

# Control de configuraciones peligrosas a través de matrices de dependencias en centrales nucleares

**Antonio Torres Valle, Manuel Perdomo Ojeda**

Instituto Superior de Tecnologías y Ciencias Aplicadas (InsTEC)  
Ave. Salvador Allende, esq. Luaces, Plaza. Ciudad de La Habana, Cuba  
atorres@instec.cu, mperdomo@instec.cu

## Resumen

El control de configuraciones peligrosas en instalaciones con riesgo asociado se ha realizado habitualmente a través de la consulta de los listados de conjuntos mínimos de corte obtenidos durante los análisis de riesgo previos de estas o con el uso de monitores de riesgo, los que permiten detectar on-line tales configuraciones. Esta tarea es de gran importancia por cuanto, ante una demanda real, las configuraciones representan la indisponibilidad total de sistemas o, en el mejor de los casos, el deterioro de la disponibilidad de ellos, coadyuvando así al daño de la instalación. Por otra parte, las matrices de dependencias se han utilizado habitualmente como parte de los Análisis Probabilistas de Seguridad para estudiar las interfaces entre sistemas tecnológicos. En el trabajo se presentó un método cualitativo de control de configuraciones peligrosas basado en matrices de dependencias. El algoritmo informatizado en el código CONFIGURACIÓN, se puede aplicar sin necesidad de Análisis Probabilistas de Seguridad previos ni uso de monitores de riesgo. Esta posibilidad de análisis constituye una novedad. La sencillez del método justifica su extensión a instalaciones donde estas herramientas no se han desarrollado, permitiendo así la detección de las configuraciones peligrosas en caso de simultaneidades de fallos, rotaciones de equipos, pruebas y mantenimientos. Una primera versión de este sistema se utiliza como ayuda en la operación de la Central Nuclear de Embalse.

## HAZARDOUS CONFIGURATIONS CONTROL THROUGH DEPENDENCE MATRIXES

### Abstract

The hazardous configurations control in risk related facilities has been carried out by the analysis of minimal cut sets obtained from previous risk analysis. A more complete option is the risk monitoring for the on-line detection of these configurations. This is a very important task in cases of real demand, because these configurations represent a degraded condition of system reliability and, which in the worst case, may result in the system fault, and consequently, in the loss of the facility. On the other hand, the dependence matrixes are generally used in studying the interfaces among technological systems in PSA. The paper presents a configuration control method, based on dependence matrixes. The algorithm is included in a computer code called CONFIGURACION, to determine these situations in a qualitative way, without previous PSA results or using a Risk Monitor. This possibility of analysis is a novelty. The simplicity of the method warrants its application to facilities where these tools have not been developed, thus allowing the detection of hazardous configurations in case of simultaneous failures, equipment rotations, test and/or maintenances. The first version of this configuration control system is used as an aid in the operation of NPP Embalse.

**Key words:** configuration control, risk assessment, matrixes, c codes, on-line control systems, probabilistic estimation

## Introducción

El control de configuración (combinación de indisponibilidades de equipos) es una tarea recomendada por expertos en la explotación segura de plantas con riesgo asociado a su explotación, fundamentalmente centrales nucleares [1], aunque la experiencia se ha extendido a procesos de naturaleza no nuclear [2].

Una configuración peligrosa puede aparecer en su caso más grave cuando afecta a todas las redundancias de un sistema de seguridad mitigador. Por lo que se conoce como configuración crítica, pues tal combinación de indisponibilidades de equipos corresponde con uno o varios de los conjuntos mínimos de corte que determinan el fallo del sistema. También es preocupante la aparición de configuraciones de salida de servicios de equipos muy próximas a una configuración crítica, ya que un simple fallo u otra causa de indisponibilidad, puede convertirlas en estado crítico. Para evitar estos riesgos, se limitan los períodos de explotación de las instalaciones en función de los tiempos fuera de servicio de las redundancias de sus sistemas de seguridad, por especificaciones técnicas de funcionamiento o por políticas y principios [1, 3,-5].

La aparición casuística de configuraciones peligrosas, en ocasiones críticas, han provocado accidentes como el de la Isla de las Tres Millas [6, 7] donde, por un error de mantenimiento, las dos bombas auxiliares de alimentación quedaron fuera de servicio y ayudaron a completar la secuencia accidental que provocó la fusión parcial del núcleo del reactor, con consecuencias para la planta y para el programa nucleoeenergético norteamericano y mundial.

