FIABILIDAD HUMANA

J. E. DIEZ

José Enrique DIEZ MORENO es licenciado en Física por la Universidad Complutense en 1964.
Hasta primeros de 1986 trabajó en la Junta de Energía Nuclear, siendo Supervisor de Operación de los reactores JEN-1 y JEN-2, responsable de la Instrumentación y Control, y Jefe del Grupo de Mantenimiento. Ha sido profesor en el Instituto de Estudios Nucleares y participado en proyectos nacionales e internacionales de diseño y modificación de reactores experimentales.
Actualmente pertenece a la Dirección Nuclear de UNESA como Coordinador del Programa Investigación y Desarrollo en el área nuclear. Desde abril de 1989 es Presidente del Comité de Dirección del Banco de Datos de Fiabilidad de Componentes de las Comunidades Europeas (CEDB).

¿ESO QUE ES?

En los últimos tiempos se vienen repitiendo con cierta frecuencia algunas frases o expresiones que, situadas en la frontera entre lo inquietante y lo atractivo, su solo enunciado puede en muchos casos provocar la perplejidad del interlocutor y casi siempre parecen obtenidas por el método de la selección aleatoria de palabras de varias columnas, pero que en el fondo encierran una significación profunda y arrastran tras de sí un esfuerzo considerable de investigación y estudio. Nos referimos a frases como, por ejemplo, "Evaluación de riesgo", "Análisis probabilista de Seguridad" o "Interfase Hombre-Máquina", que han llegado a formar parte integrante de la jerga de los especialistas, si bien al pueblo común y llano, aunque culto, siempre le suscita la misma pregunta: "¿Y eso qué es?"

Al hablar de "fiabilidad humana" bueno sería comenzar por eliminar fuentes de confusión tratando de dar una definición clara de esta expresión que explique el sentido en que se utilizará en este trabajo. Lo más sencillo es recurrir al diccionario, en el que puede leerse: "Fiabilidad: 1. Calidad fiable, 2. Probabilidad de buen funcionamiento de una cosa". Así que, salvando las distancias entre los humanos y las cosas, se entiende por fiabilidad humana la capacidad del hombre para realizar, en determinado plazo de tiempo y en condiciones preestablecidas, una función que le ha sido requerida; esta capacidad es una magnitud medible en términos de probabilidades de acierto o de no fallo.

El interés por el estudio de la fiabilidad humana representa un ejemplo típico de una noble y ancestral aspiración del hombre manifestada en el espíritu de superación por la vía de aprender de los propios errores. Así nos encontramos con que un cierto número de accidentes graves ocurridos en diferentes sectores industriales como el químico, el transporte, la energía nuclear o la navegación espacial, por citar algunos ejemplos típicos, han concentrado la atención de los investigadores y de los estudiosos sobre la influencia del comportamiento humano en la fiabilidad y en la seguridad de las instalaciones. Los esfuerzos se concentran en la elaboración de programas orientados a la adquisición de conocimientos sobre el comportamiento de los operadores y a la modelación de su conducta. Antes de entrar en los pormenores de esta materia debemos admitir que nos enfrentamos a una actividad muy compleja, tanto como la propia mente, en que se contemplan disciplinas tan variopintas como la psicología, la ergonomía, la sociología y la psicopatología del trabajo.

EVALUACION DEL RIESGO

A partir de ahora vamos a concentrar nuestra atención en las centrales nucleares, aunque la mayoría de los argumentos empleados sean aplicable a todo tipo de sistemas industriales complejos. Hoy en día está generalmente admitido que el método más eficaz para evaluar el riesgo de estas instalaciones consiste en determinar por una parte la probabilidad total de ocurrencia de un accidente grave y por otra parte, las consecuencias derivadas del mismo, para después efectuar el producto de ambas. El resultado será una estimación de los valores esperados de daños a la población o de perjuicios económicos al propietario de la central según el tipo de consecuencias estimadas. Por accidente grave, o accidente severo, como es más comúnmente conocido, se entiende aquél en el que se produce una fusión total o parcial del núcleo del reactor con liberación incontrolada de productos de fisión fuera del confinamiento de las vainas del combustible. En la evaluación de la probabilidad de ocurrencia de tal clase de accidentes se tienen en cuenta todos los posibles sucesos y secuencias accidentales, combinando sus probabilidades mediante el uso de una tecnología conocida como "Análisis Probabilista de Seguridad", o abreviadamente, APS.

