

# EQUIPAMIENTO DE UN PLAN DE SEGURIDAD INDUSTRIAL EN UNA INSTALACION NUCLEAR

Antonio PEÑA ROBLES

## INTRODUCCION

La Propiedad de una Instalación Nuclear, una vez superada la primera etapa del estudio sobre la Seguridad, que ha incluido el examen de la distribución física, la separación de sistemas, la compartimentación, los límites de protección con respecto a tuberías, bandejas y conductos de aire acondicionado más o menos accesibles, la elección de los modelos de agresor, etc., se encuentra enfrentada al problema de instalar «algo» que responda a esas necesidades de seguridad que, en teoría y de los estudios realizados, son necesarias para la protección de la Central.

En este momento es imprescindible que dicha Propiedad maneje de una forma eficiente el «sentido común», y plantee hasta qué punto una inversión extraproductiva, como es el caso de la Seguridad Industrial, pueda gravar los costes de explotación y mantenimiento.

El estudio del Equipamiento debe utilizar el concepto «coste-eficiencia» en forma impecable, sopesando la implementación de la Seguridad con la operación razonable de la Instalación.

Existen dos preguntas previas que deben marcar la selección de cada uno de los sistemas a instalar.

**¿Debe atenderse en forma estricta a una normativa extranjera, generada en el caso de la Seguridad, bajo circunstancias ajenas a las Nacionales?**

**¿Le compensa en cuanto a inversión mantener el síndrome de instalación nuclear en un Sistema ajeno a la producción de la Planta?**

**¿Es importante suprasofisticarse en un Sistema basado en la electrónica, mudante continuamente, o mantenerse en los justos límites que permitan cubrir los objetivos propuestos?**

A continuación se desarrollan someramente una serie de conceptos que pueden ayudar a responder las preguntas anteriores, sin pretender dogmatizar. La necesidad de ser breve, no permite un tratamiento completo de un problema tan complejo, pero si intenta marcar unos puntos básicos que ayuden a tomar decisiones, muchas veces muy importantes desde el punto de vista económico.

El esquema seguido se mueve de la periferia al núcleo de acuerdo con la figura 1.

## PROTECCION FISICA Y CONTROL DE INTRUSION

El objetivo de la barrera perimetral es, como elemento pasivo, retrasar una intrusión, y básicamente, una intrusión razonablemente inocente, porque un especialista puede atravesarla en segundos, al margen de lo que indiquen los programas del computador que simulan agresiones.

Independientemente de lo que se decida instalar, altura, alambre de espino, derrames, etc., se impone un sistema de detección, con objeto de conocer en qué momento ha sido traspasada.

Una vez más ante la Propiedad de la Instalación surge una duda razonable.

*¿Qué Sistema es tan maravillosamente fiable, que no detecte en falso, y que únicamente cuando actúe positivamente es que se ha producido una violación de la barrera?*

Probablemente todos y probablemente ninguno, pero no es objeto de este trabajo analizar los distintos métodos posibles y sus características positivas o negativas, sino fijar una filosofía de su aplicación.

Un sistema único de detección atrae continuamente la atención del operador. En cuanto existe una situación de anuncio de alguna irregularidad, le cabe la duda razonable del traspaso total de la primera barrera de retardo, moviliza la vigilancia para la comprobación y obliga a disponer en estado de aviso a las fuerzas de respaldo interiores disponibles.

¿Cuál puede ser la solución que modifique estos inconvenientes? En primer lugar, si la barrera es simple, evitar disponer un sistema de detección exclusivamente sobre la misma. Si se dispone sobre ella aparecerán todos los inconvenientes de alarmas falsas producidas por animales que existen dentro del área en exclusión, o por personas que han entrado circunstancialmente en la misma bien sea para cazar o con objetivos punibles para apoderarse de lo ajeno sin otra ulterior malicia.

En Francia se han desarrollado barreras electrificadas para ahuyentar a ambos intrusos, eventualmente sin provocar alarma, con el problema de que bajo determinadas circunstancias climáticas, la ronda perimetral puede encontrar víctimas involuntarias, pero perfectamente electrocutadas.