Entre las aplicaciones del Análisis Probabilista de Seguridad (APS) más importantes aparecen las tareas de control de configuraciones de equipos fuera de servicio y de determinación de los tiempos permisibles fuera de servicio (AOT) de las redundancias [3,4;8]. En muchas especificaciones técnicas de planta aparecen claramente declarados estos parámetros, que son producto de la utilización de los resultados de APS previos [6,7-11]. A este nivel no se pueden enunciar todas las configuraciones críticas, ya que en ocasiones se trata de miles o millones de conjuntos mínimos de corte. De esta forma, lo que se procura es prohibir las combinaciones más probables y de menor orden (menor cantidad de equipos indisponibles simultáneamente).

Como las causas de las indisponibilidades son varias (fallos propios, indisponibilidades por pruebas

o mantenimientos y rotación de equipos) y la cantidad de equipos a controlar en una instalación compleja es elevada, es posible que algunas combinaciones peligrosas escapen a estos mecanismos de control. Por ello se recomienda, una vez concluido el APS de la instalación, contar con especialistas que contrasten las combinaciones de equipos fuera de servicio en cada situación operativa, con las listas de conjuntos mínimos resultantes del análisis de riesgo, para advertir la existencia de configuraciones peligrosas. Ello resulta a veces imposible, dada la dinámica de explotación de las instalaciones. Por tanto, una solución completa a este tema es contar con un monitor de riesgo [8] soportado en los resultados del APS [9-12], el cual vigile en tiempo real (on-line) las indisponibilidades de los equipos y advierta inmediatamente al personal operador de una situación peligrosa. Un monitor de riesgo [5, 8, 13] tiene implícitas las potencialidades de la reducción booleana inherente al APS, por lo que puede vigilar millones de configuraciones peligrosas, y además incluir magnitudes cuantitativas que indican cuánto se aleja una situación operativa particular del riesgo originalmente calculado con todo el equipamiento disponible [9-12]. Como se observa, la solución de estas situaciones es compleja pues necesita de un personal calificado, competente en herramientas como el APS y conocedor de sus resultados o de un monitor de riesgo costoso, que requiere igualmente de personal especializado.

Como alternativa para solucionar este problema se diseñó un sistema de control de configuraciones peligrosas basado en matrices de dependencias, el cual consiste en la informatización de una tabla especial de dependencias que contiene los equipos de los sistemas frontales y soportes (indispensables para la explotación segura de la instalación objeto de análisis) así como sus interfaces. Por la simplicidad del método, se puede aplicar a instalaciones de interés en las que no se haya realizado un análisis de riesgo previo. Ello constituye una posibilidad novedosa en el marco de este tipo de aplicaciones.

## Materiales y Métodos

Se utilizaron los sistemas tecnológicos requeridos para la explotación segura de la Central Nuclear de Embalse (CNE) [14], resultando incluidos en el análisis 21 sistemas. Estos comprenden 12 sistemas frontales y 9 sistemas soportes, de acuerdo con el convenio de identificación utilizado en los APS [6,9;10-12].

Las matrices de dependencias son herramientas que habitualmente se utilizan en los APS [9-11] como

ayuda para estudiar las interfaces de los sistemas y documentar sus puntos de enlace los que durante la reducción booleana de los modelos de fallos de secuencias accidentales y de sistemas, se convierten en dependencias comunes para varios sistemas, y resultan en general los principales contribuyentes a nivel de fallos de equipos en el APS.

La estructura de las matrices es simple y consta de una columna para identificar los equipos correspondientes al sistema objeto de análisis de dependencia y otras para colocar las diferentes interfaces según correspondan a diferentes tipos de soporte o enlace. Un ejemplo de este tipo de matriz se presenta en la tabla 1.

**Tabla 1.** Fragmento de matriz de dependencias para sistema de agua de emergencia de CNE

| Componentes del sistema analizado | Componentes / Sistemas Interfase |            |           |           |          |       |           |           |       |
|-----------------------------------|----------------------------------|------------|-----------|-----------|----------|-------|-----------|-----------|-------|
|                                   | 3463                             | 5434-MCC10 | 5433-MCC7 | 5433-MCC8 | 3431-TK1 | 63461 | 7342-FM17 | 7342-FM18 | 67314 |
| 3461-P1                           | X                                | X          | X         |           | X        | X     | X         |           |       |
| 3461-P2                           | X                                | X          |           | X         | X        | X     |           | X         |       |
| 3461-PV7                          |                                  |            |           |           |          | X     |           |           | X     |
| 3461-PV41                         |                                  |            |           |           | D        | X     |           |           | X     |

