

EL PROBLEMA DEL “EFECTO 2000” EN LAS CENTRALES NUCLEARES. NORMATIVA, GUIAS Y REQUISITOS REGULADORES

R. CID

DESCRIPCIÓN DEL PROBLEMA

El problema del “Efecto 2000” también denominado por las siglas Y2K (Year 2000) está originado por la representación del tiempo en los programas de ordenadores y microprocesadores. El tiempo (año, mes, día y hora) se mantiene en un ordenador mediante un reloj interno, y es transferido al sistema operativo y a las aplicaciones informáticas que manejan el tiempo como una de sus variables. En el pasado se ha representado el año con la dos últimas cifras con el fin de obtener un ahorro en la memoria disponible, por tanto, muchas aplicaciones informáticas están adaptadas a este formato de dos cifras. El problema se plantea en como interpretar los ordenadores y aplicaciones informáticas el cambio de siglo es decir el paso del año “99” al “00”. Dependiendo de su programación, pueden existir ordenadores ó aplicaciones que no hayan sido pensadas para el cambio de siglo e interpreten el año “00” como año 1900, esto puede originar problemas en aplicaciones que manejen fechas ó realicen cálculos en tiempo real (valores medios, incrementos, tendencias, controles de procesos, etc.).

Hay otras fechas que también son problemáticas, esto es debido a errores de programación en los algoritmos de manejo de fecha, por ejemplo el no reconocer el año 2000 como bisiesto ó la fecha 9-9-99 utilizada en algunas aplicaciones con otro significado como es el de fin de fichero.

Es importante señalar que el problema no está limitado a ordenadores, sistemas operativos, compiladores y aplicaciones informáticas, fácilmente identificables y normalmente dentro de un inventario de informática, también

puede afectar a equipos y sistemas que incorporan dentro de su electrónica microprocesadores como elemento de control secuencial de un determinado proceso, es a esto a lo que se le denomina “software embebido” y en muchos casos no es fácil su identificación incluso para el personal técnico.

COMO PUEDE AFECTAR A LAS CENTRALES NUCLEARES

Hay que señalar en primer lugar que en nuestro país los diseños originales de las centrales nucleares se basan en tecnología analógica (no incorporan microprocesadores) tanto en sistemas de control, monitorización y alarmas de sala de control y protección del reactor. Los ordenadores de proceso de las centrales no actúan sobre los elementos de control, tienen funciones tales como la supervisión del proceso, cálculos nucleares, registro de eventos y alarmas, registro de variables, representación gráfica, etc.

No obstante, las sucesivas modificaciones introducidas en los sistemas durante la operación de la planta han incorporado, en mayor ó menor medida dependiendo de cada planta, tecnología digital en sistemas de control, monitorización de sala de control, e incluso en algún caso, de protección del reactor. Los ordenadores de proceso no han cambiado su función básica aunque si se han ido adaptando a las prestaciones de los nuevos ordenadores, incorporando mayor número de señales, mayor frecuencia y capacidad de registro así como la implementación de distintas aplicaciones informáticas de ayuda al operador.

Atendiendo a las funciones básicas, los sistemas que pudieran estar afecta-

dos en las centrales nucleares podemos clasificarlos en tres categorías:

- Sistemas de seguridad, necesarios para la protección del reactor, parada segura ó mitigación de accidentes
- Sistemas ó componentes necesarios para mantener operable el proceso de generación de energía eléctrica.
- Ordenadores y aplicaciones informáticas cuyo fallo pueden afectar ó dificultar la operación a corto ó medio plazo.

En relación con los sistemas de seguridad, es a priori poco probable que se vean afectados, dado que la incorporación de sistemas digitales en equipos de seguridad ha sido muy limitada, la normativa es muy restrictiva y requiere un proceso de licenciamiento caso a caso. Las modificaciones en este sentido son bien conocidas, obedecen generalmente a soluciones genéricas del suministrador principal que han requerido un exhaustivo proceso de Verificación y Validación. Aun así es el primer nivel de preocupación desde el punto de vista de seguridad.