La solución recomendable para evitar este tipo de accidentes y mantener la fiabilidad de un sistema se basa en las siguientes consideraciones.



Antonio PEÑA ROBLES es Dr. Ingeniero del I.C.A.I., Director Gerente de SEPISA, Gerente de INITEC-SEPISA - Unión Temporal de Empresas.

- Establecimiento de una doble barrera, de tal forma que la exterior cumpla exclusivamente una función disuasoria, sin necesidad de estar alarmada.
- Establecimiento de un doble sistema de detección, entre ambas barreras, de tal forma que la aparición de estado de alarma en una de ellas, únicamente, provoque una situación de Alerta. Esto indica al operador, en primer lugar, que no ha sido traspasada de forma total la barrera de protección perimetral; en segundo lugar, que puede permitirse el apoyo de la Televisión, y en tercer lugar, que la inspección, por medio de una simple patrulla de vigilancia, puede determinar los límites del aviso.

En aquellos emplazamientos en los que es imposible adoptar una doble barrera por sus especiales determinantes, en cuanto a emplazamiento, debe ser recomendable con mayor motivo el empleo de doble sistema de detección, ya que en caso contrario los vigilantes no llegarían a atender tantas alarmas, o sería necesario aumentar su número, con la importante repercusión económica que representan.

## BARRERAS INTERIORES Y DETECCIÓN DE INTRUSION

Con respecto a las barreras interiores, las Propiedades deben hacerse de nuevo las siguientes preguntas, después de haber diseñado más controles de acceso a la Planta suficientes.

*¿Cuántos españoles se pasean con un Magnum 44 en el bolsillo y cuántos deben ser capaces de hacerlo dentro de una Instalación Nuclear?*

*¿No puede ser más peligrosa una simple llave inglesa bien manejada, que un arma de fuego?*

*¿Debe seguirse a ultranza la normativa de otros países, como Estados Unidos, donde el comercio de armas es libre, incluso entre las de calibre elevado?*

De nuevo debe usarse el «sentido común». Cualquier puerta homologada como antifuego de una hora y media soporta ampliamente impactos de bala de calibres que razonablemente pueden ser adquiridos en España.

Debe olvidarse, por tanto, de especiales sofisticaciones y en consecuencia inversiones elevadas; tanto cristal de muchas capas, normalmente más de las necesarias, y tanto espesor de chapa en

puertas, que únicamente incrementa sus herrajes y su costo.

Con respecto a los controles de intrusión interiores, únicamente deben utilizarse dentro del concepto de Control de Accesos, de otra forma lo único que se conseguirá es introducir en el interior de la Instalación a vigilantes armados, ante la presencia de alarmas falsas o espúreas, creando el riesgo de que se produzcan accidentes vitales por posibles disparos extemporáneos. Este hecho no debe ser normal, teniendo en cuenta la alta formación de las Empresas de Vigilancia que trabajan en Plantas Nucleares, y su cuidado en la selección y capacitación de su personal, pero un arma de fuego en el interior de este tipo de centro de proceso puede ocasionar daños irreparables.

## CONTROL DE ACCESOS

Existe el concepto de que la normativa generada en Estados Unidos está basada en el sabotaje cometido por un miembro de la planta al que le mueven razones reivindicativas, políticas, causadas por agentes exteriores, etc.

Todas las Compañías de Producción Eléctrica de origen Nuclear en Europa consideran como obsesiva esta hipótesis, basándose en la teórica fidelidad a ultranza de sus empleados.

Ante esto se considera necesario establecer la siguiente cuestión.