Las X significan interfaces de apoyo, y la D representa una interfaz de intercambio de fluidos. Los componentes que encabezan las columnas pertenecen a sistemas soportes o de otro tipo y son los equipos que realizan directamente la función de enlace. El sistema de identificación de equipos utilizados en este caso, establece que los primeros dígitos antes del guión identifican a los sistemas tecnológicos de la instalación, mientras que las letras corresponden a los tipos de equipos. De esta forma, P significa bomba centrífuga, PV válvula neumática, MCC centro de distribución de motores, TK tanque y FM ventilador de local.

Durante la realización del APS de CNE [14] se prepararon, en el marco de los informes de tarea, las matrices de dependencias de los sistemas, que incluyen las interfaces con los sistemas soporte (alimentaciones eléctricas de clase IV, clase III, clase II, clase I, energía de emergencia, agua de proceso, computadoras, contra incendio y aire comprimido).

Estas matrices de dependencias, unidas al estudio detallado de las políticas y principios de CNE y los criterios de fallo de los sistemas modelados, junto con los esquemas de los sistemas tecnológicos, eléctricos y de instrumentación y control de CNE, permitieron el completamiento de las tablas necesarias para alimentar al sistema de control de configuración de la central.

De esta forma, el completamiento con calidad de las tablas es un paso esencial en la aplicación de este método. Para llenar las celdas de las tablas se utilizan, los códigos alfanuméricos de identificación de equipos

y sistemas, así como otros códigos familiares a los operadores. El seguimiento de los códigos alfanuméricos de identificación de los equipos mediante sistemas computarizados es un método común utilizado en las tareas de gestión de la explotación en las instalaciones [5]. Este método de control exige el llenado de dos tipos de tablas:

- Sistemas-Criterios.
- Matrices de dependencias de sistemas.

La primera tiene la estructura presentada en la tabla 2. En ella se diferencian las columnas de identificación del Sistema de Código (preferiblemente simple requerido para su informatización), y una última columna de Criterio, que es una combinación de caracteres utilizada para describir las razones que caracterizan al fallo del sistema.

**Tabla 2. Sistemas-Criterios**

| No | Sistema                                                      | Código | Criterio                     |
|----|--------------------------------------------------------------|--------|------------------------------|
| 1  | Sistema de Parada 1 [31730, 68200]                           | SP1    | 3/26 B-E, 2/3 LOG, 2/3 SEÑ   |
| 2  | Sistema de Parada 2 [34710]                                  | SP2    | 3/3 LINEA, 2/3 SEÑ, 1 COL    |
| 3  | Sistema de barras absorbedoras [31770]                       | SBA    | 1/4 BARRA                    |
| 4  | Sistema de zonas líquidas [34800]                            | SZL    | 3/14 ZONA, 2/3 BOMBA         |
| 5  | Sistema de Control de Presión e Inventario [33310]           | SCI    | 2/2 BOMBA, 2 LCV, 2 PV-LCV   |
| 6  | Sistema de enfriamiento de emergencia del núcleo [34320]     | SEN    | 2 RED, 2 PV-RED, 4 MV-COL    |
| 7  | Sistema de protección de sobrepresión del secundario [63614] | SPS    | 5/16 MSSV                    |
| 8  | Sistema de agua de alimentación [43210, 43230]               | SAA    | 2/2 AUX, 2/3 PRI, 1 PRI-AUX- |

La matriz de dependencias tiene el formato desarrollado en la tabla 3. En cada fila se representan los datos de un componente, el cual aparecerá en la columna Equipo, mientras que las restantes columnas a la derecha corresponden a las interfaces necesarias para el funcionamiento este. Obsérvese que se han identificado necesidades de Enfriamiento, Alimentación Eléctrica (Clase IV, III, II y I), Aire de Instrumentos, Instrumentación y Control (IC) y otras, aunque desde el punto de vista informático estas posiciones resultan transparentes. Adicionalmente, se han identificado tres columnas previas:

- Sistema: se utiliza para identificar el Sistema al que pertenece el componente (de acuerdo con el Código de la tabla 2).
- Redundancia: es el criterio de éxito para la redundancia ubicada en la fila a la que pertenece el componente.
- IDE-Criterio: es el código o identificación (IDE) de criterio de fallo que corresponde al sistema para el componente en cuestión (de acuerdo con el Criterio establecido en la tabla 2).