La utilización de ordenadores ó microprocesadores en sistemas necesarios para la operación normal de la planta, no está restringida en lo que a la normativa se refiere, su incorporación en cada planta es distinta, dependiendo de las necesidades por obsolescencia, falta de repuestos y de las inversiones que cada central ha realizado en la modernización de la instrumentación. Su importancia en estos momentos radica en que el fallo simultaneo de estos equipos en varios grupos nucleares podría hacer disparar a éstos, con la consiguiente repercusión en la estabilidad del Sistema Eléctrico Nacional, en la operación de los otros grupos nucleares y en las infraestructuras básicas del país.

El tercer grupo lo constituyen los sistemas computarizados que no tienen ninguna función directa sobre el control de la planta pero pueden dificultar el mantenimiento de la operación a corto ó medio plazo, estos sistemas son por ejemplo el ordenador de proceso y sus aplicaciones que monitorizan y supervisan las variables de proceso, el ordenador de seguridad física y control de accesos, paneles de monitorización y control de protección contra incendios, protección radio-lógica, ordenador y red de gestión de los que dependen funciones tales como la gestión de Especificaciones Técnicas de Funcionamiento, libro de turno y gestión de mantenimiento.



NORMATIVA, GUÍAS Y REQUISITOS REGULADORES

La industria americana (NEI junto con NUSMG) ha desarrollado una metodología para hacer frente a este problema, a través de un plan muy sistemático que establece las distintas fases del proyecto y que tiene como fin el de servir de marco general y guía al plan específico que ha de realizar cada central. El documento se denomina NEI-NUSMG 97-07 "Nuclear Utility Year 2000 Readiness", fue editado en Octubre del 97.

Esta metodología establece de una forma lógica las distintas fases que un plan director debe contemplar. Estas fases básicamente son:

- **Concienciación del problema:** Se ha de concienciar a la Organización tanto a los órganos de dirección como al personal del alcance y posible repercusión del problema, proporcionando información y facilitando la participación activa en el proyecto.

- **Inventario:** Se ha de inventariar todos los sistemas, componentes y aplicaciones que pudieran estar afectadas. Dentro de esta fase se incluye también la realización de un inventario de suministradores, la clasificación y priorización de los equipos dependiendo de su importancia y la petición de certificaciones a los fabricantes.

- **Análisis:** Incluye el análisis detallado de cada elemento del inventario, información aportada por el fabricante, documentación propia, pruebas realizadas, revisión de las aplicaciones desarrolladas internamente, para determinar si cada elemento inventariado está ó no está realmente afectado.

- **Desarrollo de medidas correctoras:**

Se definen las medidas correctoras para los elementos afectados que pueden ser tales como su sustitución, modificación de aplicaciones ó establecimiento de un plan de contingencias.

- **Pruebas de Verificación:** Se han de desarrollar procedimientos de prueba para cada tipo de equipo ó aplicación informática que confirme la información del fabricante y para la verificación de las modificaciones realizadas. Dada la complejidad de algunas aplicaciones informáticas puede ser necesario la realización de pruebas integradas que agrupan distintos elementos del inventario (Ordenadores, sistema operativo, software de comunicación y aplicaciones).

- **Implementación:** Realización de las medidas correctoras.

- **Información y cierre del proyecto:** Se requiere un plan de calidad en el proceso el cual debe quedar documentado de una forma clara y trazable.

Aún realizando un gran esfuerzo en la revisión de los sistemas, componentes y aplicaciones potencialmente afectadas por el "Efecto 2000", debido a la propia naturaleza del problema no hay una garantía de su total resolución. Reconociendo estos riesgos, la industria nuclear americana ha desarrollado una guía que sirva de referencia para el establecimiento de un plan de contingencias individualizado para cada central. Este documento se denomina "Nuclear Utility Year 2000 Readiness Contingency Planning" (NEI/NUSMG-98-07, Agosto 1998)

Es un documento que proporciona una guía para desarrollar un plan de contingencias integrado, es decir, contempla la posibilidad de riesgos asociados a sistemas digitales internos, en los que aunque se hayan tomado acciones hay algún riesgo de que fallen e incluye los riesgos externos, circunstancias que no están bajo control directo del explotador

Los requisitos establecidos por el

Consejo de Seguridad Nuclear (CSN) se han basado en la regulación del país de referencia de la tecnología, en este caso EE.UU. Para el caso de CN Trillo y dado que este tema no tiene implicaciones específicas al diseño se ha seguido igualmente la regulación americana.