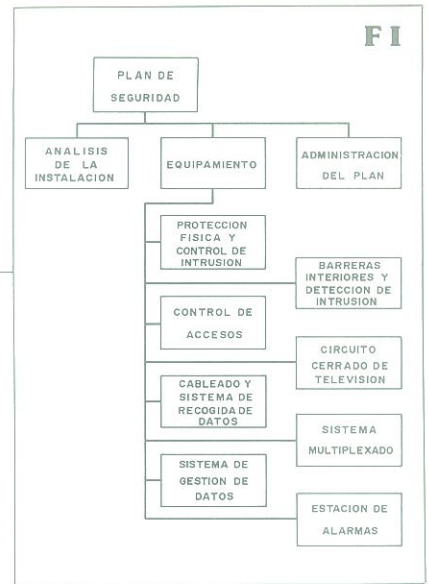
*¿Qué grupo ecologista plantea una posible agresión indiscriminada, aunque su motivación antinuclear sea aberrante, contra una planta en operación, sabiendo que puede originar un problema grave contra la comunidad, que automáticamente y de forma instintiva o consciente reaccionará contra su grupo?*

Sólo ataques militares enfrentando a distintos países se atreven a tal acción, y aún en estos casos procuran limitarlos a una destrucción convencional.

Es por esto por lo que se crea la necesidad de defender la Instalación frente a sus ocupantes. Ellos la conocen mejor y son conscientes de que una acción selectiva generará un daño mucho más profundo, e incluso mantendrá una central inactiva durante varios años, hasta que se restablezca su operatividad y sea de nuevo autorizada por los Organismos Licenciarios.

Ahora bien, ¿qué se debe controlar en un Control de Accesos?

En primer lugar, que entra quien debe entrar, y que puede ser identificado no sólo en el momento de la transac-



ción, sino en períodos de tiempo anteriores. Es decir, tener la capacidad de identificar al personal que accede a cada recinto controlado de forma continua a lo largo del tiempo, estableciendo en cada caso un registro de su recorrido.

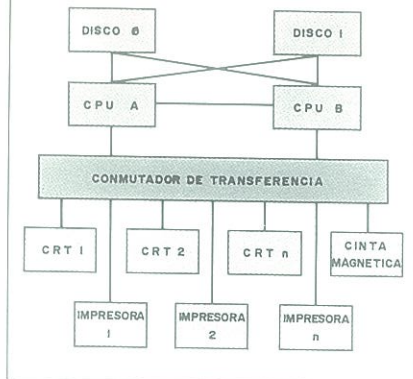
Una solución simplista sería la colocación en puestos de acceso determinados de Vigilantes que controlen el acceso. Esto puede ser solución en determinadas circunstancias (pruebas, recargas, mantenimiento pesado, etc.), pero su rentabilidad es nula, ya que no sólo no existe amortización, sino que el coste de personal se ve incrementado anualmente.

En estas condiciones es necesario equipar los accesos controlados de tal forma que permita el paso al usuario autorizado en función de su trabajo, o categoría dentro de la Instalación; que determine si la puerta se cierra en un tiempo predeterminado; que controle si el acceso se mantiene abierto o que existe un falso cierre, sin que el resbalón esté introducido en su alojamiento.

Es clásico descubrir el fenómeno en muchas plantas en explotación del *gate tail*; es decir, el paso a través de un acceso determinado, normalmente de forma bienintencionada, no sólo de la persona autorizada, sino de otros compañeros que necesitan realizar algo en aquel recinto específico.

La Propiedad de la Planta debe atender, por tanto, a los siguientes aspectos:

- Establecer un sistema de control de acceso por medio de lectores de Tarjeta codificada.
- Elegir un sistema de codificación que sea lo suficientemente inalterable e indescifrable, huyendo básicamente de las tarjetas magnéticas clásicas, fácilmente decodificables con imanes comunes. La expresión «tarjeta magnética» se ha convertido en una denominación genérica, en lugar de «tarjeta codificada», que muchas veces ha permitido la introducción de productos de baja seguridad en propiedades no avisadas, sin que esto quiera decir que las tarjetas magnéticas de alta potencia no sean válidas.



