyó la certificación del software del sistema y de los módulos de aplicación. La no-

vedad está dada por el hecho de que todo software reutilizable está sujeto a una prueba de homologación "análoga a las estipulaciones contenidas en KTA 3503". Este método representa una ventaja especial para el concepto TELEPERM XS porque el software de aplicación se compone en su totalidad de módulos de software reutilizables combinados por generadores, o sea, módulos de software que se utilizan de la misma forma que los módulos de hardware en sistemas de cableado permanente. Un módulo de software tiene una funcionalidad bien definida y un interface bien definido; los dos pueden ser sometidos a pruebas comparativas respecto de la especificación.

PRUEBA DE HOMOLOGACIÓN DE LOS MÓDULOS DE HARDWARE

Se contrataron desde febrero de 1994 con TÜV-Nord para la elaboración del análisis del módulo y de las especificaciones de prueba. La prueba práctica fue delegada al instituto de pruebas de TÜV Rheinland (ISEB). En junio de 1997 concluyeron las pruebas prácticas de los módulos de hardware, para poner fin a la cualificación.

La Figura VI presenta una visión panorámica de los principales estándares, que también son importantes para el desarrollo de la certificación.

REFERENCIAS

Actualmente existen varias referencias de los sistemas TELEPERM XP y TELEPERM XS. Adicionalmente a las más de cien referencias de TELEPERM XP en centrales térmicas repartidas en los cinco continentes, se ha instalado ó se preve instalar este sistema en diferentes centrales nucleares como son por ejemplo:

- Sistemas de ventilación C.N. Mühleberg (Suiza)
- Ordenador de Proceso C.N. Grohnde (Alemania)
- Sistema del Condemin C.N. Sta Maria de Garoña y Filtros del Condensado

TELEPERM XS por su lado tiene actualmente referencias en seis países que incluyen aplicaciones relacionadas con la seguridad y en sistemas no relacionadas con la seguridad. Algunos ejemplos son:

- Control Manual del Reactor C.N. Sta. Maria de Garoña
- Control y Limitación del Reactor C.N. Unterweser (Alemania)
- Protección del Reactor C.N. Bohunice (República Eslovaca)
- Control y Limitación del Reactor
- Sistema de Instrumentación Extra-Nuclear
- Protección del Reactor C.N. Paks (Hungría)
- Sistema de Instrumentación Extra-Nuclear
- Control de las Barras de Control C.N. Forsmark (Suecia)
- Indicación de la Posición de Barras
- Sistema de Instrumentación Nuclear C.N. Oskarshamn (Suecia)
- Rango Extendido y Rango de Potencia

ABREVIATURAS

- ANS American National Standard
- AS Automation System
- CP Communication Processor
- DIN Deutsche Industrie Norm
- EMC ElectroMagnetic Compatibility
- ES Engineering System
- ESFAS Emergency System Features Actuation System
- GRS Gesellschaft für ReaktorSicherheit
- IEC International Electrotechnical Commission
- IEEE Institute of Electrical and Electronics Engineers
- ISO International Standardization Organization
- ISTec Institut für Sicherheits Technologie
- KTA Kern Technischer Ausschub
- LAN Local Area Network
- OM Operation and Monitoring
- OSI Open System Interconnection
- SNAP Siemens Nuclear Automatic Protection
- SPACE Specification And Coding Environment
- TÜV Technischer ÜberwachungsVerein



Daniel Fernández es jefe de ventas de sistemas I&C y sistemas eléctricos para centrales nucleares en SIEMENS S.A. Estudió Ingeniería Eléctrica en Alemania y se tituló Ingeniero Superior. En 1988 se incorpora a la División KWU de SIEMENS A.G. en Alemania. Hasta 1990 trabajó en el área de ingeniería de Instrumentación y Control para sistemas operativos en centrales nucleares. Hasta 1996 ha actuado como ingeniero de proyectos y como responsable de ventas de sistemas I&C y sistemas eléctricos para ccnn en los países Hungría, España y México. En Noviembre de 1996 se incorporó en España a la División KWU de Siemens S.A..