**Tabla 3. Matriz de dependencias de Sistemas**

| No  | Sistema | Redun. | IDE-Criterio | Equipo   | Enfriam. | Clase IV | Clase III | Clase II | Clase I             | Aire Inst. | Otras                          | IC         |
|-----|---------|--------|--------------|----------|----------|----------|-----------|----------|---------------------|------------|--------------------------------|------------|
| 123 | SP2     |        |              | RETJ     |          |          |           |          |                     |            |                                | 68320-RL4J |
| 124 | SP2     | 2      |              | COL      |          |          |           |          | R1:3231-PV1/R2:3231 |            | 3231-CP1,3231                  |            |
| 125 | SBA     |        | BARRA        | 3177-CA1 |          |          |           |          | FS:5561-PL555       |            | R1:66400-CDX63732-RL54,63732-F |            |
| 126 | SBA     |        | BARRA        | 3177-CA2 |          |          |           |          | FS:5561-PL555       |            | R1:66400-CDX63732-RL55,63732-F |            |

El método de control de configuraciones propuesto se basa en el algoritmo presentado en la figura 1. El algoritmo se inicia con el LLENADO DE LAS MATRICES y una revisión cruzada independiente (COMPROBACIÓN CRUZADA) de los datos, para garantizar la calidad de la información disponible en las tablas con la que se tomarán decisiones respecto a la seguridad.

Una vez establecida la combinación de códigos de equipos indisponibles a chequear (ESTABLECIMIENTO DE CÓDIGO DE EQUIPO O COMBINACIÓN DE CÓDIGOS A ESTUDIAR) se determina si se realizará el RASTREO SIMPLE o RASTREO COMPLEJO de dichos códigos en la matriz. Un rastreo simple culmina con la determinación (LOCALIZACIÓN DE CÓDIGO) a nivel de la fila, o filas (donde está ubicado el componente) de la influencia de su indisponibilidad sobre el nivel correspondiente del sistema por ejemplo, una redundancia. La

importancia de la indisponibilidad queda codificada con un código de colores que se distingue en la columna Sistema de la tabla 3, apareciendo rojo subrayado (CELDA SISTEMA ROJO) si indisponen el componente, amarillo cursiva (CELDA SISTEMA AMARILLO) si afecta una redundancia (Rn), o verde subrayado discontinuo (CELDA SISTEMA VERDE) si lo conduce a fallo seguro (FS).

Por otra parte, el RASTREO COMPLEJO realiza un arrastre de la situación inicialmente descrita en el rastreo simple hacia el resto de los componentes que, como consecuencia de la situación de indisponibilidad inicial, cambian su estado por dependencias funcionales o directas, extrapolándose encadenadamente (con NUEVO CÓDIGO) a los restantes equipos relacionados en la tabla.

El establecimiento de la prioridad de estado (ver PRIORIDAD DE ESTADO...) tiene en cuenta la

influencia del estado (disparado, fallado o degradado) del componente antecesor en la cadena y el influjo de este en el nuevo nivel objeto de análisis (influencia directa, a través de redundancia o fallo seguro). También se considera la influencia sobre el fallo de otros componentes ubicados al mismo nivel, priorizándose el estado fallado sobre el degradado y este último sobre el disponible. Dada la posibilidad de existencia de componentes en estado disparado, durante el arrastre pueden aparecer también fallos

seguros de redundancias o viceversa (CELDA SISTEMA AQUA). Toda esta exploración es la que garantiza un análisis de la influencia de las dependencias afectadas, directa (por la combinación inicial de indisponibilidades), o indirectamente (por el arrastre de las dependencias), sobre todos los sistemas de la planta incluidos en la matriz. Este lazo aparece encerrado en un cuadro de líneas discontinuas en la figura 1 y se ha identificado como MÓDULO DE ARRASTRE DE DEPENDENCIAS.