- Ante la gran dificultad, en la actualidad, de la identificación física del usuario frente a un acceso controlado (control por huella dactilar, escritura, voz, etc.), deben establecerse procedimientos administrativos de gestión del Sistema de Seguridad que mantengan las Tarjetas Codificadas en el interior de la Instalación, entregándose por medio de identificación visual a la entrada, y recogiendo, con un control de ello, a la Salida de la misma.
- Controlar por hardware o software, y preferiblemente por ambos, el control de apertura del acceso, de tal forma que bien pasado un período de tiempo predeterminado, o bien producido el cierre físico del mismo, un intento de penetración genere una alarma específica.
- Seleccionar el hardware propio del acceso, fundamentalmente el cerraportas, de tal forma que su accionamiento sea uniforme, regulable, y no produzca rebotes innecesarios en el momento del cierre. Por otra parte, tanto las cerraduras como los cerraderos deben ser fuertes, pero no innecesariamente superhomologados.

## CIRCUITO CERRADO DE TELEVISION

El Sistema de circuito cerrado de Televisión es básicamente un Sistema de apoyo, lo cual no quiere decir que sea innecesario, sino que es complementario de los Sistemas de detección.

Las características mínimas que deben solicitarse del mismo son su simplicidad de manejo y evitar la fatiga del operador. Está demostrado que ni aún el vigilante más adiestrado y motivado es capaz de mantener su atención de una forma sistemática sobre más de cuatro monitores, y esto en régimen de dedicación exclusiva a esta tarea y durante más de tres horas.

En este típico subsistema de control debe hacerse especial hincapié en los siguientes puntos:

- Capacidad de asociación de las alarmas producidas en cualquier zona del sistema, con cámaras de CCTV complementarias, por medio del software operativo, de tal forma que en caso

de producirse una alarma en ellos, las imágenes correspondientes sean exhibidas en monitores determinados, y anunciadas de tal forma que atraigan la atención del operador.

- Grabación instantánea de las cámaras asociadas a una zona determinada en caso de alarma, de tal forma que sea posible reproducir posteriormente las incidencias acaecidas. Con inmenso respeto a los operadores de sistemas de Seguridad, se considera recomendable el uso de grabadores profesionales, evitándose tentaciones de visionar películas comerciales, aunque sean en blanco y negro.
- Acceso directo y mediante uno o dos teclados como máximo a la totalidad de las cámaras, incluso las móviles, ya que de otra forma, en caso de alarma, el operador necesitará el empleo de más de dos manos para atender al control, registro y seguimiento de la misma.
- Localización de todos los controles en un espacio del orden de un metro cuadrado como máximo, situado preferentemente a la derecha del operador (el mundo, desgraciadamente, no está pensado para los zurdos), de tal forma que el manejo sea prácticamente instintivo, sin dejar de atender a las imágenes que observa, incluyendo el uso de cámaras móviles.

## CABLEADO Y SISTEMA DE RECOGIDA DE DATOS

Este es un punto crucial con respecto al aspecto económico al equipar un Sistema de Seguridad Industrial.

Una Propiedad «no concienciada» puede gastarse varios miles de millones de pesetas más de lo necesario, por mantener el «síndrome nuclear» del que hemos hablado en la introducción, sin mejorar en absoluto la funcionalidad del Sistema.

De nuevo es interesante recalcar que un Sistema de Seguridad Industrial, en una Instalación Nuclear, ni está ligado con la producción, ni directamente con la Seguridad Nuclear, y que, por tanto, **ni es sísmico, ni es clase, ni está sometido a garantía de calidad**, a pesar de mantener sus objetivos y su funcionalidad.

Como criterios básicos que deben ser mantenidos por la Propiedad deben establecerse los siguientes:

- Elegir un sistema donde esté perfectamente establecido el modo de supervisión de línea (un 5 % y un 30 % es totalmente admisible para alarmas y tampo), de tal forma que un tratamiento convencional del cableado sea admisible. Cualquier anomalía será detectada por el sistema.
- Procurar diseñar el sistema de Seguridad como cualquier otro no nuclear de la Planta, integrando su trazado dentro del desarrollo de la Ingeniería Principal. De esta forma será un siste-

ma más; el llenado de bandejas se optimiza, y en el momento del montaje queda integrado en el general de la Instalación.