La experiencia nos muestra que las acciones humanas tienen notable importancia en el riesgo total inherente a las centrales o, dicho de otra forma, que determinados errores cometidos por los operadores de la planta contribuyen significativamente a la probabilidad total de daño severo al núcleo, de ahí que una evaluación de la fiabilidad humana sea esencial en los estudios de APS. No obstante, y por su propia naturaleza, resulta extremadamente difícil y complejo modelar el comportamiento humano de forma que puedan estimarse las probabilidades de fallo de los operadores, ya

que las teorías de fiabilidad, tal y como se aplican a sistemas y componentes, no sirven de modelo en este caso. Por ello se investiga mucho en este campo y se dedican muchos esfuerzos y recursos, a nivel internacional, a diversos tipos de estudios con orientaciones claramente diferenciadas. De ellos merecen nuestra atención tanto los que buscan la integración de modelos validados de comportamiento humano en los análisis de seguridad, como aquéllos que desarrollan y validan sistemas de ayuda al operador con objeto de reducir su probabilidad de fallo y, con ello, la influencia de sus actuaciones en la seguridad de la central.

ERRORES HUMANOS

Todos los métodos de estimación de la fiabilidad humana pasan por una etapa previa de identificación y clasificación de aquellos errores que pueden cometer los operadores que afectan, real o potencialmente, a la seguridad. La alternativa más comúnmente utilizada en la actualidad establece dos categorías fundamentales en los procesos que intervienen en el comportamiento: el nivel más alto es un proceso cognoscitivo de interpretación, diagnóstico y toma de decisión; el nivel más bajo incluye el proceso de percepción y ejecución de acciones de respuesta. Desde luego es forzoso pensar que esto no es nada nuevo, sino que, muy al contrario, nos encontramos ante la antiquísima clasificación de los trabajadores entre los que "piensan" y los que "ejecutan los trabajos", con la salvedad de que los operadores deben actuar en ambas parcelas. Esta división conduce a dos tipos de errores humanos según cual sea el proceso en el que se produce: el error de diagnóstico, o confusión ("mistake" en terminología inglesa) y el error de actuación, o desliz ("slip"). Ambas clases de error pueden darse en operación normal, durante transitorios accidentales o después del accidente, durante las acciones correctoras o de recuperación de la planta, si bien los deslices durante la operación normal y las confusiones en situación de emergencia son los errores más frecuentes.

En efecto, durante la operación normal se realizan tareas rutinarias de pruebas o mantenimiento, normalmente bien definidas en los procedimientos y en las órdenes de trabajo específicas, de forma que no hay lugar para la confusión y, en cambio, la distracción o la pérdida de atención consecuencia de la rutina puede dar lugar a deslices asociados a una incorrecta actuación física. Por el contrario, en situación accidental la atención está garantizada, así como la vigilancia de las acciones de los operadores de modo que un desliz es muy poco probable y, en todo caso sería detectado y corregido fácilmente. Sin embargo, la falta de conocimiento, la interpretación incorrecta de las indicaciones del sistema de control, la duda o la incertidumbre pueden originar confusiones.

Un nuevo recurso a la experiencia, combinada con los resultados de los APS, para afirmar que la contribución al riesgo de los deslices es muy pequeña frente a la significativa contribución de las confusiones. Por eso los estudios más importantes se concentran exclusivamente en el análisis de este tipo de errores. Contrariamente a lo que ocurre con los deslices, las confusiones están fuertemente condicionadas por el tiempo. De hecho las técnicas más avanzadas se basan en establecer correlaciones fiabilidad-tiempo obtenidas reproduciendo en simuladores de escala total diferentes transitorios accidentales y evaluando probabilidades de error de los operadores en función de los tiempos disponibles para la actuación. Además, las correlaciones se tipifican teniendo en cuenta otros factores que pueden influir decisivamente en la respuesta de los operadores como son la complejidad de las acciones a realizar, el estrés, el nivel de entrenamiento y la calidad del sistema de interacción Hombre-Máquina, por citar algunos ejemplos típicos.