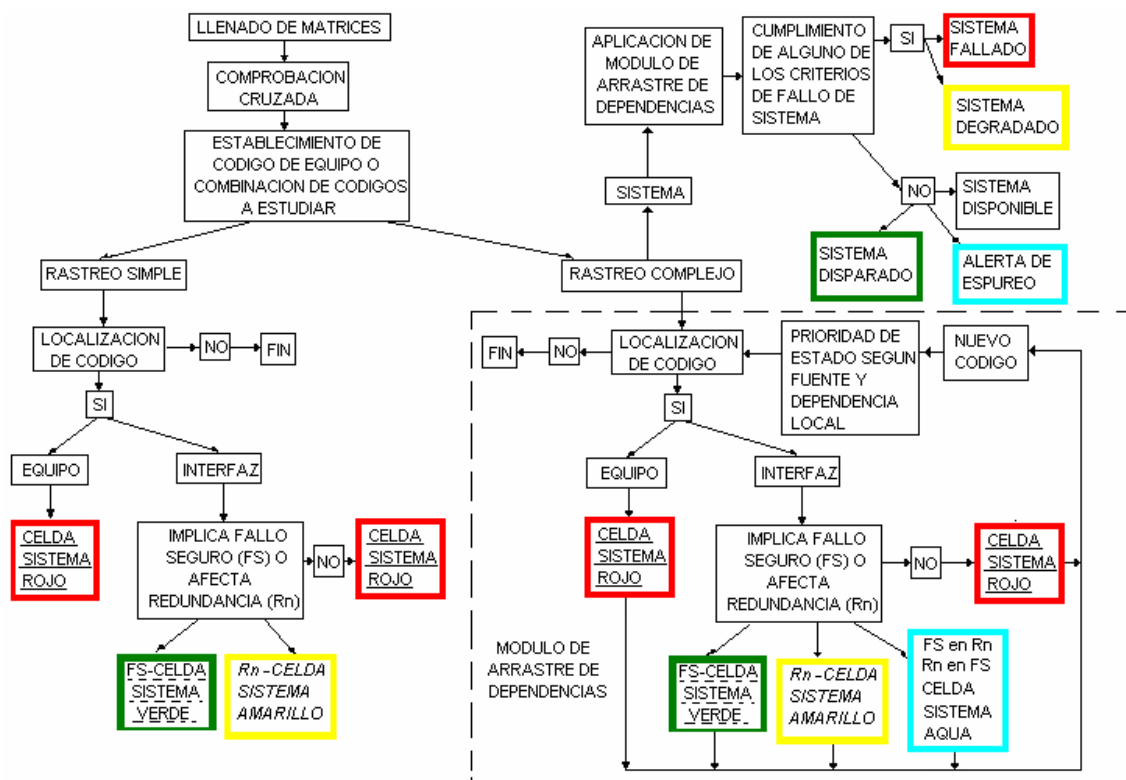


Figura 1. Algoritmo de control de configuraciones peligrosas.

Finalmente, si tras el RASTREO COMPLEJO se selecciona la opción sistema (ver SISTEMA), una vez concluido el paso anterior (APLICACIÓN DE MÓDULO DE ARRASTRE), se realiza un chequeo en toda la matriz de los criterios de fallos postulados para los sistemas (CUMPLIMIENTO DE CRITERIOS DE FALLO), de acuerdo con la tabla 2. Si se cumplen algunos de los criterios de fallo para los sistemas incluidos, estos se clasifican de acuerdo con su estado en un rango que va desde degradado hasta fallado (SISTEMA FALLADO o DEGRADADO). El estado DEGRADADO puede tener varios niveles de categorización (POCO DEGRADADO, DEGRADADO, MUY DEGRADADO) lo que corresponde a la magnitud de afectación de las redundancias,

mientras que en el estado disponible se pueden diferenciar categorías como DISPONIBLE, ALERTA DE ESPUREO y DISPARADO.

El algoritmo mostrado se ha informatizado a través de un código de computación (identificado como CONFIGURACIÓN), que permite realizar el seguimiento de configuraciones fuera de servicio de equipos con un enfoque cualitativo, práctico y de fácil acceso a los operadores, sin necesidad de disponer de personal especializado que maneje el APS ni herramientas complejas como un monitor de riesgo.

## Aplicación del algoritmo de control de configuración

El código CONFIGURACIÓN se ha aplicado a varios sistemas en CNE (12 sistemas frontales y 9 soportes) [14], algunos de ellos son:

Sistemas frontales:

- Sistema de Parada 1 (31730, 68200)
- Sistema de Parada 2 (34710)
- Sistema de enfriamiento de emergencia del núcleo (34320)
- Sistema de agua de emergencia (34610)
- Sistema del moderador (32110)

Sistemas soporte:

- Sistema de Clase III (52100, 53200)
- Sistema de computadoras (66400)
- Sistema de aire comprimido (75110)

La tabla de sistemas finalmente obtenida para CNE cuenta con 21 filas correspondientes a igual número de sistemas frontales y soportes. Por otra parte, la tabla o matriz de dependencias de los equipos de estos sistemas cuenta con más de 400 filas (que incluyen más de 1600 equipos), muchas de ellas interconectadas por las dependencias que quedan reflejadas a través de un adecuado sistema de codificación.