El CSN emitió una carta genérica a todas las centrales españolas (Mayo de 1998) endosando para su cumplimiento los requisitos establecidos por la NRC en la Generic Letter 98-01 "Year 2000 Readiness of Computer Systems at Nuclear Power Plant."

Mediante esta carta genérica se requiere a todas las centrales una respuesta escrita en 90 días indicando si están siguiendo un programa del año 2000 tal como el descrito en el documento de NEI, o similar. Requiere, así mismo, una confirmación de la finalización del programa ó de los trabajos pendientes para su conclusión, no más tarde del 1 de Julio de 1999. En principio el alcance de estos requisitos se establecía únicamente para los sistemas relacionados con la seguridad.

El Suplemento 1 a la carta genérica G.L. 98-01. Editado en Enero de 1999 pide a las CC.NN que de forma voluntaria incluyan en la respuesta a remitir (1-7-99) no solo los sistemas de seguridad sino también aquellos otros necesarios para la continuidad de la operación de la planta.

Adicionalmente, se recomienda por parte del CSN que se comparta la información y planes para abordar este asunto de forma conjunta entre los distintos explotadores de las centrales nucleares.

EVALUACIÓN Y PLAN DE INSPECCIÓN DEL CSN

En respuesta a la G.L.-98-01 las centrales confirman el seguimiento del documento de NEI como referencia o constataando que los diferentes suministradores han usado una metodología similar. Establecen unas previsiones de finalización de los trabajos para la fecha fijada (1-7-99) aunque algunas modificaciones podrían realizarse con posterioridad a esta fecha. También se establece como guía básica de referencia la metodología de NEI para la elaboración de los Planes de Contingencias.

En consecuencia al Suplemento 1 de la G.L. 89-01 referente a incluir en la respuesta al CSN las aplicaciones, equipos y sistemas potencialmente afectados por "El Efecto 2000" no sólo los relacionados con la seguridad, sino también los

que pudieran estar relacionados con la operación continuada de la planta. Se confirma que el plan director del Proyecto 2000, contempla estos equipos y se han priorizado como "CRITICOS" o "IMPORTANTES".

La coordinación entre las centrales se ha realizado a través de un grupo Ad-hoc dentro de UNESA en el que participan todas las centrales, en concreto se marcan los siguientes objetivos:

- Elaborar un Plan Director General sobre el que derivan y se desarrollan los planes específicos de cada planta.

- Desarrollado una base de datos genérica que incorpora los inventarios de sistemas y aplicaciones informáticas de todas las centrales, tiene como fin conocer y coordinar problemas y soluciones comunes.

- Preparar modelos de carta genérica para los suministradores y una homologación para las certificaciones de los mismos.

- Elaborar un procedimiento genérico de Plan de Contingencias.

- Elaboración de una Guía de Pruebas.

Durante el primer semestre de este año el CSN ha realizado un seguimiento del desarrollo de esta metodología a través de un programa de inspección (3 centrales) y reuniones con representantes del Grupo de UNESA que coordina los planes directores de todas las centrales.

Los resultados de estas inspecciones, confirman el seguimiento de la metodología referenciada en los planes directores de cada central. Se han inventariado entre 300 y 500 equipos ó aplicaciones potencialmente afectadas en cada planta, de las cuales, aproximadamente, una tercera parte, se han clasificado como críticas ó importantes.

El impacto en los equipos y sistemas de seguridad ó directamente implicados en la continuidad de la operación en las centrales inspeccionadas es muy limitado, no es así en cuanto a ordenadores de proceso, gestión y aplicaciones informáticas que están requiriendo grandes inversiones en algunas plantas. Los programas para la finalización del proyecto dejan algunos temas pendientes de cierre tras la fecha fijada.

PLANES DE CONTINGENCIAS

Desde un punto de vista del origen de los riesgos derivados del "Efecto 2000" los podemos dividir en dos categorías: Riesgos internos y externos.