- Huir, de nuevo se insiste, de la mentalidad nuclear en el tratamiento del Sistema. El empleo masivo de conductos metálicos debe ser limitado, y el uso de cables especiales, retardantes a la llama, está únicamente justificado en función del recorrido de los mismos.
- En áreas exteriores se debe evitar el manejo de conductos metálicos, el PVC debe ser suficiente, con el subsiguiente ahorro en coste. Sólo sistemas mal elegidos necesitan especiales protecciones.

En resumen, las Propiedades deben evitar el tratamiento sofisticado de algo, que si está bien diseñado, ni lo pretende, ni lo es.

## SISTEMA MULTIPLEXADO

Dada la experiencia de transmisión de información en la actualidad, no cabe la posibilidad de un Sistema que no multiplexe la señal, tanto de alarma, y también como la del control de accesos, y todas sobre un mismo cable.

Ahora bien, existen unas consideraciones mínimas a establecer sobre un Sistema de transmisión de datos multiplexado.

*¿Tamaño grande o pequeño de la unidad multiplexora?* Ni grande ni pequeño, el justo. Después del primer análisis de la Instalación, con la información razonable que existe, se debe seleccionar el número y equipamiento idóneo.

Sin embargo, una instalación nuclear hasta que entra en operación e incluso hasta su primera recarga es una personalidad cambiante. Pasa de trescientas a quinientas zonas a controlar o a la inversa. Se está inmerso en un proceso creativo que si parte de un sistema estático, cerrado desde el origen, será incapaz de acoplarse a las continuas necesidades.

El multiplexor debe, por tanto, ser una unidad altamente flexible, que mediante simple inserción de tarjetas de circuito impreso sencillas pueda variar su capacidad en más y menos un 50 % como mínimo.

*¿Qué ocurre si el sistema necesita finalmente añadir nuevas unidades de multiplexado de datos y está operativo?* El Sistema debe tener la capacidad de ampliación simplemente desconectando unos cables e introduciendo la nueva unidad. De este punto se tratará con más amplitud en la siguiente consideración.

*¿Cuál es la conexión más perfecta con el Sistema de computadores?* Ante esto, el problema se subdivide: **Cómo y Con qué.**

En primer lugar, **Cómo.** Existen tres métodos básicos.

Este número de



estará presente en

 **Expoquimia '84**

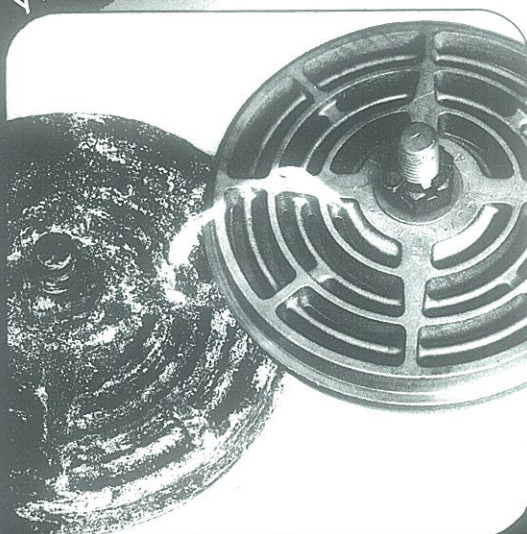
19 - 24 Noviembre 1984

Con esta ocasión  
deseamos a  
sus expositores,  
congresistas y visitantes,  
el mayor éxito  
para que sus objetivos  
de inter-comunicación  
técnica y científica  
constituyan un  
nuevo avance  
en el desarrollo  
de la  
**Química española  
y de los Sectores  
a ella vinculados:  
Ingeniería,  
Bienes de Equipo,  
Instrumentación  
y Servicios.**

**Nosotros  
sabemos  
qué deben  
hacer vds.  
para que esto  
no suceda**

... y no hacemos  
ningún secreto  
de nuestro saber.