Para ejemplificar el uso del código de control de configuraciones se ha postulado una situación compleja como la indisponibilidad simultánea de varios equipos: 3432-P2, 7512-AS15 y 5561-PL559 que corresponden a una bomba del sistema de enfriamiento de emergencia, a una estación de distribución de aire comprimido y a un panel eléctrico de clase I o alimentación ininterrumpida. Estos equipos pertenecen a diferentes sistemas (frontales y soportes) de la central nuclear (figura 2). La indisponibilidad de equipos objeto de análisis se muestra en la Lista de Componentes indisponibles que aparece en la figura 2.

|     |     |   |           |  |                        |            |                      |              |           |                     |
|-----|-----|---|-----------|--|------------------------|------------|----------------------|--------------|-----------|---------------------|
| 179 | SEN | A | 3432-PV83 |  |                        |            | FS 5561-PL559        | FS 7512-S591 |           | 63432-SV83,63432-H  |
| 180 | SEN | A | 3432-PV84 |  |                        |            | FS 5561-PL560        | FS 7512-S592 |           | 63432-SV84,63432-H  |
| 181 | SEN | P | 3432-MV79 |  | 5433-MCC5-D5532-PL128  |            | 5561-PL559,5561-PL15 |              | 3432-MV71 | 63432-HS79,63432-R  |
| 182 | SEN |   | 3432-MV71 |  | 5433-MCC5-D5532-PL128  |            | 5561-PL559,5561-PL15 |              |           | 63432-HS171,63432-I |
| 183 | SEN | P | 3432-MV80 |  | 5433-MCC5-O15532-PL184 |            | 5561-PL560,5561-PL15 |              | 3432-MV72 | 63432-HS80,63432-R  |
| 184 | SEN |   | 3432-MV72 |  | 5433-MCC5-O15532-PL184 |            | 5561-PL560,5561-PL15 |              |           | 63432-HS172,63432-I |
| 185 | SEN | M | 3432-PV10 |  |                        |            | 5561-PL560           | R1 7512-AS15 | 3432-PV23 | 63432-HS78,63432-S  |
| 186 | SEN | M | 3432-PV11 |  |                        |            | 5561-PL559           | R1 7512-AS13 | 3432-PV24 | 63432-HS77,63432-S  |
| 187 | SEN | O | 3432-P1   |  | 5323-BUC               |            | 5561-PL559           |              |           | 63432-HS71,63432-R  |
| 188 | SEN | O | 3432-P2   |  | 5323-BUD               |            | 5561-PL560           |              |           | 63432-HS72,63432-R  |
| 189 | SEN | N | 3432-MV31 |  |                        | 5532-PL128 | 5561-PL1585,5561-PL5 |              |           | 63432-HS31,63432-R  |
| 190 | SEN | N | 3432-MV50 |  |                        | 5532-PL184 | 5561-PL1586,5561-PL5 |              |           | 63432-HS50,63432-R  |

Selecione componentes indisponibles

- 3432-MV80
- 3432-P1
- 3432-P2
- 3432-PV1
- 3432-PV10
- 3432-PV11
- 3432-PV2

Lista de componentes indisponibles

- 7512-AS15,5561-PL559
- 3432-P2
- 7512-AS15
- 5561-PL559

Rastreo Simple

Rastreo Complejo

Sistema

Salir

Legenda :

**INDISPONIBLE**

**PERD. REDUNDANCIA**

**FALLO SEGURO**

**FALLO SEGURO REDUND.**

ESTADO DE SISTEMAS

Busca

- SZL DISPONIBLE
- SCI DISPONIBLE
- SEN FALLADO
- SPS FALLADO
- SAA DISPONIBLE
- SEP DISPONIBLE

Figura 2. Chequeo de indisponibilidad simultánea de equipos en CNE.

Como se aprecia en la figura 2, con un sencillo sistema de codificación de colores (ver letras subrayadas y cursivas según orienta el algoritmo) el operador recibe una información cualitativa del estado de los diferentes equipos y sistemas de planta, al ocurrir la indisponibilidad inicial de alguna configuración de componentes. Este tipo de alerta no existía hasta la fecha en la central y para la tarea se dependía básicamente de la experiencia de los jefes de turnos o de personal experto de planta.