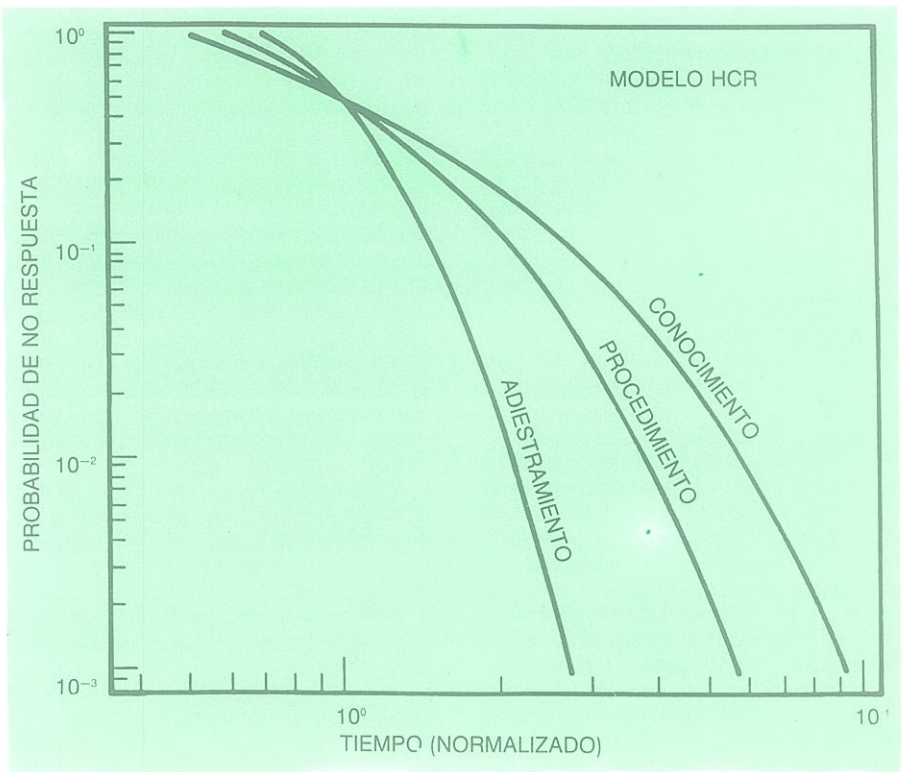
TECNICAS DE ANALISIS

Los analistas emplean diversas técnicas consistentes en metodologías para la evaluación de las probabilidades de error humano y su integración en el APS de la central, de modo que puedan identificarse aquellas actuaciones de los operadores que tienen mayor incidencia en la seguridad de la planta. Esto es algo que técnicamente se llama valoración de la calidad de la interacción Hombre-Máquina.

Algunas de estas técnicas las citaremos a continuación a título de ejemplos ilustrativos, obviando todo tipo de descripción detallada por caer fuera del alcance de este trabajo. Comenzamos por la técnica de predicción de la tasa de error humano, conocida por las siglas THERP correspondientes a la denominación en lengua inglesa. Se trata de la técnica tal vez más conocida y más comúnmente aceptada, que se utilizó por primera vez en el "Reactor Safety Study" y más tarde se ha empleado en estudios de APS para modelar el comportamiento humano. Contiene métodos para evaluar los factores que conforman el comportamiento, modelos para establecer relaciones entre las tareas y bases de datos para cuantificar las probabilidades de error humano. La técnica puede aplicarse a cualquier situación, pero el proceso es muy laborioso y complejo por lo que se ha desarrollado un modelo simplificado, el Programa para la evaluación de secuencias accidentales (ASEP), más manejable y práctico, aunque menos preciso.

Otra técnica, desarrollada por NUS Corporation bajo el patrocinio del EPRI es la de Fiabilidad de los procesos cognitivos humanos (HCR). Desarrolla un modelo

F I. *Curvas normalizadas de no-respuesta para los diferentes tipos de procesos cognitivos.*



analítico para la determinación de probabilidades de fallo de los equipos de operación, y su aplicación a los APS. En general, el modelo es compatible con las técnicas utilizadas en APS y de fácil manejo, considera diferentes procesos cognitivos, identifica los distintos factores que modifican el comportamiento y establece las correlaciones entre la probabilidad de fallo y el tiempo. Basándose en el modelo de Rasmunssen establece que los procesos cognitivos humanos pueden clasificarse en los tres conocidos tipos de "Adiestramiento", "Procedimiento" y "Conocimiento", y formula que el comportamiento de los operadores puede representarse por curvas normalizadas de fiabilidad-tiempo como las que se presentan en la figura I. No obstante, hay que señalar que el método no es completo y requiere el concurso de otros adicionales para la determinación de la probabilidad global de no respuesta, además de que no está totalmente validado y su aplicación arrastra incertidumbres.

En muchos casos ocurre que la estimación de los valores de probabilidad de error humano en los análisis de fiabilidad tiene que basarse en los llamados juicios de expertos, en los cuales un número indeterminado de personas, que saben y entienden del asunto, asignan a sucesos o tareas determinadas valores numéricos siguiendo un proceso que responde al curioso nombre de la "Ponderación psicológica", y que emplea técnicas de comparación entre pares, clasificaciones por categorías o estimaciones numéricas para, posteriormente, y mediante el uso de ciertas correlaciones, estimar las probabilidades de fallo.