*Déjense aconsejar por nuestros técnicos especialistas  
y pidan Vds. hoy mismo documentación detallada.*



Nuestra oferta — Sus ventajas.

- Reparación de válvulas por especialistas.
- Comprobación de la reparación con los más modernos métodos de medición.
- Renovación de los elementos de cierre.
- Cambio de las partes móviles.
- Disminución de su inmovilizado de almacén.
- Y finalmente, asesoramiento de una empresa líder en válvulas de compresores con un aval de 85 años de experiencias.

**HOERBIGER**

**HOERBIGER ESPAÑOLA, S.A.**  
Polígono Industrial "El Nogal" de Algete  
Km. 5,500 Ctra. Madrid-Algete - SPAIN  
Tel. 62 90 900, 62 90 901, 62 90 851. Télex: 22403 hses-e

- En estrella, donde cada unidad o serie de ellas se unen directamente con el Sistema de Gestión de Datos.
- En anillo, donde cada unidad está interconectada con la anterior y siguiente, así hasta el Sistema de Gestión de datos.
- En «margarita», donde grupos de unidades multiplexoras están conectados entre sí como anillos cerrados, pero no formando parte de un lazo único.

Indudablemente cualquier comunicación que forma anillo es más fiable que una comunicación radial; permite la transmisión bidireccional, mantiene la comunicación con el sistema de gestión de datos en caso de corte o avería en la línea de transmisión, y no sufre interrupción en la operación en caso de ser necesaria la adición de una o varias unidades nuevas.

En segundo lugar, *Con qué se realiza la transmisión.* Analizando, básicamente, de la forma más fiable, con la mejor calidad, con lo más fácilmente disponible y, por supuesto, con lo que menos gravamen económico representa para la Propiedad.

El Sistema idóneo para la transmisión debe ser, por tanto, uno o dos pares trenzados y apantallados, cuya adquisición es fácil, existen en cualquier instalación nuclear o convencional, tanto en período de instalación como de explotación.

Debe huírse, por tanto, de sistemas que exijan cable especialmente sofisticado (Coaxial, por su molesto manejo, fibra óptica, etc.), de uso muy limitado durante la ejecución de la planta, y difícilmente sustituibles en plazo razonable.

## SISTEMA DE GESTION DE DATOS

Un Sistema, como el analizado, en el que se genera un número elevado de información que es necesario procesar, exhibir y almacenar debe estar gobernado por medio de un computador.

Sin embargo, al seleccionar la configuración más idónea debe tenerse en cuenta que un problema en el computador provoca la caída de la totalidad del Sistema de gestión, y genera la necesidad de suplir, por medio de Vigilantes, todas las funciones del mismo, con el subsiguiente incremento económico.

Con este motivo se acude a la solución de configuraciones duales en las que existen dos computadores y dos discos interconectados todos entre sí, de tal forma que la información sea procesada continua y simultáneamente por todos los elementos.

Este modelo de configuración indicado en la figura 2, es conocido como «Previsión de doble fallo»; es decir, admite, manteniéndose el Sistema totalmente operativo, el fallo simple simultáneo de dos elementos cruzados. Puede

fallar, por tanto, el CPU A y el disco 1, sin alteraciones de funcionamiento.

El uso de cinta magnética, dentro de la configuración, no es imprescindible, pero sí recomendable, la inversión a realizar por la Propiedad es mínima, comparada con el coste del Sistema y, sin embargo, obtiene una herramienta que le permite almacenar información histórica por medio de volcado desde los discos, hacer cargas rápidas de programa y pasar test de diagnóstico a todos los elementos del Sistema.

Por último, y a la hora de la toma de decisión por parte de la Propiedad al seleccionar la configuración, se considera altamente recomendable que el lógico de base permita la ejecución de multita-reas. De esta forma se pueden realizar cambios *on line* en el software de aplicación, sin necesidad de detener la operación del sistema, manteniéndose de forma simultánea el procesamiento de la información en tiempo real en todos los elementos.