De esta forma, el sistema de control de configuración propuesto es capaz de detectar y encadenar a través de las diferentes interfaces los enlaces o dependencias entre equipos de sistemas frontales y soportes, resultando una aplicación de gran ayuda en la operación segura de la instalación nuclear.

A modo de comprobación, los resultados del rastreo anterior se compararon con los conjuntos mínimos de corte resultantes del APS para el sistema

de enfriamiento de emergencia (SEN). El sistema SEN, tomado como ejemplo ilustrativo, es un sistema redundante de dos líneas con 100% de capacidad de inyección cada una. Cada línea cuenta con sus válvulas neumáticas (PV) y bomba (P) para cumplir la función de inyección. A su vez, cada uno de los equipos necesita de interfaces de apoyo para operar. De esta forma las válvulas PV demandan, entre otras interfaces, de aire de instrumentos (reservado en cada una con las estaciones de aire AS y los tanques de aire TK), así como de alimentación de control representado por los paneles (PL). De manera similar las bombas necesitan, entre otras interfaces, de la alimentación de control (PL). El cruzamiento de los fallos o indisponibilidades de estos equipos e interfaces entre líneas redundantes, indisponen y degrada al sistema SEN.

**Tabla 4.** Comparación de resultados del APS de CNE y CONFIGURACIÓN

| Conjuntos Mínimos resultantes del APS de CNE                                                                                                                                                                                                                             | Combinación detectada por configuración (filas según figura 2) |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| 3432-P1.S * 3432-P2.S /<br>3432-P1.S * 3432-P2.R /<br>3432-P1.R * 3432-P2.S /<br>3432-P1.R * 3432-P2.R /<br>3432-P1.S * 5561-<br>PL560.F / 3432-P2.S *<br>5561-PL559.F / 3432-<br>P1.R * 5561-PL560.F /<br>3432-P2.R * 5561-<br>PL559.F / 5561-PL559.F<br>* 5561-PL560.F | 3432-P2 * 5561-PL559<br>(187 , 188)                            |
| 3432-PV1.0 * 3432-<br>PV2.0 / 5561-PL559.F *<br>5561-PL560.F / 7512-<br>AS15.F * 5561-PL559.F<br>* 7512-TK74#2                                                                                                                                                           | 7512-AS15 * 5561-<br>PL559 (185 , 186)                         |

La tabla 4 muestra solamente las configuraciones de interés para el ejemplo, detectadas por el código CONFIGURACIÓN para el sistema SEN (ver filas 185, 186, 187 y 188 en la figura 2), partiendo de las combinaciones inicialmente introducidas, mientras que, en aras de simplificar la demostración, sólo se muestran unos pocos conjuntos mínimos resultantes del APS de CNE (se subrayan los que sirven de base a la comparación). La coincidencia entre conjuntos mínimos y combinaciones en las columnas de la tabla 4 permite comprender la potencialidad del método. El estado final de los sistemas se aprecia en el extremo inferior derecho de la figura 2.

En la tabla 4 se muestra cómo el operador puede detectar casos de redundancias degradadas como la segunda configuración presentada (filas 185 y 186). En este caso, mientras que la válvula 3432-PV11 falla al

indisponerse su panel de alimentación de control 5561-PL559, la válvula 3432-PV10 simétrica en la línea redundante, se degrada al perderse una de sus reservas de aire comprimido (estación 7512-AS15, manteniéndose disponible el tanque de aire 7512-TK74#2). Por otra parte, el estado final fallado del SEN corresponde con la configuración de indisponibilidades de las filas 187 y 188. Para este caso, el fallo o indisponibilidad de la bomba 3432-P2 es directo (de acuerdo con la configuración inicial de equipos fuera de servicio) mientras que la indisponibilidad de la bomba 3432-P2 (simétrica en la línea redundante) se induce por el fallo de su interfaz de alimentación de control 5561-PL559.

## Conclusiones

El sistema de detección de configuraciones peligrosas propuesto, aún sin alcanzar las capacidades de determinación de conjuntos mínimos de corte, pues sólo se analizan configuraciones predefinidas, es capaz de detectar de manera conservadora combinaciones peligrosas de equipos fuera de servicio, y alertar con carácter preventivo antes de su consecución. Su capacidad de trabajo, independientemente de la realización de análisis de riesgo previos, constituye una posibilidad novedosa.