Por último, entre las técnicas que requieren juicios de expertos no queremos dejar de citar la inquietante "Matriz de Confusión" que desde el año 1981 se ha venido aplicando en numerosos PSA para determinar probabilidades de error de los operadores en situaciones de accidente donde, ciertamente, la confusión es más probable.

SISTEMAS DE AYUDA AL OPERADOR

En este apartado trataremos de adentrarnos en la otra faceta de la fiabilidad humana relacionada con la investigación y el desarrollo de los llamados sistemas de ayuda al operador, que tratan de reducir las probabilidades de ocurrencia de errores o fallos. La función principal de estos sistemas es la de facilitar información en relación con el estado actual de la central, identificando las estrategias operacionales a seguir en cualquier situación específica. Gran número de ellos se han desarrollado en la actualidad, y se aplican en los diversos estados que pueden presentarse como operación normal, transitorios y situaciones accidentales, y con distintos propósitos. Los más comúnmente empleados se presentan resumidos en la tabla de la figura II en donde se indican las áreas de aplicación respectivas.

	DIAGNOSTICO	PLANIFICACION	ACTUACION
OPERACION NORMAL	SCORPIO: Vigilancia del Núcleo	SCORPIO	COPMA: Informatización de procedimiento
SITUACION ANORMAL	HALO: Gestión de Alarmas EFD: Detección temprana DISKET: Diagnóstico DDP: Diagnóstico detallado	DDP	COPMA
ACCIDENTE	CFMS (C-E): Vigilancia de las funciones críticas	SMPS (C-E): Línea de éxito	COPMA

F II. *Sistemas de ayuda al operador clasificados según las áreas de aplicación.*

El sistema de vigilancia del núcleo en operación normal SCORPIO ("Surveillance of reactor core by picture on-line display") tiene dos funciones principales, la predictiva y la de vigilancia, funciones que permiten al operador mejorar el conocimiento del estado del núcleo y obtener información detallada sobre márgenes de operación y distribución de potencia. Este sistema está especialmente diseñado para ayudar al operador durante la operación normal de la central. No obstante, existe la certeza de que cuando más necesaria es esta ayuda es precisamente en las primeras etapas de los transitorios que conducen a situaciones accidentales, en las cuales se dan cita los más críticos procesos de decisión, por lo que otros sistemas como el de gestión de alarmas HALO (Handling Alarms Using Logic) se ha desarrollado con el fin de conseguir una presentación simplificada y comprensible del estado de la planta facilitando la información en dos niveles, el uno de carácter general y detallado el otro, contribuyendo significativamente a las tareas de un adecuado diagnóstico.

En muchos casos el problema al que se enfrenta el operador es el de seleccionar el procedimiento a aplicar más adecuado a la situación actual de la planta, selección que se ve facilitada considerablemente con el uso de sistemas que, como el COPMA, mantienen informatizados todos los procedimientos escritos, ofreciendo el ordenador las diversas alternativas según los casos.

Un paso más en esta labor de apoyo a la toma de decisión, que permite la ampliación de los tiempos de respuesta del operador, lo proporcionan los sistemas de "detección temprana de fallo" como el EFD, basado en modelos matemáticos que describen el comportamiento dinámico de los subsistemas de proceso en condiciones operativas normales. El modelo es capaz de predecir desviaciones de la normalidad mucho antes de que actúen los sistemas de alarma, facilitando considerablemente la localización y el diagnóstico del problema. Otros sistemas como el DISKET, desarrollado por el Instituto de Investigación de Energía Atómica de Japón (JAERI), o el DDP (Detailed Diagnosis and Prognosis), realizan directamente el diagnóstico de la planta usando sistemas expertos; el primero se basa en el análisis de las indicaciones de los sistemas de alarma, mientras que el segundo establece conclusiones a partir de la información proporcionada por los sistemas de detección temprana de fallo.

Finalmente, nos vamos a referir a otro tipo de sistemas de ayuda al operador, con objetivos más avanzados que no se limitan a la detección o el diagnóstico de fallos o transitorios, sino que, utilizando bases de datos de conocimiento y sistemas expertos, proporcionan recomendaciones efectivas sobre las acciones a tomar en caso de un transitorio; ello resulta muy eficaz sobre todo en aquellas situaciones en que no existe procedimiento escrito. Tal es el caso del SPMS (Success Path Monitoring System), desarrollado por Combustion Engineering bajo el patrocinio del EPRI.

