

NOTA TÉCNICA

Comisión Técnica de la SNE

CRITERIOS DE CUALIFICACIÓN DE SOFTWARE UTILIZADO EN SISTEMAS DE INSTRUMENTACIÓN

En las centrales nucleares actuales, los sistemas analógicos de instrumentación y control tradicionales están siendo progresivamente reemplazados por sistemas digitales. Estos sistemas con tecnología digital ofrecen importantes ventajas con respecto a los convencionales, tales como menores requisitos de calibración, mayor flexibilidad, mayor capacidad de integración o mejor representación de las condiciones de planta. Resuelven algunos de los problemas asociados a los anteriores equipos, tales como la deriva, y pueden proporcionar importantes funcionalidades añadidas, pero introducen la posibilidad de aparición de nuevos modos de fallo.

Los sistemas de instrumentación y control digitales pueden fallar de forma muy diferente a los sistemas analógicos. Pueden, por ejemplo, utilizar software que contenga fallos o anomalías de comportamiento que los procedimientos de prueba empleados con los equipos analógicos no detectan.

La tecnología digital está siendo ampliamente implantada en las centrales nucleares actuales. Se está aplicando en los sistemas de protección y control, en los secuenciadores de carga de los generadores diesel, en los monitores de radiación o en la medida del flujo de agua de alimentación: tanto en sistemas de seguridad como de no seguridad.

Los sistemas de I&C nucleares son bastante simples desde un punto de vista funcional y la tecnología digital tiene capacidad suficiente para asumir estas funciones. El objetivo es aprovechar las ventajas de esta nueva tecnología sin introducir nuevos retos de seguridad: cumplir los requisitos de seguridad y fiabilidad y no aumentar las posibilidades de que se produzcan disparos espurios. Para ello, deben tenerse en cuenta los siguientes aspectos:

- Posibilidad de aparición de fallos de modo común en el software. Normalmente cuando se tienen múltiples canales en un sistema de seguridad, se ejecuta el mismo software en todos ellos. Si hay un fallo en el software, éste podrá deshabilitar todos los

canales simultáneamente. Por ello, el control de la calidad del software es un factor esencial a la hora de evitar este tipo de fallos.

- Utilización de componentes desarrollados para otras aplicaciones. Debido a condicionamientos económicos, a la necesidad de utilizar equipos probados, y a la limitación de suministradores de equipos cualificados, la industria nuclear tiende a utilizar equipos comerciales, que han sido desarrollados por otras industrias y pueden ser adaptados a su tecnología. Pero es difícil comprobar que este software comercial no tiene problemas y que puede ser dedicado a servicios de seguridad nuclear, así como establecer las normas y criterios de aceptación a los que debe someterse.

- Control de la configuración. El operador debe conocer qué tiene en la planta y cuáles son sus capacidades, qué versión del software se está ejecutando y la seguridad de que éste ha sido verificado y probado.

Seguridad de los sistemas digitales

La seguridad de un sistema digital depende de la calidad del software. Un software seguro es un software que no contiene errores o que contiene errores mínimos. A diferencia del hardware, donde el número de defectos por unidad de tiempo causados por el deterioro puede ser estimado utilizando métodos estadísticos, los fallos del software adquieren una forma diferente. Son errores de diseño que no han sido detectados en los distintos pasos de los procedimientos de verificación y validación.

La seguridad del software es una actividad de garantía de calidad del software que se centra en la identificación y evaluación de los riesgos potenciales que pueden producir un impacto negativo en el software y hacer que falle el sistema completo.

Las características y consecuencias de los fallos de procesadores de tiempo real son:

- Ocurren de forma impredecible. La consecuencia es que cualquier fallo (originado

por software o por hardware) puede ser tratado como un suceso aleatorio de manera similar a los fallos hardware analógicos.

- Existen durante la ejecución del software en un procesador que interactúa con el entorno a través de sensores, actuadores, interfaces de comunicaciones y displays. La consecuencia es que es más significativo hablar de fiabilidad del software dentro del sistema sobre el que se ejecuta.

- Son el resultado de la interacción de sucesos con defectos en el software, firmware o hardware. Como consecuencia existe el riesgo de que no se tenga en cuenta este tipo de fallos en el proceso de desarrollo.

Esto implica un número de problemas complejos que van desde la interfase con el sistema software (sistema operativo, drivers de dispositivos, etc), al comportamiento no predecible, el manejo de errores y fallos, o la carga de procesamiento o temporización.

Dos son los parámetros fundamentales a la hora de determinar la calidad del software en un sistema de seguridad: disponibilidad y fiabilidad. La disponibilidad es la probabilidad de que un programa funcione de acuerdo con los requisitos en un momento dado. La fiabilidad se define como la probabilidad de operación libre de fallos de un programa software en un entorno determinado y durante un tiempo específico. (Se entiende como fallo la falta de concordancia con los requisitos del software. No se tienen en cuenta defectos en las especificaciones, a los que son atribuibles una proporción significativa de fallos en sistemas bien probados.). La medida de la fiabilidad de un sistema software es tanto posible como deseable en la determinación de la fiabilidad de un sistema de seguridad.

La fiabilidad se calcula midiendo la frecuencia de fallos y su importancia, la eficacia de los resultados de salida, el tiempo medio entre fallos (TMEF), la posibilidad de recuperarse ante los fallos y la previsibilidad del programa.

Debe considerarse tanto el software como el hardware cuando se persigue un objetivo de fiabilidad cuantitativo. Ha de considerarse el sistema software como un todo (hardware, software, firmware y aplicaciones). Debido a que éste puede fallar debido a causas diversas, es necesario considerar cómo determinar, medir y evaluar la probabilidad de