El sistema se caracteriza por su simplicidad, muy bajos requerimientos de especialización para su comprensión y explotación, así como por una información de partida más limitada y accesible que la comúnmente utilizada para realizar APS y sus aplicaciones. Por ello, resulta idóneo para aquellas instalaciones donde no se han realizado análisis cuantitativos de riesgo.

El algoritmo se puede considerar también como un paso intermedio antes de contar con las potencialidades de los resultados de un APS o de un monitor de riesgo a plena capacidad. Sin embargo, se puede utilizar en paralelo con estas herramientas, aprovechando las ventajas que lo distinguen en contraste con ellas. De hecho, su implementación se facilita si ya se ha ejecutado un análisis de riesgo previo.

Una primera versión del código CONFIGURACIÓN se utiliza actualmente como consejero en la Central Nuclear de Embalse para determinar combinaciones de equipos fuera de servicio peligrosas para la explotación segura de la instalación.

## Referencias Bibliográficas

- [1] SAMANTA PK, MANKAMO IS, VESELY WE. *Handbook of Methods for Risk-Based Analyses of Technical Specification*, U.S. Washington DC: Nuclear Regulatory Commission, 1994. p. 3-1 to 3-22, p. 5-1 to 6-18. NUREG/CR-6141, BNL-NUREG 52398.
- [2] SAM SAMDANI G. *Safety & Risk Management Tools & Techniques in the Chemical Processes Industry*. New York: McGraw Hill, 1996. p. 57-67.
- [3] US-NRC. *Commission Briefing Proposed Rulemaking. Technical Specifications*. 10 CFR 50.36. USA: CFR, 1994.
- [4] US-NRC. *Maintenance Rules*. 10 CFR 50.65. USA: CFR, 1993.
- [5] TORRES VALLE Antonio. *Mantenimiento Orientado a la Seguridad*. Primera Edición. La Habana: CUBAENERGIA, 2006. ISBN 959-7136-10-4. p. 282 – 303.
- [6] TORRES A, PERDOMO M. *Seguridad Ambiental, Salud Ocupacional y Garantía de Calidad. Retos de la Industria Moderna* [en línea]. Universidad Nacional de Córdoba, 2008. <<http://www.efn.uncor.edu/investigacion/reactor>> [consulta: 25 de mayo del 2010] (ver Novedades).
- [7] COX S, TAIT R. *Safety, Reliability and Risk Management: an integrated approach*. Second Edition. Oxford: Butterworth – Heinemann, 1998. ISBN 0-7506-4016-2. p. 290–315.
- [8] KAFKA P. «Probabilistic Risk Assessment for Nuclear Power Plant». En *Handbook of Performability Engineering*. London: Springer. 2008. ISBN 978-1-84800-130-5. p. 1179-1192.
- [9] FULLWOOD RR. *Probabilistic Safety Assessment in the Chemical and Nuclear Industries*. Second Edition. Oxford: Butterworth – Heinemann, 2000. ISBN 0-7506-7208-0. p. 97–122.
- [10] IAEA. *Procedures for Conducting PSA in NPP*. Safety Series No. 50-P-4. Vienna: IAEA, 1992.
- [11] US-NRC. *Probabilistic Safety Analysis Procedures Guide*. NUREG/CR-2815. 1985.
- [12] SMITH DJ. *Reliability, Maintainability and Risk. Practical Methods for engineers*. Second Edition. Oxford: Butterworth–Heinemann, 2001. ISBN 0-7506-5168-7. p. 128-144,
- [13] TORRES VALLE A, RIVERO OLIVA, J. Gestión de Mantenimiento Orientado a la Seguridad. *Revista Ingeniería Mecánica*. 2004; 7(2): 7-15.
- [14] TORRES A, PERDOMO M, SALOMÓN J, RIVERO J. Grupo de Análisis de Riesgo y Confiabilidad de Cuba: 20 años de experiencia en los servicios de análisis de seguridad, confiabilidad y mantenimiento [monografía en internet]. 2009. <<http://www.monografias.com/trabajos-pdf2/analisis-riesgo-confiabilidad-seguridad-mantenimiento/analisis-riesgo-confiabilidad-seguridad-mantenimiento.shtml>> [consulta: 25 de mayo del 2010].

**Recibido:** 16 de marzo de 2010

**Aceptado:** 13 de mayo de 2010