EL REACTOR HALDEN Y SUS PROYECTOS

No debemos terminar este trabajo sin referirnos al proyecto Halden, por su importante significación en lo que han constituido los recientes avances en la investigación en Fiabilidad Humana. El reactor Halden tiene la particularidad de que fue diseñado y construido antes de que la primera central nuclear entrase en operación comercial en el mundo. En el año 1957, y esto es ciertamente historia, la agencia de la energía nuclear (NEA) de la OCDE lanzó la idea de acometer un programa común europeo de investigación en energía nuclear lo que condujo a analizar la posibilidad de convertir el reactor Halden, entonces en construcción en una empresa conjunta. El año siguiente se estableció finalmente el primer programa experimental Halden, de cinco años de duración, patrocinado

por diversos centros nucleares de varios países agrupados en la NEA. Este primer programa ha sido sucesivamente ampliado por programas trienales, el último de los cuales ha comenzado el presente año y en el que España ha sido invitada a participar.

Actualmente el proyecto consta de dos áreas bien definidas, la primera de ellas, que se refiere al comportamiento del combustible y ensayos de materiales, no será objeto de nuestra atención, centrándonos en la segunda que trata de factores humanos. Los esfuerzos desarrollados en la investigación de sistemas Hombre-Máquina han pasado por varias etapas enfocadas a intereses concretos y han ido evolucionando con el uso y la aplicación de computadores en el control de los procesos.

En términos muy generales se puede establecer que el objetivo básico que se persigue con las investigaciones es el de evitar que se produzcan errores de los operadores facilitándoles las tareas de toma de decisión y mejorando los sistemas de presentación de la información en la sala de control. Para ello se han establecido dos líneas principales de actuación relacionadas con la interacción Hombre-Máquina y el desarrollo de sistemas de ayuda al operador, y se ha creado un laboratorio, conocido por el acrónimo HAMMLAB, dotado de un simulador PWR de alcance total y de dispositivos de observación sistemática de la conducta de los operadores. En este laboratorio trabajan un grupo amplio de especialistas, en el que se incluyen psicólogos, sociólogos e informáticos, en el desarrollo y evaluación de técnicas de presentación de la información y sistemas de ayuda al operador.

Desde el año 1985 las prioridades se han orientado al incremento del uso de sistemas expertos y de técnicas de modelación matemática. La aparición de las nuevas generaciones de computadores ha facilitado el crecimiento, en número y complejidad, de los sistemas informatizados de ayuda al operador desarrollados y validados gracias al uso del HAMMLAB.

El programa de investigación formulado para el presente trienio 1991-93 está particularmente orientado a problemas relacionados con la fiabilidad de los sistemas informatizados de ayuda al operador, como son la verificación del contenido de las bases de conocimiento, la validación de la interfase Hombre-Máquina y la fiabilidad del "software". Por otra parte, continuarán las actividades relacionadas con el desarrollo de sistemas informatizados de diagnóstico, de aplicación de procedimientos y de asesoría al operador; en éstos se incluyen de forma especial los sistemas gráficos de presentación de información y de comunicación con el ordenador. Finalmente, otros aspectos del programa contemplan la integración de los diversos sistemas de control y vigilancia, actividad que se lleva a cabo mediante el desarrollo de un prototipo denominado ISACS (Integrated Surveillance and Control System), que se espera puede realizar diversas funciones de ayuda al operador, como detección de anomalías, diagnósticos y planificación de actuaciones.

CONCLUSION

Hay un antiguo proverbio chino que dice que "si miras al gusano te pierdes el eclipse" que si bien puede interpretarse como una manifestación de la imposibilidad de encaminarse simultáneamente en direcciones opuestas, también nos trae la profunda enseñanza de que si nos entretenemos con las cosas insignificantes perderemos el tren que puede conducirnos a empresas de más alto valor. Y esto viene a cuento porque ya se han realizado en España diversos esfuerzos, de dudoso éxito y reducido alcance, en el área de la fiabilidad humana. La importancia y la trascendencia de este tema, los cuantiosos recursos y elevadas inversiones que se requieren para afrontarlo con seriedad exigen en muchos casos el establecimiento de programas de cooperación internacional como el mencionado Halden. Si tenemos, como es de esperar, la sana aspiración de "contemplar el eclipse", deberíamos comenzar aprovechando las oportunidades que nos brindan.