Los riesgos internos están asociados con los componentes digitales de la planta a los que por determinadas circunstancias no se les ha dado una solución definitiva, debido por ejemplo a

problemas de disponibilidad para su sustitución. También pueden derivarse de componentes ó sistemas digitales internos que aunque se consideran como resueltos por haberse adoptado las soluciones previstas, debido a la importancia que tienen para la operación de la planta ó su complejidad, es recomendable estar preparados para un eventual fallo de tal componente, al objeto de reducir el impacto en la operación de la planta. Un ejemplo de estos elementos sería un sistema de control cuyas señales derivan del computador de proceso, contiene software embebido ó disponen de complejas interfases con otros sistemas.

Los riesgos externos son los derivados de circunstancias, condiciones ó sucesos que no están bajo control del explotador tales como:

- Perturbaciones en la red exterior (inestabilidades y fluctuaciones de tensión, fluctuaciones de carga, pérdida de los elementos de control de la red, ó incluso la pérdida de la energía eléctrica exterior)

- Pérdida de telecomunicaciones de la red pública ó privada.

- Pérdida de suministros esenciales para la operación de la planta (gasoil, hidrógeno, nitrógeno, etc.)

- Perturbaciones en el sumidero de calor (control de nivel ó caudal de agua del río).

Cada uno de estos riesgos, tanto internos como externos, constituyen los elementos para los que se prepara un plan de contingencias individual, básicamente es una hoja en la que se identifica el riesgo, se analiza las consecuencias de un posible fallo, se establecen las acciones de mitigación necesarias, se definen los medios tanto materiales como de personal necesarios, entrenamiento y el proceso de verificación y aprobación.

El plan de contingencias global lo constituye la recopilación de los planes de contingencias individuales así como los aspectos más generales como la organización, asignación de responsabilidades de dirección y realización, programa de recursos necesarios, coordinación entre departamentos y organizaciones exteriores y los planes generales de entrenamiento del personal.

En las inspecciones realizadas por el CSN se ha podido constatar que los Planes de Contingencias de las centrales están en proceso de elaboración siguiendo la metodología anteriormente indicada (NEI/NUSMG 98-07). Se ha elaborado un procedimiento genérico de Plan de Contingencias por parte del grupo de UNESA que cada central debe desarrollar a su caso específico.

La interacción de las centrales nucleares con la red eléctrica exterior es uno de los aspectos de mayor importancia.

En lo que a los aspectos de seguridad nuclear se refiere, las centrales están diseñadas para un suceso de pérdida de energía exterior de larga duración, disponen de Generadores Diesel de Emergencia redundantes y con autonomía para 7 días, su operabilidad está regulada a través de las vigentes Especificaciones Técnicas de Funcionamiento.

En cuanto a la repercusión sobre otras infraestructuras del país, se ha creado el Comité Eléctrico para el Efecto 2000 presidido por el Directo General de la Energía, en el que participan todas las empresas del sector, el MINER y el CSN, su objetivo fundamental es la elaboración de un Plan de Contingencias que minimice los riesgos y coordine las actuaciones, los recursos y los planes de contingencia de las distintas empresas ante una potencial degradación del Sistema Eléctrico Nacional debido al "Efecto 2000".



Rafael CID CAMPO es licenciado en Ciencias Físicas por la Universidad Autónoma de Madrid y Diplomado en Ingeniería Nuclear por el Instituto de Estudios Nucleares. Comenzó su carrera profesional en el departamento de Seguridad Nuclear de la JEN (actual Ciemat) en 1980 en tareas de licenciamiento en temas de I&C, pasando en 1983 a formar parte del Cuerpo Técnico del Consejo de Seguridad Nuclear. En este Organismo ha desarrollado funciones de Evaluación e Inspección durante la puesta en marcha, licenciamiento y operación de las Centrales Nucleares. Actualmente es Jefe de Área de Sistemas Eléctricos y de Instrumentación y Control del CSN, es miembro del "International Working Group on Nuclear Power Plant Control and Instrumentation" de la OIEA y ha sido nominado por el CSN como coordinador para el "Efecto 2000" ante la OCDE-NEA.