Con respecto al «software» de aplicación, únicamente tres observaciones cruciales para una Propiedad.

- Que sea modular y, por tanto, adaptable a la situación en continuo cambio durante el diseño del Plan de Seguridad de una Instalación Nuclear.
- Que tenga un sistema de exhibición de datos de manejo sencillo y fácil de comprender por el operador, y que permita la exhibición en pantalla de por lo menos diez alarmas simultáneamente, así como el reconocimiento y borrado de las mismas, en forma totalmente aleatoria, independientemente de su orden de exhibición.
- Que esté suficientemente probado en instalaciones similares. Nadie desea ser objeto de experimentaciones más o menos afortunadas, que al final le obliguen a «importar temporalmente» un técnico extranjero que desarrolle la aplicación.

## ESTACION CENTRAL Y SECUNDARIA DE ALARMAS

La totalidad de las consideraciones anteriores están basadas en la generación de un Sistema de Seguridad Industrial con un índice de fiabilidad lo más elevado posible, dentro de unas consideraciones económicas razonables.

Ahora bien, después de haber seleccionado equipos, transmisión de datos y sistemas de gestión de los mismos, de tal forma que no se vean alterados por un fallo simple, casual o no, no parece lógico perder la fiabilidad establecida, precisamente en la cabeza del conjunto.

*¿Qué sucede si el operador de la instalación de Seguridad posee un trastorno temporal reversible o irreversible?*

*¿Qué ocurre si el operador es extorcionado directa o indirectamente?*

*¿Qué ocurre si un trabajador de la Planta sufre los mismos efectos mencionados anteriormente y toma en forma agresiva el centro de seguridad industrial?*

Estos puntos, someramente apuntados, conducen al concepto de Estaciones de Alarma redundantes y atendidas las veinticuatro horas del día. Una Instalación Nuclear es tan vulnerable durante las horas oficiales de oficina como durante las horas, en teoría, de reposo. Siempre hay alguien circulando en su interior, y siempre debe estar productiva, o en gestión de ello.

Aunque se sigue manteniendo la denominación de Estación Central, y Estación Secundaria, la realidad es que para asegurar un correcto funcionamiento del Plan de Seguridad, ambas deben ser capaces de operar en cualquier caso indistintamente, debiendo establecerse controles tanto por hardware como por software que mantengan determinados niveles que permitan un acceso restringido a instrucciones específicas.

Suele ser recomendable establecer como mínimo cuatro niveles de acceso. El más inferior permitirá el acceso simple de cualquier operador o persona que habitualmente tenga contacto con el sistema. El segundo escalón permitirá el acceso únicamente al operador de turno, que fijará, al principio del mismo, una clave personal. En tercer escalón, para la ejecución de otro grupo de instrucciones sería necesario el permiso, vía software, del operador de la otra consola. Por último existiría un nivel de alta confidencialidad que necesitaría para su acceso la introducción de una clave en el sistema, y el empleo de un conmutador de llave, la cual estaría en poder del Jefe de Seguridad de la instalación.

En relación con la disposición física de las consolas, que debe permitir su manejo completo por un único operador, sin necesidad de moverse de su puesto de trabajo, se recomienda que las de ambas estaciones sean exteriormente iguales, facilitándose de esta forma el entrenamiento del personal.

## CONCLUSION

El tratamiento, necesidades y análisis del Equipamiento de un Plan de Seguridad en una Instalación Nuclear desborda los límites de un artículo por muy generosa que sea su extensión.

En cualquier caso, y como se comentó en la Introducción, la idea básica que ha guiado este trabajo ha sido el Equipamiento desde el aspecto conceptual y de optimización económica.

No se ha entrado en estudios detallados sobre equipos y marcas específicas, ni sobre la totalidad de funciones y operatividad del Sistema de Seguridad, que puede ser objeto de tratamiento en futuras publicaciones.